GRUNDLAGEN DER ALGEBRA

Notizen zur Vorlesung im Sommersemester 2010
Universität Stuttgart, Studiengang Mathematik

Rohfassung
compiliert am 10. Januar 2011

www.igt.uni-stuttgart.de/eiserm

Für die Mitteilung von Unklarheiten und Fehlern aller Art
sowie für Vorschläge und Kritik bin ich stets dankbar!

Inhaltsverzeichnis

Kapitel 0. Vorwort i

Kapitel 1. Konstruktion mit Zirkel und Lineal 1
§1A. Was können wir mit Zirkel und Lineal konstruieren? – §1B. Von der Geometrie zur Algebra. – §1C. Algebraische Antworten auf geometrische Fragen. – §1D. Wie geht es weiter? – §1E. Übungen und Ergänzungen.

I Grundlagen der Ringtheorie

Kapitel 2. Monoide und Gruppen 15
§2A. Einführung und Überblick. – §2B. Verknüpfungen. – §2C. Monoide. – §2D. Gruppen. – §2E. Kommutativität. – §2F. Der Satz von Cayley. – §2G. Quotientenstrukturen. – §2H. Freie Monoide und freie Gruppen. – §2I. Übungen und Ergänzungen.

Kapitel 3. Ringe und Körper 47
§3A. Ringe und Körper. – §3B. Homomorphismen. – §3C. Integritätsringe und Bruchkörper. – §3D. Ideale und Quotientenringe. – §3E. Neue Ringe aus alten. – §3F. Der chinesische Restsatz. – §3G. Monoidringe. – §3H. Übungen und Ergänzungen.

Kapitel 4. Polynomringe 79
§4A. Definition und universelle Eigenschaft. – §4B. Gradfunktion und euklidische Division. – §4C. Faktorisierung von Nullstellen. – §4D. Übungen und Ergänzungen.

Kapitel 5. Teilbarkeitstheorie in Integritätsringen 89
§5A. Motivation. – §5B. Grundbegriffe. – §5C. Euklidische Ringe. – §5D. Hauptidealringe. – §5E. Faktorielle Ringe. – §5F. Teilerfremdheit und Invertierbarkeit. – §5G. Primideale und maximale Ideale. – §5H. Übungen und Ergänzungen.

Kapitel 6. Primfaktorzerlegung in Polynomringen 111
§6A. Motivation und Überblick. – §6B. Primfaktorzerlegung. – §6C. Exponentenbewertung und Normierung. – §6D. Inhalt und Normierung von Polynomen. – §6E. Der Satz von Gauß. – §6F. Fortsetzung des ggT von einem Ring R auf den Polynomring $R[X]$. – §6G. Irreduzibilitätskriterien. – §6H. Übungen und Ergänzungen.

Kapitel 7. Matrizenringe und der Elementarteilersatz 135
§7A. Einführung und Motivation. – §7B. Matrizenringe. – §7C. Die Determinante. – §7D. Der Algorithmus von Gauß–Bézout. – §7E. Eindeutigkeit der Elementarteiler.

Kapitel 8. Moduln und Vektorräume 153
§8A. Motivation und Überblick. – §8B. Moduln über einem Ring. – §8C. Quotientenmoduln und Isomorphiesätze. – §8D. Basen und freie Moduln. – §8E. Moduln über Hauptidealringen. – §8F. Vektorräume. – §8G. Beispiele, Anwendungen, Übungen.

II Grundlagen der Gruppentheorie

Kapitel 9. Grundbegriffe der Gruppentheorie 175
§9A. Der Satz von Lagrange. – §9B. Normale Untergruppen und Quotientengruppen. – §9C. Kommutieren. – §9D. Zyklische Gruppen. – §9E. Konjugation und innere Automorphismen. – §9F. Operationen. – §9G. Übungen und Ergänzungen.

Kapitel 10. Symmetrische und alternierende Gruppen 197
§10A. Die symmetrische Gruppe. – §10B. Zykelzerlegung. – §10C. Die Signatur. – §10D. Die alternierende Gruppe. – §10E. Einfache Gruppen. – §10F. Semidirekte Produkte. – §10G. Übungen und Ergänzungen.

Kapitel 11. Sylow–Sätze und Anwendungen 221
§11A. Einführung und Überblick. – §11B. Die Sylow-Sätze. – §11C. Einfache Klassifikationssätze. – §11D. Auflösbare Gruppen. – §11E. Übungen und Ergänzungen.

III Grundlagen der Körpertheorie

Kapitel 12. Körpererweiterungen 233
§12A. Einleitung und Überblick. – §12B. Körpererweiterungen. – §12C. Algebraische Erweiterungen. – §12D. Zerfällungskörper. – §12E. Algebraischer Abschluss. – §12F. Übungen und Ergänzungen.

Kapitel 13. Endliche Körper 253
§13A. Einführung und Überblick. – §13B. Klassifikation endlicher Körper. – §13C. Konstruktion endlicher Körper. – §13D. Übungen und Ergänzungen.

Kapitel 14. Der Hauptsatz der Galois-Theorie 265
§14A. Einleitung und Überblick. – §14B. Separable Erweiterungen. – §14C. Normale Erweiterungen. – §14D. Galois-Gruppe einer Gleichung.

Kapitel 15. Anwendungen der Galois-Theorie 283
§15A. Konstruierbarkeit mit Zirkel und Lineal. – §15B. Auflösbare Erweiterungen.

KAPITEL 0

Vorwort

Was ist und was soll die Algebra?

Mathematik ist die Lehre von Zahlen und Figuren. Über die Jahrhunderte hat sich eine Erfahrung herausgebildet und erhärtet: mathematische Methoden lassen sich erstaunlich erfolgreich auf eine Fülle von natürlichen Phänomenen und menschlichen Aktivitäten anwenden. Eine typische Anwendungen sind Gleichungen, und die Algebra ist, grob gesagt, die mathematische Theorie zum Lösen von Gleichungen. Sie untersucht dazu die Struktur der Rechenoperationen und der zugehörigen Objekte.

Die Algebra ist die mathematische Theorie zum Lösen von Gleichungen. Wir werden uns dieses Semester vor allem mit polynomiellen Gleichungen beschäftigen:

$$\begin{aligned} a_1X + a_0 &= 0 \\ a_2X^2 + a_1X + a_0 &= 0 \\ a_3X^3 + a_2X^2 + a_1X + a_0 &= 0 \\ a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 &= 0 \\ a_5X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 &= 0 \\ &\text{etc.}\ldots \end{aligned}$$

Das einfachste Beispiel sind Gleichungen der Form $a \cdot x + b = 0$. Für $a \neq 0$ hat diese Gleichung die Lösung $x = -b/a$. Die hierzu nötigen Operationen $+$ und $\cdot$ und ihre Inversen $-$ und $/$ führen unmittelbar zum algebraischen Begriff des Körpers. Lineare Gleichungssysteme über einem Körper werden in der linearen Algebra untersucht.

In dieser Vorlesung werden wir uns mit nicht-linearen, und zwar polynomiellen Gleichungen beschäftigen. Das einfachste und bekannteste Beispiel ist die quadratische Gleichung $ax^2 + bx + c = 0$. Für $a \neq 0$ hat diese Gleichung zwei Lösungen, und diese können durch die berühmte Formel $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ ausgedrückt werden. Diese Formel nutzt neben den Körperoperationen nur das Ziehen von Quadratwurzeln. In diesem Sinne ist die quadratische Gleichung also "durch Wurzeln auflösbar".

Ähnliche Lösungen für Gleichungen dritten Grades wurden von den italienischen Mathematikern Nicolo Tartaglia (1499–1557) und Gerolamo Cardano (1501–1576) gefunden,

und Gleichungen vierten Grades wurden von Cardanos Schüler Lodovico Ferrari (1522–1565) gelöst. Diese Lösungsformeln sind zwar zunehmend kompliziert, benutzen aber nur die Körperoperationen und das Wurzelziehen.

Nach solchen Lösungsformeln für Gleichungen fünften und höheren Grades wurde mehrere Jahrhunderte lang vergeblich gesucht. Dann kam die große Überraschung: der norwegische Mathematiker Niels Henrik Abel (1802–1829) bewies, dass es derartige allgemeine Formeln nicht geben kann. Die tieferen Gründe hierfür wurden von dem französischen Mathematiker Évariste Galois (1811–1832) aufgedeckt. Die Entwicklung der nach ihm benannten Galois-Theorie ist das Hauptziel dieser Vorlesung.

Die Grundidee ist einfach: zu jeder Gleichung betrachtet man die Symmetrien, die zwischen ihren Wurzeln bestehen. Dies führt zum Begriff der Gruppe: die Galois-Gruppe misst die Kompliziertheit einer Gleichung, und eine auflösbare Gleichung erkennt man daran, dass ihre Galois-Gruppe auflösbar ist.

Die Galois-Theorie ist ein faszinierendes Beispiel dafür, dass manchmal konkrete Probleme erst lösbar werden, wenn man sie mit der nötigen Abstraktion behandelt. So entsteht aus der klassischen Algebra (über den reellen und komplexen Zahlen) durch Abstraktion und Vereinheitlichung die moderne Algebra (über allgemeineren Ringen und Körpern). Die Vorlesung wird sich hierzu mit dem nötigen Handwerkszeug der Gruppen, Ringe und Körper befassen, die auch überall sonst in der Algebra unerlässlich sind.

Algebra ist das Studium von Verknüpfungen. Viele konkrete Rechnungen weisen Ähnlichkeiten und Gesetzmäßigkeiten auf. Diese können gewinnbringend im Rahmen allgemeinener Strukturen untersucht werden und tragen so wohlklingende Namen wie *Ring* oder *Körper*. Diese Konzepte treten schon beim Aufbau des Zahlensystems natürlich auf:

$$(\mathbb{N},+,\cdot) \subset (\mathbb{Z},+,\cdot) \subset (\mathbb{Q},+,\cdot) \subset (\mathbb{R},+,\cdot) \subset (\mathbb{C},+,\cdot)$$

Solche Strukturen, insbesondere Ringe, findet man aber in vielen Situationen:

- Die Menge $\mathbb{Q}[X]$ der Polynome (zum Beispiel über dem Körper $\mathbb{Q}$ der rationalen Zahlen) mit ihrer Addition $+\colon \mathbb{Q}[X] \times \mathbb{Q}[X] \to \mathbb{Q}[X]$ und ihrer Multiplikation $\cdot\colon \mathbb{Q}[X] \times \mathbb{Q}[X] \to \mathbb{Q}[X]$ bildet einen kommutativen Ring.
- Die Menge $M = \mathbb{C}^{n\times n}$ der $n \times n$-Matrizen (zum Beispiel über dem Körper $\mathbb{C}$ der komplexen Zahlen) mit ihrer Addition $+\colon M \times M \to M$ und ihrer Multiplikation $\cdot\colon M \times M \to M$ bildet einen nicht-kommutativen Ring.

Das Verständnis der allgemeinen Gesetzmäßigkeiten erweist sich als ungemein effizient beim Lösen konkreter Probleme. Die Entwicklung der hierzu nötigen Theorie wird uns das ganze Semester beschäftigen — und wird doch nur ein bescheidener Anfang sein können.

Algebra ist Koordinatisierung. Sie kennen hierzu aus dem ersten Studienjahr die lineare Algebra und analytische Geometrie. Die folgende Einführung präsentiert ein konkretes und historisch bedeutsames Beispiel: die Konstruktion mit Zirkel und Lineal.

KAPITEL 1

Konstruktion mit Zirkel und Lineal

In diesem ersten Kapitel stürzen wir uns in ein klassisches Problem der ebenen Geometrie: die Konstruktion mit Zirkel und Lineal. Diese Einführung ist ein *hors d'œuvre*; sie zeigt einerseits, dass man mit Schulmathematik und ein wenig Ausdauer schon recht weit vordringen kann. Andererseits zeigt sie auch die Notwendigkeit tiefergehender Begriffsbildungen. Deren systematischer Aufbau ist das Ziel der Algebra.

§1A. Was können wir mit Zirkel und Lineal konstruieren?

Konstruktionen mit Zirkel und Lineal sind seit der Antike sowohl von praktischem als auch von theoretischem Interesse, und bis heute in der mathematischen Schulbildung präsent. Aus praktischer Sicht möchte man wissen, wie man gewisse Figuren konstruiert. Aus theoretischer Sicht stellt sich die Frage, welche Konstruktionen überhaupt möglich sind, oder umgekehrt, welche nicht und warum.

§1Aa. Grundkonstruktionen. Beginnen wir mit drei einfachen Fragen der ebenen Geometrie, wie sie den meisten aus der Schule vertraut sein dürfte:

1. Zu gegebenen Längen a, b konstruiere man die Längen $a+b$ und $a-b$.
2. Zu gegebenen Längen $1, a, b$ konstruiere man die Längen $a \cdot b$ und a/b.
3. Zu gegebenen Längen $1, a$ konstruiere man die Länge $\sqrt{a}$.

Hier und im Folgenden heiße *konstruieren* (ohne weiteren Zusatz) stets *konstruieren mit Zirkel und Lineal*. Die Formulierung dieser Fragen verweist bereits auf die Verbindung von Geometrie und Algebra, die sich als äußerst glücklich und fruchtbar erweisen wird.

Für jede ernsthafte Untersuchung ist es unerlässlich genau zu definieren, was wir unter der Konstruktion mit Zirkel und Lineal verstehen. Hierzu sei M eine vorgegebene Menge von Punkten in der Ebene. Wir bezeichnen mit $\mathscr{G}(M)$ die Menge aller Geraden, die durch zwei verschiedenen Punkte von M laufen, und mit $\mathscr{K}(M)$ die Menge aller Kreise, deren Mittelpunkt in M liegt und deren Radius der Abstand zweier verschiedener Punkte aus M ist. Ein Punkt P heißt *in einem Schritt aus M konstruierbar*, wenn er Schnittpunkt ist von

- zwei verschiedenen Geraden aus $\mathscr{G}(M)$ oder
- zwei verschiedenen Kreisen aus $\mathscr{K}(M)$ oder
- einer Geraden aus $\mathscr{G}(M)$ und einem Kreis aus $\mathscr{K}(M)$.

Ein Punkt P heißt *in n Schritten aus M konstruierbar*, wenn es eine Folge $P_1, P_2, \ldots, P_n = P$ gibt, sodass jeder Punkt P_k in einem Schritt aus $M \cup \{P_1, \ldots, P_{k-1}\}$ konstruierbar ist.

Definition 1A1. Ein Punkt P heißt *aus M konstruierbar*, wenn es eine natürliche Zahl $n \in \mathbb{N}$ gibt, sodass P in n Schritten aus M konstruierbar ist.

Diese Definition präzisiert, wie man mit Zirkel und Lineal neue Punkte aus alten konstruiert. Die möglichen Konstruktionen hängen davon ab, welche Punkte vorgegeben sind; im einfachsten Fall nimmt man an, dass anfänglich nur zwei Punkte vorgegeben sind. Eine *Länge* oder (positive) *reelle Zahl* ist der Abstand zweier Punkte. Eine bestimme Zahl zu konstruieren bedeutet zwei Punkte zu konstruieren, die den gewünschten Abstand haben.

Übung 1A2. Man löse die ersten drei Fragen durch Angabe geeigneter Konstruktionen.

§**1Ab. Vier klassische Probleme der Geometrie.** Ausgehend von den obigen Grundkonstruktionen möchten wir die Frage der Konstruierbarkeit mit Zirkel und Lineal erkunden. Als Leitfaden dienen uns hierzu die folgenden vier Probleme:

1. Welche regelmäßigen n-Ecke lassen sich mit Zirkel und Lineal konstruieren?
2. Lässt sich zu jedem Winkel θ der Winkel $\theta/3$ konstruieren? (Winkeldreiteilung)
3. Lässt sich $\sqrt[3]{2}$ mit Zirkel und Lineal konstruieren? (Verdopplung des Würfels)
4. Lässt sich zu einem gegebenen Kreis ein flächengleiches Quadrat konstruieren? (Dies ist die sprichwörtlich gewordene *Quadratur des Kreises*.)

Wir werden in diesem einführenden Teil zunächst einen vollkommen elementaren Zugang wählen, der allein mit Schulmathematik auskommt, und doch einen beachtlichen Teil lösen können. Wie immer bedeutet *elementar* nicht unbedingt *einfach*. Nehmen wir also unseren Mut zusammen und seien wir kreativ!

Mit den entsprechenden Werkzeugen der Algebra werden sich viele Fragen später wie von selbst lösen. In Ermangelung dieser Werkzeuge werden wir es in diesem Kapitel mit bloßen (wenn auch geschickten) Händen versuchen. Wer sich hierbei ein paar Schwielen geholt hat, wird die spätere Bequemlichkeit umso mehr zu schätzen wissen.

§1B. Von der Geometrie zur Algebra

§**1Ba. Vom Problem zum Modell: analytische Geometrie.** Modellieren bedeutet, ein Problem in eine geeignete Sprache zu übersetzen, in der sich das Wesentliche des Problems beschreiben und – soweit möglich – lösen lässt. Für die Konstruierbarkeit mit Zirkel und Lineal folgen wir einer einfachen aber radikalen Idee: der *Koordinatisierung*.

Kurz gesagt: wir identifizieren die Ebene mit dem Raum $\mathbb{R}^2$.

Etwas ausführlicher: Gegeben seien zwei verschiedene Punkte O und P der Ebene. Durch diese beiden Punkte verläuft genau eine Gerade. Diese können wir durch den Körper $\mathbb{R}$ parametrisieren, wobei $0 \mapsto O$ und $1 \mapsto P$, sodass die Körperoperationen $a+b$, $a-b$, ab, a/b und die Anordnung der Punkte respektiert werden. (Hierzu wäre noch wesentlich mehr zu sagen, aber wir verzichten auf eine axiomatische Herleitung zugunsten eine raschen Skizze.) Anschließend konstruieren wir die Senkrechte durch O und wählen hierauf einen Punkt Q mit Abstand $|OQ| = |OP|$. Auch die Gerade durch O und Q parametrisieren wird durch $\mathbb{R}$. Die orthogonale Projektion auf diese beiden Achsen ordnet jedem Punkt X der Ebene ein Paar reeller Zahlen $(x,y) \in \mathbb{R}^2$ zu; diese werden die *Koordinaten* des Punktes X genannt. (Zum Beispiel gelten die Entsprechungen $O \leftrightarrow (0,0)$, $P \leftrightarrow (1,0)$, $Q \leftrightarrow (0,1)$.) Umgekehrt

entsprechen je zwei Koordinaten $(x,y) \in \mathbb{R}^2$ genau einem Punkt der Ebene. (Gewöhnlich nennt man dann die Gerade OP die x-Achse und die Gerade OQ die y-Achse.) Auf diese Weise können wir die Ebene mit dem Raum $\mathbb{R}^2$ identifizieren.

Was haben wir so gewonnen? Mit Koordinaten können wir rechnen!

Satz 1B1. *Sei $M \subset \mathbb{R}^2$ eine Menge von Punkten und sei $K := \mathrm{Koord}(M) \subset \mathbb{R}$ die Menge ihrer Koordinaten. Sei $\bar{M} \subset \mathbb{R}^2$ die Menge der aus M mit Zirkel und Lineal konstruierbaren Punkte. Sei $\bar{K} \subset \mathbb{R}$ die Menge der aus K konstruierbaren Zahlen durch Anwendung der fünf Operationen $a+b$, $a-b$, ab, a/b für $b \neq 0$, und $\sqrt{a}$ für $a > 0$. Dann gilt $\mathrm{Koord}(\bar{M}) = \bar{K}$.*

BEWEIS. Die Inklusion $\bar{K} \subset \mathrm{Koord}(\bar{M})$ folgt aus Übung 1A2: Die reellen Zahlen in K ergeben sich aus M durch Projektion auf die Koordinatenachsen, und die fünf genannten Operationen sind konstruierbar mit Zirkel und Lineal. (Man führe dies explizit aus.)

Für die umgekehrte Inklusion $\mathrm{Koord}(\bar{M}) \subset \bar{K}$ müssen wir zeigen, dass die Koordinaten der mit Zirkel und Lineal aus M konstruierbaren Punkte sich durch Anwendung der fünf Operationen berechnen lassen. Hierzu fassen wir die geometrischen Objekte algebraisch:

Die Gerade G durch zwei verschiedene Punkte (x_0,y_0) und (x_1,y_1) in M ist die Menge

$$G = \{(x,y) \in \mathbb{R}^2 \mid (x-x_0)(y_1-y_0) - (y-y_0)(x_1-x_0) = 0\}.$$

Der Kreis K um $(x_0,y_0) \in M$ mit Radius $r = \sqrt{(x_1-x_2)^2+(y_1-y_2)^2}$, gegeben durch den Abstand zweier verschiedener Punkte (x_1,y_1) und (x_2,y_2) in M, ist die Menge

$$K = \{(x,y) \in \mathbb{R}^2 \mid (x-x_0)^2 + (y-y_0)^2 = r^2\}.$$

Geraden $G \in \mathscr{G}(M)$ und Kreise $K \in \mathscr{K}(M)$ sind demnach Punktmengen der Form

$$G = \{(x,y) \in \mathbb{R}^2 \mid ax+by+c = 0\} \qquad \text{und}$$
$$K = \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2+ax+by+c = 0\}.$$

Hierbei ergeben sich die Koeffizienten $a,b,c \in \mathbb{R}$ aus den Koordinaten $\mathrm{Koord}(M)$ durch die rationalen Operationen $+,-,\cdot,/$.

Betrachten wir schließlich die Schnittpunkte solcher Mengen. Der Schnitt von zwei Geraden führt auf ein System von zwei linearen Gleichungen mit zwei Unbekannten; ihre Lösung berechnet sich durch die rationalen Operationen aus den Koeffizienten. Der Schnitt von zwei Kreisen, oder einem Kreis und einer Geraden, führt auf eine quadratische Gleichung; ihre Lösungen berechnen sich durch die rationalen Operationen und eine Quadratwurzel. Damit ist die geometrisch-algebraische Äquivalenz bewiesen. □

Übung 1B2. Führen Sie die im Beweis genannten Rechnungen explizit aus.

§**1Bb. Teilkörper der reellen Zahlen.** Wir beginnen mit einer einfachen Beobachtung: Sei K die Menge aller Zahlen, die sich aus 1 durch wiederholte Anwendung der rationalen Operationen $+,-,\cdot,/$ konstruieren lassen. Dann ist $K = \mathbb{Q}$ genau die Menge der rationalen Zahlen. Ausgehend von 1 erhält man nämlich $\mathbb{N} \subset K$ durch Addition, damit $\mathbb{Z} \subset K$ und schließlich $\mathbb{Q} \subset K$. Für die umgekehrte Inklusion $\mathbb{Q} \supset K$ genügt es festzustellen, dass $\mathbb{Q}$ abgeschlossen ist unter rationalen Operationen.

Da die *rationalen Operationen* eine herausragende Rolle spielen, heben wir sie durch die folgende Definition besonders hervor:

Definition 1B3. Eine Teilmenge $K \subset \mathbb{R}$ heißt *Körper* (genauer *Teilkörper der reellen Zahlen*) wenn sie die Zahl 1 enthält und mit je zwei Zahlen $a, b \in K$ auch deren Summe $a+b$, Differenz $a-b$, Produkt ab, und Quotient a/b. (Bei letzterem $b \neq 0$ wird vorausgesetzt.)

Wir werden später allgemein definieren, was ein Körper ist. Fürs Erste genügt uns jedoch diese Definition, da wir in diesem Kapitel mit Teilkörpern von $\mathbb{R}$ auskommen.

Beispiel 1B4. Die gesamte Menge $\mathbb{R}$ ist ein Körper. Weder die Teilmenge $\mathbb{N}$ der natürlichen Zahlen noch die Teilmenge $\mathbb{Z}$ der ganzen Zahlen sind Körper. Die Teilmenge $\mathbb{Q}$ der rationalen Zahlen ist hingegen ein Körper. und zwar der kleinste Teilkörper von $\mathbb{R}$: wir haben gerade gesehen, dass jeder Teilkörper $\mathbb{Q}$ enthält.

Die folgende Konstruktion liefert unendlich viele weitere Beispiele:

Proposition 1B5. *Sei $K \subset \mathbb{R}$ ein Körper und sei $c \in K$, $c > 0$. Dann ist die Menge*

$$K[\sqrt{c}] := \{a + b\sqrt{c} \mid a, b \in K\}$$

ein Teilkörper von $\mathbb{R}$.

Genauer gesagt ist $K[\sqrt{c}]$ der kleinste Teilkörper von $\mathbb{R}$ der sowohl den Körper K als auch das Element $\sqrt{c}$ enthält. Wir nennen dies eine *quadratische Erweiterung* von K.

BEWEIS. In Falle $\sqrt{c} \in K$ gilt trivialerweise $K[\sqrt{c}] = K$. Nehmen wir also $\sqrt{c} \notin K$ an. Seien $x = a + b\sqrt{c}$ und $y = a' + b'\sqrt{c}$ in $K[\sqrt{c}]$. Dann finden wir

- $x + y = (a + a') + (b + b')\sqrt{c}$,
- $x - y = (a - a') + (b - b')\sqrt{c}$,
- $x \cdot y = (aa' + bb'c) + (ab' + a'b)\sqrt{c}$,
- $x/y = \frac{a+b\sqrt{c}}{a'+b'\sqrt{c}} = \frac{a+b\sqrt{c}}{a'+b'\sqrt{c}} \cdot \frac{a'-b'\sqrt{c}}{a'-b'\sqrt{c}} = \frac{aa'-bb'c}{a'^2-b'^2c} + \frac{a'b-ab'}{a'^2-b'^2c}\sqrt{c}$.

Da K ein Körper ist, sind alle so aus $a, b, a', b', c \in K$ berechneten Koeffizienten wieder in K, und $x+y$, $x-y$, xy, x/y liegen demnach in $K[\sqrt{c}]$. Notwendige Präzisierung: Wann ist der Nenner $a'^2 - b'^2 c$ gleich Null? Aus $a'^2 - b'^2 c = 0$ und $b' \neq 0$ folgt $c = a'^2/b'^2$, entgegen unserer Annahme $\sqrt{c} \notin K$. Daher kann $a'^2 - b'^2 c = 0$ nur für $a' = b' = 0$ also $y = 0$ gelten. Für alle $y \neq 0$ liegt x/y in K. □

Definition 1B6. Eine Familie $K_0 \subset K_1 \subset K_2 \subset \ldots$ von Körpern nennen wir einen *Turm quadratischer Erweiterungen* wenn jeweils $K_{k+1} = K_k[\sqrt{c_k}]$ für ein $c_k \in K_k$ gilt.

Damit haben wir das passende Vokabular geschaffen, um die geometrisch-algebraische Äquivalenz aus Satz 1B1 bequem formulieren zu können:

Satz 1B7. *Für jede reelle Zahl $x \in \mathbb{R}$ sind folgende Aussagen äquivalent:*

- *x lässt sich mit Zirkel und Lineal aus dem Teilkörper $K_0 \subset \mathbb{R}$ konstruieren.*
- *x liegt in einem Turm $K_0 \subset K_1 \subset \cdots \subset K_n$ quadratischer Erweiterungen in $\mathbb{R}$.*

Die Neuerung liegt hier in der sprachlichen und konzeptuellen Eleganz. Inhaltlich tiefliegender ist folgendes Beispiel, das wir hier nur zitieren aber nicht beweisen wollen:

Beispiel 1B8 (unglaublich aber wahr)**.** Durch eine raffinierte Rechnung fand Carl Friedrich Gauß (seinem Tagebuch zufolge am 29. März 1796) folgende Gleichung:

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16}\left(\sqrt{17}-1+\sqrt{34-2\sqrt{17}}\right)+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.$$

Aus dieser Formel folgt mithilfe des Satzes, dass das regelmäßige 17-Eck mit Zirkel und Lineal konstruierbar ist. Dies war seit der griechischen Antike die erste große Neuerung zu den klassischen Fragen der Konstruierbarkeit mit Zirkel und Lineal. Seine Entdeckung bewegte den 18-jährigen Gauß sich endgültig der Mathematik zuzuwenden. Für eine schöne und nicht minder raffinierte geometrische Konstruktion verweise ich auf Stewart §19.5.

Der vorhergehende Satz liefert ein praktisches Kriterium für die Konstruierbarkeit mit Zirkel und Lineal, in Form einer notwendigen und hinreichenden algebraischen Begingung. Die Menge $\bar{M} \subset \mathbb{R}^2$ aller aus $M \subset \mathbb{R}$ konstruierbaren Punkte lässt sich wie folgt charakterisieren durch den von M erzeugten *quadratisch abgeschlossenen Teilkörper*:

Satz 1B9. *Sei $M \subset \mathbb{R}$ eine Menge mit $0,1 \in M$. Sei $\bar{M} \subset \mathbb{R}^2$ die Menge aller Punkte, die sich hieraus mit Zirkel und Lineal konstruieren lassen. Sei $K \subset \mathbb{R}$ der kleinste Teilkörper, der M umfasst und zu jedem $c > 0$ auch $\sqrt{c}$ enthält. Dann gilt $\bar{M} = K \times K$.* □

§1C. Algebraische Antworten auf geometrische Fragen

§1Ca. Das regelmäßige Fünfeck. Die Konstruktion des regelmäßigen n-Ecks gelingt vergleichsweise leicht für $n = 3,4,6,8$. Die Fälle $n = 5$ sowie $n = 7,9$ sind kniffeliger, und zwar aus entgegengesetzten Gründen: Um zu zeigen, dass eine Konstruktion möglich ist, muss man eine Konstruktion finden. Um zu beweisen, dass eine Konstruktion unmöglich ist, genügt es nicht geduldig zu scheitern. Man muss das Hindernis identifizieren!

Satz 1C1. *Die folgenden regelmäßigen n-Ecke sind mit Zirkel und Lineal konstruierbar:*

- *das gleichseitige Dreieck ($n = 3$).*
- *das Quadrat ($n = 4$).*
- *das regelmäßige Fünfeck ($n = 5$).*
- *das regelmäßige Sechseck ($n = 6$).*
- *das regelmäßige Achteck ($n = 8$).*

BEWEIS. Nur der Fall $n = 5$ ist delikat. (Nach einigen Fehlversuchen könnte man den Verdacht hegen, diese Konstruktion sei unmöglich…) Um die Situation zu klären, nutzen wir unsere oben entwickelten algebraischen Techniken!

Wir betrachten den Winkel $\theta = 2\pi/5$ und das regelmäßige Fünfeck mit Zentrum 0 und den Ecken $(\cos(k\theta), \sin(k\theta))$ wobei $k = 0, \pm 1, \pm 2$. Regelmäßig bedeutet hierbei invariant unter Drehung um θ. Der Schwerpunkt der fünf Ecken ist demnach 0. Wir finden somit

$$\begin{aligned} 0 &= 1 + 2\cos(\theta) + 2\cos(2\theta) \\ &= 1 + 2\cos\theta + 2(2\cos^2\theta - 1) \\ &= 4\cos^2\theta + 2\cos\theta - 1 \\ &= x^2 + x - 1 \quad \text{wobei} \quad x = 2\cos\theta. \end{aligned}$$

Dies erlaubt uns, den Wert $x = \frac{\sqrt{5}-1}{2}$ und damit $\cos(2\pi/5) = \frac{\sqrt{5}-1}{4}$ zu berechnen. Nach Satz 1B1 kann man also das regelmäßige Fünfeck mit Zirkel und Lineal konstruieren. □

Übung 1C2. Führen Sie eine Konstruktion des regelmäßigen $3,4,5,6,8$-Ecks explizit aus.

Bemerkung 1C3. Das Argument des Schwerpunkts erlaubt uns nicht nur die genannte algebraische Relation zu *beweisen* sondern überhaupt erst zu *finden*. Die geometrische Interpretation ist daher eine nützliche Hilfe, sich die Rechnung zu merken und wiederzufinden, falls Sie einmal auf einer einsamen Insel mathematische Zerstreuung suchen.

Bemerkung 1C4. Mithilfe der komplexen Zahlen kann man die algebraische Relation für $\cos(2\pi/5)$ ebenso gut aus der geometrischen Summe $1+e^{i\theta}+e^{2i\theta}+e^{3i\theta}+e^{4i\theta}=0$ und der Eulerschen Formel $\cos\theta = \frac{1}{2}(e^{i\theta}+e^{-i\theta})$ ableiten. Da ich eingangs die Schulmathematik beschwor, ziehe ich in diesem Kapitel eine Formulierung ohne komplexe Zahlen vor.

Bemerkung 1C5. Wenn man das regelmäßige n-Eck mit Zirkel und Lineal konstruieren kann, dann auch das regelmäßige $2n$-Eck durch Halbierung des zentralen Winkels. Demnach sind auch regelmäßige Vielecke konstruierbar mit $3\cdot 2^k$ Ecken, mit $4\cdot 2^k$ Ecken, und mit $5\cdot 2^k$ Ecken, für alle $k\in\mathbb{N}$.

Bemerkung 1C6. Wenn man das regelmäßige p-Eck und das regelmäßige q-Eck mit Zirkel und Lineal konstruieren kann, wobei $\mathrm{ggT}(p,q)=1$, dann auch das regelmäßige pq-Eck. Es gibt dann nämlich ganz Zahlen $u,v\in\mathbb{Z}$ sodass $up+vq=1$. Daraus folgt $\frac{2\pi}{pq} = u\frac{2\pi}{q} + v\frac{2\pi}{p}$. Zum Beispiel kann man somit das regelmäßige 15-Eck konstruieren: es gilt $2\cdot 3 - 1\cdot 5 = 1$, und somit $2\cdot\frac{2\pi}{5} - 1\cdot\frac{2\pi}{3} = \frac{2\pi}{15}$.

§**1Cb. Das regelmäßige Siebeneck.** Da unser algebraischer Ansatz so wunderbar für das Fünfeck funktioniert, wollen wir das regelmäßige Siebeneck ebenso untersuchen.

Lemma 1C7. *Die Zahl* $\eta = 2\cos(2\pi/7)$ *erfüllt die Gleichung* $\eta^3+\eta^2-2\eta-1=0$.

BEWEIS. Wir betrachten den Winkel $\theta = 2\pi/7$ und das regelmäßige Siebeneck mit Mittelpunkt 0 und den Eckpunkten $(\cos(k\theta),\sin(k\theta))$ für $k=0,\pm1,\pm2,\pm3$. Diese sind invariant unter Drehung um θ, ihr Schwerpunkt ist demnach 0. So finden wir

$$\begin{aligned}
0 &= 1+2\cos(\theta)+2\cos(2\theta)+2\cos(3\theta)\\
&= 1+2\cos\theta+(4\cos^2\theta-2)+(8\cos^3\theta-6\cos\theta)\\
&= 8\cos^3\theta+4\cos^2\theta-4\cos\theta-1\\
&= \eta^3+\eta^2-2\eta-1.
\end{aligned}$$

Hierbei benutzen wir $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$ sowie $\cos(2\theta) = 2\cos^2\theta - 1$. □

Bemerkung 1C8. Die algebraische Relation $\eta^3+\eta^2-2\eta-1=0$ bietet uns einen konkreten Zugriff auf die Zahl $\eta = 2\cos(2\pi/7)$. Wenn man komplexe Zahlen verwenden möchte, kann man diese Relation ebenso aus der geometrischen Summe $1+e^{i\eta}+e^{2i\eta}+e^{3i\eta}+e^{4i\eta}+e^{5i\eta}+e^{6i\eta}=0$ und der Eulerschen Formel $\cos\eta = \frac{1}{2}(e^{i\eta}+e^{-i\eta})$ ableiten.

Lemma 1C9. *Das Polynom* X^3+X^2-2X-1 *hat keine rationale Nullstellen.*

BEWEIS. Angenommen, es gäbe eine rationale Zahl $x = \frac{a}{b}$ so dass $x^3+x^2-2x-1=0$. Hierbei ist $a,b \in \mathbb{Z}$ und $b \geq 1$, und wir können $\mathrm{ggT}(a,b) = 1$ annehmen. Wir erhalten so $a^3+a^2b-2ab^2-b^3=0$. Daraus sehen wir: a teilt b, also $a = \pm 1$, und b teilt a, also $b = 1$. Es bleibt demnach nur die Möglichkeit $x = \pm 1$. Aber $x = \pm 1$ erfüllt nicht $x^3+x^2-2x-1=0$. Also erfüllt keine rationale Zahl x die Gleichung $x^3+x^2-2x-1=0$. □

Insbesondere ist $\eta = 2\cos(2\pi/7)$ nicht rational. Um $\cos(2\pi/7)$ mit Zirkel und Lineal zu konstruieren brauchen wir also mindestens eine Quadratwurzel. Reicht eine?

Lemma 1C10. *Sei $K_0 \subset K_1 = K_0[\sqrt{c}]$ eine quadratische Erweiterung. Wenn das Polynom X^3+X^2-2X-1 eine Wurzel in K_1 hat, dann liegt auch bereits in K_0 eine solche Wurzel.*

BEWEIS. Wir haben $x^3+x^2-2x-1=0$ für ein Element $x \in K_1$, das heißt $x = a+b\sqrt{c}$ mit $a,b,c \in K_0$, $c > 0$. Wir entwickeln

$$0 = x^3+x^2-2x-1 = \alpha+\beta\sqrt{c}$$

und nach einer kleinen Rechnung finden wir

$$\alpha = a^3+3ab^2c+a^2+b^2c-2a-1,$$
$$\beta = 3a^2b+b^3c+2ab-2b.$$

Wir unterscheiden zwei Fälle:

- Wenn $\beta \neq 0$, dann folgt sofort $\sqrt{c} = -\alpha/\beta \in K_0$, also auch $x \in K_0$.
- Wenn $\beta = 0$, dann $c = \frac{2-2a-3a^2}{b^2}$ und $\alpha = -8a^3-8a^2+2a+1$.
  Wegen $\alpha = 0$ folgt $a \neq 0$, und $y = \frac{1}{2a} \in K_0$ erfüllt $y^3+y^2-2y-1=0$.

In beiden Fällen hat X^3+X^2-2X-1 eine Wurzel in K_0. □

Dieses Argument können wir nun iterieren und erhalten daraus folgendes Ergebnis:

Satz 1C11. *Das regelmäßige Siebeneck ist nicht mit Zirkel und Lineal konstruierbar.*

BEWEIS. Die Konstruktion des regelmäßigen Siebenecks ist äquivalent zur Konstruktion der Zahl $\cos(2\pi/7)$. Nehmen wir an, $\eta = 2\cos(2\pi/7)$ sei mit Zirkel und Lineal konstruierbar ausgehend von der Länge 1. Dann gäbe es einen Turm $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n \subset \mathbb{R}$ quadratischer Erweiterungen in $\mathbb{R}$ sodass $\eta \in K_n$. Also hat das Polynom X^3+X^2-2X-1 eine Wurzel in K_n. Das vorhergehende Lemma zeigt, dass eine Wurzel in K_{n-1} liegt, demnach auch in $K_{n-2}, \ldots$, und schließlich in $K_0 = \mathbb{Q}$. Aber X^3+X^2-2X-1 hat keine rationale Wurzel. Also ist $\eta = 2\cos(2\pi/7)$ nicht mit Zirkel und Lineal konstruierbar, und damit auch nicht das regelmäßige Siebeneck. □

§**1Cc. Das regelmäßige Neuneck.** Ein mathematisches Argument, das einmal funktioniert, ist ein Trick. Ein Argument, das zwei- oder mehrmals funktioniert ist eine Theorie. Führen wir also unsere kleine Theorie noch ein klein wenig weiter, um die Konstruierbarkeit des regelmäßigen Neunecks zu klären. Diese zusätzliche Anstrengung lässt uns auch eine unerwartete Antwort zur Dreiteilung des Winkels in den Schoß fallen.

Lemma 1C12. *Die Zahl $\kappa = 2\cos(2\pi/9)$ erfüllt die Gleichung $\kappa^3-3\kappa+1=0$.*

BEWEIS. Einerseits gilt $\cos(3\theta) = \cos(2\pi/3) = -1/2$. Andererseits wissen wir $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$. Daraus folgt $8\cos^3\theta - 6\cos\theta + 1 = 0$, also $\kappa^3 - 3\kappa + 1 = 0$. □

Lemma 1C13. *Das Polynom $X^3 - 3X + 1$ hat keine rationale Nullstellen.*

BEWEIS. Angenommen, es gäbe eine rationale Zahl $x = \frac{a}{b}$ so dass $x^3 + x^2 - 2x - 1 = 0$. Hierbei ist $a, b \in \mathbb{Z}$ und $b \geq 1$, und wir können $\mathrm{ggT}(a,b) = 1$ annehmen. Wir erhalten so $a^3 + 3ab^2 - b^3 = 0$. Daraus sehen wir: a teilt b, also $a = \pm 1$, und b teilt a, also $b = 1$. Es bleibt also nur die Möglichkeit $x = \pm 1$. Aber $x = \pm 1$ erfüllt nicht die Gleichung $x^3 - 3x + 1 = 0$. Also erfüllt keine rationale Zahl x die Gleichung $x^3 - 3x + 1 = 0$. □

Insbesondere ist $\kappa = 2\cos(2\pi/9)$ nicht rational. Um $\cos(2\pi/9)$ mit Zirkel und Lineal zu konstruieren brauchen wir also mindestens eine Quadratwurzel. Reicht eine?

Lemma 1C14. *Sei $K_0 \subset K_1$ eine quadratische Erweiterung. Wenn das Polynom $X^3 - 3X + 1$ eine Wurzel in K_1 hat, dann liegt auch bereits in K_0 eine solche Wurzel.*

BEWEIS. Wir haben $x^3 - 3x + 1 = 0$ für ein Element $x \in K_1$, das heißt $x = a + b\sqrt{c}$ mit $a, b, c \in K_0$, $c > 0$. Wir entwickeln

$$0 = x^3 - 3x + 1 = \alpha + \beta\sqrt{c}$$

und nach einer kleinen Rechnung finden wir

$$\alpha = a^3 + 3ab^2c - 3a + 1,$$
$$\beta = 3a^2b + b^3c - 3b.$$

Wir unterscheiden zwei Fälle:

- Wenn $\beta \neq 0$, dann folgt sofort $\sqrt{c} = -\alpha/\beta \in K_0$, also auch $x \in K_0$.
- Wenn $\beta = 0$, dann $c = \frac{3-3a^2}{b^2}$ und $\alpha = -8a^3 + 6a + 1$.
  Wegen $\alpha = 0$ erfüllt $y = -2a \in K_0$ die Gleichung $y^3 - 3y + 1 = 0$.

In beiden Fällen hat $X^3 - 3X + 1$ eine Wurzel in K_0. □

Als Krönung unserer Bemühungen erhalten wir das folgende Ergebnis:

Satz 1C15. *Das regelmäßige Neuneck ist nicht mit Zirkel und Lineal konstruierbar.*

Der Beweis verläuft genauso wie für das regelmäßige Siebeneck (1C11).

§**1Cd. Die Dreiteilung des Winkels.** Ausgehend von manchen Winkeln θ kann man den Winkel $\theta/3$ konstruieren. Dies gelingt zum Beispiel sehr leicht für einen rechten Winkel $\theta = \pi/2$. (Übung!) Zweitausend Jahre lang suchte man vergeblich nach einer Konstruktion mit Zirkel und Lineal, die die Dreiteilung eines *beliebigen* Winkels ermöglicht.

Mit unseren algebraischen Hilfsmitteln können wir nun mühelos zeigen, dass eine solche Konstruktion im Allgemeinen unmöglich ist:

Satz 1C16. *Es gibt keine Konstruktion mit Zirkel und Lineal, die einen beliebig vorgegebenen Winkel dreiteilt. Dies folgt aus einem einfachen und konkreten Gegenbeispiel: die Dreiteilung des Winkels $\pi/3$ (d.h. 60°) ist mit Zirkel und Lineal nicht möglich.*

BEWEIS. Wir können das regelmäßige Sechseck mit Zirkel und Lineal konstruieren (1C1). Wenn wir den zentralen Winkel $\pi/3$ dreiteilen könnten, dann entstünde so der Winkel $\pi/9$. Daraus ließe sich ein regelmäßiges Neuneck konstruieren. Dessen Konstruktion ist aber mit Zirkel und Lineal nicht möglich (1C15). □

Falls dieses Ergebnis Sie überrascht oder beunruhigt (was durchaus möglich und legitim ist), dann sollten Sie die Gelegenheit nutzen, alle Argumente dieses Kapitels genau nachzuprüfen. Vielleicht hat sich ein Fehler eingeschlichen? Nach eingehender Prüfung werden Sie Gewissheit haben und die nötigen Techniken sicher beherrschen.

§1D. Wie geht es weiter?

§**1Da. Rückblick.** Welche Kernideen haben zum Erfolg unserer mutigen Ersterkundung beigetragen? Rückblickend hat uns vor allem die Koordinatisierung große Dienste erwiesen. Man beachte jedoch, dass weder die ursprüngliche Frage noch unsere Antwort von Koordinaten sprechen: Das regelmäßige $3,4,5,6,8,10$-Eck ist mit Zirkel und Lineal konstruierbar, das $7,9$-Eck hingegen nicht. Die Koordinatisierung ist gänzlich Teil der Modellierung, ein Konstrukt mit dessen Hilfe wir das ursprüngliche Problem umformuliert und einer algebraischen Lösung zugänglich gemacht haben.

Unsere Ergebnisse, so bescheiden sie auch sein mögen, zeigen bereits eindrucksvoll, wie fruchtbar die Verbindung von Geometrie und Algebra sein kann. Hierzu haben wir folgende Techniken aus der Schulmathematik mobilisiert:

- die Konstruktion mit Zirkel und Lineal,
- die Benutzung von kartesischen Koordinaten,
- Die Lösung von Gleichungen ersten und zweiten Grades,
- algebraisches Rechnen mit Quadratwurzeln in $\mathbb{R}$,
- die Irrationalität von $\sqrt{2}$ und einige Varianten,
- die Parametrisierung des Kreises durch $(\cos\theta, \sin\theta)$,
- die Gleichungen $\cos(2\theta) = 2\cos^2\theta - 1$ und $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$.

Erstaunlicherweise ist nicht mehr als dies nötig gewesen.

> Man kann sich naiv fragen, warum uns dieses Vorgehen heutzutage leicht fällt, nicht aber den Geometern des antiken Griechenlands. Entscheidend ist hierbei die Idee der Koordinatisierung, die den antiken Geometern weitgehend fremd und vor allem aber suspekt war. Erst durch die Koordinatisierung jedoch wird Möglichkeit erschlossen, geometrische Phänomene mit Hilfe der Algebra zu beschreiben und umgekehrt. Ohne dies hier vertiefen zu wollen, möchte ich damit eins unterstreichen: Wir erben die Erfahrungen und Errungenschaften von über zweitausend Jahren wissenschaftlicher Entwicklung, insbesondere auch mathematischen Fortschritts. Dieses Wissen wurde uns durch eine solide allgemeine Schulbildung weitergegeben und ermöglicht uns nun den Ausbau zu neuen Anwendungen. Zum Beispiel haben wir gelernt, in Koordinaten zu denken und algebraische Rechnungen vorzunehmen. Die Ergebnisse dieses Kapitels sind nur ein kleines Beispiel für die Früchte dieser Kenntnisse.

§**1Db. Welche der klassischen Fragen bleiben noch offen?** Wir haben nicht alle eingangs gestellten Fragen aus §1Ab auf einen Streich lösen können. Zur Konstruierbarkeit des regelmäßigen n-Ecks kennen die Antwort für $n \leq 10$. Die allgemeine Lösung wird sich aus der Untersuchung des Kreisteilungspolynoms $X^n - 1$ ergeben.

Die Verdopplung des Würfels, also die Konstruktion von $\sqrt[3]{2}$ mit Zirkel und Lineal, wird als Übung empfohlen und sollte mit den Techniken dieses Kapitels leicht fallen. (Zur Geschichte dieses *Delischen Problems* lese man den englischen Wikipedia-Artikel. Wer mutig und versiert ist, möchte vielleicht einen ordentlichen deutschen Wikipedia-Artikel hierzu schreiben und pflegen.)

Zur Quadratur des Kreises haben wir bislang noch gar nichts sagen können: Lässt sich zu einem gegebenen Kreis ein flächengleiches Quadrat konstruieren? Die Antwort folgt aus der Untersuchung der Kreiszahl π: Der berühmte Satz von Hermite–Lindeman besagt, dass π nicht algebraisch über $\mathbb{Q}$ ist, also nicht Nullstelle eines Polynoms $X^n + c_1X^{n-1} + \cdots + c_n$ mit rationalen Koeffizienten $c_1, \ldots, c_n \in \mathbb{Q}$ sein kann. Wenn man dieses (deutlich tieferliegende) Ergebnis voraussetzt, so folgt die Antwort mit den Techniken dieses Kapitels: Allein mit Zirkel und Lineal ist die Quadratur des Kreises nicht möglich.

§**1Dc. Ausblick.** Die Beweise der Sätze 1C11 und 1C15 sind etwas repetitiv: Diese Rechnungen kommen zwar glücklich zum Ziel, sind auf Dauer aber lästig. Das ist der Preis, den man für einen elementaren Zugang bezahlen muss. Unser Ziel wird sein, unseren mathematischen Werkzeugkasten durch allgemeinere Techniken zu erweitern. Es wird sich herausstellen, dass mit ein wenig Abstraktion vieles leichter geht!

Nach Abschluss dieses einführenden und motivierenden Kapitels werden wir daher mit der systematischen Entwicklung der Algebra beginnen. Das bisher Gesehene enthält hierzu bereits den Keim einiger zentralen Ideen, die wir im Folgenden vertiefen werden:

- Der Begriff des Polynoms, seiner Wurzeln, und allgemein seiner Zerlegungen.
- Der Begriff der Symmetrie, und allgemein von Gruppen und ihren Operationen.
- Der Begriff des Körpers, der Körpererweiterung, und schließlich der Galois-Theorie.

§1E. Übungen und Ergänzungen

§**1Ea. Von reellen zu komplexen Zahlen.** Dieses Kapitel hat aus didaktischen Gründen die Verwendung von komplexen Zahlen vermieden, vielleicht zu Unrecht. Mathematisch ist die Frage durchaus interessant:

Übung 1E1. Sei $M \subset \mathbb{R}$ eine Menge mit $0, 1 \in M$. Sei $\bar{M} \subset \mathbb{R}^2$ die Menge aller Punkte, die sich hieraus mit Zirkel und Lineal konstruieren lassen. Ist $\bar{M}$, als Teilmenge von $\mathbb{C} = \mathbb{R}^2$ betrachtet, ein Teilkörper? Wie lässt sich die Menge $\bar{M} \subset \mathbb{C}$ algebraisch charakterisieren?

§**1Eb. Variationen des Themas.** Der *Satz von Mohr–Mascheroni* (1672/1797) besagt, dass jeder Punkt, der mit Zirkel und Lineal konstruierbar ist, auch alleine mit Zirkel konstruierbar ist. Versuchen Sie doch mal, einige einfache Konstruktionen ohne Lineal durchzuführen! Wie könnte man den Satz von Mohr–Mascheron beweisen?

Wenn man hingegen nur das Lineal zulässt, dann sind manche Konstruktionen nicht mehr möglich. (Warum?) Der *Satz von Steiner* besagt, dass ein Lineal genügt, wenn man einen einzigen Kreis und seinen Mittelpunkt vorgibt. Daraus folgt, dass man alle Konstruktionen mit Zirkel und Lineal auch noch mit einem Lineal und einem rostigen Zirkel (mit festem Radius) ausführen kann.

Zirkel und Lineal sind die klassische Wahl seit der Antike. Aber auch andere Werkzeuge sind denkbar und führen eventuell zu anderen Konstruktionen. Zur weiteren Lektüre empfehle ich den Klassiker von Courant–Robbins: *What is Mathematics?*, Oxford University Press 1996, sowie George E. Martin: *Geometric Constructions*, Springer 1997.

TEIL I

Grundlagen der Ringtheorie

KAPITEL 2

Monoide und Gruppen

§2A. Einführung und Überblick

§**2Aa. Konkrete Monoide und Gruppen.** Monoide und Gruppen sind grundlegende Strukturen der Algebra und treten in der Mathematik fast überall auf: Die wichtigsten Beispiele sind Rechenoperationen von Zahlen sowie Symmetrien mathematischer Objekte. Wir stellen daher zwei fundamentale Beispiele voran:

Beispiel 2A1. Die Menge $\mathbb{N} = \{0,1,2,3,\dots\}$ der natürlichen Zahlen zusammen mit ihrer Addition $+\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ erfreut sich folgender Eigenschaften:

0. *Kommutativität:* Es gilt $a+b=b+a$ für alle a,b.
1. *Assoziativität:* Es gilt $(a+b)+c=a+(b+c)$ für alle a,b,c.
2. *Neutrales Element:* Es gilt $0+a=a+0=a$ für alle a.

Durch die Erweiterung zur Menge $\mathbb{Z} = \{\dots,-3,-2,-1,0,1,2,3,\dots\}$ der ganzen Zahlen mit ihrer Addition $+\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ erreichen wir zusätzlich folgende Eigenschaft:

3. *Invertierbarkeit:* Zu jedem $a\in\mathbb{Z}$ existiert $b\in\mathbb{Z}$ sodass $a+b=b+a=0$ gilt.

Beispiel 2A2. Sei X eine Menge und sei $\operatorname{Abb}(X)$ die Menge aller Abbildungen $X\to X$. Die Komposition definiert hierauf eine Verknüpfung $\circ\colon \operatorname{Abb}(X)\times\operatorname{Abb}(X)\to\operatorname{Abb}(X)$. Diese erfreut sich folgender Eigenschaften:

1. *Assoziativität:* Es gilt $f\circ(g\circ h)=(f\circ g)\circ h$ für alle f,g,h.
2. *Neutrales Element:* Die Abbildung id_X erfüllt $\mathrm{id}_X\circ f=f\circ\mathrm{id}_X=f$ für alle f.

Sei $\operatorname{Sym}(X)\subset\operatorname{Abb}(X)$ die Teilmenge der bijektiven Abbildungen $X\xrightarrow{\sim}X$. Die Komposition bijektiver Abbildungen ist wieder bijektiv. Durch Einschränkung erhalten wir so die Verknüpfung $\circ\colon \operatorname{Sym}(X)\times\operatorname{Sym}(X)\to\operatorname{Sym}(X)$ mit folgender zusätzlichen Eigenschaft:

3. *Invertierbarkeit:*
   Zu jedem $g\in\operatorname{Sym}(X)$ existiert $f\in\operatorname{Sym}(X)$ sodass $g\circ f=f\circ g=\mathrm{id}_X$ gilt.

§**2Ab. Abstrakte Monoide und Gruppen.** Die Eigenschaften (1–3) spielen in vielen Situationen eine wichtige Rolle, auch wenn die betrachteten Objekte sehr unterschiedlicher Herkunft sind. Um solche Strukturen allgemein und effizient behandeln zu können, erheben wir die wesentlichen Eigenschaften zu Axiomen und geben ihnen griffige Namen:

Definition 2A3. Ein *Magma* $(A,*)$ besteht aus einer Menge A zusammen mit einer inneren zweistelligen Verknüpfung $*\colon A\times A\to A$.

- Eine *Halbgruppe* $(A,*)$ ist ein Magma mit assoziativer Verknüpfung:
  1. $\forall a,b,c\in A : (a*b)*c = a*(b*c)$

  In diesem Fall ist die Klammerung unerheblich (2C5).

- Ein *Monoid* $(A,*)$ ist eine Halbgruppe mit neutralem Element
  2. $\exists e\in A\ \forall a\in A : e*a = a*e = a$

  In diesem Fall ist e eindeutig durch die Verknüpfung $*$ bestimmt (2C2).

- Eine *Gruppe* $(A,*)$ ist ein Monoid, in dem jedes Element invertierbar ist:
  3. $\forall a\in A\ \exists b\in G : a*b = b*a = e$

  In diesem Fall ist das zu a inverse Element eindeutig (2D1).

- Die Verknüpfung $*\colon A\times A\to A$ heißt *kommutativ* oder *abelsch* wenn gilt:
  0. $\forall a,b\in A : a*b = b*a$

  Ist $*$ zudem assoziativ, so können Faktoren beliebig umgeordnet werden (2E1).

Bemerkung 2A4. Die Kommutativität ist eine kostbare zusätzliche Eigenschaft, die in vielen Situationen eine wichtige Rolle spielt. Der Begriff *abelsch* wird hier genutzt zu Ehren des großen norwegischen Mathematikers Niels Henrik ABEL (1802–1829).

Beispiel 2A5. Für $\mathbb{N}^* = \mathbb{N}\smallsetminus\{0\}$ ist $(\mathbb{N}^*,+)$ eine Halbgruppe, $(\mathbb{N},+)$ ist ein Monoid, und $(\mathbb{Z},+)$ eine Gruppe. Diese Verknüpfungen sind kommutativ.

Beispiel 2A6. Für jede Menge X ist $(\mathrm{Abb}(X),\circ)$ ein Monoid, aber keine Gruppe sobald $|X|\geq 2$. Nach Definition ist $(\mathrm{Sym}(X),\circ)$ eine Gruppe, und wird die *symmetrische Gruppe* auf X genannt. Diese ist nicht-abelsch sobald $|X|\geq 3$.

Notation. Mit Permutationen einer endlichen Menge X lässt sich wunderbar rechnen. Wir nutzen folgende praktische Schreibweise: Für $\ell\geq 2$ verschiedene Elemente $i_1,i_2,\ldots,i_\ell\in X$ bezeichnen wir mit $\sigma=(i_1,i_2,\ldots,i_\ell)$ die Permutation $\sigma\in \mathrm{S}_X$ definiert durch $\sigma(i_1)=i_2$, $\sigma(i_2)=i_3$, …, $\sigma(i_\ell)=i_1$ sowie $\sigma(k)=k$ für alle $k\in X\smallsetminus\{i_1,i_2,\ldots,i_\ell\}$. Für $X=\{1,2\}$ gilt $\mathrm{Sym}(X)=\{\mathrm{id},(1,2)\}$, und die Komposition $\circ$ ist kommutativ. Für $|X|\geq 3$ ist $(\mathrm{Sym}(X),\circ)$ nicht kommutativ, denn $(a,b)(b,c)=(a,b,c)$ ist verschieden von $(b,c)(a,b)=(a,c,b)$.

Beispiel 2A7. Monoide und Gruppen gibt es wie Sand am Meer: Betrachtet man ein beliebiges mathematisches Objekt X, zum Beispiel ein Monoid, eine Gruppe, einen Ring, einen Körper, einen Vektorraum, etc., dann ist die Menge $\mathrm{End}(X)$ der Endomorphismen von X ein Monoid, und die Menge $\mathrm{Aut}(X)$ der Automorphismen von X ist eine Gruppe.

§**2Ac. Ziel dieses Kapitels.** Dieses Kapitel führt Monoide und Gruppen schrittweise ein, liefert einfache Beispiele und erläutert die nötigen Grundlagen. Dieses Vokabeltraining enthält viele Definitionen, einige Beispiele, aber noch kaum Sätze. Den Zusammenhang zwischen konkreten und abstrakten Gruppen stellt der Satz von Cayley (1854) her:

Satz 2A8. *Jede Gruppe $(G,*)$ ist isomorph zu einer Untergruppe $U\subset\mathrm{Sym}(X)$ einer symmetrischen Gruppe auf einer geeigneten Menge X. Hierbei kann $X=G$ gewählt werden.*

Dieses Ergebnis spielte für die Entwicklung der Gruppentheorie im 19. Jahrhundert eine wichtige Rolle, denn es stellt sicher, dass sich jede abstrakte Gruppe in eine konkrete Gruppe einbetten lässt. Uns dient dies zunächst zur Illustration der grundlegenden Begriffe.

Der Satz von Cayley ist ein universelles *Konstruktionswerkzeug*, denn er erlaubt auf direkte Weise konkrete Beispiele zu erzeugen. Als *Analysewerkzeug* eignet er sich jedoch oft schlecht. Hier hat sich das duale Konzept der Quotientenstrukturen (§2G) bewährt, die im Folgenden für alle algebraischen Strukturen eine wichtige Rolle spielen werden. Erst hier entfaltet die axiomatische Herangehensweise ihre volle Kraft. Auf diesen Begriff werden wir daher am Ende dieses Kapitels ausführlich eingehen.

§2B. Verknüpfungen

Wir beginnen mit einem sehr allgemeinen und daher grundlegenden Begriff:

Definition 2B1. Eine *Verknüpfung* ist eine Abbildung $*\colon A \times B \to C$.

Hierbei sind A, B, C Mengen und $A \times B$ ist die Menge aller Paare (a,b) mit $a \in A$ und $b \in B$. Die Abbildung $*$ ordnet jedem solchen Paar (a,b) ihr Bild $c = *(a,b)$ zu, das *Ergebnis* der Verknüpfung von a und b. Man nutzt zumeist die Schreibweise $a * b = *(a,b)$.

Eine solche Verknüpfung nennt man zur Betonung auch *zweistellige* Verknüpfung. Dies wird nötig, wenn man nebenbei auch *mehrstellige* Verknüpfungen betrachtet.

Beispiel 2B2. Addition und Multiplikation auf entsprechenden Mengen von Zahlen sind zweistellige Verknüpfungen. Als konkretes Beispiel betrachten wir die Menge $\mathbb{Z}$ der ganzen Zahlen mit der üblichen Addition und Multiplikation

$$+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},$$
$$\cdot\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}.$$

Auf der Menge $\mathbb{Z}$ der ganzen Zahlen ist auch die Subtraktion eine zweistellige Verknüpfung:

$$-\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

Durch die Division einer ganzen Zahl $a \in \mathbb{Z}$ durch eine von Null verschiedene ganze Zahl $b \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ entsteht eine rationale Zahl $c = a/b$. Dies entspricht einer Verknüpfung

$$/\colon \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Q}.$$

Beispiel 2B3. Sind $A = \{a_1, \dots, a_m\}$ und $B = \{b_1, \dots, b_n\}$ endliche Mengen, so können wir die Verknüpfung $*\colon A \times B \to C$ durch eine *Verknüpfungstafel* darstellen:

$*$	b_1	$\cdots$	b_j	$\cdots$	b_n
a_1	$a_1 * b_1$	$\cdots$	$a_1 * b_j$	$\cdots$	$a_1 * b_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_i	$a_i * b_1$	$\cdots$	$a_i * b_j$	$\cdots$	$a_i * b_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_m	$a_m * b_1$	$\cdots$	$a_m * b_j$	$\cdots$	$a_m * b_n$

Umgekehrt definiert jede solche $A \times B$-Tafel mit Werten in C eine Verknüpfung $A \times B \to C$.

Definition 2B4 (Komplexverknüpfung)**.** Seien $a \in A$ und $b \in B$ Elemente und seien $S \subset A$ und $T \subset B$ Teilmengen. Dann definieren wir durch Verknüpfung folgende Mengen:

$$a * T := \{\, a * t \mid t \in T \,\}$$
$$S * b := \{\, s * b \mid s \in S \,\}$$
$$S * T := \{\, s * t \mid s \in S, t \in T \,\}$$

Beispiel 2B5. In dieser Notation ist $2 \cdot \mathbb{Z}$ die Menge der geraden ganzen Zahlen und somit $1 + (2 \cdot \mathbb{Z})$ die Menge der ungeraden ganzen Zahlen.

Bemerkung 2B6. Ist $*\colon A \times B \to C$ eine Verknüpfung und sind $S \subset A$, $T \subset B$ Teilmengen, so können wir die Verknüpfung einschränken zu $*|_{S\times T}\colon S \times T \to C$. Liegt das Bild $S * T$ in der Teilmenge $U \subset C$, dann erhalten wir eine Abbildung $*|_{S\times T}\colon S \times T \to U$.

Beispiel 2B7. Aus der linearen Algebra kennen Sie den Begriff des Vektorraums V über einem Körper K. Neben der Addition von Vektoren $+\colon V \times V \to V$ gehört hierzu die Skalarmultiplikation $\cdot\colon K \times V \to V$. (Als Übung wiederhole man die geforderten Eigenschaften dieser Verknüpfungen.) Ist $U \subset V$ eine nicht-leere Teilmenge, so lassen sich diese Verknüpfungen auf U einschränken wenn $U + U \subset U$ und $K \cdot U \subset U$ gilt. In diesem Fall nennen wir U einen *Untervektorraum* von V; mit den eingeschränkten Verknüpfungen $+\colon U \times U \to U$ und $\cdot\colon K \times U \to U$ wird U selbst zu einem Vektorraum. Die einfachen Beispiele dieser Art sind von der Form $U = K \cdot v$ für $v \in V$. Ist $v = 0$, dann ist $U = \{0\}$ der Nullraum; ist $v \neq 0$, dann ist U ein eindimensionaler Unterraum, also eine Gerade in V. Sind $v_1, \ldots, v_n \in V$ gegeben, so ist $U = K \cdot v_1 + \cdots + K \cdot v_n$ die Menge aller Linearkombinationen von $v_1, \ldots, v_n$. Dies ist ein Untervektorraum von V, und zwar der kleinste, der $v_1, \ldots, v_n$ enthält. Man sagt daher auch: U ist der von $v_1, \ldots, v_n$ erzeugte (oder aufgespannte) Unterraum.

Statt beliebiger Verknüpfungen $*\colon A \times B \to C$ werden wir meist *innere* Verknüpfungen betrachten; für diese gilt $A = B = C$, und wir vereinbaren folgende Sprechweise:

Definition 2B8. Eine *Verknüpfung* auf einer Menge M ist eine Abbildung $*\colon M \times M \to M$.

Zur Betonung nennt man $*\colon M \times M \to M$ zuweilen auch eine *zweistellige innere* Verknüpfung: *zweistellig* weil immer genau zwei Operanden miteinander verknüpft werden und *inner* weil sowohl die Operanden a, b als auch das Ergebnis $a * b$ in M liegen.

Sprech- und Schreibweisen. Anstelle von $*$ benutzt man oft das Symbol $\cdot$. Man spricht dann von der *Multiplikation* $\cdot\colon M \times M \to M$, und $ab = a \cdot b$ heißt das *Produkt* von a und b. Ebenso geläufig ist das Symbol $+$. Man spricht dann von der *Addition* $+\colon M \times M \to M$, und $a + b$ heißt die *Summe* von a und b. Die gewählte Schreibweise ist für den mathematischen Begriff jedoch nebensächlich und richtet sich im gegebenen Kontext allein nach Bequemlichkeit und Tradition.

Beispiel 2B9. Ist die zugrunde liegende Menge M endlich, so kann jede Verknüpfung auf M in Form einer Tabelle angegeben werden. Als Beispiel betrachten wir die Menge $M = \{1, i, -1, -i\} \subset \mathbb{C}$ mit folgender Multiplikation:

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

§**2Ba. Homomorphismen.** Ein *Magma* $(M,*)$ besteht aus einer Menge M zusammen mit einer Verknüpfung $*\colon M\times M\to M$. Dieser Begriff erlaubt zwar für sich allein noch keine interessante Theorie, bildet aber die gemeinsame Grundlage für viele nützliche Begriffsbildungen, allen voran den Begriff des Homomorphismus:

Definition 2B10. Ein *Homomorphismus* zwischen zwei Magmen $(M,*)$ und $(N,\bullet)$ ist eine Abbildung $h\colon M\to N$ die $h(a*b)=h(a)\bullet h(b)$ für alle $a,b\in M$ erfüllt.

Die Menge aller Homomorphismen $M\to N$ bezeichnen wir mit $\operatorname{Hom}(M,N)$.

Beispiel 2B11.
1. Die Exponentialfunktion $\exp\colon(\mathbb{R},+)\to(\mathbb{R},\cdot)$ ist ein Homomorphismus denn sie erfüllt $\exp(x+y)=\exp(x)\cdot\exp(y)$ für alle $x,y\in\mathbb{R}$.
2. Ebenso ist die Logarithmusfunktion $\log\colon(\mathbb{R}_{>0},\cdot)\to(\mathbb{R},+)$ ein Homomorphismus denn sie erfüllt $\log(x\cdot y)=\log(x)+\log(y)$ für alle $x,y\in\mathbb{R}_{>0}$.

Sprech- und Schreibweise. Wenn die in Rede stehende Verknüpfung aus dem Zusammenhang hervorgeht, so spricht man abkürzend von dem Magma M anstelle der korrekten aber schwerfälligen Bezeichnung $(M,*)$. Dieser laxe Sprachgebrauch empfiehlt sich allerdings nur, wenn keine Verwechslungen zu befürchten sind. Um umgekehrt die Verknüpfungen zu betonen, schreibt man zum Beispiel einen Homomorphismus $h\colon M\to N$ gelegentlich auch als $h\colon(M,*)\to(N,\bullet)$.

Proposition 2B12. *Magmen und ihre Homomorphismen bilden eine* Kategorie*:*

1. *Für jedes Magma $(M,*)$ ist die Identität $\mathrm{id}_M\colon M\to M$ ein Homomorphismus.*
2. *Sind $f\colon(A,*)\to(B,\bullet)$ und $g\colon(B,\bullet)\to(C,\cdot)$ Homomorphismen, so ist auch ihre Komposition $g\circ f\colon(A,*)\to(C,\cdot)$ ein Homomorphismus.*
3. *Die Komposition von Homomorphismen $f\colon A\to B$ und $g\colon B\to C$ und $h\colon C\to D$ ist assoziativ, d.h. $(h\circ g)\circ f=h\circ(g\circ f)$.*

BEWEIS. Die Aussage (1) ist klar. Zu (2) rechnen wir nach, dass für alle $a,b\in A$ gilt

$$\begin{aligned}(g\circ f)(a*b)&=g(f(a*b))=g(f(a)\bullet f(b)\\&=g(f(a))\cdot g(f(b))=(g\circ f)(a)\cdot(g\circ f)(b).\end{aligned}$$

Die Aussage (3) gilt für die Komposition beliebiger Abbildungen. □

§**2Bb. Untermagmen.** Ist $(M,*)$ ein Magma und $U\subset M$ eine Teilmenge, so können wir die Verknüpfung einschränken zu $*|_{U\times U}\colon U\times U\to M$. Gilt zudem $U*U\subset U$, so erhalten wir auf U die Verknüpfung $*|_U\colon U\times U\to U$ und nennen $(U,*|_U)$ ein *Untermagma* von M. Die Inklusion $\iota_U^M\colon U\hookrightarrow M$ ist dann ein Homomorphismus $\iota_U^M\colon(U,*|_U)\to(M,*)$.

Proposition 2B13. *Für jeden Homomorphismus $f\colon M\to N$ gilt:*

(a) Für jedes Untermagma $A\subset M$ ist das Bild $f(A)\subset N$ ein Untermagma.
(b) Für jedes Untermagma $B\subset N$ ist das Urbild $f^{-1}(B)\subset M$ ein Untermagma.

BEWEIS. (a) Seien $x,y\in f(A)$. Das bedeutet, es gibt $u,v\in A$ sodass $x=f(u)$ und $y=f(v)$. Hieraus folgt $x\bullet y=f(u)\bullet f(v)=f(u*v)$ mit $u*v\in A$, also $x\bullet y\in f(A)$.

(b) Seien $x,y\in f^{-1}(B)$. Das bedeutet $f(x),f(y)\in B$. Die Multiplikativität von f garantiert $f(x*y)=f(x)\bullet f(y)\in B$. Das bedeutet $x*y\in f^{-1}(B)$. □

§**2Bc. Isomorphismen.** Einen bijektiven Homomorphismus $f\colon A \to B$ nennt man *Isomorphismus*, geschrieben $A \xrightarrow{\sim} B$.

Beispiel 2B14. Die Exponentialfunktion $\exp\colon (\mathbb{R},+) \to (\mathbb{R}_{>0},\cdot)$ und die Logarithmusfunktion $\log\colon (\mathbb{R}_{>0},\cdot) \to (\mathbb{R},+)$ sind zueinander inverse Isomorphismen.

Dieses Beispiel verweist auf folgenden allgemeinen Sachverhalt:

Proposition 2B15. *Für jeden Isomorphismus $f\colon A \to B$ zwischen zwei Magmen $(A,*)$ und $(B,\bullet)$ ist auch die Umkehrabbildung $f^{-1}\colon B \to A$ ein Isomorphismus.*

BEWEIS. Wir haben $f^{-1}(x \bullet y) = f^{-1}(x) * f^{-1}(y)$ für alle $x,y \in B$ zu zeigen. Da f bijektiv ist, gilt $x = f(u)$ und $y = f(v)$ für $u = f^{-1}(x)$ und $v = f^{-1}(y)$. Hieraus erhalten wir $f^{-1}(x \bullet y) = f^{-1}(f(u) \bullet f(v)) = f^{-1}(f(u * v)) = u * v = f^{-1}(x) * f^{-1}(y)$. □

Gibt es zwischen zwei Magmen $(A,*)$ und $(B,\bullet)$ einen Isomorphismus $f\colon A \xrightarrow{\sim} B$, dann nennen wir A und B *isomorph*, geschrieben $A \cong B$. Die beiden Magmen sind im Wesentlichen gleich: der Isomorphismus $f\colon A \xrightarrow{\sim} B$ und der hierzu inverse Isomorphismus $f^{-1}\colon B \to A$ übersetzen alle Eigenschaften von A nach B und zurück von B nach A.

Beispiel 2B16. Ist $f\colon A \to B$ ein injektiver Homomorphismus, dann erhält man durch Einschränkung auf das Bild einen Isomorphismus $f\colon A \to f(A)$ von A auf sein Bild $f(A)$.

Beispiel 2B17. Sind $(M_1,*_1),\dots,(M_n,*_n)$ Magmen, dann ist ihr Produkt

$$M = M_1 \times \cdots \times M_n$$

ein Magma bezüglich der komponentenweisen Verknüpfung

$$(a_1,\dots,a_n) * (b_1,\dots,b_n) = (a_1 *_1 b_1,\dots,a_n *_n b_n).$$

Die Projektion $\pi_k\colon M \to M_k$ mit

$$\pi_k(a_1,\dots,a_{k-1},a_k,a_{k+1},\dots,a_n) = a_k$$

ist ein surjektiver Homomorphismus.

Beispiel 2B18. Sei $(M,*)$ ein Magma und X eine Menge. Dann wird $M^X = \mathrm{Abb}(X,M)$ zu einem Magma mittels der punktweisen Verknüpfung: für $f,g\colon X \to M$ definieren wir $f * g\colon X \to M$ durch $(f*g)(x) = f(x) * g(x)$ für alle $x \in X$. Für $X = \{1,\dots,n\}$ ist dies das vorangehende Beispiel im Spezialfall $(M,*) = (M_1,*_1) = \cdots = (M_n,*_n)$.

Definition 2B19. Für Homomorphismen $f\colon A \to A$ eines Magmas $(A,*)$ in sich selbst sind folgende Begriffe nützlich:

- Ein *Endomorphismus* von A ist ein Homomorphismus $A \to A$ von A in sich. Die Menge aller Endomorphismen von A bezeichnen wir mit $\mathrm{End}(A)$.
- Ein *Automorphismus* von A ist ein Isomorphismus $A \xrightarrow{\sim} A$ von A in sich. Die Menge aller Automorphismen von A bezeichnen wir mit $\mathrm{Aut}(A)$.

Schreibweise. Ausführlicher oder zur Betonung der Verknüpfung $*$ schreibt man besser $\mathrm{End}(A,*)$ und $\mathrm{Aut}(A,*)$. Nur wenn die in Rede stehende Verknüpfung aus dem Zusammenhang hervorgeht, schreibt man abkürzend $\mathrm{End}(A)$ und $\mathrm{Aut}(A)$.

Bemerkung 2B20. Aus Proposition 2B12 folgt, das wir $\mathrm{End}(A)$ mit der Komposition $\circ$ von Endomorphismen ausstatten können: Die Komposition von zwei Endomorphismen ist wieder ein Endomorphismus. Somit erhalten wir auf $\mathrm{End}(A)$ die Verknüpfung

$$\circ\colon \mathrm{End}(A) \times \mathrm{End}(A) \to \mathrm{End}(A)$$

Gleiches gilt für die Menge $\mathrm{Aut}(A)$: Die Komposition von zwei Automorphismen ist wieder ein Automorphismus. Somit erhalten wir auf $\mathrm{Aut}(A)$ die Verknüpfung

$$\circ\colon \mathrm{Aut}(A) \times \mathrm{Aut}(A) \to \mathrm{Aut}(A)$$

Mit dieser Verknüpfung ist $(\mathrm{End}(A), \circ)$ ein Monoid und $(\mathrm{Aut}(A), \circ)$ eine Gruppe.

§2C. Monoide

§2Ca. Neutrale Elemente. Gegeben sei eine Verknüpfung $*\colon M \times M \to M$ auf einer Menge M. Ein Element $e \in M$ heißt *neutral* für die Verknüpfung $*$, wenn für alle $a \in M$ gilt

$$e * a = a * e = a.$$

Beispiel 2C1. Für die Addition $+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ist die Null $0 \in \mathbb{Z}$ neutrales Element.
Für die Multiplikation $\cdot\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ist die Eins $1 \in \mathbb{Z}$ neutrales Element.

Man beachte, dass Neutralität nur bezüglich einer vorgegebenen Verknüpfung einen Sinn hat. Eine Verknüpfung kann höchstens ein neutrales Element haben:

Bemerkung 2C2. Sind $e, f \in M$ beide neutral für $*$, dann gilt $e = e * f = f$.

Es kann durchaus vorkommen, dass eine Verknüpfung gar kein neutrales Element hat:

Beispiel 2C3. Die Subtraktion $-\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ hat kein neutrales Element: 0 ist zwar rechtsneutral im Sinne von $a - 0 = a$ für alle $a \in \mathbb{Z}$, es gibt aber kein linksneutrales Element.

Sprech- und Schreibweisen. Schreibt man die Verknüpfung als Multiplikation $\cdot\colon M \times M \to M$, so nennt man das neutrale Element meist "Eins", geschrieben 1_M oder kurz 1. Schreibt man die Verknüpfung hingegen als Addition $+\colon M \times M \to M$, so nennt man das neutrale Element meist "Null", geschrieben 0_M oder kurz 0. Diese Konvention ist besonders nützlich in den Fällen, wo wir zwei Verknüpfungen auf derselben Menge betrachten, wie im obigen Beispiel $(\mathbb{Z}, +, \cdot)$.

§2Cb. Assoziativität. Eine Verknüpfung $*\colon M \times M \to M$ auf einer Menge M heißt *assoziativ*, wenn $a * (b * c) = (a * b) * c$ für alle $a, b, c \in M$ gilt.

Beispiel 2C4. Die Addition $+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ist assoziativ. Die Subtraktion $-\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ hingegen nicht: zum Beispiel sind $1 - (2 - 3) = 2$ und $(1 - 2) - 3 = -4$ verschieden.

Assoziativität bedeutet, dass die beiden möglichen Klammerungen der Verknüpfung $a * b * c$ dasselbe Ergebnis liefern. Die folgende Proposition verallgemeinert diese Aussage von drei auf eine beliebige Anzahl von Faktoren. Das ist wohl kaum überraschend aber auch nicht selbstverständlich, bedarf also eines Beweises.

Proposition 2C5 (allgemeines Assoziativgesetz)**.** *Sei $*\colon M \times M \to M$ eine assoziative Verknüpfung. Für alle $a_1, a_2, a_3, \ldots, a_n \in M$ liefern dann alle Klammerungen des Produkts $a_1 * a_2 * a_3 * \cdots * a_n$ dasselbe Ergebnis.*

BEWEIS. Wir führen Induktion über n: Für $n \leq 2$ ist nichts zu zeigen, wir können also gleich $n \geq 3$ annehmen. Für $1 \leq i < j < n$ haben wir zu zeigen dass

$$(a_1 * \cdots * a_i) * (a_{i+1} * \cdots * a_n) = (a_1 * \cdots * a_j) * (a_{j+1} * \cdots * a_n)$$

Die Produkte in den Klammern haben Länge $< n$, und nach Induktionsvoraussetzung ist daher die innere Klammersetzung unerheblich. Daraus folgt:

$$\begin{aligned}(a_1 * \cdots * a_i) * (a_{i+1} * \cdots * a_n) &= (a_1 * \cdots * a_i) * ((a_{i+1} * \cdots * a_j) * (a_{j+1} * \cdots * a_n)) \\ &= ((a_1 * \cdots * a_i) * (a_{i+1} * \cdots * a_j)) * (a_{j+1} * \cdots * a_n) = (a_1 * \cdots * a_j) * (a_{j+1} * \cdots * a_n)\end{aligned}$$

Hierbei wurde nur das Assoziativgesetz auf drei Faktoren verwendet. □

§**2Cc. Monoide.** Wir gelangen nun zu der eingangs des Kapitels erwähnten Definition:

Definition 2C6. Ein *Monoid* $(M, *, e)$ ist eine Menge M zusammen mit einer assoziativen Verknüpfung $*\colon M \times M \to M$ und einem für $*$ neutralen Element $e \in M$.

Beispiel 2C7. $(\mathbb{N}, +, 0)$ ist ein Monoid, ebenso $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$.

Des weiteren ist $(\mathbb{N}, \cdot, 1)$ ist ein Monoid, ebenso $(\mathbb{Z}, \cdot, 1)$, $(\mathbb{Q}, \cdot, 1)$, $(\mathbb{R}, \cdot, 1)$, $(\mathbb{C}, \cdot, 1)$.

Hingegen ist $(\mathbb{N}^*, +)$ mit $\mathbb{N}^* = \mathbb{N} \smallsetminus \{0\}$ kein Monoid: zwar definiert die Addition eine assoziative Verknüpfung $+\colon \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*$, allein es fehlt das neutrale Element.

Die Abbildung $*\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ mit $a * b = |a - b|$ hat zwar 0 als neutrales Element, ist aber nicht assoziativ, wie das Gegenbeispiel $|3 - |2 - 1|| = 2$ und $||3 - 2| - 1| = 0$ zeigt.

Sprech- und Schreibweisen. Das neutrale Element $e \in M$ ist durch die Verknüpfung $*\colon M \times M \to M$ eindeutig bestimmt. Es genügt daher, seine Existenz zu fordern. Zur Betonung ist es jedoch gelegentlich vorteilhaft, das Einselement in der Struktur $(M, *, e)$ explizit beim Namen zu nennen. Ist seine Nennung nicht erwünscht, so lässt man es weg und spricht kurz von dem Monoid $(M, *)$. Wenn die Verknüpfung $*$ aus dem Kontext hervorgeht, spricht man noch kürzer von dem Monoid M. Dieser laxe Sprachgebrauch empfiehlt sich allerdings nur, wenn keine Verwechslungen zu befürchten sind.

Beispiel 2C8 (entgegengesetztes Monoid)**.** Ist $(M, *, e)$ ein Monoid, dann ist auch $(M, \bar{*}, e)$ ein Monoid mit der entgegengesetzten Multiplikation $a \mathbin{\bar{*}} b = b * a$. Dieses Monoid nennen wir das zu M *entgegengesetzte Monoid*, geschrieben M^{op}.

Es gilt $M = M^{\mathrm{op}}$ genau dann, wenn das Monoid M kommutativ ist.

§**2Cd. Potenzgesetz in Monoiden.** Für beliebige Elemente $a_1, a_2, a_3, \ldots, a_N \in M$ in einem Magma $(M, *)$ definieren wir das Produkt

$$\prod_{k=1}^{n} a_k = (\cdots((a_1 * a_2) * a_3) \cdots) * a_n$$

für $1 \leq n \leq N$ induktiv wie folgt: Für $n = 1$ setzen wir $\prod_{k=1}^{n} a_k = a_1$. Für $2 \leq n \leq N$ nehmen wir $\prod_{k=1}^{n-1} a_k$ als zuvor definiert an und setzen $\prod_{k=1}^{n} a_k = \bigl(\prod_{k=1}^{n-1} a_k\bigr) * a_n$.

Die von uns gewählte Klammerung erfolgt hier von links nach rechts. Ist $(M, *)$ ein Monoid, so wissen wir vom allgemeinen Assoziativgesetz (2C5), dass die Wahl der Klammerung unerheblich ist. Dies lässt sich nun wie folgt formulieren:

$$\Bigl(\prod_{k=1}^{m} a_k\Bigr) * \Bigl(\prod_{k=1}^{n} a_{m+k}\Bigr) = \prod_{k=1}^{m+n} a_k$$

Für $n = 1$ ist dies obige Definition. Gilt die Gleichung für n, dann auch für $n+1$:

$$\Big(\prod_{k=1}^{m} a_k\Big) * \Big(\prod_{k=1}^{n+1} a_{m+k}\Big) = \Big(\prod_{k=1}^{m} a_k\Big) * \Big[\Big(\prod_{k=1}^{n} a_{m+k}\Big) * a_{m+n+1}\Big]$$
$$= \Big[\Big(\prod_{k=1}^{m} a_k\Big) * \Big(\prod_{k=1}^{n} a_{m+k}\Big)\Big] * a_{m+n+1} = \Big(\prod_{k=1}^{m+n} a_k\Big) * a_{m+n+1} = \prod_{k=1}^{m+n+1} a_k$$

Den wichtigen Spezialfall $a_1 = a_2 = a_3 = \cdots = a_N$ halten wir gesondert fest und definieren die *Potenz* $a^n = a * a * \cdots * a$ (mit n Faktoren) wie folgt:

Proposition 2C9 (Potenzgesetz)**.** *Sei $(M, *, e)$ ein Monoid. Wir definieren die (äußere) Verknüpfung $\hat{}\colon M \times \mathbb{N} \to M$, $(a,n) \mapsto a^n$, durch $a^0 = e$ und induktiv $a^{n+1} = a^n * a$ für alle $n \in \mathbb{N}$. Für alle $a \in M$ und $m, n \in \mathbb{N}$ erfüllt die Potenz die Gleichungen*

$$a^m * a^n = a^{m+n} \quad \text{und} \quad (a^m)^n = a^{mn}.$$

Sprech- und Schreibweisen. Bei multiplikativer Schreibweise $(M, \cdot)$ spricht man von dem *Produkt* $\prod_{k=1}^{n} a_k = a_1 \cdots a_n$ und der *Potenz* $a^n = a \cdots a$ mit n *Faktoren*. Bei additiver Schreibweise $(M, +)$ spricht man von der *Summe* $\sum_{k=1}^{n} a_k = a_1 + \cdots + a_n$ und dem *Vielfachen* $na = a + \cdots + a$ mit n *Summanden*. Das Potenzgesetz schreibt sich dann $ma + na = (m+n)a$ und $m(na) = (mn)a$ für alle $a \in M$ und $m, n \in \mathbb{N}$

§**2Ce. Homomorphismen von Monoiden.** Ein *Homomorphismus* zwischen Monoiden $(M, *, e_M)$ und $(N, \bullet, e_N)$ ist eine Abbildung $h\colon M \to N$, die

$$h(e_M) = e_N \qquad \text{und} \qquad h(a * b) = h(a) \bullet h(b) \qquad \text{für alle } a, b \in M \text{ erfüllt.}$$

Die Menge aller Homomorphismen $M \to N$ bezeichnen wir mit $\mathrm{Hom}(M, N)$.

Proposition 2C10. *Monoide und ihre Homomorphismen bilden eine* Kategorie*:*

1. *Für jedes Monoid M ist die Identität $\mathrm{id}_M\colon M \to M$ ein Monoidhomomorphismus.*
2. *Sind $f\colon A \to B$ und $g\colon B \to C$ Monoidhomomorphismen, so ist auch ihre Komposition $g \circ f\colon A \to C$ ein Monoidhomomorphismus.*
3. *Diese Komposition ist assoziativ, das heißt $(h \circ g) \circ f = h \circ (g \circ f)$.* □

Wir vereinbaren den in jeder Kategorie üblichen Sprachgebrauch:

Definition 2C11. Ein bijektiver Monoidhomomorphismus $f\colon M \to N$ heißt *Isomorphismus*. Falls solch ein Isomorphismus existiert, so nennen wir die Monoide M und N *isomorph*, geschrieben $M \cong N$. Dies ist eine Äquivalenzrelation.

Weiterhin definieren wir:

- Ein *Endomorphismus* von M ist ein Homomorphismus $M \to M$.
  Die Menge aller Endomorphismen von M bezeichnen wir mit $\mathrm{End}(M)$.
- Ein *Automorphismus* von M ist ein Isomorphismus $M \xrightarrow{\sim} M$.
  Die Menge aller Automorphismen von M bezeichnen wir mit $\mathrm{Aut}(M)$.

Beispiel 2C12. Jede einelementige Menge $\{e\}$ ist ein Monoid mit $e * e = e$; dieses wird das *triviale Monoid* genannt. In jeden anderen Monoid $(N, \bullet, e_N)$ existiert genau ein Monoidhomomorphismus $\{e\} \to N$, nämlich $e \mapsto e_N$. Umgekehrt existiert von jedem Monoid $(M, *, e_M)$ aus genau ein Monoidhomomorphismus $M \to \{e\}$.

Beispiel 2C13. Für je zwei Monoide M und N ist die konstante Abbildung $h\colon M \to N$ mit $h(a) = e_N$ für alle $a \in M$ ein Monoidhomomorphismus, der *triviale* Homomorphismus.

Die folgenden Beispiele zeigen nicht-triviale Homomorphismen:

Beispiel 2C14. Sei X eine Menge und $\mathfrak{P}X$ ihre Potenzmenge. Dann sind $(\mathfrak{P}X, \cup, \emptyset)$ und $(\mathfrak{P}X, \cap, X)$ Monoide. Beide sind isomorph mittels der Komplementbildung $A \mapsto X \smallsetminus A$.

Beispiel 2C15. Die Exponentialfunktion $\exp\colon (\mathbb{R}, +, 0) \to (\mathbb{R}_{>0}, \cdot, 1)$ und der Logarithmus $\log\colon (\mathbb{R}_{>0}, \cdot, 1) \to (\mathbb{R}, +, 0)$ sind zueinander inverse Monoidisomorphismen.

Bemerkung 2C16. Für jeden Monoidisomorphismus $f\colon M \xrightarrow{\sim} N$ ist die Umkehrabbildung $f^{-1}\colon N \to M$ ein Monoidisomorphismus. Dies beweist man genauso wie für Magmen (2B15)

Beispiel 2C17. Der Absolutbetrag $|\ |\colon \mathbb{Z} \to \mathbb{N}$ erfüllt $|a \cdot b| = |a| \cdot |b|$ sowie $h(1) = 1$ und ist damit ein Monoidhomomorphismus von $(\mathbb{Z}, \cdot, 1)$ nach $(\mathbb{N}, \cdot, 1)$.

Bemerkung 2C18. Die Bedingung $h(e_M) = e_N$ muss gesondert gefordert werden und folgt nicht automatisch aus der Multiplikativität. Zum Beispiel ist die Abbildung $h\colon \mathbb{Z} \to \mathbb{N}$, mit $h(a) = 0$ für alle $a \in \mathbb{N}$, kein Monoidhomomorphismus von $(\mathbb{Z}, \cdot, 1)$ nach $(\mathbb{N}, \cdot, 1)$: sie erfüllt zwar $h(a \cdot b) = h(a) \cdot h(b)$ für alle $a, b \in M$, aber $h(1) = 0 \neq 1$.

Das Potenzgesetz führt uns auf folgende universelle Eigenschaft des Monoids $(\mathbb{N}, +)$:

Beispiel 2C19. Für jedes Monoid $(M, \cdot)$ und jedes Element $a \in M$ existiert genau ein Monoidhomomorphismus $\mathbb{N} \to M$ mit $1 \mapsto a$, nämlich $\exp_a\colon n \mapsto a^n$.

BEWEIS. Die Abbildung $\exp_a$ ist ein Monoidhomomorphismus; dies ist die Aussage des Potenzgesetzes in §2Cd. Ist umgekehrt $h\colon \mathbb{N} \to M$ ein Homomorphismus mit $h(1) = a$, dann folgt $h(n) = h(1 + \cdots + 1) = h(1) \cdots h(1) = a^n$ für alle $n \in \mathbb{N}$. □

Diese Eigenschaft charakterisiert das Monoid $(\mathbb{N}, +)$ bis auf eindeutige Isomorphie. Wir sagen daher: $(\mathbb{N}, +)$ ist *das freie Monoid* über dem Element 1.

Korollar 2C20. *Die Endomorphismen des Monoids* $(\mathbb{N}, +)$ *sind die Abbildungen* $h_a\colon \mathbb{N} \to \mathbb{N}$ *mit* $h_a(n) = na$. *Für* $a = 0$ *ist* $h_a = 0$ *die Nullabbildung und weder injektiv noch surjektiv. Für* $a \geq 2$ *ist* h_a *injektiv aber nicht surjektiv. Für* $a = 1$ *erhalten wir* $h_1 = \mathrm{id}$. *Demnach gilt* $\mathrm{End}(\mathbb{N}, +) \cong \mathbb{N}$ *mit der Multiplikation als Verknüpfung und* $\mathrm{Aut}(\mathbb{N}, +) = \{\mathrm{id}\}$.

Beispiel 2C21. Sind $(M_1, *_1, e_1), \ldots, (M_n, *_n, e_n)$ Monoide, dann ist ihr Produkt

$$M = M_1 \times \cdots \times M_n$$

ein Monoid bezüglich der komponentenweisen Verknüpfung (2B17). Neutrales Element ist $e = (e_1, \ldots, e_n)$. Die Abbildung $\iota_k\colon M_k \to M$ mit

$$\iota_k(a) = (e_1, \ldots, e_{k-1}, a, e_{k+1}, \ldots, e_n)$$

ist ein injektiver Monoidhomomorphismus. Die Projektion $\pi_k\colon M \to M_k$ mit

$$\pi_k(a_1, \ldots, a_{k-1}, a_k, a_{k+1}, \ldots, a_n) = a_k$$

ist ein surjektiver Monoidhomomorphismus. Es gilt $\pi_k \circ \iota_k = \mathrm{id}_{M_k}$ für alle k. Für $j \neq k$ ist $\pi_j \circ \iota_k\colon M_k \to M_j$ der triviale Monoidhomomorphismus.

Beispiel 2C22. Sei $(M,*,e_M)$ ein Monoid und X eine Menge. Dann wird $M^X = \mathrm{Abb}(X,M)$ zu einem Monoid mittels der punktweisen Verknüpfung (2B18). Neutrales Element ist die konstante Abbildung $e\colon X \to M$ mit $x \mapsto e_M$ für alle $x \in X$.

Der *Träger* einer Abbildung $f\colon X \to M$ ist die Menge $\{x \in X \mid f(x) \neq e_M\}$. Die Menge $M^{(X)}$ aller Abbildungen $f\colon X \to M$ mit endlichem Träger ist ein Monoid bezüglich der punktweisen Verknüpfung. Für eine endliche Menge X gilt $M^X = M^{(X)}$; für eine unendliche Menge X hingegen ist $M^{(X)}$ strikt kleiner als M^X.

§**2Cf. Untermonoide.** Eine Teilmenge $U \subset M$ eines Monoids $(M,*,1)$ heißt *Untermonoid* falls $1 \in U$ gilt und $U * U \subset U$.

In diesem Fall ist $(U,*,1)$ selbst ein Monoid bezüglich der Einschränkung $*\colon U \times U \to U$, und die Inklusion $\iota_U^M\colon U \hookrightarrow M$ ist ein Monoidhomomorphismus.

Proposition 2C23. *Für jeden Monoidhomomorphismus $f\colon M \to N$ gilt:*

(a) Für jedes Untermonoid $A \subset M$ ist das Bild $f(A) \subset N$ ein Untermonoid.
(b) Für jedes Untermonoid $B \subset N$ ist das Urbild $f^{-1}(B) \subset M$ ein Untermonoid.

BEWEIS. Dies folgt wie für Magmen (2B13) zusammen mit der für Monoidhomomorphismen geforderten Bedingung $f(e_M) = e_N$. □

Beispiel 2C24. Für jedes $a \in \mathbb{N}$ ist die Menge $a\mathbb{N}$ ein Untermonoid von $(\mathbb{N},+,0)$. Dies ist das Bild des Endomorphismus $h\colon \mathbb{N} \to \mathbb{N}$ mit $h(n) = an$. Für $a \neq 0$ ist h injektiv, und somit $h\colon \mathbb{N} \xrightarrow{\sim} a\mathbb{N}$ ein Isomorphismus zwischen den Monoiden $(\mathbb{N},+,0)$ und $(a\mathbb{N},+,0)$.

§**2Cg. Erzeugte Untermonoide.**

Proposition 2C25. *Ist $(U_i)_{i\in I}$ eine Familie von Untermonoiden $U_i \subset M$ eines Monoids $(M,*)$, dann ist auch ihr Durchschnitt $U = \bigcap_{i\in I} U_i$ ein Untermonoid.*

BEWEIS. Es gilt $1 \in U_i$ für alle $i \in I$, also auch $1 \in U$. Für $a,b \in U$ gilt $a,b \in U_i$ für alle $i \in I$, also $a * b \in U_i$ für alle $i \in I$, also auch $a * b \in U$. □

Definition 2C26. Sei $X \subset M$ eine Teilmenge eines Monoids $(M,*)$. Sei $\langle X\rangle^+$ der Durchschnitt aller Untermonoide von M, die X enthalten. Dann ist $\langle X\rangle^+$ das kleinste Untermonoid von M, das X enthält, und heißt das *von X erzeugte Untermonoid*.

Proposition 2C27. *Es gilt* $\langle X\rangle^+ = \{\, x_1^{e_1} \cdots x_n^{e_n} \mid n \geq 0;\ x_1,\dots,x_n \in X;\ e_1,\dots,e_n \in \mathbb{N} \,\}$.

BEWEIS. Es gilt "$\supset$", denn $\langle X\rangle^+$ ist ein Untermonoid, das X enthält, also auch alle Produkte. Es gilt "$\subset$", denn auch die rechte Seite ist ein Untermonoid, das X enthält. □

Beispiel 2C28. Im Monoid $(\mathbb{N},+)$ gilt $\langle a\rangle^+ = a\mathbb{N}$ für jedes $a \in \mathbb{N}$.
Für $X = \{3,5\}$ gilt $\langle 3,5\rangle^+ = 3\mathbb{N} + 5\mathbb{N} = \{0,3,5,6,8,9,10,11,12,\dots\}$.

§**2Ch. Zyklische Monoide.** Ein Monoid M heißt *monogen* oder *zyklisch*, wenn es von einem einzigen Element erzeugt wird. Das heißt, es gibt ein Element $a \in N$ sodass $M = \langle a\rangle^+$ gilt, oder anders gesagt, jedes Element von M ist eine Potenz a^k mit $k \in \mathbb{N}$. In diesem Fall nennt man a ein *erzeugendes Element* oder einen *Erzeuger* von M.

Beispiel 2C29. Das Monoid $(\mathbb{N},+)$ wird von dem Element 1 erzeugt.

Zur Klassifikation zyklischer Monoide siehe §2Gb.

§2D. Gruppen

§2Da. Invertierbare Elemente. Zwei Elemente a,b in einem Monoid $(M,*,e)$ heißen *zueinander invers* wenn $a*b=b*a=e$ gilt. Ein Element $a\in M$ heißt *invertierbar*, falls ein zu a inverses Element $b\in M$ existiert. In diesem Fall ist b eindeutig durch a bestimmt:

Bemerkung 2D1. Aus $a*b=e$ und $b'*a=e$ folgt

$$b=e*b=(b'*a)*b=b'*(a*b)=b'*e=b'.$$

Daher bezeichnen wir das zu a inverse Element (falls es existiert) unmissverständlich mit a^{-1}. Zum Beispiel ist das neutrale Element $e\in M$ invertierbar mit $e^{-1}=e$.

Für den Begriff der Invertierbarkeit benötigen wir nur das neutrale Element. Zur Eindeutigkeit des Inversen hingegen ist die Assoziativität wesentlich. Ist die Verknüpfung nicht assoziativ, so kann ein Element durchaus mehrere Inverse haben, wie die folgende Verknüpfungstafel vorführt.

·	a	b	c
a	a	b	c
b	b	a	c
c	b	b	a

Definition 2D2. Die Teilmenge der invertierbaren Elemente eines Monoids $(M,*)$ bezeichnen wir mit $M^\times$. Auf dieser Menge erhalten wir die Abbildung ${}^{-1}\colon M^\times\to M^\times$, geschrieben $a\mapsto a^{-1}$, die $a*a^{-1}=a^{-1}*a=e$ erfüllt.

Schreibweisen. Bei multiplikativer Schreibweise $(M,\cdot)$ wird das zu a inverse Element als a^{-1} geschrieben. Bei additiver Schreibweise $(M,+)$ wird das zu a inverse Element als $-a$ geschrieben.

Beispiel 2D3. In $(\mathbb{N},+)$ ist nur 0 invertierbar. In $(\mathbb{N},\cdot)$ ist nur 1 invertierbar.

In $(\mathbb{Z},+)$ sind alle Elemente invertierbar. In $(\mathbb{Z},\cdot)$ sind nur 1 und -1 invertierbar.

In $(\mathbb{Q},+,0)$ sind alle Elemente invertierbar. In $(\mathbb{Q},\cdot)$ sind alle Elemente $a\neq 0$ invertierbar. Entsprechendes gilt für $\mathbb{R}$ und $\mathbb{C}$.

Im jedem Endomorphismenmonoid $\mathrm{End}(A)$ gilt $\mathrm{End}(A)^\times=\mathrm{Aut}(A)$.

Proposition 2D4. *Sei $(M,*,e)$ ein Monoid. Für jedes invertierbare Element $a\in M^\times$ ist auch a^{-1} invertierbar und es gilt $(a^{-1})^{-1}=a$.*

Für je zwei invertierbare Elemente $a,b\in M^\times$ in einem Monoid $(M,*,e)$ ist auch ihr Produkt $a*b$ invertierbar und es gilt $(a*b)^{-1}=b^{-1}*a^{-1}$.

BEWEIS. Die erste Aussage ist klar wegen $a*a^{-1}=a^{-1}*a=e$.

Die zweite Aussage lässt sich leicht aus der Assoziativität ableiten:

$$(a*b)*(b^{-1}*a^{-1})=a*(b*b^{-1})*a^{-1}=a*a^{-1}=e,$$
$$(b^{-1}*a^{-1})*(a*b)=b^{-1}*(a^{-1}*a)*b=b^{-1}*b=e.\qquad\square$$

Das bedeutet, dass die Menge $M^\times$ der invertierbaren Elemente ein Untermonoid bildet. In diesem Monoid $(M^\times,*,e)$ ist nach Definition jedes Element invertierbar. Damit sind wir beim eingangs des Kapitels erwähnten Begriff der Gruppe angelangt:

Nach unserer Vorarbeit können wir nun den Gruppenbegriff wie folgt zusammenfassen:

Definition 2D5. Eine *Gruppe* ist ein Monoid, in dem jedes Element invertierbar ist.

Beispiel 2D6. $(\mathbb{Z},+)$ ist eine Gruppe, ebenso $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$.

Des weiteren ist $(\mathbb{Q}^*,\cdot)$ mit $\mathbb{Q}^* = \mathbb{Q} \smallsetminus \{0\}$ eine Gruppe, ebenso $(\mathbb{R}^*,\cdot)$ und $(\mathbb{C}^*,\cdot)$.

Hingegen ist das Monoid $(\mathbb{N},+)$ keine Gruppe: Natürliche Zahlen $n > 0$ haben in $\mathbb{N}$ keine additiven Inversen; dieses Manko wird durch die Vervollständigung zur Gruppe $(\mathbb{Z},+)$ der ganzen Zahlen behoben. Ebenso ist $(\mathbb{Z}^*,\cdot)$ mit $\mathbb{Z}^* = \mathbb{Z} \smallsetminus \{0\}$ keine Gruppe: ganze Zahlen $a \neq \pm 1$ haben in $\mathbb{Z}^*$ keine multipliaktiven Inversen; dieses Manko wird durch die Vervollständigung zur Gruppe $(\mathbb{Q}^*,\cdot)$ der rationalen Zahlen behoben.

Beispiel 2D7 (symmetrische Gruppen)**.** Die Permutationen der Menge $X = \{1,2,\dots,n\}$ bilden die symmetrische Gruppe S_n mit der Komposition von Abbildungen als Verknüpfung. Allgemein bilden zu jeder Menge X die Bijektionen $X \to X$ die symmetrische Gruppe $\mathrm{Sym}(X)$ mit der Komposition als Verknüpfung.

Beispiel 2D8 (entgegengesetzte Gruppe)**.** Ist $(G,*)$ eine Gruppe, dann ist auch $(G,\bar{*})$ eine Gruppe mit der entgegengesetzten Multiplikation $a \mathbin{\bar{*}} b = b * a$. Diese Gruppe nennen wir die zu G *entgegengesetzte Gruppe*, geschrieben G^{op}.

Es gilt $G = G^{\mathrm{op}}$ genau dann, wenn die Gruppe G kommutativ ist.

Schreibweisen. Ist $(G,*,e)$ eine Gruppe, dann ist das neutrale Element $e \in G$ durch die Verknüpfung $*\colon G \times G \to G$ eindeutig bestimmt. In der Bezeichnung lässt man es daher weg und spricht kurz von der Gruppe $(G,*)$. Wenn die Verknüpfung $*$ aus dem Kontext hervorgeht, spricht man noch kürzer von der Gruppe G. Dieser laxe Sprachgebrauch empfiehlt sich allerdings nur, wenn keine Verwechslungen zu befürchten sind.

Beispiel 2D9 (lineare Gruppen)**.** In der linearen Algebra spielt die allgemeine lineare Gruppe $\mathrm{GL}_n(\mathbb{R})$ eine wichtige Rolle: Diese besteht aus allen invertierbaren $n \times n$-Matrizen über $\mathbb{R}$ mit der Matrizenmultiplikation als Verknüpfung. Diese Gruppe enthält auch die spezielle lineare Gruppe $\mathrm{SL}_n(\mathbb{R})$, die orthogonale Gruppe $\mathrm{O}_n(\mathbb{R})$ und die die spezielle orthogonale Gruppe $\mathrm{SO}_n(\mathbb{R})$, die in der Mathematik und in der Physik eine wichtige Rolle spielen.

Beispiel 2D10 (Isometriegruppen)**.** Die Isometrien des euklidischen Raumes $\mathbb{R}^n$ bilden eine Gruppe $\mathrm{Isom}(\mathbb{R}^n)$ mit der Komposition von Abbildungen als Verknüpfung. Diese Gruppe enthält auch die Translationsgruppe $\mathrm{Trans}(\mathbb{R}^n)$ und die Rotationsgruppe $\mathrm{SO}(\mathbb{R}^n)$.

Zu jedem geometrischen Körper $K \subset \mathbb{R}^n$ gehört die Gruppe $\mathrm{Isom}(K)$ seiner Isometrien. Dies ist die Untergruppe von $\mathrm{Isom}(\mathbb{R}^n)$ aller Isometrien, die K auf sich selbst abbilden, zusammen mit der Komposition von Abbildungen als Verknüpfung. So erhält man zum Beispiel die Diedergruppe als Isometriegruppe des regelmäßigen n-Ecks in der Ebene.

Bemerkung 2D11 (Automorphismengruppen)**.** Für jedes mathematisches Objekt X bilden die invertierbaren Abbildungen $X \to X$ eine Gruppe bezüglich Komposition. Hierbei verlangt man strukturerhaltende Abbildungen, also Automorphismen von X, und die so entstehende Gruppe $\mathrm{Aut}(X)$ heißt dann Automorphismengruppe. Dies ist die eingangs des Kapitels hervorgehobene universelle Bedeutung des Gruppenbegriffs.

§**2Db. Äquivalente Definitionen.** In der obigen Darstellung sind wir über Monoide zum Begriff der Gruppe gelangt. Die folgenden zwei Charakterisierungen präsentieren zwei alternative Definitionen, die zum selben Begriff führen.

Proposition 2D12. *Eine Menge G mit einer assoziativen Verknüpfung $*\colon G\times G\to G$ ist genau dann eine Gruppe, wenn es ein linksneutrales Element $e\in G$ gibt sodass $e*a=a$ für alle $a\in G$ gilt, und zu jedem $a\in G$ ein linksinverses Element a^{-1} existiert sodass $a^{-1}*a=e$.*

Entsprechendes gilt wenn man ein rechtneutrales Element und Rechtsinverse fordert.

BEWEIS. Jedes linksinverse Element ist auch rechtsinvers, denn für $a\in G$ gilt:

$$\begin{aligned}a*a^{-1}&=e*(a*a^{-1})=((a^{-1})^{-1}*a^{-1})*(a*a^{-1})=(a^{-1})^{-1}*(a^{-1}*(a*a^{-1}))\\&=(a^{-1})^{-1}*((a^{-1}*a)*a^{-1})=(a^{-1})^{-1}*(e*a^{-1})=(a^{-1})^{-1}*a^{-1}=e.\end{aligned}$$

Jedes linksneutrale Element ist auch rechtsneutral, denn für beliebiges $a\in G$ gilt:

$$a*e=a*(a^{-1}*a)=(a*a^{-1})*a=e*a=a.$$ □

Die folgende Charakterisierung geht von einer einfachen Beobachtung aus: In jeder Gruppe $(G,*)$ hat zu gegebenen Elementen $a,b\in G$ die Gleichung $a*x=b$ genau eine Lösung $x\in G$, nämlich $x=a^{-1}*b$. Ebenso hat die Gleichung $y*a=b$ genau eine Lösung $y\in G$, nämlich $y=b*a^{-1}$. Diese Eigenschaft charakterisiert Gruppen in folgendem Sinne:

Proposition 2D13. *Eine nicht-leere Menge G mit einer assoziativen Verknüpfung $*\colon G\times G\to G$ ist genau dann eine Gruppe, wenn für jedes Paar $a,b\in G$ die Gleichung $a*x=b$ eine Lösung $x\in G$ hat und ebenso die Gleichung $y*a=b$ eine Lösung $y\in G$ hat.*

BEWEIS. Da G nicht-leer ist, können wir ein Element $a\in G$ wählen. Zu diesem gibt es ein Element $e\in G$, sodass $e*a=a$ gilt. Zu jedem anderen Element $b\in G$ gibt es $y\in G$, sodass $a*y=b$ gilt. Daraus folgt

$$e*b=e*(a*y)=(e*a)*y=a*y=b.$$

Also ist $e\in G$ linksneutral für die Verknüpfung $*$. Für jedes Element $a\in G$ existiert ein Element $y\in G$, sodass $y*a=e$ gilt; dieses ist also ein zu a linksinverses Element. Wir schließen mit Hilfe der vorigen Proposition. □

§**2Dc. Potenzgesetz in Gruppen.** Sei $(G,*,1)$ eine Gruppe. Für $a\in G$ und $n\in\mathbb{N}$ definieren wir die *Potenz* $a^n=a*a*\cdots*a$ (mit n Faktoren) wie für Monoide in §2Cd.

Da a invertierbar ist, können wir nun negative Potenzen definieren durch

$$a^{-n}=(a^{-1})^n=a^{-1}*a^{-1}*\cdots*a^{-1}.$$

Nach obigen Rechenregeln stimmt dies überein mit

$$a^{-n}=(a^{-n})^{-1}=(a*a*\cdots*a)^{-1}.$$

Proposition 2D14 (Potenzgesetz)**.** *Auf jeder Gruppe $(G,*,1)$ definieren wir die (äußere) Verknüpfung $\hat{}\colon G\times\mathbb{Z}\to G$ durch $(a,n)\mapsto a^n$. Für alle $a\in G$ und $m,n\in\mathbb{Z}$ gilt*

$$a^m*a^n=a^{m+n}\quad\text{und}\quad(a^m)^n=a^{mn}.$$

Sprech- und Schreibweisen. Bei multiplikativer Schreibweise $(G,\cdot)$ spricht man von der *Potenz* $G\times\mathbb{Z}\to G$ mit $(a,n)\mapsto a^n$. Bei additiver Schreibweise $(G,+)$ spricht man von dem *Vielfachen* $\mathbb{Z}\times G\to G$ mit $(n,a)\mapsto na$. Das Potenzgesetz schreibt sich dann $(m+n)a=ma+na$ und $m(na)=(mn)a$ für alle $a\in G$ und $m,n\in\mathbb{Z}$.

§**2Dd. Homomorphismen von Gruppen.** Ein *Homomorphismus* zwischen Gruppen $(G,*)$ und $(H,\bullet)$ ist eine Abbildung $h\colon G\to H$, die

$$h(a*b)=h(a)\bullet h(b) \qquad \text{für alle } a,b\in G \text{ erfüllt.}$$

Bemerkung 2D15. Anders als bei Monoiden folgt aus der Multiplikativität automatisch $h(e_G)=e_H$: es gilt $h(e_G)=h(e_G*e_G)=h(e_G)\bullet h(e_G)$, und nach Multiplikation mit $h(e_G)^{-1}$ folgt hieraus $e_H=h(e_G)$. Ebenso automatisch folgt $h(a^{-1})=h(a)^{-1}$ für alle $a\in G$, denn $e_H=h(e_G)=h(a*a^{-1})=h(a)\bullet h(a^{-1})$.

Beispiel 2D16.
1. Die Exponentialfunktion $\exp\colon(\mathbb{R},+)\to(\mathbb{R},\cdot)$ ist ein Gruppenhomomorphismus denn sie erfüllt $\exp(x+y)=\exp(x)\cdot\exp(y)$ für alle $x,y\in\mathbb{R}$.
2. Ebenso ist die Logarithmusfunktion $\log\colon(\mathbb{R}_{>0},\cdot)\to(\mathbb{R},+)$ ein Gruppenhomomorphismus denn sie erfüllt $\log(x\cdot y)=\log(x)+\log(y)$ für alle $x,y\in\mathbb{R}_{>0}$.

Proposition 2D17. *Gruppen und ihre Homomorphismen bilden eine* Kategorie*:*

1. *Für jede Gruppe G ist die Identität $\mathrm{id}_G\colon G\to G$ ein Gruppenhomomorphismus.*
2. *Sind $f\colon G\to H$ und $g\colon H\to K$ Gruppenhomomorphismen, so ist auch ihre Komposition $g\circ f\colon G\to K$ ein Gruppenhomomorphismus.*
3. *Diese Komposition ist assoziativ, das heißt $(h\circ g)\circ f=h\circ(g\circ f)$.* □

Beispiel 2D18. Jede einelementige Menge $\{e\}$ ist eine Gruppe mit $e*e=e$; dieses wird die *triviale Gruppe* genannt. In jede andere Gruppe $(H,\bullet,e_H)$ existiert genau ein Homomorphismus $\{e\}\to H$, nämlich $e\mapsto e_H$. Umgekehrt existiert von jeder Gruppe $(G,*,e_G)$ aus genau ein Homomorphismus $G\to\{e\}$.

Beispiel 2D19. Für je zwei Gruppen G und H ist die konstante Abbildung $h\colon G\to H$ mit $h(g)=e_H$ für alle $g\in G$ ein Gruppenhomomorphismus, der *triviale* Homomorphismus.

Wir vereinbaren den in jeder Kategorie üblichen Sprachgebrauch:

Definition 2D20. Ein bijektiver Gruppenhomomorphismus $f\colon G\to H$ heißt *Isomorphismus*. Weiterhin definieren wir:

- Ein *Endomorphismus* von G ist ein Homomorphismus $G\to G$.
  Die Menge aller Endomorphismen von G bezeichnen wir mit $\mathrm{End}(G)$.
- Ein *Automorphismus* von G ist ein Isomorphismus $G\xrightarrow{\sim}G$.
  Die Menge aller Automorphismen von G bezeichnen wir mit $\mathrm{Aut}(G)$.

Beispiel 2D21. Jede Gruppe G ist zu ihrer entgegengesetzten Gruppe G^{op} (2D8) isomorph vermöge der Abbildung $\varphi\colon G\xrightarrow{\sim}G^{\mathrm{op}}$ mit $\varphi(g)=g^{-1}$, siehe 2D4.

Dies ist insofern bemerkenswert, da die entsprechende Aussage für Monoide nicht gilt. Für jede Menge X mit $|X|\geq 2$ ist das Monoid $\mathrm{Abb}(X)$ mit der Verknüpfung $(f\circ g)(x)=f(g(x))$ nicht isomorph zum entgegengesetzten Monoid $\mathrm{Abb}(X)^{\mathrm{op}}$ mit der Verknüpfung $(f\mathbin{\bar\circ}g)(x)=g(f(x))$. In $\mathrm{Abb}(X)$ erfüllt jede konstanten Abbildung $c\colon X\to\{x\}\subset X$ nämlich $c\circ g=c$ für alle $g\in\mathrm{Abb}(X)$, und es gibt keine Abbildung $f\in\mathrm{Abb}(X)$ mit $g\circ f=f$ für alle $g\in\mathrm{Abb}(X)$. Im Monoid $\mathrm{Abb}(X)^{\mathrm{op}}$ ist es genau umgekehrt, also gilt $\mathrm{Abb}(X)\ncong\mathrm{Abb}(X)^{\mathrm{op}}$.

Beispiel 2D22. Die Exponentialfunktion $\exp\colon(\mathbb{R},+,0)\to(\mathbb{R},\cdot,1)$ und der Logarithmus $\log\colon(\mathbb{R}_{>0},\cdot,1)\to(\mathbb{R},+,0)$ sind zueinander inverse Gruppenisomorphismen.

Bemerkung 2D23. Für jeden Gruppenisomorphismus $f\colon G \xrightarrow{\sim} H$ ist die Umkehrabbildung $f^{-1}\colon H \to G$ ein Gruppenisomorphismus. Dies beweist man wie für Monoide (2C16).

Beispiel 2D24. Die Abbildung $\varphi\colon \mathbb{R} \to \mathbb{C}^\times$ mit $\varphi(t) = \exp(it) = \cos(t) + i\sin(t)$ ist ein surjektiver Homomorphismus der Gruppe $(\mathbb{R},+)$ auf die Gruppe $(\mathbb{C}^\times,\cdot)$. Dieser ist nicht injektiv: Es gilt $\varphi(t) = 0$ genau dann wenn $t \in 2\pi\mathbb{Z}$.

Beispiel 2D25 (aus der linearen Algebra)**.**
1. Jeder Homomorphismen $\varphi\colon V \to W$ von Vektorräumen über einem Körper ist insbesondere ein Gruppenhomomorphismus von $(V,+)$ nach $(W,+)$.
2. Die Determinante definiert einen Gruppenhomomorphismus $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$.
3. Die Signatur definiert einen Gruppenhomomorphismus $\mathrm{sign}\colon S_n \to \{\pm 1\}$.

Das Potenzgesetz führt uns auf folgende universelle Eigenschaft der Gruppe $(\mathbb{Z},+)$:

Beispiel 2D26. Für jede Gruppe $(G,\cdot)$ und jedes Element $a \in G$ existiert genau ein Gruppenhomomorphismus $\mathbb{Z} \to G$ mit $1 \mapsto a$, nämlich $\exp_a\colon n \mapsto a^n$.

BEWEIS. Die Abbildung $\exp_a$ ist ein Gruppenhomomorphismus; dies ist die Aussage des Potenzgesetzes in §2Dc. Sei umgekehrt $h\colon \mathbb{Z} \to G$ ein Homomorphismus mit $h(1) = a$. Daraus folgt $h(n) = h(1+\cdots+1) = h(1)\cdots h(1) = a^n$ für alle $n \in \mathbb{N}$, und damit auch $h(-n) = h(n)^{-1} = a^{-n}$. □

Diese Eigenschaft charakterisiert die Gruppe $(\mathbb{Z},+)$ bis auf eindeutige Isomorphie. Wir sagen daher: $(\mathbb{Z},+)$ ist *die freie Gruppe* über dem Element 1.

Korollar 2D27. *Die Endomorphismen der Gruppe* $(\mathbb{Z},+)$ *sind die Abbildungen* $h_a\colon \mathbb{Z} \to \mathbb{Z}$ *mit* $h_a(n) = na$. *Für* $a = 0$ *ist* $h_a = 0$ *die Nullabbildung und weder injektiv noch surjektiv. Für* $|a| \geq 2$ *ist* h_a *injektiv aber nicht surjektiv. Für* $a = \pm 1$ *erhalten wir* $\pm\mathrm{id}$. *Demnach gilt* $\mathrm{End}(\mathbb{Z},+) \cong \mathbb{Z}$ *mit der Multiplikation als Verknüpfung und* $\mathrm{Aut}(\mathbb{Z},+) = \{\pm\mathrm{id}\}$.

Beispiel 2D28. Sind $(G_1,*_1,e_1),\ldots,(G_n,*_n,e_n)$ Gruppen, dann ist ihr Produkt

$$G = G_1 \times \cdots \times G_n$$

eine Gruppe bezüglich der komponentenweisen Verknüpfung (2B17). Neutrales Element ist $e = (e_1,\ldots,e_n)$. Das zu $a = (a_1,\ldots,a_n)$ inverse Element ist $a^{-1} = (a_1^{-1},\ldots,a_n^{-1})$. Die Abbildung $\iota_k\colon G_k \to G$ mit

$$\iota_k(a) = (e_1,\ldots,e_{k-1},a,e_{k+1},\ldots,e_n)$$

ist ein injektiver Gruppenhomomorphismus. Die Projektion $\pi_k\colon G \to G_k$ mit

$$\pi_k(a_1,\ldots,a_{k-1},a_k,a_{k+1},\ldots,a_n) = a_k$$

ist ein surjektiver Gruppenhomomorphismus. Es gilt $\pi_k \circ \iota_k = \mathrm{id}_{G_k}$ für alle k. Für $j \neq k$ ist $\pi_j \circ \iota_k\colon G_k \to G_j$ der triviale Gruppenhomomorphismus.

Beispiel 2D29. Sei $(G,*,e_G)$ eine Gruppe und X eine Menge. Dann wird $G^X = \mathrm{Abb}(X,G)$ zu einer Gruppe mittels der punktweisen Verknüpfung (2B18). Neutrales Element ist die konstante Abbildung $e\colon X \to G$ mit $x \mapsto e_G$ für alle $x \in X$. Das zu $f\colon X \to G$ inverse Element ist $g\colon X \to G$ mit $g(x) = f(x)^{-1}$ für alle $x \in X$. Gleiches gilt für die Menge $M^{(X)}$ aller Abbildungen $f\colon X \to M$ mit endlichem Träger (2C22).

§**2De. Untergruppen.** Sei $(G,*,1)$ eine Gruppe. Eine Teilmenge $U \subset G$ heißt *Untergruppe*, geschrieben $U < G$, falls $1 \in U$ gilt und $U * U \subset U$ sowie $U^{-1} \subset U$.

Ausführlicher bedeutet dies:

1. Die Menge U enthält das neutrale Element der Gruppe G, also $1 \in U$.
2. Zu je zwei Elementen $a,b \in U$ enthält U auch deren Produkt, also $a * b \in U$.
3. Zu jedem Element $a \in U$ enthält U auch dessen Inverses, also $a^{-1} \in U$.

In diesem Fall ist $(U,*,1)$ selbst eine Gruppe bezüglich der Einschränkung $*\colon U \times U \to U$, und die Inklusion $\iota_U^G\colon U \hookrightarrow G$ ist ein Gruppenhomomorphismus.

Beispiel 2D30.
- In jeder Gruppe $(G,*,e)$ sind $\{e\}$ und G Untergruppen.
- $\mathbb{Z}$ ist eine Untergruppe der additiven Gruppe $(\mathbb{Q},+,0)$ der rationalen Zahlen.
- $\mathbb{N}$ ist keine Untergruppe der additiven Gruppe $(\mathbb{Z},+,0)$ der ganzen Zahlen.

Beispiel 2D31. Für jedes $a \in \mathbb{Z}$ ist die Menge $a\mathbb{Z}$ eine Untergruppe von $(\mathbb{Z},+,0)$. Dies ist das Bild des Endomorphismus $h\colon \mathbb{Z} \to \mathbb{Z}$ mit $h(n) = an$. Für $a \neq 0$ ist h injektiv, und somit $h\colon \mathbb{Z} \xrightarrow{\sim} a\mathbb{Z}$ ein Isomorphismus zwischen den Gruppen $(\mathbb{Z},+,0)$ und $(a\mathbb{Z},+,0)$.

Proposition 2D32. *Eine Teilmenge $U \subset G$ einer Gruppe $(G,*)$ ist genau dann eine Untergruppe wenn U nicht-leer ist und $U * U^{-1} \subset U$ erfüllt, also $a * b^{-1} \in U$ für alle $a,b \in U$.*

BEWEIS. Ist U eine Untergruppe, so ist U nicht-leer wegen $1 \in U$, und für alle $a,b \in U$ gilt $b^{-1} \in U$ und damit $a * b^{-1} \in U$. Nehmen wir umgekehrt an, U ist nicht-leer und für alle $a,b \in U$ gilt $a * b^{-1} \in U$. Wir wählen $a \in U$ und erhalten $1 = a * a^{-1} \in U$. Für alle $b \in U$ folgt daraus $b^{-1} = 1 * b^{-1} \in U$. Für alle $a,b \in U$ gilt schließlich $a * b = a * (b^{-1})^{-1} \in U$. □

Proposition 2D33. *Für jeden Gruppenhomomorphismus $f\colon G \to H$ gilt:*

(a) Für jede Untergruppe $A \subset G$ ist das Bild $f(A) \subset H$ eine Untergruppe.
(b) Für jede Untergruppe $B \subset H$ ist das Urbild $f^{-1}(B) \subset G$ eine Untergruppe.

BEWEIS. Dies folgt wie für Monoide (2C23) zusammen mit der Tatsache, dass jeder Gruppenhomomorphismus f auch $f(g^{-1}) = f(g)^{-1}$ für alle $g \in G$ erfüllt (2D15). □

Beispiel 2D34. Für jeden Gruppenhomomorphismus $f\colon G \to H$ ist das Bild $\operatorname{im}(f) = f(G)$ eine Untergruppe von H und der Kern $\ker(f) = f^{-1}(\{1_H\})$ eine Untergruppe von G.

Wir halten das folgende nützliche Injektivitätskriterium fest:

Proposition 2D35. *Ein Gruppenhomomorphismus $f\colon G \to H$ ist genau dann injektiv wenn $\ker(f) = \{1_G\}$ gilt.*

BEWEIS. Für $a,b \in G$ gilt $f(a) = f(b)$ genau dann wenn $ab^{-1} \in \ker(f)$ gilt, denn

$$f(a) = f(b) \quad \Leftrightarrow \quad f(a)f(b)^{-1} = 1 \quad \Leftrightarrow \quad f(ab^{-1}) = 1 \quad \Leftrightarrow \quad ab^{-1} \in \ker(f).$$

Ist $\ker(f) = \{1_G\}$, dann ist dies nur für $a = b$ möglich. □

Beispiel 2D36. Für $\varphi\colon \mathbb{R} \to \mathbb{C}^\times$ mit $\varphi(t) = \exp(it) = \cos(t) + i\sin(t)$ gilt $\ker(\varphi) = 2\pi\mathbb{Z}$. Daher gilt $\varphi(a) = \varphi(b)$ genau dann wenn $a - b \in 2\pi\mathbb{Z}$.

§2Df. Erzeugte Untergruppen.

Proposition 2D37. *Ist $(U_i)_{i\in I}$ eine Familie von Untergruppen $U_i \subset G$ einer Gruppe $(G,*)$, dann ist auch ihr Durchschnitt $U = \bigcap_{i\in I} U_i$ eine Untergruppe.*

BEWEIS. Es gilt $1 \in U_i$ für alle $i \in I$, also auch $1 \in U$. Für $a,b \in U$ gilt $a,b \in U_i$ für alle $i \in I$, also $a * b^{-1} \in U_i$ für alle $i \in I$, also auch $a * b^{-1} \in U$. □

Definition 2D38. Sei $X \subset G$ eine Teilmenge einer Gruppe $(G,*)$. Sei $\langle X\rangle$ der Durchschnitt aller Untergruppen von G, die X enthalten. Dann ist $\langle X\rangle$ die kleinste Untergruppe von M, die X enthält, und heißt die *von X erzeugte Untergruppe*.

Proposition 2D39. *Es gilt* $\langle X\rangle = \{\, x_1^{e_1} \cdots x_n^{e_n} \mid n \geq 0;\ x_1,\ldots,x_n \in X;\ e_1,\ldots,e_n \in \mathbb{Z} \,\}$.

BEWEIS. Es gilt "$\supset$", denn $\langle X\rangle$ ist eine Untergruppe, die X enthält, also auch alle Inversen und Produkte von Elementen aus X. Es gilt "$\subset$", denn auch die rechte Seite ist eine Untergruppe, die X enthält. □

Beispiel 2D40. In der Gruppe $(\mathbb{Z},+)$ gilt $\langle a\rangle = a\mathbb{Z}$ für jedes $a \in \mathbb{Z}$.
Für $X = \{3,5\}$ gilt $\langle 3,5\rangle = 3\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$.
Für $X = \{9,12\}$ gilt $\langle 9,12\rangle = 9\mathbb{Z} + 12\mathbb{Z} = 3\mathbb{Z}$.

Allgemein werden wir für die Gruppe $(\mathbb{Z},+)$ später zeigen, dass $\langle a,b\rangle = \mathrm{ggT}(a,b)\cdot\mathbb{Z}$.

§2Dg. Zyklische Gruppen. Eine Gruppe G heißt *monogen* oder *zyklisch*, wenn sie von einem einzigen Element erzeugt wird. Das heißt, es gibt ein Element $a \in G$ sodass $G = \langle a\rangle$, oder anders gesagt, jedes Element von G ist einen Potenz a^k mit $k \in \mathbb{Z}$. In diesem Fall nennt man a ein erzeugendes Element von G.

Beispiel 2D41. Die Gruppen $(\mathbb{Z},+)$ und $(\mathbb{Z}/_n,+)$ sind zyklisch. Diese Gruppen werden, zum Beispiel, jeweils von 1 erzeugt.

Dieses Beispiel schöpft bereits alle Möglichkeiten aus: Jede zyklische Gruppe ist isomorph entweder zur unendlich zyklischen Gruppe $\mathbb{Z}$ oder zu einer zyklischen Gruppe $\mathbb{Z}/_n$ der Ordnung $n \geq 1$ (siehe §2Gb und §9Da).

§2Dh. Ordnung einer Gruppe und eines Elements. Die *Ordnung* einer Gruppe G ist ihre Kardinalität, geschrieben $\mathrm{ord}(G) := |G|$. Dieser Begriff ist vor allem für endliche Gruppen interessant: In diesem Fall ist die Ordnung $\mathrm{ord}(G) \in \mathbb{N}$ die Anzahl der Elemente der Gruppe G.

Entsprechend definiert man die Ordnung einer Untergruppe $H < G$ als $\mathrm{ord}(H) := |H|$. Die Ordnung eines Elements $a \in G$ definieren wir $\mathrm{ord}(a) := |\langle a\rangle|$ als die Ordnung der von a erzeugten zyklischen Untergruppe.

§2E. Kommutativität

Eine Verknüpfung $*\colon M \times M \to M$ heißt *kommutativ* oder *abelsch* wenn

$$a * b = b * a$$

für alle $a,b \in M$ gilt. Zusammen mit der Assoziativität erhält man hieraus die folgende Verallgemeinerung für beliebig viele Faktoren:

Proposition 2E1 (allgemeines Kommutativgesetz)**.** *Seien $a_1,\dots,a_n$ Elemente einer kommutativen Halbgruppe $(M,*)$. Dann lassen sich die Faktoren des Produkts $a_1*\cdots*a_n$ beliebig umordnen, ohne das Ergebnis zu ändern. Es gilt also*

$$a_1*\cdots*a_n = a_{i_1}*\cdots*a_{i_n}$$

für jede Permutation $\{i_1,\dots,i_n\}=\{1,\dots,n\}$.

BEWEIS. Für $n=2$ ist dies die Definition von Kommutativität. Für $n\geq 3$ führen wir Induktion über n. Es gibt genau ein $k\in\{1,\dots,n\}$ mit $i_k=n$.

$$\begin{aligned} a_{i_1}*\cdots*a_{i_n} &= a_{i_1}*\cdots*a_{i_{k-1}}*a_n*a_{i_{k+1}}*\cdots*a_{i_n}\\ &= (a_{i_1}*\cdots*a_{i_{k-1}})*(a_n*(a_{i_{k+1}}*\cdots*a_{i_n}))\\ &= (a_{i_1}*\cdots*a_{i_{k-1}})*((a_{i_{k+1}}*\cdots*a_{i_n})*a_n)\\ &= (a_{i_1}*\cdots*a_{i_{k-1}}*a_{i_{k+1}}*\cdots*a_{i_n})*a_n\\ &= (a_1*\cdots*a_{n-1})*a_n \end{aligned}$$

Die letzte Umordnung folgt aus der Induktionsvoraussetzung. □

Spezieller sagen wir, zwei Elemente $a,b\in M$ *kommutieren* wenn $a*b=b*a$ gilt.

Korollar 2E2. *Für kommutierende Element $a,b\in M$ in einem Monoid gilt $(a*b)^n=a^n*b^n$ für alle $n\in\mathbb{N}$. Sind zudem a,b invertierbar, so gilt $(a*b)^n=a^n*b^n$ für alle $n\in\mathbb{Z}$.* □

Bei additiver Schreibweise spricht man statt von der Potenz vom Vielfachen:

Korollar 2E3 (Modulgesetze)**.** *Für jedes kommutative Monoid $(A,+)$ erfreut sich die Operation $\mathbb{N}\times A\to A$, $(n,a)\mapsto na$, der Eigenschaften*

$$\begin{array}{lll} 0a=0 & (m+n)a=ma+na & n(a+b)=na+nb\\ 1a=a & (mn)a=m(na) & \end{array}$$

für alle $a,b\in A$ und $m,n\in\mathbb{N}$. Ist $(A,+)$ eine abelsche Gruppe, dann erfreut sich die Operation $\mathbb{Z}\times A\to A$, $(n,a)\mapsto na$, dieser Eigenschaften für alle $a,b\in A$ und $m,n\in\mathbb{Z}$. □

Übung 2E4. Sind $a_1,\dots,a_n$ kommutierende Elemente in einem Monoid M, dann ist das von ihnen erzeugte Untermonoid $\langle a_1,\dots,a_n\rangle^+$ kommutativ und es gilt

$$\langle a_1,\dots,a_n\rangle^+ = \{\, a_1^{e_1}\cdots a_n^{e_n} \mid e_1,\dots,e_n\in\mathbb{N}\,\}.$$

Gleiches gilt, wenn $a_1,\dots,a_n$ in M invertierbar sind, für die erzeugte Untergruppe

$$\langle a_1,\dots,a_n\rangle = \{\, a_1^{e_1}\cdots a_n^{e_n} \mid e_1,\dots,e_n\in\mathbb{Z}\,\}.$$

§**2Ea. Summen.** Sei $(A,+,0)$ ein abelsches Monoid und I eine Menge. Eine Familie $(a_i)_{i\in I}$ von Elementen $a_i\in A$ ist eine Abbildung $a\colon I\to A$, geschrieben $i\mapsto a_i$.

Für jede *endliche* Familie können wir die Summe $\sum_{i\in I}a_i$ wie folgt definieren: Wir nehmen an, I habe n Elemente, wir nummerieren diese durch, sodass $I=\{i_1,\dots,i_n\}$, und setzen $\sum_{i\in I}a_i := \sum_{k=1}^n a_{i_k}$. Nach dem allgemeinen Kommutativgesetz ist das Ergebnis wohldefiniert, das heißt von der gewählten Reihenfolge der Indizes unabhängig.

Der *Träger* einer Abbildung $a\colon I \to A$ ist die Menge $\operatorname{supp}(a) = \{i \in I \mid a_i \neq 0\}$. Für jede Menge J mit $\operatorname{supp}(a) \subset J \subset I$ gilt $\sum_{j\in J} a_j = \sum_{i\in I} a_i$, denn die zusätzlichen Terme $a_i = 0$ für alle $i \in I \smallsetminus J$ addieren jeweils das Nullelement von A.

Ist I eine unendliche Menge, so können wir $\sum_{i\in I} a_i$ nur für Abbildungen $a\colon I \to A$ mit endlichem Träger definieren: In diesem Fall setzen wir $\sum_{i\in I} a_i := \sum_{i\in \operatorname{supp}(a)} a_i$. Für jede endliche Menge J mit $\operatorname{supp}(a) \subset J \subset I$ gilt wiederum $\sum_{i\in J} a_i = \sum_{i\in I} a_i$.

Für $a, b\colon I \to A$ mit endlichem Träger gilt $\left(\sum_{i\in I} a_i\right) + \left(\sum_{i\in I} b_i\right) = \sum_{i\in I}(a_i + b_i)$. Allgemeiner, für jede Abbildung $a\colon I \times J \to A$ mit endlichem Träger gilt

$$\sum_{(i,j)\in I\times J} a_{ij} = \sum_{i\in I}\Big(\sum_{j\in J} a_{ij}\Big) = \sum_{j\in J}\Big(\sum_{i\in I} a_{ij}\Big).$$

§**2Eb. Homomorphismen.** Für abelsche Gruppen stehen uns gewisse Konstruktionen zur Verfügung, die die Kommutativität in wesentlicher Weise benutzen.

Übung 2E5. Sei $(G, *)$ eine Gruppe.

1. G ist genau dann abelsch, wenn $x \mapsto x^{-1}$ ein Automorphismus ist.
2. G ist genau dann abelsch, wenn $x \mapsto x^2$ ein Endomorphismus ist.

Proposition 2E6. *Sind $(G, *, e_G)$ und $(H, \bullet, e_H)$ Gruppen, dann ist die Menge* $\operatorname{Abb}(G,H)$ *aller Abbildungen $G \to H$ eine Gruppe bezüglich punktweiser Verknüpfung (2D29). Ist zudem H abelsch, dann ist die Menge* $\operatorname{Hom}(G,H)$ *eine Untergruppe.*

BEWEIS. Die konstante Abbildung $e\colon G \to H$ mit $a \mapsto e_H$ für alle $a \in G$ ist ein Gruppenhomomorphismus, also $e \in \operatorname{Hom}(G,H)$. Sind $f, g\colon G \to H$ Homomorphismen, dann gilt

$$\begin{aligned}(f\cdot g)(a*b) &= f(a*b)\bullet g(a*b)\\ &= f(a)\bullet f(b)\bullet g(a)\bullet g(b)\\ &= f(a)\bullet g(a)\bullet f(b)\bullet g(b)\\ &= (f\cdot g)(a)\bullet(f\cdot g)(b)\end{aligned}$$

Für das zu einem Homomorphismus $f\colon G \to H$ inverse Element komponiert man f mit dem Automorphismus $^{-1}\colon H \to H$, siehe die vorhergehende Übung. □

Übung 2E7. Sind A, B, C abelsche Gruppen, dann sind $\operatorname{Hom}(A,B)$ und $\operatorname{Hom}(B,C)$ sowie $\operatorname{Hom}(A,C)$ abelsche Gruppen bezüglich der oben definiereten Addition. Die Komposition

$$\operatorname{Hom}(B,C) \times \operatorname{Hom}(A,B) \to \operatorname{Hom}(A,C), \quad (f,g) \mapsto f \circ g$$

ist distributiv über die Addition: Für alle $f, f' \in \operatorname{Hom}(B,C)$ und $g, g' \in \operatorname{Hom}(A,B)$ gilt:

(DL) $(f + f') \circ g = (f \circ g) + (f' \circ g)$ (Linksdistributivität)
(DR) $f \circ (g + g') = (f \circ g) + (f \circ g')$ (Rechtsdistributivität)

Bemerkung 2E8. Für jede abelsche Gruppe A, trägt $\operatorname{End}(A)$ zwei Verknüpfungen:

- $\operatorname{End}(A)$ ist eine abelsche Gruppe bezüglich punktweiser Addition $+$ (2E6).
- $\operatorname{End}(A)$ ist ein Monoid bezüglich der Komposition $\circ$ (2B20).

Beide Verknüpfungen sind miteinander verträglich, in dem Sinne, dass die Komposition $\circ$ distributiv ist über die Addition $+$: Für alle $f, g, h \in \operatorname{End}(A)$ gilt

(DL) $(f+g)\circ h = (f\circ h)+(g\circ h)$ (Linksdistributivität)
(DR) $f\circ(g+h) = (f\circ g)+(f\circ h)$ (Rechtsdistributivität)

Diese Eigenschaften von $(\mathrm{End}(A),+,\circ)$ sind der Prototyp eines *Rings*. Diesen Begriff werden wir im folgenden Kapitel axiomatisch einführen.

§2F. Der Satz von Cayley

Wir haben eingangs Gruppen auf zwei Arten betrachtet: zunächst die unmittelbar gegebenen "konkreten" Gruppen, etwa die Gruppe $\mathrm{Sym}(X)$ der bijektiven Transformationen $f\colon X \xrightarrow{\sim} X$. Daneben "abstrakte" Gruppen $(G,*)$ für die wir nur die Gruppenaxiome fordern. Diese Unterscheidung hat allerdings nur historische Bedeutung: Es ist nämlich möglich, jede abstrakte Gruppe als eine konkrete Gruppe von Transformationen darzustellen:

Satz 2F1. *Jedes Monoid $(M,*)$ ist isomorph zu einem Untermonoid von $\mathrm{Abb}(X)$ auf einer geeigneten Menge X. Jede Gruppe $(G,*)$ ist isomorph zu einer Untergruppe der symmetrischen Gruppe $\mathrm{Sym}(X)$ auf einer geeigneten Menge X. Hierbei kann $X = G$ gewählt werden.*

Vor dem eigentlichen Beweis lohnt es sich, die wesentliche Idee an einem Beispiel zu illustrieren. Der nachfolgende Beweis formuliert dann die gemachten Beobachtungen aus.

Beispiel 2F2. Betrachten wir zur Illustration die Kleinsche Vierergruppe $(V,*)$, die wir hier durch die Menge $V = \{1,2,3,4\}$ mit folgender Verknüpfungstafel darstellen:

$*$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

In der ersten Zeile sehen wir die Permutation $\tau_1 = \left(\begin{smallmatrix}1&2&3&4\\1&2&3&4\end{smallmatrix}\right)$, und in den folgenden Zeilen die Permutationen $\tau_2 = \left(\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}\right)$, $\tau_3 = \left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right)$, $\tau_4 = \left(\begin{smallmatrix}1&2&3&4\\4&3&2&1\end{smallmatrix}\right)$. Diese Permutationen sind untereinander verschieden, die Abbildung $T\colon V \to S_4$ mit $a \mapsto \tau_a$ ist also injektiv.

Man rechnet direkt nach, dass T ein Gruppenhomomorphismus ist, also $T(a*b) = T(a)\circ T(b)$ für alle $a,b \in V$ erfüllt. Dies folgt ganz allgemein aus den Gruppenaxiomen, wie wir nun zeigen werden.

BEWEIS DES SATZES. Sei zunächst $(M,*)$ ein Monoid. Als Menge wählen wir $X := M$. Für jedes Element $a \in M$ definieren wir die *Linksmultiplikation mit a* $\tau_a\colon M \to M$ durch $\tau_a(x) := a*x$ für alle $x \in X$. Die Assoziativität $a*(b*x) = (a*b)*x$ für alle $a,b \in M$ und $x \in X$ ist gleichbedeutend mit $\tau_a \circ \tau_b = \tau_{a*b}$. Die Tatsache, dass $e \in M$ neutral ist, also $e*x = x$ für alle $x \in M$ erfüllt, ist gleichbedeutend mit $\tau_e = \mathrm{id}_M$.

Wir erhalten also einen Monoidhomomorphismus $T\colon M \to \mathrm{End}(M)$ durch $T(a) = \tau_a$. Dieser Homomorphismus ist injektiv: falls $\tau_a = \tau_b$, dann gilt insbesondere $\tau_a(e) = \tau_b(e)$ und daher $a = a*e = b*e = b$. Damit ist T ein Isomorphismus zwischen dem Monoid M und dem Untermonoid $U = \mathrm{im}(T) = \{\tau_a \mid a \in M\}$ von $\mathrm{End}(X)$.

Ist $(G,*)$ eine Gruppe, so gelten die vorherigen Aussagen entsprechend für G. Sind $a,b \in G$ zueinander invers, also $a*b = e$, dann folgt $\tau_a \circ \tau_b = \tau_{a*b} = \tau_e = \mathrm{id}_X$. Da in einer Gruppe G alle Elemente invertierbar sind, ist demnach jede der Abbildungen τ_a bijektiv.

Wir erhalten also einen Gruppenhomomorphismus $T\colon G \to \mathrm{Sym}(X)$ durch $T(a) = \tau_a$. Sein Bild ist die Untergruppe $T(G) = \{\tau_a \mid a \in G\}$ in $\mathrm{Sym}(X)$. □

Der Beweis für Gruppen lässt sich analog führen, wenn man statt der Linksmultiplikation die Rechtsmultiplikation mit dem Inversen verwendet. Er liefert dann unter Umständen eine andere Untergruppe von $\mathrm{Sym}(G)$, die aber ebenfalls isomorph zu G ist.

§2G. Quotientenstrukturen

Seien $(M,*)$ und $(N,\cdot)$ Magmen und sei $f\colon M \to N$ ein Homomorphismus. Auf M definiert dies eine Äquivalenzrelation $\equiv$, durch $a \equiv b$ genau dann wenn $f(a) = f(b)$, und diese ist mit der Verknüpfung $*$ verträglich, das heißt für alle $a,a',b,b' \in M$ gilt

$$a \equiv a', \quad b \equiv b' \quad \Rightarrow \quad a*b \equiv a'*b'$$

Satz 2G1 (Quotientenstruktur)**.** *Sei $(M,*)$ ein Magma und sei $\equiv$ eine Äquivalenzrelation auf M, die mit der Verknüpfung $*\colon M\times M \to M$ verträglich ist.*

Dann gibt es auf der Quotientenmenge $\bar{M} := M/_{\equiv}$ genau eine Verknüpfung $\bar{*}\colon \bar{M}\times\bar{M} \to \bar{M}$, die die Quotientenabbildung $\pi\colon M \to \bar{M}$ zu einem Homomorphismus macht.

Die Eigenschaften der Verknüpfung $*\colon M\times M \to M$ (wie Kommutativität, Assoziativität, neutrales Element, inverse Elemente) übertragen sich in offensichtlicher Weise auf $\bar{*}$.

BEWEIS. *Eindeutigkeit:* Wenn π ein Homomorphismus ist, dann muss notwendigerweise $\mathfrak{cl}(a) \mathbin{\bar{*}} \mathfrak{cl}(b) = \mathfrak{cl}(a*b)$ für alle $a,b \in M$ gelten.

Existenz: Da die Äquivalenzrelation $\equiv$ mit der Multiplikation $*$ verträglich ist, ist die Verknüpfung $\bar{*}\colon \bar{M}\times\bar{M} \to \bar{M}$ durch $\mathfrak{cl}(a) \mathbin{\bar{*}} \mathfrak{cl}(b) := \mathfrak{cl}(a*b)$ wohldefiniert.

Die Eigenschaften von $*$ übertragen sich in offensichtlicher Weise auf $\bar{*}$:

- Wenn $*$ kommutativ ist, dann auch $\bar{*}$, denn
$$\mathfrak{cl}(a) \mathbin{\bar{*}} \mathfrak{cl}(b) = \mathfrak{cl}(a*b) = \mathfrak{cl}(b*a) = \mathfrak{cl}(b) \mathbin{\bar{*}} \mathfrak{cl}(a).$$
- Wenn $*$ assoziativ ist, dann auch $\bar{*}$, denn
$$(\mathfrak{cl}(a) \mathbin{\bar{*}} \mathfrak{cl}(b)) \mathbin{\bar{*}} \mathfrak{cl}(c) = \mathfrak{cl}((a*b)*c) = \mathfrak{cl}(a*(b*c)) = \mathfrak{cl}(a) \mathbin{\bar{*}} (\mathfrak{cl}(b) \mathbin{\bar{*}} \mathfrak{cl}(c)).$$
- Wenn $1 \in M$ neutral für $*$ ist, dann ist auch $\mathfrak{cl}(1) \in \bar{M}$ neutral für $\bar{*}$, denn
$$\mathfrak{cl}(1) \mathbin{\bar{*}} \mathfrak{cl}(a) = \mathfrak{cl}(1*a) = \mathfrak{cl}(a) \quad \text{und} \quad \mathfrak{cl}(a) \mathbin{\bar{*}} \mathfrak{cl}(1) = \mathfrak{cl}(a*1) = \mathfrak{cl}(a).$$
- Wenn $a,b \in M$ zueinander invers sind, also $a*b = b*a = 1$ erfüllen, dann sind auch $\mathfrak{cl}(a), \mathfrak{cl}(b) \in \bar{M}$ zueinander invers, denn
$$\mathfrak{cl}(a) \mathbin{\bar{*}} \mathfrak{cl}(b) = \mathfrak{cl}(a*b) = \mathfrak{cl}(1) \quad \text{und} \quad \mathfrak{cl}(b) \mathbin{\bar{*}} \mathfrak{cl}(a) = \mathfrak{cl}(b*a) = \mathfrak{cl}(1).$$ □

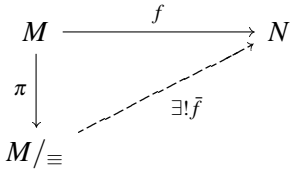
§2Ga. Homomorphiesatz. Die Quotientenstruktur $M/_{\equiv}$ hat folgende universelle Abbildungseigenschaft:

Satz 2G2 (Homomorphiesatz)**.** *Sei $(M,*)$ ein Magma, sei $\equiv$ eine Äquivalenzrelation auf M, die mit der Verknüpfung $*\colon M\times M \to M$ verträglich ist, und sei $\pi\colon M \to M/_{\equiv}$ der Quotientenhomomorphismus. Für jeden Homomorphismus $f\colon M \to N$ sind äquivalent:*

1. *Für alle $a,b \in M$ mit $a \equiv b$ gilt $f(a) = f(b)$.*

2. *Es existiert ein Homomorphismus* $\bar{f}\colon M/_{\equiv} \to N$ *sodass* $f = \bar{f} \circ \pi$.

In diesem Fall sagen wir, der Homomorphismus $f\colon M \to N$ *induziert* den Homomorphismus $\bar{f}\colon M/_{\equiv} \to N$ auf dem Quotienten $M/_{\equiv}$. Dieser Sachverhalt wird durch das folgende kommutative Diagramm veranschaulicht:



BEWEIS. "(1) $\Leftarrow$ (2)" ist klar. "(1) $\Rightarrow$ (2)" sieht man wie folgt: Wir definieren $\bar{f}(\mathfrak{cl}(a)) = f(a)$. Dies ist wohldefiniert, denn für $\mathfrak{cl}(a) = \mathfrak{cl}(b)$ gilt $a \equiv b$, also $f(a) = f(b)$. Man rechnet problemlos nach, dass $\bar{f}$ tatsächlich ein Homomorphismus ist:

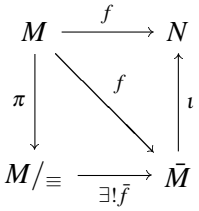
$$\bar{f}(\mathfrak{cl}(a) \mathbin{\bar{*}} \mathfrak{cl}(b)) = \bar{f}(\mathfrak{cl}(a*b)) = f(a*b) = f(a) \cdot f(b) = \bar{f}(\mathfrak{cl}(a)) \cdot \bar{f}(\mathfrak{cl}(b)). \qquad \square$$

Satz 2G3 (kanonische Faktorisierung)**.** *Jeder Homomorphismus* $f\colon M \to N$ *zwischen zwei Magmen M und N faktorisiert gemäß*

$$f\colon M \xrightarrow{\pi} M/_{\equiv} \xrightarrow{\bar{f}} \bar{M} \xrightarrow{\iota} N$$

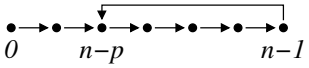
in die Projektion π*, einen Isomorphismus* $\bar{f}\colon R/\mathfrak{a} \xrightarrow{\sim} \bar{R}$*, und die Inklusion* ι*. Hierbei ist* $\bar{M} = f(M)$ *das Bild von M in N, und die Äquivalenzrelation* $\equiv$ *auf M ist definiert durch* $a \equiv b$ *genau dann wenn* $f(a) = f(b)$.

Die Situation wird durch das folgende kommutative Diagramm veranschaulicht:



BEWEIS. Dies folgt unmittelbar aus dem Homomorphiesatz 2G2. $\square$

§**2Gb. Klassifikation zyklischer Monoide.** Für natürliche Zahlen $1 \leq p \leq n$ wollen wir das Monoid $(M_n^p, \cdot)$ wie folgt definieren:



Diese Graphik soll bedeuten: Das Monoid M_n^p besteht aus n Elementen, wird von einem Element x erzeugt, also $M = \{\, x^k \mid k \in \mathbb{N} \,\}$, neutrales Element ist x^0 und es gilt $x^n = x^{n-p}$. Für $a, b \in \mathbb{N}$ gilt also $x^a = x^b$ wenn es $a', b' \in \mathbb{N}_{\geq 1}$ gibt, sodass $a + a'p = b + b'p \geq n$ gilt.

Zur Konstruktion von M_n^p definieren wir auf dem Monoid $(\mathbb{N}, +)$ die Relation $\equiv$ durch $a \equiv b$ genau dann wenn es $a', b' \in \mathbb{N}_{\geq 1}$ gibt, sodass $a + a'p = b + b'p \geq n$ gilt.

Übung 2G4. Dies ist eine Äquivalenzrelation auf $\mathbb{N}$, die mit der Addition $+$ verträglich ist. Das Quotientenmonoid $M_n^p := \mathbb{N}/_{\equiv}$ hat n Elemente, wird von $x = 1$ erzeugt und erfüllt (multiplikativ geschrieben)die Relation $x^n = x^{n-p}$.

Nach dem Satz von Cayley können wir M_n^p auch als Untermonoid von $\mathrm{Abb}(X)$ über einer geeigneten Menge X auffassen. Dies führt zu folgender alternativen Konstruktion:

Übung 2G5. Auf der Menge $X = \{0,\dots,n-1\}$ sei $x\colon X \to X$ die Abbildung mit $x(k) = k+1$ für alle $0 \le k < n-1$ und $x(n-1) = n-p$. Das in $\mathrm{Abb}(X)$ von x erzeugte Untermonoid $\langle x\rangle^+$ besteht aus n Elementen $x^0, x^1, \dots, x^{n-1}$ und es gilt $x^{n-1} = x^{n-p}$.

Dieses Monoid ist zu dem zuvor konstruierten Monoid M_n^p isomorph.

Übung 2G6. Das Monoid $(M_n^p, \cdot)$ ist genau dann eine Gruppe, wenn $p = n$ gilt.
In diesem Fall nennen wir $\mathbb{Z}/_n := M_n^p$ die *zyklische Gruppe der Ordnung n*.

Übung 2G7. Im Falle $1 \le p < n$ hat das Monoid $(M_n^p, \cdot)$ nur einen Erzeuger.

Übung 2G8. Einen Monoidisomorphismus $M_n^p \cong M_{n'}^{p'}$ gibt es nur für $(n,p) = (n',p')$.

Sei $(M,\cdot)$ ein zyklisches Monoid, das heißt M wird von einem Element $x \in M$ erzeugt, also $M = \{\, x^k \mid k \in \mathbb{N} \,\}$. Ist M endlich, so können wir zwei Zahlen definieren: die *Ordnung* $n := |M|$ sowie die *Periode* $p \ge 1$ durch $x^n = x^{n-p}$.

Übung 2G9. Man zeige, dass jedes zyklische Monoid $(M,\cdot)$ entweder zu $(\mathbb{N},+)$ oder zu genau einem der obigen Modelle $(M_n^p,\cdot)$ isomorph ist.

§2H. Freie Monoide und freie Gruppen

§2Ha. Freie Monoide. Nach Beispiel 2C19 ist $(\mathbb{N},+)$ das *freie Monoid* über dem Element 1. Wir wollen nun das freie Monoid über einer beliebigen Menge A konstruieren.

Definition 2H1. Ein Monoid M heißt *frei* über einer Teilmenge $A \subset M$ wenn sich jedes Element $x \in M$ auf genau eine Weise als ein Produkt $x = a_1 a_2 \cdots a_n$ mit Faktoren $a_1, a_2, \dots, a_n \in A$ schreiben lässt.

Etwas ausführlicher treffen wir folgende Definitionen. Ein *Wort* über A ist ein Produkt $a_1 a_2 \cdots a_n$ mit Faktoren $a_1, a_2, \dots, a_n \in A$. Eine Teilmenge $A \subset M$ heißt *Erzeugendensystem* von M wenn sich jedes Element in M als ein Wort über A schreiben lässt. Eine Teilmenge $A \subset M$ heißt *frei* in M, wenn für je zwei Wörter über A aus der Gleichheit $a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_m$ in M folgt, dass $n = m$ gilt sowie $a_1 = b_1$, $a_2 = b_2$, …, $a_n = b_n$.

Eine Teilmenge $A \subset M$ heißt *Basis* des Monoids M wenn sich jedes Element in M auf genau eine Weise als Wort über A schreiben lässt. Ein Monoid M heißt *frei*, wenn es eine Basis $A \subset M$ besitzt. In diesem Fall sagen wir, das Monoid M ist *frei über A*.

Beispiel 2H2. Das Monoid $(\mathbb{N},+)$ ist frei über 1. Für $1 \le p \le n$ ist das zyklische Monoid M_n^p nicht frei über 1, und ganz allgemein nicht frei, egal über welcher Teilmenge.

Beispiel 2H3. Ist das Monoid M frei über $\{a,b\}$, dann besteht M aus den Elementen

$$1,\ a^{e_1},\ b^{e_1},\ a^{e_1}b^{e_2},\ b^{e_1}a^{e_2},\ a^{e_1}b^{e_2}a^{e_3},\ b^{e_1}a^{e_2}b^{e_3}, \dots$$

mit $e_1, e_2, e_3, \dots$ in $\mathbb{N}^*$, und jedes Element von M tritt in dieser Liste genau einmal auf.

Satz 2H4. *Zu jeder Menge A gibt es ein freies Monoid A^* über A.*

KONSTRUKTION. Wir bezeichnen mit $A^n = A \times \cdots \times A$ das n-fache kartesische Produkt. Jedes Element $(a_1, \ldots, a_n) \in A^n$ betrachten wir als Wort der Länge n über dem Alphabet A. Für $n = 0$ enthält $A^0 = \{\varepsilon\}$ nur das leere Wort ε. Die Menge $A^* = \bigcup_{n\in\mathbb{N}} A^n$ besteht aus allen endlichen Wörtern über dem Alphabet A. Hierauf definieren wir die Verknüpfung $\circ\colon A^* \times A^* \to A^*$ durch Aneinanderhängen von Wörtern gemäß $(a_1, \ldots, a_m) \circ (b_1, \ldots, b_n) := (a_1, \ldots, a_m, b_1, \ldots, b_n)$. Nach Konstruktion ist das Monoid A^* frei über A. □

Beispiel 2H5. Ist A die leere Menge, dann ist A^* das einelementige Monoid, das nur aus dem neutralen Element besteht. Für die einelementige Menge $A = \{a\}$ erhalten wir den Isomorphismus $\mathbb{N} \xrightarrow{\sim} A^*$, $k \mapsto a^k$.

Neben dieser inneren Charakterisierung können wir das freie Monoid auch durch seine universelle Abbildungseigenschaft in der Kategorie der Monoide charakterisieren:

Satz 2H6 (universelle Eigenschaft)**.** *Das freie Monoid A^* über einer Menge A erfreut sich folgender Eigenschaft: Für jede Abbildung $f\colon A \to M$ der Menge A in ein Monoid M existiert genau ein Monoidhomomorphismus $h\colon A^* \to M$ mit $h|_A = f$.*

BEWEIS. Jedes Element $a \in A^*$ schreibt sich eindeutig als Produkt $a = a_1 a_2 \cdots a_n$ mit $a_1, a_2, \ldots, a_n \in A$. Wir definieren also $h(a) = f(a_1) f(a_2) \cdots f(a_n)$. Die so definierte Abbildung $h\colon A^* \to M$ ist offenbar ein Monoidhomomorphismus, der f fortsetzt. Diese Fortsetzung ist eindeutig, denn A ist ein Erzeugendensystem von A^*. □

Korollar 2H7. *Jedes Monoid M ist isomorph zu einem Quotienten eines freien Monoids.*

BEWEIS. Sei $A \subset M$ ein Erzeugendensystem; in Ermangelung besserer Ideen kann man $A = M$ wählen. Die Inklusion $A \hookrightarrow M$ mit $\langle A \rangle^+ = M$ induziert einen surjektiven Monoidhomomorphismus $A^* \twoheadrightarrow M$. Der gewünschte Isomorphismus folgt nun aus 2G3. □

Diese Technik haben wir in §2Gb bereits zur Klassifikation zyklischer Monoid angewendet. Dort diente uns $(\mathbb{N}, +)$ als das freie Monoid über einem Erzeuger.

Korollar 2H8. *Sei M ein Monoid. Für jede Teilmenge $A \subset M$ induziert die Inklusion $A \hookrightarrow M$ einen Monoidhomomorphismus $\Phi\colon A^* \to M$.*

- *A ist genau dann ein Erzeugendensystem von M, wenn Φ surjektiv ist.*
- *A ist genau dann frei in M, wenn Φ injektiv ist.*
- *A ist genau dann eine Basis von M, wenn Φ bijektiv ist.* □

Satz 2H9. *Seien A und B zwei Mengen. Die freien Monoide A^* und B^* sind genau dann isomorph, wenn die Mengen A und B gleiche Kardinalität haben.*

BEWEIS. Gemäß 2H6 setzt sich jede Bijektion $A \xrightarrow{\sim} B$ fort zu einem Monoidisomorphismus $A^* \xrightarrow{\sim} B^*$. Wir zeigen die Umkehrung für endliche Mengen mit $m = |A|$ und $n = |B|$ Elementen. Nach 2H6 hat $\operatorname{Hom}(A^*, \mathbb{Z}/2)$ genau 2^m Elemente, und entsprechend hat $\operatorname{Hom}(B^*, \mathbb{Z}/2)$ genau 2^n Elemente. Aus einem Monoidisomorphismus $A^* \cong B^*$ folgt $2^m = 2^n$ und somit $m = n$. □

Korollar 2H10. *Ist M ein freies Monoid mit Basen A und B, dann existiert eine Bijektion $A \cong B$.*

BEWEIS. Die Inklusion $A \hookrightarrow M$ induziert einen Monoidisomorphismus $A^* \xrightarrow{\sim} M$, und die Inklusion $B \hookrightarrow M$ induziert einen Monoidisomorphismus $B^* \xrightarrow{\sim} M$. Aus dem so erhaltenen Monoidisomorphismus $A^* \cong B^*$ folgt $A \cong B$. □

Anders gesagt, je zwei Basen eines freien Monoids M haben dieselbe Kardinalität. Dies erlaubt uns den Rang $\operatorname{rang}(M)$ zu definieren als die Kardinalität einer Basis, denn diese Kardinalität ist unabhängig von der gewählten Basis.

Bemerkung 2H11. Untermonoide eines freien Monoids müssen nicht frei sein: Zum Beispiel ist $(\mathbb{N},+)$ frei, nicht aber das Untermonoid $\{0,2,3,4,5,6,\dots\}$

Selbst wenn $U \subset M$ beide frei sind, muss nicht $\operatorname{rang}(U) \leq \operatorname{rang}(M)$ gelten. Das freie Monoid $M = \{a,b\}^*$ vom Rang zwei enthält die freie Familie $x_k = ab^k a$, $k \in \mathbb{N}$. Somit ist $U = \langle x_1, x_2, \dots, x_k \rangle^+ \subset M$ ein freies Monoid vom Rang k.

§**2Hb. Freie abelsche Monoide.** Das freie Monoid A^* über A ist nicht abelsch für $|A| \geq 2$, denn $aa' \neq a'a$ für alle Basiselemente $a,a' \in A$ mit $a \neq a'$. Das *freie abelsche Monoid* $A^*/_{\text{ab}}$ über A entsteht aus dem freien Monoid A^* durch Quotientenbildung modulo der von $uv \equiv vu$ erzeugten Äquivalenzrelation. Die Menge $A \subset A^*$ wird dabei injektiv nach $A^*/_{\text{ab}}$ abgebildet, so dass wir sie mit ihrem Bild in $A^*/_{\text{ab}}$ identifizieren können.

Satz 2H12 (universelle Eigenschaft)**.** *Das freie abelsche Monoid $A^*/_{\text{ab}}$ über A erfreut sich folgender Eigenschaft: Für jede Abbildung $f\colon A \to M$ der Menge A in ein abelsches Monoid M existiert genau ein Monoidhomomorphismus $h\colon A^*/_{\text{ab}} \to M$ mit $h|_A = f$.* □

Korollar 2H13. *Jedes abelsche Monoid ist isomorph zu einem Quotienten eines freien abelschen Monoids.* □

Den Begriff der *Basis* definiert man für freie abelsche Monoide entsprechend wie für freie Monoide und zeigt, dass je zwei Basen eines freien abelschen Monoids M dieselbe Kardinalität haben. Dies erlaubt uns den Rang $\operatorname{rang}(M)$ zu definieren als die Kardinalität einer Basis, denn diese Kardinalität ist unabhängig von der gewählten Basis.

Proposition 2H14. *Das freie abelsche Monoid $A^*/_{\text{ab}}$ ist isomorph zum Monoid $\mathbb{N}^{(A)}$.*

BEWEIS. Das Monoid $\mathbb{N}^{(A)}$ besteht aus allen Abbildungen $e\colon A \to \mathbb{N}$ mit endlichem Träger (2C22). Der kanonische Isomorphismus $\mathbb{N}^{(A)} \xrightarrow{\sim} A^*/_{\text{ab}}$ ist definiert durch die Abbildung $e \mapsto \prod_{a\in A} a^{e(a)}$, und diese ist wohldefiniert gemäß §2Ea. Die Umkehrabbildung $A^*/_{\text{ab}} \xrightarrow{\sim} \mathbb{N}^{(A)}$ folgt aus der universellen Eigenschaft 2H12. □

Korollar 2H15. *Sei M ein abelsches Monoid. Für jede Teilmenge $A \subset M$ haben wir einen Monoidhomomorphismus $\Phi\colon \mathbb{N}^{(A)} \to M$, $e \mapsto \prod_{a\in A} a^{e(a)}$.*

- *A ist genau dann ein Erzeugendensystem von M, wenn Φ surjektiv ist.*
- *A ist genau dann frei in M, wenn Φ injektiv ist.*
- *A ist genau dann eine Basis von M, wenn Φ bijektiv ist.* □

Beispiel 2H16. Der Hauptsatz der Arithmetik besagt, dass das Monoid $(\mathbb{Z}_{>0},\cdot)$ frei abelsch ist über der Menge $\mathcal{P} = \{2,3,5,7,11,13,\dots\}$ der positiven Primzahlen. Genauer sei $(p_n)_{n\in\mathbb{N}}$ die Familie der Primzahlen, etwa in aufsteigender Reihenfolge $p_0 = 2$, $p_1 = 3$, $P_2 = 5$, ... Dann ist die Abbildung $\mathbb{N}^{(\mathbb{N})} \to \mathbb{Z}_{>0}$, $e \mapsto \prod_{n\in\mathbb{N}} p_n^{e_n}$ ein Monoidisomorphismus.

Freie abelsche Monoide treten ebenso auf als multiplikative Struktur von faktoriellen Ringen (siehe Kapitel 5 und Kapitel 6).

§**2Hc. Freie Gruppen.** Nach Beispiel 2D26 ist $(\mathbb{Z},+)$ die *freie Gruppe* über dem Element 1. Wir wollen nun die freie Gruppe über einer beliebigen Menge S konstruieren.

Definition 2H17. Eine Gruppe G heißt *frei* über einer Teilmenge $S \subset G$ wenn sich jedes Gruppenelement $a \in G$ auf genau eine Weise schreiben lässt als Produkt $a = s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n}$ mit Faktoren $s_1, s_2, \ldots, s_n \in S$, wobei $s_i \neq s_{i+1}$ für alle $i = 1, \ldots, n-1$, und Exponenten $e_1, e_2, \ldots, e_n \in \mathbb{Z}$, wobei $e_i \neq 0$ für alle $i = 1, \ldots, n$.

Etwas ausführlicher treffen wir folgende Definitionen. Ein *(Gruppen-)Wort* über S ist ein Produkt $s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n}$ mit Faktoren $s_1, s_2, \ldots, s_n \in S$ und Exponenten $e_1, e_2, \ldots, e_n \in \mathbb{Z}$. Wir nennen dieses Wort *reduziert*, wenn $s_i \neq s_{i+1}$ für alle $i = 1, \ldots, n-1$ gilt sowie $e_i \neq 0$ für alle $i = 1, \ldots, n$.

Eine Teilmenge $S \subset M$ heißt *Erzeugendensystem* von G wenn sich jedes Element in G als ein Wort über S schreiben lässt. Eine Teilmenge $S \subset G$ heißt *frei* in G, wenn für je zwei reduzierte Wörter über S aus der Gleichheit $s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n} = t_1^{f_1} t_2^{f_2} \cdots t_m^{f_m}$ in G folgt, dass $n = m$ gilt sowie $s_i = t_i$ und $e_i = f_i$ für alle i.

Eine Teilmenge $S \subset G$ heißt *Basis* der Gruppe G wenn sich jedes Element in G auf genau eine Weise als ein reduziertes Wort über S schreiben lässt. Eine Gruppe G heißt *frei*, wenn sie eine Basis $S \subset G$ besitzt. In diesem Fall sagen wir, die Gruppe G ist *frei über* S.

Beispiel 2H18. Die Gruppe $(\mathbb{Z},+)$ ist frei über 1. Für $n \geq 2$ ist die zyklische Gruppe $(\mathbb{Z}/_n,+)$ nicht frei über 1, und ganz allgemein nicht frei, egal über welcher Teilmenge.

Beispiel 2H19. Ist die Gruppe F frei über $\{a,b\}$, dann besteht F aus den Elementen

$$1,\ a^{e_1},\ b^{e_1},\ a^{e_1}b^{e_2},\ b^{e_1}a^{e_2},\ a^{e_1}b^{e_2}a^{e_3},\ b^{e_1}a^{e_2}b^{e_3}, \ldots$$

mit $e_1, e_2, e_3, \ldots$ in $\mathbb{Z}^*$, und jedes Element von F tritt in dieser Liste genau einmal auf.

Satz 2H20. *Zu jeder Menge S gibt es eine freie Gruppe $F(S)$ über S.*

KONSTRUKTION. Um zunächst zu jedem Element $s \in S$ auch ein Inverses s^{-1} zu haben, betrachten wir das Alphabet $A = S \times \{\pm 1\}$ und definieren hierauf die Involution $^{-1}\colon A \to A$ durch $(s,\varepsilon)^{-1} = (s,-\varepsilon)$. Wir identifizieren hierbei S mit $S \times \{+1\}$ vermöge der Abbildung $s \mapsto (s,+1)$. Sei $M = A^*$ das freie Monoid über A, das heißt die Menge aller endlichen Wörter über dem Alphabet A (§2Ha).

Auf dem Monoid $(M,\cdot)$ betrachten wir die Äquivalenzrelation, die durch die elementaren Umformungen $uaa^{-1}v \equiv uv$ erzeugt wird. Zwei Wörter in M sind also genau dann äquivalent, wenn sie durch eine endliche Folge von Einfügen oder Entfernen von Unterwörtern der Form aa^{-1} mit $a \in A$ ineinander übergehen.

Die Menge $M/_{\equiv}$ der Äquivalenzklassen bezeichnen wir mit $F = F(S)$. Die Verknüpfung auf M induziert auf der Quotientenmenge F eine wohldefinierte Verknüpfung $\cdot\colon F \times F \to F$. Nach Konstruktion wird $(F,\cdot)$ damit zu einer Gruppe. Offenbar ist S ein Erzeugendensystem, und die folgenden Lemmata zeigen, dass S eine Basis ist. □

Beispiel 2H21. Ist S die leere Menge, dann ist $F(S)$ die einelementige Gruppe, die nur aus dem neutralen Element besteht. Für die einelementige Menge $S = \{s\}$ erhalten wir den Isomorphismus $\mathbb{Z} \xrightarrow{\sim} F(S)$, $k \mapsto s^k$.

Lemma 2H22. *Der folgende Algorithmus 1 zur Reduktion von Wörtern ist korrekt.*

Algorithmus 1 Reduktion von Wörtern

Eingabe: Ein Wort $w_0 = x_1 x_2 \cdots x_n$ im freien Monoid A^* über $A = S \cup S^{-1}$
Ausgabe: Ein reduziertes Wort $w \equiv w_0$ in A^*

$w \leftarrow w_0$ // Invariante: $w \equiv w_0$
repeat
  Finde in $w = x_1 \cdots x_n$ die erste Stelle i sodass $x_i = x_{i+1}^{-1}$.
  Wenn keine solche Stelle existiert, dann ist w reduziert.
  Andernfalls reduziere $w \leftarrow x_1 \cdots x_{i-1} x_{i+2} \cdots x_n$. // Invariante: $w \equiv w_0$
until w ist reduziert
return w // $w \equiv w_0$ ist reduziert

Lemma 2H23. *Jedes Element von $F(S)$ schreibt sich eindeutig als reduziertes Wort über S.*

BEWEIS. Die Existenz eines reduzierten Wortes wird durch Algorithmus 1 sichergestellt. Wir haben zu zeigen: Sind zwei äquivalente Wörter $w \equiv w'$ im freien Monoid $M = A^*$ beide reduziert, dann gilt $w_0 = w_1$. Äquivalenz bedeutet, es gibt eine endliche Folge $w = w_0 \equiv w_1 \equiv \cdots \equiv w_n = w'$ von elementaren Kürzungen (von $w_k = uaa^{-1}v$ zu $w_{k+1} = uv$) oder Einfügungen (von $w_k = uv$ zu $w_{k+1} = uaa^{-1}v$). Wenn wir auf diese Folge jeweils den Kürzungsalgorithmus anwenden, so erhalten wir eine Folge $w = \bar{w}_0 \equiv \bar{w}_1 \equiv \cdots \equiv \bar{w}_n = w'$ von reduzierten Wörtern. Inspektion der elementaren Umformungen zeigt schließlich die Gleichheit $w = \bar{w}_0 = \bar{w}_1 = \cdots = \bar{w}_n = w'$. □

Neben dieser inneren Charakterisierung können wir die freie Gruppe auch durch ihre universelle Abbildungseigenschaft in der Kategorie der Gruppen charakterisieren:

Satz 2H24 (universelle Eigenschaft)**.** *Die freie Gruppe $F(S)$ über S erfreut sich folgender Eigenschaft: Ist $f\colon S \to G$ eine beliebige Abbildung der Menge S in eine Gruppe G, dann gibt es genau einen Gruppenhomomorphismus $h\colon F(S) \to G$ mit $h|_S = f$.*

BEWEIS MITTELS HOMOMORPHIESATZ. Wir können $f\colon S \to G$ auf $A = S \cup S^{-1}$ fortsetzen durch $f(s^{-1}) = f(s)^{-1}$. Das freie Monoid $M = A^*$ erlaubt genau einen Monoidhomomorphismus $g\colon M \to G$ mit $g|_A = f$. Da die Äquivalenzrelation $\equiv$ mit g verträglich ist, induziert g auf dem Quotienten $F = M/_{\equiv}$ einen Gruppenhomomorphismus $h\colon F \to G$ mit $h|_S = f$. Diese Fortsetzung ist eindeutig, denn S ist ein Erzeugendensystem von F. □

BEWEIS MITTELS REDUZIERTER WÖRTER. Wenn F frei über S ist, dann schreibt sich jedes Element $a \in F$ eindeutig als reduziertes Wort $a = s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n}$ über S. Wir können daher jede Abbildung $f\colon S \to G$ fortsetzen durch $h(a) := f(s_1)^{e_1} f(s_2)^{e_2} \cdots f(s_n)^{e_n}$, und diese Abbildung ist wohldefiniert. Es bleibt schließlich noch nachzurechnen, dass h ein Gruppenhomomorphismus ist. □

Korollar 2H25. *Jede Gruppe G ist isomorph zu einem Quotienten einer freien Gruppe.*

BEWEIS. Sei $S \subset G$ ein Erzeugendensystem; in Ermangelung besserer Ideen kann man $S = G$ wählen. Die Inklusion $S \hookrightarrow G$ mit $\langle S \rangle = G$ induziert einen surjektiven Gruppenhomomorphismus $F(S) \twoheadrightarrow G$. Der gewünschte Isomorphismus folgt nun aus 2G3. □

Korollar 2H26. *Sei G eine Gruppe. Für jede Teilmenge $S \subset G$ induziert die Inklusion $S \hookrightarrow G$ einen Gruppenhomomorphismus $\Phi\colon F(S) \to G$.*

- *S ist genau dann ein Erzeugendensystem von G, wenn Φ surjektiv ist.*
- *S ist genau dann frei in G, wenn Φ injektiv ist.*
- *S ist genau dann eine Basis von G, wenn Φ bijektiv ist.* □

Satz 2H27. *Seien S und T zwei Mengen. Die freien Gruppen $F(S)$ und $F(T)$ sind genau dann isomorph, wenn die Mengen S und T gleiche Kardinalität haben.*

BEWEIS. Gemäß 2H24 setzt sich jede Bijektion $S \xrightarrow{\sim} T$ fort zu einem Gruppenisomorphismus $F(S) \xrightarrow{\sim} F(T)$. Wir zeigen die Umkehrung für endliche Mengen mit $m = |A|$ und $n = |B|$ Elementen. Nach 2H24 hat $\operatorname{Hom}(F(S), \mathbb{Z}/2)$ genau 2^m Elemente, und entsprechend hat $\operatorname{Hom}(F(T), \mathbb{Z}/2)$ genau 2^n Elemente. Aus einem Gruppenisomorphismus $F(S) \cong F(T)$ folgt $2^m = 2^n$ und somit $m = n$. □

Korollar 2H28. *Ist F eine freie Gruppe mit Basen S und T, dann existiert eine Bijektion $S \cong T$.*

BEWEIS. Die Inklusion $S \hookrightarrow F$ induziert einen Gruppenisomorphismus $F(S) \xrightarrow{\sim} F$, und die Inklusion $T \hookrightarrow M$ induziert einen Gruppenisomorphismus $F(T) \xrightarrow{\sim} F$. Aus dem so erhaltenen Gruppenisomorphismus $F(S) \cong F(T)$ folgt $S \cong T$. □

Anders gesagt, je zwei Basen einer freien Gruppe F haben dieselbe Kardinalität. Dies erlaubt uns den Rang $\operatorname{rang}(F)$ zu definieren als die Kardinalität einer Basis, denn diese Kardinalität ist unabhängig von der gewählten Basis.

Bemerkung 2H29. Jede Untergruppe einer freien Gruppe ist frei: Dies ist der Satz von Nielsen–Schreier. Wir können hier leider nicht darauf eingehen.

Wenn $G < F$ freie Gruppen sind, dann ist $\operatorname{rang}(G) > \operatorname{rang}(F)$ möglich. Die freie Gruppe $F = F(a,b)$ über der Basis $\{a,b\}$ enthält zum Beispiel die freie Familie $x_k = a^k b^{-k}$, $k \in \mathbb{Z}$. (Beweis?) Somit ist $G = \langle x_1, x_2, \ldots, x_k \rangle < F$ eine freie Gruppe vom Rang k.

§**2Hd. Freie abelsche Gruppen.** Die freie Gruppe $F(S)$ über S ist nicht abelsch für $|S| \geq 2$, denn $ss' \neq s's$ für alle Basiselemente $s, s' \in S$ mit $s \neq s'$. Die *freie abelsche Gruppe* $F(S)/_{\text{ab}}$ über S entsteht aus der freien Gruppe $F(S)$ durch Quotientenbildung modulo der von $uv \equiv vu$ erzeugten Äquivalenzrelation. Die Menge $S \subset F(S)$ wird dabei injektiv nach $F(S)/_{\text{ab}}$ abgebildet, so dass wir sie mit ihrem Bild in $F(S)/_{\text{ab}}$ identifizieren können.

Satz 2H30 (universelle Eigenschaft)**.** *Die freie abelsche Gruppe $F(S)/_{\text{ab}}$ über S erfreut sich folgender Eigenschaft: Für jede Abbildung $f\colon S \to A$ der Menge S in eine abelsche Gruppe A existiert genau ein Gruppenhomomorphismus $h\colon F(S)/_{\text{ab}} \to A$ mit $h|_S = f$.* □

Korollar 2H31. *Jede abelsche Gruppe ist isomorph zu einem Quotienten einer freien abelschen Gruppe.* □

Den Begriff der *Basis* definiert man für freie abelsche Gruppen entsprechend wie für freie Gruppen und zeigt, dass je zwei Basen einer freien abelschen Gruppe F dieselbe Kardinalität haben. Dies erlaubt uns den Rang $\operatorname{rang}(F)$ zu definieren als die Kardinalität einer Basis, denn diese Kardinalität ist unabhängig von der gewählten Basis.

Proposition 2H32. *Die freie abelsche Gruppe $F(S)/_{\text{ab}}$ ist isomorph zur Gruppe $\mathbb{Z}^{(S)}$.*

BEWEIS. Die Gruppe $\mathbb{Z}^{(S)}$ besteht aus allen Abbildungen $e\colon S \to \mathbb{Z}$ mit endlichem Träger (2D29). Der kanonische Isomorphismus $\mathbb{Z}^{(A)} \xrightarrow{\sim} F(S)/_{\text{ab}}$ ist definiert durch die Abbildung $e \mapsto \prod_{s\in S} s^{e(s)}$, und diese ist wohldefiniert gemäß §2Ea. Die Umkehrabbildung $F(S)/_{\text{ab}} \xrightarrow{\sim} \mathbb{Z}^{(S)}$ folgt aus der universellen Eigenschaft 2H30. □

Korollar 2H33. *Sei A eine abelsche Gruppe. Für jede Teilmenge $S \subset A$ haben wir einen Gruppenhomomorphismus $\Phi\colon \mathbb{Z}^{(S)} \to A$, $e \mapsto \prod_{a\in A} a^{e(a)}$.*

- *S ist genau dann ein Erzeugendensystem von A, wenn Φ surjektiv ist.*
- *S ist genau dann frei in A, wenn Φ injektiv ist.*
- *S ist genau dann eine Basis von A, wenn Φ bijektiv ist.* □

Beispiel 2H34. Nach dem Hauptsatz der Arithmetik ist die Gruppe $(\mathbb{Q}_{>0}, \cdot)$ frei abelsch über der Menge $\mathcal{P} = \{2,3,5,7,11,13,\dots\}$ der positiven Primzahlen. Genauer sei $(p_n)_{n\in\mathbb{N}}$ die Familie der Primzahlen, etwa in aufsteigender Reihenfolge $p_0 = 2$, $p_1 = 3$, $P_2 = 5$, ... Dann ist die Abbildung $\mathbb{Z}^{(\mathbb{N})} \to \mathbb{Q}_{>0}$, $e \mapsto \prod_{n\in\mathbb{N}} p_n^{e_n}$ ein Monoidisomorphismus.

Freie abelsche Gruppen treten ebenso auf als multiplikative Struktur des Quotientenkörpers eines faktoriellen Rings (siehe Kapitel 6).

Freie abelsche Gruppen spielen auch eine wichtige Rolle bei der Klassifikation der endlich erzeugten abelschen Gruppen (siehe Kapitel 8).

§2I. Übungen und Ergänzungen

§**2Ia. Verknüpfungen.** Wir definieren die Verknüpfung $*\colon \mathbb{N} \to \mathbb{N}$ durch $a * b = a^b$.

Übung 2I1. Zu welchen Elementen $x \in \mathbb{N}$ existiert ein rechtsneutrales Element y sodass $x * y = x$? und ein rechtsneutrales Element z sodass $z * x = x$?

Übung 2I2. Welche Paare (x,y) kommutieren, erfüllen also $x * y = y * x$?

Übung 2I3. Welche Tripel (x,y,z) erfüllen das Assoziativitätsgesetz $(a*b)*c = a*(b*c)$?

§**2Ib. Vervollständigung von Halbgruppen zu Monoiden.** Falls eine Verknüpfung kein neutrales Element hat, so kann man eines hinzufügen. Die Assoziativität wird dabei nicht gestört, sodass die erweiterte Verknüpfung wieder assoziativ ist.

Zur bequemen Sprechweise führen wir folgenden Begriff ein:

Definition 2I4. Eine *Halbgruppe* $(M,*)$ besteht aus einer Menge M zusammen mit einer assoziativen Verknüpfung $*\colon M \times M \to M$. (Ein neutrales Element wird nicht gefordert.)

Man kann jede Halbgruppe auf kanonische Weise zu einem Monoid vervollständigen:

Sei $*\colon M \times M \to M$ eine Verknüpfung auf der Menge M. Auf der Menge $\bar{M} = M \cup \{1\}$ mit $1 \notin M$ erweiterten wir $*$ zu der Verknüpfung $\bar{*}\colon \bar{M} \times \bar{M} \to \bar{M}$ durch $1 \,\bar{*}\, a = a \,\bar{*}\, 1 = a$ für alle $a \in \bar{M}$ und $a \,\bar{*}\, b = a * b$ für alle $a, b \in M$.

Proposition 2I5. *Ist $(M, *)$ eine Halbgruppe, dann ist $(\bar{M}, \bar{*})$ ein Monoid. Die Inklusion $M \hookrightarrow \bar{M}$ ist ein Homomorphismus von Halbgruppen. Zu jedem Homomorphismus $h\colon M \to N$ in einen Monoid N existiert genau ein Monoidhomomorphismus $\bar{h}\colon \bar{M} \to N$ mit $\bar{h}|_M = h$.* □

Übung 2I6. Man beweise die vorstehende Proposition.

§**2Ic. Vervollständigung von Monoiden zu Gruppen.** Ein Element a in einem Monoid M heißt *links-kürzbar* wenn aus $ab = ac$ stets $b = c$ folgt. Entsprechend heißt a *rechts-kürzbar* wenn aus $ba = ca$ stets $b = c$ folgt. Schließlich heißt a *kürzbar*, wenn es sowohl links- als auch rechts-kürzbar ist. Ein Monoid M heißt *kürzbar*, wenn jedes Element $a \in M$ kürzbar ist. Zum Beispiel ist jedes invertierbare Element kürzbar. Jede Gruppe ist daher ein kürzbares Monoid, aber die Umkehrung ist falsch wie das Monoid $(\mathbb{N}, +)$ zeigt.

Übung 2I7. Ein Element $a \in M$ ist genau dann linkskürzbar, wenn die Linksmultiplikation $\tau_a\colon M \to M$ mit $\tau_a(x) = a * x$ injektiv ist. Entsprechendes gilt für Rechtskürzbarkeit.

Übung 2I8. Jedes endliche, kürzbare Monoid ist eine Gruppe.

Wir wollen folgenden Satz beweisen:

Satz 2I9. *Ein kommutatives (!) Monoid lässt sich genau dann in eine Gruppe einbetten, wenn es kürzbar ist.*

Als Vorbild dient hierbei die Konstruktion der ganzen Zahlen $\mathbb{Z}$ aus den natürlichen Zahlen $\mathbb{N}$:

Übung 2I10. Sei M ein kommutatives Monoid. Man konstruiere eine Gruppe G und einen Monoidhomomorphismus $\varphi\colon M \to G$ mit folgender universelle Eigenschaft: zu jedem Monoidhomomorphismus $\psi\colon M \to H$ in eine Gruppe H existiert genau ein Gruppenhomomorphismus $h\colon G \to H$ mit $\psi = h \circ \varphi$.

KAPITEL 3

Ringe und Körper

Mit diesem Kapitel beginnen wir unsere Untersuchung der Ringe und Körper. Nach ein paar einführenden Beispielen und Definitionen zum Begriff des Rings (§3A) besprechen wir den zugehörigen Begriff des Ringhomomorphismus (§3B).

Der Rest des Kapitels widmet sich der Konstruktion von neuen Ringen aus alten:

- Konstruktion des Bruchkörpers (§3C).
- Konstruktion von Quotientenringen (§3D).
- Produkte von Ringen (§3Ea) und der chinesische Restsatz (§3F).
- Matrizenringe (§3Ec) und Monoidringe (§3G).

Damit haben wir eine Fülle von interessanten Beispielen und universellen Konstruktionen, die uns im Zuge der weiteren Entwicklung gute Dienste leisten werden. (Polynomring zum Beispiel sind spezielle Monoidringe; sie werden in Kapitel 4 genauer untersucht und spielen für alles Weitere eine wichtige Rolle. Matrizenringe werden in Kapitel 7 betrachtet und zum Beispiel für den Elementarteilersatz über Hauptidealringen verwendet.)

Im Hinblick auf unsere späteren Anwendungen klärt dieses Kapitel sozusagen einen Großteil der "äußeren Angelegenheiten" in der Kategorie der Ringe, bevor wir uns in den folgenden Kapiteln den "inneren Angelegenheiten" wie Teilbarkeitsfragen zuwenden.

§3A. Ringe und Körper

Zur Orientierung beginnen wir mit ein paar grundlegenden Beispielen bevor wir daraus die wesentlichen Eigenschaften als Axiome extrahieren.

§3Aa. Einführende Beispiele.

Beispiel 3A1. Die ganzen Zahlen $(\mathbb{Z},+,0,\cdot,1)$ mit ihrer Addition $+\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ und ihrer Multiplikation $\cdot\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ erfreuen sich folgender Eigenschaften:

(A) Die Addition bildet eine abelsche Gruppe:

(A0)	$\forall a,b\colon a+b=b+a$	(Kommutativität)
(A1)	$\forall a,b,c\colon (a+b)+c=a+(b+c)$	(Assoziativität)
(A2)	$\forall a\colon a+0=0+a=a$	(Neutrales Element)
(A3)	$\forall a\ \exists b\colon a+b=b+a=0$	(Inverse Elemente)

(D) Die Multiplikation ist distributiv über die Addition:

(DL) $\forall a,b,c\colon a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ (Linksdistributivität)
(DR) $\forall a,b,c\colon (a+b)\cdot c=(a\cdot c)+(b\cdot c)$ (Rechtsdistributivität)

(M) Die Multiplikation bildet ein kommutatives Monoid:

(M0) $\forall a,b\colon a\cdot b=b\cdot a$ (Kommutativität)
(M1) $\forall a,b,c\colon (a\cdot b)\cdot c=a\cdot(b\cdot c)$ (Assoziativität)
(M2) $\forall a\colon a\cdot 1=1\cdot a=a$ (Neutrales Element)

Beispiel 3A2. Die rationalen Zahlen $(\mathbb{Q},+,0,\cdot,1)$ mit ihrer Addition $+\colon \mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}$ und ihrer Multiplikation $\cdot\colon \mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}$ erfreuen sich der zusätzlichen Eigenschaft, dass jedes Element in $\mathbb{Q}^*=\mathbb{Q}\smallsetminus\{0\}$ invertierbar ist, und somit ist $(\mathbb{Q}^*,\cdot,1)$ eine Gruppe:

(M3) $\forall a\neq 0\ \exists b\colon a\cdot b=b\cdot a=1$ (Inverse Elemente)

Selbst wenn man von kommutativen Verknüpfungen ausgeht, führen nicht alle Konstruktionen wieder auf kommutative Verknüpfungen. Hierzu ein wichtiges Beispiel:

Beispiel 3A3. Die Menge $R=\mathbb{Z}^{n\times n}$ der $n\times n$-Matrizen über $\mathbb{Z}$ mit ihrer Addition und Multiplikation $+,\cdot\colon R\times R\to R$ (§3Ec) erfüllen alle obigen Axiome außer (M0) und (M3): Für $n\geq 2$ ist $(R,\cdot)$ ein nicht-kommutatives Monoid und nicht jede Matrix $a\neq 0$ ist invertierbar. Gleiches gilt für die Menge $\mathbb{Q}^{n\times n}$ der $n\times n$-Matrizen über $\mathbb{Q}$.

§**3Ab. Axiomatische Definition.** Die vorangegangenen grundlegenden Beispiele weisen uns die Richtung; ihre Eigenschaften erheben wir nun zu Axiomen:

Definition 3A4 (Ring)**.** Ein *Ring* $(R,+,0,\cdot,1)$ ist eine Menge R zusammen mit zwei Verknüpfungen $+,\cdot\colon R\times R\to R$ und zwei ausgezeichnete Elementen $0,1\in R$, die die obigen Axiome (A), (D) und (M1–2) erfüllen. Ein Ring heißt *kommutativ* wenn (M0) gilt.

Schreibweise. Das Element 0 ist durch $+$ bestimmt; es genügt daher, seine Existenz zu fordern:

(A2') $\exists 0\ \forall a\colon a+0=0+a=a$ (Existenz des neutralen Elements der Addition)

In der Bezeichnung lässt man es dann weg und spricht kurz von der additiven Gruppe $(R,+)$.

Ebenso ist das Element 1 eindeutig durch $\cdot$ bestimmt; es genügt daher, seine Existenz zu fordern:

(M2') $\exists 1\ \forall a\colon a\cdot 1=1\cdot a=a$ (Existenz des neutralen Elements der Multiplikation)

In der Bezeichnung lässt man es dann weg und spricht kurz von dem multiplikativen Monoid $(R,\cdot)$. Dies rechtfertigt die abkürzende Schreibweise $(R,+,\cdot)$ für einen Ring; 0 und 1 sind hier nur implizit. Zur Betonung ist es jedoch gelegentlich vorteilhaft, die Elemente 0 und 1 explizit zu nennen. Zur besseren Unterscheidung schreibt man für 0 und 1 im Ring R auch 0_R und 1_R.

Wenn für einen Ring $(R,+,\cdot)$ die in Rede stehenden Verknüpfungen aus dem Zusammenhang hervorgehen, so spricht man abkürzend von dem Ring R anstelle der korrekten aber schwerfälligen Bezeichnung $(R,+,\cdot)$. Dieser laxe Sprachgebrauch empfiehlt sich allerdings nur, wenn keine Verwechslungen zu befürchten sind.

Das in (A3) geforderte zu a inverse Element in $(R,+)$ ist eindeutig durch $+$ bestimmt und wird mit $-a$ bezeichnet. Damit definieren wir die *Subtraktion* $a-b$ durch $a+(-b)$.

Das in (M3) geforderte zu a inverse Element in $(R,\cdot)$ ist, wenn es existiert, eindeutig durch $\cdot$ bestimmt und wird mit a^{-1} bezeichnet. In diesem Fall definieren wir die *Division* a/b durch ab^{-1}.

Definition 3A5 (Körper)**.** Ein *Divisionsring* oder *Schiefkörper* ist ein Ring $(R,+,0,\cdot,1)$ mit $1 \neq 0$ sodass jedes Element $a \neq 0$ invertierbar ist (M3). Ein *Körper* ist ein kommutativer Divisionsring, also ein Ring mit $1 \neq 0$, der zusätzlich (M0) und (M3) erfüllt.

Beispiel 3A6. $(\mathbb{Z},+,\cdot)$ ist ein Ring, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sind Körper.

Die natürlichen Zahlen $(\mathbb{N},+,\cdot)$ sind kein Ring, denn $(\mathbb{N},+)$ ist nur ein Monoid aber keine Gruppe. Wir nennen $\mathbb{N}$ daher einen Halbring in folgendem Sinne:

Definition 3A7 (Halbring)**.** Ein *Halbring* $(R,+,0,\cdot,1)$ ist eine Menge R mit Verknüpfungen $+,\cdot\colon R\times R\to R$ und ausgezeichneten Elementen $0,1\in R$, die die obigen Axiome (A0–2), (D) und (M1–2) erfüllen. Ein Halbring heißt *kommutativ* wenn (M0) gilt.

Anmerkung. Halbringe erlauben keine so schöne Theorie wie Ringe, und wir werden sie daher nur am Rande betrachten. Sie treten in der Natur auf, wie das Beispiel $\mathbb{N}$ zeigt, und sind allein deshalb schon als Begriffsbildung nützlich.

Wir fassen diese Begriffe in folgender Übersicht zusammen:

	A0	A1	A2	A3	D	M0	M1	M2	M3	$1\neq 0$	Beispiele
Ring	✓	✓	✓	✓	✓		✓	✓			$\mathbb{Z}^{2\times 2}$
kommutativer Ring	✓	✓	✓	✓	✓	✓	✓	✓			$\mathbb{Z}$
Divisionsring	✓	✓	✓	✓	✓		✓	✓	✓	✓	$\mathbb{H}\subset\mathbb{C}^{2\times 2}$
Körper	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	$\mathbb{Q},\mathbb{R},\mathbb{C}$
komm. Halbring	✓	✓	✓		✓	✓	✓	✓			$\mathbb{N}$
Halbring	✓	✓	✓		✓		✓	✓			$\mathbb{N}^{2\times 2}$

Beispiel 3A8 (Nullring)**.** Die Menge $\{0\}$ ist ein Ring mit $0+0=0$ und $0\cdot 0=0$, genannt *Nullring*. In diesem Fall ist $1=0$ gleichzeitig das neutrale Element der Multiplikation.

Beispiel 3A9 (Matrizenringe)**.** Für jeden Ring R bildet die Menge $R^{n\times n}$ der $n\times n$-Matrizen über R einen Ring (siehe §3Ec). Es gilt $\mathbb{R}^{1\times 1}=R$. Selbst wenn R ein Körper ist, so ist $R^{n\times n}$ für $n\geq 2$ ein nicht-kommutativer Ring und nicht jede Matrix $a\neq 0$ ist invertierbar.

Matrizenringe lassen sich noch verallgemeinern:

Beispiel 3A10 (Endomorphismenringe)**.** Für jede abelsche Gruppe A ist $(\mathrm{End}(A),+,\circ)$ ein Ring (2E8). Für jeden K-Vektorraum V ist ebenso $\mathrm{End}_K(V)$ ein Ring; jede Basis $(v_1,\dots,v_n)$ von V stiftet einen Isomorphismus zwischen $\mathrm{End}_K(V)$ und $K^{n\times n}$.

Das Beispiel $(\mathrm{End}(A),+,\circ)$ enthält bereits alle Ringe in folgendem Sinne:

Satz 3A11 (Satz von Cayley für Ringe)**.** *Jeder Ring ist isomorph zu einem Unterring des Endomorphismenrings* $(\mathrm{End}(A),+,\circ)$ *einer geeigneten abelschen Gruppe* $(A,+)$*. Hierbei kann* $(A,+)=(R,+)$ *gewählt werden.*

Dies ermöglicht oft die bequeme Konstruktion von Ringen als Unterringe.

Beispiel 3A12 (Quaternionen)**.** Im Matrizenring $\mathbb{C}^{2\times 2}$ ist die Menge

$$\mathbb{H}=\left\{\left(\begin{smallmatrix} a & b \\ -\bar b & \bar a\end{smallmatrix}\right) \mid a,b\in\mathbb{C}\right\}$$

ein nicht-kommutativer Unterring (§3Ba). Zudem ist jede Matrix $x=\left(\begin{smallmatrix} a & b \\ -\bar b & \bar a\end{smallmatrix}\right)\neq 0$ invertierbar mit $x^{-1}=\frac{1}{|a|^2+|b|^2}\left(\begin{smallmatrix} \bar a & -b \\ \bar b & a\end{smallmatrix}\right)$. Demnach ist $\mathbb{H}$ ein Divisionsring.

Beispiel 3A13 (entgegengesetzter Ring)**.** Ist $(R,+,\cdot)$ ein Ring, dann ist auch $(R,+,\bar{\cdot})$ ein Ring mit der entgegengesetzten Multiplikation $a \mathbin{\bar{\cdot}} b = b \cdot a$. Diesen nennen wir den zu R *entgegesetzten Ring*, geschrieben R^{op}. Es gilt $R = R^{\mathrm{op}}$ genau dann, wenn der Ring R kommutativ ist.

Beispiel 3A14 (Polynomringe)**.** Für jeden Ring R bilden die Polynome $a_0 + a_1X + \cdots + a_nX^n$ mit Koeffizienten $a_0, a_1, \ldots, a_n \in R$ und einer Unbestimmten X einen Ring $R[X]$. Diesen konstruieren wir in §3G, eine ausführliche Diskussion folgt in Kapitel 4.

Beispiel 3A15 (Funktionenringe)**.** Ringe treten auch in der Analysis auf, zumeist als Funktionenringe wobei Addition und Multiplikation punktweise definiert sind. Zunächst:

- Die Menge $\mathrm{Abb}(\mathbb{R},\mathbb{R})$ aller Funktionen $\mathbb{R} \to \mathbb{R}$ ist ein Ring.

Unter den Funktionen $\mathbb{R} \to \mathbb{R}$ betrachtet man solche mit besonderen Eigenschaften. Es stellt sich dann oft heraus, das diese einen Unterring bilden. Zum Beispiel:

- $C(\mathbb{R},\mathbb{R}) = \{\, f\colon \mathbb{R} \to \mathbb{R} \mid f \text{ stetig} \,\}$
- $C^\infty(\mathbb{R},\mathbb{R}) = \{\, f\colon \mathbb{R} \to \mathbb{R} \mid f \text{ beliebig oft differenzierbar} \,\}$

Beispiel 3A16 (Ringe ohne Eins)**.** In der Analysis tritt auch die Funktionenmenge

- $C_0(\mathbb{R},\mathbb{R}) = \{\, f \in C(\mathbb{R},\mathbb{R}) \mid \lim_{|x|\to\infty} f(x) = 0 \,\}$

natürlich auf: Dies sind die stetigen Funktionen, die im Unendlichen verschwinden. Bezüglich Addition bilden sie eine abelsche Gruppe, bezüglich Multiplikation eine Halbgruppe, und die Distributivgesetze gelten. Nach unserer Definition ist die Menge $C_0(\mathbb{R},\mathbb{R})$ dennoch kein Ring, denn sie enthält kein Einselement: die hierfür in Frage kommende Funktion ist die konstante Funktion $x \mapsto 1$ für alle $x \in \mathbb{R}$, und diese liegt nicht in $C_0^\infty(\mathbb{R},\mathbb{R})$.

Gleiches gilt für die Menge der Funktionen mit kompaktem Träger:

- $C_c(\mathbb{R},\mathbb{R}) = \{\, f \in C(\mathbb{R},\mathbb{R}) \mid f \text{ hat kompakten Träger} \,\}$

Dennoch wollen wir an unserer Definition festhalten und von jedem Ring ein neutrales Element der Multiplikation fordern. Manche Autoren fassen die Definition weiter und erlauben auch Ringe ohne Einselement; Ringe mit Einselement heißen dann *Ringe mit Eins* oder *unitäre Ringe*. Beide Zugänge sind äquivalent: Man kann jeden Ring $(R,+,\cdot)$ ohne Eins durch Hinzunahme eines Einselements zu einem Ring mit Eins vervollständigen (§3Ha).

Beispiel 3A17 (Nicht-assoziative Ringe)**.** Nicht-assoziative Ringe treten seltener auf und erlauben keine so schöne Theorie. Eine nennenswerte Ausnahme sind Lie-Ringe: Auf jedem assoziativen Ring $(A,+,\cdot)$ definieren wir die Lie-Klammer durch $[a,b] := a\cdot b - b\cdot a$. Damit wird $(A,+,[])$ zu einem nicht-assoziativen Ring: die Distributivgesetze gelten weiterhin, aber an die Stelle des des Assoziativgesetzes der Multiplikation tritt die Jacobi-Identität $[a,[b,c]] + [b,[c,a]] + [c,[a,b]] = 0$ für alle $a,b,c \in A$.

Bemerkung 3A18. Die vorangegangenen Beispiele belegen, dass der Ringbegriff geeignet ist, eine Vielzahl sehr unterschiedlicher Beispiele in einer gemeinsamen Sprache zu fassen. Das ersetzt nicht die genaue Untersuchung der Einzelfälle, ermöglicht aber, das Gemeinsame zu erkennen und wiederkehrende Argumente effizient einzusetzen.

Zu diesem Zweck wurden der Ringbegriff im Laufe des 19. Jahrhunderts aus unzähligen Beispielen destilliert und hat sich als zentraler Untersuchungsgegenstand der Algebra etabliert. In Bezug auf Zahlen hat bereits Richard Dedekind (1888) solche Strukturen betrachtet. David Hilbert sprach in seinem *Zahlbericht* (1897) von *Zahlringen*.

Die axiomatische Definition wurde jedoch erst zu Beginn des 20. Jahrhunderts in ihre heutige Form gebracht. Die erste abstrakte Axiomatik findet sich bei Adolf Fraenkel (1914), die jedoch durch allzu spezielle Zusatzannahmen verunstaltet ist. Die hier angegebenen Axiome finden sich in dieser Form zuerst bei Emmy Noether (1921).

§**3Ac. Rechenregeln.** Aus Bequemlichkeit und zur besseren Lesbarkeit nutzen wir die Regel "Punkt vor Strich" und schreiben statt $(a\cdot b)+c$ kurz $a\cdot b+c$. Für die Multiplikation schreiben wir statt $a\cdot b$ kurz ab.

Proposition 3A19. *In jedem Ring $(R,+,\cdot)$ gelten die üblichen Rechenregeln:*

1. *Es gilt $0\cdot a = a\cdot 0 = 0$ für alle $a\in R$.*
2. *Es gilt $-a = (-1)\cdot a = a\cdot(-1)$ für alle $a\in R$.*
3. *Die Assoziativität der Addition erübrigt die Klammern in Summen $a_1+\cdots+a_m$; die Kommutativität erlaubt die beliebige Umordnung der Summanden.*
4. *Die Assoziativität der Multiplikation erübrigt die Klammern in Produkten $a_1\cdots a_m$; die Faktoren können beliebig umgeordnet werden falls sie paarweise kommutieren.*
5. *Die Distributivgesetze verallgemeinern sich auf längere Summen*

$$a(b_1+\cdots+b_n) = ab_1+\cdots+ab_n$$
$$(a_1+\cdots+a_m)b = a_1b+\cdots+a_mb$$

Hieraus folgt das allgemeine Distributivgesetz

$$\Big(\sum_{i=1}^m a_i\Big)\cdot\Big(\sum_{j=1}^n b_j\Big) = \sum_{i=1}^m\sum_{j=1}^n a_ib_j.$$

6. *Wir haben die Operation $\mathbb{Z}\times R\to R$, $(n,a)\mapsto na$, mit*

$$\begin{array}{lll} 0a=0 & (m+n)a=ma+na & n(a+b)=na+nb \\ 1a=a & (mn)a=m(na) & n(ab)=(na)b=a(nb) \end{array}$$

7. *Wir haben die Operation $R\times\mathbb{N}\to R$, $(a,n)\mapsto a^n$, mit*

$$\begin{array}{ll} a^0=1 & a^{m+n}=a^m\cdot a^n \\ a^1=a & (a^m)^n=a^{mn} \end{array}$$

Ist a invertierbar in $(R,\cdot)$, dann gelten diese Regeln für alle $m,n\in\mathbb{Z}$.

8. *Wenn $a,b\in R$ kommutieren, also $ab=ba$ erfüllen, dann gilt*

$$(ab)^n = a^nb^n$$

für alle $n\in\mathbb{N}$ sowie die binomische Formel

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^kb^{n-k}.$$

BEWEIS. (1) Es gilt $0 \cdot a = (0+0) \cdot a = (0 \cdot a) + (0 \cdot a)$. Durch Addition des additiven Inverse von $0 \cdot a$ folgt $0 = 0 \cdot a$. Entsprechend für $a \cdot 0 = 0$.

(2) Es gilt $0 = 0 \cdot a = (1+(-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a$, also $(-1) \cdot a = a$.

Die weiteren Aussagen folgen per Induktion. (Übung) □

Bemerkung 3A20. Wenn wir für einen Ring R den Sonderfall $1 = 0$ annehmen, dann folgt $a = 1a = 0a = 0$ für alle a, also ist R der Nullring. Von dieser Ausnahme abgesehen können wir also stets von $1 \neq 0$ ausgehen. Für Körper fordern wir $1 \neq 0$ explizit in der Definition.

Beispiel 3A21. Als Mahnung möchte ich kurz illustrieren, dass die obigen Rechenregeln zwar allseits vertraut aber keineswegs selbstverständlich sind; sie bedürfen eines Beweises. Auf $\mathbb{R}_{\geq 0}$ betrachten wir hierzu neben der Addition $+$ die Verknüpfung $\vee\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ mit $a \vee b = \max\{a,b\}$. Damit wird $(\mathbb{R}_{\geq 0}, \vee, +)$ zu einem kommutativen Halbring, in dem sowohl $0 \vee a = a \vee 0 = a$ als auch $a + 0 = 0 + a = a$ gilt. In diesem Halbring gilt also "$1 = 0$" aber $\mathbb{R}_{\geq 0}$ ist nicht der Nullring. Zur Übung überprüfe man, welche der obigen Rechenregeln in diesem Halbring noch gelten. Man nennt $(\mathbb{R}_{\geq 0}, \vee, +)$ den *Max-Plus-Halbring* oder werbewirksamer den *tropischen Halbring*. Dieser erfreut sich seit den 1990er Jahren großer Beliebtheit bei Abzählbarkeitsfragen in der algebraischen Geometrie.

§**3Ad. Äquivalente Definitionen.** Man könnte vermuten, dass man für Ringe $(R,+,\cdot)$ auch nicht-abelsche Gruppen $(R,+)$ zulassen könnte. Dies ist jedoch nicht der Fall: Die Kommutativität der Addition (A0) folgt aus den übrigen Ringaxiomen.

Proposition 3A22. *$(R,+,\cdot)$ ist genau dann ein Ring wenn gilt:*

(1) $(R,+)$ ist eine Gruppe.
(2) $(R,\cdot)$ ist ein Monoid.
(3) Die Multiplikation $\cdot$ ist distributiv über die Addition $+$.

BEWEIS. Es bleibt nur, die Kommutativität (A0) zu beweisen. Für $a, b \in R$ gilt

$$\begin{aligned} a+b+a+b &= (a+b)+(a+b) &&= 1(a+b)+1(a+b) \\ &= (1+1)(a+b) &&= (1+1)a+(1+1)b \\ &= (a+a)+(b+b) &&= a+a+b+b. \end{aligned}$$

Hierbei verwenden wir der Reihe nach (A1), (M2), (DR), (DL), (M2), (A1). Mit (A2) und (A3) können wir von links $-a$ und von rechts $-b$ addieren, und erhalten $b+a = a+b$. □

Proposition 3A23. *$(R,+,\cdot)$ ist genau dann ein Divisionsring wenn gilt:*

(1) $(R,+)$ ist eine Gruppe (mit neutralem Element 0).
(2) $(R^*,\cdot)$ ist eine Gruppe (wobei $R^* = R \smallsetminus \{0\}$).
(3) Die Multiplikation $\cdot$ ist distributiv über die Addition $+$.

BEWEIS. Wenn R ein Divisionsring ist, dann gelten (1), (2) und (3). Gelten umgekehrt die Bedingungen (1), (2) und (3), dann ist $(R,+)$ eine abelsche Gruppe, wie in der vorangegangenen Proposition gesehen. Da $(R^*,\cdot)$ eine Gruppe ist, gilt $R \neq \{0\}$ und demnach $1 \neq 0$. Die Assoziativität von $(R^*,\cdot)$ weitet sich auf $(R,\cdot)$ aus wegen $0a = a0 = 0$. □

Proposition 3A24. *$(R,+,\cdot)$ ist genau dann ein Körper wenn gilt:*

(1) $(R,+)$ *ist eine abelsche Gruppe (mit neutralem Element* 0*).*
(2) $(R^*,\cdot)$ *ist eine abelsche Gruppe (wobei* $R^* = R \smallsetminus \{0\}$*).*
(3) Die Multiplikation $\cdot$ *ist distributiv über die Addition* $+$*.*

BEWEIS. Dies folgt aus der vorangegangenen Proposition. Die Kommutativität von $(R^*,\cdot)$ weitet sich auf $(R,\cdot)$ aus wegen $0a = a0 = 0$. □

§**3Ae. Invertierbare Elemente.** Für jeden Ring $(R,+,0,\cdot,1)$ definieren wir

- $R^* = R \smallsetminus \{0\}$ die Menge der von Null verschiedenen Elemente,
- $R^\times$ die im Monoid $(R,\cdot,1)$ invertierbaren Elemente.

Wie in jedem Monoid ist $(R^\times,\cdot,1)$ eine Gruppe. Die invertierbare Elemente $a \in R^\times$ werden auch *Einheiten* des Rings R genannt. Dementsprechend heißt $R^\times$ auch die *Einheitengruppe*.

Beispiel 3A25. Es gilt $\mathbb{Z}^\times = \{\pm 1\}$ und $\mathbb{Q}^\times = \mathbb{Q}^*$.

Proposition 3A26. *Ein Ring* R *ist genau dann ein Divisionsring, wenn* $R^\times = R^*$ *gilt.*

BEWEIS. Die Inklusion $R^* \subset R^\times$ ist gleichbedeutend mit der Invertierbarkeit jedes Elements $a \neq 0$ (A3). Andererseits ist $R^\times \subset R^*$ gleichbedeutend mit $1 \neq 0$: Im Nullring $R = \{0\}$ gilt $R^* = \emptyset$, wegen $1 = 0$ aber $R^\times = \{0\}$. Gilt hingegen $1 \neq 0$, so folgt $R^\times \subset R^*$, denn 0 ist nicht invertierbar wegen $0a = a0 = 0 \neq 1$. □

§**3Af. Nullteiler.** Gilt $a \neq 0$ und $b \neq 0$ aber $ab = 0$, dann nennen wir a einen *Linksnullteiler* und b einen *Rechtsnullteiler*. In kommutativen Ringen stimmen beide Begriffe überein, und wir sprechen einfach nur von *Nullteilern*.

Beispiel 3A27.
- In $\mathbb{Z}/_6$ gilt $\bar{2} \neq 0$ und $\bar{3} \neq 0$ aber dennoch $\bar{2} \cdot \bar{3} = 0$.
- Für $a = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ und $b = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ in $\mathbb{Z}^{2\times 2}$ gilt $a \neq 0$ und $b \neq 0$ aber $ab = 0$.
- Auch $C^\infty(\mathbb{R},\mathbb{R})$ hat Nullteiler, zum Beispiel $f, g \neq 0$ mit disjunkten Trägern.

Definition 3A28. Ein Ring $(R,+,0,\cdot,1)$ heißt *nullteilerfrei* wenn $R^* \cdot R^* \subset R^*$ gilt.
Ein *Integritätsring* ist ein kommutativer, nullteilerfreier Ring mit $1 \neq 0$.

Ausführlicher bedeutet dies, dass für alle $a \neq 0$ und $b \neq 0$ in R auch $ab \neq 0$ gilt. Ein Ring mit $1 \neq 0$ ist also genau dann nullteilerfrei, wenn R^* ein Untermonoid von $(R,\cdot)$ ist.

Beispiel 3A29. Jeder Körper oder Divisionsring ist nullteilerfrei.
Der Ring $\mathbb{Z}$ ist zwar kein Körper aber ein Integritätsring.

Proposition 3A30. *Für einen Ring* R *sind äquivalent:*

1. R *ist nullteilerfrei.*
2. *Jedes Element* $a \neq 0$ *ist links- und rechtskürzbar, das heißt:*
   aus $ab = ac$ *folgt* $b = c$*, und aus* $ba = ca$ *folgt* $b = c$*, für alle* $b, c \in R$*.*

BEWEIS. (1) ⇒ (2): Aus $ab = ac$ folgt $a(b-c) = 0$. Aus der Nullteilerfreiheit folgt wegen $a \neq 0$ also $b - c = 0$ und somit $b = c$.

(2) ⇒ (1): Gilt $ab = 0$ mit $a \neq 0$, so folgt aus $ab = a0$ sofort $b = 0$. □

Übung 3A31. Jeder endliche Integritätsring ist ein Körper.

§3B. Homomorphismen

Definition 3B1. Ein *Homomorphismus* zwischen zwei Ringen $(R,+,\cdot)$ und $(S,+,\cdot)$ ist eine Abbildung $f\colon R \to S$ sodass gilt:

$$f(a+b) = f(a)+f(b) \text{ und } f(a\cdot b) = f(a)\cdot f(b) \text{ für alle } a,b \in R \text{ sowie } f(1_R) = 1_S.$$

Mit anderen Worten, $f\colon R \to S$ ist ein Ringhomomorphismus wenn gilt:

1. f ist ein Gruppenhomomorphismus von $(R,+)$ nach $(S,+)$,
2. f ist ein Monoidhomomorphismus von $(R,\cdot)$ nach $(S,\cdot)$.

Einen Ringhomomorphismus zwischen zwei Körpern nennen wir *Körperhomomorphismus*.

Proposition 3B2. *Ringe und ihre Homomorphismen bilden eine* Kategorie*:*

1. *Für jeden Ring R ist die Identität $\mathrm{id}_R\colon R \to R$ ein Ringhomomorphismus.*
2. *Sind $f\colon R \to S$ und $g\colon S \to T$ Ringhomomorphismen, so ist auch ihre Komposition $g\circ f\colon R \to T$ ein Ringhomomorphismus.*
3. *Diese Komposition ist assoziativ, das heißt $(h\circ g)\circ f = h\circ(g\circ f)$.* □

In dieser Kategorie bilden die Körper und ihre Homomorphismen eine volle Unterkategorie.

Wir vereinbaren den in jeder Kategorie üblichen Sprachgebrauch:

Definition 3B3. Ein bijektiver Ringhomomorphismus $f\colon R \to S$ heißt *Isomorphismus*. Weiterhin definieren wir:

- Ein *Endomorphismus* von R ist ein Homomorphismus $R \to R$.
  Die Menge aller Endomorphismen von R bezeichnen wir mit $\mathrm{End}(R)$.
- Ein *Automorphismus* von R ist ein Isomorphismus $R \xrightarrow{\sim} R$.
  Die Menge aller Automorphismen von R bezeichnen wir mit $\mathrm{Aut}(R)$.

Als einfaches aber nützliches Beispiel vermerken wir die universelle Eigenschaft des Rings $(\mathbb{Z},+,\cdot)$ der ganzen Zahlen in der Kategorie der Ringe:

Proposition 3B4. *Für jeden Ring R existiert genau ein Ringhomomorphismus $f\colon \mathbb{Z} \to R$, nämlich $f(n) = n1_R$ für alle $n \in \mathbb{Z}$.*

BEWEIS. *Eindeutigkeit:* Für jeden Ringhomomorphismus $f\colon \mathbb{Z} \to R$ muss $f(1) = 1_R$ gelten. Da f ein Gruppenhomomorphismus ist, folgt $f(n) = n1_R$, siehe 2D26.

Existenz: Die Abbildung $f\colon \mathbb{Z} \to R$ mit $f(n) = n1_R$ ist ein Gruppenhomomorphismus von $(\mathbb{Z},+)$ nach $(R,+)$, siehe 2D26. Sie ist zudem ein Monoidhomomorphismus von $(\mathbb{Z},\cdot)$ nach $(R,\cdot)$, denn sie erfüllt $f(1) = 1_R$ sowie $f(mn) = (mn)1_R = (m1_R)\cdot(n1_R) = f(m)\cdot f(n)$, siehe 3A19. □

Korollar 3B5. *Der Ring $(\mathbb{Z},+,\cdot)$ erlaubt als Endomorphismen nur die Identität.*

Gleiches gilt für den Körper $(\mathbb{Q},+,\cdot)$, insbesondere gilt $\mathrm{Aut}(\mathbb{Q},+,\cdot) = \{\mathrm{id}\}$. □

Für jeden Ringhomomorphismus $h\colon \mathbb{Z} \to \mathbb{Z}$ verlangen wir $h(1) = 1$, und daraus folgt $h(n) = n$ für alle $n \in \mathbb{Z}$. Die Gruppe $(\mathbb{Z},+)$ allein erlaubt mehr Endomorphismen (2D27). Ein Ring bzw. Körper kann durchaus eine nicht-triviale Automorphismengruppe haben, und diese spielt in der Galois-Theorie eine entscheidende Rolle:

Beispiel 3B6. Der Ring $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$, definiert als Unterring von $\mathbb{C}$, erlaubt als Automorphismen neben der Identität noch die Konjugation $a+bi \mapsto a-bi$.

Gleiches gilt für den Körper $\mathbb{Q}(i) = \{a+bi \mid a,b \in \mathbb{Q}\}$.

Proposition 3B7. *Jeder Ringhomomorphismus $f\colon R \to S$ induziert einen Gruppenhomomorphismus $f\colon R^\times \to S^\times$ zwischen den Gruppen der invertierbaren Elemente.*

BEWEIS. Für alle $a \in R^\times$ gilt $1_S = f(1_R) = f(aa^{-1}) = f(a)f(a^{-1})$. Also ist $f(a)$ invertierbar in S mit Inversem $f(a)^{-1} = f(a^{-1})$. Daher gilt $f(R^\times) \subset S^\times$ wie behauptet. □

Für Körper und Divisionsringe halten wir folgendes fest:

Korollar 3B8. *Jeder Ringhomomorphismus $f\colon R \to S$ von einem Divisionsring R in einen Ring S mit $1_S \neq 0_S$ ist injektiv.*

BEWEIS. Aus $R^* = R^\times$ folgt $f(R^*) = f(R^\times) \subset S^\times \subset S^*$, also $\ker(f) = \{0_R\}$. Die Injektivität des Homomorphismus f folgt dann aus dem Kriterium 2D35. □

Korollar 3B9. *Jeder Körperhomomorphismus ist injektiv.*

§3Ba. Unterringe und Unterkörper. Sei $(R,+,\cdot)$ ein Ring. Eine Teilmenge $S \subset R$ heißt *Unterring* oder *Teilring* von R, wenn gilt

1. S ist eine Untergruppe von $(R,+)$.
2. S ist ein Untermonoid von $(R,\cdot)$.

In diesem Fall lassen sich die Verknüpfungen auf S einschränken, $(S,+,\cdot)$ wird damit selbst zu einem Ring, und die Inklusion $\iota_S^R\colon S \to R$ ist ein Ringhomomorphismus.

Beispiel 3B10.
- In jedem Ring $(R,+,0,\cdot,1)$ ist die Gesamte Menge R ein Unterring.
- $\mathbb{Z}$ ist ein Unterring des Körpers $(\mathbb{Q},+,\cdot)$ der rationalen Zahlen.
- $\mathbb{N}$ ist kein Unterring von $(\mathbb{Z},+,\cdot)$, denn $\mathbb{N}$ ist keine Untergruppe von $(\mathbb{Z},+)$.
- $2\mathbb{Z}$ ist kein Unterring von $(\mathbb{Z},+,\cdot)$: zwar ist $dir\mathbb{Z}$ eine Untergruppe von $(\mathbb{Z},+)$, aber wegen $1 \notin 2\mathbb{Z}$ ist $2\mathbb{Z}$ kein Untermonoid von $(\mathbb{Z},\cdot)$.

Proposition 3B11. *Eine Teilmenge $S \subset R$ ist genau dann ein Unterring von $(R,+,\cdot)$ wenn $1 \in S$ sowie $S-S \subset S$ und $S \cdot S \subset S$ gilt.*

BEWEIS. Dieses Kriterium folgt unmittelbar aus den Kriterien für Untergruppen (§2De) und Untermonoide (§2Cf). □

Proposition 3B12. *Für jeden Ringhomomorphismus $f\colon R \to S$ gilt:*

(a) Für jeden Unterring $R' \subset R$ ist das Bild $f(R') \subset S$ ein Unterring.
(b) Für jeden Unterring $S' \subset S$ ist das Urbild $f^{-1}(S') \subset R$ ein Unterring.

BEWEIS. Dies folgt aus den entsprechenden Beobachtungen für Gruppenhomomorphismen (2D33) und Monoidhomomorphismen (2C23). □

Definition 3B13. Ein Unterring $S \subset R$ heißt *Unterkörper* oder *Teilkörper* wenn $(S,+,\cdot)$ ein Körper ist. Ist der gesamte Ring R ein Körper, so ist ein Unterring $S \subset R$ genau dann ein Unterkörper, wenn $a^{-1} \in S$ für alle $a \in S^*$ gilt.

Beispiel 3B14.
- In jedem Körper $(K,+,\cdot)$ ist die gesamte Menge K ein Unterkörper.
- $\mathbb{Q}$ ist ein Unterkörper des Körpers $(\mathbb{R},+,\cdot)$ der reellen Zahlen.
- $\mathbb{Z}$ ist zwar ein Unterring aber kein Unterkörper von $(\mathbb{Q},+,\cdot)$.

Proposition 3B15. *Für jeden Ringhomomorphismus $f\colon R \to S$ mit $1_S \neq 0_S$ gilt:*

(a) Für jeden Unterkörper $K \subset R$ ist das Bild $f(K) \subset S$ ein Unterkörper.
(b) Für jeden Unterkörper $L \subset S$ ist das Urbild $f^{-1}(L) \subset R$ ein Unterkörper.

Übung 3B16. In jedem Ring R ist das *Zentrum*

$$Z(R) := \{\, a \in R \mid ab = ba \text{ für alle } b \in R \,\}$$

ein kommutativer Unterring. Ist R ein Divisionsring, dann ist $Z(R)$ ein Unterkörper.

Nach Definition gilt $Z(R) = R$ genau dann wenn R kommutativ ist.

§3Bb. Erzeugte Unterringe und Unterkörper.

Proposition 3B17. *Ist $(R_i)_{i\in I}$ eine Familie von Unterringen $R_i \subset R$ eines Rings R, dann ist auch ihr Durchschnitt $S = \bigcap_{i\in I} R_i$ ein Unterring.*

Sind zudem alle R_i Unterkörper, dann ist auch S ein Unterkörper.

BEWEIS. Es gilt $1 \in R_i$ für alle $i \in I$, also auch $1 \in S$. Für $a,b \in S$ gilt $a,b \in R_i$ für alle $i \in I$, also $a-b \in R_i$ und $ab \in R_i$ für alle $i \in I$, also auch $a-b \in S$ und $ab \in S$.

Nehmen wir zusätzlich an, alle R_i sind Unterkörper. Für $a \in S$, $a \neq 0$, gilt $a \in R_i$ für alle $i \in I$, also $a^{-1} \in R_i$ für alle $i \in I$. (Das Inverse in R_i ist auch das Inverse in R, also durch a in R eindeutig bestimmt und unabhängig von R_i.) Wir schließen daraus, dass $a^{-1} \in S$. □

Beispiel 3B18. In jedem Ring R ist $\{n1_R \mid n \in \mathbb{Z}\}$ der Durchschnitt aller Unterringe und damit der kleinste Unterring von R. Man nennt ihn den *charakteristischen Unterring* oder *Primring* von R. Dies ist das Bild des Ringhomomorphismus $\mathbb{Z} \to R$.

Definition 3B19 (erzeugter Unterring)**.** Sei S ein Ring, $R \subset S$ ein Unterring und $\mathscr{X} \subset S$ eine Teilmenge. Dann bezeichnet $R[\mathscr{X}]$ den Durchschnitt aller Unterringe von S, die R und $\mathscr{X}$ enthalten. Dies ist der kleinste Unterring, der R und $\mathscr{X}$ enthält, und heißt der *von $\mathscr{X}$ über R erzeugte Unterring*.

Definition 3B20 (erzeugter Unterkörper)**.** Sei L ein Körper, $K \subset L$ ein Unterkörper und $\mathscr{X} \subset L$ eine Teilmenge. Dann bezeichnet $K(\mathscr{X})$ den Durchschnitt aller Unterkörper von L, die K und $\mathscr{X}$ enthalten. Dies ist der kleinste Unterkörper, der K und $\mathscr{X}$ enthält, und heißt der *von $\mathscr{X}$ über K erzeugte Unterkörper*.

Proposition 3B21. *Es sei $M = \langle \mathscr{X} \rangle^+$ das von $\mathscr{X}$ in $(S,\cdot)$ erzeugte Untermonoid, also*

$$M = \{\, x_1^{e_1} \cdots x_n^{e_n} \mid n \geq 0;\ x_1,\dots,x_n \in \mathscr{X};\ e_1,\dots,e_n \in \mathbb{N} \,\}.$$

Angenommen, die Elemente des Unterrings $R \subset S$ kommutieren mit den Elementen von $\mathscr{X}$, das heißt $rx = xr$ für alle $r \in R$ und $x \in \mathscr{X}$. Dann kommutiert R auch mit M und es gilt

$$R[\mathscr{X}] = \{\, \sum_{m\in M} r_m \cdot m \mid r\colon M \to R \text{ mit endlichem Träger} \,\}.$$

BEWEIS. Es gilt "$\supset$", denn $R[\mathscr{X}]$ ist ein Unterring, der R und $\mathscr{X}$ enthält, also auch alle Produkte und Summen von Elementen aus R und $\mathscr{X}$. Es gilt "$\subset$", denn Dank der Kommutierbarkeit ist auch die rechte Seite ist ein Unterring, der R und $\mathscr{X}$ enthält. □

Übung 3B22. In $\mathbb{C}$ ist der von $i = \sqrt{-1}$ über $\mathbb{Z}$ erzeugte Unterring

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Man bestimme ebenso in $\mathbb{C}$ den Unterring $\mathbb{Z}[\sqrt{c}]$ für $c \in \mathbb{Z}$.

In $\mathbb{C}$ ist der von $i = \sqrt{-1}$ über $\mathbb{Q}$ erzeugte Unterkörper

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

Man bestimme ebenso in $\mathbb{C}$ den Unterkörper $\mathbb{Q}(\sqrt{c})$ für $c \in \mathbb{Q}$.

Beispiel 3B23 (polynomielle Funktionen)**.** Die identische Abbildung $X\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x$, gehört zum Ring $C^\infty(\mathbb{R},\mathbb{R})$ der unendlich differenzierbaren Funktionen. Der von X über $\mathbb{R}$ erzeugte Unterring $\mathbb{R}[X]$ besteht aus allen Funktionen $f = \sum_{k=0}^n a_k X^k$ mit $a_0, \dots, a_n \in \mathbb{R}$, und wird der *Ring der polynomiellen Funktionen* genannt. Die Koeffizienten $a_0, \dots, a_n \in \mathbb{R}$ bestimmen offenbar die Funktion $f = \sum_{k=0}^n a_k X^k$; umgekehrt bestimmt die Funktion f die Koeffizienten, das heißt, es gilt

$$f = \sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{n} b_k X^k$$

genau dann, wenn $a_k = b_k$ für alle k gilt. Dies kann man auf verschiedene Arten beweisen, zum Beispiel mittels der Ableitung: es gilt nämlich $a_k = \frac{1}{k!} f^{(k)}(0)$. Insbesondere ist der Grad $\deg f := \sup\{k \in \mathbb{N} \mid a_k \neq 0\}$ wohldefiniert und erfüllt $\deg(f+g) \leq \sup\{\deg f, \deg g\}$ sowie $\deg(fg) = \deg(f) + \deg(g)$. Daraus sieht man unschwer, dass der Ring $\mathbb{R}[X]$ nullteilerfrei ist.

In $C^\infty(\mathbb{R}^d,\mathbb{R})$ betrachtet man entsprechend die Abbildungen $X_k\colon \mathbb{R}^d \to \mathbb{R}$, $(x_1,\dots,x_d) \mapsto x_k$. Der von $X_1,\dots,X_d$ über $\mathbb{R}$ erzeugte Unterring $\mathbb{R}[X_1,\dots,X_d]$ ist der Ring der polynomiellen Funktionen in d Unbestimmten.

Für die reellen Zahlen ist die geometrische Betrachtung von polynomiellen Funktionen sehr natürlich; über einem beliebigen Ring hingegen werden wir algebraisch vorgehen: Wir werden in §3G die universelle Konstruktion des Polynomrings $R[X]$ über einem beliebigen Ring R durchführen.

Beispiel 3B24 (rationale Funktionen)**.** Wir wollen den Ring $\mathbb{R}(X)$ der rationalen Funktionen P/Q mit $P, Q \in \mathbb{R}[X]$ als Ring von Abbildungen konstruieren. Dies ist etwas mühsam, dient aber als heilsamer Kontrast zur folgenden Konstruktion von Bruchkörpern.

Zunächst fällt auf, dass für polynomielle Funktionen $P, Q \in \mathbb{R}[X] \subset C^\infty(\mathbb{R},\mathbb{R})$ mit $Q \neq 0$ der Quotient P/Q nicht überall definiert ist, sondern nur auf der Menge $D = \mathbb{R} \smallsetminus N$, wobei $N = \{\, x \in \mathbb{R} \mid Q(x) = 0 \,\}$ die (endliche!) Menge von Nullstellen des Nenners Q ist.

Zur Abhilfe definieren wir $\mathrm{Abb}^*(\mathbb{R},\mathbb{R})$ als die Menge aller Funktionen $f\colon \mathbb{R} \supset D \to \mathbb{R}$ wobei $D = \mathbb{R} \smallsetminus N$ das Komplement einer endlichen Menge $N \subset \mathbb{R}$ ist. Zwei solche Funktionen $f_1\colon D_1 \to \mathbb{R}$ und $f_2\colon D_2 \to \mathbb{R}$ betrachten wir als äquivalent, geschrieben $f_1 \equiv f_2$, wenn $f_1|_D = f_2|_D$ auf dem Durchschnitt $D = D_1 \cap D_2$ gilt. Summe $f_1 + f_2$ und Produkt $f_1 \cdot f_2$ definieren wir wie gewohnt punktweise, allerdings ist das Ergebnis nur auf $D = D_1 \cap D_2$ definiert. Dies definiert eine Ringstruktur modulo Äquivalenz.

Jede Funktion $f_1\colon D_1 \to \mathbb{R}$ mit nur endlich vielen Nullstellen ist in $\mathrm{Abb}^*(\mathbb{R},\mathbb{R})$ invertierbar: wir setzen $D_2 = \{\, x \in D_1 \mid f(x) \neq 0 \,\}$ und definieren $f_2\colon D_2 \to \mathbb{R}$ durch $f_2(x) = f_1(x)^{-1}$ für alle $x \in D_2$. Somit gilt $f_1(x) f_2(x) = 1$ für alle $x \in D_2$ und damit $f_1 f_2 \equiv 1$. Insbesondere sind alle Polynome $Q \in \mathbb{R}[X]$, $Q \neq 0$, in $\mathrm{Abb}^*(\mathbb{R},\mathbb{R})$ invertierbar. Der von $\mathbb{R}[X]$ in $\mathrm{Abb}^*(\mathbb{R},\mathbb{R})$ erzeugte Unterkörper ist der *Körper der rationalen Funktionen*. Diese Konstruktion erklärt, wie man mit Polstellen von P/Q,

also Nullstellen des Nenners Q, umgeht und dennoch vernünftig rechnen kann. Zum Beispiel gilt $(X^2+1)/(X-1) \equiv X+1$.

So erfolgreich diese Blickweise für Polynome über $\mathbb{R}$ auch sein mag, für einen beliebigen Ring werden wir uns etwas Besseres einfallen lassen müssen. Davon handelt die Konstruktion des Bruchkörpers im nächsten Abschnitt.

§3C. Integritätsringe und Bruchkörper

§**3Ca. Motivation.** Der Ring $\mathbb{Z}$ der ganzen Zahlen lässt sich in den Körper $\mathbb{Q}$ der rationalen Zahlen einbetten: $\mathbb{Q}$ ist der kleinste solche Körper und entsteht aus $\mathbb{Z}$ durch Bildung von Brüchen. Diese Konstruktion wollen wir nun verallgemeinern. Dies führt uns zu der Frage: Welche Ringe lassen sich in einen Körper einbetten?

Bemerkung 3C1. Nehmen wir zunächst an, R sei Teilring eines Körpers L. Dann muss R kommutativ und zudem nullteilerfrei sein, denn aus $ab=0$ und $a\neq 0$ folgt $b=a^{-1}(ab)=0$.

Für Brüche $\frac{a}{b} := ab^{-1}$ mit $a\in R$, $b\in R^*$ gelten folgende Rechenregeln:

$$\frac{a}{b}=\frac{c}{d} \quad\Leftrightarrow\quad ad=bc, \qquad \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}, \qquad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}. \tag{3.1}$$

Hierfür ist die Kommutativität der Multiplikation wesentlich! Aus (3.1) ersieht man, dass die Menge $K=\{\,\frac{a}{b} \mid a\in R, b\in R^*\,\}$ aller Brüche ein Unterkörper von L ist. Dies ist der von R erzeugte Unterkörper, also der kleinste Unterkörper von L, der den Ring R enthält.

Beispiel 3C2. Im Körper $\mathbb{R}$ erzeugt der Unterring $\mathbb{Z}$ der ganzen Zahlen den Unterkörper $\mathbb{Q}=\{\,\frac{a}{b} \mid a\in\mathbb{Z}, b\in\mathbb{Z}^*\,\}$ der rationalen Zahlen.

Beispiel 3C3. In $\mathbb{C}$ ist der von $i=\sqrt{-1}$ über $\mathbb{Z}$ erzeugte Unterring $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$ (Beispiel 3B22). Sein Brchkörper in $\mathbb{C}$ ist $\mathbb{Q}(i)=\{a+bi \mid a,b\in\mathbb{Q}\}$.

Beispiel 3C4. Der Ring $\mathbb{R}[X]$ der polynomiellen Funktionen $\mathbb{R}\to\mathbb{R}$ (Beispiel 3B23) lässt sich in den Körper $\mathbb{R}(X)$ der rationalen Funktionen einbetten (Beispiel 3B24).

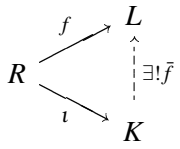
§**3Cb. Definition.** Betrachten wir nun das universelle Problem: Zu einem Ring R wollen wir einen Körper K konstruieren, in den sich R einbetten lässt. Zudem soll K minimal sein, das heißt nur aus den ohnehin notwendigen Brüchen bestehen:

Definition 3C5. Sei R ein Integritätsring. Ein *Bruchkörper* von R ist ein Körper K zusammen mit einem injektiven Ringhomomorphismus $\iota: R\to K$ sodass sich jedes Element $x\in K$ als Bruch $x=\iota(a)\iota(b)^{-1}$ mit $a\in R$, $b\in R^*$ schreiben lässt.

Von der obigen Bemerkung ausgehend zeigen wir nun zuerst die universelle Eigenschaft und Eindeutigkeit des gesuchten Bruchkörpers und dann die Existenz.

§**3Cc. Universelle Eigenschaft.**

Satz 3C6. *Jeder Bruchkörper (K,ι) von R erfreut sich folgender universeller Eigenschaft: Ist $f: R\to L$ ein injektiver Ringhomomorphismus in einen Körper L, dann existiert genau ein Körperhomomorphismus $\bar f: K\to L$ mit $f=\bar f\circ\iota$.*

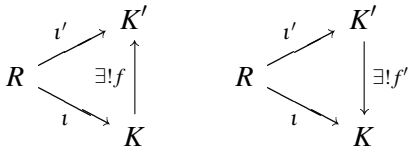


BEWEIS. Wir definieren $\bar{f}\colon K \to L$ wie folgt: jedes Element $x \in K$ schreibt sich als ein Bruch $x = \iota(a)\iota(b)^{-1}$ mit $a \in R$, $b \in R^*$. Da f injektiv ist, gilt $f(b) \neq 0$ und wir setzen $\bar{f}(x) = f(a)f(b)^{-1}$. Es bleibt allerdings zu zeigen, dass $\bar{f}$ damit wohldefiniert ist, denn x lässt sich durch verschiedene Brüche darstellen. Sind $x = \iota(a)\iota(b)^{-1} = \iota(c)\iota(d)^{-1}$ zwei Bruchschreibweisen für x, dann gilt $\iota(a)\iota(d) = \iota(b)\iota(c)$, also $\iota(ad) = \iota(bc)$, weil ι ein Homomorphismus ist. Aus der Injektivität von ι folgt $ad = bc$. Aus $f(ad) = f(bc)$ folgt wiederum $f(a)f(d) = f(b)f(c)$, weil f ein Homomorphismus ist. Daraus folgt schließlich $f(a)f(b)^{-1} = f(c)f(d)^{-1}$. Also ist $\bar{f}\colon K \to L$ in der Tat wohldefiniert. Dass $\bar{f}$ ein Körperhomomorphismus ist, folgt aus den Rechenregeln für Brüche (3.1). □

Korollar 3C7. *Je zwei Bruchkörper von R sind kanonisch isomorph.*

Der Beweis folgt leicht aus der universellen Eigenschaft des vorigen Satzes und ist ein schönes Beispiel für die Effizienz des "abstract general nonsense" der Kategorientheorie:

BEWEIS. Sind $(K, \iota\colon R \to K)$ und $(K', \iota'\colon R \to K')$ zwei Bruchkörper, dann existiert nach obigem Satz genau ein Homomorphismus $f\colon K \to K'$ mit $\iota' = f \circ \iota$.



Umgekehrt existiert genau ein Homomorphismus $f'\colon K' \to K$ mit $\iota = f' \circ \iota'$. Die Komposition $f' \circ f\colon K \to K$ ist ein Homomorphismus mit $\iota = (f' \circ f) \circ \iota$, also folgt aus der Eindeutigkeitsaussage $f' \circ f = \mathrm{id}_K$. Ebenso folgt $f \circ f' = \mathrm{id}_{K'}$. Damit sind f und f' die gesuchten Isomorphismen zwischen den Bruchkörpern (K, ι) und (K', ι'). □

§**3Cd. Konstruktion.** Anders als die Eindeutigkeit verlangt die Existenz eine explizite Konstruktion eines Bruchkörpers. Diese wollen wir nun ausführen:

Satz 3C8. *Zu jedem Integritätsring R existiert ein Bruchkörper* (K, ι).

BEWEIS. Auf der Menge $\tilde{K} = R \times R^*$ definieren wir die Verknüpfungen

$$(a,b) + (c,d) := (ad + bc, bd) \qquad \text{und} \qquad (a,b) \cdot (c,d) := (ac, bd).$$

Offenbar ist $(\tilde{K}, \cdot)$ ein kommutatives Monoid, nämlich das Produktmonoid $R \times R^*$ (2C21). Einselement ist $1_{\tilde{K}} = (1,1)$, invertierbar sind genau die Elemente $(a,b) \in R^\times \times R^\times$.

Man rechnet leicht nach, dass auch $(\tilde{K}, +)$ ein kommutatives Monoid ist:

- Neutrales Element der Addition ist $0_{\tilde{K}} = (0,1)$:
$$(0,1)+(a,b) = (0b+1a,1b) = (a,b)$$
$$(a,b)+(0,1) = (a1+b0,a1) = (a,b)$$
- Die Assoziativität der Addition auf $\tilde{K}$ folgt aus der von $+$ und $\cdot$ auf R:
$$[(a,b)+(c,d)]+(e,f) = (ad+bc,bd)+(e,f) = (adf+bcf+bde,bdf)$$
$$(a,b)+[(c,d)+(e,f)] = (a,b)+(cf+de,df) = (adf+bcf+bde,bdf)$$
- Die Kommutativität der Addition auf $\tilde{K}$ folgt aus der von $+$ und $\cdot$ auf R:
$$(a,b)+(c,d) = (ad+bc,bd) = (cb+da,db) = (c,d)+(a,b)$$
- Ist (a,b) invertierbar in $(\tilde{K},+)$, dann muss $b \in R^\times$ gelten. Alle Elemente $(a,b) \in R \times R^\times$ sind in $(\tilde{K},+)$ invertierbar, denn $(a,b)+(-ab^{-2},b^{-1}) = (0,1)$.

Die Multiplikation ist beinahe distributiv über die Addition:

$$(a,b)\cdot[(c,d)+(e,f)] = (a,b)\cdot(cf+de,df) = (acf+ade,bdf)$$
$$(a,b)\cdot(c,d)+(a,b)\cdot(e,f) = (ac,bd)+(ae,bf) = (acbf+bdae,bdbf)$$

Gleichheit gilt hier nur für $b = 1$: Multiplikation mit $(a,1)$ ist distributiv über die Addition.

Die Abbildung $\tilde{\iota}\colon R \to \tilde{K}$, $a \mapsto (a,1)$, ist ein injektiver Homomorphismus von $(R,+,\cdot)$ nach $(\tilde{K},+,\cdot)$. Leider ist $\tilde{K}$ in Anbetracht der obigen Rechnungen noch kein Körper.

Wir definieren die Relation $(a,b) \sim (c,d)$ durch $ad = cb$. Insbesondere gilt also $(ax,bx) \sim (a,b)$: die so eingeführte Relation entspricht also dem gewohnten Kürzen von Brüchen.

Wir zeigen zunächst, dass $\sim$ eine Äquivalenzrelation ist. Reflexivität und Symmetrie sind klar. Die Transitivität folgt aus Kommutativität und Kürzungsregel der Multiplikation: Gilt $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f)$, dann $ad = cb$ und $cf = ed$, also $adf = cbf = edb$, und daher $af = eb$, also $(a,b) \sim (e,f)$.

Addition und Multiplikation sind wohldefiniert modulo $\sim$, das heißt:

- Aus $(a,b) \sim (a',b')$ und $(c,d) \sim (c',d')$ folgt $(a,b)\cdot(c,d) \sim (a',b')\cdot(c',d')$.
  Denn $ab' = a'b$ und $cd' = c'd$ garantieren $acb'd' = a'c'bd$.
- Aus $(a,b) \sim (a',b')$ und $(c,d) \sim (c',d')$ folgt $(a,b)+(c,d) \sim (a',b')+(c',d')$.
  Denn $ab' = a'b$ und $cd' = c'd$ garantieren $(ad+bc,bd) \sim (a'd'+b'c',b'd')$: man vergleiche $(ad+bc)b'd' = adb'd'+bcb'd'$ und $(a'd'+b'c')bd = a'd'bd+b'c'bd$.

Auf der Quotientenmenge $K = \tilde{K}/_\sim$ induziert dies zwei Operationen $+,\cdot\colon K \times K \to K$, so dass die Quotientenabbildung $q\colon \tilde{K} \to K$ ein Homomorphismus ist. Die Äquivalenzklasse von (a,b) schreiben wir $q(a,b) = [a,b]$.

Nach obigen Rechnungen in $\tilde{K}$ ist auch $(K,+)$ ein kommutatives Monoid mit neutralem Element $[0,1]$. Ebenso ist $(K,\cdot)$ ein kommutatives Monoid mit neutralem Element $[1,1]$. Dank der Quotientenbildung gilt nun das Distributivgesetz für alle Elemente. Zudem gilt $[a,b]+[-a,b] = [0,b^2] = [0,1]$, also ist $(K,+)$ eine abelsche Gruppe. Es gilt $[a,b] = [0,1]$ genau dann, wenn $a = 0$; für alle $[a,b] \neq [0,1]$ gilt $[a,b]\cdot[b,a] = [ab,ab] = [1,1]$. Damit haben wir gezeigt, dass $(K,+,\cdot)$ ein Körper ist.

Nach Konstruktion ist die Abbildung $\iota = q \circ \tilde{\iota}\colon R \to K$, $a \mapsto [a,1]$ ein injektiver Ringhomomorphismus von R in den Körper K, denn $[a,1] = [a',1]$ bedeutet $a = a'$. Jedes Element

$x = [a,b] \in K$ mit $a \in R$, $b \in R^*$ schreibt sich als Bruch $x = \iota(a)\iota(b)^{-1}$. Damit ist (K,ι) der gesuchte Bruchkörper des Integritätsrings R. □

Bemerkung 3C9. Wir wissen nun, dass zu jedem Integritätsring R ein Bruchkörper (K,ι) existiert, und zwar bis auf eindeutige Isomorphie genau einer. Dies rechtfertigt, von *dem* Bruchkörper (K,ι) von R zu sprechen.

Da $\iota\colon R \to K$ ein injektiver Ringhomomorphismus ist, können wir den Ring R mit seinem Bild $\iota(R)$ in K identifizieren. Damit können wir R als Unterring von K betrachten, und der Homomorphismus ι wird dann zur Inklusion $R \subset K$. Diese Sichtweise ist für $\mathbb{Z} \subset \mathbb{Q}$ üblich und dient auch im allgemeinen Fall der Bequemlichkeit.

Notation. Wo eine abkürzende Bezeichnung gewünscht wird, werden wir zu einem Integritätsring R den Bruchkörper mit $\operatorname{Frac}(R)$ bezeichnen, in Anlehnung an den englischen Begriff *field of fractions*, mit der wie oben vereinbarten Inklusion $\iota\colon R \subset \operatorname{Frac}(R)$.

Bemerkung 3C10. Die Konstruktion $R \mapsto \operatorname{Frac}(R)$ ordnet jedem Integritätsring R seinen Bruchkörper zu. Aus $R \subset S$ folgt dabei $\operatorname{Frac}(R) \subset \operatorname{Frac}(S)$. Selbstverständlich können verschiedene Ringe denselben Bruchkörper ergeben. So gilt zum Beispiel für $R = \mathbb{Z}[\frac{1}{2}]$, oder für jeden Ring R mit $\mathbb{Z} \subset R \subset \mathbb{Q}$, offenbar $\mathbb{Q} = \operatorname{Frac}(\mathbb{Z}) \subset \operatorname{Frac}(R) \subset \operatorname{Frac}(\mathbb{Q}) = \mathbb{Q}$.

§3D. Ideale und Quotientenringe

Für jeden Ringhomomorphismus $f\colon R \to S$ erfreut sich der Kern

$$\mathfrak{a} = \ker(f) = f^{-1}(\{0\}) = \{\, a \in R \mid f(a) = 0 \,\}$$

der folgenden Eigenschaften:

(1) $\mathfrak{a}$ ist eine Untergruppe von $(R,+)$.
(2) $\mathfrak{a}$ ist absorbierend in $(R,\cdot)$, das heißt $R \cdot \mathfrak{a} \subset \mathfrak{a}$ und $\mathfrak{a} \cdot R \subset \mathfrak{a}$.

BEWEIS. Der Ringhomomorphismus $f\colon R \to S$ ist insbesondere ein Gruppenhomomorphismus von $(R,+)$ nach $(S,+)$, daher ist $\ker(f)$ eine Untergruppe von $(R,+)$ (2D34).

Für jedes $r \in R$ und $a \in \ker(f)$ gilt $f(ra) = f(r)f(a) = f(r)0 = 0$ also $ra \in \ker(f)$, und ebenso $f(ar) = f(a)f(r) = 0f(r) = 0$ also $ar \in \ker(f)$. □

Definition 3D1. Eine Teilmenge $\mathfrak{a} \subset R$ heißt *Ideal in R*, geschrieben $\mathfrak{a} \lhd R$, wenn gilt

(I1) $0 \in \mathfrak{a}$ und $\mathfrak{a} + \mathfrak{a} \subset \mathfrak{a}$,
(I2) $R\mathfrak{a} \subset \mathfrak{a}$ und $\mathfrak{a}R \subset \mathfrak{a}$.

Wegen $-1 \in R$ ist dies gleichbedeutend mit obigen Eigenschaften (1) und (2).

Bemerkung 3D2. In einem kommutativen Ring gilt $R\mathfrak{a} = \mathfrak{a}R$ und (I2) reduziert sich auf $R\mathfrak{a} \subset \mathfrak{a}$. In einem nicht-kommutativen Ring nennt man eine additive Untergruppe $\mathfrak{a} < R$ ein *Linksideal*, wenn $R\mathfrak{a} \subset \mathfrak{a}$ gilt, und ein *Rechtsideal* wenn $\mathfrak{a}R \subset \mathfrak{a}$ gilt.

Beispiel 3D3. In jedem Ring R sind $\{0\}$ und R Ideale, die sogenannten *trivialen Ideale*.

Bemerkung 3D4. Man beachte, dass ein Ideal $\mathfrak{a} \subsetneq R$ wegen $1 \notin \mathfrak{a}$ kein Unterring ist. Wäre $1 \in \mathfrak{a}$, dann folgte aus $R\mathfrak{a} \subset \mathfrak{a} \subset R$ automatisch $\mathfrak{a} = R$.

Beispiel 3D5. Ein Divisionsring R hat nur die trivialen Ideale $\{0\}$ und R. Ist nämlich $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{a} \neq \{0\}$, dann existiert $a \in \mathfrak{a}$ mit $a \neq 0$. Für alle $b \in R$ gilt also demnach $b = (ba^{-1})a \in \mathfrak{a}$, also $\mathfrak{a} = R$.

Proposition 3D6. *Ist $(\mathfrak{a}_i)_{i\in I}$ eine Familie von Idealen $\mathfrak{a}_i \subset R$ eines Rings R, dann ist auch ihr Durchschnitt $\mathfrak{a} = \bigcap_{i\in I} \mathfrak{a}_i$ ein Ideal.* □

Definition 3D7. Sei R ein Ring und $\mathscr{X} \subset R$ eine Teilmenge. Dann ist das von $\mathscr{X}$ in R *erzeugte Ideal* $(\mathscr{X})_R$ das kleinste Ideal von R, das $\mathscr{X}$ enthält, also

$$(\mathscr{X})_R := \bigcap \{\, \mathfrak{a} \lhd R \mid \mathfrak{a} \supset \mathscr{X} \,\}$$

Ist der Ring R aus dem Zusammenhang klar, so schreibt man statt $(\mathscr{X})_R$ kurz $(\mathscr{X})$. Besteht die Menge $\mathscr{X} = \{a_1, \ldots, a_n\}$ aus endlich vielen Elementen $a_1, \ldots, a_1 \in R$ so schreibt man schreibt man statt $(\mathscr{X})$ kurz $(a_1, \ldots, a_n)$.

Beispiel 3D8. In jedem Ring gilt $(0) = \{0\}$ und $(1) = R$; dies sind die trivialen Ideale.

Proposition 3D9. *1. Für jeden Ring R und jede Teilmenge $\mathscr{X} \subset R$ gilt*

$$(\mathscr{X}) = \Big\{ \sum_{i=1}^{n} r_i a_i r_i' \mid n \in \mathbb{N}, a_i \in \mathscr{X}, r_i, r_i' \in R \Big\}.$$

2. Sind $\mathfrak{a}_1, \ldots, \mathfrak{a}_m \subset R$ Ideale, dann erzeugt ihre Vereinigung das Ideal

$$(\mathfrak{a}_1 \cup \cdots \cup \mathfrak{a}_n)_R = \mathfrak{a}_1 + \cdots + a_n.$$

3. Sind $\mathfrak{a}, \mathfrak{b}$ Ideale, dann erzeugen die Produkte ab mit $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ das Produktideal

$$\mathfrak{a}\mathfrak{b} := \Big\{ \sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \Big\}$$

Man beachte: Für Ideale bezeichnet $\mathfrak{a}\mathfrak{b}$ nicht wie sonst üblich das Komplexprodukt $\{\, ab \mid a \in \mathfrak{a}, b \in \mathfrak{b} \,\}$ sondern das hiervon erzeugte Ideal in R.

BEWEIS. Die behauptete Gleichheit in (1) zeigt man wie folgt: Es gilt "$\supset$", denn die rechte Seite ist ein Ideal in R und enthält $\mathscr{X}$; da $(\mathscr{X})_R$ das kleinste solche Ideal ist, muss es in der rechten Seite enthalten sein. Umgekehrt gilt "$\supset$", denn das Ideal $(\mathscr{X})_R$ enthält $\mathscr{X}$ und damit auch alle Summen von Produkten, die auf der rechten Seite auftreten.

Die Punkte (2) und (3) beweist man ebenso. □

Korollar 3D10. *In jedem kommutativen Ring R gilt*

$$(a)_R = Ra = aR \qquad \text{und} \qquad (a_1, \ldots, a_n)_R = Ra_1 + \cdots + Ra_n.$$

Proposition 3D11. *Ein kommutativer Ring R ist genau dann ein Körper, wenn er nur die beiden trivialen Ideale $\{0\}$ und R hat.*

BEWEIS. Jeder Ring hat die trivialen Ideale $\{0\}$ und R. Ist R ein Divisionsring, dann sind diese beiden die einzigen Ideale (3D5).

Sei umgekehrt R ein kommutativer Ring, der nur die beiden trivialen Ideale $\{0\}$ und R hat. Zunächst gilt $\{0\} \neq R$, also ist $1_R \neq 0_R$. Für $a \neq 0$ gilt $(a) \neq \{0\}$ also $(a) = R$. Wegen $(a) = Ra$ bedeutet dies, es existiert ein $b \in R$ mit $ba = 1$, also ist a invertierbar. □

§3Da. Ideale im Ring $\mathbb{Z}$ der ganzen Zahlen.

Satz 3D12. *Im Ring $\mathbb{Z}$ ist jedes Ideal $\mathfrak{a}$ von der Form $\mathfrak{a} = (a)$ für ein $a \in \mathbb{Z}$.*

BEWEIS. Wenn $\mathfrak{a} = \{0\}$, dann erfüllt $a = 0$ das Verlangte. Andernfalls wählen wir $a \in \mathfrak{a}$ mit $a \neq 0$ und minimalem Betrag $|a|$, und zeigen $\mathfrak{a} = (a)$.

"$\mathfrak{a} \supset (a)$" ist klar: aus $a \in \mathfrak{a}$ folgt $(a) = \mathbb{Z}a \subset \mathbb{Z}\mathfrak{a} = \mathfrak{a}$.

"$\mathfrak{a} \subset (a)$" Für jedes $x \in \mathfrak{a}$ liefert Division mit Rest $x = qa + r$ mit $|r| < |a|$. Aus $x \in \mathfrak{a}$ und $qa \in \mathfrak{a}$ folgt $r = x - qa \in \mathfrak{a}$, also $r = 0$ aufgrund der Minimalität von a. Das bedeutet $x = qa$, also $x \in (a)$. Wir schließen daraus $\mathfrak{a} = (a)$. □

Bemerkung 3D13. Die Inklusion $(a) \subset (b)$ bedeutet $a = kb$ für ein $k \in \mathbb{Z}$, also $b \mid a$.

Der Durchschnitt $(a) \cap (b) = (c)$ bedeutet, dass c ein kleinstes gemeinsames Vielfaches von a und b ist. Denn $x \in (a) \cap (b)$ bedeutet, dass x ein gemeinsames Vielfaches von a und b ist, und nach obiger Konstruktion ist c ein kleinstes.

Die Summe $(a) + (b) = (c)$ bedeutet, dass c größter gemeinsamer Teiler von a und b ist. Wegen $a \in (c)$ und $b \in (c)$ ist c ein gemeinsamer Teiler von a und b. Zudem gilt $ma + nb = c$ für $m, n \in \mathbb{Z}$, also ist c ein größter gemeinsamer Teiler: Wenn $d \mid a$ und $d \mid b$ gilt, das heißt $a = ud$ und $b = vd$ mit $u, v \in \mathbb{Z}$, dann folgt $c = mud + nvd$, also $d \mid c$.

Für das Produkt gilt $(a) \cdot (b) = (ab)$. Das Beispiel $(2) \cap (2) = (2) \supsetneq (2) \cdot (2) = (4)$ zeigt, das Produkt und Durchschnitt von Idealen im Allgemeinen verschieden sind.

§3Db. Kongruenzen. Sei R ein Ring und $\mathfrak{a} \subset R$ ein Ideal. Für $x, y \in R$ definieren wir die *Kongruenz modulo* $\mathfrak{a}$, geschrieben $x \equiv y \pmod{\mathfrak{a}}$, durch die Bedingung $x - y \in \mathfrak{a}$.

1. Da $\mathfrak{a}$ eine Untergruppe von $(R, +)$ ist, ist $\equiv$ eine Äquivalenzrelation:
   (a) *Reflexivität:* Es gilt $x \equiv x$ denn $x - x = 0 \in \mathfrak{a}$.
   (b) *Symmetrie:* Aus $x \equiv y$ folgt $y \equiv x$, denn aus $x - y \in \mathfrak{a}$ folgt $y - x = -(x - y) \in \mathfrak{a}$.
   (c) *Transitivität:* Aus $x \equiv y$ und $y \equiv z$ folgt $x \equiv z$, denn aus $x - y \in \mathfrak{a}$ und $y - z \in a$ folgt $x - z = (x - y) + (y - z) \in \mathfrak{a}$.
2. Die Kongruenz modulo $\mathfrak{a}$ ist mit der Addition verträglich, das heißt:
   $$\text{Aus } x \equiv x' \text{ und } y \equiv y' \text{ folgt } x + x' \equiv y + y'.$$
   Die Voraussetzungen $x - x' \in \mathfrak{a}$ und $y - y' \in \mathfrak{a}$ garantieren nämlich, dass $(x - x') + (y - y') = (x + y) - (x' + y')$ ebenfalls in $\mathfrak{a}$ liegt.
3. Die Absorbtionseigenschaft $R\mathfrak{a} \subset \mathfrak{a}$ und $\mathfrak{a}R \subset \mathfrak{a}$ garantiert, dass die Kongruenz modulo $\mathfrak{a}$ auch mit der Multiplikation verträglich ist:
   $$\text{Aus } x \equiv x' \text{ und } y \equiv y' \text{ folgt } xx' \equiv yy'.$$
   die Voraussetzungen $x - x' \in \mathfrak{a}$ und $y - y' \in \mathfrak{a}$ garantieren nämlich, dass $xy - x'y' = (x - x')y + x'(y - y')$ ebenfalls in $\mathfrak{a}$ liegt.

§3Dc. Quotientenringe. Die Äquivalenzklasse $\mathfrak{cl}(x)$ eines Elementes $x \in R$ bezüglich der Kongruenz $\equiv$ ist die Menge aller zu x äquivalenten Elemente:

$$\mathfrak{cl}(x) = \{\, x' \in R \mid x' \equiv x \,\}$$

Es gilt $\mathfrak{cl}(x) = x + \mathfrak{a}$, denn $x' - x \in \mathfrak{a}$ ist gleichbedeutend mit $x' \in x + \mathfrak{a}$. Man nennt $x + \mathfrak{a}$ die *Nebenklasse* von x modulo $\mathfrak{a}$. Die *Quotientenmenge* ist die Menge aller Äquivalenzklassen:

$$R/\mathfrak{a} = \{\ \mathfrak{cl}(x) \mid x \in R\ \}.$$

Für die Summe zweier Nebenklassen $x + \mathfrak{a}$ und $y + \mathfrak{a}$ gilt

$$(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}.$$

Für das Produkt zweier Nebenklassen $x + \mathfrak{a}$ und $y + \mathfrak{a}$ gilt

$$(x + \mathfrak{a}) \cdot (y + \mathfrak{a}) = (x \cdot y) + \mathfrak{a}.$$

Somit kann man auf der Quotientenmenge $R/\mathfrak{a}$ Addition und Multiplikation definieren:

Satz 3D14. *Sei R ein Ring und $\mathfrak{a} \subset R$ ein Ideal. Dann existiert auf der Quotientenmenge $R/\mathfrak{a}$ genau eine Ringstruktur, die die Projektion $\pi\colon R \to R/\mathfrak{a}$, $x \mapsto \mathfrak{cl}(x)$, zu einem Ringhomomorphismus macht.*

BEWEIS. *Eindeutigkeit:* Wenn π ein Ringhomomorphismus ist, dann muss notwendigerweise $\mathfrak{cl}(x) + \mathfrak{cl}(y) = \mathfrak{cl}(x + y)$ und $\mathfrak{cl}(x) \cdot \mathfrak{cl}(y) = \mathfrak{cl}(x \cdot y)$ gelten.

Existenz: Die obigen Überlegungen zeigen, dass die Operationen

$$\mathfrak{cl}(x) + \mathfrak{cl}(y) := \mathfrak{cl}(x + y) \qquad \text{und} \qquad \mathfrak{cl}(x) \cdot \mathfrak{cl}(y) := \mathfrak{cl}(x \cdot y)$$

auf der Quotientenmenge $R/\mathfrak{a}$ wohldefiniert sind. Die Gültigkeit der Ringaxiome für $(R/\mathfrak{a}, +, \cdot)$ folgen nun aus der Gültigkeit der Ringaxiome für $(R, +, \cdot)$, siehe 2G1

Schließlich rechnen wir die Distributivität nach:

- $\mathfrak{cl}(x) \cdot (\mathfrak{cl}(y) + \mathfrak{cl}(z)) = \mathfrak{cl}(x \cdot (y + z)) = \mathfrak{cl}(xy + xz) = \mathfrak{cl}(x) \cdot \mathfrak{cl}(y) + \mathfrak{cl}(x) \cdot \mathfrak{cl}(z)$.
- $(\mathfrak{cl}(x) + \mathfrak{cl}(y)) \cdot \mathfrak{cl}(z) = \mathfrak{cl}((x + y) \cdot z) = \mathfrak{cl}(xz + yz) = \mathfrak{cl}(x) \cdot \mathfrak{cl}(z) + \mathfrak{cl}(y) \cdot \mathfrak{cl}(z)$.

Damit ist $(R/\mathfrak{a}, +, \cdot)$ ein Ring wie behauptet. □

Bemerkung 3D15. Das Nullelement von $R/\mathfrak{a}$ ist $\mathfrak{cl}(0) = \mathfrak{a}$, das Einselement ist $\mathfrak{cl}(1) = 1 + \mathfrak{a}$. Der Kern von $\pi\colon R \to R/\mathfrak{a}$ ist $\mathfrak{a}$. Daraus folgt insbesondere:

1. Jedes Ideal $\mathfrak{a} \subset R$ tritt als Kern eines Ringhomomorphismus auf.
2. Für $\mathfrak{a} = \{0\}$ erhalten wir einen Isomorphismus $\pi\colon R \xrightarrow{\sim} R/\{0\}$.
3. Für $\mathfrak{a} = R$ ist der Quotient $R/R = \{\mathfrak{cl}(0)\}$ der Nullring.

Beispiel 3D16. Für den Ring $\mathbb{Z}$ und das Ideal $(n) = n\mathbb{Z}$ erhalten wir den Quotientenring $\mathbb{Z}/_n := \mathbb{Z}/n\mathbb{Z}$. Für $n = 0$ gilt $\mathbb{Z}/_0 \cong \mathbb{Z}$. Für $n > 0$ hingegen hat $\mathbb{Z}/_n$ genau n Elemente:

$$\mathbb{Z}/_n = \{\overline{0}, \ldots, \overline{n-1}\}.$$

Für jede ganze Zahl $a \in \mathbb{Z}$ existiert nämlich gemäß Division mit Rest genau ein Paar $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ mit $a = qn + r$ und $0 \le r < n$. Wir können demnach $r := a \operatorname{rem} n$ als kanonischen Repräsentanten der Äquivalenzklasse $\mathfrak{cl}(a) = a + n\mathbb{Z}$ wählen. Damit ist die Abbildung

$$\varphi\colon \{0, \ldots, n-1\} \to \mathbb{Z}/_n \quad \text{mit} \quad a \mapsto \mathfrak{cl}(a) = a + n\mathbb{Z}$$

eine Bijektion. Wir können noch etwas mehr sagen: Die Abbildung φ wird zu einem Ringisomorphismus wenn wir auf der Repräsentantenmenge $\{0, \ldots, n-1\} \subset \mathbb{Z}$ die Addition

$$a \underset{n}{+} b := (a + b) \operatorname{rem} n$$

und die Multiplikation

$$a \cdot_n b := (a \cdot b) \operatorname{rem} n$$

definieren. Anders gesagt, das Rechnen mit Restklassen $\mathfrak{cl}(a) \in \mathbb{Z}/_n$ entspricht dem Rechnen mit Elementen $a \in \mathbb{Z}$, wobei man stets nur den Rest der Division mit n behält.

Proposition 3D17. *Der Ring $\mathbb{Z}/_n$ ist genau dann ein Körper, wenn p eine Primzahl ist.*

BEWEIS. Ist $n = pq$ eine zusammengesetzte Zahl mit Faktoren $p, q \geq 2$, dann hat der Ring $\mathbb{Z}/_n$ Nullteiler: es gilt $\overline{p} \neq \overline{0}$ und $\overline{q} \neq \overline{0}$ aber $\overline{pq} = \overline{0}$.

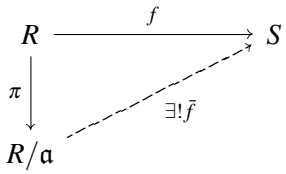
Ist $p \geq 2$ hingegen eine Primzahl, dann ist $\mathbb{Z}/_p$ nullteilerfrei: $\overline{ab} = \overline{0}$ bedeutet nämlich $ab \in (p)$, und für jede Primzahl p impliziert $p \mid ab$ dass $p \mid a$ oder $p \mid b$, also $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$ in $\mathbb{Z}/_p$. Als endlicher Integritätsring ist $\mathbb{Z}/_p$ dann ein Körper (3A31). □

§**3Dd. Homomorphiesatz.** Der Quotientenring $R/\mathfrak{a}$ hat folgende universelle Abbildungseigenschaft:

Satz 3D18 (Homomorphiesatz)**.** *Sei $\mathfrak{a} \lhd R$ ein Ideal und sei $\pi\colon R \to R/\mathfrak{a}$ die Projektion auf den Quotientenring. Für jeden Ringhomomorphismus $f\colon R \to S$ sind äquivalent:*

1. *Es gilt $\mathfrak{a} \subset \ker(f)$.*
2. *Es existiert ein Ringhomomorphismus $\bar{f}\colon R/\mathfrak{a} \to S$ sodass $f = \bar{f} \circ \pi$.*

In diesem Fall sagen wir, der Homomorphismus $f\colon R \to S$ *induziert* den Homomorphismus $\bar{f}\colon R/\mathfrak{a} \to S$ auf dem Quotienten $R/\mathfrak{a}$. Dieser Sachverhalt wird durch das folgende kommutative Diagramm veranschaulicht:



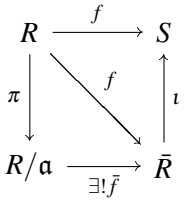
BEWEIS. "(1) $\Leftarrow$ (2)" ist klar. "(1) $\Rightarrow$ (2)" sieht man wie folgt: Wir definieren $\bar{f}(\mathfrak{cl}(x)) = f(x)$. Dies ist wohldefiniert, denn für $\mathfrak{cl}(x) = \mathfrak{cl}(x')$ gilt $x - x' \in \mathfrak{a} \subset \ker(f)$, also $f(x) = f(x')$. Man rechnet problemlos nach, dass $\bar{f}$ tatsächlich ein Ringhomomorphismus ist. □

Satz 3D19 (kanonische Faktorisierung)**.** *Jeder Ringhomomorphismus $f\colon R \to S$ mit Kern $\mathfrak{a} = \ker(f)$ und Bild $\bar{R} = f(R)$ faktorisiert gemäß*

$$f\colon R \xrightarrow{\pi} R/\mathfrak{a} \xrightarrow{\bar{f}} \bar{R} \xrightarrow{\iota} S$$

in die Projektion π, einen Isomorphismus $\bar{f}\colon R/\mathfrak{a} \xrightarrow{\sim} \bar{R}$, und die Inklusion ι.

Die Situation wird durch das folgende kommutative Diagramm veranschaulicht:



BEWEIS. Dies folgt aus dem Homomorphiesatz 3D18 angewendet auf $\mathfrak{a} = \ker(f)$. □

Satz 3D20 (Isomorphiesatz)**.** *Sei $f\colon R \to S$ ein surjektiver Homomorphismus von Ringen.*

1. *Das Bild eines Ideals $\mathfrak{a} \lhd R$ ist wieder ein Ideal $f(\mathfrak{a}) \lhd S$.*
2. *Das Urbild eines Ideal $\mathfrak{b} \lhd S$ ist wieder ein Ideal $f^{-1}(\mathfrak{b}) \lhd R$.*

Diese Zuordnung stiftet eine Bijektion zwischen den Idealen $\mathfrak{a} \subset R$, die $\ker(f)$ enthalten, und den Idealen $\mathfrak{b} \subset S$. Für diese induziert f einen Ringisomorphismus $R/\mathfrak{a} \cong S/f(\mathfrak{a})$.

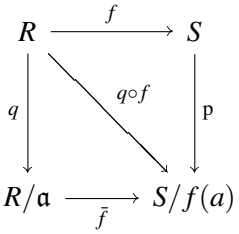
Für jeden Quotientenring $S = R/\mathfrak{m}$ und $\mathfrak{m} \subset \mathfrak{a} \lhd R$ gilt demnach $R/\mathfrak{a} \cong (R/\mathfrak{m}) \,/\, (\mathfrak{a}/\mathfrak{m})$.

BEWEIS. (a) Sei $\mathfrak{a} \lhd R$. Das Bild $\mathfrak{b} = f(\mathfrak{a})$ ist eine Untergruppe in $(S,+)$, siehe 2D33. Sei $b \in \mathfrak{b}$ und $s \in S$. Dann gibt es $a \in \mathfrak{a}$ mit $f(a) = b$ und wegen der Surjektivität von f auch ein $r \in R$ mit $f(r) = s$. Dann ist $sb = f(r)f(a) = f(ra) \in f(\mathfrak{a})$, da $\mathfrak{a}$ ein Ideal ist.

(b) Sei $\mathfrak{b} \lhd S$. Das Urbild $\mathfrak{a} = f^{-1}(\mathfrak{b})$ ist eine Untergruppe in $(S,+)$, siehe 2D33. Sind $a \in \mathfrak{a}$ und $r \in R$, dann ist $f(ra) = f(r)f(a) \in S \cdot \mathfrak{b} \subset \mathfrak{b}$, also $ra \in f^{-1}(\mathfrak{b})$.

Aus der Surjektivität von f folgt $f(f^{-1}(\mathfrak{b})) = \mathfrak{b}$ für alle Teilmengen $\mathfrak{b} \subset S$, und insbesondere für alle Ideale. Die Umkehrung $f^{-1}(f(\mathfrak{a})) = \mathfrak{a}$ für alle Ideale $\mathfrak{a} \lhd R$ mit $\ker(f) \subset \mathfrak{a}$ beweist man wie für Gruppen (9B14).

Sei ein Ideal $a \lhd R$ mit $\ker(f) \subset \mathfrak{a}$ gegeben. Dann ist $f(\mathfrak{a})$ ein Ideal in S und wir können die Projektion $q\colon S \to S/f(\mathfrak{a})$ auf den Quotientenring betrachten:



Die Komposition $q \circ f\colon R \to S/f(\mathfrak{a})$ ist surjektiv und hat als Kern das Ideal $\mathfrak{a}$. Auf dem Quotientenring $R/\mathfrak{a}$ induziert dies einen Isomorphismus $\bar{f}\colon R/\mathfrak{a} \xrightarrow{\sim} S/f(\mathfrak{a})$. □

§**3De. Charakteristik eines Rings.** Der Ring $\mathbb{Z}$ der ganzen Zahlen hat folgende universelle Eigenschaft (3B4): Zu jedem Ring R existiert genau ein Ringhomomorphismus

$$\varphi\colon \mathbb{Z} \to R.$$

Sein Bild ist der charakteristische Unterring von R, also

$$\operatorname{im}(\varphi) = \{\, n1_R \mid n \in \mathbb{Z} \,\}.$$

Sein Kern ist ein Ideal in $\mathbb{Z}$, und somit wissen wir, dass $\ker(\varphi) = (n)$ für ein $n \in \mathbb{N}$ gilt (§3Da). Dies induziert einen Isomorphismus

$$\bar{\varphi}\colon \mathbb{Z}/_n \xrightarrow{\sim} \operatorname{im}(\varphi) \subset R.$$

Definition 3D21. Wir nennen $\operatorname{char}(R) := n$ die *Charakteristik* des Rings R.

Beispiel 3D22. Es gilt $\operatorname{char}(\mathbb{Z}) = 0$, $\operatorname{char}(\mathbb{Q}) = 0$, $\operatorname{char}(\mathbb{Z}/_n) = n$.

Wir wissen, dass $\mathbb{Z}/_n$ genau dann ein Körper ist, wenn n eine Primzahl ist (3D17).

Korollar 3D23. *Für jeden nullteilerfreien Ring R gilt entweder* $\operatorname{char}(R) = 0$ *oder aber* $\operatorname{char}(R) > 0$ *ist eine Primzahl.* □

In jedem Körper K ist der Durchschnitt aller Unterkörper der kleinste Unterkörper von K. Man nennt ihn den *charakteristischen Unterkörper* oder *Primkörper* von K.

Korollar 3D24. *Sei K ein Körper und sei $P \subset K$ sein Primkörper. Im Falle* $\operatorname{char}(K) = 0$ *induziert der Ringhomomorphismus $\varphi\colon \mathbb{Z} \to K$ einen Körperisomorphismus $\mathbb{Q} \xrightarrow{\sim} P$, im Falle* $\operatorname{char}(K) = p > 0$ *einen Isomorphismus $\mathbb{Z}/_p \xrightarrow{\sim} P$.* □

§3Df. Frobenius-Homomorphismus.

Satz 3D25. *Sei R ein kommutativer Ring der Charakteristik p, wobei $p \geq 2$ eine Primzahl sei. Dann ist die Abbildung $\mathfrak{f}\colon R \to R$ mit $x \mapsto x^p$ ein Ringhomomorphismus.*

BEWEIS. Die Multiplikativität $\mathfrak{f}(xy) = \mathfrak{f}(x)\mathfrak{f}(y)$ und $\mathfrak{f}(1) = 1$ sind klar. Es bleibt die Additivität $\mathfrak{f}(x+y) = \mathfrak{f}(x) + \mathfrak{f}(y)$ zu zeigen. Hier gilt

$$\mathfrak{f}(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p = \mathfrak{f}(x) + \mathfrak{f}(y).$$

Das Verschwinden der mittleren Terme beruht auf dem nachfolgenden Lemma. □

Lemma 3D26. *Für jede Primzahl $p \geq 2$ und $0 < k < p$ gilt $p \mid \binom{p}{k}$.*

BEWEIS. Der Binomialkoeffizient $\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$ ist eine ganze Zahl. Die Primzahl p teilt $p(p-1)\cdots(p-k+1) = \binom{p}{k}k!$, aber nicht $k!$, also gilt $p \mid \binom{p}{k}$. □

Korollar 3D27. *Für jeden Körper K der Charakteristik $p \geq 2$ ist der Frobenius-Homomorphismus $\mathfrak{f}\colon K \to K$ injektiv. Ist K endlich, dann ist $\mathfrak{f}$ ein Automorphismus des Körpers K.*

BEWEIS. Jeder Körperhomomorphismus ist injektiv (3B9). Für jede endliche Menge impliziert injektiv automatisch surjektiv. □

Übung 3D28. Der Frobenius-Homomorphismus $\mathfrak{f}\colon K \to K$ lässt den Primkörper $P \subset K$ punktweise fest. Insbesondere gilt $x^p = x$ für alle $x \in \mathbb{Z}/_p$ und alle Primzahlen p. Daraus folgt der kleine Satz von Fermat:

Satz 3D29. *Für alle $a \in \mathbb{Z}$ und Primzahlen p gilt $a^p \equiv a \pmod{p}$.*

§3E. Neue Ringe aus alten

Wir haben bislang zwei wichtige Konstruktionen kennengelernt: Jedem Integritätsring R können wir seinen Bruchkörper zuordnen, und zu jedem Ideal $\mathfrak{a} \lhd R$ können wir den Quotientenring R/a konstruieren. Wir kommen nun zu weiteren ebenso einfachen wie nützlichen Konstruktionen: Produktringe und Matrizenringe.

§3Ea. Produkte von Ringen.

Sind $R_1, \ldots, R_n$ Ringe, dann ist ihr Produkt

$$R = R_1 \times \cdots \times R_n$$

ein Ring bezüglich der komponentenweisen Verknüpfungen Addition und Multiplikation:

$$(a_1,\dots,a_n)+(b_1,\dots,b_n)=(a_1+b_1,\dots,a_n+b_n),$$
$$(a_1,\dots,a_n)\cdot(b_1,\dots,b_n)=(a_1\cdot b_1,\dots,a_n\cdot b_n).$$

Nullelement ist $0_R=(0_1,\dots,0_n)$, Einselement ist $1_R=(1_1,\dots,1_n)$.

Proposition 3E1. *Der Produktring $R=R_1\times\cdots\times R_n$ erfreut sich folgender universeller Eigenschaft: Für $k=1,\dots,n$ ist jede Projektion $\pi_k\colon R\to R_k$ mit*

$$\pi_k(a_1,\dots,a_{k-1},a_k,a_{k+1},\dots,a_n)=a_k$$

ein Ringhomomorphismus. Sind $f_k\colon S\to R_k$ Ringhomomorphismen, für $k=1,\dots,n$, dann existiert genau ein Ringhomomorphismus $f\colon S\to R$, der $f_k=\pi_k\circ f$ für alle $k=1,\dots,n$ erfüllt. Mit anderen Worten, wir haben eine natürliche Bijektion

$$\operatorname{Hom}(S,R_1\times\cdots\times R_n)\cong\operatorname{Hom}(S,R_1)\times\cdots\times\operatorname{Hom}(S,R_n),$$
$$f\mapsto(\pi_1\circ f,\dots,\pi_n\circ f).$$

Übung 3E2. Man beweise die universelle Eigenschaft des Produktrings.

Übung 3E3. Für die Gruppe der invertierbaren Elemente gilt $R^\times=R_1^\times\times\cdots\times R_n^\times$.

Übung 3E4. Sind $\mathfrak{a}_1\lhd R_1,\dots,\mathfrak{a}_n\lhd R_n$ Ideale, dann ist $\mathfrak{a}=\mathfrak{a}_1\times\cdots\times\mathfrak{a}_n$ ein Ideal in R. Dies ist der Kern des Ringhomomorphismus $R_1\times\cdots\times R_n\to R_1/\mathfrak{a}_1\times\cdots\times R_n/\mathfrak{a}_n$. Umgekehrt ist jedes Ideal $\mathfrak{a}\lhd R$ von der Form $\mathfrak{a}=\mathfrak{a}_1\times\cdots\times\mathfrak{a}_n$ mit $\mathfrak{a}_1\lhd R_1,\dots,\mathfrak{a}_n\lhd R_n$. Also ist jedes homomorphe Bild eines Produktrings wieder ein Produktring.

Bemerkung 3E5. Die Abbildung $\iota_k\colon R_k\to R$ mit

$$\iota_k(a)=(0_1,\dots,0_{k-1},a,0_{k+1},\dots,0_n)$$

sendet den Ring R_k bijektiv auf das Ideal

$$I_k=\{0_1\}\times\cdots\times\{0_{k-1}\}\times R_k\times\{0_{k+1}\}\times\cdots\times\{0_n\}.$$

Dieses ist für sich selbst gesehen ein Ring, aber das Einselement $e_k=(0,\dots,0,1_k,0,\dots,0)$ von I_k ist von dem Einselement 1_R des Rings R verschiedenen. Also ist I_k kein Unterring.

Übung 3E6. Die Elemente $e_1,\dots,e_n$ liegen im Zentrum von R und erfüllen:

1. Idempotenz: $e_i^2=e_i$ für alle i.
2. Orthogonalität: $e_ie_j=0$ für alle $i\neq j$.
3. Vollständigkeit: $e_1+\cdots+e_n=1_R$.

Seien umgekehrt in einem Ring R Elemente $e_1,\dots,e_n\in R$ mit diesen Eigenschaften gegeben. Dann ist $R_k=Re_k$ ein Ideal in R. Für sich genommen ist I_k ein Ring mit Einselement e_k. Der Ring R ist isomorph zum Produktring $R_1\times\cdots\times R_n$.

§**3Eb. Potenzen von Ringen.** Sei R ein Ring und X eine Menge. Wir machen die Menge R^X aller Abbildungen $f,g\colon X\to R$ zu einem Ring mit den punktweisen Verknüpfungen

$$f+g\colon X\to R,\qquad (f+g)(x)=f(x)+g(x),$$
$$f\cdot g\colon X\to R,\qquad (f\cdot g)(x)=f(x)\cdot g(x).$$

Für $X = \{1,\dots,n\}$ ist dies der Produktring $R^n = R \times \cdots \times R$ mit n Faktoren. Für $Y \subset X$ definiert die Einschränkung den Ringhomomorphismus $\pi_X^Y \colon R^X \to R^Y$, $f \mapsto f|_Y$. Für die einelementige Menge $Y = \{x\}$ gilt $R^Y \cong R$ und $\pi_X^Y \colon R^X \to R$ ist die Auswertung $f \mapsto f(x)$.

Wir definieren die Operation $\cdot \colon R \times R^X \to R^X$ durch $(r \cdot f)(x) = r \cdot f(x)$ für alle $x \in X$. Diese ist mit den anderen Operationen in der offensichtlichen Weise verträglich.

Übung 3E7. Man übertrage die obigen Aussagen von Produktringen $R_1 \times \cdots \times R_n$ soweit möglich auf Potenzringe R^I und beweise die so umformulierten Aussagen.

§**3Ec. Matrizenringe.** Zu natürlichen Zahlen $m,n \in \mathbb{N}$ setzen wir $I = \{1,\dots,m\}$ und $J = \{1,\dots,n\}$. Eine *Matrix* der Größe $m \times n$ mit Koeffizienten in R ist eine Familie $A = (a_{ij})$ von Elementen $a_{ij} \in R$ indiziert durch $(i,j) \in I \times J$. Dies ist nichts anderes als eine Abbildung $a \colon I \times J \to R$, geschrieben als $(i,j) \mapsto a_{ij}$. Die Menge $R^{I\times J}$ dieser Matrizen bezeichnen wir kurz mit $R^{m\times n}$. In der Praxis schreibt man eine Matrix $A \in R^{m\times n}$ als rechteckiges Schema mit m Zeilen und n Spalten. In dieser Schreibweise ist $v \in R^{m\times 1}$ ein Spaltenvektor mit m Zeilen, und $w \in R^{1\times n}$ ein Zeilenvektor mit n Spalten. Ist $(R,+,\cdot)$ ein Ring, dann definieren wir die Addition und die Multiplikation von Matrizen über R wie folgt:

$$+ \colon R^{m\times n} \times R^{m\times n} \to R^{m\times n}, \quad (A,B) \mapsto C = A + B \quad \text{mit } c_{ij} = a_{ij} + b_{ij}, \tag{3.2}$$

$$\cdot \colon R^{m\times n} \times R^{n\times r} \to R^{m\times r}, \quad (A,B) \mapsto C = A \cdot B \quad \text{mit } c_{ik} = \textstyle\sum_{j=1}^{n} a_{ij} \cdot b_{jk}. \tag{3.3}$$

Man beachte, dass nur Matrizen passender Größe miteinander multipliziert werden können. Zudem definieren wir die Multiplikation

$$\cdot \colon R \times R^{m\times n} \to R^{m\times n}, \quad (r,A) \mapsto B = r \cdot A \quad \text{mit } b_{ij} = r \cdot a_{ij}. \tag{3.4}$$

Übung 3E8. Beweisen Sie die folgenden Aussagen:

1. Die Addition von Matrizen definiert eine abelsche Gruppe $(R^{m\times n},+)$.
2. Die Multiplikation von Matrizen ist assoziativ und distributiv über die Addition.
3. Zu jeder Matrix $A \in R^{m\times n}$ ist die Einheitsmatrix $1_{m\times m}$ links-neutral, also $1_{m\times m} \cdot A = A$, und die Einheitsmatrix $1_{n\times n}$ rechts-neutral, also $A \cdot 1_{n\times n} = A$.

Leiten Sie daraus folgendes Ergebnis ab:

Proposition 3E9. *Ist R ein Ring, so ist auch $R^{n\times n}$ ein Ring.*

Übung 3E10. Man bestimme das Zentrum $Z(R^{n\times n})$ in Abhängigkeit von $Z(R)$.

Übung 3E11. Für $m,n \geq 1$ konstruiere man einen Isomorphismus $R^{mn\times mn} \cong (R^{m\times m})^{n\times n}$.

Übung 3E12. Jeder Ringhomomorphismus $R \to S$ induziert einen Ringhomomorphismus $R^{n\times n} \to S^{n\times n}$ durch Anwendung auf alle Einträge einer Matrix.

Übung 3E13. Ist $\mathfrak{a} \subset R$ ein Ideal, dann ist $\mathfrak{a}^{n\times n} \subset R^{n\times n}$ ein Ideal.
Dies ist der Kern des Ringhomomorphismus $R^{n\times n} \to \bar{R}^{n\times n}$ mit $\bar{R} = R/\mathfrak{a}$.
Umgekehrt ist jedes Ideal des Matrizenrings $R^{n\times n}$ von der Form $\mathfrak{a}^{n\times n}$.
Also ist jedes homomorphe Bild eines Matrizenrings wieder ein Matrizenring.

§3F. Der chinesische Restsatz

§**3Fa. Motivation.** Der chinesische Restsatz verallgemeinert folgende Beobachtung:

Beispiel 3F1. Die Ringe $\mathbb{Z}/6$ und $\mathbb{Z}/2 \times \mathbb{Z}/3$ sind isomorph vermöge der Abbildung $\bar{\varphi}$:

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{\varphi}(x)$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{2})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{2})$

Wenn es überhaupt einen Ringisomorphismus gibt, dann muss $\bar{\varphi}(0) = 0$ und $\bar{\varphi}(1) = 1$ gelten, sowie $\bar{\varphi}(1+1) = 1+1$, etc. Für die obigen Ringe $\mathbb{Z}/6$ und $\mathbb{Z}/2 \times \mathbb{Z}/3$ erhält man so die angegebene Abbildung und stellt fest, dass $\bar{\varphi}$ bijektiv ist. Umgekehrt sieht man leicht, dass $\bar{\varphi}$ tatsächlich ein Ringhomomorphismus ist, zum Beispiel mittels 3E1.

Beispiel 3F2. Man sollte nicht leichtfertig glauben, es gelte immer $\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$. Kleinstes Gegenbeispiel: Die Ringe $\mathbb{Z}/4$ und $\mathbb{Z}/2 \times \mathbb{Z}/2$ nicht isomorph, denn in $\mathbb{Z}/4$ gilt $1+1 \neq 0$ während in $\mathbb{Z}/2 \times \mathbb{Z}/2$ gilt $1+1=0$.

§3Fb. Der chinesische Restsatz für zwei Faktoren.

Definition 3F3. Zwei Ideale $\mathfrak{a}_1, \mathfrak{a}_2 \subset R$ heißen *teilerfremd* wenn $\mathfrak{a}_1 + \mathfrak{a}_2 = R$ gilt.

Das bedeutet, es gilt $1 = a_1 + a_2$ für gewisse Elemente $a_1 \in \mathfrak{a}_1$ und $a_2 \in \mathfrak{a}_2$.

Satz 3F4. *Seien $\mathfrak{a}_1, \mathfrak{a}_2 \subset R$ Ideale in einem Ring R. Dann hat der Ringhomomorphismus*

$$\varphi\colon R \to R/\mathfrak{a}_1 \times R/\mathfrak{a}_2, \qquad z \mapsto (z+\mathfrak{a}_1, z+\mathfrak{a}_2)$$

den Kern $\ker(\varphi) = \mathfrak{a}_1 \cap \mathfrak{a}_2$. *Dies induziert einen injektiven Homomorphismus*

$$\bar{\varphi}\colon R/(\mathfrak{a}_1 \cap \mathfrak{a}_2) \to R/\mathfrak{a}_1 \times R/\mathfrak{a}_2, \qquad z+\mathfrak{a}_1\cap\mathfrak{a}_2 \mapsto (z+\mathfrak{a}_1, z+\mathfrak{a}_2)$$

Dieser ist genau dann ein Isomorphismus wenn $\mathfrak{a}_1 + \mathfrak{a}_2 = R$ gilt.

In diesem Fall existieren $a_1 \in \mathfrak{a}_1$ und $a_2 \in \mathfrak{a}_2$ mit $a_1 + a_2 = 1$. Die Abbildung

$$\psi\colon R \times R \to R/(\mathfrak{a}_1 \cap \mathfrak{a}_2), \qquad (x,y) \mapsto xa_2 + ya_1 + \mathfrak{a}_1 \cap \mathfrak{a}_2$$

erfüllt $\mathfrak{a}_1 \times \mathfrak{a}_2 \subset \ker(\psi)$ und der induzierte Homomorphismus

$$\bar{\psi}\colon R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \to R/(\mathfrak{a}_1 \cap \mathfrak{a}_2), \qquad (x+\mathfrak{a}_1, y+\mathfrak{a}_2) \mapsto xa_2 + ya_1 + \mathfrak{a}_1 \cap \mathfrak{a}_2$$

ist der zu $\bar{\varphi}$ inverse Isomorphismus.

BEWEIS. Die Aussage $\ker(\varphi) = \mathfrak{a}_1 \cap \mathfrak{a}_2$ ist klar. Ist φ surjektiv, so gibt es $a_1, a_2 \in R$ mit $\varphi(a_1) = (0,1)$ und $\varphi(a_2) = (1,0)$. Das heißt

$$a_1 \equiv 0 \pmod{a_1} \qquad a_1 \equiv 1 \pmod{a_2}$$
$$a_2 \equiv 1 \pmod{a_1} \qquad a_2 \equiv 0 \pmod{a_2}$$

Also $a_1 \in \mathfrak{a}_1$, $a_2 \in \mathfrak{a}_2$ mit $\varphi(a_1 + a_2) = (1,1)$. Daher gilt $a_1 + a_2 \equiv 1$ modulo $\mathfrak{a}_1 \cap \mathfrak{a}_2$. Dann gilt aber auch $1 = a_1 + a_2'$ mit $a_2' = a_2 + (1 - a_1 - a_2) \in \mathfrak{a}_2 + \mathfrak{a}_2 = \mathfrak{a}_2$.

Umgekehrt: Aus $1 = a_1 + a_2$ folgt $1 \equiv a_2 \pmod{\mathfrak{a}_1}$ und $1 \equiv a_1 \pmod{\mathfrak{a}_2}$. Für $x, y \in R$ erhalten wir so $\varphi(ya_1 + xa_2) = (x+\mathfrak{a}_1, y+\mathfrak{a}_2)$. Also ist φ surjektiv. Die angegebenen Formeln für $\bar{\varphi}$ und $\bar{\psi}$ erlauben, direkt $\bar{\varphi} \circ \bar{\psi} = \mathrm{id}$ und $\bar{\psi} \circ \bar{\varphi} = \mathrm{id}$ nachzurechnen. □

Bemerkung 3F5. Wenn wir den chinesischen Restsatz auf den Ring $\mathbb{Z}$ der ganzen Zahlen anwenden, dann wissen wir bereits , dass jedes Ideal $\mathfrak{a} \lhd \mathbb{Z}$ die Form $\mathfrak{a} = (a)$ hat (§3Da). Wir werden später in der Teilbarkeitslehre sehen, dass zwei Ideale (m) und (n) in $\mathbb{Z}$ genau dann teilerfremd sind, wenn die ganzen Zahlen m und n teilerfremd sind, also $\mathrm{ggT}(m,n) = 1$

erfüllen. In diesem Fall kann man geeignete Vielfache $a_1 = um$ und $a_2 = vn$ mit $um+vn = 1$ mittels des euklidischen Algorithmus finden. Damit wird der chinesische Restsatz durch eine algorithmische Formulierung vervollständigt.

§**3Fc. Der chinesische Restsatz für mehrere Faktoren.** Wir wollen den chinesischen Restsatz nun von zwei auf mehrere Faktoren verallgemeinern. Zur Vereinfachung nehmen wir im Folgenden den Ring R als kommutativ an.

Lemma 3F6. *Für alle $a_1, a_2 \lhd R$ gilt $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}_1 \cap \mathfrak{a}_2$. Aus $\mathfrak{a}_1 + \mathfrak{a}_2 = 1$ folgt $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_1 \cap \mathfrak{a}_2$.*

BEWEIS. Die erste Aussage ist klar. Angenommen es gilt $1 = a_1 + a_2$ für $a_1 \in \mathfrak{a}_1$, $a_2 \in \mathfrak{a}_2$. Für alle $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$ folgt dann $x = xa_1 + xa_2$, also $x \in \mathfrak{a}_1\mathfrak{a}_2$. □

Lemma 3F7. *Sind $\mathfrak{a}_1, \mathfrak{a}_2$ und $\mathfrak{a}_1, \mathfrak{a}_3$ teilerfremd, dann sind auch $\mathfrak{a}_1$ und $\mathfrak{a}_2\mathfrak{a}_3$ teilerfremd.*

BEWEIS. Aus $1 = a_1 + a_2$ und $1 = a_1' + a_3$ mit $a_1, a_1' \in \mathfrak{a}_1$, $a_2 \in \mathfrak{a}_2$, $a_3 \in \mathfrak{a}_3$ folgt

$$1 = (a_1 + a_2)(a_1' + a_3) = (a_1a_1' + a_2a_1' + a_1a_3) + a_2a_3 \in \mathfrak{a}_1 + \mathfrak{a}_2\mathfrak{a}_3.$$

Also $\mathfrak{a}_1 + \mathfrak{a}_2\mathfrak{a}_3 = R$. □

Satz 3F8. *Seien $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subset R$ paarweise teilerfremde Ideale eines kommutativen Rings R. Dann haben wir einen Ringisomorphismus*

$$R/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \to R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n,$$
$$z + (\mathfrak{a}_1 \cdots \mathfrak{a}_n) \mapsto (z + \mathfrak{a}_1, \dots, z + \mathfrak{a}_n).$$

BEWEIS. Wir führen Induktion über n: Für $n = 1$ ist nichts zu beweisen. Wir nehmen an, der Satz gilt für $n-1$ Faktoren und beweisen ihn für n Faktoren. Nach Voraussetzung ist $\mathfrak{a}_n$ teilerfremd zu jedem der Ideale $\mathfrak{a}_1, \dots, \mathfrak{a}_{n-1}$. Nach Lemma 3F7 ist $\mathfrak{a}_n$ dann teilerfremd zum Produkt $\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}$, und mit 3F6 folgt $\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}\mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} \cap \mathfrak{a}_n$:

$$R/(\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}\mathfrak{a}_n) = R/(\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} \cap \mathfrak{a}_n) \xrightarrow{\sim} R/(\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}) \times R/\mathfrak{a}_n \xrightarrow{\sim} R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n$$

Der erste Isomorphismus wird von Satz 3F4 geliefert, der zweite Isomorphismus durch die Induktionsvoraussetzung. □

§3G. Monoidringe

§**3Ga. Motivation.** Zur Orientierung beginnen wir mit ein paar vertrauten Beispielen. Wir knüpfen hierzu an das Beispiel 3B23 der polynomiellen Funktionen.

Beispiel 3G1. Ein Polynom ist ein Ausruck der Form

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{k=0}^{n} a_nX^n.$$

Die Koeffizienten $a_0, a_1, a_2, \dots, a_n$ sind hierbei Elemente in einem Ring R, und wir stellen uns X als eine "Variable" oder "Unbestimmte" vor — was immer das sein mag. (Hierzu gilt immer noch der hintersinnige Ausspruch von Hermann Weyl: "Niemand kann sagen, was eine Variable ist.") Pragmatisch gesehen bedeutet dies lediglich, dass man formal mit obigen Ausdrücken arbeitet, und Gleichheit $\sum a_nX^n = \sum b_nX^n$ gilt genau dann, wenn $a_k = b_k$ für alle

k gilt. Mehr muss man nicht wissen um mit Polynomen zu rechnen, und diese Eigenschaft wird daher im folgenden Abschnitt (§3Gb) zur Definition gemacht.

Beispiel 3G2. Man kann sich unschwer vorstellen, was Polynome in d Unbestimmten sind:

$$\sum_{\nu\in\mathbb{N}^d} a_\nu \cdot X_1^{\nu_1} X_2^{\nu_2} \cdots X_d^{\nu_d}.$$

Damit hierbei die Summe endlich ist, verlangen wir wie zuvor, dass nur endlich viele der Koeffizienten $a_\nu \in R$ von 0 verschieden sind. Die Menge $M = \{\, X_1^{\nu_1} X_2^{\nu_2} \cdots X_d^{\nu_d} \mid \nu \in \mathbb{N}^d \,\}$ bildet dabei einen Monoid bezüglich Multiplikation bildet. Wir wollen diese Beobachtung zum Ausgangspunkt der folgenden allgemeinen Konstruktion machen.

Die allgemeine Zielsetzung ist also folgende: Ist R ein kommutativer Ring und M ein Monoid, so wollen wir mit "formalen Summen" $r_1m_1 + \cdots + r_km_k$ rechnen, wobei $r_1,\dots,r_k \in R$ und $m_1,\dots,m_k \in M$. Solche Ausdrücke sollen dabei in der offensichtlichen Weise addiert werden, und für das Produkt soll gelten

$$\Big(\sum_{i=1}^{k} r_i m_i\Big)\Big(\sum_{j=1}^{\ell} r'_j m'_j\Big) = \sum_{i=1}^{k}\sum_{j=1}^{\ell} (r_i r'_j)(m_i m'_j).$$

Hierbei ist $r_ir'_j$ das Produkt in R, und $m_im'_j$ das Produkt im Monoid M. Des Weiteren wollen wir "ganz normal" rechnen, das heißt, alle Rechenregeln für Ringe sollen erfüllt sein. Wir suchen also einen Ring S, in dem solche "formalen Summen" einen Sinn haben. Außer diesen Forderungen soll S keinen weiteren Einschränkungen unterliegen.

§**3Gb. Definition.** Nach den vorangegangenen Überlegungen präzisieren wir nun unser Vorhaben durch folgende Definition:

Definition 3G3. Sei $(R,+,\cdot)$ ein kommutativer Ring und $(M,\cdot)$ ein Monoid. Wir nennen einen Ring $(S,+,\cdot)$ *Monoidring* von M über R wenn gilt:

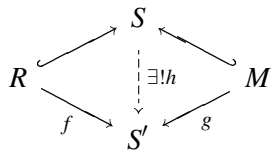
(1) $(R,+,\cdot)$ ist ein Unterring im Zentrum des Rings $(S,+,\cdot)$.
(2) $(M,\cdot)$ ist ein Untermonoid des Monoids $(S,\cdot)$.
(3) Jedes Element $s \in S$ schreibt sich eindeutig als Linearkombination $s = \sum_{m\in M} r_m \cdot m$, wobei $r\colon M \to R$, $m \mapsto r_m$, eine Abbildung mit endlichem Träger ist.

Bemerkung 3G4. Aus dieser Definition ergeben sich folgende Rechenregeln:

$$\begin{aligned}
\Big(\sum_{m\in M} r_m \cdot m\Big) + \Big(\sum_{m\in M} r'_m \cdot m\Big) &= \sum_{m\in M} (r_m + r'_m)\cdot m \\
\Big(\sum_{a\in M} r_a \cdot a\Big)\Big(\sum_{b\in M} r'_b \cdot b\Big) &= \sum_{a\in M}\sum_{b\in M} (r_a r'_b)\cdot(ab) \\
&= \sum_{c\in M} s_c \cdot c \quad \text{mit} \quad s_c = \sum_{\substack{a,b\in M\\ ab=c}} r_a r'_b
\end{aligned}$$

§**3Gc. Universelle Eigenschaft.**

Satz 3G5. *Jeder Monoidring S von M über R erfreut sich folgender universeller Eigenschaft: Sei S' ein Ring, $f\colon R \to S'$ ein Ringhomomorphismus in das Zentrum des Rings S', und $g\colon M \to S'$ ein Monoidhomomorphismus in das Monoid $(S',\cdot)$. Dann existiert genau ein Ringhomomorphismus $h\colon S \to S'$, der $h|_R = f$ und $h|_M = g$ erfüllt.*



BEWEIS. *Eindeutigkeit:* Seien $h,h' \colon S \to S'$ Ringhomomorphismen mit $h|_R = h'|_R = f$ und $h|_M = h'|_M = g$. Jedes Element $s \in S$ schreibt sich als $s = \sum_{m\in M} r_m \cdot m$, also muss gelten

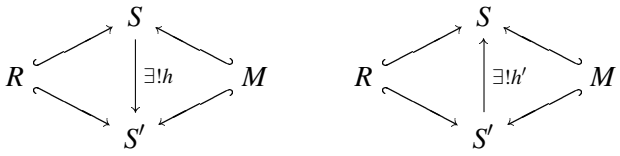
$$h(s) = \sum_{m\in M} h(r_m)\cdot h(m) = \sum_{m\in M} f(r_m)\cdot g(m) = \sum_{m\in M} h'(r_m)\cdot h'(m) = h(s).$$

Existenz: Jedes $s \in S$ schreibt sich eindeutig als $s = \sum_{m\in M} r_m \cdot m$, also können wir $h(s) := \sum_{m\in M} f(r_m)\cdot g(m)$ in S' definieren. Aus den oben bemerkten Rechenregeln (3G4) folgt, dass die Abbildung $h \colon S \to S'$ ein Ringhomomorphismus ist. □

Korollar 3G6. *Je zwei Monoidringe S,S' von M über R sind kanonisch isomorph.*

Die Idee ist folgende: Die eindeutige Schreibweise als Linearkombination (3) stiftet eine Bijektion $\varphi \colon S \xrightarrow{\sim} S'$. Aus den Bedingungen (1) und (2) folgen die obigen Rechenregeln sowohl für S als auch für S', also ist φ ein Isomorphismus. Formal folgt der Beweis leicht aus der universellen Eigenschaft des vorigen Satzes und ist ein weiteres Beispiel für "abstract general nonsense" der Kategorientheorie:

BEWEIS. Sind S,S' zwei Monoidringe von M über R, dann existiert nach obigem Satz genau ein Ringhomomorphismus $h \colon S \to S'$ mit $h|_R = \mathrm{id}_R$ und $h|_M = \mathrm{id}_M$.



Umgekehrt existiert genau ein Ringhomomorphismus $h' \colon S' \to S$ mit $h'|_R = \mathrm{id}_R$ und $h'|_M = \mathrm{id}_M$. Die Komposition $h' \circ h \colon S \to S$ ist ein Ringhomomorphismus mit $(h'\circ h)|_R = \mathrm{id}_R$ und $(h'\circ h)|_M = \mathrm{id}_M$, also folgt aus der Eindeutigkeitsaussage $h' \circ h = \mathrm{id}_S$. Ebenso folgt $h \circ h' = \mathrm{id}_{S'}$. Damit sind h und h' die gesuchten Isomorphismen zwischen den Ringen S und S'. □

§**3Gd. Konstruktion.** Man kann viel definieren, aber es bleibt die Existenz nachzuweisen. Anders als die Eindeutigkeit verlangt die Existenz eine explizite Konstruktion:

Satz 3G7. *Zu jedem kommutativen Ring R und Monoid M existiert ein Monoidring von M über R.*

BEWEIS. Wir betrachten die Menge $S = R^{(M)}$ aller Abbildungen $M \to R$ mit endlichem Träger. Diese ist eine abelsche Gruppe bezüglich punktweiser Addition (2D29): für $f,g \colon M \to R$ definieren wir $f+g \colon M \to R$ durch

$$(f+g)(m) = f(m)+g(m) \tag{3.5}$$

für alle $m \in M$. Das Produkt $f \cdot g \colon M \to R$ definieren wir durch die Faltung

$$(f \cdot g)(m) = \sum_{\substack{a,b \in M \\ ab=m}} f(a)g(b). \tag{3.6}$$

Diese Summe ist endlich, denn f und g haben endliche Träger. Auch ihr Produkt $f \cdot g$ hat daher nur endlichen Träger. Damit wird $(S, +, \cdot)$ zu einem Ring. Die Distributivgesetze rechnet man problemlos nach. Wir zeigen die Assoziativität der Multiplikation:

$$((f \cdot g) \cdot h)(m) = \sum_{\substack{x,y \in M \\ xy=m}} (f \cdot g)(x)h(y) = \sum_{\substack{x,y \in M \\ xy=m}} \Big[\sum_{\substack{a,b \in M \\ ab=x}} f(a)g(b) \Big] h(y) = \sum_{\substack{a,b,c \in M \\ abc=m}} [f(a)g(b)]h(c),$$
$$(f \cdot (g \cdot h))(m) = \sum_{\substack{x,y \in M \\ xy=m}} f(x)(g \cdot h)(y) = \sum_{\substack{x,y \in M \\ xy=m}} f(x) \Big[\sum_{\substack{b,c \in M \\ bc=y}} g(b)h(c) \Big] = \sum_{\substack{a,b,c \in M \\ abc=m}} f(a)[g(b)h(c)].$$

Für $m \in M$ sei $\delta_m \colon M \to R$ definiert durch $\delta_m(m) = 1$ und $\delta_m(m') = 0$ für alle $m' \neq m$. Ist $e \in M$ das neutrale Element des Monoids $(M, \cdot)$, dann ist δ_e das neutrale Element in $(S, \cdot)$:

$$(\delta_e \cdot f)(m) = \sum_{\substack{a,b \in M \\ ab=m}} \delta_e(a) f(b) = f(m), \qquad (f \cdot \delta_e)(m) = \sum_{\substack{a,b \in M \\ ab=m}} f(a)\delta_e(b) = f(m).$$

Ebenso sieht man, dass $\delta_a \cdot \delta_b = \delta_{ab}$ für alle $a, b \in M$ gilt. Demnach ist $M \to R$, $m \mapsto \delta_m$, ein Isomorphismus des Monoids M auf das Untermonoid $\{\, \delta_m \mid m \in M \,\}$ in S. Wir können somit M mit diesem Untermonoid in S identifizieren.

Wir definieren die Operation $\cdot \colon R \times S \to S$ durch $(r \cdot s)(m) = r \cdot s(m)$ für alle $m \in M$. Für $r, r' \in R$ gilt $r\delta_e + r'\delta_e = (r + r')\delta_e$ und $(r\delta_e) \cdot (r'\delta_e) = (rr')\delta_e$. Demnach ist $R \to S$, $r \mapsto r\delta_e$, ein Isomorphismus des Rings R auf den Unterring $\{\, r\delta_e \mid r \in R \,\}$. Somit können wir R mit diesem Unterring in S identifizieren. Nach obiger Definition der Multiplikation liegt $r\delta_e$ im Zentrum von S. Jedes Element $s \in S$ schreibt sich eindeutig als Linearkombination $s = \sum_{m \in M} s_m \cdot \delta_m$. Damit erfüllt S die Forderungen eines Monoidrings von M über R. □

Bemerkung 3G8. Wir wissen nun, dass zu jedem kommutativen Ring R und jedem Monoid M ein Monoidring existiert, und zwar bis auf eindeutige Isomorphie genau einer. Dies rechtfertigt, von *dem* Monoidring von M über R zu sprechen. Diesen Ring bezeichnen wir mit RM oder $R[M]$. Ist G eine Gruppe, so nennen wir RG den *Gruppenring* von G über R.

Korollar 3G9. *Seien M, N zwei Monoide und seien RM, RN die Monoidringe über R. Dann setzt sich jeder Monoidhomomorphismus $h \colon M \to N$ zu genau einem Ringhomomorphismus $f \colon RM \to RN$ mit $f|_R = \mathrm{id}_R$ und $f|_M = h$ fort.*

Als einfachen aber wichtigen Spezialfall halten wir fest:

Korollar 3G10. *Für das triviale Monoid $N = \{1\}$ gilt $RN = R$ und wir erhalten somit den Ringhomomorphismus $\varepsilon \colon RM \to R$ mit $m \mapsto 1$ für alle $m \in M$, also $\varepsilon(\sum_{m \in M} s_m \cdot m) = \sum_{m \in M} s_m$. Dieser wird die* Augmentation *des Monoidrings RM über R genannt.*

Notation. Die obige Schreibweise geht von einem multiplikativ geschriebenen Monoid $(M, \cdot)$ aus. Ist $(A, +)$ ein additiv geschriebenes Monoid, dann können wir dies auch multiplikativ schreiben als $M = \{\, X^a \mid a \in A \}$ mit der Multiplikation $X^a \cdot X^b = X^{a+b}$. Hierbei ist X nur ein Symbol um $a \in A$ und $X^a \in M$ zu unterscheiden, und $A \to M$, $a \mapsto X^a$, ist

ein Monoidisomorphismus. Der Monoidring $RM = R\{\, X^a \mid a \in A \,\}$ besteht dann aus allen endlichen Summen $\sum_{a\in A} r_a X^a$ und es gilt die vertraute Schreibweise

$$\big(\sum_{a\in A} r_a X^a\big)\big(\sum_{b\in A} r'_b X^b\big) = \sum_{a,b\in A} (r_a r'_b) X^{a+b}.$$

Beispiel 3G11. Für das Monoid $(\mathbb{N},+)$ erhalten wir den Ring der *Polynome*

$$R[X] := R\{\, X^n \mid n \in \mathbb{N} \,\}.$$

Für das Monoid $(\mathbb{N}^d,+)$ erhalten wir den Ring der Polynome in d Variablen

$$R[X_1,\dots,X_d] := R\{\, X_1^{\nu_1}\cdots X_d^{\nu_d} \mid \nu \in \mathbb{N}^d \,\}.$$

Jedes Element $P \in R[X_1,\dots,X_d]^*$ schreibt sich eindeutig als $P = \sum_{\nu\in\mathbb{N}^d} c_\nu X_1^{\nu_1}\cdots X_d^{\nu_d}$ mit Koeffizienten $c_\nu \in R$, wobei wie immer $c_\nu \neq 0$ nur für endlich viele $\nu \in \mathbb{N}^d$ gilt.

Proposition 3G12. *Es gilt* $R[X_1,\dots,X_{d-1},X_d] = R[X_1,\dots,X_{d-1}][X_d]$.

BEWEIS. Wir haben zu zeigen:

(1) Der Ring $R[X_1,\dots,X_{d-1}]$ ist ein Unterring im Zentrum von $R[X_1,\dots,X_d]$.
(2) Das Monoid $\{\, X_d^n \mid n \in \mathbb{N} \,\}$ ist ein Untermonoid von $(R[X_1,\dots,X_d],\cdot)$.
(3) Jedes Element $P \in R[X_1,\dots,X_d]$ schreibt sich eindeutig als $P = \sum_{n=0}^\infty f_n X_d^n$, wobei $f_n \neq 0$ nur für endliche viele n gilt.

Bedingungen (1) und (2) sind offenbar erfüllt; (3) sieht man wie folgt. Sei $P \in R[X_1,\dots,X_d]$, also $P = \sum_{\nu\in\mathbb{N}^d} c_\nu X_1^{\nu_1}\cdots X_d^{\nu_d}$ (mit endlichem Träger). Wir fassen alle Terme mit dem Faktor X_d^n zusammen in $P_n = \sum_{\nu\in\mathbb{N}^d,\nu_d=n} c_\nu X_1^{\nu_1}\cdots X_d^{\nu_d}$ (mit endlichem Träger) und erhalten $P = \sum_{n=0}^\infty P_n$ (mit endlichem Träger). Nun gilt $P_n = f_n X_d^n$ mit $f_n \in R[X_1,\dots,X_{d-1}]$, also $P = \sum_{n=0}^\infty f_n X_d^n$ (mit endlichem Träger) und diese Darstellung ist eindeutig. □

Beispiel 3G13. Für die abelsche Gruppe $(\mathbb{Z},+)$ erhalten wir den Ring der *Laurent-Polynome*

$$R[X^{\pm 1}] := R\{\, X^k \mid k \in \mathbb{Z} \,\}.$$

Jedes Laurent-Polynom schreibt sich $a_m X^m + \cdots + a_n X^n$, wobei $m \le n$ in $\mathbb{Z}$ und Koeffizienten $a_m,\dots,a_n \in R$, und diese Schreibweise ist eindeutig bis auf Nullterme.

Beispiel 3G14. Wir betrachten das additive Monoid $(\mathbb{Q}_{\ge 0},+)$, multiplikativ geschrieben als $M = \{X^a \mid a \in \mathbb{Q}_{\ge 0}\}$ mit $X^a \cdot X^b = X^{a+b}$, sodass $(\mathbb{Q}_{\ge 0},+) \to (M,\cdot)$ mit $a \mapsto X^a$ ein Monoidisomorphismus ist. Als Monoidring erhalten wir den Ring der *Puiseux-Polynome*

$$RM = R\{\, X^r \mid r \in \mathbb{Q}_{\ge 0} \,\}.$$

Jedes Puiseux-Polynom schreibt sich eindeutig als eine Summe $a_1 X^{e_1} + \cdots + a_n X^{e_n}$ der Länge $n \in \mathbb{N}$ mit Koeffizienten $a_1,\dots,a_n \in R^*$ und Exponenten $0 \le e_1 < \cdots < e_n$ in $\mathbb{Q}$.

Beispiel 3G15. Sei $\mathscr{X} = \{X_1,\dots,X_d\}$ eine d-elementige Menge und $\mathscr{X}^*$ das freie Monoid über $\mathscr{X}$ (§2Ha). Dieses besteht aus allen endlichen Wörtern über dem Alphabet $\mathscr{X}$ mit der Aneinanderhängung als Verknüpfung und dem leeren Wort als neutralem Element. Der Monoidring $R\mathscr{X}^*$ ist der Polynomring in den nicht-kommutierenden Variablen $X_1,\dots,X_d$.

§3H. Übungen und Ergänzungen

§3Ha. Hinzufügen eines Einselements. Zu einem Ring $(R,+,\cdot)$ ohne Eins wollen wir einen Ring $(\bar{R},+,\cdot)$ mit einem Einselement 1 konstruieren. Dieser enthält dann $n1$ für alle $n \in \mathbb{Z}$. Angenommen $R \subset \bar{R}$, dann lässt sich für Elemente $m1+a$ und $n1+b$ mit $m,n \in Z$ und $a,b \in R$ das Produkt ausrechnen gemäß $(m1+a)(n1+b) = mn1+(mb+na+ab)$.

Diese Beobachtung nutzen wir nun zur Konstruktion. Wir setzen $\bar{R} = \mathbb{Z} \times R$.

- Mit komponentenweiser Addition ist $(\bar{R},+)$ eine abelsche Gruppe.
- Als Multiplikation definieren wir $(m,a)\cdot(n,b) = (mn, mb+na+ab)$.

Übung 3H1. Zeigen Sie, dass $(\bar{R},+,\cdot)$ ein Ring mit Eins ist, und dass R mittels der Identifikation $a \mapsto (0,a)$ ein Unterring ist. Ist R kommutativ, dann ist auch $\bar{R}$ kommutativ.

Übung 3H2. Der zu einem Ring R ohne Eins so konstrierte Ring $\bar{R}$ mit Eins erfreut sich folgender universeller Eigenschaft: für jeden Homomorphismus $f\colon R \to S$ in einen Ring S mit Eins existiert genau ein Ringhomomorphismus $\bar{f}\colon \bar{R} \to S$, der $\bar{f}|_R = f$ erfüllt. Diese Eigenschaft charakterisiert den Ring $\bar{R}$ bis auf eindeutige Isomorphie.

§3Hb. Mengenoperationen. Sei E eine Menge und $M = \mathfrak{P}E$ ihre Potenzmenge. Die Vereinigung definiert eine Abbildung $\cup\colon M \times M \to M$ durch $(A,B) \mapsto A \cup B$.

Diese Verknüpfung ist kommutativ und assoziativ, das heißt es gilt

$$A \cup B = B \cup A \quad \text{und} \quad (A \cup B) \cup C = A \cup (B \cup C)$$

für alle $A,B,C \in M$. Die leere Menge fungiert für die Vereinigung als neutrales Element, das heißt $A \cup \emptyset = \emptyset \cup A = A$. Die so entstehende Struktur $(M,\cup)$ ist ein *Monoid*.

Analog hierzu definiert der Durchschnitt eine Abbildung $\cap\colon M \times M \to M$ durch $(A,B) \mapsto A \cap B$. Auch diese Verknüpfung ist kommutativ und assoziativ, das heißt es gilt

$$A \cap B = B \cap A \quad \text{und} \quad (A \cap B) \cap C = A \cap (B \cap C)$$

für alle $A,B,C \in M$. Die Gesamtmenge E fungiert für den Durchschnitt als neutrales Element $A \cup E = E \cup A = A$. Die so entstehende Struktur $(M,\cap)$ ist ein *Monoid*.

Der Durchschnitt ist distributiv über die Vereinigung, das heißt

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Die so entstehende Struktur $(M,\cup,\cap)$ ist ein Beispiel eines *Halbrings*.

Umgekehrt ist auch die Vereinigung distributiv über den Durchschnitt, das heißt

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Damit ist auch $(M,\cap,\cup)$ ein Halbring. Sind diese beiden Halbringe isomorph?

Die Komplementabbildung $\complement A\colon M \to M$ ist definiert durch $\complement A = E \smallsetminus A$. Offenbar gilt $\complement\emptyset = E$ und $\complement E = \emptyset$. Weiterhin gelten die Regeln $\complement(A \cup B) = \complement A \cap \complement B$ und $\complement(A \cap B) = \complement A \cup \complement B$. Diese Abbildung definiert also einen Isomorphismus $\complement\colon (M,\cup,\cap) \xrightarrow{\sim} (M,\cap,\cup)$.

Neben Vereinigung und Durchschnitt zweier Mengen $A,B \subset E$ betrachten wir auch die *symmetrische Differenz* $A \triangle B = (A \smallsetminus B) \cup (B \smallsetminus A)$.

Auch diese Verknüpfung ist *kommutativ*, das heißt $A \triangle B = B \triangle A$, und *assoziativ*, das heißt $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ für alle $A,B,C \in M$. Die leere Menge fungiert als *neutrales*

Element $A \cup \emptyset = \emptyset \cup A = A$. Interessanterweise erlaubt jede Menge A ein *Inverse*, genauer gesagt gilt $A \triangle A = \emptyset$. Die so entstehende Struktur $(M, \triangle)$ ist eine *Gruppe*.

Der Durchschnitt ist distributiv über die symmetrische Differenz, das heißt es gilt $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$. Die so entstehende Struktur $(M, \triangle, \cap)$ ist demnach ein *Ring*.

Übung 3H3. Der Ring $(M, \triangle, \cap)$ ist isomorph zum Ring $((\mathbb{Z}/_2)^E, +, \cdot)$.

§**3Hc. Gruppenringe.** Da Gruppen in der Mathematik eine wichtige Rolle spielen, erfreuen sich auch Gruppenringe großer Beliebheit. Hier eine leichte Frage, um sich im Umgang mit ihnen zu üben:

Übung 3H4. Sei R ein Integritätsring und G eine Gruppe. Wenn es ein Element $g \in G$ endlicher Ordnung gibt, also $g \neq 1$ aber $g^n = 1$ für ein $n \geq 1$, dann hat der Gruppenring $R[G]$ Nullteiler. *Hinweis:* endliche geometrische Reihe.

Eine berühmte Vermutung von Kaplansky fragt nach der Umkehrung: Wenn eine Gruppe G keine Elemente endlicher Ordnung hat, dann hat der Gruppenring $R[G]$ über einem Integritätsring R keine Nullteiler. Diese Vermutung ist bis heute offen.

Übung 3H5. Gibt es Nullteiler im Gruppenring $R[\mathbb{Z}]$ der Gruppe $(\mathbb{Z}, +)$ über einem Integritätsring R? (Dies ist der Ring der Lauent-Polynome aus Beispiel 3G13.) Man bestimme die Gruppe $R[\mathbb{Z}]^\times$ der invertierbaren Elemente.

§**3Hd. Potenzreihenringe.** In der Konstruktion des Monoidrings RM eines Monoids M über einem Ring R (§3G) haben wir Abbildungen $f, g\colon M \to R$ mit endlichem Träger betrachtet. Für die Summe (3.5) ist diese Bedingung unerheblich, aber für das Produkt (3.6) ist sie wesentlich. Für bestimmte Monoide können wir diese Einschränkung fallen lassen und dennoch das Produkt in der gewohnten Weise definieren:

Definition 3H6. Wir sagen in einem Monoid $(M, \cdot)$ gilt *endliche Zerlegbarkeit* wenn zu jedem $m \in M$ nur endlich viele Paare $(a, b) \in M \times M$ existieren, die $ab = m$ erfüllen

Beispiel 3H7.
- In $(\mathbb{N}, +)$ gilt endliche Zerlegbarkeit, ebenso in $(\mathbb{N}^d, +)$.
- In $(\mathbb{Z}, +)$ und $(\mathbb{Q}_{\geq 0}, +)$ gilt endliche Zerlegbarkeit hingegen nicht.

Sei R ein kommutativer Ring und M ein Monoid, in dem endliche Zerlegbarkeit gilt. Auf der Menge $S = R^M$ aller Abbildungen $f, g\colon M \to R$ definieren wir die Summe $f + g$ punktweise und das Produkt $f \cdot g$ durch Faltung:

$$(f+g)(m) = f(m) + g(m) \qquad \text{und} \qquad (f \cdot g)(m) = \sum_{\substack{a,b \in M \\ ab = m}} f(a) g(b)$$

Übung 3H8. Man weise nach, dass $(S, +, \cdot)$ ein Ring ist.
Der Ring S ist genau dann kommutativ wenn das Monoid M kommutativ ist

Beispiel 3H9. Wir wollen die Konstruktion im Falle des Monoids $(\mathbb{N}, +)$ illustrieren. Hier betrachten wir Abbildungen $F\colon \mathbb{N} \to R$, die wir uns als unendliche Summen $F = \sum_{k=0}^{\infty} f_k X^k$ mit Koeffizienten $f_k = F(k)$ vorstellen. Hier hat das Summenzeichen $\sum$ zunächst nur einen symbolischen Sinn: algebraisch können wir nur Summen für endlich viele Terme definieren.

Wir können allerdings einer unendlichen Summe $\sum_{k=0}^{\infty} F_k$ einen Sinn geben, wenn sie lokal-endlich ist: Hierzu seien $F_0, F_1, F_2, \ldots : \mathbb{N} \to R$ Abbildungen, sodass es für jedes $n \in \mathbb{N}$

nur endlich viele Indizes k gibt, für die $F_k(n) \neq 0$ gilt. Dann können wir die Summe $F = \sum_{k=0}^{\infty} F_k$ gradweise definieren durch $F(n) = \sum_{k=0}^{\infty} F_k(n)$. Mit $X^k = \delta_k$ schreibt sich dann jede Funktion $F : \mathbb{N} \to R$ tatsächlich als eine lokal-endliche Summe $F = \sum_{k=0}^{\infty} f_k X^k$.

Für Summe und Produkt gilt in dieser Schreibweise

$$\Big(\sum_{k=0}^{\infty} f_k X^k\Big) + \Big(\sum_{k=0}^{\infty} g_k X^k\Big) = \sum_{k=0}^{\infty} (f_k + g_k) X^k$$

$$\Big(\sum_{k=0}^{\infty} f_k X^k\Big) \cdot \Big(\sum_{\ell=0}^{\infty} g_\ell X^\ell\Big) = \sum_{n=0}^{\infty} \Big(\sum_{k+\ell=n} f_k g_\ell\Big) X^n$$

Den so entstehenden Ring $R[[X]]$ nennt man den Ring der *Potenzreihen* über R. Zur Betonung spricht man auch von *formalen Potenzreihen*, denn anders als in der Analysis umgehen wir hier alle Fragen der Konvergenz: Diese Potenzreihen sind nur formale Ausdrücke und beschreiben nicht etwa Funktionen. Wichtig ist allein, dass sie einen Ring bilden.

Übung 3H10. Wenn R ein Integritätsring ist, ist dann auch $R[[X]]$ ein Integritätsring?

Übung 3H11. Für jedes $n \in \mathbb{N}$ ist $\mathfrak{m}^n = \{ \sum_{k=n}^{\infty} f_k X^k \mid f_k \in R\}$ ein Ideal in $R[[X]]$.
Es gilt $\mathfrak{m}^0 = R[[X]]$ sowie $\mathfrak{m}^k + \mathfrak{m}^\ell = \mathfrak{m}^{\min(k,\ell)}$ und $\mathfrak{m}^k \cap \mathfrak{m}^\ell = \mathfrak{m}^{\max(k,\ell)}$ und $\mathfrak{m}^k \mathfrak{m}^\ell = \mathfrak{m}^{k+\ell}$.

Übung 3H12. Wir haben einen injektiven Ringhomomorphismen $\iota : R \to R[[X]]$, $a \mapsto aX^0$, und einen surjektiven Ringhomomorphismus $\varepsilon : R[[X]] \to R$, $\sum_{k=0}^{\infty} f_k X^k \mapsto f_0$, mit $\ker \varepsilon = \mathfrak{m}$.

Übung 3H13. In $R[[X]]$ ist $1 - X$ invertierbar mit $(1-X)^{-1} = 1 + X + X^2 + \ldots$.
Man bestimme die Gruppe $R[[X]]^\times$ der invertierbaren Elemente in $R[[X]]$.

Übung 3H14. Ist R ein Körper, so sind $\mathfrak{m}^0, \mathfrak{m}^1, \mathfrak{m}^2, \ldots, \{0\}$ die einzigen Ideale in $R[[X]]$.

KAPITEL 4

Polynomringe

Das vorangegangene Kapitel hat den Ringbegriff eingeführt und mehrere Konstruktionen vorgestellt, wie man neue Ringe aus alten gewinnen kann. In diesem Kapitel betrachten wir einen wichtigen Spezialfall dieser Konstruktionen: den Polynomring $K[X]$ über einem kommutativen Ring K, der für das Folgende eine wesentliche Rolle spielen wird.

Konvention. In diesem Kapitel betrachten wir ausschließlich kommutative Ringe soweit nichts Gegenteiliges angegeben wird.

§4A. Definition und universelle Eigenschaft

Den Polynomring $K[X]$ über einem kommutativen Ring K haben wir bereits am Ende des letzten Kapitels kennengelernt, als Beispiel eines Monoidrings KM, wobei das multiplikativ geschriebene Monoid $(M,\cdot)$ mit $M = \{\, X^n \mid n \in \mathbb{N} \,\}$ isomorph zu $(\mathbb{N},+)$ ist. In diesem Spezialfall können wir die Definition des Monoidrings KM wie folgt umformulieren:

Definition 4A1. Sei K ein kommutativer Ring. Ein kommutativer Ring R heißt *Polynomring* in der Variablen X über K, wenn folgendes gilt:

- Der Ring R enthält K als Unterring und X als Element.
- Jedes Element $P \in R$ mit $P \neq 0$ schreibt sich eindeutig als

$$P = a_0 + a_1 X + \cdots + a_n X^n \quad \text{wobei} \quad n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in K,\ a_n \neq 0.$$

In diesem Fall nennen wir P ein *Polynom* in X über K und definieren seinen *Grad* $\deg P := n$ und *Leitkoeffizient* $\operatorname{lc} P := a_n$. Für das Nullpolynom 0 setzen wir $\deg 0 := -\infty$ und $\operatorname{lc} 0 := 0$.

Für den Nullring $K = \{0\}$ besteht $K[X]$ nur aus dem Nullpolynom. Erfüllt K hingegen $1 \neq 0$, so gilt dies wegen $K \subset K[X]$ auch für den Polynomring $K[X]$ über K.

Bemerkung 4A2. Jedes Polynom können wir ebenso schreiben als Summe der Form

$$P = \sum_{k=0}^{\infty} a_k X^k$$

mit der Vereinbarung, dass nur endlich viele Koeffizienten von 0 verschieden sind. Das hat den Vorteil, den Grad nicht explizit angeben zu müssen. In dieser Schreibweise gilt dann

$$\deg P = \sup\{\, k \in \mathbb{N} \mid a_k \neq 0 \,\}$$

mit der üblichen Konvention $\sup \emptyset = -\infty$.

Aus der Definition folgt, dass jedes Polynom seine Koeffizienten eindeutig bestimmt:

$$\sum_{k=0}^{\infty} a_k X^k = \sum_{k=0}^{\infty} b_k X^k \quad \Longleftrightarrow \quad a_k = b_k \text{ für alle } k \in \mathbb{N}.$$

Zudem legt die obige Definition des Polynomrings fest, wie Summe und Produkt zu berechnen sind. Aus Axiomen eines kommutativen Rings folgt nämlich

$$\left(\sum_{k=0}^{\infty} a_k X^k\right) + \left(\sum_{k=0}^{\infty} b_k X^k\right) = \sum_{k=0}^{\infty} (a_k + b_k) X^k,$$
$$\left(\sum_{i=0}^{\infty} a_i X^i\right) \cdot \left(\sum_{j=0}^{\infty} b_j X^j\right) = \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j\right) X^k.$$

§4Aa. Universelle Eigenschaft.

Satz 4A3. *Für jeden kommutativen Ring K existiert ein Polynomring, nämlich der Monoidring KM über dem freien Monoid $M = \{X\}^* = \{ X^n \mid n \in \mathbb{N} \}$. Dieser Ring ist durch die Definition 4A1 bis auf Isomorphie eindeutig festgelegt.* □

Dies rechtfertigt, von *dem* Polynomring in X über K zu sprechen; wir bezeichnen diesen Ring mit $K[X]$. Seine universelle Eigenschaft formulieren wir zur Betonung erneut aus:

Satz 4A4. *Sei $\varphi\colon K \to R$ ein Homomorphismus zwischen kommutativen Ringen K und R. Zu jedem Element $x \in R$ existiert genau einen Ringhomomorphismus $\tilde{\varphi}\colon K[X] \to R$ mit $\tilde{\varphi}|_K = \varphi$ und $\tilde{\varphi}(X) = x$. Dieser ist gegeben durch*

$$\tilde{\varphi}(a_0 + a_1 X + \cdots + a_n X^n) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n.$$

Diese Situation wird durch das folgende kommutative Diagramm dargestellt:

$$\begin{array}{ccc} K[X], X & \overset{\exists!\tilde{\varphi}}{\dashrightarrow} & R, x \\ \text{inc.}\uparrow & & \uparrow\text{inc.} \\ K & \xrightarrow[\varphi]{} & R \end{array}$$

BEWEIS. Eindeutigkeit und Existenz rechnet man direkt nach. Abstrakt betrachtet steht alles Notwendige schon bereit: Der Satz folgt unmittelbar aus der universellen Eigenschaft des freien Monoids $M = \{ X^n \mid n \in \mathbb{N} \}$ (2C19) kombiniert mit der universellen Eigenschaft des Monoidrings $K[X] = KM$ von M über K (3G5). □

Notation. Im Falle $K = R$ und $\varphi = \mathrm{id}_K$, oder allgemeiner, wenn $K \subset R$ ein Teilring und $\varphi\colon K \hookrightarrow R$ die Inklusion ist, schreiben wir kurz $P(x)$ für $\tilde{\varphi}(P)$. Man ersetzt also die Variable $X \in K[X]$ durch den Wert $x \in R$: Aus dem Polynom $P = a_0 + a_1 X + \cdots + a_n X^n$ in $K[X]$ erhält man so das Element $a_0 + a_1 x + \cdots + a_n x^n$ in R. Dass das Ergebnis wohldefiniert ist, verdanken wir der Definition 4A1 des Polynomrings $K[X]$. Die so definierte Abbildung $K[X] \to R$ mit $P \mapsto P(x)$ nennt man auch *Einsetzungshomomorphismus*.

§**4Ab. Einfache Erweiterungen.** Die folgende Beobachtung wird uns in der Galois-Theorie gute Dienste leisten:

Definition 4A5. Ist K ein kommutativer Ring und $E \supset K$ ein kommutativer Oberring, dann nennen wir E eine *Erweiterung* von K. Wird E von einem Element $x \in E$ über K erzeugt, gilt also $E = K[x]$, dann nennt man E eine *einfache Erweiterung* von K.

Zum Beispiel ist der Polynomring $K[X]$ in der Variablen X über K eine einfache Erweiterung. Dies ist die universelle einfache Erweiterung: Zu jeder einfachen Erweiterung $E = K[x]$ gibt genau einen Ringhomomorphismus $f\colon K[X] \to E$ mit $X \mapsto x$. Dieser Ringhomomorphismus ist surjektiv, daher gilt $K[X]/\ker(f) \cong E$ nach Satz 3D19.

§**4Ac. Polynome versus polynomielle Abbildungen.** Wir erinnern daran, dass für jeden Ring K die Menge K^X aller Abbildungen $X \to K$ ein Ring ist bezüglich punktweiser Addition und Multiplikation. Daraus ersehen wir folgenden Zusammenhang:

Korollar 4A6. *Jedes Polynom $P \in K[X]$ definiert eine Abbildung $f_P\colon K \to K$ durch $f_P(x) = P(x)$ für alle $x \in K$. Für jedes $a \in K$ ist $f_a = a$ die konstante Abbildung mit Wert a, und $f_X = \mathrm{id}_K$ ist die Identität. Zudem gilt*

$$f_{P+Q} = f_P + f_Q \quad \textit{und} \quad f_{P\cdot Q} = f_P \cdot f_Q.$$

Dies definiert einen Ringhomomorphismus $K[X] \to K^K$, $P \mapsto f_P$, mit $X \mapsto \mathrm{id}_K$. □

Bemerkung 4A7. Der Fall der reellen Zahlen $K = \mathbb{R}$ lässt die Angewohnheit entstehen, jedes Polynom $P \in \mathbb{R}[X]$ mit seiner polynomiellen Abbildung $f_P\colon \mathbb{R} \to \mathbb{R}$ zu identifizieren. Das ist allerdings nur zulässig, solange die Zuordnung $P \mapsto f_P$ injektiv ist. Für unendliche Körper wie $\mathbb{R}$ werden dies später beweisen. Für endliche Körper gilt dies jedoch nicht:

Beispiel 4A8. Wir betrachten den Körper $\mathbb{Z}/_p$ mit p Elementen, wobei $p \geq 2$ eine Primzahl ist. Im Polynomring $\mathbb{Z}/_p[X]$ betrachten wir das Polynom $P = X^p - X$. Es gilt $P \neq 0$ aber dennoch $f_P = f_0$ nach dem kleinen Satz von Fermat (3D28). Alternativ kann man dies für kleine Werte $p = 2, 3, 5, \ldots$ auch direkt nachrechnen.

§4B. Gradfunktion und euklidische Division

§**4Ba. Eigenschaften des Grades.** Es sei weiterhin K ein kommutativer Ring.

Proposition 4B1. *Der Grad* $\deg\colon K[X] \to \mathbb{N} \cup \{-\infty\}$ *erfreut sich folgender Eigenschaften:*

(a) Für alle $P, Q \in K[X]$ gilt $\deg(P+Q) \leq \sup\{\deg P, \deg Q\}$.
Gleichheit gilt genau dann, wenn $\deg P \neq \deg Q$ *oder* $\mathrm{lc}\, P + \mathrm{lc}\, Q \neq 0$.

(b) Für alle $P, Q \in K[X]$ gilt $\deg(PQ) \leq \deg P + \deg Q$.
Gleichheit gilt genau dann, wenn $P = 0$ oder $Q = 0$ oder $\mathrm{lc}\, P \cdot \mathrm{lc}\, Q \neq 0$.
In diesem Fall gilt für die Leitkoeffizienten $\mathrm{lc}(PQ) = \mathrm{lc}\, P \cdot \mathrm{lc}\, Q$.

BEWEIS. Dies folgt aus den Formeln für Summe und Produkt in Bemerkung 4A2. □

Beispiel 4B2. Wider Erwarten gilt nicht immer $\deg(PQ) = \deg P + \deg Q$. In $\mathbb{Z}/_6[X]$ zum Beispiel sind $P = \bar{1} + \bar{2}X$ und $Q = \bar{1} + \bar{3}X$ vom Grad 1 aber ihr Produkt

$$PQ = (\bar{1} + \bar{2}X) \cdot (\bar{1} + \bar{3}X) = \bar{1} + \bar{5}X + \bar{6}X^2 = \bar{1} + \bar{5}X$$

ist nur vom Grad 1 und nicht 2. Dies liegt offenbar an der Anwesenheit von Nullteilern:

Korollar 4B3. *Für jeden kommutativen Ring K sind äquivalent*

1. *Der Ring K ist nullteilerfrei.*
2. *Es gilt $\deg(PQ) = \deg P + \deg Q$ für alle $P, Q \in K[X]$.*
3. *Der Polynomring $K[X]$ ist nullteilerfrei.*

BEWEIS. "(1) $\Rightarrow$ (2)" folgt aus den obigen Eigenschaften des Grades (4B1). "(2) $\Rightarrow$ (3)" ebenso: Wenn $P \neq 0$, $Q \neq 0$, dann gilt $\deg P \geq 0$ und $\deg Q \geq 0$, also $\deg(PQ) = \deg P + \deg Q \geq 0$, und somit $PQ \neq 0$. "(3) $\Rightarrow$ (1)" ist klar, denn jeder Unterring eines Integritätsrings ist selbst ein Integritätsring. □

Beispiel 4B4. Wider Erwarten können auch Polynome vom Grad ≥ 1 invertierbar sein. In $\mathbb{Z}/_4[X]$ zum Beispiel ist $P = \bar{1} + \bar{2}X$ invertierbar, denn

$$P \cdot P = (\bar{1} + \bar{2}X) \cdot (\bar{1} + \bar{2}X) = \bar{1} + \bar{4}X + \bar{4}X^2 = \bar{1}.$$

Über einem Integritätsring kann dies nicht passieren:

Korollar 4B5. *Für jeden Integritätsring K gilt $K[X]^\times = K^\times$.*

BEWEIS. Offenbar gilt stets $K^\times \subset K[X]^\times$. Es bleibt $K[X]^\times \subset K^\times$ zu zeigen: Gilt $PQ = 1$ mit $P, Q \in K[X]$, dann folgt $0 = \deg 1 = \deg(PQ) = \deg P + \deg Q$, also $\deg P = \deg Q = 0$, da K nach Voraussetzung ein Integritätsring ist. Das bedeutet $P, Q \in K$, also $P, Q \in K^\times$. □

§**4Bb. Division mit Rest.** Es sei weiterhin K ein kommutativer Ring. Die folgende Definition präzisiert, was wir unter der *Division mit Rest* von Polynomen verstehen, auch *euklidische Division* genannt. Hierzu zunächst der grundlegende Satz:

Satz 4B6. *Sei $P \in K[X]$ ein Polynom mit invertierbarem Leitkoeffizienten $\operatorname{lc} P \in K^\times$. Dann existiert zu jedem Polynom $S \in K[X]$ genau ein Paar $Q, R \in K[X]$, für das gilt*

$$S = PQ + R \quad \textit{und} \quad \deg R < \deg P.$$

Definition 4B7. In diesem Fall nennt man $S \operatorname{quo} P := Q$ den *Quotienten* und $S \operatorname{rem} P := R$ den *Rest* der euklidischen Division von S durch P (auf Englisch *quotient* und *remainder*).

BEWEIS. *Eindeutigkeit:* Gilt $S = PQ + R = PQ' + R'$ und $\deg R, \deg R' < \deg P$, dann folgt $P(Q - Q') = R' - R$. Wegen $\operatorname{lc} P \in R^\times$ gilt

$$\deg P + \deg(Q - Q') = \deg[P(Q - Q')] = \deg(R - R') < \deg P.$$

Dies ist nur für $\deg(Q - Q') < 0$ möglich, also $Q - Q' = 0$. Daraus folgt $Q = Q'$ und $R = R'$.

Existenz: Wenn $\deg S < \deg P$, dann genügen $Q = 0$ und $R = S$. Für $\deg S \geq \deg P$ führen wir Induktion über $\deg S$. Wir nehmen an, die Aussage gelte für alle $\tilde{S} \in K[X]$ mit $\deg \tilde{S} < \deg S$. Wir setzen $M = \operatorname{lc}(P)^{-1} \operatorname{lc}(S) \cdot X^{\deg S - \deg P} \in K[X]$ und $\tilde{S} = S - PM$. Aus 4B1 folgt $\deg(PM) = \deg S$ und $\operatorname{lc}(PM) = \operatorname{lc} S$, also $\deg \tilde{S} < \deg S$. Nach Induktionsvoraussetzung gibt es $\tilde{Q}, R \in R[X]$ mit $\tilde{S} = P\tilde{Q} + R$ und $\deg R < \deg P$. Daher gilt $S = \tilde{S} + PM = PQ + R$ für $Q = \tilde{Q} + M$. □

Die euklidische Division von Polynomen lässt sich algorithmisch sehr einfach und effizient ausführen. Wir wollen dies zur Ergänzung explizit ausformulieren. In iterativer Form

führt dies zum untenstehenden Algorithmus 2. Er formalisiert das aus der Schule bekannte Divisionsverfahren.

Algorithmus 2 Division mit Rest von zwei Polynomen

Eingabe: zwei Polynome $S,P \in K[X]$ wobei $\operatorname{lc} P \in K^\times$.
Ausgabe: zwei Polynome $Q,R \in K[X]$ sodass $S = PQ+R$ und $\deg R < \deg P$.

```
Q ← 0;  R ← S                                  // Invariante: S = PQ + R
while deg R ≥ deg P do
  M ← lc(P)^{-1} lc(R) · X^{deg R − deg P}
  Q ← Q + M;  R ← R − PM                       // Invariante: S = PQ + R
end while
return (Q, R)                                  // S = PQ + R und deg R < deg P
```

Proposition 4B8. *Algorithmus 2 ist korrekt.*

BEWEIS. *Der Algorithmus terminiert:* Das Monom M ist so gewählt, dass R und PM denselben Grad und denselben Leitkoeffizienten haben. Also gilt $\deg(R-PM) < \deg R$. Der Algorithmus endet demnach nach höchstens $1+\deg S-\deg P$ Iterationen.

Das Ergebnis erfüllt die geforderten Bedingungen: Die Initialisierung $Q \leftarrow 0$, $R \leftarrow S$ garantiert, dass $S = PQ+R$. Jede Iteration $Q \leftarrow Q+M$, $R \leftarrow R-PM$ erhält diese Gleichung. Zum Schluss gilt also $S = PQ+R$ mit $\deg R < \deg P$, wie gewünscht. □

Man beachte, dass dieser Algorithmus und sein Korrektheitsbeweis erneut die Existenz von $Q,R \in K[X]$ mit $S = PQ+R$ und $\deg R < \deg P$ zeigen; man könnte also obigen Induktionsbeweis durch die iterative Konstruktion ersetzen. Beide sind logisch äquivalent; die erste Form ist in der Mathematik geläufiger, die zweite Form in der Informatik.

§**4Bc. Anwendung auf Quotientenringe.** Für $n \in \mathbb{N}$ sei

$$K[X]_{<n} = \{\, P \in K[X] \mid \deg P < n \,\}$$

die Menge der Polynome mit Grad $< n$. Jedes Polynom $P \in K[X]_{<n}$ schreibt sich demnach eindeutig als $P = a_0 + \cdots + a_{n-1}X^{n-1}$ mit $a_0,\dots,a_{n-1} \in K$. Offenbar gilt $K[X]_{<0} = \{0\}$.

Ebenso definieren wir $K[X]_{\le n} = \{\, P \in K[X] \mid \deg P \le n \,\} = K[X]_{<n+1}$. Man beachte, dass $K[X]_{\le n}$ eine Untergruppe von $(K[X],+)$ ist. Hingegen ist $K[X]_{\le n}$ für $n \ge 1$ kein Unterring von $(K[X],+,\cdot)$, denn $K[X]_{\le n}$ ist nicht abgeschlossen unter Multiplikation.

Korollar 4B9. *Sei $P \in K[X]$ ein Polynom vom Grad $n \in \mathbb{N}$ mit invertierbarem Leitkoeffizient, $\operatorname{lc} P \in K^\times$. Dann ist die Abbildung*

$$K[X]_{<n} \to K[X]/(P) \quad \textit{mit} \quad A \mapsto \mathfrak{cl}(A)$$

eine Bijektion, und sogar ein Gruppenisomorphismus bezüglich der Addition. Dieser wird zu einem Ringisomorphismus wenn wir auf $K[X]_{<n}$ die Multiplikation

$$A \underset{P}{\cdot} B := (A \cdot B) \operatorname{rem} P$$

definieren. Anders gesagt, das Rechnen mit Restklassen $\mathfrak{cl}(A) \in K[X]/(P)$ entspricht dem Rechnen mit Elementen $A \in K[X]$, wobei man stets nur den Rest der Division mit P behält.

BEWEIS. In jeder Äquivalenzklasse $\mathfrak{cl}(S) \in K[X]/(P)$ existiert genau ein Repräsentant $R \in \mathfrak{cl}(S)$ mit $\deg R < \deg P$, nämlich $R = S \operatorname{rem} P$ (der Rest der Division durch P). □

Übung 4B10. Sei $\mathbb{F}_4 := \mathbb{Z}/_2[X]/(X^2+X+1)$.

1. Bestimmen Sie die Anzahl der Elemente von $\mathbb{F}_4$ und zählen sie diese auf.
2. Erstellen Sie die Additions- und Multiplikationstafeln von $\mathbb{F}_4$.
3. Ist der Quotientenring $\mathbb{F}_4$ ein Körper?

Übung 4B11. Sei $P \in \mathbb{Z}/_m[X]$ ein Polynom mit $\deg P = d$ und $\operatorname{lc} P = 1$.

1. Man bestimme die Anzahl der Elemente von $\mathbb{Z}/_m[X]/(P)$.
2. Wenn $\mathbb{Z}/_m[X]/(P)$ ein Körper ist, dann ist m eine Primzahl und das Polynom P ist irreduzibel, das heißt $P = QR$ ist nur mit entweder $Q \in \mathbb{Z}/_m^\times$ oder $R \in \mathbb{Z}/_m^\times$ möglich. (Wir werden später sehen, dass diese Bedingungen auch hinreichend sind.)

Warnung. — Für die besonders einfache Form des Quotienten $K[X]/(P)$ ist die Invertierbarkeit des Leitkoeffizienten, $\operatorname{lc} P \in K^\times$, wesentlich. Andernfalls kann der Quotient sehr viel unübersichtlicher ausfallen. Hier eines der einfachsten Beispiele:

Beispiel 4B12. Im Polynomring $\mathbb{Z}[X]$ betrachten wir $P = kX^n$ mit $k,n \in \mathbb{N}_{\geq 1}$. Jede Restklasse im Quotientenring $\mathbb{Z}[X]/(kX^n)$ hat genau einen Repräsentanten der Form

$$a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \quad + \quad a_nX^n + a_{n+1}X^{n+1} + \ldots$$

wobei $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ sowie $a_n, a_{n+1}, \cdots \in \{0, 1, \ldots, k-1\}$. Die Addition in den ersten n Koeffizienten ist die in $\mathbb{Z}$, die Addition in allen weiteren Koeffizienten entspricht der in $\mathbb{Z}/_k$. Ähnliches gilt für die Multiplikation solcher Restklassen, die wir hier nicht ausschreiben.

§4C. Faktorisierung von Nullstellen

§4Ca. Nullstellen eines Polynoms. Sei K ein kommutativer Ring und $P \in K[X]$ ein Polynom über K. Wir sagen $a \in K$ ist eine *Nullstelle* des Polynoms P, oder eine *Wurzel* der Gleichung $P(X) = 0$, wenn $P(a) = 0$ gilt.

Proposition 4C1. *Ein Element $a \in K$ ist genau dann Nullstelle von $P \in K[X]$ wenn $P = (X-a)Q$ für ein $Q \in K[X]$ gilt. In diesem Fall ist Q eindeutig bestimmt.*

BEWEIS. Es gibt genau ein Paar $Q, R \in K[X]$ so dass $P = (X-a)Q + R$ und $\deg R < \deg(X-a) = 1$, also $R \in K$. Demnach verschwindet $P(a) = R$ genau dann, wenn $R = 0$. Dies ist gleichbedeutend mit $P = (X-a)Q$. □

Korollar 4C2. *Für jedes Polynom $P \in K[X]^*$ und $a \in K$ gibt es genau eine natürliche Zahl $m \in \mathbb{N}$ und genau ein Polynom $Q \in K[X]$ so dass $P = (X-a)^m Q$ mit $Q(a) \neq 0$ gilt.* □

Definition 4C3. Im Falle $m \geq 1$ nennen wir a eine Nullstelle der *Vielfachheit m*.

- Wir nennen a eine *einfache Nullstelle* wenn $m = 1$.
- Wir nennen a eine *mehrfache Nullstelle* wenn $m \geq 2$.

Korollar 4C4. *Jedes Polynom $P \in K[X]^*$ schreibt sich als Produkt*

$$P = (X-a_1)^{m_1} \cdots (X-a_k)^{m_k} Q \tag{4.1}$$

mit paarweise verschiedenen Nullstellen $a_1,\dots,a_k \in K$ und Vielfachheiten $m_1,\dots,m_k \geq 1$ sodass das verbleibende Polynom $Q \in K[X]^*$ keine Nullstellen in K hat.

BEWEIS. Wir führen Induktion über den Grad von P. Wenn $\deg P = 0$, dann hat P keine Nullstellen und $P = Q$ genügt. Wenn $\deg P \geq 1$, dann unterscheiden wir zwei Fälle. Wenn P keine Nullstellen hat, dass genügt $P = Q$; wenn P mindestens eine Nullstelle hat, dann gilt $P = (X-a_1)^{m_1}P^*$ mit $m_1 \geq 1$ und $P^* \in K[X]$ erfüllt $P^*(a_1) \neq 0$ und $0 \leq \deg P^* < \deg P$. Nach Induktionsannahme wissen wir, dass $P^* = (X-a_2)^{m_2}\cdots(X-a_k)^{m_k}Q$ wobei $a_1, a_2, \dots, a_k \in K$ paarweise verschiedenen Nullstellen sind mit $m_1, m_2, \dots, m_k \geq 1$, und $Q \in K[X]$ hat keine Nullstellen in K. Daraus folgt $P = (X-a_1)^{m_1}\cdots(X-a_k)^{m_k}Q$ wie behauptet. □

§**4Cb. Anzahl der Nullstellen.** Wir wollen nun den ebenso einfachen wie wichtigen Zusammenhang herstellen zwischen dem Grad eines Polynoms $P \in K[X]$ und der möglichen Anzahl seiner Nullstellen in K. Ist eine Zerlegung wie in (4.1) gegeben, so hat P *mindestens* die Nullstellen $a_1,\dots,a_k$, und deren Anzahl (mit Vielfachheiten) ist $m_1 + \cdots + m_k \leq n$.

Im allgemeinen ist die Zerlegung (4.1) jedoch *nicht* eindeutig und bedeutet auch nicht, das P nur die angegebenen Nullstellen hat:

Beispiel 4C5. Über $\mathbb{Z}/_8$ erlaubt das Polynom $P = X^2 - \bar{1}$ vier verschiedene Nullstellen, nämlich $\pm\bar{1}$ et $\pm\bar{3}$. Tatsächlich finden wir $P = (X-\bar{1})(X+\bar{1}) = (X-\bar{3})(X+\bar{3})$.

Das Problem liegt offenbar in der Anwesenheit von Nullteilern:

Satz 4C6. *Ist K ein Integritätsring, so ist für jedes Polynom $P \in K[X]^*$ die Zerlegung* (4.1) *eindeutig bis auf die Reihenfolge der Faktoren. Insbesondere kann ein Polynom $P \in K[X]$ vom Grad n höchstens n Nullstellen haben (mit Vielfachheiten gezählt).*

BEWEIS. Wir vergleichen zwei solche Zerlegungen

$$P = (X-a_1)^{m_1}\cdots(X-a_k)^{m_k}Q = (X-b_1)^{n_1}\cdots(X-b_\ell)^{n_\ell}R.$$

Wir wollen zeigen, dass $k = \ell$ gilt und nach Umordnung sowohl $a_1 = b_1, \dots, a_k = b_k$ als auch $m_1 = n_1, \dots, m_k = n_k$. Wir führen dazu Induktion über k. Wenn $k = 0$, dann hat $P = Q$ keine Nullstellen in K und daher gilt auch $\ell = 0$ und $P = R$. Wenn $k \geq 1$, dann folgt aus $P(a_k) = 0$ und der Nullteilerfreiheit von K, dass einer der Faktoren $(a_k - b_1), \dots, (a_k - b\ell)$ gleich 0 sein muss. Nach Umordnung können wir $a_k = b_\ell$ annehmen. Mit 4C2 folgt $m_k = n_\ell$ und $(X-a_1)^{m_1}\cdots(X-a_{k-1})^{m_{k-1}}Q = (X-b_1)^{n_1}\cdots(X-b_{\ell-1})^{n_{\ell-1}}R$. Nach Induktionsannahme folgt dann $k-1 = \ell-1$ und $a_1 = b_1, \dots, a_{k-1} = b_{k-1}$ und $m_1 = n_1, \dots, m_{k-1} = n_{k-1}$.

Ist $a \in K$ eine Nullstelle, also $P(a) = 0$, dann muss $a \in \{a_1,\dots,a_k\}$ gelten. Die Gesamtzahl der Nullstellen, mit Vielfachheiten gezählt, ist demnach $m_1 + \cdots + m_k \leq n$. □

Dass neben der Nullteilerfreiheit auch die Kommutativität des Grundrings K eine entscheidende Rolle spielt, zeigt das folgende drastische Beispiel:

Beispiel 4C7. Im Matrizenring $\mathbb{C}^{2\times 2}$ hat das Polynom X^2+1 unendlich viele Nullstellen: für jedes Tripel $(x,y,z) \in \mathbb{R}^3$ mit $x^2+y^2+z^2 = 1$ erfüllt die Matrix $M = \left(\begin{smallmatrix} ix & y+iz \\ -y+iz & -ix \end{smallmatrix}\right)$ die Gleichung $M^2 = -1$. Dies gilt ebenso im Divisionsring der Quaternionen (3A12).

§**4Cc. Mehrfache Nullstellen und Ableitung.** Wir kennen von reellen Polynomen $P \in \mathbb{R}[X]$ das folgende nützliche Kriterium: $a \in \mathbb{R}$ ist genau dann eine einfache Nullstelle von P wenn $P(a) = 0$ aber $P'(a) \neq 0$ gilt. Diese schöne Charakterisierung wollen wir auch über einem beliebigen Körper nutzen.

Definition 4C8. Sei K ein kommutativer Ring und $K[X]$ der Polynomring in X über K. Die *Ableitung* $\partial = \frac{\partial}{\partial X} \colon K[X] \to K[X]$, geschrieben $P \mapsto \partial P = P'$, ist definiert durch

$$\partial\Big(\sum_{k=0}^{n} a_k X^k\Big) := \sum_{k=0}^{n} k a_k X^{k-1}.$$

Proposition 4C9. *Die Ableitung $\partial \colon K[X] \to K[X]$ ist K-linear, das heißt*

$$\partial(P+Q) = \partial P + \partial Q \qquad \text{und} \qquad \partial(aP) = a(\partial P) \qquad \text{für alle } a \in K,$$

und erfüllt die Leibniz-Regel

$$\partial(PQ) = (\partial P)\cdot Q + P \cdot (\partial Q).$$

BEWEIS. Die K-Linearität folgt offensichtlich aus der Definition. Die Leibniz-Regel prüft man für $P = X^m$ und $Q = X^n$ leicht nach:

$$\partial(PQ) = \partial X^{m+n} = (m+n)X^{m+n-1} = mX^{m-1}\cdot X^n + X^m \cdot nX^{n-1} = (\partial P)\cdot Q + P\cdot(\partial Q).$$

Diese Formel ist K-linear in P und in Q, also setzt sie sich auf alle Polynome fort. □

Proposition 4C10. *Ein Element $a \in K$ ist genau dann mehrfache Nullstelle von $P \in K[X]^*$ wenn a eine gemeinsame Nullstelle von P und seiner Ableitung P' ist.*

BEWEIS. Sei $P = (X-a)^m Q$ mit $m \geq 0$ und $Q(a) \neq 0$. Nach Leibniz gilt

$$P' = m(X-a)^{m-1}Q + (X-a)^m(\partial Q).$$

Wenn a eine mehrfache Nullstelle ist, also $m \geq 2$, dann gilt $P(a) = 0$ und $P'(a) = 0$.

Umgekehrt folgt aus $P(a) = 0$, dass $m \geq 1$ gilt. Für $m = 1$ hätten wir $P'(a) = Q(a) \neq 0$. Aus $P(a) = P'(a) = 0$ folgt somit $m \geq 2$. □

Beispiel 4C11. Sei $p \geq 2$ eine Primzahl. Hat $P = X^p - X$ mehrfache Nullstellen in $\mathbb{Z}/_p$?

Erste Lösung: Wir haben $P' = pX^{p-1} - 1 = -1$ wegen $\bar{p} = 0$ in $\mathbb{Z}/_p$. Also gibt es keine gemeinsamen Nullstellen von P et P', und damit auch keine mehrfachen Nullstellen von P.

Zweite Lösung: Wir kennen bereits alle Nullstellen von P. Jedes Element $a \in \mathbb{Z}/_p$ erfüllt $a^p = a$ nach dem kleinen Satz von Fermat (3D28). Damit haben wir p verschiedene Nullstellen gefunden, und somit $X^P - X = \prod_{a\in\mathbb{Z}/_p}(X-a)$.

Beispiel 4C12. Für welche n hat $P = X^n - 1$ mehrfache Nullstellen in $\mathbb{Z}/_p$?

Wir haben $P' = nX^{n-1}$. Wenn $p \nmid n$, dann ist nur 0 Nullstelle von P', also existiert keine gemeinsame Nullstelle von P und P'. Gilt hingegen $n = mp$, dann tritt jede Nullstelle von P mehrfach auf: Nach Frobenius haben wir nämlich $X^n - 1 = (X^m - 1)^p$.

Bemerkung 4C13. Wir werden im nächsten Kapitel sehen, wie man im Polynomring $K[X]$ über einem Körper K den größten gemeinsamen Teiler von P und P' mit Hilfe des euklidischen Algorithmus berechnen kann. Dies liefert ein praktisches Verfahren, um gemeinsame Nullstellen herauszufiltern.

§4Cd. Interpolation.

Satz 4C14. *Sei K ein Körper. Zu je $n+1$ verschiedenen Stellen $x_0, x_1, \ldots, x_n \in K$ und beliebigen Werten $y_0, y_1, \ldots, y_n \in K$ existiert genau ein Polynom $P \in K[X]$ vom Grad $\leq n$, das $P(x_0) = y_0, P(x_1) = y_1, \ldots, P(x_n) = y_n$ erfüllt.*

BEWEIS. *Eindeutigkeit:* Sind P_1 und P_2 zwei solche Polynome, dann ist $P_1 - P_2$ vom Grad $\leq n$ hat aber mindestens die $n+1$ Nullstellen $x_0, x_1, \ldots, x_n$. Das ist nach Satz 4C6 nur für das Nullpolynom möglich. Also gilt $P_1 = P_2$.

Existenz: Nach Voraussetzung gilt $x_k - x_j \neq 0$ für alle $j \neq k$. Da wir über einem Körper arbeiten, sind diese Elemente invertierbar. Das Polynom

$$P_k = \prod_{j \neq k} \frac{X - x_j}{x_k - x_j} \quad \in K[X]$$

hat Grad n und erfüllt $P_k(x_k) = 1$ und $P_k(x_j) = 0$ für alle $j \neq k$. Daher ist

$$P = \sum_{k=0}^{n} y_k P_k$$

ein Polynom vom Grad $\leq n$ und erfüllt $P(x_k) = y_k$ für alle $k = 0, 1, \ldots, n$. □

Korollar 4C15. *Der Ringhomomorphismus $K[X] \to K^{n+1}$, $P \mapsto (P(x_0), P(x_1), \ldots, P(x_n))$ ist surjektiv und hat als Kern das von $P_0 = (X - x_0)(X - x_1) \cdots (X - x_n)$ erzeugte Ideal (P_0).*

BEWEIS. Surjektivität folgt mittels Interpolation aus Satz 4C14. Jedes Polynom P im Kern ist von der Form $P = P_0 Q$ mit $Q \in K[X]$ gemäß Satz 4C6. □

Dies kann man auch als Anwendung des chinesischen Restsatzes auffassen: Der Ringhomomorphismus $K[X] \to K$ mit $P \mapsto P(x_k)$ ist surjektiv und hat als Kern $(X - x_k)$. Die zusammengesetzte Abbildung $K[X] \to K^{n+1}$, $P \mapsto (P(x_0), P(x_1), \ldots, P(x_n))$ hat demnach als Kern $(X - x_0) \cap (X - x_1) \cap \cdots \cap (X - x_n)$. Da diese Ideale paarweise teilerfremd sind, ist ihr Durchschnitt gleich dem Produktideal $\big((X - x_0)(X - x_1) \cdots (X - x_n)\big)$.

§4D. Übungen und Ergänzungen

Übung 4D1. Man bestimme die Gruppe $\mathbb{Z}/4[X]^\times$ der invertierbaren Elemente in $\mathbb{Z}/4[X]$.

Übung 4D2. $P \in \mathbb{Z}[X]$ hat keine Nullstellen in $\mathbb{Z}$ wenn $P(0)$ und $P(1)$ ungerade sind.

Übung 4D3. Im Polynomring $K[X]$ über einem Körper K sind Ideale der Form $(X - a)$ und $(X - b)$ mit $a, b \in K$ genau dann teilerfremd, wenn $a \neq b$.

Übung 4D4. Sei $K[X]$ der Polynomring über einem Körper K. Wie in §4Ac ist für jedes Polynom $P = \sum_{k=0}^{n} a_k X^k$ die zugehörige polynomielle Abbildung $f_P \colon K \to K$ definiert durch $x \mapsto P(x) = \sum_{k=0}^{n} a_k x^k$. Dies stiftet einen Ringhomomorphismus $f \colon K[X] \to K^K$.

1. Wenn K unendlich viele Elemente hat, dann ist f injektiv, aber nicht surjektiv.
2. Wenn K nur endlich viele Elemente hat, dann ist f surjektiv, aber nicht injektiv.

Übung 4D5. Sei $p \geq 2$. In $\mathbb{Z}[X]$ zeige man, dass die Division von $M = X^{p^m} - X$ durch $N = X^{p^n} - X$ den Rest $R = X^{p^r} - X$ lässt, wobei $r = m \operatorname{rem} n$. (Hinweis: modulo $X^{p^n} - X$ nutze man die Kongruenz $X^{p^n} \equiv X$.) Also gilt $X^{p^n} - X \nmid X^{p^m} - X$ genau dann, wenn $n \nmid m$.

§4Da. Charakterisierung des Polynomrings über einem Körper.

Übung 4D6. Ist $R = K[X]$ der Polynomring über einem Körper K, dann definiert der Grad eine surjektive Abbildung $\nu\colon R \to \mathbb{N} \cup \{-\infty\}$, die folgende Eigenschaften erfüllt:

(a) Für alle $a, b \in R$ mit $b \neq 0$ existieren $c, d \in R$ so dass $a = bc + d$ mit $\nu(d) < \nu(b)$.
(b) Für alle $a, b \in R$ gilt $\nu(ab) = \nu(a) + \nu(b)$ und $\nu(a+b) \leq \sup\{\nu(a), \nu(b)\}$ mit Gleichheit wenn $\nu(a) \neq \nu(b)$.

Übung 4D7. Sei R ein kommutativer Ring mit einer surjektiven Abbildung $\nu\colon R \to \mathbb{N} \cup \{-\infty\}$, die obige Eigenschaften (a) und (b) erfüllt.

1. Man zeige $\nu(a) = -\infty \Leftrightarrow a = 0$ und $\nu(a) = 0 \Leftrightarrow a \in R^\times$.
2. Man zeige, dass $K = \{\, a \in R \mid \nu(a) \leq 0 \,\}$ ein Unterkörper von R ist.
3. Für $X \in R$ mit $\nu(X) = 1$ ist $R = K[X]$ der Polynomring in X über K und $\nu = \deg$.

KAPITEL 5

Teilbarkeitstheorie in Integritätsringen

§5A. Motivation

Teilbarkeitsbegriffe sind von den natürlichen Zahlen allgemein geläufig, zum Beispiel:

- Die Zahl 4 teilt die Zahl 12. Die Zahl 12345 ist ein Vielfaches von 3.
- Die Zahl 6 ist der größte gemeinsame Teiler von 24 und 90.
- Die Zahl 12 ist zerlegbar, zum Beispiel in $2 \cdot 6$ oder in $3 \cdot 4$.
- Die Zahl 13 ist unzerlegbar, erlaubt nur die trivialen Zerlegungen $1 \cdot 13$ und $13 \cdot 1$.
- Die Zahl 60 lässt sich als ein Produkt von unzerlegbare Faktoren schreiben, etwa $60 = 2 \cdot 2 \cdot 3 \cdot 5$, und diese Zerlegung ist eindeutig bis auf die Reihenfolge.

Wir wollen nun die grundlegenden Begriffe der Teilbarkeit in beliebigen Ringen definieren und die für die ganzen Zahlen erfolgreichen Techniken soweit möglich verallgemeinern. Zu diesem Behufe widmen uns zunächst der Trilogie *euklidische Ringe, Hauptidealringe, faktorielle Ringe*. Im folgenden Kapitel wird dies für Polynomringe verfeinert.

Der Ringbegriff ist von großer Allgemeinheit — hierin liegt seine Stärke und vielseitige Anwendbarkeit. Das richtige Maß an Allgemeinheit und Anwendbarkeit zu erreichen, und zugleich möglichen Gefahren und Pathologien auszuweichen, bedarf besonderer Sorgfalt in der Begriffsbildung. Viele Beispiele und Gegenbeispiele sind daher zur Illustration und für das Verständnis der Feinheiten wesentlich.

Beispiel. Dass die eindeutige Zerlegbarkeit selbst für natürliche Zahlen nicht selbstverständlich ist, zeigt folgendes (künstliche aber einfache) Beispiel. Die Menge $M = \{1\} \cup \{\, n \in \mathbb{N} \mid n \geq 3 \,\}$ ist ein Monoid bezüglich Multiplikation. Hierin sind 4 und 8 unzerlegbar, denn die aus $\mathbb{N}$ gewohnten Zerlegungen $4 = 2 \cdot 2$ und $8 = 2 \cdot 4 = 4 \cdot 2$ stehen in M nicht mehr zur Verfügung. Die Zahl 60 lässt sich nur auf eine Weise in unzerlegbare Faktoren zerlegen, nämlich $60 = 3 \cdot 4 \cdot 5$. Die Zahl 64 hingegen lässt sich auf zwei Arten in unzerlegbare Faktoren zerlegen, nämlich $64 = 4 \cdot 4 \cdot 4 = 8 \cdot 8$.

Dieses bizarre Verhalten kennen wir aus $\mathbb{N}$ nicht, zumindest nicht bei den experimentell zugänglichen kleinen Beispielen. Dass dies auch noch für beliebig große natürliche Zahlen, die sich unserer Erfahrung und Intuition entziehen, gültig bleibt, bedarf eines Beweises. Die Faktorialität des Rings $\mathbb{Z}$, die wir in diesem Kapitel beweisen, wird nebenbei auch die eindeutige Zerlegbarkeit in $\mathbb{N}$ sicherstellen.

Konvention. In diesem Kapitel betrachten wir ausschließlich Integritätsringe, also kommutative Ringe mit $1 \neq 0$ ohne Nullteiler.

§5B. Grundbegriffe

§**5Ba. Assoziierte Elemente.** Im Folgenden sei $(R,+,\cdot)$ ein Integritätsring. Dann ist $R^* = R \setminus \{0\}$ ein Untermonoid von $(R,\cdot)$, da aus $a \neq 0$ und $b \neq 0$ auch $ab \neq 0$ folgt. Mit $R^\times$ bezeichnen wir die Untergruppe der in $(R,\cdot)$ invertierbaren Elemente.

Beispiel 5B1.
- R ist genau dann ein Körper, wenn $R^\times = R^*$ gilt.
- Im Ring $\mathbb{Z}$ der ganzen Zahlen gilt $\mathbb{Z}^\times = \{-1,+1\} \subsetneq \mathbb{Z}^*$.
- Im Polynomring $\mathbb{Q}[X]$ gilt $\mathbb{Q}[X]^\times = \mathbb{Q}^*$, gemäß 4B5

Definition 5B2. Zwei Elemente $a,b \in R$ heißen *assoziiert*, wenn es ein Element $u \in R^\times$ gibt sodass $au = b$. Dies ist eine Äquivalenzrelation, geschrieben $a \underset{R}{\sim} b$ oder kurz $a \sim b$.

Demnach ist $aR^\times$ die Äquivalenzklasse der zu $a \in R$ assoziierten Elemente. Insbesondere sind die invertierbaren Elemente in R gerade die mit 1 assoziierten.

In jedem kommutativen Ring R gilt $(1) = R$, und $a \in R$ ist genau dann invertierbar, $(a) = R$ gilt. In einem Integritätsring gilt allgemeiner folgende Regel:

Proposition 5B3. *In einem Integritätsring gilt $(a) = (b)$ genau dann, wenn $a \sim b$.*

BEWEIS. "$\Leftarrow$" Aus $au = b$ mit $u \in R^\times$ folgt $a \in (b)$ also $(a) \subset (b)$. Aus $a = bu^{-1}$ folgt umgekehrt $b \in (a)$ also $(b) \subset (a)$. (Diese Implikation benötigt nicht die Nullteilerfreiheit.)

"$\Rightarrow$" Sei $(a) = (b)$. Wegen $b \in (a)$ haben wir $b = au$ mit $u \in R$, und wegen $a \in (b)$ auch $a = bv$ mit $v \in R$. Daraus folgt $a = bv = auv$, also $a(1-uv) = 0$. Wenn $a = 0$, dann folgt $b = 0$, also insbesondere $a \sim b$. Wenn $a \neq 0$, dann folgt $1 - uv = 0$, da wir den Ring R als nullteilerfrei voraussetzen. Also gilt $uv = 1$, das heißt $u,v \in R^\times$, und somit $a \sim b$. □

Assoziierte Elemente haben bezüglich Teilbarkeit dieselben Eigenschaften, wie wir gleich sehen werden. Häufig wollen wir daher aus der Äquivalenzklasse $aR^\times$ einen (möglichst einfachen oder bevorzugten) Repräsentanten auswählen:

Beispiel 5B4. In $\mathbb{Z}$ sind a und $-a$ assoziiert; als Repräsentanten wählt man gewöhnlich $|a|$. In $\mathbb{Q}[X]$ ist jedes Polynom $P \neq 0$ zu genau einem normierten Polynom $\operatorname{lc}(P)^{-1}P$ assoziiert.

Im Allgemeinen ist eine solche kanonische Wahl eines Repräsentanten nicht gegeben. In diesem Fall tun wir gut daran, unsere Begriffe so zu formulieren, dass sie dieser mangelnden Eindeutigkeit Rechnung tragen.

§**5Bb. Teilbarkeit.** Den Begriff der Teilbarkeit verallgemeinern wir in offensichtlicher Weise von den ganzen Zahlen auf Elemente in einem beliebigen Integritätsring:

Definition 5B5. Seien $a,b \in R$. Wir sagen b teilt a in R, oder a ist ein Vielfaches von b in R, falls es $c \in R$ gibt mit $a = bc$. Dies schreiben wir $b \underset{R}{\mid} a$ oder kurz $b \mid a$.

Bemerkung 5B6. Es gilt $b \mid a$ genau dann wenn $(a) \subset (b)$.

Bemerkung 5B7. In obiger Definition ist $b = 0$ zugelassen: Die Relation $0 \mid a$ bedeutet "0 teilt a" oder besser "a ist Vielfaches von 0", also $a = 0 \cdot c = 0$. Bedeutet "0 teilt a", dass man a durch 0 teilen darf? Nein, das bleibt auch hier unmöglich, aus immer demselben Grund:

Ist a teilbar durch b, also $\exists c \in R : a = bc$, dann wollen wir a durch b teilen und als Ergebnis $a/b := c$ definieren. Wir müssen hierzu allerdings sicherstellen, dass das Ergebnis c wohldefiniert ist, das heißt nur von a und b abhängt. Angenommen es gäbe $c, c' \in R$, sodass $a = bc = bc'$, dann folgt $b(c-c') = 0$. Ist R ein Integritätsring und $b \neq 0$, dann muss $c = c'$ gelten. Diese Eindeutigkeit stellt sicher, dass wir $a/b := c$ definieren können.

Proposition 5B8. *Auf jedem Integritätsring R definiert die Teilbarkeit eine (Prä)Ordnung. Das heißt, für alle $a, b, c \in R$ gilt*

- *Reflexivität: $a \mid a$,*
- *Transitivität: Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$,*
- *Antisymmetrie: Aus $a \mid b$ und $b \mid a$ folgt $a \sim b$.*

Diese Ordnung ist im Allgemeinen nicht linear, d.h. es kann $a \nmid b$ und $b \nmid a$ vorkommen.

- *Es gilt $1 \mid a$ und $a \mid 0$, das heißt 1 ist kleinstes Element und 0 ist größtes Element.*
- *Es gilt $0 \mid a$ genau dann wenn $a = 0$, und $a \mid 1$ genau dann wenn a invertierbar ist.*

Die Teilbarkeit ist mit Addition und Multiplikation in folgendem Sinne verträglich:

- *Aus $a \mid b$ folgt $a \mid bc$.*
- *Aus $a \mid b$ und $a \mid c$ folgt $a \mid b + c$.*

Bemerkung 5B9. Vermöge der Äquivalenz $a \mid b \Leftrightarrow (b) \subset (a)$ lassen sich obige Aussagen zur Teilbarkeit wie folgt in die Sprache der Ideale übersetzen: Für alle $a, b, c \in R$ gilt

- Reflexivität: $(a) \subset (a)$,
- Transitivität: Aus $(b) \subset (a)$ und $(c) \subset (b)$ folgt $(c) \subset (a)$,
- Antisymmetrie: Aus $(b) \subset (a)$ und $(a) \subset (b)$ folgt $(a) = (b)$.

Diese Ordnung ist im Allgemeinen nicht linear: möglicherweise $(b) \not\subset (a)$ und $(a) \not\subset (b)$.

- Es gilt $(0) \subset (a) \subset (1)$, das heißt (0) ist kleinstes Ideal und (1) ist größtes Ideal.
- Es gilt $(a) \subset (0)$ genau dann wenn $a = 0$, und $(1) \subset (a)$ genau dann wenn $a \in R^\times$.

Die Teilbarkeit ist mit Addition und Multiplikation in folgendem Sinne verträglich:

- Aus $(b) \subset (a)$ folgt $(bc) \subset (a)$.
- Aus $(b) \subset (a)$ und $(c) \subset (a)$ folgt $(b + c) \subset (a)$.

§**5Bc. Größte gemeinsame Teiler.** Mit Hilfe der Teilbarkeit können wir nun formulieren, was ein größter gemeinsamer Teiler (kurz ggT) sein soll. In einem beliebigen Ring ist allerdings zunächst nicht klar, ob es einen ggT überhaupt gibt und inwiefern solch ein ggT eindeutig ist. Wir formulieren unsere Definition also vorsichtig wie folgt:

Definition 5B10. Die Menge der *gemeinsamen Teiler* von $a_1, \dots, a_n \in R$ ist

$$\mathrm{GT}(a_1, \dots, a_n) = \{\, t \in R \colon t \mid a_1, \dots, t \mid a_n \,\}.$$

In dieser Menge heißen die größten Elemente *größte gemeinsame Teiler* (kurz ggT):

$$\mathrm{GGT}(a_1, \dots, a_n) = \{\, t \in \mathrm{GT}(a_1, \dots, a_n) \colon \forall s \in \mathrm{GT}(a_1, \dots, a_n) : s \mid t \,\}.$$

Man beachte, dass "größer" hier im Sinne der Teilbarkeit verstanden wird: Diese hat in jedem Integritätsring einen Sinn und definiert eine Ordnung wie oben erklärt.

Beispiel 5B11.
- In $\mathbb{Q}[X]$ gilt $\mathrm{GT}(X, X-1) = \mathbb{Q}^\times$ und daher $\mathrm{GGT}(X, X-1) = \mathbb{Q}^\times$.
- In $\mathbb{Z}$ gilt $\mathrm{GT}(24,90) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$ und daher $\mathrm{GGT}(24,90) = \{\pm 6\}$.

Bemerkung 5B12. Falls ein ggT existiert, ist dieser im Allgemeinen nicht eindeutig, das heißt, die Menge $\mathrm{GGT}(a_1, \dots, a_n)$ kann mehrere Elemente enthalten:

- Ist d ein ggT von $a_1, \dots, a_n$, dann auch jedes assoziierte Elemente $d' \sim d$.
- Umgekehrt sind je zwei ggT d, d' von $a_1, \dots, a_n$ assoziiert, denn $d \mid d'$ und $d' \mid d$.

In $\mathbb{Z}$ können wir stets *den positiven ggT* bevorzugen. Im Polynomring $K[X]$ über einem Körper K können wir stets den *normierten ggT* mit Leitkoeffizient 1 bevorzugen. In einem beliebigen Ring gibt es keine kanonische Wahl, welcher unter den möglichen ggT bevorzugt werden sollte. Es ist dann ratsam, von *einem* ggT zu sprechen und nicht von *dem* ggT.

Bemerkung 5B13. Ein ggT zu $a_1, \dots, a_n$ braucht im Allgemeinen nicht zu existieren, das heißt, die Menge $\mathrm{GGT}(a_1, \dots, a_n)$ kann leer sein. Hierzu ein einfaches Beispiel:

Beispiel 5B14. Im Polynomring $\mathbb{Z}/_2[X]$ über dem Körper $\mathbb{Z}/_2$ ist die Menge

$$R = \mathbb{Z}/_2[X^2, X^3] = \{\, a_0 + a_2 X^2 + a_3 X^3 + \dots + a_n X^n \mid a_0, a_2, a_3, \dots, a_n \in \mathbb{Z}/_2 \,\}.$$

ein Unterring. Hier gilt $\mathrm{GT}(X^5, X^6) = \{1, X^2, X^3\}$ und daher $\mathrm{GGT}(X^5, X^6) = \emptyset$: In R gilt $1 \mid X^2$ und $1 \mid X^3$ aber $X^2 \nmid X^3$ und $X^3 \nmid X^2$. (Dieses Beispiel wird in Übung 5H10 vertieft.)

§**5Bd. Kleinste gemeinsame Vielfache.** Analog zu größten gemeinsamen Teilern definiert man kleinste gemeinsame Vielfache. Auch hier ist Vorsicht geboten solange Existenz und Eindeutig nicht geklärt sind. Wir formulieren unsere Definition daher wie folgt:

Definition 5B15. Die Menge der *gemeinsamen Vielfachen* von $a_1, \dots, a_n \in R$ ist

$$\mathrm{GV}(a_1, \dots, a_n) = \{\, v \in R \colon a_1 \mid v, \dots, a_n \mid v \,\}.$$

In dieser Menge heißen die kleinsten Elemente *kleinste gemeinsame Vielfache* (kurz kgV):

$$\mathrm{KGV}(a_1, \dots, a_n) = \{\, v \in \mathrm{GV}(a_1, \dots, a_n) \colon \forall u \in \mathrm{GV}(a_1, \dots, a_n) : v \mid u \,\}.$$

Man beachte, dass "kleiner" hier im Sinne der Teilbarkeit verstanden wird: Diese hat in jedem Integritätsring einen Sinn und definiert eine Ordnung wie oben erklärt.

Bemerkung 5B16. Falls ein kgV existiert, ist dieses im Allgemeinen nicht eindeutig:

- Ist v ein kgV von $a_1, \dots, a_n$, dann auch jedes assoziierte Elemente $v' \sim v$.
- Umgekehrt sind je zwei kgV v, v' von $a_1, \dots, a_n$ assoziiert, denn $v \mid v'$ und $v' \mid v$.

Ein kgV zu $a_1, \dots, a_n$ braucht im Allgemeinen nicht zu existieren, das heißt, die Menge $\mathrm{KGV}(a_1, \dots, a_n)$ kann leer sein. Wir führen hierzu obiges Gegenbeispiel weiter:

Beispiel 5B17. Im Ring $R = \mathbb{Z}/_2[X^2, X^3]$ gilt $\mathrm{GV}(X^5, X^6) = \{X^8, X^9, X^{10}, \dots\}$ aber hierin existiert kein kleinstes Element wegen $X^8 \nmid X^9$ in R. Daher gilt $\mathrm{KGV}(X^5, X^6) = \emptyset$.

Allgemein ist es zweckmäßig, sich auf die Untersuchung der ggT zu beschränken. Alle Ergebnisse verallgemeinern sich auf die kgV durch folgende Dualisierung:

Übung 5B18. Man untersuche die Dualität zwischen ggT und kgV:

1. Wenn t ein gemeinsamer Teiler von a und b ist,
   ist dann ab/t ein gemeinsames Vielfaches von a und b.
2. Wenn v ein gemeinsames Vielfaches von a und b ist und $v \mid ab$,
   ist dann ab/v ein gemeinsamer Teiler von a und b?
3. Wenn t ein ggT von a und b ist, ist dann ab/t ein kgV von a und b?
4. Wenn v ein kgV von a und b ist, ist dann ab/v ein ggT von a und b?

§5C. Euklidische Ringe

§5Ca. Division mit Rest. Die ganzen Zahlen erlauben eine Division mit Rest: zu $a, b \in \mathbb{Z}$ mit $b \neq 0$ existieren $q, r \in \mathbb{Z}$ sodass $a = bq + r$ und $|r| < |b|$ gilt. Hierzu nutzen wir den Betrag $\mathbb{Z} \to \mathbb{N}$, $a \mapsto |a|$, um sicherzustellen, dass der Rest r kleiner ist als b.

Um dies auf einen beliebigen Integritätsring R zu verallgemeinern, benötigen wir eine "Gradfunktion" $\nu\colon R \to \mathbb{N}$, um formulieren zu können, dass in $a = bq + r$ der Rest r kleiner ist als b. Dies ist in günstigen Fällen möglich, und führt uns zu folgender Definition:

Definition 5C1. Eine *euklidische Division* auf dem Ring R ist gegeben durch eine Funktion $\nu\colon R \to \mathbb{N}$ mit $\nu(0) = 0$ und eine Abbildung $\delta\colon R \times R^* \to R \times R$ mit $(a,b) \mapsto (q,r)$ so dass

$$a = bq + r \quad \text{mit} \quad \nu(r) < \nu(b).$$

In diesem Fall nennt man ν eine *euklidische Gradfunktion* auf R, und δ eine *euklidische Division* auf R bezüglich des Grades ν. Ein *euklidischer Ring* (R, ν, δ) besteht aus einem Integritätsring R zusammen mit einer euklidische Division (ν, δ). Abkürzend nennt man einen Integritätsring R *euklidisch*, wenn es auf ihm eine euklidische Division gibt.

Ist (R, ν, δ) ein euklidischer Ring, dann können wir die Abbildungen "Quotient" und "Rest" $\operatorname{quo}, \operatorname{rem}\colon R \times R^* \to R$ definieren durch $\delta(a,b) = (a \operatorname{quo} b, a \operatorname{rem} b)$. Aus jeder der beiden Abbildungen quo und rem kann man die jeweils andere rekonstruieren.

Beispiel 5C2. Der Ring $\mathbb{Z}$ der ganzen Zahlen ist euklidisch: wie eingangs erwähnt kann man $\nu(a) = |a|$ wählen zusammen mit der üblichen euklidischen Division $\mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Z} \times \mathbb{N}$.

Beispiel 5C3. Der Polynomring $K[X]$ über einem Körper K ist euklidisch bezüglich $\nu(0) = 0$ und $\nu(P) = 1 + \deg(P)$ für $P \neq 0$ zusammen mit der üblichen euklidischen Division.

Beispiel 5C4. Der Ring $\mathbb{Z}[i]$ der gaußschen Zahlen ist euklidisch (§5He). Die Übungen in §5Hf zeigen weitere Beispiele euklidischer Ringe.

Beispiel 5C5. Nicht jeder Ring ist euklidisch, zum Beispiel ist der Polynomring $\mathbb{Z}[X]$ nicht euklidisch. (Dazu später mehr: $\mathbb{Z}[X]$ ist kein Hauptidealring, siehe die Übungen in §5Hb.)

Bemerkung 5C6. Ist R euklidisch, so gibt es im Allgemeinen mehrere Gradfunktionen ν und zu jeder Gradfunktion auch mehrere euklidische Divisionen δ. Diese sind demnach nicht durch den Ring R bestimmt sondern zusätzliche Strukturen. Es gibt jedoch genau eine minimale Gradfunktion (siehe §5Hi). Auf $\mathbb{Z}$ ist die minimale Gradfunktion gegeben durch $\nu(0) = 0$ und $\nu(a) = 1 + \lfloor \log_2 |a| \rfloor$ für $a \neq 0$. Dies ist die Länge der Binärdarstellung des Absolutbetrages. (Übung 5H30)

§5Cb. Der euklidische Algorithmus. Der von den ganzen Zahlen bekannte euklidische Algorithmus verallgemeinert sich auf jeden euklidischen Ring. Es genügt hierbei,

den ggT für je zwei Elemente berechnen zu können. Für $a \in \mathrm{GGT}(a_2,\dots,a_n)$ gilt nämlich $\mathrm{GT}(a_1,a_2,\dots,a_n) = \mathrm{GT}(a_1,a)$ und daher $\mathrm{GGT}(a_1,a_2,\dots,a_n) = \mathrm{GGT}(a_1,a)$.

Die für den Algorithmus grundlegende Beobachtung ist die folgende:

Bemerkung 5C7. Für alle $a,b,c \in R$ gilt

- $\mathrm{GT}(a,b) = \mathrm{GT}(b,a) = \mathrm{GT}(b,a-bc)$,
- $\mathrm{GGT}(a,b) = \mathrm{GGT}(b,a) = \mathrm{GGT}(b,a-bc)$,
- $\mathrm{GGT}(a,0) = \mathrm{GGT}(a) = aR^\times$.

Für euklidische Ringe folgt daraus:

Satz 5C8 (Euklid)**.** *In einem euklidischen Ring gibt es zu je zwei Elementen einen ggT. Der folgende Algorithmus 3 berechnet einen solchen.*

Algorithmus 3 Berechnung eines ggT in einem euklidischen Ring

Eingabe: zwei Elemente $a_0, b_0 \in R$ in einem euklidischen Ring R
Ausgabe: ein Element $a \in \mathrm{GGT}(a_0,b_0)$

$a \leftarrow a_0,\quad b \leftarrow b_0$	// Invariante: $\mathrm{GGT}(a,b) = \mathrm{GGT}(a_0,b_0)$
while $b \neq 0$ **do**	
$\quad r \leftarrow a \operatorname{rem} b,\quad a \leftarrow b,\quad b \leftarrow r$	// $\mathrm{GGT}(a,b) = \mathrm{GGT}(b,a-qb)$
end while	
return a	// Wir wissen, dass $a \in \mathrm{GGT}(a,0)$

BEWEIS. *Der Algorithmus terminiert:* Die Gradfunktion $\nu(b)$ ist streng monoton abnehmend, muss also nach höchstens $\nu(b_0)$ Iterationen mit $\nu(b) = 0$ enden.

Das Ergebnis erfüllt die geforderten Bedingungen: Die Initialisierung $a \leftarrow a_0$, $b \leftarrow a_0$ garantiert $\mathrm{GGT}(a,b) = \mathrm{GGT}(a_0,b_0)$. Jede Iteration erhält $\mathrm{GGT}(a,b) = \mathrm{GGT}(b,a-qb)$. Zum Schluss gilt also $\mathrm{GGT}(a_0,b_0) = \mathrm{GGT}(a,0) = aR^\times$. Also ist a ein ggT von a_0,b_0. □

§**5Cc. Der erweiterte euklidische Algorithmus.** Der euklidische Algorithmus ist extrem einfach und dabei überaus praktisch und effizient. Mit Hilfe einer kleinen Erweiterung lässt sich noch eine wertvolle Zusatzinformation gewinnen:

Satz 5C9 (Bézout)**.** *Sei R ein euklidischer Ring. Dann gibt es zu je zwei Elementen $a,b \in R$ Koeffizienten $u,v \in R$ so dass $au+bv \in \mathrm{GGT}(a,b)$. Der folgende Algorithmus 4 berechnet ein solches Paar (u,v).*

BEWEIS. *Der Algorithmus terminiert:* Die Gradfunktion $\nu(b)$ ist streng monoton abnehmend, muss also nach höchstens $\nu(b_0)$ Iterationen mit $\nu(b) = 0$ enden.

Das Ergebnis erfüllt die geforderten Bedingungen: In der ersten Spalte sehen wir den euklidischen Algorithmus, dessen Korrektheit wir oben gezeigt haben. Die Initialisierung garantiert $a = a_0u + b_0v$ und $b = a_0s + b_0t$. Jede Iteration erhält diese Gleichung. Zum Schluss gilt also $a \in \mathrm{GGT}(a_0,b_0)$ und $a = a_0u + b_0v$, wie gefordert. □

Algorithmus 4 Berechnung von Bézout-Koeffizienten in einem euklidischen Ring

Eingabe: zwei Elemente $a_0, b_0 \in R$ in einem euklidischen Ring R
Ausgabe: drei Elemente $a, u, v \in R$ so dass $a = a_0u + b_0v \in \mathrm{GGT}(a_0, b_0)$.

$\begin{pmatrix} a & u & v \\ b & s & t \end{pmatrix} \leftarrow \begin{pmatrix} a_0 & 1 & 0 \\ b_0 & 0 & 1 \end{pmatrix}$ // Invariante $\begin{cases} a = a_0u + b_0v \\ b = a_0s + b_0t \end{cases}$

while $b \neq 0$ **do**

$q \leftarrow a \operatorname{quo} b$, $\begin{pmatrix} a & u & v \\ b & s & t \end{pmatrix} \leftarrow \begin{pmatrix} b & s & t \\ a - qb & u - qs & v - qt \end{pmatrix}$ // Invariante $\begin{cases} a = a_0u + b_0v \\ b = a_0s + b_0t \end{cases}$

end while

return (a, u, v) // $a = a_0u + b_0v \in \mathrm{GGT}(a_0, b_0)$

§5D. Hauptidealringe

Definition 5D1. Ein *Hauptideal* in einem Ring R ist ein Ideal der Form $(a) = aR$ mit $a \in R$. Ein Integritätsring R heißt *Hauptidealring* wenn jedes Ideal in R ein Hauptideal ist.

Beispiel 5D2. Nicht jeder Ring ist Hauptidealring: In $\mathbb{Z}[X]$ zum Beispiel ist das Ideal $(2, X)$ nicht von der Form (P) für $P \in \mathbb{Z}[X]$. (Die Übungen in §5Hb vertiefen diese Beobachtung.)

Beispiel 5D3. In §3Da haben wir bereits gesehen, dass $\mathbb{Z}$ ein Hauptidealring ist, und die Beweistechnik wollen wir sogleich auf euklidische Ringe ausdehnen:

Satz 5D4. *Jeder euklidische Ring ist ein Hauptidealring.*

BEWEIS. Sei R ein euklidischer Ring und sei $I \subset R$ ein Ideal. Wir haben zu zeigen, dass $I = (a)$ für ein $a \in R$ gilt. Wenn $I = \{0\}$, dann erfüllt $a = 0$ das Verlangte. Andernfalls wählen wir $a \in I$ mit $a \neq 0$ und minimalem Grad $\nu(a)$, und zeigen $I = (a)$.

Die Inklusion $I \supset (a)$ ist klar: aus $a \in I$ folgt $(a) = Ra \subset RI = I$.

Es bleibt die Inklusion $I \subset (a)$ zu zeigen. Für jedes $x \in I$ liefert Division mit Rest $x = qa + r$ mit $\nu(r) < \nu(a)$. Aus $x \in I$ und $qa \in I$ folgt $r = x - qa \in I$, also $r = 0$ aufgrund der Minimalität von a. Das bedeutet $x = qa$, also $x \in I$. Wir schließen daraus $I = (a)$. □

Wir erinnern daran, dass $(a_1, \ldots, a_n)_R$ das kleinste Ideal in R ist, das die Elemente $a_1, \ldots, a_n$ enthält. Da wir hier über kommutative Ringe sprechen, gilt

$$(a_1, \ldots, a_n)_R = a_1R + \cdots + a_nR = \{\, a_1u_1 + \cdots + a_nu_n \mid u_1, \ldots, u_n \in R \,\}.$$

Satz 5D5. *In einem Hauptidealring R besitzt jede Familie $a_1, \ldots, a_n \in R$ einen ggT:*

$$\textit{Es gilt } d \in \mathrm{GGT}(a_1, \ldots, a_n) \textit{ genau dann wenn } (a_1, \ldots, a_n) = (d).$$

In diesem Fall gibt es Koeffizienten $u_1, \ldots, u_n \in R$ so dass

$$a_1u_1 + \cdots + a_nu_n = d \quad \in \quad \mathrm{GGT}(a_1, \ldots, a_n).$$

Analog hierzu besitzt jede Familie $a_1, \ldots, a_n \in R$ ein kgV:

$$\textit{Es gilt } v \in \mathrm{KGV}(a_1, \ldots, a_n) \textit{ genau dann wenn } (a_1) \cap \cdots \cap (a_n) = (v).$$

BEWEIS. Es gibt ein Element $d \in R$ mit $(a_1, \ldots, a_n) = (d)$.

- Wegen $a_k \in (a_1,\dots,a_n) = (d)$ haben wir $d \mid a_k$ für alle k.
- Wenn $c \mid a_k$ für alle k, dann $a_k \in (c)$, somit $(d) = (a_1,\dots,a_n) \subset (c)$, also $c \mid d$.

Demnach ist d ein größter gemeinsamer Teiler von $a_1,\dots,a_n$. Umgekehrt ist jeder größte gemeinsame Teiler d' von $a_1,\dots,a_n$ zu d assoziiert, also $(d') = (d) = (a_1,\dots,a_n)$.

Die duale Aussage zum kgV zeigt man genauso. Man beachte hierzu, dass der Durchschnitt $(a_1) \cap \dots \cap (a_n)$ das größte Ideal ist, das in allen $(a_1),\dots,(a_n)$ enthalten ist. □

Bemerkung 5D6. Anders als für euklidische Ringe ist dieser Satz für Hauptidealringe zunächst nur eine Existenz-Aussage. Zur konkreten Berechnung der Koeffizienten $u_1,\dots,u_n$ benötigen wir einen *Bézout-Algorithmus* $\beta\colon R \times R \to R \times R$, $(a,b) \mapsto (u,v)$, so dass $au+bv$ ein ggT von a,b ist. Für euklidische Ringen liefert der erweiterte euklidische Algorithmus 4 eine effiziente Berechnungsmethode.

§5E. Faktorielle Ringe

Es sei weiterhin R ein Integritätsring. Wir untersuchen Zerlegungen von Elementen $a \in R$. Insbesondere interessieren uns unzerlegbare Elemente, und wir gehen der Frage nach, ob und wie sich ein beliebiges Element $a \in R$ in unzerlegbare Faktoren zerlegen lässt.

§5Ea. Irreduzible Elemente. Wenn für Elemente $a,b,c \in R$ die Gleichung $a = bc$ gilt, dann sagen wir "a kann in die Faktoren b und c zerlegt werden".

Zum Beispiel gilt stets $a = 1 \cdot a = a \cdot 1$, und allgemeiner $a = u \cdot (u^{-1}a) = (au^{-1}) \cdot u$ für alle invertierbaren Element $u \in R^\times$. Dies nennen wir die *trivialen Zerlegungen* von a. Wir nennen a *unzerlegbar* oder *irreduzibel*, wenn es nur die trivialen Zerlegungen erlaubt:

Definition 5E1. Sei R ein Integritätsring. Ein Element $a \in R$ heißt *irreduzibel* wenn gilt:

Für alle $b,c \in R$ folgt aus $a = bc$ entweder $b \sim 1$ oder $c \sim 1$.

Bemerkung 5E2. Für jedes $a \in R$ sind folgende Umformulierungen zueinander äquivalent:

- Für alle $b,c \in R$ folgt aus $a = bc$ entweder $b \sim 1$ oder $c \sim 1$.
- Für alle $b,c \in R$ folgt aus $a = bc$ entweder $b \sim a$ oder $c \sim a$.
- Für alle $b \in R$ folgt aus $b \mid a$ entweder $b \sim 1$ oder $b \sim a$.

Bezüglich der Ordnung $\mid$ auf R sind die kleinsten Elemente genau die invertierbaren Elemente $a \in R^\times$. Die minimalen Elemente der Restmenge $R \smallsetminus R^\times$ sind genau die irreduziblen: Ist a irreduzibel, so folgt aus $b \mid a$ entweder $b \sim 1$ oder $b \sim a$.

Beispiel 5E3. Das Nullelement 0 ist nicht irreduzibel, wie man aus $0 = 0 \cdot 0$ ersieht.

Beispiel 5E4. Invertierbare Elemente $a \in R^\times$ sind nicht irreduzibel, denn für $a \sim 1 \cdot a$ gilt sowohl $1 \sim 1$ also auch $a \sim 1$ (also gerade nicht "entweder… oder…").

Definition 5E5. Ein Element $a \in R^*$ erlaubt eine *Zerlegung in irreduzible Faktoren* wenn es irreduzible Elemente $p_1,\dots,p_n \in R$ und $u \in R^\times$ gibt so dass $a = up_1 \cdots p_n$ gilt.

Wir lassen hier auch $n = 0$ zu; in diesem Fall ist die Zerlegung als $a = u$ zu lesen. Zerlegungen in $n = 0$ irreduzible Faktoren entsprechen gerade den invertierbaren Elementen.

Da wir in einem kommutativen Ring arbeiten, können wir Produkte beliebig umordnen. Ebenso können wir von $a = up_1 \cdots p_n$ stets zu $a = (uu_1^{-1} \cdots u_n^{-1})(u_1 p_1) \cdots (u_n p_n)$ übergehen mit beliebigen invertierbaren Elementen $u_1, \ldots, u_n \in R^\times$. Diese offensichtlichen Umformungen können wir nicht verbieten. Wir nennen die Zerlegung von a eindeutig, wenn je zwei Zerlegungen allein durch die offensichtlichen Umformungen ineinander übergehen:

Definition 5E6. Wir sagen, die Zerlegung von a in irreduzible Faktoren ist *eindeutig*, wenn für je zwei Zerlegungen $a = up_1 \cdots p_n = vq_1 \cdots q_m$ mit $u, v \in R^\times$ und irreduziblen Faktoren $p_q, \ldots, p_n, q_1, \ldots, q_m \in R$ gilt, dass $m = n$ und nach Umordnung $p_1 \sim q_1, \ldots, p_n \sim q_n$.

Beispiel 5E7. In $\mathbb{Z}$ gilt zum Beispiel $-12 = (-1) \cdot 2 \cdot 2 \cdot 3 = 1 \cdot (-3) \cdot (-2) \cdot (-2)$ und dennoch betrachten wir diese beiden Zerlegungen im Wesentlichen als gleich.

Definition 5E8. Ein Integritätsring R heißt *faktoriell* wenn jedes Element $a \in R^*$ eine *eindeutige* Zerlegung in irreduzible Faktoren erlaubt.

Wir werden gleich sehen, dass der Ring $\mathbb{Z}$ der ganzen Zahlen faktoriell ist, ebenso jeder Polynomring $K[X]$ über einem Körper K. Nicht alle Ringe sind jedoch faktoriell:

Beispiel 5E9. In $R = \mathbb{Z}/_2[X^2, X^3]$ sind X^2 und X^3 irreduzibel, denn die Zerlegungen $X^2 = X \cdot X$ und $X^3 = X \cdot X^2$ stehen in R nicht mehr zur Verfügung. Das Element X^6 hat zwei verschiedene Zerlegungen in irreduzible Faktoren, nämlich $X^6 = X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3$.

Proposition 5E10. *Sei $a = up_1 \cdots p_n$ eine Zerlegung in $u \in R^\times$ und irreduzible Elemente $p_1, \ldots, p_n \in R$. Für jede Teilmenge $J \subset \{1, \ldots, n\}$ ist $a_J = \prod_{j \in J} p_j$ ein Teiler von a. Ist der Ring R faktoriell, dann ist jeder Teiler von a zu einem solchen a_J assoziiert.*

Insbesondere hat in einem faktoriellen Ring R jedes Element $a \in R^*$ nur endlich viele Teiler, wobei wir assoziierte Teiler nicht unterscheiden.

BEWEIS. Offenbar gilt $a = (u \cdot A_{\complement J}) \cdot a_J$, also $a_J \mid a$. Sei umgekehrt $b \mid a$, also $a = bc$ mit $a, b \in R$. Da wir R als faktoriell voraussetzen, existieren Zerlegungen $b = q_1 \cdots q_m$ und $c = q_{m+1} \cdots q_n$ in irreduzible Elemente $q_1, \ldots, q_n \in R$. Aus $a = bc$ folgt $up_1 \cdots p_n = q_1 \cdots q_m \cdot q_{m+1} \cdots q_n$. Aufgrund der Eindeutigkeit von Zerlegungen existiert eine Bijektion $k \mapsto i_k$ sodass $q_k \sim p_{i_k}$ für alle $k = 1, \ldots, n$. Daraus folgt $b \sim a_J$ für $J = \{i_1, \ldots, i_m\}$. □

Beispiel 5E11. Wir werden gleich sehen, dass $\mathbb{Z}$ faktoriell ist. In $\mathbb{Z}$ ist $60 = 2 \cdot 2 \cdot 3 \cdot 5$ eine Zerlegung und die Teiler von 60 sind in der Tat $\pm\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$.

Beispiel 5E12. In $\mathbb{Z}/_2[X^2, X^3]$ ist $X^6 = X^3 \cdot X^3$ eine Zerlegung in irreduzible Elemente. Daraus sehen wir die Teiler $1, X^3, X^6$. Es gibt aber noch zwei weitere Teiler, X^2 und X^4, die aus dieser Zerlegung nicht hervorgehen. (siehe 5E9).

§**5Eb. Primelemente.** Aus $\mathbb{N}$ kennen wir folgende nützliche Eigenschaft: Wenn eine Primzahl p ein Produkt ab teilt, dann teilt p auch mindestens einen der Faktoren a oder b. Diese Eigenschaft erheben wir nun zur Definition:

Definition 5E13. Ein Element $a \in R \setminus R^\times$ heißt *prim* wenn gilt:

$$\text{Für alle } b, c \in R \text{ folgt aus } a \mid bc \text{ stets } a \mid b \text{ oder } a \mid c.$$

Beispiel 5E14. In jedem Integritätsring ist 0 prim, denn $0 \mid ab$ ist gleichbedeutend mit $ab = 0$, und dies bedeutet $a = 0$ oder $b = 0$, also $0 \mid a$ oder $0 \mid b$.

Proposition 5E15. *In einem Integritätsring ist jedes Primelement $p \neq 0$ irreduzibel.*

BEWEIS. Angenommen es gilt $p = ab$. Dann $p \mid a$ oder $p \mid b$. Nehmen wir $p \mid a$ an, also $b = pc$ für ein $c \in R$. Damit gilt $p = ab = pcb$, und nach Kürzung $1 = bc$, also $b \in R^\times$. Analog folgt aus $p \mid b$, dass $a \in R^\times$. Für jede Zerlegung $p = ab$ folgt also $a \sim 1$ oder $b \sim 1$. Beides kann nicht gelten, da $p = ab$ sonst invertierbar wäre, im Widerspruch zur Voraussetzung, dass p prim ist. □

Die Umkehrung gilt im Allgemeinen nicht, wie unser Beispiel 5B14 zeigt:

Beispiel 5E16. In $R = \mathbb{Z}/_2[X^2, X^3]$ ist X^2 irreduzibel, denn die Zerlegung $X^2 = X \cdot X$ steht in R nicht mehr zur Verfügung. Hingegen ist X^2 in R nicht prim: es gilt $X^2 \mid X^3 \cdot X^3$, denn $X^6 = X^2 \cdot X^4$, aber in R gilt nicht $X^2 \nmid X^3$. (Siehe Übung 5H10.)

§**5Ec. Die Lemmata von Gauß und Euklid.** Wir wollen zeigen, dass in einem Hauptidealring jedes irreduzible Element prim ist. Wir beginnen mit folgender Beobachtung:

Lemma 5E17 (Gauß)**.** *Sind (a) und (b) teilerfremd, dann folgt aus $a \mid bc$ stets $a \mid c$.*

BEWEIS. Teilerfremdheit der Ideale (a) und (b) bedeutet $(a)+(b) = 1$, also $au+bv = 1$ für gewisse Elemente $u, v \in R$. Die Teilbarkeit $a \mid bc$ bedeutet $aa' = bc$ für ein $a' \in R$. Daraus folgt $c = (au+bv)c = auc+bcv = a(uc+a'v)$, also $a \mid c$. □

Lemma 5E18 (Euklid)**.** *In einem Hauptidealring ist jedes irreduzible Element prim.*

BEWEIS. Sei R ein Hauptidealring und sei $p \in R$ irreduzibel. Insbesondere ist p nicht invertierbar (5E4) und es bleibt zu zeigen, dass aus $p \mid ab$ folgt $p \mid a$ oder $p \mid b$. Es existiert $d \in \mathrm{GGT}(p,a)$, denn es gibt ein Element $d \in R$ sodass $(d) = (p) + (a)$ wie in Satz 5D5. Insbesondere gilt $d \mid p$, und da p irreduzibel ist, folgt $d \sim 1$ oder $d \sim p$.

- Wenn $d \sim p$, dann gilt wegen $d \mid a$ auch $p \mid a$.
- Wenn $d \sim 1$, dann gilt $p \mid b$ nach dem Lemma von Gauß. □

Satz 5E19. *Sei R ein Integritätsring, in dem jedes irreduzible Element prim ist. Dann sind Zerlegungen in irreduzible Faktoren eindeutig.*

BEWEIS. Wir betrachten zwei Zerlegungen $a = up_1 \cdots p_n = vq_1 \cdots q_m$ mit $u, v \in R^\times$ invertierbar und $p_1, \ldots, p_n, q_1, \ldots, q_m \in R$ irreduzibel. Wir haben zu zeigen, dass $n = m$ gilt und nach geeigneter Umordnung $p_1 \sim q_1, \ldots, p_n \sim q_n$.

Wir können $n \leq m$ annehmen und führen Induktion über n. Wenn $n = 0$, dann ist a invertierbar und damit auch $m = 0$. Angenommen es gilt $n \geq 1$, und die Eindeutigkeit gilt alle Zerlegungen der Länge $< n$. Da p_n nicht nur irreduzibel sondern auch prim ist, folgt $p_n \mid q_k$ für ein $k = 1, \ldots, m$. Nach Umordnung können wir $k = m$ annehmen, also $p_n \mid q_m$. Da auch q_m irreduzibel ist, folgt entweder $p_n \sim 1$ oder $p_n \sim q_m$. Ersteres ist ausgeschlossen, also bleibt nur $p_n \sim q_m$, das heißt $q_m = v' p_n$ mit $v \in R^\times$. Nach Kürzen folgt hieraus $up_1 \cdots p_{n-1} = (vv')q_1 \cdots q_{m-1}$. Nach Induktionsvoraussetzung folgt hieraus $n-1 = m-1$ und nach Umordnung $p_1 \sim q_1, \ldots, p_{n-1} \sim q_{n-1}$. □

§**5Ed. Noethersche Ringe.** Wir befassen uns schließlich mit der Frage, ob sich jedes Element $a \in R$ überhaupt in ein Produkt von irreduziblen Faktoren zerlegen lässt.

Proposition 5E20. *Wenn $a_0 \in R$ keine Zerlegung in irreduzible Faktoren erlaubt, dann gibt es eine unendliche aufsteigende Kette von Idealen $(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$ in R.*

BEWEIS. Da $a_0 \in R$ keine Zerlegung in irreduzible Faktoren erlaubt, ist a_0 weder invertierbar noch irreduzibel. Demnach existiert eine echte Zerlegung $a_0 = a_1 a_1'$ mit $a_1, a_1' \notin R^\times$. Mindestens einer der beiden Faktoren a_1, a_1' erlaubt keine Zerlegung in irreduzible Faktoren. Nehmen wir an, dies sei a_1. Wegen $a_1 \not\sim a_0$ erhalten wir so $(a_0) \subsetneq (a_1)$. Dieses Argument kann nun iteriert werden: Jede Kette $(a_0) \subsetneq \dots \subsetneq (a_n)$ bei der a_n keine Zerlegung in irreduzible Faktoren erlaubt, lässt sich verlängern zu einer Kette $(a_0) \subsetneq \dots \subsetneq (a_n) \subsetneq (a_{n+1})$ sodass auch a_{n+1} keine Zerlegung in irreduzible Faktoren erlaubt. Mit Auswahlaxiom und Rekursionssatz folgt daraus die Existenz einer unendlichen Kette $(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$. □

Es gibt Ringe, in denen unendliche aufsteigende Ketten von Idealen möglich sind (Übung 5H23). In vielen Anwendungen hat sich daher folgende Begriffsbildung bewährt:

Definition 5E21. Ein Ring R heißt *noethersch*, wenn jede aufsteigende Kette $I_0 \subset I_1 \subset I_2 \subset \dots$ von Idealen in R stationär ist, also $I_n = I_{n+1} = I_{n+2} = \dots$ ab einem gewissen $n \in \mathbb{N}$ gilt.

Diese Bedingung nennt man auch *aufsteigende Kettenbedingung*, auf englisch *ascending chain condition*, kurz *ACC*. Damit gelangen wir zu folgender Charakterisierung:

Satz 5E22. *Ein Integritätsring R ist genau dann faktoriell wenn folgendes gilt:*

1. *Im Ring R ist jedes irreduzible Element prim.*
2. *Der Ring R erfüllt die aufsteigende Kettenbedingung für Hauptideale.*

BEWEIS. "⇒" Nehmen wir an, p sei irreduzibel und es gelte $p \mid ab$, also $pc = ab$. Da R als faktoriell vorausgesetzt wird, existieren Zerlegungen $a = a_1 \cdots a_n$ und $b = b_1 \cdots b_m$ und $c = c_1 \cdots c_k$ in irreduzible Faktoren. Dann gilt $pc_1 \cdots c_k = a_1 \cdots a_n \cdot b_1 \cdots b_m$. Aufgrund der Eindeutigkeit der Zerlegung muss der Faktor p auch auf der rechten Seite auftreten, also $p \sim a_i$ für ein $i = 1, \dots, n$ oder $p \sim b_j$ für ein $j = 1, \dots, m$. Im ersten Fall gilt $p \mid a$, im zweiten Fall gilt $p \mid b$. Wir schließen daraus, dass p prim ist.

In einem faktoriellen Ring R hat jedes Element $a \in R$ nur endlich viele Teiler (5E10), wobei wir assoziierte Teiler nicht unterscheiden wollen. Ist nämlich $a = p_1 \cdots p_n$ eine Zerlegung in irreduzible Faktoren, so ist für jede Teilmenge $J \subset \{1, \dots, n\}$ das Element $a_J = \prod_{j \in J} p_j$ ein Teiler von a und jeder Teiler von a ist zu einem solchen a_J assoziiert (5E10). Demnach muss jede strikt aufsteigende Kette $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$ spätestens nach n Schritten abbrechen.

"⇐" Die aufsteigende Kettenbedingung für Hauptideale garantiert, dass jedes Element eine Zerlegung in irreduzible Faktoren erlaubt (5E20) und wegen der Primalitätsbedingung ist diese Zerlegung eindeutig (5E19). □

§**5Ee. Hauptidealringe sind faktoriell.** Die Vereinigung von Idealen I_0, I_1 in R ist im Allgemeinen kein Ideal in R. Zum Beispiel enthält $(3) \cup (2)$ zwar 3 und -2 aber nicht $3 - 2 = 1$. Trivialerweise ist die Vereinigung $I_0 \cup I_1$ ein Ideal, wenn $I_0 \subset I_1$ gilt. Diese Aussage gilt auch für Vereinigungen unendlicher Ketten von Idealen:

Lemma 5E23. *Ist $I_0 \subset I_1 \subset I_2 \subset \dots$ eine aufsteigende Kette von Idealen in einem Ring R, dann ist ihre Vereinigung $I = \bigcup_{n\in\mathbb{N}} I_n$ auch ein Ideal in R.*

BEWEIS. Offenbar gilt $0 \in I$. Zu $a,b \in I$ gilt $a \in I_k$ und $b \in I_\ell$ für gewisse Indizes $k,\ell \in \mathbb{N}$, und aus der Kettenbedingung folgt $a,b \in I_n$ für $n = \max\{k,\ell\}$. Da I_n ein Ideal ist, gilt $a+b \in I_n$ und $ra \in I_n$ für alle $r \in R$, und damit auch $a+b \in I$ und $ka \in I$. □

Satz 5E24. *Jeder Hauptidealring ist noethersch.*

BEWEIS. Sei $I_0 \subset I_1 \subset I_2 \subset \dots$ eine aufsteigende Kette von Idealen in R. Die Vereinigung $I = \bigcup_{n\in\mathbb{N}} I_n$ ist dann ebenfalls ein Ideal in R. Ist R ein Hauptidealring, dann gilt $I = (a)$ für ein $a \in R$. Dann aber muss $a \in I_n$ für ein $n \in \mathbb{N}$ gelten. Es folgt dann $(a) \subset I_n \subset I_m \subset (a)$ für alle $m \geq n$, also $I_m = (a)$ für alle $m \geq n$, das heißt die Kette ist stationär. □

Wir fassen unsere Ergebnisse wie folgt zusammen:

Satz 5E25. *Jeder euklidische Ring ist Hauptidealring. Jeder Hauptidealring ist faktoriell.*

BEWEIS. Jeder euklidische Ring ist ein Hauptidealring (5D4). Jeder Hauptidealring ist noethersch (5E24), daher erlaubt jedes Element eine Zerlegung in irreduzible Faktoren (5E20). Nach dem Lemma von Euklid (5E18) ist in einem Hauptidealring jedes irreduzible Element prim. Daher ist die Zerlegung in irreduzible Faktoren eindeutig (5E19). □

Korollar 5E26. *Der Ring $\mathbb{Z}$ der ganzen Zahlen ist faktoriell.* □

Korollar 5E27. *Der Ring $\mathbb{Z}[i]$ der gaußschen Zahlen ist faktoriell.* □

Korollar 5E28. *Der Polynomring $K[X]$ über jedem Körper K ist faktoriell.* □

Dies rechtfertigt die üblichen Primalitätsargumente für den Ring $\mathbb{Z}$, die jeder aus der Schule kennen dürfte (die dort aber zumeist ohne Beweis nur empirische Beobachtungen blieben). Dank unseres allgemeinen Ergebnisses stehen uns diese Techniken gleich in vielen weiteren Ringen zur Verfügung. Im nächsten Kapitel werden wir diese auf $\mathbb{Z}[X]$ ausdehnen, und allgemeiner auf jeden Polynomring $R[X]$ über einem faktoriellen Ring R.

§5F. Teilerfremdheit und Invertierbarkeit

§5Fa. Teilerfremdheit. Wir erinnern daran, dass zwei Ideale $I,J \lhd R$ teilerfremd heißen, wenn $I+J = R$ gilt. Diese Sprechweise erweitern wir nun auf Elemente $a,b \in R$:

Definition 5F1. In einem Integritätsring R nennen wir zwei Elemente $a,b \in R$ *teilerfremd* wenn $1 \in \mathrm{GGT}(a,b)$ gilt. Dies entspricht der Bedingung $\mathrm{GGT}(a,b) = R^\times$.

- In einem faktoriellen Ring sind zwei Elemente genau dann teilerfremd, wenn ihre Primfaktorzerlegungen keine gemeinsamen Primfaktoren enthalten (5E10).
- Ist R ein Hauptidealring, ist $(a)+(b) = (d)$ äquivalent zu $d \in \mathrm{GGT}(a,b)$. Demnach sind $a,b \in R$ genau dann teilerfremd, wenn ihre Ideale $(a),(b) \lhd R$ teilerfremd sind.
- Ist R ein euklidischer Ring, dann kann diese Bedingung mit Hilfe des euklidischen Algorithmus getestet werden, indem man einen ggT von a und b ausrechnet.

§**5Fb. Invertierbarkeit.** Es gilt folgender Zusammenhang zwischen Teilerfremdheit und Invertierbarkeit:

Proposition 5F2. *Sei R ein Ring. Für je zwei Elemente $a,b \in R$ sind äquivalent:*

1. *Die Restklasse $\mathfrak{cl}(a)$ ist invertierbar im Quotientenring $R/(b)$.*
2. *Es gilt $au \equiv 1 \mod (b)$ für ein $u \in R$.*
3. *Es gilt $au+bv = 1$ für gewisse $u,v \in R$.*
4. *Es gilt $(a)+(b) = 1$, das heißt, die Ideale (a) und (b) sind teilerfremd.* □

Korollar 5F3. *Ist R ein Hauptidealring, dann ist $\mathfrak{cl}(a)$ genau dann in $R/(b)$ invertierbar, wenn die Elemente $a,b \in R$ teilerfremd sind.* □

Beispiel 5F4. In $\mathbb{Z}/_n$ ist $\mathfrak{cl}(a)$ genau dann invertierbar, wenn a und n teilerfremd sind.

Beispiel 5F5. Sei K ein Körper und $P,Q \in K[X]$. Im Quotientenring $K[X]/(P)$ ist $\mathfrak{cl}(Q)$ genau dann invertierbar, wenn P und Q teilerfremd sind.

Ist R kein Hauptidealring, so gilt dieses einfache Kriterium nicht mehr:

Beispiel 5F6. In $\mathbb{Z}[X]$ sind 2 und X teilerfremd, aber 2 ist nicht invertierbar in $\mathbb{Z} = \mathbb{Z}[X]/(X)$.

§**5Fc. Invertierung nach Euklid-Bézout.** Im Falle eines euklidischen Rings R kann man die Invertierbarkeit von $\mathfrak{cl}(a)$ in $R/(b)$ wie folgt testen und zugleich ein Inverses ausrechnen, falls ein solches existiert:

Satz 5F7 (Invertierung nach Euklid-Bézout)**.** *Seien $a,b \in R$ Elemente in einem euklidischen Ring. Dann ist $\mathfrak{cl}(a)$ genau dann in $R/(b)$ invertierbar, wenn a und b in R teilerfremd sind, also $1 \in \mathrm{GGT}(a,b)$ gilt. In diesem Fall berechnet der folgende Algorithmus 5 ein Inverses $u \in R$ sodass $au \equiv 1 \mod (b)$.*

Algorithmus 5 Invertierung nach Euklid-Bézout

Eingabe: zwei Elemente $a_0, b_0 \in R$ in einem euklidischen Ring R
Ausgabe: zwei Elemente $a,u \in R$ so dass $a \in \mathrm{GGT}(a_0,b_0)$ und $a_0u \equiv a \mod (b_0)$.

$\begin{pmatrix} a & u \\ b & s \end{pmatrix} \leftarrow \begin{pmatrix} a_0 & 1 \\ b_0 & 0 \end{pmatrix}$ // Invariante $\begin{cases} a \equiv a_0u \mod (b) \\ b \equiv a_0s \mod (b) \end{cases}$

while $b \neq 0$ **do**

$q \leftarrow a \operatorname{quo} b,\ \begin{pmatrix} a & u \\ b & s \end{pmatrix} \leftarrow \begin{pmatrix} b & s \\ a-qb & u-qs \end{pmatrix}$ // Invariante $\begin{cases} a \equiv a_0u \mod (b) \\ b \equiv a_0s \mod (b) \end{cases}$

end while

return (a,u) // $a \in \mathrm{GGT}(a_0,b_0)$ und $a \equiv a_0u$

BEWEIS. Dies ist eine Spezialisierung von Algorithmus 4. □

§5G. Primideale und maximale Ideale

Proposition 5G1 (Primideale)**.** *Sei R ein Ring. Für ein Ideal $I \lhd R$ sind äquivalent:*

1. *Der Quotient R/I ist ein Integritätsring.*

2. *Es gilt $I \neq R$ und aus $ab \in I$ folgt stets $a \in I$ oder $b \in I$.*

In diesem Fall nennen wir I ein Primideal *von R.*

BEWEIS. Der Quotientenring R/I ist genau dann der Nullring wenn $I = R$ gilt, und diesen Fall schließen wir sowohl in (1) als auch in (2) ausdrücklich aus. Im Quotienten R/I gilt $\mathfrak{cl}(a) = 0$ genau dann, wenn $a \in I$. Nullteiler $\mathfrak{cl}(a), \mathfrak{cl}(b) \neq 0$ mit $\mathfrak{cl}(ab) = 0$ in R/I entsprechen Elementen $a, b \in R$ mit $a, b \notin I$ aber $ab \in I$. □

Beispiel 5G2. In $\mathbb{Z}$ ist (2) ein Primideal. Dies kann man auf zwei Weisen sehen:

1. Der Quotient $Z/(2)$ ist ein Integritätsring.
2. Es gilt $(2) \neq \mathbb{Z}$ und aus $ab \in (2)$ folgt stets $a \in (2)$ oder $b \in (2)$.

Hingegen ist (6) kein Primideal, wie man auf die gleiche Weise sieht.

Proposition 5G3. *Genau dann ist $p \in R$ ein Primelement wenn $(p) \lhd P$ ein Primideal ist.*

BEWEIS. Primelemente sind nach Definition nicht invertierbar, und $p \notin R^\times$ ist gleichbedeutend mit $(p) \neq R$. Die behauptete Äquivalenz ergibt sich aus folgendem Diagramm:

$$\begin{array}{ccc} p \mid ab & \overset{p \text{ prim}}{\Longrightarrow} & p \mid a \vee p \mid b \\ \Updownarrow & & \Updownarrow \\ ab \in (p) & \overset{(p) \text{ prim}}{\Longrightarrow} & a \in (p) \vee b \in (p) \end{array}$$

Ist $p \in R$ ein Primelement und $a, b, \in R$, dann gilt:

$$ab \in (p) \implies p \mid ab \implies p \mid a \vee p \mid b \implies a \in (p) \vee b \in (p).$$

Ist umgekehrt $(p) \lhd R$ ein Primideal und $a, b \in R$, dann gilt:

$$p \mid ab \implies ab \in (p) \implies a \in (p) \vee b \in (p) \implies p \mid a \vee p \mid b. \qquad \square$$

Sind $R \subset S$ Integritätsringe, dann können die Begriffe "prim" und "irreduzibel" in R und S sehr verschieden ausfallen (Übung 5H4). Für Polynomringe ist alles leichter:

Korollar 5G4. *Genau dann ist $p \in R$ prim in R, wenn p prim in $R[X]$ ist.*

BEWEIS. Für die Primalität von $p \in R$ betrachten wir das Ideal $(p)_R = pR$ in R und das Ideal $(p)_{R[X]} = pR[X]$ in $R[X]$. Der surjektive Ringhomomorphismus $\varphi\colon R \to R/pR$ setzt sich zu einem surjektiven Ringhomomorphismus $\Phi\colon R[X] \to (R/pR)[X]$ fort gemäß

$$\Phi(a_0 + \cdots + a_n X^n) = \varphi(a_0) + \cdots + \varphi(a_n) X^n.$$

Der Kern von Φ ist demnach das Ideal $pR[X]$. Hieraus erhalten wir den Isomorphismus $R[X]/pR[X] \xrightarrow{\sim} (R/pR)[X]$. Somit ist $pR \lhd R$ genau dann ein Primideal wenn $pR[X] \lhd R[X]$ ein Primideal ist. Aufgrund der vorangegangenen Proposition bedeutet das: genau dann ist $p \in R$ ein Primelement in R wenn p ein Primelement in $R[X]$ ist. □

Der Beweis mittels Idealen und Quotientenringen besticht durch Kürze und Eleganz; der zu zahlende Preis ist ein etwas höherer Abstraktionsgrad. Man kann diesen abstrakten Beweis auch in eine konkrete Rechnung übersetzen; der Preis ist dann umgekehrt eine etwas längere Ausführung:

ALTERNATIVER BEWEIS. Wir nehmen zur Vereinfachung an, dass R ein Integritätsring ist. Dann gilt insbesondere $R[X]^\times = R^\times$, somit ist die Bedingung $p \notin R^\times$ äquivalent zu $p \notin R[X]^\times$. Es bleibt die Teilbarkeitsbedingung nachzuweisen.

"$\Leftarrow$" Angenommen für alle $A, B \in R[X]$ folgt aus $p \mid AB$ stets $p \mid A$ oder $p \mid B$ in $R[X]$, also existiert $A' \in K[X]$ mit $pA' = A$ oder $B' \in K[X]$ mit $pB' = B$. Sind nun $A, B \in R$, so muss aus Gradgründen auch $A' \in R$ bzw. $B' \in R$ gelten. Also folgt für alle $A, B \in R$ aus $p \mid AB$ stets $p \mid A$ oder $p \mid B$ in R.

"$\Rightarrow$" Angenommen für alle $a, b \in R$ folgt aus $p \mid ab$ stets $p \mid a$ oder $p \mid b$ in R. Seien nun Polynome $A = \sum_i a_i X^i$ und $B = \sum_j b_j X^j$ in $R[X]$ gegeben, und sei $AB = \sum_k c_k X^k$ ihr Produkt, wobei $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. Wir haben zu zeigen, dass aus $p \mid AB$ stets $p \mid A$ oder $p \mid B$ in $R[X]$ gilt. Angenommen $p \nmid A$ und $p \nmid B$. Dann gibt es einen Index s mit $p \nmid a_s$; wir wählen s minimal. Ebenso gibt es einen Index t mit $p \nmid b_t$; wir wählen auch t minimal. In der Summe $c_{s+t} = \sum_{i=0}^{s+t} a_i b_{s+t-i}$ sind bis auf $a_s b_t$ alle Summanden durch p teilbar, denn für $i < s$ gilt $p \mid a_i$ und für $i > s$ gilt $p \mid b_{s+t-i}$. Aus $p \nmid a_s$ und $p \nmid b_t$ folgt $p \nmid a_s b_t$, denn p ist prim in R. Hieraus folgt $p \nmid c_{s+t}$ und somit $p \nmid AB$. □

Beispiel 5G5. In $\mathbb{Z}[X]$ ist das Ideal (2) prim, denn $\mathbb{Z}[X]/(2) \cong \mathbb{Z}/_2[X]$ ist nullteilerfrei. Ebenso ist das Ideal (X) prim, denn der Quotientenring $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ ist nullteilerfrei. Schließlich ist auch $(2,X)$ prim, denn $\mathbb{Z}[X]/(2,X) \cong \mathbb{Z}/_2$ ist sogar ein Körper.

Proposition 5G6 (maximale Ideale)**.** *Sei R ein Ring. Für ein Ideal $I \subset R$ sind äquivalent:*

1. *Der Quotient R/I ist ein Körper.*
2. *Für jedes Ideal $J \lhd R$ mit $I \subset J \subset R$ gilt entweder $I = J$ oder $J = R$.*

In diesem Fall nennen wir I ein maximales Ideal *von R.*

BEWEIS. Die Ideale $I \subset J \subset R$ entsprechen bijektiv den Idealen $\bar{J} \subset R/I$. Der Ring R/I ist genau dann ein Körper, wenn er nur die beiden trivialen Ideale hat (3D11). □

Beispiel 5G7. In $\mathbb{Z}[X]$ ist $(2,X)$ maximal, denn $\mathbb{Z}[X]/(2,X) \cong \mathbb{Z}/_2$ ist ein Körper. Hingegen ist (X) zwar prim aber nicht maximal, denn $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ ist kein Körper. Dass (X) nicht maximal ist, sieht man auch an der Kette $(X) \subsetneq (2,X) \subsetneq \mathbb{Z}[X]$.

Satz 5G8. *In einem Hauptidealring ist jedes Primideal $I \neq (0)$ maximal.*

BEWEIS. Es gilt $I = (p)$ und $p \neq 0$ ist prim. Für jedes Ideal J mit $(p) \subset J \subset R$, gilt $J = (q)$ für ein $q \in R$ und somit $q \mid p$. Da p irreduzibel ist (5E15), folgt entweder $q \sim 1$ oder $q \sim p$, also entweder $J = R$ oder $J = (p)$. □

Korollar 5G9. *Sei R ein Hauptidealring und $p \in R^*$. Dann ist der Quotientenring $R/(p)$ genau dann ein Körper wenn p irreduzibel ist.*

BEWEIS. "$\Leftarrow$" Nach dem Lemma von Euklid (5E18) ist in einem Hauptidealring jedes irreduzible Element prim. Demnach ist $(p) \subset R$ ein Primideal und somit maximal.

"$\Rightarrow$" Ist $R/(p)$ ein Körper, dann ist (p) maximal, also insbesondere prim. Damit ist p ein Primelement (5G3). Da wir $p \neq 0$ voraussetzen, ist p auch irreduzibel (5E15). □

Beispiel 5G10. Der Quotientenring $\mathbb{Z}/p\mathbb{Z}$ ist genau dann ein Körper wenn p irreduzibel ist, also eine Primzahl ($\neq 0$).

Beispiel 5G11. Sei K ein Körper und $P \in K[X]$ ein Polynom über K. Dann ist $K[X]/(P)$ genau dann ein Körper wenn P irreduzibel in $K[X]$ ist.

In diesen Beispielen sind die Ringe $\mathbb{Z}$ und $K[X]$ euklidisch. Inverse können daher mittels des euklidischen Algorithmus berechnet werden, wie in §5Fc erklärt.

Satz 5G12. *Jeder Ring R mit $1 \neq 0$ besitzt mindestens ein maximales Ideal $m \lhd R$.*

Etwas allgemeiner gilt: Sei R ein Ring mit $1 \neq 0$ und sei $\mathfrak{a} \lhd R$ ein Ideal mit $\mathfrak{a} \neq R$. Dann existiert ein maximales Ideal $m \lhd R$, das $\mathfrak{a}$ enthält.

BEWEIS. Sei S die Menge aller Ideale $I \lhd R$ mit $\mathfrak{a} \subset I \subsetneq R$. Diese Menge ist nicht-leer, wegen $\mathfrak{a} \in S$, und durch Inklusion geordnet. Wir wollen das Zornsche Lemma anwenden, um die Existenz eines maximalen Elements zu zeigen. Zu jeder Kette $T \subset S$ ist $J := \bigcup_{I \in T} I$ ein Ideal, denn für je zwei Elemente $x, y \in J$ existiert $I \in T$ mit $x, y \in I$. Da I ein Ideal ist, gilt $x + y \in I$ und $rx \in I$ für alle $r \in R$, und damit auch $x + y \in J$ und $rx \in J$. Es gilt $J \neq R$, denn andernfalls wäre $1 \in J$ und somit $1 \in I$ für ein $I \in T$. Demnach ist J in S eine obere Schranke der Kette T. Das Zornsche Lemma versichert uns nun die Existenz eines maximalen Elements in S. □

§5H. Übungen und Ergänzungen

§5Ha. Prim versus irreduzibel.

Übung 5H1. Für $n \in \mathbb{N}$ definieren wir $n!$ rekursiv durch

$$0! := 1 \quad \text{und} \quad n! := (n-1)! \cdot n \quad \text{für } n \geq 1.$$

Für $0 \leq k \leq n$ definieren wir den *Binomialkoeffizienten* durch

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}.$$

Schließlich setzen wir $\binom{n}{k} := 0$ falls $k < 0$ oder $k > n$.

1. Man zeige die Regel des Pascalschen Dreiecks $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.
   Man folgere daraus, dass $\binom{n}{k}$ in $\mathbb{Z}$ liegt.
2. Sei $p \in \mathbb{N}$ unzerlegbar. Für $0 < k < p$ zeige man, dass p teilt $\binom{p}{k}$.
   Welches Ergebnis benutzt man hier? Teilt n auch $\binom{n}{k}$ wenn n zerlegbar ist?

Übung 5H2. Welches sind die irreduziblen Elemente in $\mathbb{C}[X]$. Und in $\mathbb{R}[X]$?

Übung 5H3. Sei R ein Integritätsring und $a \in R$. Ist $(X - a)$ in $R[X]$ irreduzibel? prim?

Übung 5H4. Wie verhalten sich die Begriffe "prim" und "irreduzibel" bezüglich Ringerweiterung bzw. Einschränkung? Genauer: Seien $R \subset S$ Integritätsringe und sei $a \in R$.

1. Sei a irreduzibel in R. Ist a dann auch irreduzibel in S?
2. Sei a irreduzibel in S. Ist a dann auch irreduzibel in R?
3. Sei a prim in R. Ist a dann auch prim in S?
4. Sei a prim in S. Ist a dann auch prim in R?

Zu jedem dieser vier Fälle gebe man entweder einen Beweis oder ein Gegenbeispiel.

Übung 5H5. Seien $R \subset S$ Integritätsringe, sodass für alle $a, b \in R$ und $c \in S$ aus $a = bc$ stets $c \in R$ folgt, d.h. die Teilbarkeitsrelationen $b \underset{R}{\mid} a$ und $b \underset{S}{\mid} a$ stimmen für alle $a, b \in R$ überein.

1. Gilt die Voraussetzung für $\mathbb{Z} \subset \mathbb{Q}$? für $\mathbb{R}[X] \subset \mathbb{C}[X]$?
2. Gilt die Voraussetzung für $R \subset R[X]$ über jedem Integritätsring R?
3. Aus obiger Voraussetzung folgere man $R \cap S^\times = R^\times$.

Man untersuche, wie sich die Begriffe "prim" und "irreduzibel" bezüglich solcher Ringerweiterung verhalten: Zu jeder der vier Fragen aus Übung 5H4 gebe man entweder einen Beweis oder ein Gegenbeispiel.

§**5Hb. Hauptidealringe.** Nicht alle Ringe sind Hauptidealringe:

Übung 5H6. Man zeige, dass $\mathbb{Z}[X]$ kein Hauptidealring ist.
Zum Beispiel ist das Ideal $(2,X)$ in $\mathbb{Z}[X]$ kein Hauptideal.
Man zeige $\mathrm{GGT}(2,X) = \{\pm 1\}$. Gilt $1 = 2P + XQ$ für geeignete $P, Q \in \mathbb{Z}[X]$?

Übung 5H7. Für einen Polynomring $K[X]$ über einem Integritätsring K sind äquivalent:

1. Der Polynomring $K[X]$ ist ein euklidischer Ring.
2. Der Polynomring $K[X]$ ist ein Hauptidealring.
3. Der Grundring K ist ein Körper.

§**5Hc. Faktorzerlegung in kommutativen Monoiden.** Das Monoid $(\mathbb{N}, \cdot)$ der natürlichen Zahlen bezüglich Multiplikation erfreut sich bemerkenswert schöner Eigenschaften. Dass diese nicht selbstverständlich sind, illustrieren folgende Beispiele.

Übung 5H8. Für jedes $k \in \mathbb{N}$ ist $M_k = 1 + k\mathbb{N}$ ein Untermonoid von $(\mathbb{N}, \cdot)$. $M_0 = \{1\}$ ist das triviale Monoid. In $M_1 = \{1,2,3,4,\dots\}$ lässt sich jedes Element eindeutig in irreduzible Faktoren zerlegen. Gilt dies auch in $M_2 = \{1,3,5,7,\dots\}$? und in $M_3 = \{1,4,7,10,\dots\}$? Und in M_k für $k \geq 4$? (Zur Vertiefung siehe R.D. James, I. Niven: *Unique factorization in multiplicative systems.* Proc. Amer. Math. Soc. 5 (1954), 834–838.)

Übung 5H9. In der Topologie untersucht man die Menge $\mathscr{S}$ der zusammenhängenden geschlossenen Flächen bis auf Homöomorphie. Mit der verbundenen Summe $\sharp$ wird diese ein kommutatives Monoid, neutrales Element ist die Sphäre $\mathbb{S}^2$. Lässt sich jede Fläche bezüglich $\sharp$ in unzerlegbare Summanden zerlegen? Ist diese Zerlegung eindeutig?

Zur Erinnerung — Die Struktur des Monoids $(\mathscr{S}, \sharp)$ folgt aus dem Klassifikationssatz: Die Euler-Charakteristik $\chi\colon \mathscr{S} \to \mathbb{Z}$ erfüllt $\chi(A\sharp B) = \chi(A) + \chi(B) - 2$. Die Menge $\mathscr{S}$ besteht aus den orientierbaren Flächen $F_0 = \mathbb{S}^2, F_1, F_2, \dots$ mit $\chi(F_k) = 2 - 2k$, und den nichtorientierbaren Flächen $G_0, G_1, G_2, \dots$ mit $\chi(G_k) = 1 - k$. Die Abbildung $h = 2 - \chi\colon \mathscr{S} \to \mathbb{N}$ erfüllt also $h(A\sharp B) = h(A) + h(B)$ und es gilt $h(A) = 0$ genau dann wenn $A = \mathbb{S}^2$. Die Summe $A\sharp B$ ist genau dann orientierbar, wenn beide Summanden A und B orientierbar sind. Damit ist $(\mathscr{S}, \sharp)$ isomorph zu $\{\ (1,2k), (0,1+k) \mid k \in \mathbb{N}\ \}$ mit $(a,m)\sharp(b,n) = (ab, m+n)$.

§**5Hd. Ringe mit nicht-eindeutiger Faktorzerlegung.** Wir beginnen mit einfachen Beispielen von Ringen, die keine eindeutige Zerlegung in irreduzible Elemente gestatten:

Übung 5H10. Ein faktorieller Ring kann durchaus nicht-faktorielle Unterringe haben. Das ist selbst in einem Polynomring möglich:

1. Man zeige, dass $R := \{\ P \in \mathbb{Q}[X] \mid P'(0) = 0\ \}$ ein Unterring von $\mathbb{Q}[X]$ ist.
   Es ist $R = \mathbb{Q}[X^2, X^3]$ der von $\{X^2, X^3\}$ über $\mathbb{Q}$ erzeugte Unterring.

2. Man bestimme die Gruppe $R^\times$ der in R invertierbaren Elemente.
3. Lässt sich jedes Element in R als Produkt irreduzibler Faktoren schreiben?
4. Sind die Polynome X^2 und X^3 im Ring R irreduzibel? Sind sie prim?
5. X^7 lässt sich in R nur auf eine Art in irreduzible Faktoren zerlegen, X^6 auf zwei.
6. Man gebe zwei Polynome in R an, die in R keinen größten gemeinsamen Teiler haben. (Hierbei ist "größer" wie immer im Sinne der Teilbarkeit zu verstehen.)

Übung 5H11. Sei $\mathbb{Q}[X,Y]$ der Polynomring in den Variablen X,Y über $\mathbb{Q}$. Hierin betrachten wir die "geraden" Polynome bezüglich der Punktsymmetrie in $(0,0)$:

1. Man zeige, dass $R = \{\, P \in \mathbb{Q}[X,Y] \mid P(-X,-Y) = P(X,Y) \,\}$ ein Unterring ist. Es ist $R = \mathbb{Q}[X^2, XY, Y^2]$ der von $\{X^2, XY, Y^2\}$ über $\mathbb{Q}$ erzeugte Unterring.
2. Man bestimme die Gruppe $R^\times$ der in R invertierbaren Elemente.
3. Sind die Polynome X^2, XY, Y^2 im Ring R irreduzibel? Sind sie prim?
4. Lässt sich jedes Element in R als Produkt irreduzibler Faktoren schreiben?
5. $X^{2n}Y^{2n}$ lässt sich auf $n+1$ verschiedene Arten in irreduzible Faktoren zerlegen.
6. Man gebe zwei Polynome $P,Q \in R$ an, so dass $\operatorname{GGT}(P,Q) = \emptyset$.

Übung 5H12. Die Gleichung $\sin^2 + \cos^2 = 1$ entspricht der Zerlegung

$$\sin \cdot \sin = (1+\cos)(1-\cos).$$

Um dies genauer zu untersuchen betrachten wir trigonometrische Polynome $f\colon \mathbb{R} \to \mathbb{R}$,

$$f(x) = a_0 + a_1\cos(x) + b_1\sin(x) + \cdots + a_n\cos(nx) + b_n\sin(nx),$$

mit $a_0, a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{R}$. Wir nennen n den *Grad* dieser Summe falls $a_n \neq 0$ oder $b_n \neq 0$. Für die leere Summe vereinbaren wir wie üblich $\deg 0 = -\infty$. Es gilt

$$f(x) = \sum_{k=-n}^{n} c_k e^{ikx}$$

mit $c_0 = a_0$ sowie $c_k = \frac{1}{2}(a_k - ib_k)$ und $c_{-k} = \overline{c_k} = \frac{1}{2}(a_k + ib_k)$ für $k = 1, \ldots, n$.

1. Die Menge R der trigonometrischen Polynome ist ein Unterring von $\mathbb{C}^\infty(\mathbb{R},\mathbb{R})$. Es ist $R = \mathbb{R}[\cos,\sin]$ der von $\{\cos,\sin\}$ über $\mathbb{R}$ erzeugte Unterring.
2. Jedes trigonometrische Polynom f bestimmt seine Koeffizienten. Der Grad $\deg\colon R \to \mathbb{N} \cup \{-\infty\}$ erfüllt $\deg(fg) = \deg(f) + \deg(g)$.
3. Hat R Nullteiler? Man bestimme die Gruppe $R^\times$ der in R invertierbaren Elemente.
4. Sind die Elemente $\sin$ und $1 \pm \cos$ in R irreduzibel? Sind sie prim?
5. Lässt sich jedes Element in R als Produkt irreduzibler Faktoren schreiben?
6. Man zeige, dass eine solche Zerlegung im Allgemeinen nicht eindeutig ist.

§5He. Der Ring $\mathbb{Z}[i]$ der gaußschen Zahlen.

Übung 5H13.

1. Die Menge $\mathbb{Z}[i] = \{\, a+bi \mid a,b \in \mathbb{Z} \,\}$ ist ein Unterring von $\mathbb{C}$.
2. Die Abbildung $N\colon \mathbb{Z}[i] \to \mathbb{N}$ mit $N(z) = z\bar{z}$ ist multiplikativ.
3. Es gilt $N(z) = 0$ genau dann wenn $z = 0$.
4. Es gilt $N(z) = 1$ genau dann wenn $z \in \mathbb{Z}[i]^\times$.
5. Jede komplexe Zahl $q \in \mathbb{C}$ erlaubt eine Näherung $z \in \mathbb{Z}[i]$ mit $|q-z|^2 \leq \frac{1}{2}$.
6. Man folgere daraus, dass $\mathbb{Z}[i]$ ein euklidischer Ring ist bezüglich der Norm N.

Dass der Ring $\mathbb{Z}[i]$ euklidisch ist, hat erstaunliche Konsequenzen für Primzahlen in $\mathbb{Z}$:

Übung 5H14. 1. Wenn $N(z)$ irreduzibel in $\mathbb{N}$ ist, dann ist z irreduzibel in $\mathbb{Z}[i]$.
2. Jede Primzahl $p \in \mathbb{Z}$ lässt sich auf höchstens eine Art als Summe von zwei Quadraten schreiben, das heißt, aus $p = a^2 + b^2 = c^2 + d^2$ folgt $\{a^2, b^2\} = \{c^2, d^2\}$. Man betrachte $p = (a+ib)(a-ib) = (c+id)(c-id)$ in $\mathbb{Z}[i]$.

Für die Primzahl 2 gilt $2 = 1^2 + 1^2$. Für die Primzahlen $3, 7, 11, \ldots$ gibt es keine solche Zerlegung. Andererseits gilt $5 = 1^2 + 2^2$ und $13 = 2^2 + 3^2$ und $17 = 1^2 + 4^2, \ldots$.

Satz (Zwei-Quadrate-Satz von Fermat)**.** *Keine Primzahl $p \in \mathbb{N}$ mit $p \equiv 3 \pmod 4$ lässt sich als Summe von zwei Quadraten schreiben. Zu jeder Primzahl $p \in \mathbb{N}$ mit $p \equiv 1 \pmod 4$ existiert genau ein Paar $a < b$ in $\mathbb{N}$ sodass $p = a^2 + b^2$.*

Übung 5H15. Für $p \equiv 3 \pmod 4$ ist $p = a^2 + b^2$ schon modulo 4 unmöglich.

Im Folgenden sei $p \in Z$ eine Primzahl mit $p \equiv 1 \pmod 4$.

Übung 5H16. 1. Es gibt $\xi \in \mathbb{Z}/_p$ mit $\xi^2 = -1$. *Hinweis:* In $\mathbb{Z}/_p$ vergleiche man $1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}$ und $\frac{p+1}{2} \cdots (p-2) \cdot (p-1)$ und berechne ihr Produkt.
2. In $\mathbb{Z}[i]$ zerfällt p in zwei irreduzible Faktoren, $p = (a+ib)(a-ib)$.
Hinweis: Aus $p \mid q^2 + 1$ in $\mathbb{Z}$ folgt $p \mid (q+i)(q-i)$ in $\mathbb{Z}[i]$.

Übung 5H17. Als Zusammenfassung ermittelt man aus den vorangegangenen Ergebnissen alle irreduziblen Elemente des Rings $\mathbb{Z}[i]$:

- Die Primzahl $2 \in \mathbb{N}$ zerfällt in $\mathbb{Z}[i]$ in das Produkt $2 = (1+i)(1-i)$.
Die Elemente $1+i$ und $1-i$ sind irreduzibel in $\mathbb{Z}[i]$ und zueinander assoziiert.
- Jede Primzahl $p \in \mathbb{N}$ mit $p \equiv 1 \pmod 4$ zerfällt in $\mathbb{Z}[i]$ in $p = (a+ib)(a-ib)$ mit $a < b$ in $\mathbb{N}$. Die Elemente $a \pm ib$ sind irreduzibel in $\mathbb{Z}[i]$ und nicht assoziiert.
- Jede Primzahl $p \in \mathbb{N}$ mit $p \equiv 3 \pmod 4$ bleibt irreduzibel in $\mathbb{Z}[i]$.

Diese Liste ist redundanzfrei und vollständig: Jedes irreduzible Element in $\mathbb{Z}[i]$ ist assoziiert zu genau einem irreduziblen Element aus dieser Liste. (In Kapitel 6 führen wir hierzu den allgemeinen Begriff ein und nennen dies ein *Repräsentantensystem irreduzibler Elemente*.)

§**5Hf. Quadratische Erweiterungen von $\mathbb{Z}$.** Der Ring $\mathbb{Z}[i]$ ist ein schönes und wichtiges Beispiel eines euklidischen Rings. Er ist das erste Mitglied einer unendlichen Familie von Ringen der Form $\mathbb{Z}[\xi] \subset \mathbb{C}$, wobei $\xi \in \mathbb{C}$ eine quadratische Gleichung $\xi^2 + c_1\xi + c_0 = 0$ mit $c_0, c_1 \in \mathbb{Z}$ erfüllt. Je nach Wahl von ξ entstehen Ringe mit besonderen Eigenschaften. Ihre Untersuchung beginnt man am besten durch ein Studium der kleinsten Fälle:

Übung 5H18. 1. Für $\xi = i\sqrt{2}$ ist $\mathbb{Z}[\xi] = \{\, a + b\xi \mid a, b \in \mathbb{Z} \,\}$ ein Unterring von $\mathbb{C}$.
2. Man zeichne das Gitter $\mathbb{Z}[\xi]$ in der komplexen Ebene und bestimme $\mathbb{Z}[\xi]^\times$.
3. Jede komplexe Zahl $q \in \mathbb{C}$ erlaubt eine Näherung $z \in \mathbb{Z}[\xi]$ mit $|q - z|^2 \leq \frac{3}{4}$.
4. Man folgere daraus, dass $\mathbb{Z}[\xi]$ ein euklidischer Ring ist bezüglich $N(z) = z\bar{z}$.

Übung 5H19. 1. Für $\xi = i\sqrt{3}$ ist $\mathbb{Z}[\xi] = \{\, a + b\xi \mid a, b \in \mathbb{Z} \,\}$ ein Unterring von $\mathbb{C}$.
2. Man zeichne das Gitter $\mathbb{Z}[\xi]$ in der komplexen Ebene und bestimme $\mathbb{Z}[\xi]^\times$.
3. Jede komplexe Zahl $q \in \mathbb{C}$ erlaubt eine Näherung $z \in \mathbb{Z}[\xi]$ mit $|q - z|^2 \leq 1$.
Warum bricht die Konstruktion einer euklidischen Division hier zusammen?
4. Man zähle die kleinsten Werte der Norm $N\colon \mathbb{Z}[\xi] \to \mathbb{N}$, $N(z) = z\bar{z}$, auf und folgere daraus, dass jedes Element $z \in \mathbb{Z}[\xi]$ mit $N(z) = 4$ irreduzibel ist.

5. Man betrachte $2\cdot 2 = (1+i\sqrt{3})(1-i\sqrt{3})$. Ist $\mathbb{Z}[i\sqrt{3}]$ faktoriell?

Übung 5H20. Die komplexe Zahl $j = e^{2\pi i/3} = -\frac{1}{2} + \frac{i}{2}\sqrt{3}$ erfüllt $j^2 = 1-j$ und $j^3 = 1$.

1. Die Menge $\mathbb{Z}[j] = \{\, a+bj \mid a,b \in \mathbb{Z} \,\}$ ist ein Unterring von $\mathbb{C}$.
2. Man zeichne $\mathbb{Z}[j]$ in der komplexen Zahlenebene und bestimme die Gruppe $\mathbb{Z}[j]^\times$.
3. Jede komplexe Zahl $q \in \mathbb{C}$ erlaubt eine Näherung $z \in \mathbb{Z}[j]$ mit $|q-z|^2 \le \frac{1}{3}$.
4. Man folgere daraus, dass $\mathbb{Z}[j]$ ein euklidischer Ring ist.

Übung 5H21. Man zeige, dass der Ring $\mathbb{Z}[i\sqrt{5}]$ nicht faktoriell ist:

1. Man bestimme die Gruppe $\mathbb{Z}[i\sqrt{5}]^\times$ der invertierbaren Elemente.
2. Man zähle die kleinsten Werte der Norm $N\colon \mathbb{Z}[i\sqrt{5}] \to \mathbb{N}$, $N(z) = z\bar{z}$, auf und folgere daraus, dass die Elemente 2, 3, $1 \pm i\sqrt{5}$ in $\mathbb{Z}[i\sqrt{5}]$ irreduzibel sind.
3. Man betrachte $2\cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5})$. Ist $\mathbb{Z}[i\sqrt{5}]$ faktoriell?

Übung 5H22. Sei $d \in \mathbb{Z}_{<0}$ eine negative ganze Zahl mit $d \equiv 1 \pmod 4$.

1. Für $\xi = \frac{1}{2}(1+\sqrt{d})$ ist $\mathbb{Z}[\xi] = \{\, a+b\xi \mid a,b \in \mathbb{Z} \,\}$ ein Unterring von $\mathbb{C}$.
2. Die Abbildung $N\colon \mathbb{Z}[\xi] \to \mathbb{N}$ mit $N(z) = z\bar{z}$ ist multiplikativ.
   Man berechne $N(\xi)$ und $N(a+b\xi)$ für $a,b \in \mathbb{Z}$.
3. Sei D der maximale Abstand von $q \in \mathbb{C}$ zum Gitter $\mathbb{Z}[\xi]$.
   Wenn $D < 1$, ist dann der Ring $\mathbb{Z}[\xi]$ euklidisch?
4. Man bestimme D in Abhängigkeit von d.
   Man schließe daraus , dass $D < 1$ äquivalent ist zu $d \in \{-3,-7,-11\}$.

§**5Hg. Ringe ohne Zerlegung in irreduzible Elemente.** Es ist nicht ganz einfach, einen Ring zu finden, in dem sich manche Elemente nicht als Produkt von irreduziblen Elementen schreiben lassen. Hier eines der einfachsten Beispiele:

Das additive Monoid $(\mathbb{Q}_{\ge 0}, +)$ schreiben wir multiplikativ als $M = \{X^r \mid r \in \mathbb{Q}_{\ge 0}\}$ mit $X^r \cdot X^s = X^{r+s}$. Sei K ein Körper und $R = K[M]$ der Monoidring von M über K (3G14):

Jedes Element $P \in R$ schreibt sich eindeutig als Summe $P = a_1X^{e_1} + \cdots + a_nX^{e_n}$ der Länge $n \in \mathbb{N}$ mit Koeffizienten $a_1,\dots,a_n \in K^*$ und Exponenten $0 \le e_1 < \cdots < e_n$ in $\mathbb{Q}$. Dies erlaubt, den *Grad* $\deg P := e_n \in \mathbb{Q}_{\ge 0}$ und den *Leitkoeffizienten* $\operatorname{lc} P := a_n \in K$ zu definieren. Das Nullelement ist wie immer speziell und wir setzen $\deg 0 = -\infty$ und $\operatorname{lc} 0 = 0$.

Übung 5H23.
1. Man zeige $\deg(PQ) = \deg P + \deg Q$ und $\operatorname{lc}(PQ) = \operatorname{lc} P \cdot \operatorname{lc} Q$.
2. Hat R Nullteiler? Man bestimme die Gruppe $R^\times$ der in R invertierbaren Elemente.
3. Ist der Ring R noethersch? faktoriell? ein Hauptidealring? euklidisch?
4. Im Falle $K = \mathbb{C}$ bestimme man alle irreduziblen Elemente in R.
5. Jede Familie $P_1,\dots,P_n \in R$ liegt in einem Polynomring $K[X^{1/q}] \subset R$ mit $q \in \mathbb{N}$.
6. Jedes endlich erzeugte Ideal $(P_1,\dots,P_n)$ in R ist ein Hauptideal.
7. Existiert zu $P_1,\dots,P_n \in R$ stets ein ggT in R?
8. Zu $A \in R$ und $B \in R^*$ existiert genau ein Paar $C,D \in R$, für das gilt
$$A = BC + D \quad \text{und} \quad \deg D < \deg B.$$
9. Man zeige, dass der (erweiterte) euklidische Algorithmus in R anwendbar ist.

Wir erhalten somit die erstaunliche Situation, dass $R = K[X^{\mathbb{Q}_{\ge 0}}]$ zwar kein euklidischer Ring ist, aber der euklidische Algorithmus in R dennoch bestens funktioniert. (Dieser Ring

ist lokal euklidisch in dem Sinne, dass jede endliche Familie $P_1, \ldots, P_n \in R$ in einem euklidischen Unterring liegt.)

Übung 5H24. Man untersuche ebenso den Monoidring $K[X^{\mathbb{R}_{\geq 0}}]$ des Monoids $(\mathbb{R}_{\geq 0}, +)$ anstelle von $(\mathbb{Q}_{\geq 0}, +)$. Existiert zu $X^{\sqrt{2}} - 1$ und $X - 1$ ein ggT? Kann man die euklidische Division durchführen? Ist der euklidische Algorithmus 3 hier anwendbar?

§**5Hh. Zur Definition euklidischer Ringe.** Wir betrachten hier für euklidische Ringe der Einfachheit halber nur Gradfunktionen $\nu\colon R \to \mathbb{N}$. Mit etwas Abstraktion stellt man fest, dass wir hierbei nur die Ordnung auf $\mathbb{N}$ benutzen. Sei allgemeiner $(N, \leq)$ eine *wohlgeordnete Menge*. Das bedeutet, jede nicht-leere Teilmenge $X \subset N$ hat ein kleinstes Element. Man denke an $\mathbb{N}$ oder $\mathbb{N} \cup \{-\infty\}$ oder $\mathbb{N} \times \mathbb{N}$ mit lexikographischer Ordnung. Insbesondere hat jede strikt fallende Folge $n_1 > n_2 > n_3 > \ldots$ in N eine endliche Länge.

Übung 5H25. Man definiere den Begriff der euklidischen Division bezüglich einer Gradfunktion $\nu\colon R \to N$ mit Werten in einer wohlgeordneten Menge $(N, \leq)$ und beweise die naheliegenden Erweiterungen der obigen Aussagen zu euklidischen Ringen, insbesondere den euklidischen Algorithmus und die Hauptideal-Eigenschaft. Als Beispiel betrachte man den Ring $\mathbb{Z} \times \mathbb{Z}$ mit Gradfunktion $\nu\colon \mathbb{Z}^2 \to \mathbb{N}^2$, $\nu(a,b) = (|a|, |b|)$, und lexikographischer Ordnung. (Dieses einfache Beispiel ist leider kein Integritätsring.)

§**5Hi. Die minimale Gradfunktion.** Ist R ein euklidischer Ring, dann gibt es mehrere euklidische Gradfunktionen $\nu\colon R \to \mathbb{N}$. Zum Beispiel kann man ν mit jeder streng wachsenden Funktion $\phi\colon \mathbb{N} \to \mathbb{N}$, $\phi(0) = 0$, komponieren. Umgekehrt kann man sich für die *minimale* euklidische Gradfunktion auf R interessieren:

Übung 5H26. Sei R ein euklidischer Ring. Wir definieren $\mu\colon R \to \mathbb{N}$ durch $\mu(x) = \min_\nu \nu(x)$, wobei ν alle euklidischen Gradfunktionen auf R durchläuft. (Nach Voraussetzung ist diese Menge nicht leer.) Man zeige, dass μ eine euklidische Gradfunktion ist.

Übung 5H27. Sei K ein Körper. Ist K ein euklidischer Ring? Man bestimme alle euklidischen Gradfunktionen auf K. Welche ist die kleinste? Wenn K ein euklidischer Ring ist bezüglich einer Gradfunktion $\nu\colon K \to \{0,1\}$, ist dann K ein Körper?

Übung 5H28. Der Polynomring $K[X]$ über einem Körper K ist euklidisch bezüglich der Funktion $\nu\colon K[X] \to \mathbb{N}$, definiert durch $\nu(0) = 0$ und $\nu(P) = 1 + \deg(P)$ für $P \neq 0$. Man zeige, dass ν die minimale euklidische Gradfunktion auf $K[X]$ ist.

Auf $\mathbb{Z}$ ist $a \mapsto |a|$ nicht die einzige interessante euklidische Gradfunktion. Wir definieren $\nu\colon \mathbb{Z} \to \mathbb{N}$ durch $\nu(a) = \min\{\, \ell \in \mathbb{N} \mid |a| < 2^\ell \,\}$. Demnach ist $\nu(a)$ die Länge der Binärdarstellung des Absolutbetrages $|a|$, also $\nu(0) = 0$ und $1 + \lfloor \log_2 |a| \rfloor$ für $a \neq 0$.

Übung 5H29. Man zeige, dass ν eine euklidische Gradfunktion ist, indem man hierzu eine euklidische Division konstruiert: Für alle $a, b \in \mathbb{Z}$ mit $b \neq 0$ gibt es $q, r \in \mathbb{Z}$ sodass $a = bq + r$ und $|r| \leq \frac{1}{2}|b|$ gilt, also $\nu(r) < \nu(b)$.

Übung 5H30. Man zeige dass ν die minimale euklidische Gradfunktion auf $\mathbb{Z}$ ist.

Auf einem euklidischen Ring R hängt die minimale euklidische Gradfunktion $\mu\colon R \to \mathbb{N}$ nur vom Ring R ab. Die folgende Konstruktion liefert eine intrinsische Definition von μ:

Übung 5H31. Sei R ein Integritätsring. Wir definieren Teilmengen $A_0 \subset A_1 \subset A_2 \subset \cdots \subset R$ wie folgt: Wir setzen $A_0 = \{0\}$ und rekursiv $A_n = A_{n-1} \cup \{\, a \in R \mid aR + A_{n-1} = R \,\}$. Wir sehen zum Beispiel $A_1 = \{0\} \cup R^\times$. Man zeige, dass R genau dann euklidisch ist, wenn $R = \bigcup A_n$ gilt. In diesem Fall definieren wir $\mu\colon R \to \mathbb{N}$ durch $\mu(a) = \min\{n \in \mathbb{N} \mid a \in A_n\}$, und erhalten so die minimale euklidische Gradfunktion auf R.

Übung 5H32. Die minimale euklidische Gradfunktion $\mu\colon R \to \mathbb{N}$ hat offensichtliche praktische Vorteile, zum Beispiel garantiert sie den schnellst-möglichen Ablauf des euklidischen Algorithmus. Außerdem erfreut sie sich folgender Eigenschaften:

1. Es gilt $\mu(a) = 1$ genau dann, wenn a invertierbar ist.
2. Für alle $a, b \in R^*$ gilt die Ungleichung $\mu(ab) \geq \mu(a) + \mu(b) - 1$.
3. Ist δ eine euklidische Division bzgl. μ, so folgt aus $a = bq$ stets $\delta(a,b) = (q,0)$.

Dies sind vertraute Eigenschaften der üblichen euklidischen Division auf dem Ring $\mathbb{Z}$ der ganzen Zahlen oder dem Polynomring $K[X]$ über einem Körper K. Diese bleiben auf jedem euklidischen Ring bestehen, zumindest für die minimale Gradfunktion.

Übung 5H33. Sei R ein euklidischer Ring mit minimaler Gradfunktion μ. Man folgere aus den Eigenschaften von Übung 5H32 direkt, dass R faktoriell ist:

1. Jedes Element erlaubt eine Zerlegung in irreduzible Elemente.
2. Jede Zerlegung in irreduzible Elemente ist eindeutig.

Übung 5H34. Als abschreckendes Beispiel definieren wir $\nu\colon \mathbb{Z} \to \mathbb{N}$ durch $\nu(b) = b$ für $b \geq 0$, und $\nu(b) = -2b$ für $b < 0$. Man zeige, dass ν eine euklidische Gradfunktion ist, aber keine der sympathischen Eigenschaften aus Übung 5H32 erfüllt.

Wenn man also diese Eigenschaften ausnutzen möchte, muss man sie entweder explizit fordern oder zur minimalen euklidischen Gradfunktion übergehen.

Für eine Diskussion euklidischer Ringe und eine Lösung der obigen Übungsaufgaben lese man den Artikel von P. Samuel, *About Euclidean Rings*, Journal of Algebra 19 (1971), 282–301; der Abschnitt §4 behandelt die minimale euklidische Gradfunktion.

KAPITEL 6

Primfaktorzerlegung in Polynomringen

§6A. Motivation und Überblick

Über jedem Körper K ist der Polynomring $K[X]$ euklidisch, also ein Hauptidealring, und somit faktoriell (5E25). Daher ist zum Beispiel $\mathbb{Q}[X]$ faktoriell. Unsere bisherigen Techniken erlauben noch keine Aussage darüber, ob der Ring $\mathbb{Z}[X]$ faktoriell ist. Wir wissen lediglich, dass $\mathbb{Z}[X]$ kein Hauptidealring ist (5H6) und somit auch nicht euklidisch sein kann.

Dieses Kapitel widmet sich daher der naheliegenden Frage: Ist der Ring $\mathbb{Z}[X]$ faktoriell? Diese ist nicht nur vom systematischem Standpunkt aus interessant, sondern stellt sich ganz praktisch wenn man versucht, ein gegebenes Polynom in $\mathbb{Z}[X]$ oder $\mathbb{Q}[X]$ zu zerlegen: Wenn $P \in \mathbb{Z}[X]$ unzerlegbar in $\mathbb{Z}[X]$ ist, ist dann P auch unzerlegbar in $\mathbb{Q}[X]$?

Beide Fragen wurden zuerst von Gauß behandelt und positiv beantwortet:

Satz (Gauß)**.** *Ist der Ring R faktoriell, dann ist auch der Polynomring $R[X]$ faktoriell. Jedes über R irreduzible Polynom vom Grad ≥ 1 bleibt auch über dem Bruchkörper irreduzibel.*

Wie schon bei den grundlegenden Teilbarkeitsfragen in Kapitel 5 liegt die Hauptarbeit in der präzisen Begriffsbildung. Im vorliegenden Kapitel liegt die technische Schwierigkeit in der lückenlosen Buchhaltung der invertierbaren Elemente, und wir diskutieren daher minutiös alle Normierungsfragen. Das mag zunächst pedantisch erscheinen, macht aber alle Argumente durchsichtiger, manche geradezu trivial. Als Dreingabe erhalten wir ohne Mehraufwand einen Algorithmus (§6Eb) zur Berechnung des ggT im Polynomring $R[X]$.

Korollar (Gauß, algorithmische Fassung)**.** *Wenn wir im Ring R den ggT berechnen können, dann induziert dies einen Algorithmus zur Berechnung des ggT in $R[X]$.*

Neben der notwendigen Buchhaltung ist die Kernidee das Lemma von Gauß (6D3). Ein Polynom $P = a_0 + \cdots + a_n X^n$ in $R[X]^*$ heißt *primitiv* wenn $1 \in \mathrm{GGT}(a_0, \ldots, a_n)$.

Lemma ("Lemma von Gauß")**.** *Über jedem faktoriellen Ring R (oder Ring mit ggT) gilt: Sind zwei Polynome $P, Q \in R[X]^*$ primitiv, dann ist auch ihr Produkt PQ primitiv.*

Sobald diese Grundlagen geklärt sind, werden wir einfache Kriterien aufstellen, um Polynome als irreduzibel zu erkennen, insbesondere das Kriterium von Eisenstein.

§6B. Primfaktorzerlegung

In einem Integritätsring ist jedes Primelement $p \neq 0$ irreduzibel (5E15) und in einem faktoriellen Ring ist umgekehrt auch jedes irreduzible Element prim (5E22). In diesem Fall unterscheidet man daher im Sprachgebrauch oft nicht zwischen irreduzibel und prim (und klammert das Primelement 0 stillschweigend aus). So sagt man bequemer "Primfaktorzerlegung" statt "Zerlegung in irreduzible Faktoren". Dieser laxe Sprachgebrauch ist insbesondere für den Ring $\mathbb{Z}$ der ganzen Zahlen gebräuchlich: Man nennt $60 = 2 \cdot 2 \cdot 3 \cdot 5$ die Primfaktorzerlegung von 60. Nun ist aber auch $60 = (-2) \cdot 2 \cdot (-3) \cdot 5$ eine Primfaktorzerlegung von 60. Wir werden uns als erstes bemühen, eine eindeutige Wahl zu treffen.

§**6Ba. Repräsentantensystem irreduzibler Elemente.** In einem Ring R heißt eine Teilmenge $\mathcal{P} \subset R$ *Repräsentantensystem irreduzibler Elemente* in R wenn gilt:

- Jedes Element $p_0 \in \mathcal{P}$ ist irreduzibel in R.
- Zu jedem irreduziblen Element $p \in R$ existiert genau ein $p_0 \in \mathcal{P}$ mit $p_0 \sim p$.

Ist R ein faktorieller Ring und $\mathcal{P} \subset R$ ein Repräsentantensystem irreduzibler Elemente, dann schreibt sich jedes Element $a \in R^*$ als ein Produkt

$$a = u p_1^{e_1} \cdots p_n^{e_n}$$

mit $u \in R^\times$ und paarweise verschiedenen $p_1, \ldots, p_n \in \mathcal{P}$ und Exponenten $e_1, \ldots, e_n \geq 1$, und diese Schreibweise ist eindeutig bis auf die Reihenfolge der Faktoren.

Beispiel 6B1. Ist R ein Körper, dann gilt $R^* = R^\times$ und $\mathcal{P} = \emptyset$. In obiger Situation schreibt sich dann jedes Element $a \in R^*$ als $a = u$ mit $u \in K^\times$.

Beispiel 6B2. Für den Ring $\mathbb{Z}$ wählt man üblicherweise die Menge der positiven Primzahlen $\mathcal{P} = \{2, 3, 5, 7, 11, 13, \ldots\}$. Im Polynomring $K[X]$ über einem Körper K kann man für $\mathcal{P}$ die Menge der irreduziblen Polynome mit Leitkoeffizient 1 wählen.

Bemerkung 6B3. In jedem Ring R zerlegt sich die Menge aller irreduziblen Elemente in Äquivalenzklassen assoziierter Elemente und das Auswahlaxiom garantiert dass ein Repräsentantensystem irreduzibler Elemente in R existiert. Es gibt im Allgemeinen aber keine kanonische Wahl: Ist $\mathcal{P}$ ein Repräsentantensystem, dann auch $\mathcal{P}' = \{\, u(p) \cdot p \mid p \in \mathcal{P} \,\}$ für jede Abbildung $u\colon \mathcal{P} \to R^\times$. Jedes Repräsentantensystem $\mathcal{P}'$ lässt sich so aus $\mathcal{P}$ erzeugen.

Beispiel 6B4. Der Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen ist euklidisch, also faktoriell (§5He). Hier gilt $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Das Element $1 + i$ ist irreduzibel in $\mathbb{Z}[i]$ und mit ihm seine Assoziierten $1 - i$, $-1 + i$, $-1 - i$. Als Repräsentant ist jedes dieser Elemente gleich geeignet. (Übung 5H17 zeigt ein Repräsentantensystem irreduzibler Elemente in $\mathbb{Z}[i]$.)

§**6Bb. Primfaktorzerlegung.** Mit $\mathbb{N}^{(\mathcal{P})}$ bezeichnen wir wie üblich die Menge aller Abbildungen $\mathcal{P} \to \mathbb{N}$ mit endlichem Träger. Hierauf definieren wir die Abbildung

$$\Phi_\mathcal{P}\colon R^\times \times \mathbb{N}^{(\mathcal{P})} \to R^*, \qquad \Phi_\mathcal{P}(u, e) = u \cdot \prod_{p \in \mathcal{P}} p^{e_p} \tag{6.1}$$

Es handelt sich hierbei um ein *endliches* Produkt, denn nur endlich viele Exponenten e_p sind ungleich Null und daher nur endlich viele Faktoren p^{e_p} ungleich Eins. Die Menge $R^\times \times \mathbb{N}^{(\mathcal{P})}$

wird zu einem Monoid durch die komponentenweise Verknüpfung

$$(u,e)\cdot(v,f)=(uv,e+f).$$

Nach Konstruktion ist $\Phi_{\mathcal{P}}$ ein Monoidhomomorphismus, denn es gilt

$$\Phi_{\mathcal{P}}(uv,e+f)=\Phi_{\mathcal{P}}(u,e)\cdot\Phi_{\mathcal{P}}(v,f).$$

Satz 6B5. *Ein Integritätsring R ist genau dann faktoriell, wenn es eine Teilmenge $\mathcal{P}\subset R$ gibt, sodass die Abbildung* (6.1) *bijektiv ist. In diesem Fall ist $\mathcal{P}$ ein Repräsentantensystem irreduzibler Elemente in R.*

BEWEIS. "⇒" Wir können ein Repräsentantensystem $\mathcal{P}\subset R$ irreduzibler Elemente in R wählen (6B3). Die Bijektivität von $\Phi_{\mathcal{P}}$ entspricht der Faktorialität des Rings R: Die Abbildung $\Phi_{\mathcal{P}}$ ist genau dann surjektiv, wenn sich jedes Element $a\in R$ in irreduzible Elemente zerlegen lässt. $\Phi_{\mathcal{P}}$ ist genau dann injektiv, wenn diese Zerlegung eindeutig ist.

"⇐" Angenommen, $\Phi_{\mathcal{P}}$ ist bijektiv. Im Monoid $R^\times\times\mathbb{N}^{(\mathcal{P})}$ sind die irreduziblen Elemente von der Form (u,δ_p) mit $u\in R^\times$ und $p\in\mathcal{P}$, wobei $\delta_p\colon\mathcal{P}\to\mathbb{N}$ definiert ist durch $\delta_p(p)=1$ und $\delta_p(p')=0$ für alle $p'\neq p$ in $\mathcal{P}$. Vermöge des Monoidisomorphismus $\Phi_{\mathcal{P}}$ sind in R^* die irreduziblen Elemente von der Form up mit $u\in R^\times$ und $p\in\mathcal{P}$. Demnach ist R faktoriell und $\mathcal{P}$ ein Repräsentantensystem irreduzibler Elemente in R. □

Bemerkung 6B6. Die Umkehrabbildung $\Phi_{\mathcal{P}}^{-1}\colon R^*\to R^\times\times\mathbb{N}^{(\mathcal{P})}$ nennt man die *Primfaktorzerlegung* bezüglich des Repräsentantensystems $\mathcal{P}$. Während das Produkt $\Phi_{\mathcal{P}}$ im Allgemeinen leicht zu berechnen ist, kann die Zerlegung $\Phi_{\mathcal{P}}^{-1}$ sehr schwierig sein.

Als Beispiel denke man an den Ring $\mathbb{Z}$: Hier ist das Produkt großer Zahlen leicht zu berechnen, aber die Primfaktorzerlegung ist algorithmisch ungleich aufwändiger.

Hierzu effiziente Algorithmen zu finden, oder deren Nicht-Existenz zu beweisen, ist ein bislang ungelöstes Problem. Einstweilen, in Ermangelung schneller Algorithmen zur Primfaktorzerlegung in $\mathbb{Z}$, macht man aus der Not eine Tugend und verwendet große Primzahlen und ihre Produkte in vielen kryptographischen Anwendungen.

§**6Bc. Eine erste Anwendung.** Wir nutzen Satz 6B5 zu einer ersten Anwendung:

Satz 6B7. *Sei R ein Ring. Ist $R[X]$ faktoriell, dann ist auch R faktoriell.*

BEWEIS. Sei $R[X]$ faktoriell und sei $\mathcal{P}\subset R[X]$ ein Repräsentantensystem irreduzibler Elemente in $R[X]$. Wir zerlegen $\mathcal{P}$ in zwei Teilmengen

$$\mathcal{P}_0:=\mathcal{P}\cap R=\{\,P\in\mathcal{P}\mid\deg P=0\,\},$$
$$\mathcal{P}_1:=\mathcal{P}\smallsetminus\mathcal{P}_0=\{\,P\in\mathcal{P}\mid\deg P\geq 1\,\}.$$

Jedes Element $A\in R[X]^*$ zerlegt sich eindeutig gemäß

$$A=u\cdot\prod_{p\in\mathcal{P}}p^{e_p}=u\cdot\prod_{p\in\mathcal{P}_0}p^{e_p}\cdot\prod_{P\in\mathcal{P}_1}P^{e_P}$$

mit $u\in R[X]^\times=R^\times$. Hierbei gilt $A\in R^*$ genau dann, wenn $\deg A=0$. Dies ist gleichbedeutend mit $e_P=0$ für alle $P\in\mathcal{P}_1$. Also schreibt sich jedes $A\in R^*$ eindeutig als

$$A=u\cdot\prod_{p\in\mathcal{P}_0}p^{e_p}$$

mit $u \in R^\times$. Nach dem vorangegangenen Satz 6B5 ist also R faktoriell und $\mathcal{P}_0 \subset R$ ist ein Repräsentantensystem irreduzibler Elemente in R. □

Der eingangs angekündigte Satz von Gauß (6E1) behandelt die Umkehrung: wenn R faktoriell ist, dann ist auch $R[X]$ faktoriell. Der Beweis, den wir im Folgenden vorbereiten, kehrt den obigen Beweisgang um: ausgehend von $\mathcal{P}_0 \subset R$ konstruieren wir $\mathcal{P}_1 \subset R[X]$ sodass $\mathcal{P} = \mathcal{P}_0 \cup \mathcal{P}_1$ ein Repräsentantensystem irreduzibler Elemente in $R[X]$ ist.

§6C. Exponentenbewertung und Normierung

Sei weiterhin R ein faktorieller Ring und sei $\mathcal{P} \subset R$ ein gewähltes Repräsentantensystem irreduzibler Elemente in R. Die Primfaktorzerlegung (6.1) bezüglich $\mathcal{P}$ definiert Abbildungen $\mathrm{lu}_\mathcal{P}\colon R^* \to R^\times$ und $e_p\colon R^* \to \mathbb{N}$ für $p \in \mathcal{P}$ durch die Bedingung

$$a = \mathrm{lu}_\mathcal{P}(a) \cdot \prod_{p\in\mathcal{P}} p^{e_p(a)} \qquad \text{für alle } a \in R^*. \tag{6.2}$$

Wir nennen $\mathrm{lu}_\mathcal{P}(a)$ die *Leiteinheit* von a bezüglich $\mathcal{P}$ (auf englisch *leading unit*) und $e_p(a)$ die *Exponentenbewertung* von a bezüglich $p \in \mathcal{P}$. Erstere hängt vom gewählten Repräsentantensystem $\mathcal{P}$ ab. Wenn $\mathcal{P}$ aus dem Kontext unmissverständlich hervorgeht, werde ich die laxe Schreibweise $\mathrm{lu}(a)$ vorziehen.

Beispiel 6C1. Ist R ein Körper, dann gilt $R^* = R^\times$, $\mathcal{P} = \emptyset$, und $\mathrm{lu}\colon R^* \to R^\times$ ist die Identität.

Beispiel 6C2. Im Ring $\mathbb{Z}$ gilt $\mathbb{Z}^\times = \{\pm 1\}$. Als Repräsentantensystem irreduzibler Elemente wählt man üblicherweise die Menge der positiven Primzahlen $\mathcal{P} = \{2,3,5,7,\dots\}$. In diesem Fall ist $\mathrm{lu}(a) \in \{\pm 1\}$ das Vorzeichen von $a \in \mathbb{Z}^*$.

Beispiel 6C3. Im Polynomring $K[X]$ über einem Körper K gilt $K[X]^\times = K^\times = K^*$. Man kann daher als Repräsentantensystem $\mathcal{P} \subset K[X]$ die Menge der irreduziblen Polynome mit Leitkoeffizient 1 wählen. Für jedes $P \in K[X]^*$ ist dann $\mathrm{lu}(P) \in K^\times$ der Leitkoeffizient von P. Andere Wahlen sind ebenfalls möglich, und das werden wir in diesem Kapitel auch nutzen.

Bemerkung 6C4. Das Nullelement $0 \in R$ spielt wie immer eine Sonderrolle. Wir können die Abbildung $\mathrm{lu}\colon R^* \to R^\times$ durch $\mathrm{lu}(0) = 0$ fortsetzen zu $\mathrm{lu}\colon R \to R^\times \cup \{0\}$. Im Beispiel 6C2 gilt dann $\mathrm{lu} = \mathrm{sign}\colon \mathbb{Z} \to \{0, \pm 1\}$. Im Beispiel 6C3 gilt dann $\mathrm{lu} = \mathrm{lc}\colon K[X] \to K$.

§6Ca. Exponentenbewertung. Die Exponentenbewertung $e_p\colon R^* \to \mathbb{N}$ setzen wir auf R fort, indem wir für das Nullelement $e_p(0) = \infty$ setzen. Für alle $a \in R$ gilt dann

$$e_p(a) = \sup\{\, k \in \mathbb{N} : p^k \mid a \,\}.$$

Dies zeigt, dass e_p nur von p abhängt, nicht aber von $\mathcal{P} \subset R$.

Proposition 6C5. *Es gilt* $e_p(a+b) \geq \inf\{e_p(a), e_p(b)\}$ *und* $e_p(ab) = e_p(a) + e_p(b)$.

BEWEIS. Die Aussage ist klar für $a = 0$ oder $b = 0$. Wir können also $a, b \in R^*$ annehmen. In jedem Ring folgt aus $p^k \mid a$ und $p^\ell \mid b$, dass $p^{\inf\{k,\ell\}} \mid a+b$ und $p^{k+\ell} \mid ab$. Das bedeutet $e_p(a+b) \geq \inf\{e_p(a), e_p(b)\}$ und $e_p(ab) \geq e_p(a) + e_p(b)$. Die Faktorialität von R und die Primalität von p garantieren, dass $e_p(ab) = e_p(a) + e_p(b)$ gilt. □

Sei K der Bruchkörper des Rings R. Man kann die Exponentenbewertung von R zu $e_p\colon K \to \mathbb{Z} \cup \{\infty\}$ erweitern durch $e_p(a/b) = e_p(a) - e_p(a)$ für alle $a \in R$, $b \in R^*$.

Dies ist wohldefiniert: $a/b = a'/b'$ in K mit $a, a' \in R$, $b, b' \in R^*$ bedeutet $ab' = a'b$ in R. Hieraus folgt $e_p(a) + e_p(b') = e_p(a') + e_p(b)$, also $e_p(a) - e_p(b) = e_p(a') - e_p(b')$.

Proposition 6C6. *Jedes Element $x \in K^*$ besitzt die Darstellung*

$$x = u \cdot \prod_{p \in \mathcal{P}} p^{e_p(x)} \qquad \text{mit } u \in R^\times.$$

Hierbei gilt $x \in R^*$ genau dann, wenn $e_p(x) \geq 0$ für alle $p \in \mathcal{P}$.
Weiterhin gilt $e_p(x+y) \geq \inf\{e_p(x), e_p(y)\}$ und $e_p(xy) = e_p(x) + e_p(y)$. □

§**6Cb. Normierung.** Aufgrund der Definition (6.2) ist die Abbildungen $\mathrm{lu}\colon R^* \to R^\times$ multiplikativ, also $\mathrm{lu}(ab) = \mathrm{lu}(a)\,\mathrm{lu}(b)$ für alle $a, b \in R^*$, und erfüllt $\mathrm{lu}(u) = u$ für alle $u \in R^\times$.

Definition 6C7. Wir nennen $a \in R^*$ *normiert* bezüglich $\mathcal{P}$, wenn $\mathrm{lu}(a) = 1$ gilt.

Normierung bedeutet also, dass $a = \prod_{p \in \mathcal{P}} p^{e_p(a)}$ gilt, ohne Leiteinheit.

Beispiel 6C8. Die Menge $R^\times$ der invertierbaren Elemente sind alle zu 1 assoziert, und letzteres ist in $R^\times$ das einzige normierte Element.

Beispiel 6C9. Im Ring $\mathbb{Z}$ gilt $\mathbb{Z}^\times = \{\pm 1\}$. Als Repräsentantensystem irreduzibler Elemente wählen wir die Menge der positiven Primzahlen $\mathcal{P} = \{2, 3, 5, 7, \dots\}$. In diesem Fall ist $a \in \mathbb{Z}$ genau dann normiert bezüglich $\mathcal{P}$ wenn $a > 0$ gilt.

Beispiel 6C10. Im Polynomring $K[X]$ über einem Körper K gilt $K[X]^\times = K^\times = K^*$. Man kann daher für $\mathcal{P} \subset K[X]$ die Menge der irreduziblen Polynome mit Leitkoeffizient 1 wählen. In diesem Fall ist $P \in K[X]^*$ genau dann normiert bezüglich $\mathcal{P}$ wenn $\mathrm{lc}\, P = 1$ gilt.

Proposition 6C11. *Jedes Element $a \in R^*$ ist zu genau einem normierten Element $a_1 \in R^*$ assoziiert, nämlich $a_1 = \mathrm{lu}(a)^{-1} a$.* □

Anders gesagt, die Wahl eines Repräsentantensystems $\mathcal{P} \subset R$ irreduzibler Elemente in R induziert auf natürliche Weise die Wahl eines Repräsentanten a_1 in der Klasse $aR^\times$ der zu a assoziierten Elemente. (Die Normierung hängt natürlich von $\mathcal{P}$ ab.)

In Kapitel 5 haben wir die *Mengen* $\mathrm{GGT}(a,b)$ und $\mathrm{KGV}(a,b)$ definiert. Die Normierung bezüglich $\mathcal{P}$ beschert uns nun bevorzugte Repräsentanten:

Definition 6C12. Wir definieren $\mathrm{ggT}, \mathrm{kgV}\colon (R^*)^n \to R^*$ für $n \geq 1$ durch

$$\mathrm{ggT}(a_1, \dots, a_n) := \prod_{p \in \mathcal{P}} p^{\min\{e_p(a_1), \dots, e_p(a_n)\}},$$
$$\mathrm{kgV}(a_1, \dots, a_n) := \prod_{p \in \mathcal{P}} p^{\max\{e_p(a_1), \dots, e_p(a_n)\}}.$$

Für $n = 0$ vereinbaren wir die Konvention $\mathrm{ggT}() = 0$ und $\mathrm{kgV}() = 1$, denn 0 und 1 sind bezüglich Teilbarkeit das größte bzw. kleinste Element in R. Diese Abbildungen setzen wir in der offensichtlichen Weise zu $\mathrm{ggT}, \mathrm{kgV}\colon R^n \to R$ fort, sodass schließlich gilt:

$$\mathrm{ggT}(\dots, a_{i-1}, 0, a_{i+1}, \dots) = \mathrm{ggT}(\dots, a_{i-1}, a_{i+1}, \dots) \qquad \mathrm{ggT}(\dots, a_{i-1}, 1, a_{i+1}, \dots) = 1$$
$$\mathrm{kgV}(\dots, a_{i-1}, 1, a_{i+1}, \dots) = \mathrm{kgV}(\dots, a_{i-1}, a_{i+1}, \dots) \qquad \mathrm{kgV}(\dots, a_{i-1}, 0, a_{i+1}, \dots) = 0$$

Die Primfaktorzerlegung (6B5) zeigt, dass $\operatorname{ggT}(a_1,\dots,a_n) \in R$ tatsächlich ein größter gemeinsamer Teiler von $a_1,\dots,a_n$ in R ist, und ebenso $\operatorname{kgV}(a_1,\dots,a_n) \in R$ ein kleinstes gemeinsames Vielfaches von $a_1,\dots,a_n$ in R ist. Wir nennen daher $\operatorname{ggT}(a_1,\dots,a_n)$ den *normierten größten gemeinsamen Teiler* und $\operatorname{kgV}(a_1,\dots,a_n)$ das *normierte kleinste gemeinsame Vielfache* von $a_1,\dots,a_n$ in R. Erst die Normierung bezüglich $\mathcal{P}$ rechtfertigt hier den Gebrauch des bestimmten Artikels und beschert uns Abbildungen $R^n \to R$. Hat man diese Subtilität erst einmal gemeistert, so sagt man abkürzend "der ggT" und "das kgV" und lässt den Hinweis auf die gewählte Normierung stillschweigend weg.

Korollar 6C13. *Im Bruchkörper eines faktoriellen Rings R lässt sich jedes Element x eindeutig schreiben als $x = \frac{a}{b}$ mit $a,b \in R$ sodass $\operatorname{ggT}(a,b) = 1$ gilt und b normiert ist.* □

Für eine Ausführung im Falle eines Rings mit ggT siehe Korollar 6F7.

§6D. Inhalt und Normierung von Polynomen

§6Da. Inhalt von Polynomen. Sei weiterhin R ein faktorieller Ring und $\mathcal{P} \subset R$ ein Repräsentantensystem irreduzibler Elemente in R. Mit $\operatorname{ggT}\colon R^n \to R$ bezeichnen wir den normierten ggT bezüglich $\mathcal{P}$. Jedes Polynom $P \in R[X]^*$ schreibt sich eindeutig als

$$P = a_0 + a_1 X + \cdots + a_n X^n$$

wobei $n \in \mathbb{N}$, $a_0, a_1, \dots, a_n \in R$, $a_n \neq 0$. Hierdurch definieren wir seinen *Grad* $\deg P := n$ und *Leitkoeffizient* $\operatorname{lc} P := a_n$. Sein *Inhalt* (auf englisch *content*) ist definiert durch

$$\operatorname{cont}(P) := \operatorname{ggT}(a_0,\dots,a_n).$$

Definition 6D1. Wir nennen $P \in R[X]^*$ *primitiv* wenn $\operatorname{cont}(P) = 1$ gilt.

Offenbar teilt der Inhalt $\operatorname{cont}(P)$ das Polynom P und $P_0 = P/\operatorname{cont}(P)$ ist primitiv.

Beispiel 6D2. In $\mathbb{Z}[X]$ hat das Polynom $P = -4X^3 + 10X + 12$ den Inhalt $\operatorname{cont}(P) = 2$. Durch diesen können wir dividieren und das Polynom $P/2 = -2X^3 + 5X + 6$ ist primitiv.

Über faktoriellen Ringen gilt folgendes wichtige Ergebnis:

Lemma 6D3 ("Lemma von Gauß")**.** *Sind $P, Q \in R[X]^*$ primitiv, dann ist auch PQ primitiv.*

BEWEIS. Angenommen $\operatorname{cont}(PQ) \neq 1$. Dann gibt es $p \in \mathcal{P}$ sodass $p \mid \operatorname{cont}(PQ)$. Im Quotientenring $R[X]/(p) \cong (R/p)[X]$ gilt dann $\overline{PQ} = 0$. Das Element p ist irreduzibel im faktoriellen Ring R, also auch prim in R. Demnach ist R/p nullteilerfrei, also auch der Polynomring $(R/p)[X]$. (Dieses Argument wurde in Korollar 5G4 ausgeführt.) Das bedeutet, es gilt $\overline{P} = 0$ oder $\overline{Q} = 0$. Dann aber wäre $p \mid \operatorname{cont}(P)$ oder $p \mid \operatorname{cont}(Q)$. Das ist aber aufgrund der Voraussetzung $\operatorname{cont}(P) = \operatorname{cont}(Q) = 1$ nicht möglich. □

Man kann diesen abstrakten Beweis durch eine konkrete Rechnung ersetzen:

ALTERNATIVER BEWEIS. Das Produkt von $P = \sum_i a_i X^i$ und $Q = \sum_j b_j X^j$ ist $PQ = \sum_k c_k X^k$ mit $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. Sei $p \in \mathcal{P}$. Wegen $\operatorname{cont}(P) = 1$ gibt es einen Index s mit $p \nmid a_s$; wir wählen s minimal. Wegen $\operatorname{cont}(Q) = 1$ gibt es ebenso einen Index t mit $p \nmid b_t$; wir wählen auch t minimal. In der Summe $c_{s+t} = \sum_{i=0}^{s+t} a_i b_{s+t-i}$ sind bis auf $a_s b_t$ alle Summanden durch p teilbar, denn für $i < s$ gilt $p \mid a_i$ und für $i > s$ gilt $p \mid b_{s+t-i}$. Aus $p \nmid a_s$ und $p \nmid b_t$ folgt $p \nmid a_s b_t$, denn p ist prim in R. Hieraus folgt $p \nmid c_{s+t}$ und somit $p \nmid \operatorname{cont}(PQ)$. Da dies für alle $p \in \mathcal{P}$ gilt, muss $\operatorname{cont}(PQ) = 1$ gelten. □

Wir werden mit Lemma 6F11 einen weiteren Beweis dieses wichtigen Ergebnisses angeben, der ohne die Verwendung von Primelementen auskommt und nur den ggT der Koeffizienten benutzt.

Das Lemma von Gauß lässt sich etwas allgemeiner wie folgt formulieren:

Proposition 6D4. *Die Abbildung* $\operatorname{cont}\colon R[X]^* \to R^*$ *ist ein Monoidhomomorphismus.*

BEWEIS. Für $a \in R^*$ gilt $\operatorname{cont}(a) = \operatorname{ggT}(a) = \operatorname{lu}(a)^{-1}a$ gemäß unserer Normierung des ggT. Insbesondere folgt hieraus $\operatorname{cont}(1) = 1$.

Zu $P, Q \in R[X]^*$ gilt $P = \operatorname{cont}(P)P_1$ und $Q = \operatorname{cont}(Q)Q_1$ mit $P_1, Q_1 \in R[X]^*$ primitiv. Also gilt $PQ = \operatorname{cont}(P)\operatorname{cont}(Q)P_1Q_1$ wobei P_1Q_1 primitiv ist nach obigem Lemma von Gauß. Also ist $\operatorname{cont}(PQ) = \operatorname{cont}(P)\operatorname{cont}(Q)$. □

Warnung. — Das Lemma von Gauß (6D3) gilt über faktoriellen Ringen. Über einem nicht-faktoriellen Ring muss das Produkt primitiver Polynome nicht primitiv sein:

Beispiel 6D5. Der Ring $R = \mathbb{Q}[X^2, X^3]$ ist nicht faktoriell (5H10). In $R[Y]$ ist $P = X^2Y + X^3$ primtiv, das heißt $1 \in \operatorname{GGT}(X^2, X^3)$, denn X^2 und X^3 sind in R irreduzibel aber nicht assoziiert. Das Produkt $P^2 = X^4Y^2 + 2X^5Y + X^6$ ist nicht primitiv, denn $X^2 \in \operatorname{GT}(X^4, X^5, X^6)$.

Beispiel 6D6. Der Ring $R = \mathbb{Z}[i\sqrt{5}]$ ist nicht faktoriell (5H21). Es gilt $R^\times = \{\pm 1\}$. Sowohl 2 als auch $1 \pm i\sqrt{5}$ sind in R irreduzibel aber untereinander nicht assoziiert. Die Polynome $P_\pm = 2X + (1 \pm i\sqrt{5})$ über R sind daher primitiv, aber $P_+ \cdot P_- = 4X^2 + 4X + 6$ nicht.

§**6Db. Normierung von Polynomen.** Wir können jedem Polynom $P \in R[X]^*$ das primitive Polynom $P_0 = P/\operatorname{cont}(P)$ zuordnen. Allerdings ist dies nicht das einzige primitive Polynom, das in Frage kommt, denn für jedes invertierbare Element $u \in R^\times$ ist uP_0 ebenfalls primitiv. Auch hier werden wir nun eine Normierung durchführen. Wir setzen die Abbildung $\operatorname{lu}\colon R^* \to R^\times$ aus §6Cb zu einer Abbildung $\operatorname{lu}\colon R[X]^* \to R^\times$ fort durch $\operatorname{lu}(P) := \operatorname{lu}(\operatorname{lc} P)$. Es gilt dann $\operatorname{lu}(PQ) = \operatorname{lu}(P)\operatorname{lu}(Q)$ für alle $P, Q \in R[X]^*$ sowie $\operatorname{lu}|_{R^\times} = \mathrm{id}_{R^\times}$.

Definition 6D7. Wir nennen P *normiert* bezüglich $\mathcal{P}$ wenn $\operatorname{lu}(P) = 1$ gilt.

Beispiel 6D8. In $\mathbb{Z}$ wählen wir wie üblich $\mathcal{P} = \{2, 3, 5, 7, \dots\}$; somit gilt $\operatorname{lu}(a) = \operatorname{sign}(a)$. In $\mathbb{Z}[X]$ hat das Polynom $P = -6X^3 + 15X + 12$ die Leiteinheit -1 und den Inhalt 3, so dass $P = (-1) \cdot 3 \cdot (2X^3 - 5X - 4)$. Das solcherart reduzierte Polynom $P_1 = 2X^3 - 5X - 4$ ist sowohl primitiv als auch normiert (bezüglich $\mathcal{P} = \{2, 3, 5, 7, \dots\}$).

Lemma 6D9. *Zu jedem Polynom* $P \in R[X]^*$ *existiert genau ein* $a \in R^*$ *und* $P_1 \in R[X]$*, so dass* $P = aP_1$ *gilt und* P_1 *normiert und primitiv ist. Hierbei ist* $a = \operatorname{lu}(P)\operatorname{cont}(P)$.

BEWEIS. *Existenz:* Jeder Koeffizient von P ist durch $a = \operatorname{lu}(P)\operatorname{cont}(P)$ teilbar. Somit können wir dividieren und erhalten $P_1 = P/a$ in $R[X]$. Es gilt $\operatorname{lu}(a) = \operatorname{lu}(P)$ und $\operatorname{cont}(a) = \operatorname{cont}(P)$. Aus $P = aP_1$ folgt somit $\operatorname{lu}(P_1) = 1$ und $\operatorname{cont}(P_1) = 1$.

Eindeutigkeit: Gilt $P = aP_1$ mit P_1 normiert, dann folgt $\operatorname{lu}(P) = \operatorname{lu}(a)$. Ist P zudem primitiv, dann folgt $\operatorname{cont}(P) = \operatorname{cont}(a) = \operatorname{lu}(a)^{-1}a$. Damit liegt der Faktor $a = \operatorname{lu}(P)\operatorname{cont}(P)$ eindeutig fest, und damit auch $P_1 = P/a$. □

§**6Dc. Polynome über dem Bruchkörper.** Sei K der Bruchkörper des Rings R. Da wir $R \subset K$ als Unterring auffassen, sehen wir auch $R[X] \subset K[X]$ als Unterring. Wir wollen jedem Polynom $P \in K[X]^*$ ein normiertes primitives Polynom $P_1 \in R[X]^*$ zuordnen.

Beispiel 6D10. Wir betrachten das Polynom

$$P = -\tfrac{3}{5}X^3 + \tfrac{3}{2}X + \tfrac{6}{5} \qquad \text{in } \mathbb{Q}[X].$$

Dieses multiplizieren wir zunächst mit einem gemeinsamen Nenner und erhalten

$$10 \cdot P = -6X^3 + 15X + 12 \qquad \text{in } \mathbb{Z}[X].$$

Hierzu finden wir dann in $\mathbb{Z}[X]$ das normierte und primitive Polynom

$$P_1 = \left(-\tfrac{10}{3}\right) \cdot P = 2X^3 - 5X - 4.$$

Satz 6D11. *Zu jedem Polynom $P \in K[X]^*$ existiert genau ein $c \in K^*$ und $P_1 \in R[X]$ mit $P = cP_1$ und P_1 normiert und primitiv. Zusätzlich gilt $c \in R^*$ genau dann wenn $P \in R[X]^*$.*

BEWEIS. *Existenz:* Es gilt $P = c_0 + \cdots + c_n X^n$ mit $c_k \in K$, also $c_k = a_k/b_k$ mit $a_k, b_k \in R$ und $b_k \neq 0$ für alle $k = 0, \ldots, n$. Sei $b \in R^*$ ein gemeinsames Vielfaches der Nenner $b_0, \ldots, b_n$. Dann liegt $P_0 = bP = a_0(b/b_0) + \cdots + a_n(b/b_n)X^n$ in $R[X]$. Wir zelegen $P_0 = aP_1$ in $a \in R^*$ und $P_1 \in R[x]$ normiert und primitiv (6D9). Also gilt $P = cP_1$ mit $c = a/b$ in K.

Eindeutigkeit: Angenommen $P = cP_1 = c'Q_1$ mit $c, c' \in K^*$ und $P_1, Q_1 \in R[X]$ primitiv und normiert. Dann gilt $c = a/b$ und $c' = a'/b'$ mit $a, b, a', b' \in R^*$. Aus $ab'P_1 = a'bQ_1$ mit $ab', a'b \in R^*$ folgt mit Lemma 6D9, dass $P_1 = Q_1$ und $ab' = a'b$, also $c = c'$.

Zusatz: Wenn $c \in R$, dann liegt mit $P_1 \in R[X]$ offenbar auch das Produkt $P = cP_1$ in $R[X]$. Gilt umgekehrt $P \in R[X]$, dann folgt aus der Eindeutigkeit und Lemma 6D9, dass $c = \mathrm{lu}(P)\,\mathrm{cont}(P)$ gelten muss und somit in R liegt. □

Existenz und Eindeutigkeit dieser Zerlegung definieren die Abbildungen

$$\begin{aligned} \mathrm{red}_R \colon K[X]^* &\to R[X]^*, & P &\mapsto P_1 \text{ normiert und primitiv,} \\ \mathrm{scal}_R \colon K[X]^* &\to K^*, & P &\mapsto c \text{ so dass } P = cP_1. \end{aligned}$$

Wir nennen red_R die *Reduktion* auf $R[X]$ und scal_R die *Skalierung*. Die Reduktion $\mathrm{red}_R(P)$ wählt aus der Äquivalenzklasse von P in $K[X]$ das eindeutige normierte primitive Polynom $P_1 \in R[X]$ mit $P_1 \sim P$ aus. Die wichtigsten Eigenschaften fassen wir wie folgt zusammen:

Proposition 6D12. *Die Abbildung scal_R erfreut sich folgender Eigenschaften:*

1. $\mathrm{scal}_R \colon K[X]^* \to K^*$ *ist ein Monoidhomomorphismus mit* $\mathrm{scal}_R|_{K^*} = \mathrm{id}_{K^*}$.
2. *Es gilt* $\mathrm{scal}_R(P) \in R^*$ *genau dann wenn* $P \in R[X]^*$.
3. *Es gilt* $\mathrm{scal}_R(P) = 1$ *genau dann wenn* $P \in R[X]^*$ *normiert und primitiv ist.* □

Lemma 6D13 ("Lemma von Gauß")**.** *Seien $P, Q \in K[X]$ Polynome über dem Körper K mit Leitkoeffizienten* $\mathrm{lc}(P) = \mathrm{lc}(Q) = 1$. *Aus $PQ \in R[X]$ folgt dann $P, Q \in R[X]$.*

BEWEIS. Wir zerlegen $P = aP_1$ und $Q = bQ_1$ in $a, b \in K^*$ und $P_1, Q_1 \in R[X]$ normiert und primitiv. Das Produkt $P_1Q_1 \in R[X]$ ist dann normiert und primitiv nach 6D3. Andererseits ist auch $PQ = abP_1Q_1 \in R[X]$ normiert und primitiv wegen $\mathrm{lc}(PQ) = \mathrm{lc}(P)\,\mathrm{lc}(Q) = 1$. Also gilt $1 = \mathrm{scal}(PQ) = \mathrm{scal}(ab)\,\mathrm{scal}(P_1Q_1) = ab$, das heißt $a = b^{-1}$. Da P_1, Q_1 in $R[X]$

liegen, müssen insbesondere ihre Leitkoeffizienten $\mathrm{lc}(P_1) = \mathrm{lc}(P/a) = a^{-1}$ und $\mathrm{lc}(Q_1) = \mathrm{lc}(Q/b) = b^{-1} = a$ in R liegen. Daraus ersehen wir $a, b \in R^\times$, also auch $P, Q \in R[X]$. □

§6E. Der Satz von Gauß

Nach diesen Vorbereitungen stehen nun alle Begriffe und Techniken bereit, um den Satz von Gauß zu beweisen: Ist R ein faktorieller Ring, so ist auch $R[X]$ faktoriell. Als Mehrwert unserer minutiösen Vorbereitung erhalten wir zudem einen Algorithmus: Wenn wir in R den ggT berechnen können, dann auch in $R[X]$.

§**6Ea. Der Satz von Gauß.** Den eingangs des Kapitels angekündigten Satz von Gauß formulieren wir ausführlicher wie folgt:

Satz 6E1 ("Satz von Gauß")**.** *Ist R ein faktorieller Ring, so ist auch $R[X]$ faktoriell.*

Genauer gilt: Sei $\mathcal{P}_0 \subset R$ ein Repräsentantensystem irreduzibler Elemente in R. Sei K der Bruchkörper von R und sei $\mathcal{P}_1 \subset K[X]$ ein Repräsentantensystem irreduzibler Elemente in $K[X]$ bestehend aus normierten primitiven Polynomen aus $R[X]$. Dann ist $R[X]$ faktoriell und $\mathcal{P} = \mathcal{P}_0 \cup \mathcal{P}_1$ ist ein Repräsentantensystem irreduzibler Elemente in $R[X]$.

BEWEIS. Der vorangegangene Satz 6D11 garantiert, dass es ein Repräsentantensystem $\mathcal{P}_1 \subset K[X]$ der gewünschten Art gibt. Wir werden zeigen, dass sich jedes Polynom $A \in R[X]^*$ eindeutig bezüglich $\mathcal{P} = \mathcal{P}_0 \cup \mathcal{P}_1$ zerlegen lässt. Da der Polynomring $K[X]$ über dem Körper K faktoriell ist (5E25) schreibt sich A eindeutig als

$$A = a \cdot \prod_{P \in \mathcal{P}_1} P^{e_P}$$

mit $a \in K[X]^\times = K^*$ und natürlichen Zahlen $e_P \geq 0$, wobei wie immer $e_P \neq 0$ nur für endlich viele $P \in \mathcal{P}_1$ gilt. Das Produkt dieser normierten primitiven Polynome ist normiert und primitiv. Satz 6D11 garantiert nun, dass $a \in R^*$ gilt. In R schreibt sich a eindeutig als

$$a = u \cdot \prod_{p \in \mathcal{P}_0} p^{e_p}$$

mit $u \in R^\times$ und natürlichen Zahlen $e_p \geq 0$, wobei wie immer $e_P \neq 0$ nur für endlich viele $P \in \mathcal{P}_0$ gilt. Damit schreibt sich jedes Polynom $A \in R[X]$ eindeutig als

$$A = u \cdot \prod_{p \in \mathcal{P}_0} p^{e_p} \cdot \prod_{P \in \mathcal{P}_1} P^{e_P} = u \cdot \prod_{p \in \mathcal{P}} p^{e_p}$$

mit $u \in R[X]^\times = R^\times$. Mit Satz 6B5 sehen wir nun, dass der Ring $R[X]$ faktoriell ist und dass $\mathcal{P} = \mathcal{P}_0 \cup \mathcal{P}_1$ ein Repräsentantensystem irreduzibler Elemente in $R[X]$ ist. □

Korollar 6E2. *Ist R ein faktorieller Ring, dann ist für jedes $n \in \mathbb{N}$ auch der Polynomring $R[X_1, \ldots, X_n]$ in n Variablen über R faktoriell.*

BEWEIS. Wir führen Induktion über n. Die Aussage für $n = 0$ ist trivial, denn für der Ring R wird als faktoriell vorausgesetzt. Ist für $n \geq 1$ der Ring $R[X_1, \ldots, X_{n-1}]$ faktoriell, dann ist auch $R[X_1, \ldots, X_{n-1}][X_n]$ faktoriell nach dem vorangegangenen Satz von Gauß. Schließlich gilt $R[X_1, \ldots, X_{n-1}][X_n] = R[X_1, \ldots, X_{n-1}, X_n]$ nach Proposition 3G12. □

§**6Eb. Berechnung des ggT in Polynomringen.** In jedem faktoriellen Ring R können wir den ggT definieren (6C12) und dies hat uns bereits gute Dienste geleistet. Leider ist die Definition 6C12 für praktische Berechnungen oft ungeeignet, denn sie setzt die Primfaktorzerlegung in R voraus, und diese ist meist sehr schwer zu berechnen (6B6). In einem euklidischen Ring hingegen, zum Beispiel $\mathbb{Z}$ oder $\mathbb{Q}[X]$, erlaubt der euklidische Algorithmus eine schnelle Berechnung des ggT, die ohne die kostspielige Primfaktorzerlegung auskommt.

Wir wissen, dass $\mathbb{Z}[X]$ faktoriell ist, insbesondere existiert ein ggT zu je zwei Polynomen $P,Q \in \mathbb{Z}[X]$. Anders als in $\mathbb{Q}[X]$ können wir den ggT in $\mathbb{Z}[X]$ leider nicht unmittelbar durch den euklidischen Algorithmus berechnen: $\mathbb{Z}[X]$ ist nicht euklidisch (5H6). Bei genauer Betrachtung liefert der Satz von Gauß dennoch ein praktisches Rechenverfahren:

Sei R ein faktorieller Ring, in dem wir die Funktion $\mathrm{ggT}_R\colon R\times R\to R$ berechnen können. Über dem Bruchkörper K können wir $\mathrm{ggT}_{K[X]}\colon K[X]\times K[X]\to K[X]$ durch den euklidischen Algorithmus (6) berechnen mit anschließender Normierung auf $\mathrm{lc}=1$.

Algorithmus 6 Berechnung des normierten ggT in $K[X]$

Eingabe: zwei Polynome $A_0,B_0\in K[X]$ über einem Körper K.
Ausgabe: das Polynom $A\in\mathrm{GGT}(A_0,B_0)$ mit $\mathrm{lc}\,A=1$ oder $A=0$.

$A\leftarrow A_0,\quad B\leftarrow B_0$	// Invariante: $\mathrm{GGT}(A,B)=\mathrm{GGT}(A_0,B_0)$
while $B\neq 0$ **do**	
$\quad R\leftarrow A \operatorname{rem} B,\quad A\leftarrow B,\quad B\leftarrow R$	// $\mathrm{GGT}(A,B)=\mathrm{GGT}(B,A-QB)$
end while	
if $A=0$ **then return** 0 **else return** $\mathrm{lc}(A)^{-1}A$	// Wir wissen, dass $A\in\mathrm{GGT}(A,0)$

Aus ggT_R und $\mathrm{ggT}_{K[X]}$ lässt sich dann die Abbildung $\mathrm{ggT}_{R[X]}\colon R[X]\times R[X]\to R[X]$ wie in Algorithmus 7 berechnen:

Algorithmus 7 Berechnung von $\mathrm{ggT}_{R[X]}$ mittels ggT_R

Eingabe: zwei Polynome $A,B\in R[X]$
Ausgabe: das Polynom $C=\mathrm{ggT}_{R[X]}(A,B)$.

$c\leftarrow \mathrm{ggT}_R(\mathrm{cont}(A),\mathrm{cont}(B))$	// ggT der Inhalte in R
$C_1\leftarrow \mathrm{red}_R(\mathrm{ggT}_{K[X]}(A,B))$	// ggT in $K[X]$ und Reduktion über R
return $C=cC_1$	

Satz 6E3. *Algorithmus 7 ist korrekt.*

BEWEIS. Der Algorithmus ist korrekt für $A=0$ oder $B=0$. Wir können also $A,B\in R[X]^*$ annehmen. Wir zerlegen A, B und $C=\mathrm{ggT}_{R[X]}(A,B)$ gemäß $A=aA_1$ und $B=bB_1$

und $C = cC_1$ in $a,b,c \in R^*$ und $A_1,B_1,C_1 \in R[X]$ normiert und primitiv.

$$A = \underbrace{\operatorname{lu}(A) \prod_{p\in\mathcal{P}_0} p^{e_p(A)}}_{a} \cdot \underbrace{\prod_{P\in\mathcal{P}_1} P^{e_P(A)}}_{A_1}$$
$$B = \underbrace{\operatorname{lu}(B) \prod_{p\in\mathcal{P}_0} p^{e_p(B)}}_{b} \cdot \underbrace{\prod_{P\in\mathcal{P}_1} P^{e_P(B)}}_{B_1}$$
$$C = \underbrace{\prod_{p\in\mathcal{P}_0} p^{e_p(C)}}_{c} \cdot \underbrace{\prod_{P\in\mathcal{P}_1} P^{e_P(C)}}_{C_1}$$

Die Primfaktorzerlegungen aus dem Satz von Gauß (6E1) zeigen, dass $c = \operatorname{ggT}_R(a,b)$ und $C_1 \sim \operatorname{ggT}_{K[X]}(A,B)$ gilt. Nach Satz 6D11 folgt daraus $C_1 = \operatorname{red}_R(\operatorname{ggT}_{K[X]}(A,B))$. □

Beispiel 6E4. Dieser Algorithmus lässt sich auf $\mathbb{Z}[X]$ anwenden: Wir können $\operatorname{ggT}_{\mathbb{Z}}$ und $\operatorname{ggT}_{\mathbb{Q}[X]}$ jeweils durch den euklidischen Algorithmus berechnen, und die obige Normierung fügt dies zu $\operatorname{ggT}_{\mathbb{Z}[X]}$ zusammen. Dieses Argument lässt sich iterieren: Man kann auf diese Weise den ggT in $\mathbb{Z}[X_1,\dots,X_n]$ berechnen, ebenso in $K[X_1,\dots,X_n]$ über jedem Körper K.

§6F. Fortsetzung des ggT von einem Ring R auf den Polynomring $R[X]$

Der obige Algorithmus 7 ist so bestechend einfach, dass wir diesen Aspekt genauer untersuchen wollen. Wir werden hierzu einen Integritätsring R mit ggT betrachten und zeigen, dass auch der Polynomring $R[X]$ einen ggT erlaubt. Dies verallgemeinert den obigen Satz von Gauß in dem Sinne, dass wir nicht annehmen R sei faktoriell sondern nur den ggT benutzen. Die Faktorialität ist von großem theoretischen Wert aber für die Berechnung des ggT stellt sie sich als nicht notwendig heraus.

§**6Fa. Eigenschaften des ggT.** Ist R ein faktorieller Ring, dann können wir wie in §6Cb gesehen eine Abbildung $\operatorname{ggT}\colon R\times R\to R$ mit folgenden Eigenschaften definieren:

(ggT1) Das Element $\operatorname{ggT}(a,b)$ ist ein größter gemeinsame Teiler von a und b in R.
(ggT2) Es gilt $\operatorname{ggT}(a,1) = 1$ und aus $\operatorname{ggT}(a,b) \sim \operatorname{ggT}(c,d)$ folgt $\operatorname{ggT}(a,b) = \operatorname{ggT}(c,d)$.

Die Bedingung (ggT2) besagt, dass $\operatorname{ggT}(a,b)$ normiert ist. Insbesondere folgt hieraus:

(ggT3) Es gilt $\operatorname{ggT}(au,bv) = \operatorname{ggT}(a,b)$ für alle $a,b \in R$ und $u,v \in R^\times$.
(ggT4) Es gilt $\operatorname{ggT}(a,b) = 1$ falls $a \in R^\times$ oder $b \in R^\times$.

Hieraus folgt weiterhin:

(ggT5) Es gilt die Kommutativität $\operatorname{ggT}(a,b) = \operatorname{ggT}(b,a)$ für alle $a,b \in R$.
(ggT6) Es gilt die Assoziativität $\operatorname{ggT}(\operatorname{ggT}(a,b),c) = \operatorname{ggT}(a,\operatorname{ggT}(b,c))$ für alle $a,b,c \in R$.

Rekursiv können wir daher $\operatorname{ggT}\colon R^n \to R$ für alle $n \geq 3$ definieren durch

$$\operatorname{ggT}(a_1,a_2,\dots,a_n) = \operatorname{ggT}(\operatorname{ggT}(a_1,\dots,a_{n-1}),a_n)$$

und das Ergebnis bleibt unverändert bei Umordnung (Proposition 2E1). Für $n = 1$ setzen wir $\operatorname{ggT}(a) := \operatorname{ggT}(a,0)$ und für $n = 0$ vereinbaren wir die Konvention wir $\operatorname{ggT}() := 0$, denn 0 ist bezüglich Teilbarkeit das größte Element in R.

Bedingung (ggT3) besagt, dass ggT wohldefiniert ist auf Äquivalenzklassen assoziierter Elemente. Insbesondere wählt dies aus jeder Äquivalenzklasse $aR^\times$ den Repräsentanten $\operatorname{ggT}(a)$ aus und induziert eine Abbildung $\operatorname{lu}\colon R^* \to R^\times$ für die $a = \operatorname{lu}(a)\operatorname{ggT}(a)$ gilt. Diese haben wir oben *Leiteinheit* genannt. Für das Nullelement setzen wir $\operatorname{lu}(0) = 0$.

Wir nennen ein Element $a \in R$ *normiert* wenn $\operatorname{lu}(a) = 1$. Jeder ggT ist normiert, denn es gilt $\operatorname{ggT}(\operatorname{ggT}(a,b)) = \operatorname{ggT}(\operatorname{ggT}(a,b),0) = \operatorname{ggT}(a,\operatorname{ggT}(b,0)) = \operatorname{ggT}(a,ub) = \operatorname{ggT}(a,b)$.

§**6Fb. Ringe mit ggT.** Die obigen Eigenschaften erheben wir nun zu Axiomen:

Definition 6F1. Ein *Ring mit ggT* ist ein Paar (R,ggT) bestehend aus einem Integritätsring R und einer Abbildung $\operatorname{ggT}\colon R\times R \to R$, die obige Eigenschaften (ggT1) und (ggT2) erfüllt.

Beispiel 6F2. Jeder faktorielle Ring ist ein Ring mit ggT wie in §6Cb erklärt.

Beispiel 6F3. Jeder Polynomring $K[X]$ über einem Körper K ist ein Ring mit ggT: der euklidische Algorithmus berechnet einen ggT und erfüllt damit (ggT1). Die Normierung in Algorithmus 6 garantiert zusätzlich die Eigenschaft (ggT2).

Beispiel 6F4. Es gibt auch nicht-faktorielle Ringe mit ggT, zum Beispiel der Ring der Puiseux-Polynome $R = K[X^{\mathbb{Q}_{\geq 0}}]$ über einem Körper K (5H23). In R lässt sich der ggT wie in einem Polynomring berechnen, denn jede Familie $P_1,\dots,P_k \in R$ liegt in einem Polynomring $K[X^{1/n}]$ für ein geeignetes n

Wir haben also folgende Situation:

$$\left\{\begin{array}{c}\text{euklidische}\\ \text{Ringe}\end{array}\right\} \subsetneq \left\{\begin{array}{c}\text{Hauptideal-}\\ \text{ringe}\end{array}\right\} \subsetneq \left\{\begin{array}{c}\text{faktorielle}\\ \text{Ringe}\end{array}\right\} \subsetneq \left\{\begin{array}{c}\text{Ringe}\\ \text{mit ggT}\end{array}\right\}$$

In diesem Abschnitt wollen wir Ringe mit ggT untersuchen und sehen, inwieweit sich unsere bisherigen Ergebnisse auf diese Klasse von Ringen erweitern lassen.

Proposition 6F5. *In jedem Ring R mit ggT gelten folgende Regeln:*

1. $\operatorname{ggT}(ab) = \operatorname{ggT}(a)\operatorname{ggT}(b)$ *und somit* $\operatorname{lu}(ab) = \operatorname{lu}(a)\operatorname{lu}(b)$.
2. $\operatorname{ggT}(a_1 b,\cdots,a_n b) = \operatorname{ggT}(a_1,\cdots,a_n)\operatorname{ggT}(b)$.
3. $\operatorname{ggT}(a_1,\dots,a_n) = \operatorname{ggT}(b_1,\dots,b_m)$ *wenn* $\{a_1,\dots,a_n\} = \{b_1,\dots,b_m\}$.
4. $\operatorname{ggT}(a_1,a_2,\dots,a_n) = \operatorname{ggT}(a_1,a_2+b_2a_1,\dots,a_n+b_na_1)$.
5. *Aus* $a \mid a'$ *und* $b \mid b'$ *folgt* $\operatorname{ggT}(a,b) \mid \operatorname{ggT}(a',b')$.
6. $\operatorname{ggT}(a,bc) \mid \operatorname{ggT}(a,b)\operatorname{ggT}(a,c)$.

BEWEIS. (1) Aus $a \sim \operatorname{ggT}(a)$, $b \sim \operatorname{ggT}(b)$ und $ab \sim \operatorname{ggT}(ab)$ folgt $\operatorname{ggT}(a\cdot b) \sim \operatorname{ggT}(a)\cdot \operatorname{ggT}(b)$. Die Normierung (ggT2) garantiert hier Gleichheit. Daraus folgt $\operatorname{lu}(ab) = \operatorname{lu}(a)\operatorname{lu}(b)$.

Die Eigenschaften (2) bis (4) gelten bis auf Assoziierte für jeden größten gemeinsamen Teiler, und die Normierung (ggT2) garantiert hier Gleichheit.

Zu (5): Aus $\operatorname{ggT}(a,b) \mid a \mid a'$ und $\operatorname{ggT}(a,b) \mid b \mid b'$ folgt $\operatorname{ggT}(a,b) \mid \operatorname{ggT}(a',b')$.

Zu (6): Einerseits gilt $\operatorname{ggT}(a,bc) \mid a$ und $a \mid a\operatorname{ggT}(a,c)$, also

$$\operatorname{ggT}(a,bc) \mid a\operatorname{ggT}(a,c).$$

Andererseits gilt $a \mid ba$ also $\operatorname{ggT}(a,bc) \mid \operatorname{ggT}(ba,bc) \sim b\operatorname{ggT}(a,c)$, also

$$\operatorname{ggT}(a,bc) \mid b\operatorname{ggT}(a,c).$$

Aus diesen beiden Eigenschaften folgt

$$\operatorname{ggT}(a,bc) \mid \operatorname{ggT}(a\operatorname{ggT}(a,c), b\operatorname{ggT}(a,c)) = \operatorname{ggT}(a,b)\operatorname{ggT}(a,c). \qquad \square$$

§6Fc. Die Lemmata von Gauß und Euklid.

Lemma 6F6 (Gauß)**.** *In einem Ring mit ggT folgt aus $a \mid bc$ und $\operatorname{ggT}(a,b) = 1$ stets $a \mid c$.*

BEWEIS. Wir haben $a \mid \operatorname{ggT}(a,bc)$ und $\operatorname{ggT}(a,bc) \mid \operatorname{ggT}(a,b)\operatorname{ggT}(a,c) = \operatorname{ggT}(a,c)$. Wegen Transitivität gilt $a \mid \operatorname{ggT}(a,c)$ und somit $a \mid c$. $\square$

Korollar 6F7. *Sei (R, ggT) ein Ring mit ggT. Im Bruchkörper lässt sich dann jedes Element x eindeutig schreiben als $x = \frac{a}{b}$ mit $a,b \in R$ sodass $\operatorname{ggT}(a,b) = 1$ gilt und b normiert ist.*

BEWEIS. *Existenz:* Jedes Element x des Bruchkörpers schreibt sich als Bruch $x = \frac{p}{q}$ mit $p,q \in R$, $q \neq 0$. Das Element $c = \operatorname{lu}(q)\operatorname{ggT}(p,q)$ teilt sowohl p als auch q. Für $a = p/c$ und $b = q/c$ gilt also $x = \frac{p}{q} = \frac{ac}{bc} = \frac{a}{b}$ mit $a,b \in R$ sodass $\operatorname{ggT}(a,b) = 1$ gilt und b normiert ist: Es gilt $\operatorname{ggT}(p,q) = \operatorname{ggT}(ac,bc) = \operatorname{ggT}(a,b)\operatorname{ggT}(c)$, wegen $\operatorname{ggT}(c) = \operatorname{ggT}(p,q)$ also $\operatorname{ggT}(a,b) = 1$. Ferner gilt $\operatorname{lu}(b) = \operatorname{lu}(q)\operatorname{lu}(c)^{-1}$, wegen $\operatorname{lu}(c) = \operatorname{lu}(q)$ also $\operatorname{lu}(b) = 1$.

Eindeutigkeit: Angenommen, $x = \frac{a}{b} = \frac{c}{d}$ mit $a,b,c,d \in R$ sodass $\operatorname{ggT}(a,b) = \operatorname{ggT}(c,d) = 1$ und b,d normiert. Es gilt dann $ad = bc$, und nach dem Lemma von Gauß folgt $b \mid d$ und $d \mid b$, also $b \sim d$. Wegen der Normierung folgt $b = d$ und damit auch $a = c$. $\square$

Lemma 6F8 (Euklid)**.** *In einem Ring mit ggT ist jedes irreduzible Element prim.*

BEWEIS. Sei R ein Ring mit ggT und sei $p \in R$ irreduzibel. Insbesondere ist p nicht invertierbar (5E4) und es bleibt zu zeigen, dass aus $p \mid ab$ folgt $p \mid a$ oder $p \mid b$. Das Element $\operatorname{ggT}(p,a)$ teilt p, und da p irreduzibel ist, folgt $\operatorname{ggT}(p,a) = 1$ oder $\operatorname{ggT}(p,a) \sim p$.

- Wenn $\operatorname{ggT}(p,a) \sim p$, dann gilt $p \mid a$.
- Wenn $\operatorname{ggT}(p,a) = 1$, dann gilt $p \mid b$ nach dem Lemma von Gauß. $\square$

Aus Satz 5E19 folgt nun:

Korollar 6F9. *In jedem Ring mit ggT sind Zerlegungen in irreduzible Faktoren eindeutig.* $\square$

In jedem Ring mit ggT haben wir das kanonische Repräsentantensystem $\mathcal{P} \subset R$ irreduzibler Elemente in R, das aus jeder Äquivalenzklasse $aR^\times$ assoziierter irreduzible Elemente das normierte Element $\operatorname{ggT}(a)$ auswählt. Die Abbildung

$$\Phi_{\mathcal{P}} \colon R^\times \times \mathbb{N}^{(\mathcal{P})} \to R^*, \qquad \Phi_{\mathcal{P}}(u,e) = u \cdot \prod_{p \in \mathcal{P}} p^{e_p} \tag{6.3}$$

ist nach 6F9 injektiv, aber eventuell nicht surjektiv: In R kann es eventuell nicht genügend irreduzible Elemente geben (siehe $K[X^{\mathbb{Q}_{\geq 0}}]$, Übung 5H23).

Korollar 6F10. *Ein Integritätsring R ist genau dann faktoriell, wenn R einen ggT erlaubt und sich jedes Element in R als Produkt irreduzibler Faktoren darstellen lässt.* $\square$

§**6Fd. Das Lemma von Gauß ohne Primelemente.** Sei (R,ggT_R) ein Ring mit ggT gemäß Definition 6F1. Wie zuvor definieren wir zu jedem Polynom $P=a_0+\cdots+a_nX^n$ in $R[X]$ seinen Inhalt $\mathrm{cont}(P):=\mathrm{ggT}(a_0,\ldots,a_n)$ und seine Leiteinheit $\mathrm{lu}(P):=\mathrm{lu}(\mathrm{lc}\,P)$. Wir nennen $P\in R[X]^*$ *primitiv* wenn $\mathrm{cont}(P)=1$ gilt, und *normiert* wenn $\mathrm{lu}(P)=1$ gilt.

Wir beweisen zunächst das Lemma von Gauß (6D3) für Ringe mit ggT. Hierzu stehen uns nach obiger Bemerkung im Allgemeinen keine Primelemente zur Verfügung. Der folgende Beweis beruht statt dessen auf einer handfesten Rechnung mit Hilfe des ggT und erhält dadurch seinen ganz eigenen Reiz:

Lemma 6F11 ("Lemma von Gauß" für Ringe mit ggT)**.** *Sei R ein Ring mit ggT. Sind zwei Polynome $P,Q\in R[X]^*$ primitiv, dann ist auch ihr Produkt PQ primitiv.*

BEWEIS. Das Produkt von $P=a_0+\cdots+a_mX^m$ und $Q=b_0+\cdots+b_nX^n$ bezeichnen wir mit $PQ=c_0+\cdots+c_sX^s$ wobei $s=m+n$. Wir nehmen $\mathrm{ggT}(a_0,\ldots,a_m)=\mathrm{ggT}(b_0,\ldots,b_n)=1$ an und haben $\mathrm{ggT}(c_0,\ldots,c_s)=1$ zu zeigen. Wir führen Induktion über s. Wenn $m=0$, dann gilt $P=a_0\sim 1$ und die Aussage ist klar. Gleiches gilt für $n=0$. Seien also im Folgenden $m,n\geq 1$. Wegen $c_s=a_mb_n$ gilt nach 6F5(6)

$$\mathrm{ggT}(c_0,\ldots,c_s)=\mathrm{ggT}(c_0,\ldots,c_{s-1},a_mb_n)\mid \mathrm{ggT}(c_0,\ldots,c_{s-1},a_m)\,\mathrm{ggT}(c_0,\ldots,c_{s-1},b_n).$$

Für den ersten Faktor gilt nach 6F5(4)

$$\begin{aligned}\mathrm{ggT}(c_0,\ldots,c_{s-1},a_m)&=\mathrm{ggT}(c_0,\ldots,c_{m-1},c_m-a_mb_0,\ldots,c_{s-1}-a_mb_{n-1},a_m)\\&=\mathrm{ggT}(\mathrm{cont}((P-a_mX^m)Q),a_m)\end{aligned}$$

und nach Induktionsvoraussetzung

$$\begin{aligned}&=\mathrm{ggT}(\mathrm{cont}(P-a_mX^m)\,\mathrm{cont}(Q),a_m)\\&=\mathrm{ggT}(\mathrm{cont}(P-a_mX^m),a_m)\\&=\mathrm{ggT}(a_0,\ldots,a_{m-1},a_m)=1.\end{aligned}$$

Ebenso zeigt man $\mathrm{ggT}(c_0,\ldots,c_{s-1},b_n)=1$. Daraus folgt $\mathrm{ggT}(c_0,\ldots,c_s)=1$. □

Proposition 6F12. *Die Abbildungen*

$$\mathrm{cont}\colon R[X]^*\to R^* \qquad \textit{und} \qquad \mathrm{lu}\colon R[X]^*\to R^\times$$

sind Monoidhomomorphismen.

BEWEIS. Zu $P,Q\in R[X]^*$ gilt $P=\mathrm{cont}(P)P_1$ und $Q=\mathrm{cont}(Q)Q_1$ mit $P_1,Q_1\in R[X]^*$ primitiv. Also gilt $PQ=\mathrm{cont}(P)\,\mathrm{cont}(Q)P_1Q_1$ mit P_1Q_1 primitiv nach obigem Lemma von Gauß. Also ist $\mathrm{cont}(PQ)=\mathrm{cont}(P)\,\mathrm{cont}(Q)$ gemäß der Normierung (ggT2).

Die Multiplikativität von lu haben wir bereits in Proposition 6F5(1) gesehen. □

§**6Fe. Konstruktion des ggT für Polynomringe.** Sei (R,ggT_R) ein Ring mit ggT gemäß Definition 6F1. Auf dem Polynomring $R[X]$ konstruieren wir nun eine Abbildung $\mathrm{ggT}_{R[X]}\colon R[X]\times R[X]\to R[X]$, die wiederum den Bedingungen von Definition 6F1 genügt.

Wir gehen hierzu genauso vor wie in den Abschnitten §6D und §6E. Da wir nun jedoch nur über einem Ring mit ggT arbeiten, werden wir in allen Aussagen und Beweisen ohne Primelemente auskommen müssen. Dies gelingt erstaunlich problemlos.

Genauso wie Lemma 6D9 beweist man zunächst:

Lemma 6F13. *Zu jedem Polynom $P \in R[X]^*$ existiert genau ein $c \in R^*$ und $P_1 \in R[X]$, so dass $P = cP_1$ gilt und P_1 normiert und primitiv ist. Hierbei ist $c = \mathrm{lu}(P)\,\mathrm{cont}(P)$.* □

Analog zu Satz 6D11 gehen wir zum Bruchkörper K von R über und erhalten:

Satz 6F14. *Zu jedem Polynom $P \in K[X]^*$ existiert genau ein $c \in K^*$ und $P_1 \in R[X]$ mit $P = cP_1$ und P_1 normiert und primitiv. Zusätzlich gilt $c \in R^*$ genau dann wenn $P \in R[X]^*$.* □

Existenz und Eindeutigkeit dieser Zerlegung definieren die Abbildungen

$$\begin{aligned} \mathrm{red}_R\colon K[X]^* &\to R[X]^*, & P &\mapsto P_1 \text{ normiert und primitiv,} \\ \mathrm{scal}_R\colon K[X]^* &\to K^*, & P &\mapsto c \text{ so dass } P = cP_1. \end{aligned}$$

Die wichtigsten Eigenschaften fassen wir wie in 6D12 zusammen:

Proposition 6F15. *Die Abbildung scal_R erfreut sich folgender Eigenschaften:*

1. *$\mathrm{scal}_R\colon K[X]^* \to K^*$ ist ein Monoidhomomorphismus mit $\mathrm{scal}_R|_{K^*} = \mathrm{id}_{K^*}$.*
2. *Es gilt $\mathrm{scal}_R(P) \in R^*$ genau dann wenn $P \in R[X]^*$.*
3. *Es gilt $\mathrm{scal}_R(P) = 1$ genau dann wenn $P \in R[X]^*$ normiert und primitiv ist.* □

Analog zu Lemma 6D13 leiten wir hieraus ab:

Lemma 6F16 ("Lemma von Gauß" für Ringe mit ggT)**.** *Seien $P, Q \in K[X]$ Polynome mit Leitkoeffizienten $\mathrm{lc}(P) = \mathrm{lc}(Q) = 1$. Aus $PQ \in R[X]$ folgt dann $P, Q \in R[X]$.* □

Schließlich gilt folgender "Satz von Gauß ohne Primelemente":

Satz 6F17 ("Satz von Gauß" für Ringe mit ggT)**.** *Sei (R, ggT_R) ein Ring mit ggT. Dann induziert $\mathrm{ggT}_R\colon R \times R \to R$ eine Abbildung $\mathrm{ggT}_{R[X]}\colon R[X] \times R[X] \to R[X]$ gemäß Algorithmus 7 und $(R[X], \mathrm{ggT}_{R[X]})$ ist ebenfalls ein Ring mit ggT.*

BEWEIS. Das Normierungsaxiom (ggT2) für $\mathrm{ggT}_{R[X]}$ folgt unmittelbar aus der Normierung von ggT_R und $\mathrm{ggT}_{K[X]}$. Es bleibt nur das Axiom (ggT1) nachzuweisen.

Wir haben zu zeigen, dass Algorithmus 7 tatsächlich einen ggT in $R[X]$ liefert. Die Aussage ist klar für $A = 0$ oder $B = 0$. Wir können also $A, B \in R[X]^*$ annehmen. Wir zerlegen $A = aA_1$ und $B = bB_1$ in $a, b \in R^*$ und $A_1, B_1 \in R[X]^*$ normiert und primitiv. In $K[X]$ gilt $A \sim A_1$ und $B \sim B_1$, somit $\mathrm{ggT}_{K[X]}(A,B) = \mathrm{ggT}_{K[X]}(A_1,B_1)$. Deshalb ist $C_1 = \mathrm{red}_R(\mathrm{ggT}_{K[X]}(A,B))$ ein ggT von A_1 und B_1 in $K[X]$.

- C_1 ist ein größter gemeinsamer Teiler von A_1 und B_1 in $R[X]$.

In $K[X]$ gilt dies nach Konstruktion. Daher gilt $C_1 Q = A_1$ mit $Q \in K[X]$, und somit

$$1 = \mathrm{scal}(A_1) = \mathrm{scal}(C_1 Q) = \mathrm{scal}(C_1)\,\mathrm{scal}(Q) = \mathrm{scal}(Q),$$

also $Q \in R[X]$. Das bedeutet, C_1 teilt A_1 in $R[X]$. Ebenso sehen wir: C_1 teilt B_1 in $R[X]$.

Sei nun $D \in R[X]$ ein beliebiger gemeinsamer Teiler von A_1 und B_1 in $R[X]$. Dann gilt $DQ = A_1$ mit $Q \in R[X]$, also $1 = \mathrm{scal}(A_1) = \mathrm{scal}(DQ) = \mathrm{scal}(D)\,\mathrm{scal}(Q)$. Anders gesagt, $\mathrm{scal}(D) \in R^\times$. Weiter gilt $DP = C_1$ mit $P \in K[X]$. Daraus folgt $\mathrm{scal}(P) = \mathrm{scal}(D)^{-1} \in R^\times$. Somit gilt $P \in R[X]$, also $D \mid C_1$ in $R[X]$.

- cC_1 ist ein größter gemeinsamer Teiler von A und B in $R[X]$.

Nach Konstruktion gilt $c \mid a,b$ in R und $C_1 \mid A_1, B_1$ in $R[X]$, also ist cC_1 ein gemeinsamer Teiler von $A = aA_1$ und $B = bB_1$ in $R[X]$. Sei nun $D \in R[X]^*$ ein beliebiger gemeinsamer Teiler von A und B in $R[X]$. Wir zerlegen $D = dD_1$ mit $d \in R^*$ und $D_1 \in R[X]^*$ normiert und primitiv. Aus $DQ = A$ mit $Q \in R[X]^*$, folgt $dD_1qQ_1 = A$. Somit $a = \operatorname{scal}(A) = \operatorname{scal}(dD_1qQ_1) = dq$, also $d \mid a$. Ebenso sehen wir $d \mid b$. Demnach gilt $d \mid c = \operatorname{ggT}_R(a,b)$. Wegen $D_1 \mid A_1$ und $D_1 \mid B_1$ wissen wir bereits $D_1 \mid C_1$. Daraus folgt $dD_1 \mid cC_1$. Also ist cC_1 tatsächlich ein ggT von $A = aA_1$ und $B = bB_1$ in $R[X]$. □

§**6Ff. Alternativer Beweis des Satzes von Gauß für faktorielle Ringe.** Zum Abschluss wollen wir zeigen: Wenn in einem Integritätsring R jedes Element eine Zerlegung in irreduzible Faktoren erlaubt, dann gilt dies auch für den Polynomring $R[X]$. Nach Proposition 5E20 ist dies gleichbedeutend mit der aufsteigenden Kettenbedingung für Hauptideale.

Proposition 6F18. *Angenommen der Integritätsring R erfüllt die aufsteigende Kettenbedingung für Hauptideale. Dann gilt dies auch für den Polynomring $R[X]$.*

BEWEIS. Sei $(P_0) \subset (P_1) \subset (P_2) \subset \dots$ eine aufsteigende Kette von Hauptidealen in $R[X]$. Es gilt dann $P_{k+1} \mid P_k$ für alle $k \in \mathbb{N}$, also muss der Grad $\deg P_0 \geq \deg P_1 \geq \deg P_2 \geq \dots$ in $\mathbb{N}$ stationär werden, das heißt $\deg P_n = \deg P_{n+1} = \deg P_{n+2} = \dots$ ab einem gewissen Index $n \in \mathbb{N}$. Das bedeutet $P_k = a_k P_{k+1}$ mit $a_k \in R$ für alle $k \geq n$. Für die Leitkoeffizienten gilt $\operatorname{lc} P_{k+1} \mid \operatorname{lc} P_k$, also muss auch die Kette $(\operatorname{lc} P_0) \subset (\operatorname{lc} P_1) \subset (\operatorname{lc} P_2) \subset \dots$ in R stationär werden. Das bedeutet $\operatorname{lc} P_m \sim \operatorname{lc} P_{m+1} \sim \operatorname{lc} P_{m+2} \sim \dots$ ab einem gewissen Index $m \in \mathbb{N}$. Wir schließen daraus $a_k \in R^\times$ für alle $k \geq \max\{m,n\}$, und somit $P_k \sim P_{k+1}$. □

Zusammenfassend liefert die Fortsetzung des ggT von R auf $R[X]$ (§6F) einen alternativen Beweis des Satzes von Gauß für faktorielle Ringe (§6E). Wie wir gesehen haben, kann man nämlich Existenz und Eindeutig von Zerlegungen getrennt behandeln:

1. Erlaubt R Zerlegungen in irreduzible Faktoren, dann auch $R[X]$. (6F18)
2. Erlaubt R einen ggT, dann induziert dieser einen ggT auf $R[X]$. (6F17)

Nach Korollar 6F10 sind beide Bedingungen zusammen äquivalent zur Faktorialität.

§6G. Irreduzibilitätskriterien

Wir wissen, dass über einem faktoriellen Ring R auch der Polynomring $R[X]$ faktoriell ist (§6E). Aus praktischer Sicht können wir ausgehend vom ggT in R auch den ggT in $R[X]$ berechnen (§6F). Wir kommen nun zu einer weiteren wichtigen Frage: Wie kann man zu einem gegebenen Polynom $P \in R[X]$ feststellen, ob P irreduzibel ist? Hierzu wollen wir nun einige einfache Kriterien aufstellen, insbesondere das Abbildungskriterium und das Kriterium von Eisenstein.

§**6Ga. Folgerungen aus dem Satz von Gauß.** Sei weiterhin R ein faktorieller Ring und K sein Bruchkörper. Wie verhalten sich irreduzible Elemente beim Übergang zwischen $R[X]$ und $K[X]$? Polynome $P \in R[X]$ vom Grad 0 sind genau die Ringelemente $P \in R^*$, und diese werden in K invertierbar. Dieses Phänomen spielt auch im Grad ≥ 1 eine Rolle:

Beispiel 6G1. Das Polynom $P = 6X - 4$ ist irreduzibel in $\mathbb{Q}[X]$ aber nicht irreduzibel in $\mathbb{Z}[X]$ denn $2 \cdot (3X-2)$ ist hier eine echte Zerlegung.

Proposition 6G2. *Für $P \in R[X]$ über einem faktoriellen Ring R sind äquivalent:*

- *P ist irreduzibel in $R[X]$ und $\deg P \geq 1$.*
- *P ist irreduzibel in $K[X]$ und $\operatorname{cont}(P) = 1$.*

BEWEIS. "$\Leftarrow$" Ist $P \in R[X]$ irreduzibel in $K[X]$, dann gilt nach 6E1 die Zerlegung $P = aP_1$ mit $a \in R^*$ und $P_1 \in \mathcal{P}_1$. Gilt zudem $\operatorname{cont}(P) = 1$, dann ist P auch irreduzibel in $R[X]$.

"$\Rightarrow$" Ist $P \in R[X]$ mit $\deg P \geq 1$ irreduzibel in $R[X]$, dann gilt nach 6E1 die Zerlegung $P = uP_1$ mit $u \in R^\times$ und $P_1 \in \mathcal{P}_1$. Daher gilt $\operatorname{cont}(P) = 1$ und P ist irreduzibel in $K[X]$. □

Warnung. — Proposition 6G2 gilt für faktorielle Ringe. Ist R ein Integritätsring aber nicht faktoriell, dann kann ein irreduzibles Polynom über dem Bruchkörper zerfallen:

Beispiel 6G3. Der Ring $R = \mathbb{Q}[X^2, X^3]$ ist nicht faktoriell (5H10). In $R[Y]$ ist $P = Y^2 - X^2$ unzerlegbar, denn die (bis auf Assoziierte einzige) Zerlegung $(Y-X)(Y+X)$ in $\mathbb{Q}[X]$ steht in R nicht mehr zur Verfügung. Der Bruchkörper $K = \operatorname{Frac}(R)$ ist hier $\mathbb{Q}(X) = \operatorname{Frac}(Q[X])$, denn $X = X^3/X^2$. In $K[Y]$ zerfällt daher P wie gewohnt in $P = (Y-X)(Y+X)$.

Der Ring $R = \mathbb{Z}[i\sqrt{3}]$ ist nicht faktoriell (5H19). Das Polynom $P = X^2 + X + 1$ ist irreduzibel, denn wegen $R^\times = \{\pm 1\}$ kommen als Faktoren nur $X \pm 1$ in Frage. Über dem Bruchkörper ist P jedoch zerlegbar gemäß $P = (X + \frac{1+i\sqrt{3}}{2})(X + \frac{1-i\sqrt{3}}{2})$.

§**6Gb. Nullstellen.** Wir beginnen mit einer einfachen Vorbemerkung:

Proposition 6G4. *Über einem Körper K ist $P \in K[X]$ genau dann irreduzibel, wenn $\deg P \geq 1$ gilt und es keine Zerlegung $P = P_1P_2$ mit $0 < \deg P_1 < n$ und $0 < \deg P_2 < n$ gibt.*

BEWEIS. Wegen $K[X]^\times = K^\times = K^*$ ist P genau dann invertierbar wenn $\deg P = 0$. □

Korollar 6G5. *Sei K ein Körper und $P \in K[X]$ ein Polynom vom Grad 2 oder 3. Dann ist P genau dann irreduzibel in $K[X]$, wenn P keine Nullstellen in K hat.*

BEWEIS. "$\Rightarrow$": Wenn $P(a) = 0$, dann ist P nicht irreduzibel, denn es erlaubt eine echte Zerlegung $P = (X-a)P_1$ mit $\deg(X-a) = 1$ und $\deg P_1 \geq 1$.

"$\Leftarrow$": Angenommen $P = P_1P_2$ wäre eine echte Zerlegung. Dann muss $\deg P_1, \deg P_2 \geq 1$ gelten. Aus $\deg P \leq 3$ folgt $\deg P_1 = 1$ oder $\deg P_2 = 1$. Daher hat P eine Nullstelle. □

Beispiel 6G6. Das Polynom $P = X^2 - 2$ ist irreduzibel über $\mathbb{Q}$.
Über $\mathbb{R}$ ist $P = (X - \sqrt{2})(X + \sqrt{2})$ zerlegbar.

Beispiel 6G7. Das Polynom $P = X^3 - 2$ ist irreduzibel über $\mathbb{Q}$.
Über $\mathbb{R}$ ist $P = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$ zerlegbar.

Warnung. — Dieses einfache Kriterium gilt nicht mehr für Polynome $\deg P \geq 4$.

Beispiel 6G8. Das Polynom $P = X^4 - 4 \in \mathbb{Q}[X]$ hat keine Nullstellen in $\mathbb{Q}$, ist aber in $\mathbb{Q}[X]$ zerlegbar, denn es gilt $P = (X^2 - 2)(X^2 + 2)$.

Zum Auffinden möglicher Nullstellen ist manchmal folgende Beobachtung nützlich:

Proposition 6G9. *Sei R ein faktorieller Ring und $P = c_0 + \cdots + c_n X^n$ ein Polynom über R mit $c_0, c_n \in R^*$. Sei $x = \frac{a}{b}$ ein Element des Bruchkörpers mit $a, b \in R$, $b \neq 0$, $\operatorname{ggT}(a,b) = 1$. Wenn x eine Nullstelle von P ist, dann gilt $a \mid c_0$ und $b \mid c_n$.*

BEWEIS. Aus $P(x) = 0$ folgt $0 = b^n P(\frac{a}{b}) = b^n c_0 + ab^{n-1}c_1 + \cdots + a^{n-1}bc_{n-1} a^n c_n$. Hieraus folgt $a \mid b^n c_0$ und $b \mid a^n c_n$. Wegen $\operatorname{ggT}(a,b) = 1$ folgt dann $a \mid c_0$ und $b \mid c_n$. □

Korollar 6G10. *Sei R ein faktorieller Ring und $P = X^n + c_{n-1}X^{n-1} + \cdots + c_0 \in R[X]$. Jede Nullstelle von P im Bruchkörper von R liegt bereits in R.* □

Beispiel 6G11. Für $n \geq 2$ hat das Polynom $P = X^n - 2$ keine Nullstelle in $\mathbb{Z}$. Wegen $\operatorname{lc}(P) = 1$ hat P auch keine Nullstelle im Bruchkörper $\mathbb{Q}$. Anders gesagt, $\sqrt[n]{2} \in \mathbb{R}$ ist irrational.

Aus Kapitel 1 zu Konstruktionen mit Zirkel und Lineal kennen wir bereits folgende Beispiele, für deren Untersuchung wir bereits Proposition 6G9 benutzt haben:

Beispiel 6G12. Die Zahl $\eta = 2\cos(2\pi/7)$ erfüllt die Gleichung $\eta^3 + \eta^2 - 2\eta - 1 = 0$ (siehe §1Cb). Das Polynom $P = X^3 + X^2 - 2X - 1$ hat keine ganzzahligen Nullstellen und wegen $\operatorname{lc}(P) = 1$ auch keine rationalen Nullstellen. Daher ist $\eta \in \mathbb{R}$ nicht rational.

Beispiel 6G13. Die Zahl $\kappa = 2\cos(2\pi/9)$ erfüllt die Gleichung $\kappa^3 - 3\kappa + 1 = 0$ (siehe §1Cc). Das Polynom $P = X^3 - 3X + 1$ hat keine ganzzahligen Nullstellen und wegen $\operatorname{lc}(P) = 1$ auch keine rationalen Nullstellen. Daher ist $\kappa \in \mathbb{R}$ nicht rational.

§**6Gc. Abbildungskriterium.** Über einem Integritätsring R nennen wir ein Polynom $P = a_0 + \cdots + a_n X^n$ in $R[X]$ *primitiv*, wenn $1 \in \operatorname{GGT}(a_0, \ldots, a_n)$ gilt.

Proposition 6G14. *Sei $\varphi\colon R \to S$ ein Homomorphismus zwischen Integritätsringen, den wir zu $\Phi\colon R[X] \to S[X]$ fortsetzen. Sei $P \in R[X]$ primitiv und $\varphi(\operatorname{lc} P) \neq 0$. Wenn dann $\Phi(P)$ irreduzibel in $S[X]$ ist, dann ist P irreduzibel in $R[X]$.*

BEWEIS. Angenommen $P = P_1 P_2$ wäre eine echte Zerlegung, also $P_1, P_2 \notin R^\times$. Da P primitiv ist, bedeutet dies $\deg P_1 \geq 1$ und $\deg P_2 \geq 1$. Einerseits gilt $\deg \Phi(P_1) \leq \deg P_1$ und $\deg \Phi(P_2) \leq \deg P_2$. Andererseits hat das Bild $\Phi(P) = \Phi(P_1)\Phi(P_2)$ Grad n wegen $\varphi(\operatorname{lc} P) \neq 0$. Daher muss $\deg \Phi(P_1) = \deg P_1$ und $\deg \Phi(P_2) = \deg P_2$ gelten, und somit ist $\Phi(P) = \Phi(P_1)\Phi(P_2)$ eine echte Zerlegung in $S[X]$. □

Dieses Abbildungskriterium hat folgenden Nutzen: Das Polynom P über R ist vorgegeben. Wenn die Irreduzibilitätsfrage sich über R als zu schwer erweist, dann können wir zu einem Quotienten $S = R/I$ unserer Wahl übergehen. Die Hoffnung ist dabei, dass das Problem über S leichter zu lösen ist. Das ist manchmal tatsächlich der Fall:

Beispiel 6G15. Ist das Polynom $3X^3 + 5X + 7$ in $\mathbb{Z}[X]$ irreduzibel? Es ist primitiv und die Reduktion $\varphi\colon \mathbb{Z} \mapsto \mathbb{Z}/_2$ liefert $\Phi(P) = X^3 + X + 1$ in $\mathbb{Z}/_2[X]$. Letzteres ist irreduzibel, denn $X^3 + X + 1$ hat Grad 3 aber keine Nullstellen in $\mathbb{Z}/_2$. Also ist P in $\mathbb{Z}[X]$ irreduzibel.

Warnung. — Beide Voraussetzungen "P primitiv" und "$\varphi(\operatorname{lc} P) \neq 0$" sind wesentlich.

Beispiel 6G16. Das Polynom $P = 2X^2 + X$ ist zerlegbar in $\mathbb{Z}[X]$, aber im Quotienten $\mathbb{Z}/_2[X]$ ist $\Phi(P) = X$ irreduzibel. Zwar ist P primitiv, aber $\varphi(\operatorname{lc} P) = 0$.

Beispiel 6G17. Das Polynom $P = 3X$ ist zerlegbar in $\mathbb{Z}[X]$, aber im Quotienten $\mathbb{Z}/_2[X]$ ist $\Phi(P) = X$ irreduzibel. Zwar gilt $\varphi(\operatorname{lc} P) \neq 0$, aber P ist nicht primitiv.

§**6Gd. Das Irreduzibilitätskriterium von Eisenstein.** Das folgende Kriterium von Eisenstein verfeinert das Abbildungskriterium aus der vorhergehenden Proposition:

Satz 6G18 (Eisenstein)**.** *Sei R ein Integritätsring und $P = a_0 + \cdots + a_n X^n \in R[X]$ ein Polynom vom Grad $n \geq 1$ über R, das folgenden Bedingungen genügt:*

1. *P ist primitiv, das heißt $1 \in \operatorname{GGT}(a_0, \ldots, a_n)$.*
2. *Es gibt ein Primelement $p \in R$ sodass $p \mid a_0, \ldots, a_{n-1}$ gilt aber $p \nmid a_n$ sowie $p^2 \nmid a_0$.*

Dann ist P irreduzibel in $R[X]$.

Notation. Ein Polynom $P \in R[X]$, das Bedingung (2) erfüllt, nennen wir *Eisenstein-Polynom bezüglich des Primelements p.*

BEWEIS. Angenommen $P = P_1 P_2$ wäre eine echte Zerlegung, das heißt $P_1, P_2 \notin R^\times$. Da P primitiv ist, bedeutet dies $\deg P_1 \geq 1$ und $\deg P_2 \geq 1$, also $P_1 = b_0 + \cdots + b_k X^k$ und $P_2 = c_0 + \cdots + c_\ell X^\ell$ mit $k, \ell \geq 1$.

Sei $\varphi\colon R \to R/p$ die Quotientenabbildung, die wir zu $\Phi\colon R[X] \to (R/p)[X]$ fortsetzen. Nach Voraussetzung gilt $\Phi(P) = aX^n$ wobei $a = \varphi(a_n) \neq 0$. Daher muss $\deg \Phi(P_1) = k$ und $\deg \Phi(P_2) = \ell$ gelten, Da wir p als prim voraussetzen, ist der Ring R/p nullteilerfrei. Über dem Bruchkörper K von R/p kennen wir alle echten Zerlegungen $aX^n = \bar{P}_1 \bar{P}_2$: diese sind $\bar{P}_1 = bX^k$ und $\bar{P}_2 = cX^\ell$ mit $b, c \in K^*$ und $k, \ell \geq 1$. Da wir $\Phi(P_1), \Phi(P_2) \in (R/p)[X]$ annehmen, gilt also $\Phi(P_1) = aX^k$ und $\Phi(P_2) = bX^\ell$ mit $a, b \in (R/p)^*$.

In $R[X]$ bedeutet dies, $p \mid b_0, \ldots, b_{k-1}$ und $p \mid c_0, \ldots, c_{\ell-1}$. Demnach teilt p^2 den Koeffizienten $a_0 = b_0 c_0$. Das ist aber nach Voraussetzung ausgeschlossen. □

Beispiel 6G19. In $\mathbb{Z}[X]$ ist $P = 2X^n + 9X + 6$ primitiv für alle $n \in \mathbb{N}$ (auch $n = 1$ und $n = 0$). Für $n \geq 1$ ist P ein Eisenstein-Polynom bezüglich $p = 3$. (Für $n \leq 1$ ist P ein Eisenstein-Polynom bezüglich $p = 2$.) Es ist daher irreduzibel in $\mathbb{Z}[X]$.

Bemerkung 6G20. Der Satz besagt, dass jedes *primitive* Eisenstein-Polynom P in $R[X]$ irreduzibel ist. Ist R faktoriell, dann ist P auch irreduzibel über dem Bruchkörper (6G2). Letzteres gilt auch dann noch, wenn man die Bedingung (1) "P ist primitiv" weglässt.

Beispiel 6G21. Primitivität (1) folgt nicht aus der Eisenstein-Bedingung (2). Zum Beispiel ist $P = 2X^5 + 18X + 6$ ein Eisenstein-Polynom bezüglich $p = 3$ aber nicht primitiv und daher zerlegbar in $\mathbb{Z}[X]$: Es gilt $P = 2Q$ mit $Q = X^5 + 9X + 3$. Letzteres ist ein primitives Eisensteinpolynom, also irreduzibel in $\mathbb{Z}[X]$. Sowohl P als auch Q sind irreduzibel in $\mathbb{Q}[X]$. (Die Zerlegung $P = 2Q$ gilt in $\mathbb{Q}[X]$ nicht als echte Zerlegung wegen $2 \in \mathbb{Q}[X]^\times$.)

Beispiel 6G22. Das Kriterium von Eisenstein ist hinreichend aber selbstverständlich nicht notwendig für die Irreduzibilität. Zum Beispiel ist $3X^3 + 5X + 7$ irreduzibel in $\mathbb{Z}[X]$ nach 6G15. Es ist aber kein Eisenstein-Polynom (weder für $p = 5$ noch für $p = 7$).

§**6Ge. Kreisteilungspolynome.** Eine schöne und wichtige Anwendung des Kriteriums von Eisenstein ist der Nachweis der Irreduzibilität gewisser Kreisteilungspolynome.

Für jedes $n \geq 1$ hat das Polynom $X^n - 1$ als Nullstellen in $\mathbb{C}$ die n-ten *Einheitswurzeln* $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ wobei $\zeta = e^{2\pi i/n}$. Also gilt

$$X^n - 1 = (X-1)(X-\zeta)(X-\zeta^2)\cdots(X-\zeta^{n-1}) \qquad \text{in } \mathbb{C}[X].$$

Über den rationalen Zahlen hat man wenigstens die Zerlegung

$$X^n - 1 = (X-1)(X^{n-1} + X^{n-1} + \cdots + X + 1) \qquad \text{in } \mathbb{Q}[X].$$

Man wird nun versucht sein, den zweiten Faktor in $\mathbb{Q}[X]$ soweit möglich noch weiter zu zerlegen. Zumindest für jede Primzahl n ist diese Frage nun leicht beantwortet:

Satz 6G23. *Ist $p \geq 2$ prim, dann ist*

$$\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1$$

irreduzibel in $\mathbb{Q}[X]$.

BEWEIS. Aus $(X-1)\Phi_p(X) = X^p - 1$ erhalten wir durch Substitution $X \mapsto X+1$

$$X\Phi_p(X+1) = (X+1)^p - 1 = X^p + \binom{p}{1}X^{p-1} + \cdots + \binom{p}{p-1}X.$$

Demnach berechnet sich das Polynom $P(X) = \Phi_p(X+1)$ zu

$$P = X^{p-1} + \binom{p}{1}X^{p-2} + \cdots + \binom{p}{p-2}X + p.$$

Dieses Polynom liegt in $\mathbb{Z}[X]$ und ist ein primitives Eisenstein-Polynom bezüglich der Primzahl p, denn $p \mid \binom{p}{k}$ für alle $0 < k < p$ (Übung 5H1). Damit ist $\Phi_p(X+1)$ also irreduzibel in $\mathbb{Z}[X]$. Die Ersetzungen $X \mapsto X+1$ und $X \mapsto X-1$ induzieren zueinander inverse Automorphismen $\mathbb{Z}[X] \xrightarrow{\sim} \mathbb{Z}[X]$. Also ist mit $\Phi_p(X+1)$ auch $\Phi_p(X)$ irreduzibel in $\mathbb{Z}[X]$. Insbesondere ist $\Phi_p(X)$ dann irreduzibel in $\mathbb{Q}[X]$ (6G2). □

Satz 6G24. *Ist $p \geq 2$ prim und $r \geq 0$, dann ist*

$$\Phi_p(X^{p^r}) = X^{p^r(p-1)} + X^{p^r(p-1)} + \cdots + X^{p^r} + 1$$

irreduzibel in $\mathbb{Q}[X]$.

BEWEIS. Für $r = 0$ ist dies der vorhergehende Satz: Wir haben oben gesehen, dass $P(X) = \Phi_p(X+1)$ ein Eisenstein-Polynom bezüglich p ist. Also ist auch $P(X^{p^r})$ ein Eisenstein-Polynom bezüglich p. Modulo p gilt aber

$$P(X^{p^r}) \equiv P(X)^{p^r} = \Phi_p(X+1)^{p^r} \equiv \Phi_p((X+1)^{p^r}),$$

das heißt, p teilt alle Koeffizienten von $\Phi_p((X+1)^{p^r})$ bis auf den Leitkoeffizienten. Wegen $\Phi_p(1) = p$ ist damit auch $\Phi_p((X+1)^{p^r})$ ein Eisenstein-Polynom bezüglich p. Da es zudem primitiv ist, ist $\Phi_p((X+1)^{p^r})$ somit irreduzibel in $\mathbb{Z}[X]$. Nach Substitution $X \mapsto X-1$ sehen wir schließlich, dass $\Phi_p(X^{p^r})$ irreduzibel in $\mathbb{Z}[X]$ ist, also auch in $\mathbb{Q}[X]$. □

§6H. Übungen und Ergänzungen

§6Ha. Inhalt und ggT von Polynomen.

Übung 6H1. Man bestimme den Inhalt von $P = X^3Y + X^3 + X^2Y^2 - X^2 + XY^3 - XY$ in $\mathbb{Q}[Y][X]$ und anschließend in $\mathbb{Q}[X][Y]$.

Übung 6H2. Man berechne den ggT folgender Polynome:

1. $P = 24X^3 - 81$ und $Q = 24X^2 - 72X + 54$ in $\mathbb{Z}[X]$.
2. $P = XY^3 + X^2Y - Y^2 - X$ und $Q = XY^3 - X^3Y - Y^2 + X^2$ in $\mathbb{Q}[X,Y]$.
3. In beiden Fällen zerlege man P und Q in irreduzible Faktoren.

§6Hb. Irreduzible Polynome.

Übung 6H3. Ist $P = X^2 + Y^2 - 1$ irreduzibel in $\mathbb{C}[X,Y]$? und in $\mathbb{Z}/_2[X,X]$?

Übung 6H4. Man zeige: $\sqrt[n]{a}$ mit $a \in \mathbb{N}$, $n \in \mathbb{N}_{\geq 2}$, ist entweder ganz oder irrational.

Übung 6H5. Man bestimme alle irreduziblen Polynome vom Grad ≤ 3 über $\mathbb{Z}/_2$ und $\mathbb{Z}/_3$.

Übung 6H6. Welche der folgenden Polynome sind irreduzibel in $\mathbb{Z}[X]$?

1. $X^3 + 14X^2 + 19X + 25$
2. $X^3 + 35X^2 + 18X + 45$
3. $X^3 + 5X^2 + 7X + 13$

Übung 6H7. Man zerlege die folgenden Polynome in $\mathbb{Q}[X]$:

1. $X^3 - X + 1$
2. $X^3 - X - 1$
3. $X^3 - 2X^2 + X + 15$
4. $X^3 + 5X + 3$
5. $9X^3 + 7X + 3$
6. $X^3 + 3X^2 + 6X + 5$
7. $X^3 + 3X^2 + 5X + 6$
8. $4X^2 + 4X + 1$
9. $2X^3 + 3X^2 + 3X + 1$

Übung 6H8. Man zerlege $2X^5 - 5X^4 - 21X^3 - 15X^2 - 23X - 10$ in $\mathbb{Z}[X]$.

Übung 6H9. Man zerlege $X^4 + 1$ in $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Q}[X]$, $\mathbb{Z}[X]$, $\mathbb{Z}/_2[X]$, $\mathbb{Z}/_3[X]$.

Übung 6H10. Ist $X^4 - 10X^3 + 21X^2 - 10X + 11$ irreduzibel in $\mathbb{Z}[X]$?

§6Hc. Zum Kriterium von Eisenstein.

Übung 6H11. Man finde ein irreduzibles Polynom $P \in \mathbb{Q}[X]$, sodass $P(X^n)$ zerlegbar ist für ein $n \geq 2$. Kann das auch passieren, wenn $P \in \mathbb{Z}[X]$ ein Eisenstein-Polynom ist?

Übung 6H12. Für $n \geq 3$ zerlege man $P = 6X^n - 6X^{n-1} + 24X^2 - 36X + 18$ in $\mathbb{Z}[X]$.

Übung 6H13. Man zerlege die folgenden Polynome in $\mathbb{Z}[X]$:

1. $X^4 - 4X^3 + 6$
2. $X^4 - 6X^3 + 12$
3. $X^3 + nX + 2$
4. $X^4 + 10X^2 + 1$
5. $X^4 + 4X^3 + 6X^2 + 2X + 1$
6. $X^8 - 1$

Für das Kriterium von Eisenstein ist manchmal folgender Trick hilfreich:

Übung 6H14. Ein Polynom $P \in R[X]$ ist irreduzibel genau dann wenn $P(X+b)$ es ist.

Dies führt uns zu der Frage nach den Automorphismen des Rings $R[X]$ über R:

Übung 6H15. Für $a, b \in R$ existiert genau ein Ringhomomorphismus $\varphi_{a,b}\colon R[X] \to R[X]$ mit $\varphi_{a,b}|_R = \mathrm{id}_R$ und $X \mapsto aX + b$. Man zeige, dass $\varphi_{a,b}$ genau dann ein Automorphismus ist, wenn $a \in R^\times$ gilt. In diesem Falle gebe man $\varphi_{a,b}^{-1}$ explizit an.

Übung 6H16. Es sei $\mathrm{Aut}_R(R[X])$ die Gruppe der Ringautomorphismen $\varphi\colon R[X] \xrightarrow{\sim} R[X]$ mit $\varphi|_R = \mathrm{id}_R$. Man zeige $\mathrm{Aut}_R(R[X]) = \{\ \varphi_{a,b} \mid a \in R^\times, b \in R\ \}$.

§**6Hd. Die Determinante als Polynom betrachtet.** Im Ring $R_n = \mathbb{Z}[X_{ij} \mid 1 \le i, j \le n]$ sei D_n die Determinante der allgemeinen Matrix

$$D_n = \det \begin{pmatrix} X_{11} & \dots & X_{1n} \\ \vdots & & \vdots \\ X_{n1} & \dots & X_{nn} \end{pmatrix}.$$

Übung 6H17. Man zeige, dass $D_2 = X_{11}X_{22} - X_{12}X_{21}$ irreduzibel in R_2 ist.

Übung 6H18. Man zeige per Induktion, dass D_n irreduzibel in R_n ist.

Hinweis: $R_n = R'_n[X_{nn}]$ ist der Polynomring in X_{nn} über $R'_n = \mathbb{Z}[X_{ij} \mid (i,j) \neq (n,n)]$. Man bestimme den Inhalt von $D_n = D_{n-1}X_{nn} + P_n \in R'_n[X_{nn}]$.

§**6He. Zum Lemma von Gauß in Monoidringen.** Sei M ein Monoid und R ein Ring mit ggT. Jedes Element $P \in R[M]^*$ des Monoidrings von M über R schreibt sich als Summe $P = a_1 g_1 + \dots + a_n g_n$ mit $a_1, \dots, a_n \in R^*$ und verschiedenen $g_1, \dots, g_n \in M$. Diese Schreibweise ist eindeutig bis auf die Reihenfolge der Summanden. Somit können wir den Inhalt $\mathrm{cont}(P) := \mathrm{ggT}(a_1, \dots, a_n)$ definieren. Das Lemma von Gauß gilt im Allgemeinen nicht:

Beispiel 6H19. Sei $M = \{1, g\}$ mit $g \neq 1$ und $g^2 = 1$. In $\mathbb{Z}[M]$ ist $P = 1 + g$ primitiv, aber $P^2 = 2 + 2g$ nicht. In diesem Fall hat der Ring $\mathbb{Z}[M]$ auch Nullteiler, denn $1 + g \neq 0$ und $1 - g \neq 0$ aber $(1+g)(1-g) = 1 - g^2 = 0$.

Wir nehmen nun an, das Monoid M sei linear geordnet sodass aus $a \le b$ stets $ac \le bc$ und $ca \le cb$ folgt. Jedes Element $P \in R[M]^*$ des Monoidrings von M über R schreibt sich dann eindeutig als $P = a_1 g_1 + \dots + a_n g_n$ mit $a_1, \dots, a_n \in R^*$und $g_1 < \dots < g_n$ in M. Dies erlaubt, den *Leitkoeffizienten* $\mathrm{lc}\, P := a_n$ zu definieren.

Übung 6H20. Sei R ein nullteilerfreier Ring und $(M, \le)$ ein linear geordnetes Monoid.

1. Für $P, Q \in R[M]^*$ gilt $\mathrm{lc}(PQ) = \mathrm{lc}\, P \cdot \mathrm{lc}\, Q$ und insbesondere $PQ \neq 0$.

2. Sind $P, Q \in R[M]^*$ primitiv, dann ist auch das Produkt PQ primitiv.
3. Die Abbildung $\operatorname{cont}\colon R[M]^* \to R^*$ ist ein Monoidhomomorphismus.

Übung 6H21. Als Fortsetzung von Übung 5H23 zeige man:

1. Ist K ein Körper, dann ist der Monoidring $K[X^{\mathbb{Q}_{\geq 0}}]$ ein Ring mit ggT.
   Der ggT in $K[X^{\mathbb{Q}_{\geq 0}}]$ lässt sich mit Hilfe des euklidischen Algorithmus berechnen.
2. Ist R ein Ring mit ggT, dann ist auch $R[X^{\mathbb{Q}_{\geq 0}}]$ ein Ring mit ggT.
   Der ggT in $R[X^{\mathbb{Q}_{\geq 0}}]$ lässt sich aus dem in R und in $K[X^{\mathbb{Q}_{\geq 0}}]$ berechnen.

KAPITEL 7

Matrizenringe und der Elementarteilersatz

§7A. Einführung und Motivation

Wir wollen ein *lineares Gleichungssystem* über den ganzen Zahlen lösen, zum Beispiel

$$\begin{cases} 48x_1 + 12x_2 + 18y_3 = 168 \\ 36x_1 + 21x_2 + 9y_3 = 159 \end{cases}$$

oder allgemein

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = y_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = y_2 \\ \vdots \qquad\qquad\qquad\qquad\qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = y_m \end{cases}$$

Hierbei sind die gegebenen Koeffizienten $a_{11},\dots,a_{mn}$ und $y_1,\dots,y_m$ ganze Zahlen und wir suchen Lösungen $x_1,\dots,x_n$ ebenfalls in den ganzen Zahlen. Hierzu werden wir versuchen, das Gleichungssystem auf eine äquivalente aber elementare Form zu bringen, etwa

$$\begin{cases} a'_{11}x'_1 = y'_1 \\ a'_{22}x'_2 = y'_2 \\ \ddots \\ a'_{mn}x'_n = y'_m \end{cases}$$

(Im Allgemeinen gilt hierbei $m \neq n$; zur Vereinfachung der Schreibweise können wir $m = n$ annehmen indem wir geeignet durch Nullen ergänzen.) Wenn dies gelungen ist, dann liegt die gesuchte Lösung auf der Hand: es genügt zu prüfen, ob y'_i ein Vielfaches von a'_{ii} ist, um als Lösung $x'_i = y'_i/a'_{ii}$ zu erhalten. (Im Fall $a'_{ii} = 0$ ist x'_i beliebig.) Die Lösungen unseres ursprünglichen Problems ergeben sich hieraus durch eine Umrechnung.

Wir werden hierzu von *Gleichungssystemen* zu *Matrizen* übergehen. Die obige Gleichung schreibt sich dann kurz $Ax = y$. Dies ist weit mehr als nur eine kompakte Schreibweise: Es ist der Schlüssel zur algebraischen Struktur des Problems!

Ziel dieses Kapitels. Dieses Kapitel erklärt, wie die Umformung zu einer diagonalen Matrix möglich ist. Dieses schöne Ergebnis ist als "Gauß-Algorithmus" aus der linearen Algebra über einem Körper bekannt. Für die oben skizzierte Anwendung über $\mathbb{Z}$ muss jedoch

beachtet werden, dass wir im Ring der ganzen Zahlen nicht beliebig dividieren können. Im Folgenden werden wir den Gauß-Algorithmus soweit verfeinern, dass er auch über jedem Hauptidealring K noch anwendbar ist. Dies schließt den Fall eines Körpers ausdrücklich mit ein.

Im Vorgriff auf die noch zu erläuternden Begriffe formulieren wir das Hauptergebnis:

Definition 7A1. Eine Matrix $D \in K^{m\times n}$ ist in *Elementarteilerform* wenn gilt:

1. Die Matrix D ist diagonal, das heißt $d_{ij} = 0$ für alle $i \neq j$.
2. Auf der Diagonalen gilt $d_{11} \mid d_{22} \mid \cdots \mid d_{\ell\ell}$ wobei $\ell = \min(m,n)$.

Wir sagen hierzu auch, D hat *Elementarteilerform* oder D ist eine *Elementarteilermatrix*. Die Diagonalelemente $d_{11}, d_{22}, \ldots, d_{\ell\ell}$ nennt man dann die *Elementarteiler* von D.

Der folgende Elementarteilersatz besagt, dass man über einem Hauptidealring jede Matrix in Elementarteilerform bringen kann, und diese ist im Wesentlichen eindeutig:

Satz 7A2. *Sei K ein Hauptidealring. Zu jeder Matrix $A \in K^{m\times n}$ existieren invertierbare Matrizen $S \in \mathrm{SL}_m(K)$ und $T \in \mathrm{SL}_n(K)$ so dass $D = SAT$ in Elementarteilerform ist.*

Der Algorithmus von Gauß–Bézout konstruiert solch ein Paar (S,T) und $D = SAT$.

Die Transformationsmatrizen S,T sind durch die gegebene Matrix A nicht eindeutig festgelegt, die Elementarteilerform $D = SAT$ hingegen schon: Ist auch $D' = S'AT'$ in Elementarteilerform mit $S' \in \mathrm{GL}_m(K)$ und $T' \in \mathrm{GL}_n(K)$ dann gilt $d_{ii} \sim d'_{ii}$ für alle i.

§7B. Matrizenringe

§7Ba. Matrizen. Zu natürlichen Zahlen $m,n \in \mathbb{N}$ setzen wir $I = \{1,\ldots,m\}$ und $J = \{1,\ldots,n\}$. Eine *Matrix* der Größe $m \times n$ mit Koeffizienten in K ist eine Familie $A = (a_{ij})$ von Elementen $a_{ij} \in K$ indiziert durch $(i,j) \in I \times J$. Dies ist nichts anderes als eine Abbildung $a\colon I \times J \to K$, geschrieben als $(i,j) \mapsto a_{ij}$. Die Menge dieser Matrizen bezeichnen wir mit

$$K^{m\times n} = \mathrm{Mat}(m \times n; K) = \{\, a\colon I \times J \to K \,\}.$$

Notation. In der Praxis schreibt man eine Matrix $A \in K^{m\times n}$ als rechteckiges Schema

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

mit m Zeilen und n Spalten, geschrieben $A = (a_{ij})_{j=1,\ldots,n}^{i=1,\ldots,m}$ oder kurz $A = (a_{ij})_{ij}$.

In dieser Schreibweise ist $v \in K^{m\times 1}$ ein *Spaltenvektor* mit m Zeilen, und $w \in K^{1\times n}$ ein *Zeilenvektor* mit n Spalten. (Wir identifizieren K^m mit $K^{m\times 1}$.) Zu jeder Matrix $A = (a_{ij})_{ij}$ in $K^{m\times n}$ definieren wir die *transponierte* Matrix $A^t = (a^t_{ji})_{ji}$ mit $a^t_{ji} = a_{ij}$ in $K^{n\times m}$.

Die $n \times n$-*Einheitsmatrix* ist gegeben durch die Koeffizienten $a_{ij} = 0$ für alle $i \neq j$ und $a_{ii} = 1$ für alle i. In der oben vereinbarten Notation schreibt sie sich also

$$1_{n\times n} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

Jede Matrix $A \in K^{m\times n}$ können wir auffassen als Familie

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}$$

von Zeilenvektoren $a_1, \ldots, a_m \in K^{1\times n}$. Ebenso können wir A auffassen als Familie $A = (v_1, \ldots, v_n)$ von Spaltenvektoren $v_1, \ldots, v_n \in K^m$. Die obige Einheitsmatrix $1_{n\times n} = (e_1, \ldots, e_n)$ hat als Spaltenvektoren $e_1, \ldots, e_n \in K^n$ die *Spalten-Einheitsvektoren*. Durch Transposition erhalten wir die *Zeilen-Einheitsvektoren* $e_1^t, \ldots, e_n^t \in K^{1\times n}$.

Bislang sind K und $K^{m\times n}$ nur Mengen ohne spezifische Struktur. Die Theorie wird interessant, wenn K ein Ring ist. In diesem Fall definieren wir die Addition wie folgt:

$$+\colon K^{m\times n} \times K^{m\times n} \to K^{m\times n}, \qquad (A,B) \mapsto C = A + B \qquad \text{mit } c_{ij} = a_{ij} + b_{ij}, \tag{7.1}$$

Proposition 7B1. *Die Addition definiert eine abelsche Gruppe* $(K^{m\times n}, +)$. □

Zudem können Matrizen passender Größe miteinander multipliziert werden:

$$*\colon K^{m\times n} \times K^{n\times r} \to K^{m\times r}, \qquad (A,B) \mapsto C = AB \qquad \text{mit } c_{ik} = \textstyle\sum_{j=1}^{n} a_{ij} b_{jk}. \tag{7.2}$$

Proposition 7B2. *Die Multiplikation* $*$ *ist assoziativ und distributiv über die Addition. Zu jeder Matrix* $A \in K^{m\times n}$ *ist die Einheitsmatrix* $1_{m\times m}$ *links-neutral, also* $1_{m\times m} \cdot A = A$*, und die Einheitsmatrix* $1_{n\times n}$ *rechts-neutral, also* $A \cdot 1_{n\times n} = A$*. Für die Transposition gilt* $(AB)^t = B^t A^t$. □

Bemerkung 7B3. Insbesondere operieren Matrizen $A \in K^{m\times n}$ von links auf Spaltenvektoren $v \in K^n$ vermöge der Multiplikation $*\colon K^{m\times n} \times K^n \to K^m$, $(A,v) \mapsto Av$. Somit können wir unser eingangs formuliertes Gleichungssystem $\sum_{j=1}^{n} a_{ij} x_j = y_i$ schreiben als $Ax = y$. Insbesondere ist für $A \in K^{m\times n}$ und $B = (b_1, \ldots, b_r) \in K^{n\times r}$ das Produkt $AB = (v_1, \ldots, v_r)$ gegeben durch $v_k = Ab_k$ für alle $k = 1, \ldots, r$. Entsprechendes gilt die Multiplikation von rechts.

Zudem haben wir eine Links- und Rechtsmultiplikation mit Skalaren:

$$\cdot\colon K \times K^{m\times n} \to K^{m\times n}, \quad (k,A) \mapsto B = kA \quad \text{mit } b_{ij} = k a_{ij}. \tag{7.3}$$

$$\cdot\colon K^{m\times n} \times K \to K^{m\times n}, \quad (A,k) \mapsto B = Ak \quad \text{mit } b_{ij} = a_{ij} k. \tag{7.4}$$

Links- und Rechtsmultiplikation stimmen genau dann überein, wenn K kommutativ ist.

Proposition 7B4. *Die Linksmultiplikation erfüllt* $a(A+B) = aA + aB$ *und* $(a+b)A = aA + bA$ *sowie* $a(bA) = (ab)A$ *und* $a(AB) = (aA)B$ *und* $1A = A$ *für alle* $a, b \in K$ *und* $A, B \in K^{m\times n}$*. Entsprechendes gilt für die Rechtsmultiplikation.* □

Übung 7B5. Man weise die behaupteten Eigenschaften nach.

§**7Bb. Matrizenringe.** Quadratische Matrizen (mit $m = n$) bilden einen Ring:

Korollar 7B6. *Zu jedem Ring K ist auch $(K^{n\times n}, +, \cdot)$ ein Ring.* □

Die Abbildung $K \to K^{n\times n}$, $a \mapsto a1_{n\times n}$, ist ein Isomorphismus zwischen dem Ring K und dem Unterring $K1_{n\times n} = \{\, a1_{n\times n} \mid a \in K \,\}$. Im Spezialfall $n = 1$ finden wir so den offensichtlichen Isomorphismus $K \cong K^{1\times 1}$. Für $n \geq 2$ ist $K^{n\times n}$ nicht kommutativ, selbst wenn K kommutativ ist. Außerdem hat $K^{n\times n}$ Nullteiler, selbst wenn K nullteilerfrei ist: Für $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ und $B = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ gilt $A \neq 0$ und $B \neq 0$ aber $AB = 0$.

Bemerkung 7B7. Die Transposition ${}^t\colon K^{n\times n} \to K^{n\times n}$ ist additiv, also $(A+B)^t = A^t + B^t$, und anti-multiplikativ, das heißt $(AB)^t = B^t A^t$. Mit anderen Worten, die Transposition ist ein Isomorphismus zwischen dem Matrizenring $(K^{n\times n}, +, *)$ und dem entgegengesetzten Ring $(K^{n\times n}, +, \bar{*})$ mit $A \bar{*} B = B * A$.

Bemerkung 7B8. Für $m < n$ können wir den Matrizenring $K^{m\times m}$ auf verschiedene Weise in den Ring $K^{n\times n}$ einbetten, zum Beispiel vermöge der Abbildung

$$\phi_k\colon K^{m\times m} \to K^{n\times n} \qquad \text{mit} \qquad A \mapsto \begin{pmatrix} 0_{k\times k} & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & 0_{\ell\times\ell} \end{pmatrix}.$$

Hierbei ist $k, \ell \geq 0$ und $k + \ell + m = n$.

Übung 7B9. Die Abbildung $\phi_k\colon K^{m\times m} \to K^{n\times n}$ ist ein Ringhomomorphismus.

Übung 7B10. Für das Zentrum des Matrizenrings zeige man $Z(K^{n\times n}) = Z(K)1_{n\times n}$.

Übung 7B11. Jeder Ringhomomorphismus $h\colon R \to S$ induziert einen Ringhomomorphismus $H\colon R^{n\times n} \to S^{n\times n}$ durch Anwendung auf alle Einträge einer Matrix:

$$H((a_{ij})_{ij}) = (h(a_{ij}))_{ij}.$$

Ist $I = \ker(h)$ der Kern von h, so gilt $\ker(H) = I^{n\times n}$.

Ist $I \lhd R$ ein Ideal, dann ist $I^{n\times n} \lhd R^{n\times n}$ ein Ideal, und $R^{n\times n}/I^{n\times n} \cong (R/I)^{n\times n}$.

Jedes Ideal $J \lhd R^{n\times n}$ ist von der Form $J = I^{n\times n}$ für ein Ideal $I \lhd R$.

Demnach ist jedes homomorphe Bild eines Matrizenrings wieder ein Matrizenring.

Übung 7B12. Man konstruiere einen Ringisomorphismus $K^{mn\times mn} \cong (K^{m\times m})^{n\times n}$.

§**7Bc. Die allgemeine lineare Gruppe.** Da $K^{n\times n}$ ein Ring ist, können wir das übliche Vokabular anwenden. Für invertierbare Elemente vereinbaren wir folgende Sprechweise:

Definition 7B13. Eine Matrix $A \in K^{n\times n}$ heißt *invertierbar* in $K^{n\times n}$ wenn es eine Matrix $B \in K^{n\times n}$ gibt, sodass $AB = BA = 1$. In diesem Fall ist B eindeutig durch A bestimmt und wird die zu A *inverse Matrix* genannt, geschrieben $B = A^{-1}$. Die invertierbaren Matrizen in $K^{n\times n}$ bilden eine Gruppe, genannt *allgemeine lineare Gruppe* der $n \times n$-Matrizen über K, geschrieben $\mathrm{GL}(n;K)$ oder $\mathrm{GL}_n(K)$, englisch *general linear group*.

Bemerkung 7B14. Für $m < n$ können wir die Gruppe $\mathrm{GL}_m(K)$ auf verschiedene Weise in die Gruppe $\mathrm{GL}_n(K)$ einbetten, zum Beispiel vermöge der Abbildung

$$\psi_k\colon \mathrm{GL}_m(K) \to \mathrm{GL}_n(K) \qquad \text{mit} \qquad A \mapsto \begin{pmatrix} 1_{k\times k} & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & 1_{\ell\times\ell} \end{pmatrix}.$$

Hierbei ist $k, \ell \geq 0$ und $k + \ell + m = n$.

Übung 7B15. Die Abbildung $\psi_k\colon \mathrm{GL}_m(K) \to \mathrm{GL}_n(K)$ ist ein Gruppenhomomorphismus.

Insbesondere können wir die Gruppe $\mathrm{GL}_1(K) = K^\times$ in die Gruppe $\mathrm{GL}_n(K)$ einbetten durch $\psi_k\colon K^\times \to \mathrm{GL}_n(K)$ für jedes beliebige $k \in \{0, \dots, n-1\}$.

§7C. Die Determinante

Alles bisher Gesagte gilt über jedem Ring K, kommutativ oder nicht. Für kommutative Ringe steht uns zudem die Determinante als mächtiges Werkzeug zur Verfügung.

Definition 7C1. Jede Matrix $A \in K^{m\times n}$ können wir auffassen als Familie $A = (v_1, \dots, v_n)$ von Spaltenvektoren $v_1, \dots, v_n \in K^m$. Eine Abbildung $f\colon K^{m\times n} \to K$ heißt *multilinear* wenn

$$f(\dots, v_{i-1}, av_i, v_{i+1}, \dots) = af(\dots, v_{i-1}, v_i, v_{i+1}, \dots) \qquad \text{sowie}$$
$$f(\dots, v_{i-1}, v_i + v_i', v_{i+1}, \dots) = f(\dots, v_{i-1}, v_i, v_{i+1}, \dots) + f(\dots, v_{i-1}, v_i', v_{i+1}, \dots)$$

für alle $a \in K$ und $v_1, \dots, v_{i-1}, v_i, v_i', v_{i+1}, \dots, v_n \in K^m$ gilt. Die Abbildung f heiß *alternierend*, wenn $f(v_1, \dots, v_n) = 0$ gilt sobald $v_i = v_j$ für $i \neq j$. Im Falle $m = n$ schließlich nennen wir f *normiert*, falls sie der Einheitsmatrix den Wert $f(1_{n\times n}) = 1$ zuordnet.

Bemerkung 7C2. Aus der Additivität folgt $f(v_1, \dots, v_n) = 0$ falls $v_i = 0$, denn

$$f(\dots, v_{i-1}, 0, v_{i+1}, \dots) = f(\dots, v_{i-1}, 0, v_{i+1}, \dots) + f(\dots, v_{i-1}, 0, v_{i+1}, \dots).$$

Ist f zudem alternierend, so folgt $f(\dots, v_i, \dots, v_j, \dots) = -f(\dots, v_j, \dots, v_i, \dots)$, denn

$$\begin{aligned} 0 &= f(\dots, v_i + v_j, \dots, v_i + v_j, \dots) \\ &= f(\dots, v_i, \dots, v_i, \dots) + f(\dots, v_i, \dots, v_j, \dots) \\ &\quad + f(\dots, v_j, \dots, v_i, \dots) + f(\dots, v_j, \dots, v_j, \dots) \\ &= f(\dots, v_i, \dots, v_j, \dots) + f(\dots, v_j, \dots, v_i, \dots) \end{aligned}$$

Ist f zudem normiert, so gilt $f(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = \mathrm{sign}(\sigma)$. Hierbei sind $e_1, \dots, e_n \in K^n$ die Einheitsvektoren, $\sigma \in S_n$ ist eine Permutation, und $\mathrm{sign}\colon S_n \to \{\pm 1\}$ ist die Signatur.

Bemerkung 7C3. Eine multilineare normierte Abbildung $f\colon K^{n\times n} \to K$ kann es für $n \geq 2$ nur über einem kommutativen Ring geben. Für alle $a, b \in K$ gilt nämlich

$$f\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) = af\left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right) = abf\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = ab \qquad \text{und}$$
$$f\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) = bf\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) = baf\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = ba.$$

Der folgende Satz besagt, dass die Kommutativität von K ausreicht, um die Existenz einer multilinearen, alternierenden, normierten Abbildung $K^{n\times n} \to K$ sicherzustellen.

Satz 7C4. *Sei K ein kommutativer Ring. Für jedes $n \in \mathbb{N}$ existiert genau eine multilineare, alternierende, normierte Abbildung* $\det\colon K^{n\times n} \to K$*, genannt* Determinante.

Diese erfreut sich folgender Eigenschaften:

1. *Es gilt die polynomielle Formel* $\det A = \sum_{\sigma\in S_n} \operatorname{sign}(\sigma)\cdot a_{\sigma(1),1}\cdot a_{\sigma(2),2}\cdots a_{\sigma(n),n}$.
2. *Die Determinante ist invariant unter Transposition, das heißt* $\det(A^t) = \det(A)$. *Daher ist sie auch alternierend und multilinear bezüglich der Zeilen.*
3. *Die Determinante ist multiplikativ, das heißt* $\det(AB) = \det(A)\det(B)$.
4. *Eine Matrix $A \in K^{n\times n}$ ist genau dann in $K^{n\times n}$ invertierbar, wenn ihre Determinante* $\det(A) \in K$ *im Ring K invertierbar ist. Für die Inversion $A \mapsto A^{-1}$ gibt es eine polynomielle Abbildung $K^{n\times n} \to K^{n\times n}$, $A \mapsto \tilde{A}$, sodass $A\tilde{A} = \tilde{A}A = \det(A)1_{n\times n}$ gilt.*

BEWEIS. *Eindeutigkeit:* Ist eine Abbildung $\det\colon K^{n\times n} \to K$ multilinear, alternierend und normiert, dann folgt gemäß Bemerkung 7C2 die Formel (1) wie folgt: Wir schreiben $A \in K^{n\times n}$ als Familie $A = (v_1,\dots,v_n)$ von Spaltenvektoren. Jeder Spaltenvektor schreibt sich als Linearkombination $v_k = \sum_i a_{ik}e_i$ von Einheitsvektoren. Daraus folgt:

$$\begin{aligned}\det(A) &= \det\Big(\sum_{i_1=1}^{n} a_{i_1,1}e_{i_1},\cdots\sum_{i_n=1}^{n} a_{i_n,1}e_{i_n}\Big)\\ &= \sum_{i_1=1}^{n}\cdots\sum_{i_n=1}^{n} a_{i_1,1}\cdots a_{i_n,1}\det(e_{i_1},\dots,e_{i_n})\\ &= \sum_{\sigma\in S_n}\operatorname{sign}(\sigma)\cdot a_{\sigma(1),1}\cdot a_{\sigma(2),2}\cdots a_{\sigma(n),2}.\end{aligned}$$

Existenz: Die angegeben Formel (1) definiert eine Abbildung $\det\colon K^{n\times n} \to K$. Diese ist offenbar normiert, denn für $\det(1_{n\times n})$ trägt in der Summe $\sigma = \mathrm{id}$ den Summanden 1 bei, aber für alle $\sigma \neq \mathrm{id}$ ist das Produkt Null: aus $\sigma(i) \neq 0$ folgt $a_{\sigma(i),i} = 0$. Die Formel (1) ist offenbar additiv in jedem Spaltenvektor, und K-linear wenn der Ring K kommutativ ist. Ist der Ring K kommutativ, dann ist die Formel (1) auch alternierend.

Transposition: Für alle $\sigma \in S_n$ gilt durch Umordnung

$$a_{\sigma(1),1}\cdot a_{\sigma(2),2}\cdots a_{\sigma(n),n} = a_{1,\sigma^{-1}(1)}\cdot a_{2,\sigma^{-1}(2)}\cdots a_{n,\sigma^{-1}(n)}.$$

Zudem gilt $\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma^{-1})$. Durchläuft σ alle Elemente von S_n, dann durchläuft auch σ^{-1} alle Elemente von S_n. Wir erhalten also

$$\begin{aligned}\det(A^t) &= \sum_{\sigma\in S_n}\operatorname{sign}(\sigma)\cdot a^t_{\sigma(1),1}\cdot a^t_{\sigma(2),2}\cdots a^t_{\sigma(n),n}\\ &= \sum_{\sigma\in S_n}\operatorname{sign}(\sigma)\cdot a_{1,\sigma(1)}\cdot a_{2,\sigma(2)}\cdots a_{n,\sigma(n)}\\ &= \sum_{\sigma^{-1}\in S_n}\operatorname{sign}(\sigma^{-1})\cdot a_{1,\sigma^{-1}(1)}\cdot a_{2,\sigma^{-1}(2)}\cdots a_{n,\sigma^{-1}(n)}\\ &= \sum_{\sigma\in S_n}\operatorname{sign}(\sigma)\cdot a_{\sigma(1),1}\cdot a_{\sigma(2),2}\cdots a_{\sigma(n),n} = \det(A).\end{aligned}$$

Multiplikativität: Wir vergleichen die durch $f\colon B \mapsto \det(A)\det(B)$ und $g\colon B \mapsto \det(AB)$ definierten Abbildungen $f,g\colon K^{n\times n} \to K$. Beide sind multilinear und alternierend (7B3)

mit der Normierung $f(1_{n\times n}) = g(1_{n\times n}) = \det(A)$. Der obige Eindeutigkeitsbeweis zeigt nun $f = g$. Das bedeutet $\det(AB) = \det(A)\det(B)$ für alle $A, B \in K^{n\times n}$.

Inversion: Wenn A invertierbar ist, also $AB = 1_{n\times n}$ für eine geeignete Matrix $B \in K^{n\times n}$ gilt, dann folgt aus der Multiplikativität $\det(A)\det(B) = 1$, also $\det(A) \in K^\times$. Das gilt für jeden Monoidhomomorphismus. Die Umkehrung ist interessanter:

Zu der Matrix $A \in K^{n\times n}$ als Familie von Spaltenvektoren $A = (a_1, \dots, a_n)$ definieren wir die *Komplementärmatrix* $\tilde{A} \in K^{n\times n}$ durch $\tilde{a}_{ij} := \det(a_1, \dots, a_{i-1}, e_j, a_{i+1}, \dots, a_n)$. Dann berechnet sich das Produkt $D = \tilde{A}A$ gemäß

$$\begin{aligned} d_{ij} &= \sum_{k=1}^{n} \tilde{a}_{ik} a_{kj} = \sum_{k=1}^{n} a_{kj} \det(a_1, \dots, a_{i-1}, e_k, a_{i+1}, \dots, a_n) \\ &= \det(a_1, \dots, a_{i-1}, \sum_{k=1}^{n} a_{kj} e_k, a_{i+1}, \dots, a_n) \\ &= \det(a_1, \dots, a_{i-1}, a_j, a_{i+1}, \dots, a_n) = \begin{cases} \det(A) & \text{falls } j = i, \\ 0 & \text{falls } j \neq i. \end{cases} \end{aligned}$$

Also gilt $\tilde{A}A = \det(A)1_{n\times n}$. Ebenso findet man $A\tilde{A} = \det(A)1_{1\times n}$. Hierzu prüft man zunächst, dass man dieselbe Komplementärmatrix $\tilde{A}$ erhält, wenn man Zeilen statt Spalten betrachtet: Für $B = A^t$ gilt $\tilde{B} = \tilde{A}^t$. Daraus folgt $A\tilde{A} = B^t\tilde{B}^t = (\tilde{B}B)^t = (\det(B)1_{n\times n})^t = \det(A)1_{n\times n}$.

Wenn also die Determinante $\det(A)$ in K invertierbar ist, dann ist die Matrix A in $K^{n\times n}$ invertierbar mit inverser Matrix $\det(A)^{-1}\tilde{A} \in K^{n\times n}$. Hierbei ist bemerkenswert, dass sowohl $A \mapsto \det(A)$ als auch $A \mapsto \tilde{A}$ polynomiell in den Koeffizienten von A sind. □

Beispiel 7C5. Für jede 2×2-Matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ gilt $\det(A) = ad - bc$. Im Falle $\det(A) \in K^\times$ gilt zudem $A^{-1} = \frac{1}{ad-bc}\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$. Man stelle die entsprechenden Formeln für $A \in K^{3\times 3}$ auf.

Warnung. — Die Determinante $\det\colon K^{n\times n} \to K$ ist für $n \geq 2$ kein Ringhomomorphismus! Sie ist zwar multiplikativ aber nicht additiv: Zum Beispiel gilt $\det\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = 0$ und $\det\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = 0$ aber $\det\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = 1$.

§7Ca. Die spezielle lineare Gruppe.

Korollar 7C6. *Die Determinante* $\det\colon K^{n\times n} \to K$ *induziert einen Gruppenhomomorphismus* $\det\colon \mathrm{GL}_n(K) \to K^\times$. *Dieser ist surjektiv. Sein Kern ist die* spezielle lineare Gruppe

$$\mathrm{SL}_n(K) := \ker(\det) = \{\, A \in K^{n\times n} \mid \det(A) = 1 \,\}.$$

BEWEIS. Die Surjektivität ergibt sich aus $\det \psi_0(a) = a$ für alle $a \in K$. □

Bemerkung 7C7. Der Gruppenhomomorphismus $\psi_k\colon \mathrm{GL}_m(K) \to \mathrm{GL}_n(K)$ induziert einen Gruppenhomomorphismus $\psi_k\colon \mathrm{SL}_m(K) \to \mathrm{SL}_n(K)$.

§7D. Der Algorithmus von Gauß–Bézout

Wir arbeiten im Folgenden über einen Hauptidealring K. Zu je zwei Elementen $x, y \in K$ existiert dann ein ggT $d \in K$ und es gilt $(x) + (y) = (d)$. Hieraus folgt insbesondere die Existenz von Bézout–Koeffizienten $u, v \in K$ mit $ux + vy = d$.

Bemerkung 7D1 (Bézout–Ringe)**.** Zwecks Normierung werden wir im Folgenden eine Funktion $\mathrm{ggT}\colon K\times K\to K$ voraussetzen, die wie üblich normiert ist (siehe §6Cb und §6Fb).

Zudem benötigen wir eine Abbildung $\beta\colon K\times K\to K\times K$, sodass $(x,y)\mapsto(u,v)$ die Bézout–Relation $ux+vy=\mathrm{ggT}(x,y)$ erfüllt. Über einem euklidischen Ring, wie zum Beispiel $\mathbb{Z}$ oder $\mathbb{K}[X]$ über einem Körper $\mathbb{K}$, liefert der erweiterte euklidische Algorithmus alles Gewünschte. Auch über jedem Hauptidealring ist dies stets möglich.

Allgemein nennen wir (R,ggT,β) einen *Bézout–Ring*. In einem Bézout–Ring gilt demnach $(x,y)=(\mathrm{ggT}(x,y))$, und per Induktion ist jedes endlich-erzeugte Ideal ein Hauptideal.

§**7Da. Zeilen- und Spaltenoperationen.** Wir bemühen uns zunächst um die Existenzaussage des Elementarteilersatzes, die wir durch den Algorithmus von Gauß–Bézout beweisen. Dieser beruht auf folgenden elementaren Zeilen- und Spaltenoperationen:

Lemma 7D2 (Zeilenoperationen)**.** *Wir wollen folgende Transformation ausführen:*

$$A=\begin{pmatrix}x&*\\y&*\end{pmatrix}\mapsto SA=\begin{pmatrix}d&*\\0&*\end{pmatrix}.$$

Wenn $x=y=0$, dann wählen wir für S die Einheitsmatrix. Andernfalls sei $d=\mathrm{ggT}(x,y)=ux+vy$ mit $u,v\in K$. Dann erfüllt die Transformationsmatrix

$$S:=\begin{pmatrix}u&v\\-y/d&x/d\end{pmatrix}$$

die gewünschte Bedingung. Zudem gilt $\det(S)=1$ *und* $S^{-1}=\left(\begin{smallmatrix}x/d&-v\\y/d&u\end{smallmatrix}\right)$.

Lemma 7D3 (Spaltenoperationen)**.** *Wir wollen folgende Transformation ausführen:*

$$A=\begin{pmatrix}x&y\\*&*\end{pmatrix}\mapsto AT=\begin{pmatrix}d&0\\*&*\end{pmatrix}.$$

Wenn $x=y=0$, dann wählen wir für T die Einheitsmatrix. Andernfalls sei $d=\mathrm{ggT}(x,y)=ux+vy$ mit $u,v\in K$. Dann erfüllt die Transformationsmatrix

$$T:=\begin{pmatrix}u&-y/d\\v&x/d\end{pmatrix}$$

die gewünschte Bedingung. Zudem gilt $\det(T)=1$ *und* $T^{-1}=\left(\begin{smallmatrix}x/d&y/d\\-v&u\end{smallmatrix}\right)$.

Lemma 7D4 (Diagonaloperationen)**.** *Wir wollen folgende Transformation ausführen:*

$$A=\begin{pmatrix}x&0\\0&y\end{pmatrix}\mapsto SAT=\begin{pmatrix}d&0\\0&e\end{pmatrix},$$

sodass $d\mid e$ gilt. Wenn $x=y=0$, dann wählen wir für S und T die Einheitsmatrizen. Andernfalls sei $d=\mathrm{ggT}(x,y)=ux+vy$ mit $u,v\in K$. Dann ist $e=xy/d\in KGV(x,y)$ und

$$S:=\begin{pmatrix}u&v\\-y/d&x/d\end{pmatrix}\qquad\text{und}\qquad T:=\begin{pmatrix}1&-vy/d\\1&ux/d\end{pmatrix}$$

erfüllen die gewünschte Bedingung. Beide Transformationsmatrizen haben Determinante 1.

Zeilen-, Spalten- und Diagonaloperationen können wir in der Form $A \mapsto SAT$ zusammenfassen. Für Zeilenoperationen ist dabei $T = 1_{2\times 2}$, für Spaltenoperationen entsprechend $S = 1_{2\times 2}$. Eine Folge solcher Operationen, $A_1 = S_0A_0T_0$, $A_2 = S_1A_1T_1$, …, $A_{k+1} = S_kA_kT_k$ können wir zusammenfassen durch $A_{k+1} = SA_0T$ mit $S = S_k \cdots S_1S_0$ und $T = T_0T_1 \cdots T_k$. Aus $S_0, S_1, \ldots, S_k \in SL_2(K)$ folgt $S \in \mathrm{SL}_2(K)$, und aus $T_0, T_1, \ldots, T_k \in SL_2(K)$ folgt $T \in \mathrm{SL}_2(K)$.

Beispiel 7D5. Wir versuchen die folgende Matrix in Elementarteilerform zu bringen:

$$A_0 = \begin{pmatrix} 48 & 15 \\ 36 & 9 \end{pmatrix}.$$

Für die Koeffizienten $x = 48$ und $y = 36$ finden wir $d = \mathrm{ggT}(x,y) = 12$ mit Bézout–Koeffizienten $u = 1$ und $v = -1$ sodass $d = ux + vy$. Dies definiert eine erste Transformationsmatrix

$$S_0 := \begin{pmatrix} 1 & -1 \\ -3 & 4 \end{pmatrix} \quad \text{und somit} \quad A_1 := S_0A_0 = \begin{pmatrix} 12 & 6 \\ 0 & -9 \end{pmatrix}.$$

Dies ist eine Zeilenoperation; Spaltenoperationen waren in diesem ersten Schritt nicht nötig. Der Form halber setzen wir $T_0 := 1_{3\times 3}$

Genauso löschen wir nun die erste Zeile. Für $x = 12$ und $y = 6$ in der ersten Zeile finden wir $d = 6$ sowie $u = 0$ und $v = 1$. Da wir nun auf Spalten operieren entspricht dies der Multiplikation von rechts durch die Matrix

$$T_1 := \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} \quad \text{ergibt} \quad A_2 := A_1T_1 = \begin{pmatrix} 6 & 0 \\ -9 & -18 \end{pmatrix}.$$

Dies ist eine Spaltenoperation; Zeilenoperationen waren in diesem Schritt nicht nötig. Der Form halber setzen wir $S_1 := 1_{2\times 2}$ (und entsprechend in allen weiteren Schritten).

Wir haben damit die erste Zeile gelöscht, aber leider die erste Spalte wieder verdorben. Bleiben wir optimistisch und versuchen es solange weiter, bis wir *beide* gelöscht haben. Für $x = 6$ und $y = -9$ finden wir $d = 3$ sowie $u = -1$ und $v = -1$, also

$$S_2 := \begin{pmatrix} -1 & -1 \\ 3 & 2 \end{pmatrix} \quad \text{ergibt} \quad A_3 := S_2A_2 = \begin{pmatrix} 3 & 18 \\ 0 & -36 \end{pmatrix}.$$

Wir haben damit die erste Spalte gelöscht, aber leider die erste Zeile wieder verdorben. Also nochmal: Für $x = 3$ und $y = 18$ finden wir $d = 3$ sowie $u = 1$ und $v = 0$, also

$$T_3 := \begin{pmatrix} 1 & -6 \\ 0 & 1 \end{pmatrix} \quad \text{ergibt} \quad A_4 := A_3T_3 = \begin{pmatrix} 3 & 0 \\ 0 & -36 \end{pmatrix}.$$

Wir haben also schließlich sowohl die erste Spalte als auch die erste Zeile gelöscht. Es gilt bereits $3 \mid -36$. Die zur Umformung $A_{k+1} = S_kA_kT_k$ verwendeten Transformationsmatrizen können wie schließlich zusammenfassen:

$$S := S_3S_2S_1S_0 = \begin{pmatrix} 2 & -3 \\ -3 & 5 \end{pmatrix} \quad \text{und} \quad T := T_0T_1T_2T_3 = \begin{pmatrix} 0 & -1 \\ 1 & -4 \end{pmatrix}$$

bringen die Matrix A in die gewünschte Form

$$SAT = \begin{pmatrix} 3 & 0 \\ 0 & -36 \end{pmatrix}.$$

Ihre Inversen sind

$$S^{-1} = S_0^{-1}S_1^{-1}S_2^{-1}S_3^{-1} = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix} \quad \text{und} \quad T^{-1} = T_3^{-1}T_2^{-1}T_1^{-1}T_0^{-1} = \begin{pmatrix} -4 & 1 \\ -1 & 0 \end{pmatrix}.$$

Der folgende Algorithmus 8 formuliert das Vorgehen im allgemeinen Fall.

Algorithmus 8 Algorithmus von Gauß–Bézout für 2×2-Matrizen

Eingabe: eine Matrix $A \in K^{2\times 2}$
Ausgabe: drei Matrizen $D \in K^{2\times 2}$, $S \in \mathrm{SL}_2(K)$, $T \in \mathrm{SL}_2(K)$, sodass $D = SAT$ Elementarteilerform hat

Initialisiere $D \leftarrow A$, $S \leftarrow 1_{2\times 2}$, $T \leftarrow 1_{2\times 2}$	// Invariante $D = SAT$.
while D hat noch nicht die Form $\left(\begin{smallmatrix} a_{11} & 0 \\ 0 & a_{22} \end{smallmatrix}\right)$ **do**	
Lösche a_{21} mittels Operation auf Zeilen $1,2$.	// Invariante $D = SAT$.
Lösche a_{12} mittels Operation auf Spalten $1,2$.	// Invariante $D = SAT$.
end while	
Sorge für $a_{11} \mid a_{22}$ mittels Diagonaloperation.	// Invariante $D = SAT$.
return (D,S,T)	// $D = SAT$ hat Elementarteilerform.

Satz 7D6. *Algorithmus 8 ist korrekt.*

BEWEIS. Es bleibt nur die Frage zu klären, warum die Schleife endet. In jeder Iteration wird a_{11} ersetzt durch einen Teiler, zuerst $\mathrm{ggT}(a_{11},a_{21})$ dann $\mathrm{ggT}(a_{11},a_{12})$. Das Ideal (a_{11}) wird dabei entweder echt größer oder bleibt stationär. Wegen der Kettenbedingung (§5Ee) kann es nur endlich oft größer werden. Sobald es aber stationär wird, ist a_{11} ein gemeinsamer Teiler der ersten Spalte *und* der ersten Zeile, und damit erreichen wir die Löschung der Spalte unterhalb a_{11} und der Zeile rechts von a_{11}. Anders gesagt, zerlegt sich a_{11} in ℓ Primfaktoren in R, dann endet die Schleife nach höchstens ℓ Iterationen. □

§**7Db. Der Algorithmus von Gauß–Bézout.** Zeilenoperation können wir auch auf Matrizen mit mehr als zwei Zeilen anwenden. Die Anwendung von S auf A zur Konstruktion von $A' = SA$ ist denkbar einfach: Wenn S auf die Zeilen a_i und a_j wirken soll, dann gilt $a_i' \leftarrow ua_i + va_j$ und $a_j' \leftarrow -\frac{y}{d}a_i + \frac{x}{d}a_j$. Für die Zeilen i und $i+1$ entspricht dies gerade der Operation von $\psi_{i-1}(S)$; hierbei ist $\psi_k\colon \mathrm{SL}_2(K) \to \mathrm{SL}_n(K)$ die Einbettung aus 7B14. Ebenso können wir Spaltenoperation auf Matrizen mit mehr als zwei Spalten anwenden.

Zeilen-, Spalten- und Diagonaloperationen auf $A \in K^{m\times n}$ können wir wie zuvor zusammenfassen durch $A \mapsto SAT$. Für Zeilenoperationen ist dabei $T = 1_{n\times n}$, für Spaltenoperationen entsprechend $S = 1_{m\times m}$. Eine Folge solcher Operationen, $A_1 = S_0A_0T_0$, $A_2 = S_1A_1T_1$, …, $A_{k+1} = S_kA_kT_k$ können wir zusammenfassen durch $A_{k+1} = SA_0T$ mit $S = S_k\cdots S_1S_0$ und $T = T_0T_1\cdots T_k$. Aus $S_0,S_1,\ldots,S_k \in SL_m(K)$ folgt $S \in \mathrm{SL}_m(K)$, und aus $T_0,T_1,\ldots,T_k \in SL_n(K)$ folgt $T \in \mathrm{SL}_n(K)$. Da zudem die einzelnen Matrizen leicht zu invertieren sind, gewinnen wir daraus leicht $S^{-1} = S_0^{-1}S_1^{-1}\cdots S_k^{-1}$ und $T = T_k^{-1}\cdots T_1^{-1}T_0^{-1}$.

Der Algorithmus 9 von Gauß–Bézout verfährt im allgemeinen Fall der $m \times n$-Matrizen im Wesentlichen genau so wie im Spezialfall der 2×2-Matrizen. Eine mögliche Organisation der Indizes ist in Algorithmus 9 erklärt.

Satz 7D7. *Algorithmus 9 ist korrekt.*

Algorithmus 9 Algorithmus von Gauß–Bézout

Eingabe: eine Matrix $A \in K^{m\times n}$
Ausgabe: fünf Matrizen D,S,S^{-1},T,T^{-1} wobei $D \in K^{m\times n}$, $S,S^{-1} \in \mathrm{SL}_m(K)$, $T,T^{-1} \in \mathrm{SL}_n(K)$, sodass $D = SAT$ Elementarteilerform hat

Initialisiere $D \leftarrow A$, $\ell \leftarrow \min(m,n)$ // ℓ ist die Länge der Diagonale.
Initialisiere $S,S^{-1} \leftarrow 1_{m\times m}$, $T,T^{-1} \leftarrow 1_{n\times n}$ // $D = SAT$, $SS^{-1} = 1$, $TT^{-1} = 1$.
for k **from** 1 **to** ℓ **do**
  repeat
    for i **from** m **to** $k+1$ **do**
      Lösche a_{ik} mittels Operation auf Zeilen $i-1, i$. // $D = SAT$, $SS^{-1} = 1$, $TT^{-1} = 1$.
    end for
    for j **from** n **to** $k+1$ **do**
      Lösche a_{kj} mittels Operation auf Spalten $j-1, j$. // $D = SAT$, $SS^{-1} = 1$, $TT^{-1} = 1$.
    end for
  until D hat die Form $\begin{pmatrix} \ddots & & & \\ & a_{kk} & 0 & \dots & 0 \\ & 0 & * & * & * \\ & \vdots & * & * & * \\ & 0 & * & * & * \end{pmatrix}$
end for
for k **from** 1 **to** $\ell - 1$ **do**
  for j **from** ℓ **to** $k+1$ **do**
    Sorge für $a_{j-1,j-1} \mid a_{jj}$ mittels Diagonaloperation // $D = SAT$, $SS^{-1} = 1$, $TT^{-1} = 1$.
  end for
end for
return (D,S,S^{-1},T,T^{-1}) // $D = SAT$ hat Elementarteilerform.

BEWEIS. Es bleibt nur die Frage zu klären, warum die Schleife "repeat… until…" endet. In jeder Iteration wird a_{kk} ersetzt durch einen Teiler, zuerst $\mathrm{ggT}(a_{kk}, a_{k+1,k})$ dann $\mathrm{ggT}(a_{kk}, a_{k,k+1})$. Das Ideal (a_{kk}) wird dabei entweder echt größer oder bleibt stationär. Wegen der Kettenbedingung (§5Ee) kann es nur endlich oft größer werden. Sobald es aber stationär wird, ist a_{kk} ein gemeinsamer Teiler der $k$ten Spalte *und* der $k$ten Zeile, und damit erreichen wir die Löschung der Spalte unterhalb a_{kk} und der Zeile rechts von a_{kk}. □

Wir illustrieren den Algorithmus von Gauß–Bézout mit einem detaillierten Beispiel:

Beispiel 7D8. Wir bringen die folgende Matrix in Elementarteilerform:

$$A_0 = \begin{pmatrix} 48 & 12 & 18 \\ 36 & 21 & 9 \end{pmatrix}.$$

Für die Koeffizienten $x = 48$ und $y = 36$ finden wir $d = \mathrm{ggT}(x,y) = 12$ mit Bézout–Koeffizienten $u = 1$ und $v = -1$ sodass $d = ux + vy$. Dies definiert eine erste Transformationsmatrix

$$S_0 := \begin{pmatrix} 1 & -1 \\ -3 & 4 \end{pmatrix} \quad \text{und somit} \quad A_1 := S_0 A_0 = \begin{pmatrix} 12 & -9 & 9 \\ 0 & 48 & -18 \end{pmatrix}.$$

Genauso löschen wir nun die erste Zeile. Für $x = -9$ und $y = 9$ finden wir $d = 9$ sowie $u = -1$ und $v = 0$. Da wir nun auf Spalten operieren entspricht dies der Multiplikation von

rechts durch die Matrix

$$T_1 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -1 \\ 0 & 0 & -1 \end{pmatrix} \quad \text{ergibt} \quad A_2 := A_1 T_1 = \begin{pmatrix} 12 & 9 & 0 \\ 0 & -48 & -30 \end{pmatrix}.$$

Für $x = 12$ und $y = 9$ finden wir $d = 3$ sowie $u = 1$ und $v = -1$:

$$T_2 := \begin{pmatrix} 1 & -3 & 0 \\ -1 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{ergibt} \quad A_3 := A_2 T_2 = \begin{pmatrix} 3 & 0 & 0 \\ 48 & -192 & -30 \end{pmatrix}.$$

Wir haben damit die erste Zeile gelöscht, aber leider die erste Spalte wieder verdorben. Für $x = 3$ und $y = 48$ finden wir $d = 3$ sowie $u = 1$ und $v = 0$:

$$S_3 := \begin{pmatrix} 1 & 0 \\ -16 & 1 \end{pmatrix} \quad \text{ergibt} \quad A_4 := S_3 A_3 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & -192 & -30 \end{pmatrix}.$$

Wir haben schließlich sowohl die erste Spalte als auch die erste Zeile gelöscht. Nun widmen wir uns der verbleibenden Untermatrix. Für $x = -192$ und $y = -30$ finden wir $d = 6$ und $u = 2$ und $v = -13$, also

$$T_4 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 5 \\ 0 & -13 & -32 \end{pmatrix} \quad \text{ergibt} \quad A_5 := A_4 T_4 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}.$$

Damit endet der Algorithmus. Die zur Umformung $A_{k+1} = S_k A_k T_k$ verwendeten Transformationsmatrizen können wie schließlich zusammenfassen:

$$S := S_3 S_0 = \begin{pmatrix} 1 & -1 \\ -19 & 20 \end{pmatrix} \quad \text{und} \quad T := T_1 T_2 T_4 = \begin{pmatrix} 1 & -6 & -15 \\ 1 & 5 & 12 \\ 0 & 13 & 32 \end{pmatrix}$$

bringen die Matrix A_0 in die gewünschte Elementarteilerform SA_0T. Parallel berechnet man

$$S^{-1} = S_0^{-1} S_3^{-1} = \begin{pmatrix} 20 & 1 \\ 19 & 1 \end{pmatrix} \quad \text{und} \quad T^{-1} = T_4^{-1} T_2^{-1} T_1^{-1} = \begin{pmatrix} 4 & -3 & 3 \\ -32 & 32 & -27 \\ 13 & -13 & 11 \end{pmatrix}.$$

Bemerkung 7D9. Gilt es eine Gleichung der Form $Ax = y$ zu lösen, so bringen wir diese auf Elementarteilerform $A' = SAT$. Die ursprüngliche Gleichung $Ax = y$ ist dann äquivalent zu der elementaren Gleichung $A'x' = y'$ mit $y' = Sy$ und $x = Tx'$.

Beispiel 7D10. Wir suchen die Lösungen $x = (x_1, x_2, x_3) \in \mathbb{Z}^3$ des Gleichungssystems

$$\begin{cases} 48x_1 + 12x_2 + 18x_3 = 168 \\ 36x_1 + 21x_2 + 9x_3 = 159 \end{cases}$$

Nach obigen Rechnungen ist dies äquivalent zu $A'x' = y'$ mit $y' = Sy$ und $x = Tx'$:

$$\begin{cases} 3x_1' = 9 \\ 6x_2' = -12 \end{cases}$$

Hieraus lesen wir $x_1' = 3$ und $x_2' = -2$ ab. Der Parameter $x_3' \in \mathbb{Z}$ ist frei wählbar. Für die Lösungen $x = Tx'$ folgt hieraus $x = (15 - 15x_3', 12x_3' - 7, 32x_3' - 26)$.

§**7Dc. Effiziente Berechnung der Determinante.** Im Determinanten-Satz 7C4 wird die Determinante durch die folgende explizite Leibniz–Formel charakterisiert:

$$\det A = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.$$

Für kleine Werte von n (zum Beispiel $n = 2$ oder $n = 3$) eignet sich diese Formel gut zur Berechnung der Determinante. Zum Beispiel findet man so

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

sowie die *Regel von Sarrus*

$$\begin{aligned} \det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ &\quad - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}. \end{aligned}$$

Für etwas größere Werte von n wird dies jedoch schnell unhandlich, da die Anzahl $n!$ der auszuwertenden Terme stark wächst:

$10! = 3628800$

$20! = 2432902008176640000$

$30! = 265252859812191058636308480000000$

$40! = 815915283247897734345611269596115894272000000000$

$50! = 30414093201713378043612608166064768844377641568960512000000000000$

Bemerkung 7D11. Die rekursive Entwicklung entlang einer Spalte oder einer Zeile ist eine Umformulierung der Leibniz–Formel und im Allgemeinen ebenso kostspielig. Sie lohnt sich vor allem, wenn in der gewählten Zeile/Spalte viele Nullen vorliegen. Man spricht in diesem Fall von einer *dünn besetzten Matrix*.

Im Falle einer voll besetzten Matrix (mit wenig Nullen) ist der Algorithmus von Gauß–Bézout effizienter: Zur Diagonalisierung $D = SAT$ benötigt er ungefähr n^3 Operationen im Ring K, und erlaubt auf einfache Weise die Berechnung der Determinante $\det(D) = \det(A)$.

Geht es allein um die Berechnung der Determinante $\det(A)$, so kann man sich noch Arbeit sparen: Es reicht mittels Zeilenoperationen die Matrix A auf obere Dreiecksform zu bringen, also $D = SA$ mit $S \in \mathrm{SL}_n(K)$ sodass $d_{ij} = 0$ für alle $i > j$ gilt. Es gilt dann $\det(A) = \det(D) = d_{11}d_{22}\cdots d_{nn}$.

§**7Dd. Effiziente Berechnung der inversen Matrix.** Der Determinanten-Satz 7C4 beschert uns für die inverse Matrix die Formel $A^{-1} = \det(A)^{-1}\tilde{A}$. Für kleine Werte von n (zum Beispiel $n = 2$ oder $n = 3$) eignet sich diese Formel gut, für etwas größere Werte von n wird sie jedoch schnell unhandlich. Auch hier schafft der Algorithmus von Gauß–Bézout Abhilfe. Aus $D = SAT$ folgt $A^{-1} = TD^{-1}S$, wobei die Diagonalmatrix $D = \operatorname{diag}(d_1, \ldots, d_n)$ leicht zu invertieren ist, denn $D^{-1} = \operatorname{diag}(d_1^{-1}, \ldots, d_n^{-1})$.

Es ist oft nützlich, neben S und T auch die Inversen S^{-1} und T^{-1} zu berechnen. In jedem Schritt des Algorithmus von Gauß–Bézout liegen die Transformationsmatrizen in $\mathrm{SL}_2(K)$ und sind daher sehr einfach zu invertieren. Das Inverse des Produkts berechnet man

dann als Produkt der Inversen (in umgekehrter Reihenfolge). Diese Berechnung führt man am besten schon während des obigen Algorithmus parallel aus, sodass man mit S,T auch gleich S^{-1},T^{-1} konstruiert.

§**7De. Erzeugung der Gruppen** $\mathrm{SL}_n(K)$ **und** $\mathrm{GL}_n(K)$**.** Der Algorithmus von Gauß–Bézout hat interessante Konsequenzen für die Struktur der Gruppen $\mathrm{SL}_n(K)$ und $\mathrm{GL}_n(K)$ über einem Hauptidealring K. Es lohnt sich, diese hier auszuführen.

In der obigen Formulierung des Algorithmus genügen uns Zeilenoperationen auf benachbarten Zeilen. Diese entsprechen der Operation der Untergruppe

$$\psi_k(SL_2(K)) = \begin{pmatrix} 1_{k\times k} & 0 & 0 \\ 0 & \mathrm{SL}_2(K) & 0 \\ 0 & 0 & 1_{\ell\times\ell} \end{pmatrix}$$

Gleiches gilt für Spalten- und Diagonaloperationen: auch hier operieren wir mittels $\mathrm{SL}_2(K)$ auf benachbarten Zeilen und Spalten. Das bedeutet:

Korollar 7D12. *Sei K ein Hauptidealring. Für jedes $n \geq 2$ wird die Gruppe $\mathrm{SL}_n(K)$ erzeugt durch die Untergruppen $\psi_k(\mathrm{SL}_2(K))$, wobei $k = 0,\dots,n-2$.*

BEWEIS. Wir haben zu zeigen, dass $\mathrm{SL}_n(K)$ mit der Untergruppe

$$G := \langle\, \psi_k(SL_2(K)) \mid k = 0,\dots,n-2 \,\rangle$$

übereinstimmt. Für $A \in \mathrm{SL}_n(K)$ liefert der Algorithmus von Gauß–Bézout Transformationsmatrizen $S,T \in G$ sodass $D = SAT$ Elementartailerform hat. Aufgrund unserer Normierung und der Voraussetzung $\det(D) = \det(A) = 1$ gilt dann $D = 1_{n\times n}$, also $A = ST \in G$. □

Bemerkung 7D13. Die Gruppe $\mathrm{GL}_n(K)$ wird erzeugt durch die Untergruppen $\psi_0(K^\times)$ und $\mathrm{SL}_n(K)$, denn jede Matrix $S \in \mathrm{GL}_n(K)$ schreibt sich als ein Produkt $S = S_0S_1$ mit $S_0 = \mathrm{diag}(\det(S),1,\dots,1)$ und $S_1 \in \mathrm{SL}_n(K)$.

Über einem euklidischen Ring K können wir noch mehr sagen:

Satz 7D14. *Über jedem euklidischen Ring K wird $\mathrm{SL}_2(K)$ erzeugt von den Matrizen*

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \textit{und} \quad \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \quad \textit{mit } q \in K. \tag{7.5}$$

Ebenso wird $\mathrm{SL}_2(K)$ erzeugt von den Transvektionen

$$\begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} \quad \textit{und} \quad \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \quad \textit{mit } q \in K. \tag{7.6}$$

BEWEIS. Aus $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ folgt $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^4 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Die Matrizen $\left(\begin{smallmatrix} 0 & \mp 1 \\ \pm 1 & 0 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} 1 & q \\ 0 & 1 \end{smallmatrix}\right)$ beschreiben die Operationen des euklidischen Algorithmus 3 (mit normierten Vorzeichen). Zusammen mit dem Algorithmus von Gauß–Bézout können wir so jede Matrix $A \in K^{2\times 2}$ in Diagonalform $\left(\begin{smallmatrix} u & 0 \\ 0 & v \end{smallmatrix}\right)$ bringen. Für $A \in \mathrm{SL}_2(K)$ gilt dann $uv = 1$. Solche Matrizen schließlich können erzeugt werden mittels

$$\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & u^{-1} \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & u^{-1} \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} u & 0 \\ 0 & u^{-1} \end{smallmatrix}\right)$$

Das beweist, dass die Familie (7.5) die Gruppe $\mathrm{SL}_2(K)$ erzeugt. Dass auch (7.6) ein Erzeugendensystem ist, sieht man sofort mittels $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&-1\\0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)=\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$. □

Korollar 7D15. *Die Gruppe* $\mathrm{SL}_2(\mathbb{Z})$ *wird erzeugt von den beiden Matrizen*

$$\begin{pmatrix}0&-1\\1&0\end{pmatrix} \quad \textit{und} \quad \begin{pmatrix}1&1\\0&1\end{pmatrix}$$

Ebenso wird $\mathrm{SL}_2(\mathbb{Z})$ *erzeugt von den beiden Matrizen*

$$\begin{pmatrix}1&0\\1&1\end{pmatrix} \quad \textit{und} \quad \begin{pmatrix}1&1\\0&1\end{pmatrix}$$

BEWEIS. Für alle $q\in\mathbb{Z}$ gilt $\left(\begin{smallmatrix}1&q\\0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)^q$ sowie $\left(\begin{smallmatrix}1&0\\q&1\end{smallmatrix}\right)=\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)^q$. Die Aussagen über $\mathrm{SL}_2(\mathbb{Z})$ folgen dann als Spezialfall aus Satz 7D14. □

§7E. Eindeutigkeit der Elementarteiler

Der Algorithmus von Gauß–Bézout lässt viele Varianten zu. Bereits die jeweils verwendeten Bézout–Koeffzienten sind nicht eindeutig. Auch die Reihenfolge der Operationen ist zu einem gewissen Grad willkürlich. Die daraus bestimmten Transformationsmatrizen S und T hängen von all diesen Wahlen ab und sind keineswegs eindeutig.

Man könnte sich also vorstellen, dass man ausgehend von $A\in K^{m\times n}$ auf zwei verschiedenen Wegen zu verschiedenen Elementarteilern gelangt. Für Diagonalmatrizen ist dies jedenfalls möglich, zum Beispiel sind $\left(\begin{smallmatrix}4&0\\0&6\end{smallmatrix}\right)$ und $\left(\begin{smallmatrix}2&0\\0&12\end{smallmatrix}\right)$ ineinander überführbar mittels

$$A=\begin{pmatrix}4&0\\0&6\end{pmatrix}\mapsto SAT=\begin{pmatrix}2&0\\0&12\end{pmatrix} \quad \text{mit} \quad S=\begin{pmatrix}2&-1\\-3&2\end{pmatrix} \quad \text{und} \quad T=\begin{pmatrix}1&3\\1&4\end{pmatrix}.$$

Es ist daher durchaus bemerkenswert, dass die Elementarteiler eindeutig sind:

Satz 7E1. *Die Elementarteiler einer Matrix* $A\in K^{m\times n}$ *sind eindeutig: Haben sowohl* $D=SAT$ *als auch* $D'=S'AT'$ *Elementarteilerform, wobei* $S,S'\in\mathrm{SL}_m(K)$ *und* $T,T'\in\mathrm{SL}_n(K)$*, dann gilt* $d_{ii}\sim d'_{ii}$ *für alle i.*

Bemerkung 7E2. In unserer Formulierung liefert der Algorithmus von Gauß–Bézout normierte Diagonaleinträge $d_{11},\dots,d_{\ell-1,\ell-1}$; nur der letzte Eintrag $d_{\ell\ell}$ kann im Allgemeinen nicht normiert werden. Sind $D=SAT$ und $D'=S'AT'$ in Elementarteilerform, und sind zudem die Diagonaleinträge normiert, dann gilt sogar $d_{ii}=d'_{ii}$ für alle i. Für $i=1,\dots,\ell-1$ ist dies klar, für $i=\ell$ folgt es aus der Invarianz von $\det(D)=\det(D')$.

Wir haben den obigen Satz für Transformationsmatrizen mit Determinante 1 formuliert, da dies unserem Algorithmus entspricht. Die Eindeutigkeit gilt aber ganz allgemein für Transformationen mit beliebigen invertierbaren Matrizen:

Korollar 7E3. *Sei* $A\in K^{m\times n}$*. Haben sowohl* $D=SAT$ *als auch* $D'=S'AT'$ *Elementarteilerform, wobei* $S,S'\in\mathrm{GL}_m(K)$ *und* $T,T'\in\mathrm{GL}_n(K)$*, dann gilt* $d_{ii}\sim d'_{ii}$ *für alle i.*

BEWEIS. Dies ist eine leichte Erweiterung des Satzes 7E1. Jede Matrix $S\in\mathrm{GL}_m(K)$ schreibt sich als $S=S_0S_1$ mit $S_0=\mathrm{diag}(1,\dots,1,\det(S))$ und $S_1\in\mathrm{SL}_m(K)$. Ebenso schreibt sich jede Matrix $T\in\mathrm{GL}_n(K)$ als $T=T_1T_0$ mit $T_0=\mathrm{diag}(1,\dots,1,\det(T))$ und $T_1\in\mathrm{SL}_n(K)$. Wenn also $D=SAT$ Elementarteilerform hat, dann auch $D_1=S_1AT_1$: beide Matrizen sind

gleich, lediglich die letzten Diagonalelement unterscheiden sich durch invertierbare Elemente. Entsprechendes gilt für $D' = S'AT'$ und $D'_1 = S'_1 A T'_1$. Wir können nun Satz 7E1 auf D_1 und D'_1 anwenden. □

§**7Ea. Beweis der Eindeutigkeit mittels der Determinante.** Zum Beweis dieses schönen Ergebnisses verwenden wir unser elegantestes Werkzeug: die Determinante.

Definition 7E4. Sei $A \in K^{m\times n}$ und $\ell = \min(m,n)$. Für $1 \le k \le \ell$ definieren wir das Ideal

$$\Delta_k(A) = \left(\det(A|_{I\times J}) \;\middle|\; \begin{matrix} I = \{s_1 < \cdots < s_k\} \subset \{1,\dots,m\} \\ J = \{t_1 < \cdots < t_k\} \subset \{1,\dots,n\} \end{matrix} \right)_K .$$

Hierbei bezeichnet $A|_{I\times J} \in K^{k\times k}$ die Matrix mit Koeffizienten $(a_{s_i,t_j})_{ij}$. Dies ist die $k\times k$-Untermatrix, die man aus A erhält, wenn man nur die Zeilen aus I und die Spalten aus J behält. Anders gesagt, $\Delta_k(A)$ ist das Ideal, das von den Determinanten aller $k\times k$-Untermatrizen von A erzeugt wird.

Definition 7E5. Über einem faktoriellen Ring K definieren wir

$$\delta_k(A) = \operatorname{ggT}\left(\det(A|_{I\times J}) \;\middle|\; \begin{matrix} I = \{s_1 < \cdots < s_k\} \subset \{1,\dots,m\} \\ J = \{t_1 < \cdots < t_k\} \subset \{1,\dots,n\} \end{matrix} \right).$$

Anders gesagt, $\delta_k(A)$ ist der ggT der Determinanten aller $k\times k$-Untermatrizen von A. Ist K ein Hauptidealring, dann gilt offenbar $\Delta_k(A) = (\delta_k(A))_K$.

Beispiel 7E6. Sei $D \in K^{m\times n}$ in Elementarteilerform, also diagonal mit $d_{11} \mid d_{22} \mid \cdots \mid d_{\ell\ell}$ wobei $\ell = \min(m,n)$. Wenn $I \neq J$, dann ist $\det(A|_{I\times J}) = 0$, denn $A|_{I\times J}$ enthält eine Nullzeile oder eine Nullspalte. Für $I = J = \{s_1 < \cdots < s_k\}$ ist $\det(A|_{I\times J}) = d_{s_1,s_1} d_{s_2,s_2} \cdots d_{s_k,s_k}$. Demnach gilt $\Delta_k(D) = (d_{11}d_{22}\cdots d_{kk})$ und $\delta_k(D) \sim d_{11}d_{22}\cdots d_{kk}$.

Lemma 7E7. *Sei $A \in K^{m\times n}$. Das Ideal $\Delta_k(A) \lhd K$ und das Element $\delta_k(A) \in K$ ändern sich nicht bei Zeilen-, Spalten-, oder Diagonaloperationen.*

BEWEIS. Es reicht, dies für eine Spaltenoperation zu beweisen. Angenommen $T = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \mathrm{SL}_2(K)$ operiert auf den Spalten i und j, also

$$A = (\dots, v_i, \dots, v_j, \dots) \mapsto A' = (\dots, av_i + bv_j, \dots, cv_i + dv_j, \dots)$$

Wenn J weder i noch j enthält, dann gilt $\det(A'|_{I\times J}) = \det(A|_{I\times J})$. Wenn J sowohl i als auch j enthält, dann gilt $\det(A'|_{I\times J}) = \det(A|_{I\times J})\det(T) = \det(A|_{I\times J})$. Wenn J zwar i aber nicht j enthält, dann gibt es hierzu die Menge $J' = (J \smallsetminus \{i\}) \cup \{j\}$, die zwar j aber nicht i enthält. Es gilt dann

$$\begin{aligned} \det(A'|_{I\times J}) &= a\det(A|_{I\times J}) + b\det(A|_{I\times J'}), \\ \det(A'|_{I\times J'}) &= c\det(A|_{I\times J}) + d\det(A|_{I\times J'}). \end{aligned}$$

Die Invarianz von $\Delta_k(A)$ und $\delta_k(A)$ ergibt sich dann aus dem folgenden Lemma. □

Lemma 7E8. *Für $T = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ und $x,y \in K$ gilt* $\operatorname{ggT}(x,y) = \operatorname{ggT}(ax+by, cx+dy)$ *sowie* $(x,y)_K = (ax+by, cx+dy)_K$.

BEWEIS. Offenbar gilt $\mathrm{GT}(x,y) \subset \mathrm{GT}(ax+by, cx+dy)$. Man beachte hierbei, dass $(ax+by, cx+dy) = (x,y)T$ gilt. Da T invertierbar ist, folgt $(ax+by, cx+dy)T^{-1} = (x,y)$,

und damit auch $\mathrm{GT}(ax+by,cx+dy) \subset \mathrm{GT}(x,y)$. Für die Ideal gilt entsprechend $(x,y)_K \supset (ax+by,cx+dy)_K$, und $(x,y)_K \subset (ax+by,cx+dy)_K$ weil T invertierbar ist. □

BEWEIS DES EINDEUTIGKEITSSATZES 7E1. Die Gruppe $\mathrm{SL}_n(K)$ wird von den Untergruppen $\psi_k \mathrm{SL}_2(K)$ erzeugt (7D12). Von diesen wissen wir, dass sie $\delta_k(A)$ invariant lassen (7E7). Also gilt $\delta_k(D) = \delta_k(D')$ für alle $k = 1,\dots,\ell$ wobei $\ell = \min(m,n)$. Nach 7E6 gilt $\delta_1(D) \sim d_{11}$ und $\delta_1(D') \sim d'_{11}$, also $d_{11} \sim d'_{11}$. Weiterhin gilt $\delta_2(D) \sim d_{11}d_{22}$ und $\delta_1(D') \sim d'_{11}d'_{22}$, also $d_{11}d_{22} \sim d'_{11}d'_{22}$. Wenn $d_{11} \neq 0$, dann können wir kürzen und erhalten $d_{22} \sim d'_{22}$. Wenn $d_{11} = 0$ dann $d'_{11} = 0$ und aus der Bedingung $d_{11} \mid d_{22}$ und $d'_{11} \mid d'_{22}$ folgt $d_{22} = d'_{22} = 0$. So fortfahrend erhalten wir per Induktion $d_{ii} \sim d'_{ii}$ für alle $i = 1,\dots,\ell$. □

§**7Eb. Bemerkung zu allgemeinen Ringen.** Über jedem Hauptidealring K garantiert der Algorithmus von Gauß–Bézout, dass wir jede Matrix $A \in K^{m\times n}$ in Elementarteilerform $D = SAT$ bringen können. Über allgemeinen Ringen ist dies nicht der Fall. Im Allgemeinen kann hier jedes (endlich-erzeugte) Ideal von K entstehen, denn $\Delta_1(A) = (a_{11},\dots,a_{nn})_K$.

Beispiel 7E9. Für $A = \left(\begin{smallmatrix} 2 & 0 \\ 0 & X \end{smallmatrix}\right)$ über $\mathbb{Z}[X]$ ist $\Delta_1(A) = (2,X)$ kein Hauptideal (5H6). Für den ggT gilt hier $\delta_1(A) = 1$, beide Invarianten klaffen also auseinander. Ist $D = SAT$ in Elementarteilerform, also $D = \left(\begin{smallmatrix} d_1 & 0 \\ 0 & d_2 \end{smallmatrix}\right)$ mit $d_1, d_2 \in \mathbb{Z}[X]$ und $d_1 \mid d_2$, dann wäre $\Delta_1(D) = (d_1)$ ein Hauptideal. Hier gilt offenbar $\delta_1(D) \sim d_1$, beide Invarianten stimmen also überein. Die Invarianz führt dann zu dem Widerspruch $(2,X) = \Delta_1(A) = \Delta_1(D) = (d_1)$.

KAPITEL 8

Moduln und Vektorräume

§8A. Motivation und Überblick

Die lineare Algebra beschäftigt sich mit Vektorräumen über Körpern. In diesem Kapitel erweitern wir diesen Begriff zu Moduln über Ringen. Während jeder K-Vektorraum eine Basis über K besitzt und daher bis auf Isomorphie allein durch seine Dimension bestimmt ist, erlauben Moduln über Ringen eine wesentlich größere Vielfalt an Möglichkeiten.

Zum Beispiel ist jede abelsche Gruppe ein $\mathbb{Z}$-Modul, etwa die zyklische Gruppe $\mathbb{Z}/a$. Das folgende Ergebnis verschafft uns einen Überblick über alle endlichen abelschen Gruppen:

Satz 8A1 (Klassifikation endlicher abelscher Gruppen)**.** *Jede endliche abelsche Gruppe A ist isomorph zu einem Produkt von zyklischen Gruppen, das heißt*

$$A \cong \mathbb{Z}/a_1 \times \mathbb{Z}/a_2 \times \cdots \times \mathbb{Z}/a_m \qquad \text{wobei } a_1, a_2, \ldots, a_m \in \mathbb{Z}_{\geq 2}.$$

Hierbei können wir zusätzlich verlangen, dass $a_1 \mid a_2 \mid \cdots \mid a_m$ gelte. In diesem Fall nennen wir $a_1, a_2, \ldots, a_m$ Elementarteiler *von A, und diese sind eindeutig durch A bestimmt: Gilt*

$$\mathbb{Z}/a_1 \times \cdots \times \mathbb{Z}/a_m \cong \mathbb{Z}/b_1 \times \cdots \times \mathbb{Z}/b_n$$

mit $b_1, \ldots, b_n \in \mathbb{Z}_{\geq 2}$ und $b_1 \mid b_2 \mid \cdots \mid b_n$, dann folgt daraus $m = n$ und $a_1 = b_1, \ldots, a_m = b_m$.

Ziel dieses Kapitels. Nach der Einführung des Grundvokabulars konzentrieren wir uns auf Moduln über Hauptidealringen und erstellen deren Klassifikation nach dem Muster des obigen Beispiels. Dies beinhaltet als wichtige Spezialfälle abelsche Gruppen als $\mathbb{Z}$-Moduln ebenso wie Vektorräume über Körpern.

§8B. Moduln über einem Ring

Definition 8B1. Sei $(R, +, \cdot)$ ein kommutativer Ring. Ein *R-Modul* $(M, +, \bullet)$ besteht aus einer abelschen Gruppe $(M, +)$ zusammen mit einer Operation $\bullet\colon R \times M \to M$, geschrieben $(a, x) \mapsto a \bullet x$, die für alle $a, b \in R$ und $x, y \in M$ folgenden Axiomen genügt:

1. $a \bullet (x + y) = (a \bullet x) + (a \bullet y)$,
2. $(a + b) \bullet x = (a \bullet x) + (b \bullet x)$,
3. $(a \cdot b) \bullet x = a \bullet (b \bullet x)$,

4. $1 \bullet x = x$.

Statt R-Modul sagt man auch *Modul über R*. Ist R ein Körper, so nennt man jeden R-Modul auch *R-Vektorraum* oder *Vektorraum über R*.

Beispiel 8B2. Die Menge $M = \{0\}$ ist auf genau eine Weise ein R-Modul, nämlich durch die Gruppenstruktur $0+0=0$ und die Operation $a \bullet 0 = 0$ für alle $a \in R$. Dies wird der *Nullmodul* genannt. Statt $M = \{0\}$ schreibt man gelegentlich auch $M = 0$.

Beispiel 8B3. Die abelsche Gruppe $(\mathbb{Z}/_n, +)$ ist ein $\mathbb{Z}$-Modul: die Operation $\mathbb{Z} \times \mathbb{Z}/_n \to \mathbb{Z}/_n$ ist gegeben durch $(n, \mathfrak{cl}(x)) \mapsto \mathfrak{cl}(nx)$.

Beispiel 8B4. Jede abelsche Gruppe $(M,+)$ ist auf genau eine Weise ein $\mathbb{Z}$-Modul. Die Operation $\mathbb{Z} \times M \to M$ ist hierbei das Vielfache $(n,x) \mapsto nx$ (2E3). Diesen Ansatz werden wir zur Klassifikation der endlich erzeugten abelschen Gruppen nutzen (8A1).

Beispiel 8B5. Sind $M_1, \ldots, M_n$ Moduln über R, dann wird ihr kartesisches Produkt $M = M_1 \times \cdots \times M_n$ eine abelsche Gruppe mittels der komponentenweisen Addition (2D28), und ein Modul über R mittels der komponentenweisen Operation $\bullet\colon R \times M \to M$ gegeben durch $a \bullet (x_1, \ldots, x_n) = (a \bullet x_1, \ldots, a \bullet x_n)$, siehe §8Be und §8Bf.

Notation. Ebenso wie die Multiplikation $\cdot\colon R \times R \to R$, die wir abkürzend ab schreiben statt $a \cdot b$, schreiben wir auch die Operation $\bullet\colon R \times M \to M$ kürzer ax statt $a \bullet x$. Meistens geht aus dem Kontext unmissverständlich hervor, welche Verknüpfung gemeint ist. Ebenso nutzen wir weiterhin die Konvention "Punkt vor Strich" um Klammern zu sparen. Die obigen Axiome schreiben sich dann etwas gefälliger wie folgt:

1. $a(x+y) = ax + ay$
2. $(a+b)x = ax + bx$
3. $(ab)x = a(bx)$
4. $1x = x$

§**8Ba. Links- und Rechtsmoduln.** Im Falle eines nicht-kommutativen Rings R müssen wir zwischen Links- und Rechtsmoduln über R unterscheiden. Die obige Definition 8B1 ist dann die eines *Linksmoduls*; entsprechend definiert man den Begriff des *Rechtsmoduls*:

Definition 8B6. Ein *Rechtsmodul über R* besteht aus einer abelschen Gruppe $(M,+)$ zusammen mit einer Operation $\bullet\colon M \times R \to M$, geschrieben $(x,a) \mapsto xa$, die für alle $a,b \in R$ und $x,y \in M$ folgenden Axiomen genügt:

1. $(x+y)a = xa + ya$
2. $x(a+b) = xa + xb$
3. $x(ab) = (xa)b$
4. $x1 = x$

Bemerkung 8B7. Ausgehend von $\bullet\colon M \times R \to M$ kann man $\bar{\bullet}\colon R \times M \to M$ definieren durch $a \,\bar{\bullet}\, x = x \bullet a$. Es gilt dann allerdings $a \,\bar{\bullet}\, (b \,\bar{\bullet}\, x) = (b \cdot a) \,\bar{\bullet}\, x$. Ein Rechtsmodul über dem Ring $(R,+,\cdot)$ entspricht demnach einem Linksmodul über dem entgegengesetzten Ring $(R,+,\bar{\cdot})$ wobei $a \,\bar{\cdot}\, b = b \cdot a$ gesetzt wird (3A13). Falls der Ring R kommutativ ist, dann stimmt er mit seinem entgegengesetzten Ring überein: Links- und Rechtsmoduln unterscheiden sich dann nur in der Schreibweise der Multiplikation.

Beispiel 8B8. Sei $(S,+,\cdot)$ ein Ring. Ist $R \subset S$ ein Unterring, dann ist die abelsche Gruppe $(S,+)$ ein Linksmodul über R durch Einschränkung der Multiplikation $\cdot\colon S\times S \to S$ zu $R\times S \to S$. Entsprechend ist $(S,+)$ ein Rechtsmodul über R durch Einschränkung der Multiplikation $\cdot\colon S\times S \to S$ zu $S\times R \to S$. Damit wird S zu einem (R,R)-Bimodul:

Definition 8B9. Seien R,S zwei Ringe. Ein (R,S)-Bimodul besteht aus einer abelschen Gruppe $(M,+)$ zusammen mit einer Operationen $R\times M \to M$, die M zu einem R-Linksmodul macht, und einer Operation $M\times S \to M$, die M zu einem S-Rechtsmodul macht, sodass $(rx)s = r(xs)$ gilt für alle $r \in R$, $x \in M$, $s \in S$.

Beispiel 8B10. Der Polynomring $R[X]$ ist ein Modul über R, ebenso ist jeder Monoidring RM ein Modul über R. Da wir hierbei den Ring R im Zentrum von RM annehmen (siehe §3G), stimmen die so definierten Links- und Rechtsmoduln überein.

Beispiel 8B11. Nach Beispiel 8B8 ist jeder Ring R sowohl ein Linksmodul als auch ein Rechtsmodul über sich selbst. Allgemeiner ist jedes Linksideal $\mathfrak{a} \subset R$ ein Linksmodul über R, denn $(\mathfrak{a},+)$ ist eine Untergruppe von $(R,+)$ und wegen $R\mathfrak{a} \subset \mathfrak{a}$ können wir die Multiplikation einschränken zu $R\times\mathfrak{a} \to \mathfrak{a}$. Entsprechend ist jedes Rechtsideal $\mathfrak{a} \subset R$ ein Rechtsmodul über R, denn $(\mathfrak{a},+)$ ist eine Untergruppe von $(R,+)$ und wegen $\mathfrak{a}R \subset \mathfrak{a}$ können wir die Multiplikation einschränken zu $\mathfrak{a}\times R \to \mathfrak{a}$. Unter einem Ideal $\mathfrak{a} \lhd R$ verstehen wir weiterhin stets ein beidseitiges Ideal. Dies ist dann ein (R,R)-Bimodul.

Beispiel 8B12. Für jeden Ring R ist $R^{m\times n}$ ein Linksmodul über dem Matrizenring $R^{m\times m}$ und ein Rechtsmodul über dem Matrizenring $R^{n\times n}$, wie in §7Ba erklärt.

Insbesondere ist die Menge $R^{n\times 1}$ der Spaltenvektoren ein Linksmodul über dem Matrizenring $R^{n\times n}$ vermöge der Operation $*\colon R^{n\times n}\times R^{n\times 1} \to R^{n\times 1}$, $(A,x) \mapsto Ax$.

Entsprechend ist die Menge $R^{1\times n}$ der Zeilenvektoren ein Rechtsmodul über dem Matrizenring $R^{n\times n}$ vermöge der Operation $*\colon R^{1\times n}\times R^{n\times n} \to R^{1\times n}$, $(x,A) \mapsto xA$.

Wir betrachten im Folgenden nur noch Linksmoduln und sprechen kurz von Moduln. Für kommutative Ringe ist dies keine Einschränkung. Im Falle nicht-kommutativer Ringe kann man alle Aussagen gemäß Bemerkung 8B7 von Links- auf Rechtsmoduln übertragen.

Beispiel 8B13. Für jede abelsche Gruppe $(M,+)$ ist die Menge $R = \operatorname{End}(M,+)$ aller Gruppenendomorphismen ein Ring (2E8). Damit wird M zu einem R-Modul, wobei die Operation $R\times M \to M$ durch die Auswertung $(f,x) = f(x)$ gegeben ist.

Bemerkung 8B14. Ein Modul $(M,+,\cdot)$ über R ist nichts anderes als eine abelsche Gruppe $(M,+)$ zusammen mit einem Ringhomomorphismus $\varphi\colon R \to \operatorname{End}(M,+)$.

Ist nämlich $(M,+,\bullet)$ ein Modul über R, dann operiert R auf der abelschen Gruppe $(M,+)$ durch $\bullet\colon R\times M \to M$, $(a,x) \mapsto ax$. Dies definiert einen Ringhomomorphismus $\varphi\colon R \to \operatorname{End}(M,+)$ durch $\varphi(a)\colon M \to M$, $x \mapsto a\bullet x$.

Ist umgekehrt $(M,+)$ eine abelsche Gruppe, dann definiert jeder Ringhomomorphismus $\varphi\colon R \to \operatorname{End}(M,+)$ eine Operation $\bullet\colon R\times M \to M$ durch $a\bullet x := \varphi(a)(x)$, und $(M,+,\bullet)$ wird hierdurch zu einem Modul über R.

§**8Bb. Homomorphismen.** Ein *Homomorphismus* zwischen R-Moduln M und N ist ein Gruppenhomomorphismus $f\colon M \to N$ sodass $f(ax) = af(x)$ für alle $a \in R$ und $x \in M$

gilt. Dies nennt man auch einen *R-Homomorphismus* oder eine *R-lineare Abbildung*. Die Menge aller R-Homomorphismen $M \to N$ bezeichnen wir mit $\mathrm{Hom}_R(M,N)$.

Beispiel 8B15. Vom Nullmodul $\{0\}$ aus gibt es genau einen R-Homomorphismus in jeden R-Modul N, nämlich die Nullabbildung $0 \mapsto 0_N$. Umgekehrt gibt es von jedem R-Modul M genau einen R-Homomorphismus nach $\{0\}$, nämlich die Nullabbildung $x \mapsto 0$ für alle $x \in M$. Allgemein bezeichnet man die Nullabbildung $M \to 0 \to N$ kurzerhand mit 0.

Beispiel 8B16. Jede abelsche Gruppe ist auf genau eine Weise ein $\mathbb{Z}$-Modul (8B4). Für abelsche Gruppen M,N ist jeder Gruppenhomomorphismus $f\colon M \to N$ ein $\mathbb{Z}$-Homomorphismus, das heißt es gilt $f(ax) = af(x)$ für alle $a \in \mathbb{Z}$ und $x \in M$.

Beispiel 8B17. Jede Matrix $A \in R^{m\times n}$ über einem Ring R definiert einen Gruppenhomomorphismus $R^n \to R^m$ durch $x \mapsto Ax$. Wenn der Ring R kommutativ ist, dann ist dies ein R-Homomorphismus, denn es gilt dann $A(ax) = a(Ax)$ für alle $a \in R$ und $x \in R^n$.

Ebenso definiert $A \in R^{m\times n}$ einen Gruppenhomomorphismus $R^{1\times m} \to R^{1\times n}$ durch $x \mapsto xA$. Selbst wenn der Ring R nicht-kommutativ ist, so ist dies ein R-Homomorphismus, denn es gilt dann $(ax)A = a(xA)$ für alle $a \in R$ und $x \in R^{1\times m}$.

Proposition 8B18. *Die R-Moduln und R-Homomorphismen bilden eine Kategorie:*

1. *Für jeden Modul M ist die Identität* $\mathrm{id}_M\colon M \to M$ *ein R-Homomorphismus.*
2. *Sind* $f\colon M \to N$ *und* $g\colon N \to P$ *Homomorphismen über R, so ist auch ihre Komposition* $g \circ f\colon M \to P$ *ein Homomorphismus über R.*
3. *Diese Komposition ist assoziativ, das heißt* $(h \circ g) \circ f = h \circ (g \circ f)$.

Einen bijektiven Homomorphismus $f\colon M \to N$ nennen wir wie üblich *Isomorphismus*, geschrieben $M \xrightarrow{\sim} N$. In diesem Fall ist auch die Umkehrabbildung $f^{-1}\colon N \to M$ ein Isomorphismus. Weiterhin definieren wir:

- Ein *R-Endomorphismus* von M ist ein R-Homomorphismus $M \to M$.
  Die Menge aller R-Endomorphismen von M bezeichnen wir mit $\mathrm{End}_R(M)$.
- Ein *R-Automorphismus* von M ist ein Isomorphismus $M \xrightarrow{\sim} M$.
  Die Menge aller Automorphismen von M bezeichnen wir mit $\mathrm{Aut}_R(M)$.

Proposition 8B19. *Die Menge* $\mathrm{Hom}_R(M,N)$ *der R-Homomorphismen ist eine abelsche Gruppe bezüglich punktweiser Addition,* $(f+g)(x) := f(x)+g(x)$ *für alle* $x \in M$.

Ist der Ring R kommutativ, dann ist $\mathrm{Hom}_R(M,N)$ *sogar ein R-Modul bezüglich punktweiser Multiplikation* $(af)(x) := af(x)$ *mit* $a \in R$.

BEWEIS. Den Teil für abelsche Gruppen haben wir bereits in Proposition 2E6 gesehen. Für alle $b \in R$ und $x \in M$ gilt

$$(f+g)(bx) = f(bx)+g(bx) = bf(x)+bg(x) = b(f(x)+g(x)) = b(f+g)(x).$$

Ist R kommutativ, dann gilt für alle $a,b \in R$ auch

$$(af)(bx) = af(bx) = abf(x) = baf(x) = b(af)(x). \qquad \square$$

Korollar 8B20. *Die Menge* $\mathrm{End}_R(M)$ *der R-Endomorphismen ist ein Ring bezüglich punktweiser Addition und der Komposition von Abbildungen.* $\square$

Beispiel 8B21. Sei K ein kommutativer Ring und M ein K-Modul. Gegeben sei eine K-lineare Abbildung $f \in \mathrm{End}_K(M)$. Hierdurch wird M zu einem $K[X]$-Modul mit der Operation $K[X] \times V \to V$ gegeben durch $(P,v) \mapsto P(f)(v)$. Dies entspricht der Fortsetzung des Ringhomomorphismus $\varphi\colon K \to \mathrm{End}(M,+)$ zu einem Ringhomomorphismus $\tilde{\varphi}\colon K[X] \to \mathrm{End}(M,+)$ mit $X \mapsto f$. Man beachte hierbei, dass $\varphi(a)$ für $a \in K$ mit f kommutiert: Das ist gerade die Bedingung $f(ax) = af(x)$ für alle $x \in M$. Wir können also die universelle Eigenschaft des Polynomring $K[X]$ über K wie gewünscht einsetzen (4A4). Diesen Ansatz kann man zur Konstruktion von Normalformen nutzen (§8Fd).

§**8Bc. Untermoduln.** Sei M ein Modul über einem Ring R. Eine Teilmenge $U \subset M$ heißt *Untermodul* über R falls U eine Untergruppe von $(M,+)$ ist und $RU = U$ gilt.

In diesem Fall ist U ein R-Modul bezüglich der Einschränkung $R \times U \to U$, und die Inklusion $\iota_U^M\colon U \hookrightarrow M$ ist ein R-Homomorphismus.

Die Aussage, dass U ein untermodul von M ist, schreiben wir abkürzend $U < M$.

Beispiel 8B22. Jeder kommutative Ring R ist ein Modul über sich selbst (8B8). Die Untermoduln $\mathfrak{a} < R$ sind genau die Ideale in R.

Proposition 8B23. *Ist $(U_i)_{i\in I}$ eine Familie von Untermoduln $U_i \subset M$ eines R-Moduls M, dann ist auch ihr Durchschnitt $U = \bigcap_{i\in I} U_i$ ein Untermodul.*

BEWEIS. Übung! □

Definition 8B24 (erzeugter Untermodul)**.** Sei M ein R-Modul und $\mathscr{X} \subset R$ eine Teilmenge. Dann ist der von $\mathscr{X}$ *erzeugte Untermodul* $\langle \mathscr{X} \rangle_R$ der kleinste Untermodul von M, der $\mathscr{X}$ enthält, also

$$\langle \mathscr{X} \rangle_R := \bigcap \{\, U < R \mid U \supset \mathscr{X} \,\}$$

Proposition 8B25. *Für jede Teilmenge $\mathscr{X} \subset M$ gilt*

$$\langle \mathscr{X} \rangle_R = \Big\{ \sum_{i=1}^{n} r_i x_i \mid n \in \mathbb{N}, x_i \in \mathscr{X}, r_i \in R \Big\}.$$

BEWEIS. Es gilt "$\supset$", denn die rechte Seite ist ein Untermodul von M und enthält $\mathscr{X}$; da $\langle \mathscr{X} \rangle_R$ der kleinste solche Untermodul ist, muss er in der rechten Seite enthalten sein. Umgekehrt gilt "$\supset$", denn der Untermodul $\langle \mathscr{X} \rangle_R$ enthält $\mathscr{X}$ und damit auch alle Summen von Produkten, die auf der rechten Seite auftreten. □

Ist $\mathscr{X} = \{x_1, \ldots, x_n\}$ eine endliche Menge, dann gilt

$$\langle x_1, \ldots, x_n \rangle_R := Rx_1 + \cdots + Rx_n$$

§**8Bd. Torsion.** Sei K ein Integritätsring und M ein K-Modul. Wir nennen $x \in M$ ein *Torsionselement*, wenn es $a \in K^*$ mit $ax = 0$ gibt. Dann ist auch jedes Vielfache bx mit $b \in K$ ein Torsionselement, denn $a(bx) = (ab)x = (ba)x = b(ax) = b0 = 0$. (Hierbei ist die Kommutativität von K wesentlich.) Sind $x, y \in M$ Torsionselemente, dann auch $x+y$, denn aus $a, b \in K^*$ mit $ax = by = 0$ folgt $ab \in K^*$ mit $(ab)(x+y) = 0$. (Hierbei benutzen wir, dass K nullteilerfrei ist.) Zusammenfassend bedeutet dies:

Proposition 8B26. *Die Menge $T \subset M$ der Torsionselemente von M ist ein K-Untermodul.* □

Bemerkung 8B27. Der von $x \in M$ erzeugte zyklische Untermodul Kx ist das Bild des K-Homomorphismus $f\colon K \to M, a \mapsto ax$. Wir haben daher einen Isomorphismus $\bar{f}\colon K/\ker(f) \xrightarrow{\sim} Kx$. Wenn $\ker(f) = \{0\}$ gilt, dann ist f ein Modulisomorphismus. Wenn $\ker(f) \neq \{0\}$, dann existiert $a \in \ker(f)$ mit $a \neq 0$ aber $ax = 0$, also ist x ein Torsionselement.

Ist K ein Hauptidealring, dann gilt $\ker(f) = (m)$ für ein $m \in K$, und wir erhalten somit $\bar{f}\colon K/(m) \xrightarrow{\sim} Kx$. Wir nennen dann m die *Ordnung* von $x \in M$. Das Ideal (m) ist eindeutig bestimmt, das Element m nur bis auf Assoziierte.

§**8Be. Direktes Produkt.** Ist $(M_i)_{i\in I}$ eine Familie von R-Moduln M_i, dann ist das kartesische Produkt $M = \prod_{i\in I} M_i$ eine abelsche Gruppe mittels der komponentenweisen Addition

$$(x_i)_{i\in I} + (y_i)_{i\in I} := (x_i + y_i)_{i\in I}$$

und ein Modul über R mittels der komponentenweisen Operation

$$a(x_i)_{i\in I} := (ax_i)_{i\in I}.$$

Definition 8B28. Wir nennen $M = \prod_{i\in I} M_i$ das *direkte Produkt* der Moduln $(M_i)_{i\in I}$.

Proposition 8B29. *Das Produkt $M = \prod_{i\in I} M_i$ erfreut sich folgender universeller Eigenschaft: Für jedes $i \in I$ ist die Projektion $\pi_i\colon M \to M_i$ ein Modulhomomorphismus. Sind $f_i\colon N \to M_i$ Modulhomomorphismen für $i \in I$ dann existiert genau ein Modulhomomorphismus $f\colon N \to M$, der $f_i = \pi_i \circ f$ für alle $i \in I$ erfüllt.*

Mit anderen Worten, wir haben eine natürliche Bijektion

$$\begin{aligned}\operatorname{Hom}_R(N, \prod_{i\in I} M_i) &\cong \prod_{i\in I} \operatorname{Hom}_R(N, M_i),\\ f &\mapsto (\pi_i \circ f)_{i\in I}.\end{aligned}$$

Übung 8B30. Man beweise die universelle Eigenschaft des direkten Produkts.

§**8Bf. Direkte Summe.** Im Produkt $M = \prod_{i\in I} M_i$ betrachten wir die Teilmenge M' aller Familien $(x_i)_{i\in I}$ mit endlichem Träger, das heißt $x_i \neq 0$ gilt nur für endlich viele Indizes $i \in I$. Diese bildet offenbar einen Untermodul $M' < M$.

Für endliche Indexmenge I gilt selbstverständlich $M' = M$.

Definition 8B31. Wir nennen $M' = \bigoplus_{i\in I} M_i$ die *direkte Summe* der Moduln $(M_i)_{i\in I}$.

Proposition 8B32. *Die direkte Summe $M' = \bigoplus_{i\in I} M_i$ erfreut sich folgender universeller Eigenschaft: Für jedes $i \in I$ ist die Injektion $\iota_i\colon M_i \to M$ ein Modulhomomorphismus. Sind $f_i\colon M_i \to N$ Modulhomomorphismen für $i \in I$ dann existiert genau ein Modulhomomorphismus $f\colon M' \to N$, der $f_i = f \circ \iota_i$ für alle $i \in I$ erfüllt.*

Mit anderen Worten, wir haben eine natürliche Bijektion

$$\begin{aligned}\operatorname{Hom}_R(\bigoplus_{i\in I} M_i, N) &\cong \prod_{i\in I} \operatorname{Hom}_R(M_i, N),\\ f &\mapsto (f \circ \iota_i)_{i\in I}.\end{aligned}$$

Übung 8B33. Man beweise die universelle Eigenschaft der direkten Summe.

§**8Bg. Interne direkte Summe.** Sind A und B zwei R-Moduln, dann ist ihr Produkt $M = A \times B$ ein R-Modul. In diesem sind $U = A \times \{0\}$ und $V = \{0\} \times B$ Untermoduln. Diese haben die Eigenschaft, dass $U + V = M$ und $U \cap V = \{0\}$ gilt. Anders gesagt, jedes Element $x \in M$ schreibt sich eindeutig als Summe $x = u + v$ mit $u \in U$ und $v \in V$.

Definition 8B34. Der R-Modul M ist die *interne direkte Summe* zweier Untermoduln $U, V < M$ wenn sich jedes Element $x \in M$ eindeutig als Summe $x = u + v$ mit $u \in U$ und $v \in V$ schreibt. In diesem Fall schreiben wir $M = U \oplus V$.

Proposition 8B35. *$M = U \oplus V$ ist gleichbedeutend mit $U + V = M$ und $U \cap V = \{0\}$.*

Dies lässt sich auf beliebig viele Summanden verallgemeinern:

Definition 8B36. Sei M ein R-Modul und $(M_i)_{i \in I}$ eine Familie von Untermoduln $M_i < M$. Wir sagen M ist die *interne direkte Summe* der Untermoduln $(M_i)_{i \in I}$ wenn sich jedes Element $x \in M$ eindeutig als Summe $x = \sum_{i \in I} x_i$ schreiben lässt mit $x_i \in M_i$, wobei wie üblich $x_i \neq 0$ nur für endlich viele $i \in I$ gelte. In diesem Fall schreiben wir $M = \oplus_{i \in I} M_i$.

Wir bezeichnen mit $\sum_{i \in I} M_i$ den Untermodul bestehend aus allen Summen $\sum_{i \in I} x_i$ mit $x_i \in M_i$, wobei wie üblich $x_i \neq 0$ nur für endlich viele $i \in I$ gelte.

Proposition 8B37. *$M = \oplus_{i \in I} M_i$ ist gleichbedeutend mit den Bedingungen*

1. *$\sum_{i \in I} M_i = M$ und*
2. *$M_i \cap \sum_{k \neq i} M_k = \{0\}$ für alle $k \in I$.*

Übung 8B38. Man beweise diese Charakterisierung der internen direkten Summe.

Ist M die interne direkte Summe der Untermoduln $(M_i)_{i \in I}$, geschrieben $M = \oplus_{i \in I} M_i$, dann ist M kanonisch isomorph zu der externen direkten Summe der Moduln $(M_i)_{i \in I}$. Dies rechtfertig, beide Konzepte mit demselben Symbol zu bezeichnen, solange der Sinn aus dem Kontext hervorgeht.

§**8Bh. Einfache und unzerlegbare Moduln.** In jedem Modul M sind $\{0\}$ und M Untermoduln, genannt die *trivialen Untermoduln*.

Definition 8B39. Ein R-Modul M heißt *einfach*, wenn für jeden Untermodul $U < M$ entweder $U = \{0\}$ oder $U = M$ gilt.

Beispiel 8B40. Der $\mathbb{Z}$-Modul $\mathbb{Z}$ ist nicht einfach, denn $2\mathbb{Z}$ ist ein echter Untermodul, $\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$. Der $\mathbb{Z}$-Modul $\mathbb{Z}/n$ ist genau dann einfach, wenn n eine Primzahl ist.

Proposition 8B41. *Über einem Hauptidealring K ist ein K-Modul M genau dann einfach, wenn $M \cong K/p$ für ein Primelement $p \in K$ gilt.*

BEWEIS. Ist M einfach, dann gilt $M \neq \{0\}$ und wir können $x \in M$ mit $x \neq 0$ wählen. Da M einfach ist, muss der Untermodul $Kx < M$ mit M übereinstimmen. Der Homomorphismus $f\colon K \to M$, $a \mapsto ax$, ist demnach surjektiv und $\bar{f}\colon K/\ker(f) \xrightarrow{\sim} M$ ist ein Isomorphismus. Da K ein Hauptidealring ist, gilt $\ker(f) = (p)$ für ein $p \in K$. Das Ideal (p) muss maximal sein, also p prim. □

Definition 8B42. Ein Modul M heißt *unzerlegbar*, wenn für jede direkte Summe $M = A \oplus B$ entweder $A = 0$ oder $B = 0$ gilt.

Beispiel 8B43. Der $\mathbb{Z}$-Modul $\mathbb{Z}/p$ ist unzerlegbar für jede Primzahl $p \in \mathbb{Z}$. Ebenso ist $\mathbb{Z}/p^k$ unzerlegbar für alle $k \in \mathbb{N}_{\geq 1}$. Hingegen ist $\mathbb{Z}/ab$ mit $a, b > 1$ und $\mathrm{ggT}(a,b) = 1$ zerlegbar: nach dem chinesischen Restsatz gilt nämlich $\mathbb{Z}/ab \cong \mathbb{Z}/a \times \mathbb{Z}/b$.

§8C. Quotientenmoduln und Isomorphiesätze

§8Ca. Quotientenmoduln. Sei R ein Ring, M ein Modul über R, und $U < M$ ein Untermodul. Für $x, y \in M$ definieren wir die *Kongruenz modulo* U, geschrieben $x \equiv y \pmod{U}$, durch die Bedingung $x - y \in U$.

Da U eine Untergruppe von $(M, +)$ ist, ist $\equiv$ eine Äquivalenzrelation.

Die *Äquivalenzklasse* $\mathfrak{cl}(x)$ eines Elementes $x \in M$ bezüglich der Kongruenz $\equiv$ ist die Menge aller zu x äquivalenten Elemente:

$$\mathfrak{cl}(x) := \{\, x' \in M \mid x' \equiv x \,\}$$

Es gilt $\mathfrak{cl}(x) = x + U$, denn $x' - x \in U$ ist gleichbedeutend mit $x' \in x + U$. Man nennt $x + U$ die *Nebenklasse* von x modulo U. Die *Quotientenmenge* ist die Menge aller Äquivalenzklassen:

$$M/U = \{\, \mathfrak{cl}(x) \mid x \in M \,\}.$$

Satz 8C1. *Sei R ein Ring, M ein Modul über R, und $U < M$ ein Untermodul. Dann existiert auf der Quotientenmenge M/U genau eine R-Modulstruktur, die die Projektion $\pi\colon M \to M/U$, $x \mapsto \mathfrak{cl}(x)$, zu einem R-Modulhomomorphismus macht.*

BEWEIS. Übung! □

Bemerkung 8C2. Das Nullelement von M/U ist $\mathfrak{cl}(0) = U$. Der Kern von $\pi\colon M \to M/U$ ist demnach U. Daraus folgt insbesondere:

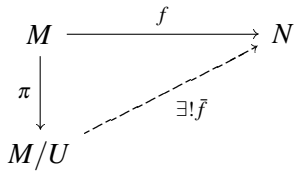
1. Jeder Untermodul $U \subset M$ tritt als Kern eines Modulhomomorphismus auf.
2. Für $U = \{0\}$ erhalten wir einen Isomorphismus $\pi\colon M \xrightarrow{\sim} M/\{0\}$.
3. Für $U = M$ ist der Quotient $M/M = \{\mathfrak{cl}(0)\}$ der Nullmodul.

§8Cb. Isomorphiesätze.

Satz 8C3 (Homomorphiesatz)**.** *Sei $U < M$ ein Untermodul und sei $\pi\colon M \to M/U$ die Projektion auf den Quotientenmodul. Für jeden Modulhomomorphismus $f\colon M \to N$ sind äquivalent:*

1. *Es gilt $U \subset \ker(f)$.*
2. *Es existiert ein Modulhomomorphismus $\bar{f}\colon M/U \to N$ sodass $f = \bar{f} \circ \pi$.*

In diesem Fall sagen wir, der Homomorphismus $f\colon M \to N$ *induziert* den Homomorphismus $\bar{f}\colon M/U \to N$ auf dem Quotienten M/U. Dieser Sachverhalt wird durch das folgende kommutative Diagramm veranschaulicht:



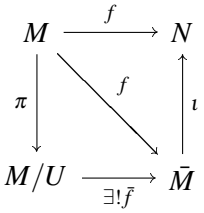
BEWEIS. Übung! □

Satz 8C4 (kanonische Faktorisierung)**.** *Jeder Modulhomomorphismus $f\colon M \to N$ mit Kern $U = \ker(f)$ und Bild $\bar{M} = f(M)$ faktorisiert gemäß*

$$f\colon M \xrightarrow{\pi} M/U \xrightarrow{\bar{f}} \bar{M} \xrightarrow{\iota} M$$

in die Projektion π, einen Isomorphismus $\bar{f}\colon M/U \xrightarrow{\sim} \bar{M}$, und die Inklusion ι.

Die Situation wird durch das folgende kommutative Diagramm veranschaulicht:



BEWEIS. Dies folgt aus dem Homomorphiesatz angewendet auf $U = \ker(f)$. □

Satz 8C5 (Isomorphiesatz)**.** *Sei $f\colon M \to N$ ein surjektiver Homomorphismus von R-Moduln.*

1. *Das Bild eines Untermoduls $U < M$ ist wieder ein Untermodul $f(U) < N$.*
2. *Das Urbild eines Untermoduls $V < N$ ist wieder ein Untermodul $f^{-1}(V) < M$.*

Diese Zuordnung stiftet eine Bijektion zwischen den Untermoduln U mit $\ker(f) < U < M$ und den Untermoduln $V < N$. Für diese induziert f einen Isomorphismus $M/U \cong N/f(U)$.

Für jeden Quotientenmodul $N = M/\mathfrak{m}$ und $\mathfrak{m} < U < M$ gilt $M/U \cong (M/\mathfrak{m}) \,/\, (U/\mathfrak{m})$.

BEWEIS. Übung! □

§8D. Basen und freie Moduln

§8Da. Basen. Sei M ein R-Modul und sei $X = (x_i)_{i\in I}$ eine Familie von Elementen $x_i \in M$.

Definition 8D1. Eine *R-Linearkombination* von X ist eine Summe der Form $x = \sum_{i\in I} a_i x_i$ mit Koeffizienten $a_i \in R$. Ist die Indexmenge I unendlich, so vereinbaren wir wie üblich, dass $a_i \neq 0$ nur für endlich viele $i \in I$ gilt (§2Ea).

Die Menge aller R-Linearkombination von X ist der von X erzeugte Untermodul $\langle X\rangle_R$.

Definition 8D2. Die Familie X heißt *Erzeugendensystem* von M über R wenn sich jedes Element $x \in M$ als eine R-Linearkombination $x = \sum_{i\in I} a_i x_i$ schreiben lässt.

Wir nennen M *endlich erzeugt*, wenn er ein endliches Erzeugendensystem zulässt.

Definition 8D3. Die Familie X heißt *linear unabhängig* über R wenn $\sum_{i\in I} a_i x_i = 0$ nur möglich ist falls $a_i = 0$ für alle $i \in I$.

Beispiel 8D4. Für den $\mathbb{Z}$-Modul $\mathbb{Z}$ ist $X = (3,5)$ ein Erzeugendensystem, denn $\mathbb{Z}3 + \mathbb{Z}5 = \mathbb{Z}$, aber nicht linear unabhängig, wie die Linearkombination $5\cdot 3 + (-3)\cdot 5 = 0$ zeigt.

Definition 8D5. Die Familie X heißt *Basis* von M über R, wenn sich jedes Element $x \in M$ eindeutig als R-Linearkombination $x = \sum_{i\in I} a_i x_i$ schreiben lässt.

Wir nennen M *frei über* R, wenn er eine Basis über R besitzt.

Beispiel 8D6. Der $\mathbb{Z}$-Modul $\mathbb{Z}$ ist frei: als Basis kommt sowohl 1 als auch -1 in Betracht. Für $n > 1$ ist der $\mathbb{Z}$-Modul $\mathbb{Z}/n$ hingegen nicht frei.

Beispiel 8D7. Über jedem Ring R ist der R-Modul R^n frei. Die Familie $(e_1,\dots,e_n)$ der Einheitsvektoren ist eine Basis, denn jedes Element $x = (x_1,\dots,x_n) \in R^n$ schreibt sich eindeutig als R-Linearkombination $x_1e_1 + \cdots + x_ne_n$. Wir nennen $(e_1,\dots,e_n)$ die *kanonische Basis* von R^n; der Modul R^n erlaubt daneben noch viele weitere Basen.

Beispiel 8D8. Der Polynomring $R[X]$ über einem kommutativen Ring R ist ein freier R-Modul: die Monome $X^0, X^1, X^2, \dots$ bilden eine Basis von $R[X]$ über R. Allgemeiner ist jeder Monoidring RM über R frei: Nach Definition 3G3 ist M eine Basis von RM über R.

Beispiel 8D9. Allgemeiner sei I eine beliebige Menge und sei $M = R^{(I)}$ der R-Modul aller Abbildungen $I \to R$ mit endlichem Träger. Dieser erlaubt als kanonische Basis die Familie $(e_i)_{i\in I}$ bestehend aus den Abbildungen $e_i\colon I \to K$ mit $e_i(i) = 1$ und $e_u(j) = 0$ für $i \neq j$. Jedes Element $x \in R^{(I)}$ schreibt sich eindeutig als (endliche) R-Linearkombination $x = \sum_{i\in I} x_i e_i$.

Proposition 8D10. *Sei M ein R-Modul. Für jede Familie $X = (x_i)_{i\in I}$ in M ist $\Phi_X\colon R^{(I)} \to M$ mit $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i x_i$ ein Modulhomomorphismus über R.*

- *X ist genau dann ein Erzeugendensystem über R, wenn Φ_X surjektiv ist.*
- *X ist genau dann linear unabhängig über R, wenn Φ_X injektiv ist.*
- *X ist genau dann eine Basis von M über R, wenn Φ_X bijektiv ist.*

Die Familie X ist genau dann eine Basis von M über R, wenn sie ein Erzeugendensystem von M und linear unabhängig über R ist. □

§**8Db. Lineare Abbildungen und Matrizen.** Sei R ein kommutativer Ring. Sei M ein freier R-Modul mit Basis $X = (x_1,\dots,x_m)$ und sei N ein freier R-Modul mit Basis $Y = (y_1,\dots,y_n)$. Dann können wir jedem R-Homomorphismus $f\colon M \to N$ wie folgt eine Matrix $A \in R^{n\times m}$ zuordnen. Für jedes $i = 1,\dots,m$ gilt

$$f(x_i) = \sum_{j=1}^{n} a_{ji} y_j$$

mit eindeutig bestimmten Koeffizienten $a_{ji} \in K$, und wir setzen $A = (a_{ji})_{ji}$.

Umgekehrt bestimmt die Matrix A die Abbildung f, denn man kann für jedes $x \in M$ das Bild $y = f(x)$ wie folgt berechnen. Es gilt $x = \sum_{i=1}^{m} \lambda_i x_i$ und somit

$$f\Big(\sum_{i=1}^{m} \lambda_i x_i\Big) = \sum_{i=1}^{m} \lambda_i f(x_i) = \sum_{i=1}^{m} \lambda_i \sum_{j=1}^{n} a_{ji} y_j = \sum_{j=1}^{n} \Big(\sum_{i=1}^{m} a_{ji} \lambda_i\Big) y_j$$

Demnach bildet f das Element $x = \sum_{i=1}^{m} \lambda_i x_i$ auf $y = \sum_{j=1}^{n} \mu_j y_j$ ab mit $\mu_j = \sum_{i=1}^{m} a_{ji} \lambda_i$. Für die Koeffizienten $\lambda \in K^m$ und $\mu \in R^n$ gilt also $\mu = A\lambda$ entsprechend unserer Definition der Matrixmultiplikation (7.2).

Diese Tatsache fassen wir in folgendem kommutativen Diagramm zusammen:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \Phi_X}\uparrow{\scriptstyle \cong} & & {\scriptstyle \Phi_Y}\uparrow{\scriptstyle \cong} \\ K^m & \xrightarrow[A]{} & K^n \end{array}$$

Die obige Konstruktion stiftet eine Bijektion $\Phi_X^Y \colon \operatorname{Hom}_R(M,N) \xrightarrow{\sim} R^{n \times m}$.

Proposition 8D11. *Die Bijektion Φ_X^Y überführt die Addition von R-Homomorphismen in die Addition von Matrizen, ist also ein Isomorphismen abelscher Gruppen.*

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \Phi_X}\uparrow{\scriptstyle \cong} & & {\scriptstyle \Phi_Y}\uparrow{\scriptstyle \cong} \\ K^m & \xrightarrow[A]{} & K^n \end{array} \quad \& \quad \begin{array}{ccc} M & \xrightarrow{g} & N \\ {\scriptstyle \Phi_X}\uparrow{\scriptstyle \cong} & & {\scriptstyle \Phi_Y}\uparrow{\scriptstyle \cong} \\ K^m & \xrightarrow[B]{} & K^n \end{array} \quad \Longrightarrow \quad \begin{array}{ccc} M & \xrightarrow{f+g} & N \\ {\scriptstyle \Phi_X}\uparrow{\scriptstyle \cong} & & {\scriptstyle \Phi_Y}\uparrow{\scriptstyle \cong} \\ K^m & \xrightarrow[A+B]{} & K^n \end{array}$$

BEWEIS. Geduldiges Nachrechnen. □

Die obige Konstruktion ist zudem mit der Komposition verträglich:

Proposition 8D12. *Seien M,N,P freie Moduln über R mit Basen X,Y,Z. Für alle $f \in \operatorname{Hom}_R(M,N)$ und $g \in \operatorname{Hom}_R(N,P)$ gilt dann $\Phi_X^Z(g \circ f) = \Phi_Y^Z(g)\Phi_X^Y(f)$.*

$$\begin{array}{ccccc} M & \xrightarrow{f} & N & \xrightarrow{g} & P \\ {\scriptstyle \Phi_X}\uparrow{\scriptstyle \cong} & & {\scriptstyle \Phi_Y}\uparrow{\scriptstyle \cong} & & {\scriptstyle \Phi_Z}\uparrow{\scriptstyle \cong} \\ K^m & \xrightarrow[A]{} & K^n & \xrightarrow[B]{} & K^p \end{array} \quad \Longrightarrow \quad \begin{array}{ccc} M & \xrightarrow{g\circ f} & P \\ {\scriptstyle \Phi_X}\uparrow{\scriptstyle \cong} & & {\scriptstyle \Phi_Z}\uparrow{\scriptstyle \cong} \\ K^m & \xrightarrow[BA]{} & K^p \end{array}$$

BEWEIS. Geduldiges Nachrechnen. □

Bemerkung 8D13. Die Ergebnisse dieses Abschnitts lassen sich so zusammenfassen:

- Freie R-Moduln sind genau die zu $R^{(I)}$ isomorphen R-Moduln, und die Wahl einer Basis entspricht der Wahl eines Isomorphismus.

- Die Homomorphismen zwischen freien R-Moduln mit endlichen Basen entsprechen Matrizen. Die Addition und Multiplikation von Homomorphismen entspricht dabei der Addition und Multiplikation von Matrizen.

Diese Übereinstimmung ist natürlich kein Zufall: Matrizen und die Struktur ihrer Addition und Multiplikation wurden gerade zu diesem Zweck erfunden!

§8E. Moduln über Hauptidealringen

Im Folgenden sei K ein Hauptidealring.

§8Ea. Freie Moduln. Als erstes widmen wir uns freien K-Moduln und beweisen die "Dimensionsinvarianz". Dass diese nicht selbstverständlich ist, zeigt bereits der Nullring $R = \{0\}$: hier ist R^n der Nullmodul für jedes $n \in \mathbb{N}$. Für Hauptidealringe verlangen wir ausdrücklich $1 \neq 0$, also ist diese Pathologie ausgeschlossen. Es gibt aber auch nicht-triviale Ringe R sodass $R^n \cong R^m$ für $n \neq m$ als R-Moduln isomorph sind, siehe Übung 8E4.

Satz 8E1. *Sei K ein Hauptidealring. Es existiert ein Isomorphismus $K^n \cong K^m$ von K-Moduln genau dann wenn $n = m$.*

BEWEIS. Da K nicht der Nullring ist, ist K^n nur für $n = 0$ der Nullmodul. Wir können also $n > m \geq 1$ annehmen. Bezüglich der kanonischen Basen stellen wir $f\colon K^n \xrightarrow{\sim} K^m$ dar als Matrix $A \in K^{m\times n}$. Der Algorithmus von Gauß-Bézout transformiert A in eine Diagonalmatrix $D = SAT$. Wegen $n > m$ besteht die letzte Spalte von D aus Nullen, also $De_n = 0$. Damit hat auch $A = S^{-1}DT^{-1}$ einen nicht-trivialen Kern, denn $\ker(A)$ enthält $Te_n \neq 0$, und somit ist A kein Isomorphismus. □

Korollar 8E2. *Sei K ein Hauptidealring, zum Beispiel ein Körper. Ist M ein freier K-Modul mit Basen $(a_1,\dots,a_n)$ und $(b_1,\dots,b_m)$, dann gilt $n = m$.* □

Dies erlaubt, den *Rang* von M zu definieren als die Kardinalität einer Basis, denn diese Kardinalität ist unabhängig von der gewählten Basis. Für dieses wichtige Konzept treffen wir allgemein folgende Vereinbarung:

Definition 8E3. Sei M ein freier R-Modul. Wenn je zwei Basen von M über R dieselbe Kardinalität haben, so nennen wir diese den *Rang* von M über R, geschrieben $\operatorname{rang}_R(M)$.

Wichtigster Spezialfall: Ist K ein Körper und M ein K-Vektorraum, dann nennt man den Rang üblicherweise *Dimension*, geschrieben $\dim_K(M)$.

Dass die "Dimensionsinvarianz" nicht selbstverständlich ist zeigt folgendes Beispiel:

Übung 8E4. Sei K ein Körper und $R = \operatorname{End}_K(K[X])$ der Ring der K-linearen Abbildungen $K[X] \to K[X]$. Man konstruiere einen Isomorphismus $R^2 \cong R$ von R-Linksmoduln.

Hinweis: Seien $f_0, f_1 \in R$ definiert durch $f_i(X^k) = X^{(k-i)/2}$ für $k-i$ gerade und $f_i(X^k) = 0$ sonst. Ist f_0, f_1 eine Basis von R über sich selbst? Kann man ebenso eine Basis von R mit beliebiger Länge $n \in \mathbb{N}_{\geq 1}$ herstellen?

Übung 8E5. Wir wollen zeigen, dass solche Pathologien über *kommutativen* Ringen nicht möglich sind. Sei hierzu R ein kommutativer Ring mit $1 \neq 0$ und sei $I \lhd R$ ein Ideal.

1. In jedem R-Modul M ist $IM := \{\sum_{k=1}^n a_k x_k \mid a_k \in I, x_k \in M\}$ ein Untermodul.

2. Wir wissen, dass M/IM ein Modul über R ist. Man zeige, dass M/IM auch ein Modul über R/I wird, wenn man $(r+I)(x+IM) := (rx+IM)$ definiert.
3. Im Fall $M = R^n$ konstruiere man einen Isomorphismus $R^n/IR^n \cong (R/I)^n$.
4. Aus einem Isomorphismus $R^m \cong R^n$ von R-Moduln folgt die Gleichheit $m = n$.

Man benutze hierzu, dass jeder kommutative Ring mit $1 \neq 0$ ein maximales Ideal $I \lhd R$ besitzt (5G12). Der Quotientenring R/I ist dann ein Körper.

§**8Eb. Untermoduln freier Moduln.** Über beliebigen Ringen können Untermoduln von freien Moduln erstaunlich kompliziert sein:

- Untermoduln eines freien Moduls sind nicht notwendig frei (Übung 8G1).
- Wenn ein Untermodul U eines freien Moduls M selbst wieder frei ist, dann muss nicht unbedingt $\operatorname{rang} U \leq \operatorname{rang} M$ gelten (Übung 8G2).

Über Hauptidealringen ist die Situation jedoch sehr übersichtlich:

Satz 8E6. *Sei K ein Hauptidealring. Jeder K-Untermodul $U < K^m$ ist frei und erfüllt* $\operatorname{rang}_K(U) \leq m$.

BEWEIS. Wir führen Induktion über m. Für $m = 0$ ist nichts zu zeigen, da $K^0 = \{0\}$.

Für $m = 1$ ist $K^1 \cong K$ und $U \subset K$ ist ein Ideal. Da wir K als Hauptidealring voraussetzen, gilt $U = Ka$ für ein Element $a \in K$. Für $a = 0$ ist $U = \{0\}$ und $\operatorname{rang}_K(U) = 0$. Für $a \neq 0$ ist $U = Ka$ frei mit Basis a und $\operatorname{rang}_K(U) = 1$.

Für $m \geq 2$ definieren wir die Projektion $p\colon K^m \to K$ durch $(x_1,\dots,x_m) \mapsto x_m$ und identifizieren K^{m-1} mit $\ker(p) = K^{m-1} \times \{0\}$ vermöge $(x_1,\dots,x_{m-1}) \mapsto (x_1,\dots,x_{m-1},0)$.

Der K-Untermodul $U_0 = \ker(p|_U) = U \cap K^{m-1}$ von K^{m-1} ist nach Induktionsvoraussetzung frei und erlaubt eine Basis $u_1,\dots,u_{n-1} \in U_0$ der Länge $n-1 \leq m-1$. Das Bild $p(U) < K$ ist wie im Fall $m = 1$ gesehen ebenfalls frei. Im Fall $p(U) = \{0\}$ gilt $U_0 = U$ und wir sind fertig. Im Fall $p(U) = Ka$ mit $a \in K^*$ wählen wir ein Urbild $u_n \in U$, $p(u_n) = a$, und zeigen, dass $u_1,\dots,u_{n-1},u_n$ eine Basis von U ist.

Die Familie $(u_1,\dots,u_{n-1},u_n)$ erzeugt U: Zu $u \in U$ gilt $p(u) = \lambda_n a$ mit $\lambda_n \in K$. Daher gilt $p(u - \lambda_n u_n) = 0$ und somit liegt $u - \lambda_n u_n$ in U_0. Nach Induktionsvoraussetzung gilt $u - \lambda_n u_n = \lambda_1 u_1 + \cdots + \lambda_{n-1} u_{n-1}$ für geeignete $\lambda_1,\dots,\lambda_{n-1} \in K$, denn $u_1,\dots,u_{n-1}$ erzeugt U_0.

Die Familie $(u_1,\dots,u_{n-1},u_n)$ ist K-linear unabhängig: Sei $\lambda_1 u_1 + \cdots + \lambda_{n-1} u_{n-1} + \lambda_n u_n = 0$. Die Projektion p ergibt dann $\lambda_n a = 0$, wegen $a \neq 0$ also $\lambda_n = 0$. Nach Induktionsvoraussetzung folgt aus $\lambda_1 u_1 + \cdots + \lambda_{n-1} u_{n-1} = 0$ schließlich $\lambda_1 = \cdots = \lambda_{n-1} = 0$, denn $u_1,\dots,u_{n-1}$ ist K-linear unabhängig. □

Korollar 8E7. *Sei M ein endlich erzeugter K-Modul. Dann ist auch jeder Untermodul $U < M$ über K endlich erzeugt.*

BEWEIS. Wird der Modul M über K von $x_1,\dots,x_m$ erzeugt, dann erhalten wir einen surjektiven K-Homomorphismus $f\colon K^m \twoheadrightarrow M$ wie in 8D10. Das Urbild $V := f^{-1}(U)$ ist nach Satz 8E6 frei vom Rang $n \leq m$. Also existiert $g\colon K^n \xrightarrow{\sim} V$ und somit $f \circ g\colon K^n \twoheadrightarrow U$. □

Auch diese Eigenschaft gilt nicht für beliebige Ringe, siehe Übung 8G3.

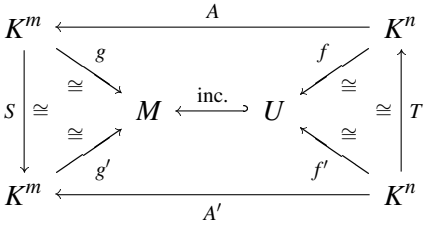
§**8Ec. Der Elementarteilersatz.**

Satz 8E8. *Sei K ein Hauptidealring und sei M ein freier K-Modul vom Rang m. Für jeden Untermodul $U \subset M$ existiert*

1. *eine Basis $b_1, b_2, \dots, b_m$ von M sowie*
2. *Elemente $a_1, a_2, \dots, a_n \in K^*$ mit $a_1 \mid a_2 \mid \cdots \mid a_n$*

sodass $a_1 b_1, a_2 b_2, \dots, a_n b_n$ eine Basis von U ist. Die Elemente $a_1, a_2, \dots, a_n$ sind dabei (bis auf Assoziierte) eindeutig durch U bestimmt und heißen die Elementarteiler *des Untermoduls $U < M$.*

BEWEIS. *Existenz:* Nach Voraussetzung erlaubt M eine Basis $v_1, \dots, v_m$ und damit einen Isomorphismus $g\colon K^m \xrightarrow{\sim} M$. Der Satz 8E6 beschert uns eine Basis $u_1, \dots, u_n$ von U und somit einen Isomorphismus $f\colon K^n \xrightarrow{\sim} U$. Sei $A \in K^{m\times n}$ die Matrix, die die Inklusion $U \hookrightarrow M$ bezüglich der Basen $u_1, \dots, u_n$ und $v_1, \dots, v_m$ darstellt.



Der Algorithmus von Gauß-Bézout (oder der Elementarteilersatz 7A2) liefert die Diagonalteilerform $A' = SAT$ mittels geeigneter Transformationsmatrizen $S \in \mathrm{SL}_m(K)$ und $T \in \mathrm{SL}_m(K)$. Seien $a_1, \dots, a_r$ die Diagonalelemente von A'. Wir erhalten so neue Isomorphismen $f' = f \circ T\colon K^n \xrightarrow{\sim} U$ und $g' = g \circ S^{-1}\colon K^m \xrightarrow{\sim} M$. Demnach bilden $b_1, \dots, b_m \in M$ mit $b_k = g'(e_k)$ eine Basis von M, und schließlich bilden $a_1 b_1, \dots, a_n b_n$ eine Basis von U, denn $f'(e_k) = g'(A' e_k) = g'(a_k e_k) = a_k g'(e_k) = a_k b_k$.

Eindeutigkeit: Wir betrachten erneut das obige kommutative Diagramm.

Sei $b_1, b_2, \dots, b_m$ eine Basis von M sowie $a_1, a_2, \dots, a_n \in K$ mit $a_1 \mid a_2 \mid \cdots \mid a_n$ sodass $a_1 b_1, a_2 b_2, \dots, a_n b_n$ eine Basis von U ist. Dies definiert $g\colon K^m \xrightarrow{\sim} M$ und $f\colon K^n \xrightarrow{\sim} U$ sowie eine Elementarteilermatrix $A \in K^{m\times n}$ mit Diagonalelementen $a_1, a_2, \dots, a_n$.

Sei $b'_1, b'_2, \dots, b'_m$ eine weitere Basis von M sowie $a'_1, a'_2, \dots, a'_n \in K$ mit $a'_1 \mid a'_2 \mid \cdots \mid a'_n$ sodass $a'_1 b'_1, a'_2 b'_2, \dots, a'_n b'_n$ eine Basis von U ist. Dies definiert $g'\colon K^m \xrightarrow{\sim} M$ und $f'\colon K^n \xrightarrow{\sim} U$ sowie eine Elementarteilermatrix $A' \in K^{m\times n}$ mit Diagonalelementen $a'_1, a'_2, \dots, a'_n$.

Nach Konstruktion definiert $g'^{-1} \circ g$ eine Matrix $S \in \mathrm{GL}_m(K)$ und $f^{-1} \circ f$ eine Matrix $T \in \mathrm{GL}_m(K)$ sodass $A' = SAT$ gilt. Aufgrund der Eindeutigkeit der Elementarteiler (Satz 7A2) gilt dann $a_k \sim a'_k$ für alle $k = 1, \dots, n$. □

Korollar 8E9. *Sei M ein freier K-Modul vom Rang m und seien $U, U' < M$ zwei Untermoduln. Dann existiert genau dann ein Automorphismus $f\colon M \xrightarrow{\sim} M$ mit $f(U) = U'$ wenn die Elementarteiler von U und U' übereinstimmen.* □

§**8Ed. Zerlegung in Elementarteiler.** Wir schließen mit folgender Klassifikation der endlich erzeugten Moduln über Hauptidealringen.

Satz 8E10. *Sei K ein Hauptidealring. Zu jedem endlich erzeugten K-Modul M existiert ein K-Isomorphismus*

$$M \cong K/(a_1) \times K/(a_2) \times \cdots \times K/(a_n) \times K^r$$

wobei $r \in \mathbb{N}$ und $a_1, a_2, \ldots, a_n \in K^* \smallsetminus K^\times$ mit $a_1 \mid a_2 \mid \cdots \mid a_n$. Hierbei sind die Zahl r und die Ideale $(a_1) \supset (a_2) \supset \cdots \supset (a_n)$ eindeutig durch M bestimmt. Anders gesagt,

$$K/(a_1) \times \cdots \times K/(a_n) \times K^r \cong K/(b_1) \times \cdots \times K/(b_m) \times K^s$$

gilt genau dann wenn $r = s$ und $n = m$ sowie $(a_k) = (b_k)$ für alle $k = 1, \ldots, n$ gilt.

BEWEIS. *Existenz:* Nach Voraussetzung existiert ein Erzeugendensystem $v_1, \ldots, v_m$ von M über K, und somit ein surjektiver K-Homomorphismus $g\colon K^m \twoheadrightarrow M$. Der Isomorphiesatz induziert $\bar{g}\colon K^m/\ker(g) \xrightarrow{\sim} M$. Nach dem Elementarteilersatz 8E8 existiert eine Basis $b_1, b_2, \ldots, b_m$ von K^m sowie Elemente $a_1, a_2, \ldots, a_n \in K^*$ mit $a_1 \mid a_2 \mid \cdots \mid a_n$ sodass $a_1 b_1, a_2 b_2, \ldots, a_n b_n$ eine Basis von $\ker(g)$ ist.

Durch Basiswechsel erhalten wir einen surjektiven K-Homomorphismus $f\colon K^m \twoheadrightarrow M$ mit $\ker(f) = \langle a_1 e_1, a_2 e_2, \ldots, a_n e_n \rangle_K$. Der Isomorphiesatz induziert nun

$$\bar{f}\colon K^m/\ker(f) \xrightarrow{\sim} M.$$

und Dank der besonders einfachen Form von $\ker(f)$ erhalten wir

$$K^m/\ker(f) = K/(a_1) \times K/(a_2) \times \cdots \times K/(a_n) \times K^r.$$

Im Falle $a_1 \in K^\times$ gilt $(a_1) = K$ und $K/(a_1)$ ist der Nullmodul. Indem wir alle Elemente $a_k \sim 1$ weglassen erhalten wir die gewünschte Darstellung.

Eindeutigkeit: Wenn man v_{m+1} zum Erzeugendensystem $(v_1, \ldots, v_m)$ hinzufügt, dann erweitert man K^m zu K^{m+1} aber auch den Kern um eine Relation $v_{m+1} = \sum_{i=1}^m \lambda_i v_i$. Die Elementarteiler ändern sich durch eine zusätzliche 1, was das obige Resultat nicht ändert.

Daher sind die Elementarteiler unabhängig von der Wahl des Erzeugendensystems: Sind $(v_1, \ldots, v_m)$ et $(v'_1, \ldots, v'_{m'})$ zwei Erzeugendensysteme, dann auch $(v_1, \ldots, v_m, v'_1, \ldots, v'_{m'})$, und alle drei führen zu denselben Elementarteilern. □

Definition 8E11. In obiger Situation nennt man $a_1, a_2, \ldots, a_n \in K$ die *Elementarteiler* des K-Moduls M und man nennt r den *Rang des freien Anteils*.

Korollar 8E12. *Über einem Hauptidealring K zerlegt sich jeder endlich erzeugte K-Modul M gemäß $M = T \oplus F$ in den Torsionsmodul $T < M$ und einen freien Modul $F < M$.* □

Der Torsionsuntermodul $T < M$ ist eindeutig durch M bestimmt (§8Bd), hier durch

$$T = \ker(M \xrightarrow{\cdot a_n} M),$$

und zerlegt sich in ein Produkt zyklischer Moduln $T \cong K/(a_1) \times K/(a_2) \times \cdots \times K/(a_n)$ wie oben. Zudem existiert ein freier Untermodul $F < M$ sodass $M = T \oplus F$ gilt.

Der Rang des freien Untermoduls F ist eindeutig durch M bestimmt.

Warnung. — Der Untermodul $F < M$ ist nicht eindeutig bestimmt:

Beispiel 8E13. Im $\mathbb{Z}$-Modul $M = \mathbb{Z} \times \mathbb{Z}/2$ gilt $T = \{0\} \times \mathbb{Z}/2$. Offenbar erfüllt der freie Untermodul $F = \mathbb{Z} \times \{0\}$ die Bedingung $T = F \oplus T$. Dies gilt aber auch für $F' = \mathbb{Z}(1, \bar{1})$.

Als Spezialfall erhalten erhalten wir die Klassifikation 8A1 endlicher abelscher Gruppen.

Beispiel 8E14. Als Anwendung hier die Liste der abelschen Gruppen der Ordnung ≤ 12:

- Ordnung 1: $\mathbb{Z}/_1$;
- Ordnung 2: $\mathbb{Z}/_2$;
- Ordnung 3: $\mathbb{Z}/_3$;
- Ordnung 4: $\mathbb{Z}/_4$, $\mathbb{Z}/_2 \times \mathbb{Z}/_2$;
- Ordnung 5: $\mathbb{Z}/_5$;
- Ordnung 6: $\mathbb{Z}/_6$;
- Ordnung 7: $\mathbb{Z}/_7$;
- Ordnung 8: $\mathbb{Z}/_8$, $\mathbb{Z}/_2 \times \mathbb{Z}/_4$, $\mathbb{Z}/_2 \times \mathbb{Z}/_2 \times \mathbb{Z}/_2$;
- Ordnung 9: $\mathbb{Z}/_9$;
- Ordnung 10: $\mathbb{Z}/_{10}$;
- Ordnung 11: $\mathbb{Z}/_{11}$;
- Ordnung 12: $\mathbb{Z}/_{12}$, $\mathbb{Z}/_2 \times \mathbb{Z}/_6$.

Satz 8E10 garantiert hierbei, dass die Liste vollständig und redundanzfrei ist. Das bedeutet, zu jeder abelschen Gruppe A der Ordnung ≤ 12 enthält unsere Liste genau ein zu A isomorphes Modell.

Übung 8E15. Die Gruppen $\mathbb{Z}/_5^\times$ und $\mathbb{Z}/_8^\times$ und $\mathbb{Z}/_{12}^\times$ sind alle der Ordnung 4. Für jede finde man jeweils die isomorphe Gruppe in unserer Liste. Wo findet sich die Gruppe $\mathbb{Z}/_{13}^\times$ der Ordnung 12?

§**8Ee. Zerlegung in unzerlegbare Moduln.** Ein zyklischer Modul K/a lässt sich unter Umständen noch weiter zerlegen: Ist $a = p_1^{n_1} \cdots p_\ell^{n_\ell}$ die Zerlegung von a in paarweise verschiedene Primfaktoren $p_1, \ldots, p_\ell \in K$, dann gilt nach dem chinesischen Restsatz (§3F)

$$K/p_1^{n_1} \cdots p_\ell^{n_\ell} \cong K/p_1^{n_1} \times \cdots \times K/p_\ell^{n_\ell}.$$

Aus dem Elementarteilersatz 8E10 folgt:

Proposition 8E16. *Über einem Hauptidealring K ist ein K-Modul M genau dann unzerlegbar, wenn $M \cong K/p^n$ für ein Primelement $p \in K$ und $n \geq 1$ gilt.* □

Satz 8E17 (Zerlegung in unzerlegbare Moduln)**.** *Über einem Hauptidealring K ist jeder endlich erzeugte Modul M isomorph zu*

$$\begin{aligned} K^r &\times K/p_1^{n_{1,1}} \times K/p_1^{n_{1,2}} \times \cdots \times K/p_1^{n_{1,k_1}} \\ &\times K/p_2^{n_{2,1}} \times K/p_2^{n_{2,2}} \times \cdots \times K/p_2^{n_{2,k_2}} \\ &\vdots \\ &\times K/p_\ell^{n_{\ell,1}} \times K/p_\ell^{n_{\ell,2}} \times \cdots \times K/p_\ell^{n_{\ell,k_\ell}}. \end{aligned}$$

Hierbei ist $r \geq 0$ der Rang des freien Anteils, $p_1, p_2, \ldots, p_\ell \in K$ sind paarweise verschiedene Primelemente, und die Exponenten erfüllen $1 \leq n_{i,1} \leq n_{i,2} \leq \cdots \leq n_{i,k_i}$. Diese Darstellung ist eindeutig bis auf Umordnung und Assoziierte der Primelemente $p_1, p_2, \ldots, p_\ell$. □

Übung 8E18. Man führe die Liste aus Beispiel 8E14 für alle abelschen Gruppen der Ordnung ≤ 32 fort (oder auch noch weiter).

Übung 8E19. Man bestimme alle abelschen Gruppen der Ordnung 8000 bis auf Isomorphie.

Übung 8E20. Man formuliere und beweise, in welchem Sinne die Zerlegung 8E17 maximal ist. Man formuliere und beweise, in welchem Sinne die Zerlegung 8E10 minimal ist.

§8F. Vektorräume

§8Fa. Charakterisierung von Basen über einem Körper.

Proposition 8F1. *Sei V ein K-Vektorraum. Für jede Familie $X = (x_i)_{i\in I}$ in M sind äquivalent:*

- *X ist eine Basis von V über K.*
- *X ist ein minimales Erzeugendensystem von V über K.*
- *X ist eine maximale K-linear unabhängige Familie in V.*

BEWEIS. Offenbar gilt "(1) $\Rightarrow$ (2)" sowie "(1) $\Rightarrow$ (3)" für jeden Modul V über jedem Ring K: Ist $X = (x_i)_{i\in I}$ eine Basis, dann ist X auch eine maximale K-linear unabhängige Familie: Jedes $v \in V$ ist Linearkombination von $(x_i)_{i\in I}$, also ist $X \cup \{v\}$ linear abhängig.

Ebenso ist jede Basis $X = (x_i)_{i\in I}$ ein minimales Erzeugendensystem von V über K, denn $(x_i)_{i\in I\smallsetminus\{j\}}$ ist kein Erzeugendensystem: Wäre x_j Linearkombination von $(x_i)_{i\in I\smallsetminus\{j\}}$, dann wäre X nicht linear unabhängig.

"(2) $\Rightarrow$ (1)": Ist $X = (x_i)_{i\in I}$ linear abhängig, dann gibt es eine Linearkombination $\sum_{i\in I} a_i x_i = 0$ wobei $a_j \neq 0$ für mindestens ein $j \in I$. Dann ist a_j invertierbar, da wir über einem Körper arbeiten, und somit $x_j = \sum_{i\in I\smallsetminus\{j\}}(-a_j^{-1}a_i)x_i$. Damit ist auch $(x_i)_{i\in I\smallsetminus\{j\}}$ ein Erzeugendensystem. Jedes minimale Erzeugendensystem ist demnach auch linear unabhängig.

"(3) $\Rightarrow$ (1)": Für jedes $v \in V$ ist $X \cup \{v\}$ linear abhängig, da X maximal ist. Also gibt es eine nicht-triviale Linearkombination $\sum_{i\in I} a_i x_i + av = 0$. Wäre $a = 0$, dann auch $a_i = 0$ für alle $i \in I$, denn X ist linear unabhängig. Also gilt $a \neq 0$, und somit ist a invertierbar, da wir über einem Körper arbeiten. Es folgt $v = \sum_{i\in I}(-a^{-1}a_i)x_i$, also ist X ein Erzeugendensystem. □

Bemerkung 8F2. Über einem Ring gelten diese Charakterisierungen nicht mehr. Im Modul $\mathbb{Z}$ über dem Ring $\mathbb{Z}$ ist zum Beispiel $\{3,5\}$ ein minimales Erzeugendensystem aber nicht linear unabhängig. Andererseits ist $\{3\}$ eine maximale $\mathbb{Z}$-linear unabhängige Familie in $\mathbb{Z}$ aber kein Erzeugendensystem von $\mathbb{Z}$.

§8Fb. Vektorräume über einem Körper K.

Satz 8F3. *Jeder Vektorraum V über einem Körper K ist frei, das heißt, es existiert eine Basis von V über K.*

Aufgrund der Dimensionsinvarianz (8E1) wissen wir zudem, dass je zwei Basen von V dieselbe Kardinalität haben: Diese nennen wir die Dimension von V, geschrieben $\dim_K(V)$.

Die Dimensionsinvarianz gilt auch für unendliche Basen; wir begnügen uns hier mit folgender Feststellung: Wenn eine Basis von V endlich ist, dann ist jede Basis von V endlich.

BEWEIS. Ist V endlich erzeugt, so folgt der Satz aus dem Elementarteilersatz 8E10.

Ist V nicht endlich erzeugt, so behilft man sich mit dem Zornschen Lemma. Der folgende elegante Beweis ist einfacher als der Satz 8E10 aber im Gegensatz zu diesem nicht konstruktiv, das heißt, er gibt keinen Hinweis zur Konstruktion der gesuchten Basis.

Wir nennen eine Teilmenge $X \subset V$ linear unabhängig, wenn die Familie $X = (x)_{x\in X}$ linear unabhängig ist. Sei S die Menge aller linear unabhängigen Teilmengen $X \subset V$. Diese ist nicht-leer, wegen $\emptyset \in S$, und durch Inklusion geordnet. Zu jeder Kette $T \subset S$ ist $Y := \bigcup_{X\in T} X$ linear unabhängig: Für jede Linearkombination $\sum_{x\in Y} a_x \cdot x = 0$ ist nach Definition der Träger $\operatorname{supp}(a)$ endlich, also in einem $X \in T$ enthalten. Da X linear unabhängig ist, gilt $a_x = 0$ für alle x. Das zeigt, dass auch Y linear unabhängig ist. Demnach ist Y in S eine obere Schranke der Kette T. Das Zornsche Lemma versichert uns nun die Existenz eines maximalen Elements in S. Nach 8F1 ist jede maximale linear unabhängige Teilmenge von V eine Basis von V. □

§8Fc. Die Dimensionsformel.

Satz 8F4. *Seien $K \subset L \subset M$ Ringe. Angenommen L ist ein freier K-Modul mit Basis $(a_i)_{i\in I}$ über K, und M ist ein freier L-Modul mit Basis $(b_j)_{j\in J}$ über L. Dann ist M ein freier K-Modul mit Basis $(a_i b_j)_{(i,j)\in I\times J}$.*

BEWEIS. *Die Familie $(a_i b_j)_{(i,j)\in I\times J}$ ist ein Erzeugendensystem:* Jedes Element $x \in M$ schreibt sich als $x = \sum_{j\in J} \lambda_j b_j$ mit $\lambda_j \in L$. Jedes λ_j schreibt sich als $\lambda_j = \sum_{i\in I} \mu_{ij} a_i$ mit $\mu_{ij} \in K$. Also gilt $x = \sum_{j\in J}(\sum_{i\in I} \mu_{ij} a_i) b_j = \sum_{(i,j)\in I\times J} \mu_{ij}(a_i b_j)$.

Die Familie $(a_i b_j)_{(i,j)\in I\times J}$ ist K-linear unabhängig: Aus $\sum_{(i,j)\in I\times J} \mu_{ij}(a_i b_j) = 0$ folgt $\sum_{j\in J}(\sum_{i\in I} \mu_{ij} a_i) b_j = 0$. Da $(b_j)_{j\in J}$ linear unabhängig über L ist, folgt $\sum_{i\in I} \mu_{ij} a_i = 0$ für alle $j \in J$. Da $(a_i)_{i\in I}$ linear unabhängig über K ist, folgt hieraus $\mu_{ij} = 0$ für alle $i \in I$. □

Korollar 8F5. *Sind $K \subset L \subset M$ Körper, dann ist L ein Vektorraum über K, und M ist ein Vektorraum sowohl über L als auch über K. Für die Dimensionen gilt*

$$\dim_K(M) = \dim_K(L) \cdot \dim_L(M).$$

BEWEIS. Für endliche Dimension folgt dies aus dem vorangegangenen Satz denn es gilt $\dim_K(L) = |I|$ und $\dim_L(M) = |J|$ sowie $\dim_K(M) = |I \times J| = |I| \cdot |J|$. Dies gilt auch noch im Falle unendlicher Dimensionen, wenn wir die obige Gleichung für Kardinalzahlen auffassen, oder schlicht die Konvention $\infty \cdot a = a \cdot \infty = \infty$ vereinbaren. □

Notation. Für Körpererweiterungen $K \subset L$ nennen wir die Dimension $\dim_K(L)$ auch den *Grad* von L über K, geschrieben $[L : K]$. Die Dimensionsformel schreibt sich dann suggestiver in der Form

$$[M : K] = [M : L] \cdot [L : K].$$

§8Fd. Normalformen von Endomorphismen eines Vektorraums.

Sei K ein Körper und sei $P = X^n + p_{n-1}X^{n-1} + \cdots + p_0$ ein Polynom in $K[X]$. Den $K[X]$-Modul $U = K[X]/(P)$ können wir vermöge $K \subset K[X]$ als K-Vektorraum auffassen. Die Multiplikation mit X definiert eine K-lineare Abbildung $\varphi\colon U \to U$.

Übung 8F6. Man zeige $\dim_K(U) = n$. Man zeige, dass sich φ bezüglich der Basis $(1, X, \ldots, X^{n-1})$ darstellt als die Matrix

$$B = \begin{pmatrix} 0 & 0 & 0 & -a_0 \\ 1 & 0 & 0 & -a_1 \\ & \ddots & 0 & \vdots \\ 0 & & 1 & -a_{n-1} \end{pmatrix}.$$

Eine solche Matrix heißt *Begleitmatrix* von P oder *rationale Normalform* von φ.

Man bestimme das charakteristische Polynom $\det(X 1_{n\times n} - B)$ der Matrix B.

Übung 8F7. Sei nun speziell $P = (X-a)^n$. Man bestimme eine Basis von U über K, bezüglich der sich φ darstellt als die Matrix

$$J = \begin{pmatrix} a & 0 & 0 & 0 \\ 1 & \ddots & 0 & 0 \\ 0 & \ddots & \ddots & 0 \\ 0 & 0 & 1 & a \end{pmatrix}.$$

Eine solche Matrix heißt *Jordanblock* oder *Jordan–Normalform* von φ.

Sei nun V ein K-Vektorraum mit $\dim_K(V) < \infty$. Gegeben sei eine K-lineare Abbildung $\varphi \in \mathrm{End}_K(V)$. Hierdurch wird V zu einem $K[X]$-Modul mit der Operation $K[X] \times V \to V$ gegeben durch $(P, v) \mapsto P(\varphi)(v)$.

Der Elementarteilersatz beschert uns nun einen $K[X]$-Modulisomorphismus

$$V \cong K[X]/(P_1) \times \cdots \times K[X]/(P_m) \tag{8.1}$$

wobei $P_1, \ldots, P_m$ normierte Polynome in $K[X]$ sind mit $P_1 \mid \cdots \mid P_m$.

Übung 8F8. Man folgere hieraus, dass es eine K-Basis von V gibt, bezüglich der sich φ darstellt als eine Blockdiagonalmatrix

$$\begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_m \end{pmatrix}.$$

wobei die Matrizen $B_1, \ldots, B_m$ in rationaler Normalform sind.

Man bestimme das charakterische Polynom von φ.

Mittels des chinesischen Restsatzes erhalten wir aus (8.1) einen $K[X]$-Modulisomorphismus $V \cong K[X]/(Q_1) \times \cdots \times K[X]/(Q_r)$, wobei jedes Q_i Potenz eines normierten irreduziblen Polynoms in K[X] ist. Dabei ist $Q_1 \cdots Q_r$ das charakteristische Polynom von φ.

Übung 8F9. Nehmen wir an, dass das charakteristische Polynom von φ über K in Linearfaktoren zerfällt. (Zum Beispiel ist dies immer der Fall für $K = \mathbb{C}$.) Man zeige, dass es eine K-Basis von V gibt, bezüglich der sich φ darstellt als eine Blockdiagonalmatrix

$$\begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_m \end{pmatrix}.$$

wobei die Matrizen $J_1, \ldots, J_m$ Jordanblöcke sind.

Übung 8F10. Sei R ein Ring und M ein R-Linksmodul. Man zeige, dass der Annihilator

$$\mathrm{ann}_R(M) := \{\, r \in R : rm = 0 \text{ für alle } m \in M \,\}$$

ein Linksideal in R ist. Man bestimme zum Beispiel $\mathrm{ann}_{\mathbb{Z}}(\mathbb{Z}/3 \times \mathbb{Z}/6)$.

Übung 8F11. Man zeige, dass in (8.1) $\operatorname{ann}_{K[X]}(V) = (P_m)$ gilt.
Damit ist P_m das Minimalpolynom von φ.

§8G. Beispiele, Anwendungen, Übungen

§**8Ga. Diverse Gegenbeispiele.** Die folgenden Übungen führen diverse Gegenbeispiele aus, die die Ergebnisse dieses Kapitels illustrieren und abgrenzen.

Übung 8G1. Sei K ein Körper und sei $R = K[X,Y]$ der Polynomring in den Variablen X,Y. Als R-Modul ist R frei mit Basis 1. Das Ideal (X,Y) ist als R-Untermodul nicht frei. Es gilt übrigens $(X,Y) = \ker(\varepsilon)$, wobei $\varepsilon\colon K[X,Y] \to K$ die Augmentation ist (3G10).

Übung 8G2. Sei $M = \{X,Y\}^*$ das freie Monoid bestehend aus allen Wörtern über dem Alphabet $\{X,Y\}$. Sei K ein Körper und sei $R = KM$ der nicht-kommutative Polynomring in den Variablen X,Y. Als R-Linksmodul ist R frei mit Basis 1. Der Untermodul RX ist frei mit Basis X; er besteht aus den R-Linearkombinationen von Monomen die mit dem Buchstaben X enden. Entsprechendes gilt für den Untermodul RY. Daraus folgt $RX \cap RY = \{0\}$. Der Untermodul $RX \oplus RY$ ist demnach frei vom Rang 2.

Übung 8G3. Sei $R = K[X_n \mid n \in \mathbb{N}]$ der Polynomring über einem Körper K in unendlich vielen Variablen $X_0, X_1, X_2, \ldots$. Als R-Modul ist R frei vom Rang 1, also insbesondere endlich erzeugt. Das Ideal $(X_n \mid n \in \mathbb{N})$ ist als R-Untermodul nicht endlich erzeugt. Es gilt übrigens $(X_n \mid n \in \mathbb{N}) = \ker(\varepsilon)$, wobei $\varepsilon\colon R \to K$ die Augmentation ist (3G10).

TEIL II

Grundlagen der Gruppentheorie

KAPITEL 9

Grundbegriffe der Gruppentheorie

§9A. Der Satz von Lagrange

§**9Aa. Nebenklassen.** Vor der allgemeinen Konstruktion betrachten wir als einführendes Beispiel die Gruppe $(\mathbb{Z},+)$ der ganzen Zahlen mit ihrer Addition. Darin ist die Menge $H = \{\dots,-6,-3,0,3,6,\dots\}$ aller ganzzahligen Vielfachen von 3 eine Untergruppe. Die Menge der ganzen Zahlen zerfällt in genau 3 Nebenklassen:

$$0+H = \{\dots,-6,-3,0,3,6,\dots\}$$
$$1+H = \{\dots,-5,-2,1,4,7,\dots\}$$
$$2+H = \{\dots,-4,-1,2,5,8,\dots\}$$

Diese Nebenklassen $r+H$ sind gerade die Restklassen modulo 3: In einer gemeinsamen Zeile stehen jeweils die Zahlen, die beim Teilen durch 3 den gleichen Rest lassen. Die Tabelle enthält alle ganzen Zahlen, wobei jede Zahl genau einmal vorkommt.

Da $(\mathbb{Z},+)$ abelsch ist, stimmen die Linksnebenklasse $r+H$ und die Rechtsnebenklasse $H+r$ überein. In einer nicht-abelschen Gruppe muss man Links- und Rechtsnebenklasse unterscheiden. Die nötigen allgemeinen Begriffe wollen wir nun ausführen.

§**9Ab. Linksnebenklassen.** Sei $(G,\cdot,1)$ eine Gruppe. Wir erinnern zunächst daran, dass eine Teilmenge $H \subset G$ eine *Untergruppe* ist, wenn gilt:

- $1 \in H$
- $x \in H \Rightarrow x^{-1} \in H$
- $x,y \in H \Rightarrow xy \in H$

Für $a,b \in G$ definieren wir $a \sim b$ durch $a^{-1}b \in H$. Dies ist eine Äquivalenzrelation:

- *Reflexivität:* Es gilt $a \sim a$ denn $a^{-1}a = 1 \in H$.
- *Symmetrie:* Aus $a \sim b$ folgt $b \sim a$, denn aus $a^{-1}b \in H$ folgt $(a^{-1}b)^{-1} = b^{-1}a \in H$.
- *Transitivität:* Aus $a \sim b$ und $b \sim c$ folgt $a \sim c$, denn aus $a^{-1}b \in H$ und $b^{-1}c \in H$ folgt $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$.

Die Äquivalenzklasse eines Elementes $a \in G$ bezüglich $\sim$ ist die Menge

$$\mathfrak{cl}(a) = \{\, b \in G \mid a \sim b \,\}$$

aller zu x äquivalenten Elemente. Diese lässt sich hier explizit beschreiben als

$$\mathfrak{cl}(a) = aH,$$

denn $a \sim b$ ist definiert als $a^{-1}b \in H$ und dies ist gleichbedeutend mit $b \in aH$.

Die Menge $\mathfrak{cl}(a) = aH$ entsteht also, indem man alle Elemente von H von links mit a multipliziert. Daher nennen wir aH die *Linksnebenklasse* von H bezüglich a.

Die *Quotientenmenge* von G bezüglich $\sim$ ist die Menge aller Äquivalenzklassen:

$$G/\sim = \{\, \mathfrak{cl}(a) \mid a \in G \,\}.$$

In unserem Fall ist dies die Menge aller Linksnebenklassen von G:

$$G/H := \{\, aH \mid a \in G \,\}.$$

Dies zerlegt G in disjunkte Teilmengen, denn zwei Äquivalenzklassen sind entweder gleich oder disjunkt. Zudem haben je zwei Äquivalenzklassen aH und bH gleich viele Elemente: Wir haben zueinander inverse Bijektionen

$$aH \xrightarrow{\sim} bH, \quad x \mapsto ba^{-1}x,$$
$$bH \xrightarrow{\sim} aH, \quad y \mapsto ab^{-1}y.$$

Damit haben wir die Menge G der Kardinalität $|G|$ zerlegt in genau $|G/H|$ gleichgroße Teilmengen der Kardinalität $|H|$. Damit haben wir gezeigt:

Satz 9A1 (Lagrange)**.** *Für jede Untergruppe $H < G$ gilt $|G| = |G/H| \cdot |H|$.* □

Definition 9A2. Die Kardinalität $|G/H|$ der Quotientenmenge G/H nennt man den *Index* der Untergruppe H in G. Dies schreibt man auch $|G : H| = |G/H|$.

Wir werden den Satz von Lagrange nur für endliche Gruppen verwenden. Hier entfaltet er seine volle Kraft, indem er eine Beziehung herstellt zwischen algebraischen Strukturen (Untergruppen) und arithmetischen Eigenschaften (Teilbarkeit):

Korollar 9A3. *Sei G eine endliche Gruppe.*

- *Die Ordnung $|H|$ jeder Untergruppe $H < G$ teilt die Gruppenordnung $|G|$.*
- *Die Ordnung* $\operatorname{ord}(x)$ *jedes Elements $x \in G$ teilt die Gruppenordnung $|G|$.* □

Korollar 9A4. *Eine Gruppe G von Primzahlordnung hat nur die beiden trivialen Untergruppen $\{1\}$ und G und ist insbesondere zyklisch.*

BEWEIS. Ist $a \in G$ nicht-trivial, dann gilt $\{1\} \neq \langle a \rangle < G$, also $G = \langle a \rangle$. □

Vorsicht! — Der Satz von Lagrange besagt: Wenn man eine Untergruppe $U < G$ vorliegen hat, dann teilt $|H|$ die Ordnung $|G|$. Die Umkehrung gilt nicht: Wenn n die Gruppenordnung $|G|$ teilt, dann braucht es keine Untergruppe $U < G$ der Ordnung n zu geben. (Diese Frage wird uns später in Form der Sylow–Sätze noch beschäftigen.)

Der Satz von Lagrange gilt genauso für Kardinalzahlen unendlicher Gruppen:

Satz 9A5. *Sei G eine Gruppe und seien $K < H < G$ Untergruppen. Sei $X \subset G$ ein Repräsentantensystem der Äquivalenzklassen G/H, und sei $Y \subset H$ ein Repräsentantensystem der Äquivalenzklassen H/K, Dann ist $\varphi\colon X \times Y \to G/K$ mit $(x,y) \mapsto xyK$ eine Bijektion.*

BEWEIS. *Surjektivität:* Sei $aK \in G/K$. Jedes Element $a \in G$ ist äquivalent zu einem Repräsentanten $x \in X$ modulo H. Äquivalenz $a \sim x$ bedeutet $a \in xH$, also existiert $h \in H$ sodass $a = xh$. Jedes Element $h \in H$ ist äquivalent zu einem Repräsentanten $y \in Y$ modulo K, also $h = yk$ mit $k \in K$. Demnach gilt $a = xyk$ und somit $aK = \varphi(x,y)$.

Injektivität: Sei $\varphi(x,y) = \varphi(x',y')$. Aus $xyK = x'y'K$ folgt, dass x und x' äquivalent sind modulo H. Da X aus jeder Äquivalenzklasse genau einen Repräsentanten enthält, muss $x = x'$ gelten. Aus $yK = y'K$ folgt, dass y und y' äquivalent sind modulo K. Da Y aus jeder Äquivalenzklasse genau einen Repräsentanten enthält, muss $y = y'$ gelten. □

Korollar 9A6. *Für Gruppen $K < H < G$ gilt $|G:K| = |G:H| \cdot |H:K|$.* □

Für $K = \{1\}$ erhalten wir hieraus als Spezialfall $|G| = |G:H| \cdot |H|$.

Bemerkung 9A7. Der Satz von Lagrange ist grundlegend für Gruppen. Er gilt nicht für Monoide: Sei zum Beispiel $M = \langle a \rangle$ das zyklische Monoid mit $a \in \mathrm{Abb}(\{1,\dots,n\})$ gegeben durch $1 \mapsto 2 \mapsto \dots \mapsto n \mapsto n$. Dieses Monoid hat n Elemente $a^0, a^1, a^2, \dots, a^{n-1} = a^n$ und enthält ein Untermonoid der Ordnung k für jede natürliche Zahl k mit $1 \leq k \leq n$.

§**9Ac. Rechtsnebenklassen.** Analog zu Linksnebenklassen können wir auch Rechtsnebenklassen von H in G betrachten. Hierzu definieren wir $a \sim b$ durch $ba^{-1} \in H$. Auch dies ist eine Äquivalentrelation. Die Äquivalenzklasse $\mathfrak{cl}(a)$ eines Elementes $a \in G$ ist nun $\mathfrak{cl}(a) = Ha$, denn $ba^{-1} \in H$ ist gleichbedeutend mit $b \in Ha$. Man nennt Ha die *Rechtsnebenklasse* von a modulo H. Die Quotientenmenge bezeichnen wir mit

$$H\backslash G := \{\, Ha \mid a \in G \,\}.$$

Bemerkung 9A8. Die Inversion $G \to G$, $x \mapsto x^{-1}$ induziert eine Bijektion

$$H\backslash G \xrightarrow{\sim} G/H, \quad Ha \mapsto a^{-1}H.$$

Insbesondere sind beide Indizes $|H\backslash G|$ und $|G/H|$ gleich. Auch der Satz von Lagrange gilt wörtlich genauso für Rechtsnebenklassen.

Beispiel 9A9. Zur Illustration betrachten wir die symmetrische Gruppe S_3. Diese besteht aus der Identität id, drei Transpositionen $(1,2)$, $(2,3)$, $(1,3)$ und den beiden 3-Zykeln $(1,2,3)$, $(1,3,2)$. In S_3 ist $H = \{\mathrm{id}, (1,2)\}$ eine Untergruppe.

Die Links- bzw. Rechtsnebenklassen von H stimmen nicht überein:

Linksnebenklassen		*Rechtsnebenklassen*
$\mathrm{id} \cdot H = \{\mathrm{id}, (1,2)\}$		$\{\mathrm{id}, (1,2)\} = H \cdot \mathrm{id}$
$(1,2,3) \cdot H = \{(1,2,3), (1,3)\}$	$\neq$	$\{(1,2,3), (2,3)\} = H \cdot (1,2,3)$
$(1,3,2) \cdot H = \{(1,3,2), (2,3)\}$	$\neq$	$\{(1,3,2), (1,3)\} = H \cdot (1,3,2)$

Anders für die Untergruppe $K = \{\mathrm{id}, (1,2,3), (1,3,2)\}$:

Linksnebenklassen		*Rechtsnebenklassen*
$\mathrm{id} \cdot K =$	$\{\mathrm{id}, (1,2,3), (1,3,2)\}$	$= K \cdot \mathrm{id}$
$(1,2) \cdot K =$	$\{(1,2), (2,3), (1,3)\}$	$= K \cdot (1,2)$

Bemerkung 9A10. Das Beispiel zeigt, dass man zwischen Rechts- und Linksnebenklassen unterscheiden muss. Rechts- und Linksnebenklassen von H stimmen bezüglich jedes $a \in G$

überein, wenn $Ha = aH$ für alle $a \in G$ gilt, und dies ist gleichbedeutend mit der Bedingung $a^{-1}Ha = H$ für alle $a \in G$.

§9B. Normale Untergruppen und Quotientengruppen

§9Ba. Normale Untergruppen. Eine Untergruppe $K < G$ heißt *normal*, wenn sie die Bedingung $aKa^{-1} = K$ für alle $a \in G$ erfüllt. Dies schreiben wir kurz $K \lhd G$.

Die Bedingung $aKa^{-1} = K$ ist äquivalent zu $aK = Ka$. Eine Untergruppe $K \lhd G$ ist demnach genau dann normal, wenn für alle $a \in$ die Linksnebenklasse aK mit der Rechtsnebenklasse Ka übereinstimmt.

Beispiel 9B1. In jeder Gruppe G gilt $\{1\} \lhd G$ und $G \lhd G$.

Beispiel 9B2. Ist G eine abelschen Gruppe, dann ist jede Untergruppe $H < G$ normal.

Beispiel 9B3. In der symmetrischen Gruppe S_3 ist die Untergruppe $H = \{\mathrm{id}, (1,2)\}$ nicht normal, $K = \{\mathrm{id}, (1,2,3), (1,3,2)\}$ hingegen schon, wie in Beispiel 9A9 gesehen.

Die folgende Beobachtung zeigt die besondere Bedeutung normaler Untergruppen:

Proposition 9B4. *Für jeden Gruppenhomomorphismus $f\colon G \to H$ ist der Kern*

$$\ker(f) = \{\, x \in G \mid f(x) = 1 \,\}$$

eine normale Untergruppe von G.

BEWEIS. Offenbar ist $\ker(f)$ eine Untergruppe (2D34), denn es gilt $1 \in \ker(f)$ und für alle $x, y \in \ker(f)$ auch $xy \in \ker(f)$ und $x^{-1} \in \ker(f)$. Für alle $x \in \ker(f)$ und $a \in G$ gilt

$$f(axa^{-1}) = f(a)f(x)f(a)^{-1} = f(a)f(a)^{-1} = 1,$$

also $axa^{-1} \in \ker(f)$. □

Bemerkung 9B5. Die deutsche Bezeichnung "normale Untergruppe" (oder englisch "normal subgroup") ist insofern irreführend, als normale Untergruppen genau genommen sehr speziell sind. Die französische Bezeichnung "sousgroupe distingué" (etwa 'ausgezeichnete Untergruppe') beschreibt die Sachlage wesentlich besser. Die jeweiligen Traditionen ändern zu wollen hat, wie für manch andere bedauernswerte Bezeichnung, trotz guter Argumente keinerlei Erfolgsaussichten.

Proposition 9B6. *Für jeden Gruppenhomomorphismus $f\colon G \to H$ gilt*

$$|G| = |\ker(f)| \cdot |\mathrm{im}(f)|\,.$$

BEWEIS. Es gilt $f(x) = f(x')$ genau dann, wenn $x'x^{-1} \in \ker(f)$. Für jedes Bildelement $y = f(x)$ gilt demnach $f^{-1}(y) = \ker(f)x$. Daraus folgt $\left|f^{-1}(y)\right| = |\ker(f)|$ und somit die Behauptung. Der Satz gilt genauso für Kardinalzahlen unendlicher Gruppen. □

§9Bb. Quotientengruppen.

Lemma 9B7. *Für jede normale Untergruppe $K \lhd G$ ist die Äquivalenzrelation $\equiv$, definiert durch $a \equiv b$ genau dann wenn $a^{-1}b \in K$, mit der Multiplikation verträglich.*

BEWEIS. Wir haben zu zeigen, dass aus $a \equiv a'$ und $b \equiv b'$ folgt $ab \equiv a'b'$. Die Äquivalenz $a \equiv a'$ bedeutet $a^{-1}a' \in K$, und $b \equiv b'$ bedeutet $b^{-1}b' \in K$. Daraus folgt $ab \equiv a'b'$, denn

$$(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = b^{-1}(a^{-1}a')b \cdot (b^{-1}b') \in K. \qquad \square$$

Satz 9B8. *Sei G eine Gruppe und sei $K \lhd G$ eine normale Untergruppe. Dann existiert auf der Quotientenmenge G/K genau eine Gruppenstruktur, die die Projektion $\pi\colon G \to G/K$, $a \mapsto aK$, zu einem Gruppenhomomorphismus macht.*

BEWEIS. Dies folgt wie immer für Quotientenstrukturen (2G1). Wir wollen es hier dennoch explizit nachrechnen.

Eindeutigkeit: Wenn $\pi\colon G \to G/K$ ein Homomorphismus ist, dann muss für das Produkt auf G/K notwendigerweise $(aK)\cdot(bK) = (ab)K$ für alle $a, b \in G$ gelten.

Existenz: Da K als normal vorausgesetzt wird, gilt für die Komplexmultiplikation

$$aK \cdot bK = a(Kb)K = a(bK)K = (ab)(KK) = (ab)K.$$

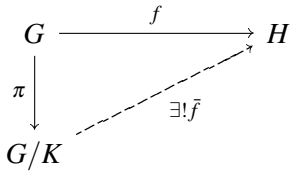
Dies definiert auf G/K eine Verknüpfung, die π zu einem Homomorphismus macht.

Die Gruppeneigenschaft von $(G,\cdot)$ überträgt sich auf $(G/K,\cdot)$, siehe 2G1. $\square$

§**9Bc. Homomorphiesatz.** Die Quotientengruppe G/K erfreut sich folgender universeller Abbildungseigenschaft:

Satz 9B9 (Homomorphiesatz)**.** *Sei $K \lhd G$ eine normale Untergruppe und $\pi\colon G \to G/K$ der Quotientenhomomorphismus. Zu jedem Gruppenhomomorphismus $f\colon G \to H$ mit $K <$ $\ker(f)$ existiert genau ein Gruppenhomomorphismus $\bar{f}\colon G/K \to H$ mit $f = \bar{f} \circ \pi$. In diesem Fall gilt* $\operatorname{im}(\bar{f}) = \operatorname{im}(f)$ *und* $\ker(\bar{f}) = \ker(f)/K$.

In diesem Fall sagen wir, der Homomorphismus $f\colon G \to H$ *induziert* den Homomorphismus $\bar{f}\colon G/K \to H$ auf der Quotientengruppe G/K. Dieser Sachverhalt wird durch das folgende kommutative Diagramm veranschaulicht:



BEWEIS. Übung (oder 2G2 nachlesen). $\square$

Korollar 9B10. *In obiger Situation gilt* $\ker(\bar{f}) = \ker(f)/K$. $\square$

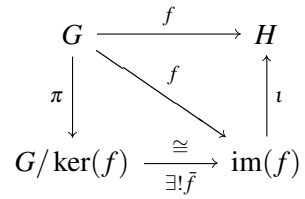
§**9Bd. Erster Isomorphiesatz.**

Satz 9B11 (kanonische Faktorisierung)**.** *Jeder Gruppenhomomorphismus $f\colon G \to H$ faktorisiert gemäß*

$$f\colon G \xrightarrow{\pi} G/\ker(f) \xrightarrow{\bar{f}} \operatorname{im}(f) \xrightarrow{\iota} H$$

in die Projektion π, den induzierten Isomorphismus und die Inklusion ι.

Dieser Sachverhalt wird durch das folgende kommutative Diagramm veranschaulicht:



BEWEIS. Dies folgt aus dem Homomorphiesatz 9B9 angewendet auf $K = \ker(f)$ und $H = \mathrm{im}(f)$. Nach Konstruktion ist $f\colon G \to \mathrm{im}(f)$ surjektiv. Übergang zur Quotientengruppe induziert einen Gruppenhomomorphismus $\bar{f}\colon G/\ker(f) \xrightarrow{\sim} \mathrm{im}(f)$. Dieser ist surjektiv und wegen $\ker(\bar{f}) = \ker(f)/K = \{1\}$ auch injektiv. □

§9Be. Zweiter Isomorphiesatz.

Lemma 9B12. *Sei G eine Gruppe und seien $H, K < G$ zwei Untergruppen.*

1. *Aus $H < G$ und $K \lhd G$ folgt $HK = KH$.*
2. *Aus $HK = KH$ folgt $HK = KH = \langle H \cup K \rangle$.*

BEWEIS. (1) Es gilt $HK = \bigcup_{h\in H} hK = \bigcup_{h\in H} Kh = KH$.

(2) Die Inklusionen $H, K \subset HK \subset \langle H \cup K \rangle$ sind klar. Für die umgekehrte Inklusion $HK \supset \langle H \cup K \rangle$ reicht es zu zeigen, dass HK eine Untergruppe von G ist:

- Es gilt $1 \in HK$.
- Es gilt $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$.
- Es gilt $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$. □

Satz 9B13. *Sei G eine Gruppe, $H < G$ und $K \lhd G$. Dann gilt $H \cap K \lhd H$ und*

$$H/(H \cap K) \cong HK/K.$$

BEWEIS. Sei $\pi\colon G \to G/K$ der Quotientenhomomorphismus. Die Einschränkung $\pi|_H$ hat Kern $\ker(\pi|_H) = H \cap K$. Das Bild von $(\pi|_H)$ besteht aus allen Nebenklassen hK mit $h \in H$, also $\mathrm{im}(\pi|_H) = HK/K$. Der erste Isomorphiesatz induziert somit den Gruppenisomorphismus $H/(H \cap K) \xrightarrow{\sim} HK/K$. □

§9Bf. Korrespondenz von Untergruppen.

Proposition 9B14. *Sei $f\colon G \to H$ ein Gruppenhomomorphismus. Auf der Menge der Untergruppen stiften f und f^{-1} eine Bijektion zwischen den Untergruppen $U < G$, die* $\ker(f)$ *enthalten, und den Untergruppen $V < H$, die im Bild* $\mathrm{im}(f)$ *enthalten sind.*

BEWEIS. Aus $V < \mathrm{im}(f)$ folgt $f(f^{-1}(V)) = V$. Für $\ker(f) < U < G$ sieht man $f^{-1}(f(U)) = U$ wie folgt: Zunächst ist $f^{-1}(f(U)) \supset U$ klar. Es bleibt $f^{-1}(f(U)) \subset U$ zu zeigen. Für $a' \in f^{-1}(f(U))$ wissen wir, dass $f(a') = f(a)$ für ein $a \in U$. Also liegt $k = a'a^{-1}$ in $\ker(f)$ und somit in U. Daher liegt auch $a' = ka$ in U. □

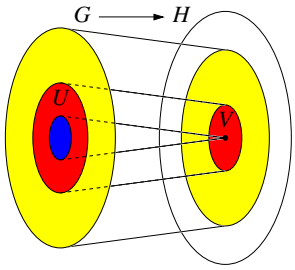


ABBILDUNG 1. Schematische Darstellung eines Gruppenhomomorphismus $f\colon G \to H$ und der Korrespondenz von Untergruppen: Die Gruppe G und ihr Bild $\mathrm{im}(f) < H$ sind gelb dargestellt, der Kern $\ker(f) < G$ und sein Bild $\{1\} < H$ blau, sich entsprechende Untergruppen U und V rot.

§9Bg. Dritter Isomorphiesatz.

Satz 9B15. *Sei $K \lhd G$ und $\pi\colon G \to G/K$ der Quotientenhomomorphismus.*

Dann stiften π und π^{-1} eine Bijektion zwischen den Untergruppen U mit $K < U < G$ und den Untergruppen $V < H$, und π induziert eine Bijektion $(G/K)/(U/K) \cong G/U$.

Dabei entsprechen normale Untergruppen $U \lhd G$ mit $K < U$ normalen Untergruppen $V \lhd H$, und für diese induziert π einen Gruppenisomorphismus $(G/K)/(U/K) \cong G/U$.

BEWEIS. Die Korrespondenz der Untergruppen haben wir bereits in 9B14 gesehen.

Wir definieren $G/K \to G/U$ durch $aK \mapsto aU$. Dies ist wohldefiniert wegen $K < U$. Dabei haben aK und bK genau dann dasselbe Bild, wenn $a^{-1}b \in U$. In der Gruppe G/K entspricht dies den Linksnebenklassen modulo der Untergruppe U/K. Übergang zur Quotientenmenge $(G/K)/(U/K)$ liefert die gewünschte Bijektion.

Ist $U \lhd G$, also $aUa^{-1} = U$ für alle $a \in G$, folgt $\pi(a)\pi(U)\pi(a)^{-1} = \pi(U)$, also $\pi(U) \lhd G$. Umgekehrt sei $V \lhd G/K$, also $(aK)V(aK)^{-1} = V$ für alle $a \in G$. Für $U = \pi^{-1}(V)$ folgt dann $\pi(aUa^{-1}) = \pi(U)$, also $aUa^{-1} = U$ für alle $a \in G$. Die zuvor konstruierte Bijektion $(G/K)/(U/K) \cong G/U$ wird in diesem Fall zu einem Gruppenisomorphismus. □

§9C. Kommutieren

§9Ca. Kommutatoren. Zwei Elemente $a, b \in G$ *kommutieren* wenn $ab = ba$ gilt. Da wir in einer Gruppe arbeiten, ist dies äquivalent zu $aba^{-1} = b$, oder auch $aba^{-1}b^{-1} = 1$.

Definition 9C1. Wir nennen $[a,b] := aba^{-1}b^{-1}$ den *Kommutator* von $a, b \in G$.

Die Menge $M = \{\, [a,b] \mid a,b \in G \,\}$ aller Kommutatoren in G bildet im Allgemeinen keine Untergruppe: Zwar gilt $1 \in M$ und $M^{-1} = M$, denn

$$[a,b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b,a],$$

aber es gibt keinen Grund, warum das Produkt zweier Kommutatoren wieder ein Kommutator sein sollte. (Im Allgemeinen ist es das nicht.) Wenn wir also zu einer Untergruppe gelangen wollen, dann müssen wir die von M erzeugte Untergruppe betrachten:

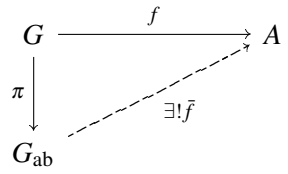
Definition 9C2. Die von allen Kommutatoren in G erzeugte Untergruppe

$$[G,G] := \langle\, [a,b] \mid a,b \in G \,\rangle$$

nennen wir die *Kommutatoruntergruppe* oder kurz *Kommutatorgruppe* von G.

§9Cb. Abelschmachung.

Satz 9C3. *Die Kommutatoruntergruppe $[G,G]$ ist normal in G und die Quotientengruppe $G_{\mathrm{ab}} := G/[G,G]$ ist abelsch. Der Quotientenhomomorphismus $\alpha\colon G \to G_{\mathrm{ab}}$ hat folgende universelle Eigenschaft: Jeder Gruppenhomomorphismus $f\colon G \to A$ in eine abelsche Gruppe A induziert einen Gruppenhomomorphismus $\bar{f}\colon G_{\mathrm{ab}} \to A$ mit $f = \bar{f} \circ \alpha$.*



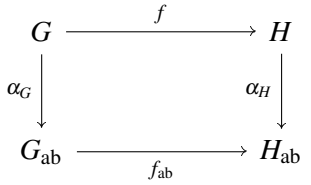
BEWEIS. Für die Menge $M = \{\, [a,b] \mid a,b \in G \,\}$ und alle $c \in G$ gilt $cMc^{-1} = M$:

$$c[a,b]c^{-1} = c(aba^{-1}b^{-1})c^{-1} = (cac^{-1})(cbc^{-1})(ca^{-1}c^{-1})(cb^{-1}c^{-1}) = [cac^{-1}, cbc^{-1}].$$

Daraus folgt für $K = \langle M \rangle$ dass $K = \langle cMc^{-1} \rangle = \langle M \rangle = K$.

Für alle $a,b \in G$ erfüllt der Quotientenhomomorphismus $\alpha\colon G \to G_{\mathrm{ab}}$ die Bedingung $\alpha(aba^{-1}b^{-1}) = 1$, also $\alpha(a)\alpha(b)\alpha(a)^{-1}\alpha(b)^{-1} = 1$. Das bedeutet, in G_{ab} kommutieren alle Elemente. Der Rest folgt aus dem Homomorphiesatz. □

Korollar 9C4. *Die Abelschmachung ordnet jeder Gruppe G eine abelsche Gruppe G_{ab} und einen natürlichen Homomorphismus $\alpha_G\colon G \to G_{\mathrm{ab}}$ zu. Jedem Gruppenhomomorphismus $f\colon G \to H$ ordnet sie einen Gruppenhomomorphismus $f_{\mathrm{ab}}\colon G_{\mathrm{ab}} \to H_{\mathrm{ab}}$ zu, sodass*



kommutiert. Für die Identität $\mathrm{id}\colon G \to G$ *von G ist* $\mathrm{id}_{\mathrm{ab}}\colon G_{\mathrm{ab}} \to G_{\mathrm{ab}}$ *die Identität von G_{ab}, und für die Komposition von Gruppenhomomorphismen $g\colon G \to H$ und $f\colon H \to K$ gilt $(f \circ g)_{\mathrm{ab}} = f_{\mathrm{ab}} \circ g_{\mathrm{ab}}$. Das bedeutet, die Abelschmachung ist ein Funktor von der Kategorie der Gruppen in die Kategorie der abelschen Gruppen.*

§9Cc. Direkte Produkte.

Wir beginnen mit folgender nützlichen Beobachtung:

Lemma 9C5. *Seien $H,K \leq G$ endliche Gruppen. Dann gilt $|H| \cdot |K| = |HK| \cdot |H \cap K|$.*

BEWEIS. Wir betrachten die Abbildung $f\colon H \times K \to G$ mit $(a,b) \mapsto ab$. Ihr Bild ist die Menge HK. Für $s \in H \cap K$ gilt $f(a,b) = (as, s^{-1}b)$. Umgekehrt gilt $f(a,b) = f(a',b')$ genau dann, wenn $ab = a'b'$. Also erfüllt $s = a^{-1}a' = bb'^{-1} \in H \cap K$ die Gleichung $(a',b') = (as, s^{-1}b)$. Demnach gilt $\left|f^{-1}(x)\right| = |H \cap K|$ für alle $x \in HK$. □

Sind H,K zwei Gruppen, dann ist das Produkt $H \times K$ eine Gruppe mit komponentenweise Verknüpfung (2D28). Man nennt zur Betonung $H \times K$ das *externe* direkte Produkt.

Definition 9C6. Eine Gruppe G ist das *interne direkte Produkt* von zwei Untergruppen $H,K < G$ wenn $f\colon H \times K \to G$ mit $f(a,b) \mapsto ab$ ein Gruppenisomorphismus ist.

Ist G das interne direkte Produkt zweier Untergruppen $H,K < G$, dann schreiben wir abkürzend $G = H \times K$. Stillschweigend identifizieren wir also $H \times K$ und $HK = G$ mittels des Isomorphismus f, und unterscheidet somit nicht mehr zwischen internem und extenem direkten Produkt. Diese Identifikation ist natürlich nur dann erlaubt, wenn f ein Gruppenisomorphismus ist. Hierzu wollen wir nun praktische Kriterien aufstellen.

Definition 9C7. Zwei Untergruppen $H,K < G$ *kommutieren*, wenn $ab = ba$ für alle $a \in H$ und $b \in K$ gilt. Für den Kommutator $[a,b] = aba^{-1}b^{-1}$ bedeutet das $[a,b] = 1$.

Zur Abkürzung definieren wir

$$[H,K] := \langle\, [a,b] \mid a \in H, b \in K \,\rangle$$

Es gilt dann $[H,K] = \{1\}$ genau dann, wenn H und K kommutieren.

Satz 9C8. *Für Gruppen $H,K < G$ sind äquivalent:*

1. *Die Gruppe G ist das interne direkte Produkt von H und K.*
2. *Es gilt $HK = G$ und $H \cap K = \{1\}$ sowie $[H,K] = 1$.*
3. *Es gilt $HK = G$ und $H \cap K = \{1\}$ sowie $H,K \lhd G$.*

BEWEIS. "(1) $\Leftrightarrow$ (2)" Die Abbildung $f\colon H \times K \to G$ mit $(a,b) \mapsto ab$ ist genau dann surjektiv, wenn $G = HK$ gilt, und genau dann injektiv, wenn $H \cap K = \{1\}$ (siehe obigen Beweis von Lemma 9C5). Die Abbildung ist f genau dann ein Gruppenhomomorphismus, wenn H und K kommutieren, denn $f(a'a,bb') = a'abb'$ und $f(a',b)f(a,b') = a'bab'$.

"(2) $\Rightarrow$ (3)" Aus $G = HK$ und $[H,K] = \{1\}$ folgt $K \lhd G$ und $H \lhd G$: Für alle $a \in H$ und $b \in K$ gilt dann $K^{ab} = K^b = K$ und $H^{ab} = H^b = H$.

"(3) $\Rightarrow$ (2)" Aus $H \cap K = \{1\}$ und $H,K \lhd G$ folgt $[H,K] = \{1\}$: Für $a \in H$ und $b \in K$ liegt $[a,b] = (aba^{-1})b^{-1}$ in K wegen $aba^{-1}, b^{-1} \in K$. Andererseits liegt $[a,b] = a(ba^{-1}b^{-1})$ in H wegen $a, ba^{-1}b^{-1} \in H$. Aus $H \cap K = \{1\}$ folgt nun $[a,b] = 1$. □

§9D. Zyklische Gruppen

Als erste Anwendung der Isomorphiesätze wollen wir im Folgenden die zyklischen Gruppen sowie ihre Homomorphismen klassifizieren.

§**9Da. Klassifikation zyklischer Gruppen.** Zur Erinnerung: Wir nennen eine Gruppe $(G,\cdot)$ *zyklisch* wenn sie von einem Element $g \in G$ erzeugt wird, also $G = \langle g \rangle$ gilt.

Proposition 9D1. *Die Gruppe G wird genau dann von $g \in G$ erzeugt, wenn der Gruppenhomomorphismus $\mathbb{Z} \to G$ mit $k \mapsto g^k$ surjektiv ist.* □

Ist $(A,+)$ eine abelsche Gruppe in additiver Schreibweise, dann schreibt man statt der Potenz g^k von $g \in G$ das Vielfache ka von $a \in A$. Die Gruppe $(A,+)$ wird von a erzeugt, wenn $A = \{\, ka \mid k \in \mathbb{Z} \,\}$. Dies kann man kurz $A = \mathbb{Z}a$ schreiben.

Beispiel 9D2. Die Gruppe $\mathbb{Z}\times\mathbb{Z}$ ist nicht zyklisch.

BEWEIS. Angenommen, $\mathbb{Z}\times\mathbb{Z}$ wäre zyklisch, also $\mathbb{Z}\times\mathbb{Z}=\mathbb{Z}(a,b)$ mit $a,b\in\mathbb{Z}$. Für $a\neq 0$ gilt $(a,b+1)\notin\mathbb{Z}(a,b)$, für $b\neq 0$ gilt $(a+1,b)\notin\mathbb{Z}(a,b)$. Für $(a,b)=(0,0)$ gilt $\mathbb{Z}(0,0)=\{(0,0)\}\neq\mathbb{Z}\times\mathbb{Z}$. □

Satz 9D3. *Jede Untergruppe $H<\mathbb{Z}$ ist zyklisch, das heißt $H=\mathbb{Z}a$ für ein $a\in\mathbb{Z}$.*

In diesem Fall wird $H=\mathbb{Z}a$ von a und $-a$ erzeugt, und wir können $a\in\mathbb{N}$ annehmen.

BEWEIS. Wenn $H=\{0\}$, dann erfüllt $a=0$ das Verlangte. Andernfalls wählen wir $a\in H$ mit $a\neq 0$ und minimalem Betrag $|a|$. Es bleibt $H=\mathbb{Z}a$ zu zeigen.

"$H\supset\mathbb{Z}a$" ist klar: Aus $a\in H$ folgt $\mathbb{Z}a\subset H$, denn H ist eine Untergruppe von $\mathbb{Z}$.

"$H\subset\mathbb{Z}a$" Für jedes $x\in H$ liefert Division mit Rest $x=qa+r$ mit $0\leq|r|<|a|$. Aus $x\in H$ und $qa\in H$ folgt $r=x-qa\in H$, also $r=0$ aufgrund der Minimalität von a. Das bedeutet $x=qa$, also $x\in\mathbb{Z}a$. Wir schließen daraus $H=\mathbb{Z}a$. □

Korollar 9D4. *Jede zyklische Gruppe G ist isomorph zu $\mathbb{Z}/n\mathbb{Z}$ für ein $n\in\mathbb{N}$.*

BEWEIS. Sei $G=\langle g\rangle$. Der Gruppenhomomorphismus $f\colon\mathbb{Z}\to G$ mit $k\mapsto g^k$ ist surjektiv. Sein Kern ist von der Form $H=\mathbb{Z}n$ für ein $n\in\mathbb{N}$ nach 9D3. Folglich induziert f einen Gruppenisomorphismus $\bar{f}\colon\mathbb{Z}/n\mathbb{Z}\xrightarrow{\sim}G$ mit $\bar{k}\mapsto g^k$ für alle $k\in\mathbb{Z}$. □

Korollar 9D5. *Jede Untergruppe $H<G$ einer zyklischen Gruppe G ist zyklisch.*
Die Untergruppen von $\mathbb{Z}/nZ$ sind genau die zyklischen Gruppen $m\mathbb{Z}/n\mathbb{Z}$ für $m\mid n$.

BEWEIS. Es genügt, die zweite, präzisere Aussage zu beweisen. Der Quotientenhomomorphismus $\pi\colon\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ ist surjektiv und hat den Kern $n\mathbb{Z}$. Nach 9B14 stiftet π eine Bijektion zwischen den Untergruppen von $\mathbb{Z}/n\mathbb{Z}$ und den Untergruppen H mit $n\mathbb{Z}<H<\mathbb{Z}$. Nach 9D3 gilt $H=m\mathbb{Z}$ für ein $m\in\mathbb{N}$, und die Bedingung $n\mathbb{Z}<m\mathbb{Z}$ bedeutet $m\mid n$. □

Korollar 9D6. *Jede zyklische Gruppe der Ordnung n hat für jeden Teiler $m\mid n$ genau eine Untergruppe vom Index m.* □

§9Db. Chinesischer Restsatz für zyklische Gruppen.

Satz 9D7. *Genau dann existiert ein Gruppenisomorphismus $\mathbb{Z}/mn\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ wenn $m,n\in\mathbb{Z}$ teilerfremd sind, also* $\mathrm{ggT}(m,n)=1$ *erfüllen.*

BEWEIS. Im Fall $m=0$ gilt $\mathbb{Z}\cong\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ genau für $n=\pm1$: Hier ist $n=0$ unmöglich denn $\mathbb{Z}\times\mathbb{Z}$ ist nicht zyklisch. Ebenso ist $|n|\geq 2$ unmöglich, denn $\mathbb{Z}$ hat keine Elemente der Ordnung ≥ 2. Gleiches gilt für $n=0$ und $m=\pm1$. Wir können also $m,n\neq 0$ annehmen.

Die Gruppenhomomorphismen

$$\varphi_1\colon\mathbb{Z}/mn\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z},\qquad \varphi_1(a+mn\mathbb{Z})=(a+m\mathbb{Z}),$$
$$\varphi_2\colon\mathbb{Z}/mn\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z},\qquad \varphi_1(a+mn\mathbb{Z})=(a+n\mathbb{Z}),$$

sind surjektiv. Sie definieren einen Gruppenhomomorphismus

$$\varphi\colon\mathbb{Z}/mn\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z},\qquad \varphi(a+mn\mathbb{Z})=(a+m\mathbb{Z},a+n\mathbb{Z}).$$

Es gilt $\ker(\varphi_1) = m\mathbb{Z}/mn\mathbb{Z}$ und $\ker(\varphi_2) = n\mathbb{Z}/mn\mathbb{Z}$, und damit $\ker(\varphi) = \ker(\varphi_1) \cap \ker(\varphi_2) = d\mathbb{Z}/mn\mathbb{Z}$ mit $d = \mathrm{kgV}(m,n)$. Sind $m,n \in \mathbb{N}$ teilerfremd, dann folgt $\ker(\varphi) = \{0\}$ und φ ist injektiv. Wegen $|\mathbb{Z}/mn\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = mn$ ist φ dann nicht nur injektiv sondern auch bijektiv.

Nehmen wir umgekehrt einen Isomorphismus $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ an. Jedes Element $x \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ erfüllt $dx = 0$ für $d = \mathrm{kgV}(m,n)$. Das Element $\bar{1} \in \mathbb{Z}/mn\mathbb{Z}$ hat jedoch Ordnung mn. Also gilt $\mathrm{kgV}(m,n) = mn$ und somit $\mathrm{ggT}(m,n) = 1$. □

§**9Dc. Erzeuger zyklischer Gruppen.** Die unendlich-zyklische Gruppe $\mathbb{Z}$ hat als Erzeuger 1 und -1. Für die endlichen zyklischen Gruppen $\mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}_{\geq 1}$ gilt:

Proposition 9D8. *Ein Element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Erzeuger der zyklischen Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$, wenn $\mathrm{ggT}(a,n) = 1$ gilt.*

BEWEIS. Aus $\mathrm{ggT}(a,n) = 1$ folgt $au + nv = 1$ für geeignete $u,v \in \mathbb{Z}$. Demnach gilt $1 \equiv au \mod n\mathbb{Z}$ und $1 \in \langle \bar{a} \rangle$. Ist umgekehrt $1 \in \langle \bar{a} \rangle$, dann gilt $1 \equiv au \mod n\mathbb{Z}$, also $au + nv = 1$ für geeignete $u,v \in \mathbb{Z}$, und somit $\mathrm{ggT}(a,n) = 1$. □

Für die Menge der Erzeuger der Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ bezeichnen wir mit

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\, \bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a,n) = 1 \,\}.$$

Dies sind die invertierbaren Elemente $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ des Rings $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

Definition 9D9. Die *Eulersche φ-Funktion* $\varphi\colon \mathbb{N} \to \mathbb{N}$ ist definiert durch

$$\varphi(n) := \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|.$$

Übung 9D10. Man zeige mit Hilfe des chinesischen Restsatzes, dass φ multiplikativ ist, dass also $\varphi(nm) = \varphi(n)\varphi(m)$ gilt, wenn (n) und (m) teilerfremd sind.

Jede natürliche Zahl $n \in \mathbb{N}_{\geq 1}$ lässt sich eindeutig in ein Produkt aus Primzahlpotenzen zerlegen, das heißt $n = p_1^{e_1} \cdots p_\ell^{e_\ell}$ mit Primzahlen $2 \leq p_1 < \cdots < p_\ell$ und Exponenten $e_1, \ldots, e_\ell \in \mathbb{N}_{\geq 1}$. Daher reicht es, φ auf Primzahlpotenzen zu kennen.

Übung 9D11.
1. Man zeige $(\mathbb{Z}/p^k\mathbb{Z})^\times = (\mathbb{Z}/p^k\mathbb{Z}) \smallsetminus p(\mathbb{Z}/p^k\mathbb{Z})$.
2. Man schließe hieraus $\varphi(p^k) = p^{k-1}(p-1)$ für $k \in \mathbb{N}$.
3. Für $n = p_1^{e_1} \cdots p_\ell^{e_\ell}$ folgt hieraus $\varphi(n) = n \prod_{i=1}^{\ell} (1 - 1/p_i)$.

Übung 9D12. Für alle $n \in \mathbb{N}_{\geq 1}$ gilt

$$n = \sum_{d|n} \varphi(d)$$

wobei d alle Teiler von n mit $1 \leq d \leq n$ durchläuft. □

§**9Dd. Klassifikation endlicher abelscher Gruppen.** Das folgende Ergebnis verschafft uns einen präzisen Überblick über alle endlichen abelschen Gruppen:

Satz 9D13 (Klassifikation endlicher abelscher Gruppen)**.** *Jede endliche abelsche Gruppe A ist isomorph zu einem Produkt von zyklischen Gruppen, das heißt*

$$A \cong \mathbb{Z}/a_1 \times \mathbb{Z}/a_2 \times \cdots \times \mathbb{Z}/a_m \qquad \text{wobei } a_1, a_2, \ldots, a_m \in \mathbb{Z}_{\geq 2}.$$

Hierbei können wir zusätzlich verlangen, dass $a_1 \mid a_2 \mid \cdots \mid a_m$ gelte. In diesem Fall nennen wir $a_1, a_2, \ldots, a_m$ Elementarteiler *von A, und diese sind eindeutig durch A bestimmt: Gilt*

$$\mathbb{Z}/a_1 \times \cdots \times \mathbb{Z}/a_m \cong \mathbb{Z}/b_1 \times \cdots \times \mathbb{Z}/b_n$$

mit $b_1, \ldots, b_n \in \mathbb{Z}_{\geq 2}$ und $b_1 \mid b_2 \mid \cdots \mid b_n$, dann folgt daraus $m = n$ und $a_1 = b_1, \ldots, a_m = b_m$.

Ebenso wie die Klassifikation der zyklischen Gruppen kann man diesen allgemeineren Satz mit den Grundtechniken der Gruppentheorie zeigen. Es ist jedoch einfacher und effizienter, diesen Satz als Spezialfall aus dem Elementarteilersatz für endlich-erzeugte Moduln über Hauptidealringen zu gewinnen 8. Mit dem chinesischen Restsatz folgt hieraus:

Satz 9D14 (Klassifikation mittels Zerlegung in unzerlegbare zyklische Gruppen)**.**
Jede endliche abelsche Gruppe A ist isomorph zu

$$\begin{aligned} &\mathbb{Z}/p_1^{n_{1,1}} \times \mathbb{Z}/p_1^{n_{1,2}} \times \cdots \times \mathbb{Z}/p_1^{n_{1,k_1}} \\ &\times \mathbb{Z}/p_2^{n_{2,1}} \times \mathbb{Z}/p_2^{n_{2,2}} \times \cdots \times \mathbb{Z}/p_2^{n_{2,k_2}} \\ &\quad \vdots \\ &\times \mathbb{Z}/p_\ell^{n_{\ell,1}} \times \mathbb{Z}/p_\ell^{n_{\ell,2}} \times \cdots \times \mathbb{Z}/p_\ell^{n_{\ell,k_\ell}}. \end{aligned}$$

Hierbei sind $2 \leq p_1 < p_2 < \cdots < p_\ell$ Primzahlen, und die Exponenten erfüllen $1 \leq n_{i,1} \leq n_{i,2} \leq \cdots \leq n_{i,k_i}$ für alle $i = 1, 2, \ldots, \ell$. Diese Zahlen sind eindeutig durch A bestimmt und heißen die Invarianten *von A.* □

§**9De. Struktur der Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$.** Für jede natürliche Zahl $n \in \mathbb{N}_{\geq 1}$ hat der Quotientenring $\mathbb{Z}/n\mathbb{Z}$ genau n Elemente Die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ der invertierbaren Elemente hat dabei Ordnung $\varphi(n)$, wie oben eingeführt. Ist $p \in \mathbb{N}$ eine Primzahl, dann ist der Quotientenring $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen, und $(\mathbb{Z}/p\mathbb{Z})^\times$ ist eine Gruppe der Ordnung $p-1$. Wir wollen nun die Struktur dieser Gruppe klären.

Beispiel 9D15. $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$ ist trivial (insbesondere zyklisch).

Beispiel 9D16. $(\mathbb{Z}/3\mathbb{Z})^\times = \{\bar{1}, \bar{2}\}$ ist zyklisch, von $\bar{2}$ erzeugt.

Beispiel 9D17. $(\mathbb{Z}/5\mathbb{Z})^\times$ ist zyklisch, von $\bar{2}$ (oder von $\bar{3}$) erzeugt:
Hier gilt $\bar{2}^0 = \bar{1}$, $\bar{2}^1 = \bar{2}$, $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{3}$ (und $\bar{2}^4 = \bar{1}$).

Beispiel 9D18. $(\mathbb{Z}/7\mathbb{Z})^\times$ ist zyklisch, von $\bar{3}$ (aber nicht von $\bar{2}$) erzeugt.
Hier gilt $\bar{3}^0 = \bar{1}$, $\bar{3}^1 = \bar{3}$, $\bar{3}^2 = \bar{2}$, $\bar{3}^3 = \bar{6}$, $\bar{3}^4 = \bar{4}$, $\bar{3}^5 = \bar{5}$ (und $\bar{3}^6 = \bar{1}$).

Beispiel 9D19. $(\mathbb{Z}/11\mathbb{Z})^\times$ ist zyklisch, von $\bar{2}$ (aber nicht von $\bar{3}$) erzeugt.

Übung 9D20. Man setze die Reihe fort und finde einen Erzeuger von $(\mathbb{Z}/13\mathbb{Z})^\times$, $(\mathbb{Z}/17\mathbb{Z})^\times$, $(\mathbb{Z}/19\mathbb{Z})^\times$, etc. Dass die Suche erfolgreich sein wird, garantiert folgender Satz:

Satz 9D21. *Für jede Primzahl $p \in \mathbb{N}$ ist die multiplikative Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch.*

Der Satz besagt: Es existiert ein Element $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ mit

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{\, g^k \mid k \in \mathbb{Z} \,\},$$

das heißt jedes Element in $(\mathbb{Z}/p\mathbb{Z})^\times$ ist eine Protenz von g. Da wir die Ordnung $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$ kennen, müssen wir also die Existenz eine Elements $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ der Ordnung $p-1$

zeigen. Ein solches Element nennt man *Erzeuger* der Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$, oder auch *primitives Element* des Körpers $\mathbb{Z}/p\mathbb{Z}$. Allgemeiner zeigen wir:

Satz 9D22. *Sei K ein Körper. Jede endliche Untergruppe $G < K^\times$ ist zyklisch. Zu jedem $n \in \mathbb{N}_{\geq 1}$ existiert höchstens eine Untergruppe $G < K^\times$ der Ordnung n.*

BEWEIS. Da K ein Körper ist, hat für jedes $n \in \mathbb{N}_{\geq 1}$ die Gleichung $X^n = 1$ höchstens n Lösungen in K. Ist $G < K^\times$ der Ordnung n, dann gilt nach Lagrange $x^n = 1$ für alle $x \in G$. Die Gleichung $X^n = 1$ hat also genau n Lösungen in K, nämlich die Elemente von G.

Sei $n = p_1^{e_1} \cdots p_k^{e_k}$ die Primfaktorzerlegung von n. Das Polynom $X^{n/p_i} - 1$ hat höchstens n/p_i Nullstellen in K. Es gibt also ein Element $z_i \in G$ mit $z_i^{n/p_i} \neq 1$. Folglich hat $g_i = (z_i)^{n/p_i^{e_i}}$ Ordnung $p_i^{e_i}$. Die Ordnungen von $p_1^{e_1}, \ldots, p_k^{e_k}$ sind teilerfremd, also hat $g = g_1 \cdots g_k$ Ordnung $n = p_1^{e_1}, \ldots, p_k^{e_k}$ nach folgendem Lemma. □

Lemma 9D23. *Seien $g_1, \ldots, g_k \in G$ kommutierende Elemente der Ordungen $n_1, \ldots, n_k$. Sind diese Ordnungen teilerfremd, dann hat das Produkt $g = g_1 \cdots g_k$ die Ordnung $n = n_1 \cdots n_k$.*

BEWEIS. Da $g_1, \ldots, g_k$ untereinander kommutieren, gilt $g^n = g_1^n \cdots g_k^n = 1$. Demnach ist $\operatorname{ord}(g)$ ein Teiler von n. Sei p ein Primteiler von n. Dann teilt p genau ein n_i. $g^{n/p} = g_1^{n/p} \cdots g_i^{n/p} \cdots g_k^{n/p} = g_i^{n/p} \neq 1$. Da dies für alle Primteiler von n gilt, kann $\operatorname{ord}(g)$ kein echter Teiler von n sein, also gilt $\operatorname{ord}(g) = n$. □

Man beachte, dass der Beweis des Satzes nicht konstruktiv ist: Er sagt nicht, welches Element die Gruppe G erzeugt, sondern nur, dass es einen Erzeuger geben muss. Mysteriöserweise erlauben selbst die Gruppen $(\mathbb{Z}/p\mathbb{Z})^\times$ keine Vorhersagen: Zu jeder Primzahl p findet man durch geschicktes Ausprobieren einen Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$, aber es ist keine Formel bekannt, die einen Erzeuger für jedes p liefert. Insbesondere ist keine solche Formel für die Funktion $g\colon \mathcal{P} \to \mathbb{N}$ bekannt, die jede Primzahl $p \in \mathcal{P}$ auf die kleineste natürliche Zahl $g(p)$ abbildet, für die $\overline{g(p)} \in \mathbb{Z}/p\mathbb{Z}$ ein Erzeuger der Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ ist.

Für die reellen und komplexen Zahlen ist die Situation hingegen klar:

Beispiel 9D24. Der Körper $\mathbb{R}$ der reellen Zahlen erlaubt n-te Einheitswurzeln nur für $n = 1$ und $n = 2$: Die endlichen Untergruppen von $\mathbb{R}^\times$ sind $\{1\}$ und $\{\pm 1\}$.

Beispiel 9D25. Im Körper $\mathbb{C}$ der komplexen Zahlen gilt: Für $n \in \mathbb{N}_{\geq 1}$ hat $\zeta_n = \exp(2\pi i/n)$ Ordnung n. Die hiervon erzeugte Gruppe $\langle \zeta_n \rangle = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$ heißt die *Gruppe der n-ten Einheitswurzeln in $\mathbb{C}$*. Ihre Erzeuger sind ζ_n^a mit $\operatorname{ggT}(a,n) = 1$.

§9E. Konjugation und innere Automorphismen

§**9Ea. Zentrum und Zentralisator.** Das *Zentrum* einer Gruppe G besteht aus allen Elementen $z \in G$, die mit allen Gruppenelementen kommutieren, geschrieben

$$Z(G) := \{\, z \in G \mid za = az \text{ für alle } a \in G \,\}.$$

Dies ist eine Untergruppe von G und zudem normal in G, denn

$$c \cdot Z(G) \cdot c^{-1} = \{\, czc^{-1} \mid z \in Z(G) \,\} = Z(G).$$

Der *Zentralisator* eines Elements $a \in G$ besteht aus allen Gruppenelementen $b \in G$, die mit a kommutieren:

$$Z_G(a) := \{\, b \in G \mid ab = ba \,\}.$$

Auch dies ist eine Untergruppe, $Z(G) < Z_G(a) < G$, aber im Allgemeinen nicht normal:

$$c \cdot Z_G(a) \cdot c^{-1} = Z_G(cac^{-1}).$$

Allgemeiner definieren wir den *Zentralisator* einer gegebenen Untergruppe $U < G$ (oder auch nur Teilmenge $U \subset G$) durch

$$Z_G(U) := \{\, b \in G \mid ab = ba \text{ für alle } a \in U \,\}.$$

Dies ist der Durchschnitt der Gruppen $Z_G(a)$ für alle $a \in U$, und damit ist auch $Z_G(U)$ eine Untergruppe von G. Auch hier gilt

$$c \cdot Z_G(U) \cdot c^{-1} = Z_G(cUc^{-1}).$$

Als Spezialfälle erhalten wir den Zentralisator $Z_G(a) = Z_G(\{a\}) = Z_G(\langle a \rangle)$ eines Elements $a \in G$ sowie das Zentrum $Z(G) = Z_G(G)$ als Zentralisator der gesamten Gruppe G.

Übung 9E1. Man weise die gemachten Aussagen nach.

§**9Eb. Konjugation und innere Automorphismen.** Für jedes Element $c \in G$ einer Gruppe G definieren wir die *Konjugation* $\gamma_c \colon G \to G$ durch $\gamma_c(g) = cgc^{-1}$.

Proposition 9E2. *Für alle $c \in G$ gilt $\gamma_c \in \mathrm{Aut}(G)$. Die Abbildung $\gamma \colon G \to \mathrm{Aut}(G)$, $c \mapsto \gamma_c$, ist ein Gruppenhomomorphismus. Sein Kern ist das Zentrum,* $\ker(\gamma) = Z(G)$.

BEWEIS. Zunächst gilt $\gamma_c \in \mathrm{End}(G)$, denn für alle $a, b \in G$ gilt

$$\gamma_c(a \cdot b) = c(ab)c^{-1} = (cac^{-1})(cbc^{-1}) = \gamma_c(a)\gamma_c(b).$$

Zudem ist $\gamma \colon G \to \mathrm{End}(G)$ multiplikativ, das heißt Komposition liefert $\gamma_c \circ \gamma_d = \gamma_{cd}$, denn

$$(\gamma_c \circ \gamma_d)(a) = \gamma_c(\gamma_d(a)) = cdad^{-1}c^{-1} = \gamma_{cd}(a).$$

Demnach ist jede Konjugation γ_c ein Automorphismus mit $\gamma_{(c^{-1})} = (\gamma_c)^{-1}$. Der Kern von $\gamma \colon G \to \mathrm{Aut}(G)$ ist das Zentrum von G, denn $\gamma_c = \mathrm{id}_G$ ist äquivalent zu $\gamma_c(a) = a$ für alle $a \in G$, also $cac^{-1} = a$ für alle $a \in G$. □

Definition 9E3. Das Bild von γ ist eine Untergruppe von $\mathrm{Aut}(G)$, und wird die Gruppe der *inneren Automorphismen* von G genannt, geschrieben $\mathrm{Inn}(G)$.

Korollar 9E4. *Der Gruppenhomomorphismus $\gamma \colon G \to \mathrm{Aut}(G)$ induziert einen Gruppenisomorphismus $G/Z(G) \xrightarrow{\sim} \mathrm{Inn}(G)$ gemäß der kanonischen Faktorisierung 9B11.*

Beispiel 9E5. In einer abelschen Gruppe G ist jede Konjugation die identische Abbildung, also ist $\gamma \colon G \to \{\mathrm{id}_G\}$ der triviale Homomorphismus, und das Zentrum ist $Z(G) = G$.

Proposition 9E6. *Für jede Gruppe G gilt* $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

BEWEIS. Für $\gamma_c \in \mathrm{Inn}(G)$ und $\alpha \in \mathrm{Aut}(G)$ sowie $a \in G$ gilt

$$(\alpha \circ \gamma_c \circ \alpha)(a) = \alpha(c \cdot \alpha^{-1}(x) \cdot c^{-1}) = \alpha(c) \cdot a \cdot \alpha(c)^{-1} = \gamma_{\alpha(c)}(a). \qquad \square$$

Definition 9E7. Die Quotientengruppe $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ nennen wir die *äußere Automorphismengruppe* von G.

Beispiel 9E8. Für jede abelsche Gruppe A gilt $\mathrm{Inn}(A) = \{\mathrm{id}\}$ und daher $\mathrm{Out}(A) = \mathrm{Aut}(A)$. Hier gibt es keine inneren Automorphismen, die von der Konjugation herrühren. Also müssen alle Automorphismen "von außen" kommen, daher der Name.

Im anderen Extrem gibt es Gruppen mit $\mathrm{Aut}(G) = \mathrm{Inn}(G)$, also $\mathrm{Out}(G)$ trivial.

Notation. Die oben betrachtete Operation von links $\gamma_c\colon a \mapsto {}^c a := cac^{-1}$ hat den Vorteil, dass sie dem Gruppenhomomorphismus $\gamma\colon G \to \mathrm{Aut}(G)$ entspricht.

Ebenso ist die analoge Schreibweise von rechts $\delta_c\colon a \mapsto a^c := c^{-1}ac$ bequem und üblich. Diese entspricht einem Anti-Homomorphismus $\delta\colon G \to \mathrm{Aut}(G)$ bzw. einem Homomorphismus $\delta\colon G \to \mathrm{Aut}(G)^{\mathrm{op}}$ in die entgegengesetzte Gruppe (2D8).

§**9Ec. Normalisator.** In nicht-abelschen Gruppen spielt die Konjugation eine wichtige Rolle, zum Beispiel bei der Betrachtung von normalen Untergruppen:

Bemerkung 9E9. Eine Untergruppe $H < G$ ist genau dann normal, wenn $H^g = H$ für alle $g \in G$ gilt. Hierbei definieren wir wie üblich $H^g = \{\, h^g \mid h \in H \,\}$.

Definition 9E10. Der Normalisator einer gegebenen Untergruppe $U < G$ ist

$$N_G(U) := \{\, g \in G \mid U^g = U \,\}.$$

Bemerkung 9E11. Immer gilt $U \lhd N_G(U)$. Es gilt $U \lhd G$ genau dann wenn $N_G(U) = G$.

Bemerkung 9E12. Es gilt $Z_G(U) < N_G(U)$, aber im Allgemeinen ist der Normalisator echt größer als der Zentralisator. In der Symmetrischen Gruppe S_3 gilt für die normale Untergruppe $U = \{\mathrm{id}, (1,2,3), (1,3,2)\}$ zum Beispiel $Z_{S_3}(U) = U$ aber $N_{S_3}(U) = G$.

Übung 9E13. Sei G eine Gruppe, $H < G$ eine Untergruppe und $K < N_G(H)$. Dann gilt $HK = KH = \langle H \cup K \rangle$.

§**9Ed. Charakteristische Untergruppen.** Eine Untergruppe $U < G$ heißt *charakteristisch* in G, wenn für alle Automorphismen $\alpha\colon G \to G$ gilt, dass $\alpha(U) = U$.

Übung 9E14.

1. Jede charakteristische Untergruppe U in G ist normal in G.
2. Man finde eine normale Untergruppe, die nicht charakteristisch ist.
3. Das Zentrum $Z(G)$ ist charakteristisch in G.
4. Die Kommutatoruntergruppe $[G,G]$ ist charakteristisch in G.
5. Sei K charakteristisch in H und H charakteristisch in G. Ist dann K charakteristisch in G?
6. Sei K normal in H und H normal in G. Ist dann K normal in G?

§9F. Operationen

§**9Fa. Operationen.** Wir wollen im Folgenden Operationen von Gruppen auf Mengen betrachten. Es ist nützlich, zunächst mit Operationen von Monoiden zu beginnen:

Definition 9F1. Sei $(M,\cdot,1)$ ein Monoid und sei X eine Menge. Eine *Operation* oder *Aktion* von M auf X ist eine Abbildung $\alpha\colon M\times X\to X$, geschrieben $(a,x)\mapsto a\bullet x$, sodass

$$(a\cdot b)\bullet x = a\bullet(b\bullet x) \quad \text{und} \quad 1\bullet x = x$$

für alle $a,b\in M$ und $x\in X$ gilt.

Beispiel 9F2. Sei $(M,\cdot,1)$ ein Monoid. Jedes Untermonoid $U\subset M$ operiert auf der Menge M durch die eingeschränkte Multiplikation $\cdot\colon M\times M\to M$, $(a,x)\mapsto a\cdot x$.

Beispiel 9F3. Das Monoid $\mathrm{Abb}(X)$ aller Abbildungen von X in sich operiert auf der Menge X durch die Auswertung $\mathrm{Abb}(X)\times X\to X$, $(f,x)\mapsto f(x)$.

Bemerkung 9F4. Eine Operation $\alpha\colon M\times X\to X$ des Monoids M auf der Menge X ist nichts anderes als ein Monoidhomomorphismus $\tilde\alpha\colon M\to\mathrm{Abb}(X)$:

- Jede Operation $\alpha\colon M\times X\to X$ definiert einen Monoidhomomorphismus $\tilde\alpha\colon M\to\mathrm{Abb}(X)$ durch $\tilde\alpha(a)\colon X\to X$, $x\mapsto a\bullet x$.
- Umgekehrt definiert jeder Monoidhomomorphismus $\tilde\alpha\colon M\to\mathrm{Abb}(X)$ eine Operation $\alpha\colon M\times X\to X$ durch $a\bullet x := \tilde\alpha(x)$.

Bemerkung 9F5. Genauer gesagt definiert 9F1 eine *Linksoperation* von M auf X. Eine *Rechtsoperation* von M auf X ist eine Abbildung $X\times M\to X$, $(x,a)\mapsto x\bullet a$, sodass

$$x\bullet(a\cdot b) = (x\bullet a)\bullet b \quad \text{und} \quad x\bullet 1 = x$$

für alle $a,b\in M$ und $x\in X$ gilt.

Ausgehend von $X\times M\to X$ kann man $M\times X\to X$ definieren durch $a\mathbin{\bar\bullet}x = x\bullet a$. Es gilt dann allerdings $a\mathbin{\bar\bullet}(b\mathbin{\bar\bullet}x) = (b\cdot a)\mathbin{\bar\bullet}x$. Eine Rechtsoperation des Monoids $(M,\cdot)$ entspricht demnach einer Linksoperation des entgegengesetzten Monoids $(M,\bar\cdot)$ wobei $a\mathbin{\bar\cdot}b = b\cdot a$ gesetzt wird (2C8). Genauso wie jede Linksoperation $M\times X\to X$ einem Monoidhomomorphismus $M\to\mathrm{Abb}(X)$ entspricht, entspricht jede Rechtsoperation $X\times M\to X$ einem Monoidhomomorphismus $M\to\mathrm{Abb}(X)^{\mathrm{op}}$.

Notation. Ebenso wie die Multiplikation $\cdot\colon M\times M\to M$, die wir abkürzend ab schreiben statt $a\cdot b$, schreiben wir auch die Operation $\bullet\colon M\times X\to X$ kürzer ax statt $a\bullet x$. Meistens geht aus dem Kontext unmissverständlich hervor, welche Verknüpfung gemeint ist. Die obigen Axiome schreiben sich dann etwas gefälliger als $(ab)x = a(bx)$ und $1x = x$.

Definition 9F6. Im Falle einer Gruppe G nennen wir jede Operation $G\times X\to X$ von G auf einer Menge X eine *Gruppenoperation*.

Bemerkung 9F7. Eine Gruppenoperation $\alpha\colon G\times X\to X$ auf der Menge X ist nichts anderes als ein Gruppenhomomorphismus $\tilde\alpha\colon G\to\mathrm{Sym}(()X)$: wobei gilt $\tilde\alpha(g)(x) = \alpha(g,x)$.

Gruppenoperationen haben besonders schöne Eigenschaften, die wir im Folgenden erkunden wollen. Zum Beispiel ist für Gruppen die Unterscheidung zwischen Links- und Rechtsoperation nur eine Frage der Schreibweise: Jede Gruppe G ist zu ihrer entgegengesetzten Gruppe G^{op} isomorph mittels $\varphi\colon G\xrightarrow{\sim}G^{\mathrm{op}}$, $\varphi(g) = g^{-1}$ (2D21). Somit können wir jede Rechtsoperation $X\times G\to X$ in eine Linksoperation $G\times X\to X$ überführen durch $gx := xg^{-1}$. Wir werden daher im Folgenden meist nur von Linksoperationen sprechen. Jede Aussage über Linksoperationen übersetzt sich in offensichtlicher Weise in die entsprechende Aussage über Rechtsoperationen.

§**9Fb. Bahn und Standgruppe.** Sei $G \times X \to X$ eine Gruppenoperation.

Definition 9F8. Für jedes Element $x \in X$ nennen wir $\mathrm{Orb}(x) := Gx := \{\, gx \mid g \in G \,\}$ die *Bahn* oder den *Orbit* von x unter der Aktion von G.

Lemma 9F9. *Je zwei Bahnen sind entweder gleich oder disjunkt.*

BEWEIS. Auf der Menge X definieren wir die Relation $\sim$ durch $x \sim y$ genau dann wenn es ein $g \in G$ gibt mit $gx = y$. Dies ist eine Äquivalenzrelation:

- *Reflexivität:* Es gilt $x \sim x$ denn $1x = x$.
- *Symmetrie:* Aus $x \sim y$ folgt $y \sim x$, denn aus $gx = y$ folgt $x = g^{-1}y$.
- *Transitivität:* Aus $x \sim y$ und $y \sim z$ folgt $x \sim z$, denn aus $g_1x = y$ und $g_2y = z$ folgt $(g_2g_1)x = g_2(g_1x) = g_2y = z$.

Die Äquivalenzklassen sind gerade die Bahnen unter der Operation von G. □

Definition 9F10. In G nennen wir die Untergruppe $\mathrm{Stab}(x) := G_x := \{\, g \in G \mid gx = x \,\}$ die *Standgruppe* oder den *Stabilisator* von x unter der Aktion von G.

Proposition 9F11. *Die Operation induziert eine Bijektion $G/G_x \xrightarrow{\sim} Gx$ durch $aG_x \mapsto ax$.*

BEWEIS. Die Abbildung $G \to Gx$, $a \mapsto ax$ ist surjektiv. Es gilt $ax = bx$ genau dann wenn $a^{-1}bx = x$, also $a^{-1}b \in G_x$. Übergang zur Quotientenmenge G/G_x stiftet demnach die gewünschte Bijektion. Der Rest folgt aus dem Satz von Lagrange. □

Korollar 9F12. *Für jedes $x \in X$ gilt $|Gx| = |G : G_x|$. Ist G eine endliche Gruppe, dann teilt jede Orbitlänge die Gruppenordnung $|G|$.* □

Wir halten zwei besonders wichtige Beispiele fest:

Beispiel 9F13. Die Konjugation definiert eine Operation (von rechts)

$$G \times G \to G, \quad (x,g) \mapsto g^{-1}xg.$$

Die Bahn von x ist die Konjugationsklasse

$$x^G = \{\, x^g \mid g \in G \,\}.$$

Die Standgruppe von x ist der Zentralisator

$$Z_G(x) = \{\, g \in G \mid x^g = x \,\}.$$

Die Anzahl der zu $x \in G$ konjugierten Elemente ist

$$\left|x^G\right| = |G : Z_G(x)|\,.$$

Diese Anzahl ist genau dann gleich 1, wenn $x \in Z(G)$.

Beispiel 9F14. Die Konjugation definiert eine Operation (von rechts)

$$\mathscr{U} \times G \to \mathscr{U}, \quad (U,g) \mapsto U^g$$

auf der Menge $\mathscr{U} = \{\, U < G \,\}$ aller Untergruppen von G. Die Bahn von U ist die Menge der zu U konjugierten Untergruppen $\{\, U^g \mid g \in G \,\}$. Die Standgruppe von U ist der Normalisator

$$N_G(U) = \{\, g \in G \mid U^g = U \,\}$$

Die Anzahl der zu $U < G$ konjugierten Untergruppen ist $|G : N_G(U)|$. Diese Anzahl ist genau dann gleich 1, wenn $U \lhd G$ eine normale Untergruppe ist.

Die Standgruppen G_x und G_y können für verschiedene $x, y \in X$ völlig verschieden sein. Liegen x, y jedoch in derselben Bahn, dann sind G_x und G_y in G konjugiert:

Proposition 9F15. *Für alle $g \in G$ und $x \in X$ gilt $G_{gx} = g \cdot G_x \cdot g^{-1}$.*

BEWEIS. Die Inklusion $g \cdot G_x \cdot g^{-1} \subset G_{gx}$ sieht man wie folgt: Für jedes $a \in G_x$ gilt $(gag^{-1})(gx) = gx$, also $gag^{-1} \in G_{gx}$. Umgekehrt gilt $g \cdot G_x \cdot g^{-1} \supset G_{gx}$: Für jedes $b \in G_{gx}$ ist nämlich $g^{-1}bg \in G_x$, also $b \in g \cdot G_x \cdot g^{-1}$. □

Satz 9F16 (Bahnengleichung)**.** *Sei $G \times X \to X$ eine Gruppenoperation. Sei $(x_i)_{i \in I}$ ein Repräsentantensystem der Bahnen von X. Dann haben wir eine disjunkte Vereinigung*

$$X = \bigsqcup_{i \in I} Gx_i.$$

Wir zerlegen $I = J \sqcup K$ sodass $(x_j)_{j \in J}$ die Fixpunkte von G sind (das heißt $Gx_j = \{x_j\}$) und $(x_k)_{k \in K}$ die Repräsentanten der nicht-trivialen Bahnen (das heißt $|Gx_k| \geq 2$). Dann gilt

$$X = \mathrm{Fix}(G) \sqcup \bigsqcup_{k \in K} Gx_k.$$

Ist X eine endliche Menge, dann sind I, J und K endlich und es gilt

$$|X| = \sum_{i \in I} |G : G_{x_i}| = |\mathrm{Fix}(G)| + \sum_{k \in K} |G : G_{x_k}|.$$

BEWEIS. Dies folgt aus der Bahnenzerlegung von X und $|Gx| = |G : G_x|$. □

Beispiel 9F17. Sei G eine endliche Gruppe, $H < G$ eine Untergruppe. Die Operation $G \times H \to G$, $(g, h) \mapsto gh$, zerlegt G in die Bahnen aH. Die Standgruppe von $a \in G$ ist die triviale Untergruppe $\{1\} < H$. Die Bahnengleichung geht somit über in den Satz von Lagrange.

§**9Fc. Anwendung auf p-Gruppen.** Im Folgenden sei $p \in \mathbb{N}$ eine Primzahl.

Definition 9F18. Eine Gruppe G heißt *p-Gruppe*, wenn $|G| = p^e$ für ein $e \in \mathbb{N}$.

Beispiel 9F19. Nach dem Klassifikationssatz 9D14 ist jede *abelsche* p-Gruppe A isomorph zu

$$A = \mathbb{Z}/p^{n_1} \times \mathbb{Z}/p^{n_2} \times \cdots \times \mathbb{Z}/p^{n_k}$$

mit $k \in \mathbb{N}$ und $1 \leq n_1 \leq n_2 \leq \cdots \leq n_k$ in $\mathbb{N}$. Da A abelsch ist gilt $Z(A) = A$.

Beispiel 9F20. Eine nicht-abelsche p-Gruppe ist zum Beispiel die Untergruppe

$$P = \begin{pmatrix} 1 & * & * & * \\ 0 & \ddots & \ddots & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & 0 & 1 \end{pmatrix} < \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$$

der oberen Dreiecksmatrizen in der speziellen linearen Gruppe $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ der $n \times n$-Matrizen über dem Körper $\mathbb{Z}/p\mathbb{Z}$. Die angegebene Menge P ist eine Untergruppe der Ordnung $p^{n(n-1)/2}$.

Für $n = 1$ ist $P = \{1\}$ trivial, für $n = 2$ ist P zyklisch der Ordnung p. Für $n \geq 3$ hingegen ist P nicht-abelsch. (Man prüfe dies zur Übung nach.) Für das Zentrum findet man

$$Z(P) = \begin{pmatrix} 1 & 0 & 0 & * \\ 0 & \ddots & \ddots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Wir wollen nun die Beobachtung des Beispiels allgemein beweisen:

Satz 9F21. *Jede nicht-triviale p-Gruppe hat ein nicht-triviales Zentrum.*

BEWEIS. Sei G eine Gruppe mit $|G| = p^e$ wobei $e \in \mathbb{N}_{\geq 1}$. Wir haben $Z(G) \neq \{1\}$ zu zeigen. Hierzu lassen wir G durch Konjugation auf sich operieren. Dann gilt $\mathrm{Fix}(G) = Z(G)$. Ist $x_1, \ldots, x_k$ ein Repräsentantensystem der nicht-trivialen Konjugationsklassen, dann gilt

$$|G| = |Z(G)| + \sum_{i=1}^{k} |G : Z_G(x_i)|.$$

Es gilt $Z_G(x_i) < G$, also $Z_G(x_i) = p^{e_i}$ nach Lagrange. Wegen $Z_G(x_i) \subsetneq G$, ist $|G : Z_G(x_i)| > 1$ durch p teilbar. Sowohl $|G|$ als auch jeder Summand $|G : Z_G(x_i)|$ ist durch p teilbar, also teilt p auch $|Z(G)|$. Nun gilt aber $|Z(G)| \geq 1$, denn $1 \in Z(G)$, also folgt $|Z(G)| \geq p$. □

Übung 9F22. Ist $G/Z(G)$ zyklisch, dann ist G abelsch.

Übung 9F23. Jede Gruppe G der Ordnung p^2 ist abelsch.

Übung 9F24. Man gebe bis auf Isomorphie alle Gruppen mit p^2 Elementen an.

Beispiel 9F25. In der Gruppe $P < \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ findet man eine Kette

$$\{1\} < \begin{pmatrix} 1 & 0 & 0 & * \\ 0 & \ddots & \ddots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} < \begin{pmatrix} 1 & 0 & * & * \\ 0 & \ddots & \ddots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} < \begin{pmatrix} 1 & 0 & * & * \\ 0 & \ddots & \ddots & * \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} < \ldots < P$$

Wir wollen nun die Beobachtung des Beispiels allgemein beweisen:

Satz 9F26. *Für jede Gruppe G der Ordnung $|G| = p^e$ existiert eine Kette*

$$\{1\} = K_0 < K_1 < \ldots < K_{e-1} < K_e = G$$

normaler Untergruppen $K_i \lhd G$ der Ordnung $|K_i| = p^i$. Insbesondere ist jede der sukzessiven Quotientengruppen K_i/K_{i-1} zyklisch von Primzahlordnung.

BEWEIS. Wir führen Induktion über e. Für $e = 0$ und $e = 1$ ist nach 9A4 alles klar. Für $e \geq 2$ betrachten wir das Zentrum $Z(G)$. Nach 9F21 gilt $|Z(G)| = p^n$ mit $1 \leq n \leq e$. Nach dem Klassifikationssatz für abelsche Gruppen gibt es eine Kette von Untergruppen

$$\{1\} = K_0 < \ldots < K_n = Z(G)$$

mit $|K_i| = p^i$. Da diese Gruppen im Zentrum von G liegen, sind sie normal in G. Sei $\pi\colon G \to \bar{G}$ der Quotientenhomomorphismus auf die Quotientengruppe $\bar{G} = G/Z(G)$. Diese hat Ordnung p^{e-n}. Nach Induktionsvoraussetzung existiert eine Kette

$$\{1\} = \bar{K}_n < \ldots < \bar{K}_e = \bar{G}$$

normaler Untergruppen $\bar{K}_j \lhd \bar{G}$ der Ordnung $\left|\bar{K}_j\right| = p^{j-n}$. Gemäß der Korrespondenz von Untergruppen (9B15) sind die Urbilder $K_j = \pi^{-1}(\bar{K}_j)$ für $j = n, \dots, e$ normale Untergruppen in G der Ordnung $\left|K_j\right| = p^j$. □

§**9Fd. Der chinesische Restsatz für G-Mengen.** Sei G eine Gruppe. Eine *G-Menge* (X, α) ist eine Menge X zusammen mit einer G-Operation $\alpha\colon G \times X \to X$. Dies schreiben wir wie üblich als Multiplikation $(g,x) \mapsto gx$.

Beispiel 9F27. Jede Gruppe $(G, \cdot)$ können wir als G-Menge auffassen mittels der Gruppenmultiplikation $\cdot\colon G \times G \times G$, $(g,x) \mapsto gx$.

Beispiel 9F28. Sei $H < G$ eine Untergruppe. Dann wird die Menge $G/H = \{\, aH \mid a \in G \,\}$ der Linksnebenklassen eine G-Menge mittels der Operation $g(aH) = (ga)H$.

Wenn die Operation α unmissverständlich aus dem Kontext hervorgeht, dann nennen wir statt des Paares (X, α) abkürzend die Menge X eine G-Menge.

Beispiel 9F29. Seien X und Y zwei G-Mengen. Wir können $X \cap Y = \emptyset$ annehmen. Dann ist ihre disjunkte Vereinigung $X \sqcup Y$ eine G-Menge.

Beispiel 9F30. Sind X und Y zwei G-Mengen, dann wird ihr Produkt $X \times Y$ eine G-Menge mittels der Operation $g(x,y) = (gx, gy)$.

Ein *Morphismus* zwischen G-Mengen (X, α) und (Y, β) oder kurz *G-Morphismus* ist eine Abbildung $f\colon X \to Y$ sodass $f(gx) = gf(x)$ für alle $x \in X$ und $g \in G$ gilt.

Satz 9F31. *Seien $H, K < G$ endliche Gruppen sodass $HK = G$. Dann haben wir einen natürlichen G-Isomorphismus $\bar{f}\colon G/H \cap K \to G/H \times G/K$.*

BEWEIS. Die Abbildung $f\colon G \to G/H \times G/K$ mit $f(a) = (aH, aK)$ ist offenbar ein G-Homomorphismus. Aus $f(a) = f(b)$ folgt $aH = bH$ und $aK = bK$, also $a^{-1}b = H \cap K$. Übergang zur Quotientenmenge $G/H \cap K$ induziert einen injektiven G-Homomorphismus $\bar{f}\colon G/H \cap K \to G/H \times G/K$ mit $a(H \cap K) \mapsto (aH, aK)$. Lemma 9C5 impliziert $|G : H \cap K| = |G : H| \cdot |G : K|$. Demnach ist $\bar{f}$ nicht nur injektiv sondern auch bijektiv. □

§**9Fe. Transitive Operationen.** Eine Gruppenoperation $\alpha\colon G \times X \to X$ heißt *transitiv* wenn X nur aus einer Ganh besteht. Das heißt es gilt $X = Gx$ für ein $x \in X$, und damit für jedes $x \in X$. Betrachten wir X als G-Menge mittels der Operation α, so nennen wir in diesem Fall die G-Menge X *transitiv*.

Beispiel 9F32. Für jede Untergruppe $H < G$ ist die G-Menge G/H transitiv.

Satz 9F33. *Seien $H, K < G$. Die G-Mengen G/H und G/K sind genau dann isomorph, wenn H und K in G konjugiert sind.*

BEWEIS. Sei $H = gKg^{-1}$ mit $g \in G$ gilt. Dann können wir einen G-Homomorphismen $f\colon G/H \to G/K$ definieren durch $aH \mapsto agK$. Dieser ist wohldefiniert, denn aus $aH = a'H$ folgt $agKg^{-1} = a'gKg^{-1}$, also $agK = a'gK$. Ebenso können wir $f^{-1}\colon G/K \to G/H$ definieren durch $bK \mapsto bg^{-1}K$. Offenbar sind f und f^{-1} zueinander inverse G-Isomorphismen.

Nehmen wir umgekehrt an, es existiert ein G-Isomorphismus $f\colon G/H \xrightarrow{\sim} G/K$. Es gilt $f(H) = gK$ für ein $g \in G$. Für jedes $h \in H$ gilt dann $gK = f(H) = f(hH) = hf(H) = hgK$.

Das bedeutet $g^{-1}hg \in K$ und somit $g^{-1}Hg < K$. Der inverse G-Isomorphismus $f^{-1}\colon G/K \xrightarrow{\sim} G/H$ erfüllt $f^{-1}(K) = g^{-1}H$ und zeigt $gKg^{-1} < H$. Zusammen gilt $gKg^{-1} = H$. □

Bemerkung 9F34. Jede G-Menge X zerfällt in die disjunkte Vereinigung $X = \bigsqcup_{i\in I} X_i$ transitiver G-Mengen X_i, nämlich die Bahnen von X unter der Aktion von G.

Wie in Proposition 9F11 zeigt man nun:

Satz 9F35. *Jede transitive G-Menge ist G-isomorph zu G/G_x für $x \in X$.* □

Korollar 9F36. *Zwei transitive G-Mengen X und Y sind genau dann G-isomorph, wenn die Standgruppen G_x für $x \in X$ und G_y für $y \in Y$ in G konjugiert sind.* □

§9G. Übungen und Ergänzungen

Übung 9G1. Jede Untergruppe $H < G$ vom Index 2 ist normal.

Übung 9G2. Jede normale Untergruppe $H \lhd G$ der Ordnung 2 ist zentral.

Übung 9G3. Sei $G = \{a, b, c\}$ versehen mit der folgenden Verknüpfung:

$\cdot$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

Ist $(G, \cdot)$ eine Gruppe? Ein Monoid? Welche Teilmenge $H \subset G$ sind Gruppen? Gilt hier, wie im Satz von Lagrange, dass die Ordnung $|H|$ die Ordnung $|G|$ teilt? Haben wir hier eine Operation $H \times G \to G$? Man bestimme die Bahnen. Sind sie alle gleich lang?

Übung 9G4. Ist jede Gruppe der Ordnung n isomorph zu $\mathbb{Z}/n\mathbb{Z}$? Und wenn n prim ist?

§**9Ga. Ordnung des Produkts versus Produkt der Ordnungen.** Sei G eine Gruppe und seien $a, b \in G$ zwei kommutierende Elemente. Wir setzen $m = \operatorname{ord}(a)$ und $n = \operatorname{ord}(b)$ und fragen, welche Aussagen über die Ordnung $\operatorname{ord}(ab)$ möglich sind.

Übung 9G5. Man zeige $\operatorname{ord}(ab) \mid \operatorname{kgV}(m,n)$ und finde ein Beispiel mit $\operatorname{ord}(ab) < \operatorname{kgV}(m,n)$.

Übung 9G6. Wenn $G = A \times B$ mit $a \in A$ und $b \in B$, dann gilt $\operatorname{ord}(ab) = \operatorname{kgV}(m,n)$.

Übung 9G7. Wenn $\operatorname{ggT}(m,n) = 1$, dann gilt $\operatorname{ord}(ab) = mn$. *Hinweis:* Bézout und Lagrange.

Übung 9G8. Man folgere hieraus, dass es stets $c \in \langle a, b\rangle$ mit $\operatorname{ord}(c) = \operatorname{kgV}(m,n)$ gibt.

Übung 9G9. Man konstruiere ein nicht-kommutatives Beispiel, wo $\operatorname{ord}(xy)$ nicht mn teilt. Ist $\operatorname{ord}(x) = \operatorname{ord}(y) = 2$ und $\operatorname{ord}(xy) = k$ für jedes $k \geq 1$ möglich?

KAPITEL 10

Symmetrische und alternierende Gruppen

§10A. Die symmetrische Gruppe

Eine *Permutation* einer Menge X ist eine bijektive Abbildung $\sigma\colon X \to X$. Die Bijektivität ist gleichbedeutend mit der Existenz einer Umkehrabbildung $\tau\colon X \to X$ sodass $\sigma\circ\tau = \tau\circ\sigma = \mathrm{id}_X$. Wenn eine solche Umkehrabbildung existiert, dann ist sie eindeutig durch σ bestimmt und wir schreiben sie σ^{-1}.

Die Menge aller Permutationen von X bildet eine Gruppe mit der Komposition $\circ$ als Verknüpfung, definiert durch $(\sigma\circ\tau)(x) = \sigma(\tau(x))$ für alle $x \in X$. Wir nennen dies die *symmetrische Gruppe* von X, geschrieben $\mathrm{Sym}(X)$ oder S_X.

§10Aa. Isomorphismen und Einbettungen. Bevor wir die Untersuchung der symmetrischen Gruppen beginnen, stellen wir zunächst einige einfache Vorbemerkungen voran.

Ist X eine Menge, dann ist die Menge $\mathrm{Abb}(X)$ aller Abbildungen $f\colon X \to X$ ein Monoid mit der Komposition als Verknüpfung. Hierin ist die symmetrische Gruppe $\mathrm{Sym}(X)$ die Gruppe der invertierbaren Elemente.

Proposition 10A1. *Jede Bijektion $f\colon X \xrightarrow{\sim} Y$ zwischen zwei Mengen X und Y induziert einen Monoidisomorphismus $f_*\colon \mathrm{Abb}(X) \xrightarrow{\sim} \mathrm{Abb}(Y)$ und somit einen Gruppenisomorphismus $f_*\colon \mathrm{Sym}(X) \xrightarrow{\sim} \mathrm{Sym}(Y)$ vermöge $f_*(\sigma) = f\circ\sigma\circ f^{-1}$.*

Dies wird durch folgendes Diagramm dargestellt:

$$\begin{array}{ccc} X & \xrightarrow[\cong]{\sigma} & X \\ {\scriptstyle f}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow{\scriptstyle f} \\ Y & \xrightarrow[f\sigma f^{-1}]{\cong} & Y \end{array}$$

BEWEIS. Offenbar ist $f_*\colon \mathrm{Abb}(X) \xrightarrow{\sim} \mathrm{Abb}(Y)$ ein Homomorphismus, denn

$$f_*(\sigma\tau) = f(\sigma\tau)f^{-1} = (f\sigma f^{-1})(f\tau f^{-1}) = f_*(\sigma)f_*(\tau).$$

Ebenso induziert die Umkehrabbildung $f^{-1}\colon Y \to X$ von f einen Homomorphismus $(f^{-1})_*\colon \mathrm{Abb}(Y) \to \mathrm{Abb}(X)$ durch $(f^{-1})_*(\sigma) = f^{-1}\circ\sigma\circ f$, und es gilt $(f^{-1})_* = (f_*)^{-1}$. □

Für jede endliche Menge Y der Kardinalität n existiert eine Bijektion $f\colon X \xrightarrow{\sim} Y$ zwischen $X = \{1,\dots,n\}$ und Y. Statt $\mathrm{Sym}(Y)$ können wir daher $\mathrm{S}_n := \mathrm{Sym}(X)$ betrachten.

Proposition 10A2. *Jede Mengeninklusion $\iota\colon Y \subset Z$ induziert einen injektiven Monoidhomomorphismus $\iota_*\colon \mathrm{Abb}(Y) \hookrightarrow \mathrm{Abb}(Z)$ und somit einen injektiven Gruppenhomomorphismus $\iota_*\colon \mathrm{Sym}(Y) \hookrightarrow \mathrm{Sym}(Z)$ durch die Zuordnung $\sigma \mapsto \tilde{\sigma}$, wobei*

$$\tilde{\sigma}(x) = \begin{cases} \sigma(x) & \text{für } x \in Y, \\ x & \text{für } x \notin Y. \end{cases}$$

Dies wird durch das folgende kommutative Diagramm dargestellt:

$$\begin{array}{ccc} Y & \xrightarrow[\cong]{\sigma} & Y \\ {\scriptstyle\iota}\downarrow & & \downarrow{\scriptstyle\iota} \\ Z & \xrightarrow[\tilde{\sigma}]{\cong} & Z \end{array}$$

BEWEIS. Offenbar ist ι_* injektiv, und es genügt zu zeigen, dass ι_* ein Monoidhomomorphismus ist. Zunächst gilt $\widetilde{\mathrm{id}_Y} = \mathrm{id}_Z$. Für $x \notin Y$ gilt

$$(\tilde{\sigma} \circ \tilde{\tau})(x) = \tilde{\sigma}(\tilde{\tau}(x)) = \tilde{\sigma}(x) = x = \widetilde{\sigma\tau}(x).$$

Für $x \in Y$ gilt

$$(\tilde{\sigma} \circ \tilde{\tau})(x) = \tilde{\sigma}(\tilde{\tau}(x)) = \tilde{\sigma}(\tau(x)) = \sigma(\tau(x)) = (\sigma\tau)(x) = \widetilde{\sigma\tau}(x). \qquad \square$$

Insbesondere für $n \le m$ haben wir eine Inklusion $\iota\colon \{1,\dots,n\} \subset \{1,\dots,m\}$ und somit eine Einbettung $\iota_*\colon \mathrm{S}_n \hookrightarrow \mathrm{S}_m$. Der Bequemlichkeit halber identifizieren wir S_n mittels ι_* mit dem Bild in $\mathfrak{m}$ und betrachten im Folgenden $\mathrm{S}_n \subset \mathrm{S}_m$ als Untergruppe.

§**10Ab. Fixpunkte und Träger.** Sei $\sigma \in \mathrm{S}_X$ eine Permutation der Menge X. Ein *Fixpunkt* von σ ist ein Element $x \in X$ mit $\sigma(x) = x$. Wir bezeichnen die Menge der Fixpunkte mit

$$\mathrm{Fix}(\sigma) := \{x \in X \mid \sigma(x) = x\}.$$

Wir sagen σ *bewegt* $x \in X$ wenn $\sigma(x) \neq x$ gilt. Der *Träger* von σ ist

$$\mathrm{supp}(\sigma) := \{x \in X \mid \sigma(x) \neq x\}.$$

Zwei Permutationen σ und τ heißen *disjunkt* wenn $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \emptyset$.

Proposition 10A3. *Disjunkte Permutationen $\sigma, \tau \in \mathrm{S}_X$ kommutieren.*

BEWEIS. Seien $\sigma, \tau \in \mathrm{S}_X$ disjunkte Permutationen. Wenn $x \in \mathrm{supp}(\sigma)$, dann gilt $\tau(x) = x$, also $\sigma(\tau(x)) = \sigma(x)$. Wegen $\sigma(x) \in \mathrm{supp}(\sigma)$, gilt dann auch $\tau(\sigma(x)) = \sigma(x)$. Symmetrisch hierzu gilt für $x \in \mathrm{supp}(\sigma)$ dann $\tau(\sigma(x)) = \tau(x)$ und $\sigma(\tau(x)) = \tau(x)$. Wenn weder $x \in \mathrm{supp}(\sigma)$ noch $x \in \mathrm{supp}(\tau)$ gilt, dann folgt offenbar $\tau(\sigma(x)) = x$ und $\sigma(\tau(x)) = x$. $\square$

Die Umkehrung gilt natürlich nicht: kommutierende Permutationen müssen nicht disjunkt sein. Zum Beispiel kommutiert jede Permutation mit sich selbst.

Bemerkung 10A4. Wir werden meist nur Permutationen auf *endlichen* Mengen betrachten. Die symmetrische Gruppe S_X ist allerdings auch für unendliche Mengen X interessant und nützlich. Eine Zwischenposition belegt hierbei die Gruppe der *endlichen* Permutationen

$$S_{(X)} = \{ \sigma \in S_X \mid \operatorname{supp}(\sigma) \text{ ist endlich} \},$$

das heißt die Permutationen mit endlichem Träger. Für jede endliche Menge X gilt natürlich $S_X = S_{(X)}$, aber für unendliche Mengen gilt $S_{(X)} \subsetneq S_X$. Für $X = \mathbb{N}$ zum Beispiel besteht $S_{(\mathbb{N})}$ aus allen Bijektionen $\sigma\colon \mathbb{N} \xrightarrow{\sim} \mathbb{N}$ für die es ein $n \in \mathbb{N}$ gibt sodass $\sigma(k) = k$ für alle $k \geq n$ gilt.

Für jedes $n \in \mathbb{N}$ induziert die Inklusion $\{1,\dots,n\} \subset \mathbb{N}$ eine Einbettung $\iota_*\colon S_n \hookrightarrow S_{(\mathbb{N})}$. Wir können somit alle Gruppen $S_1 \subset S_2 \subset S_3 \subset \dots$ als Untergruppen von $S_{(\mathbb{N})}$ auffassen.

Übung 10A5. Ist $S_{(X)}$ eine normale Untergruppe in S_X?

§**10Ac. Schreibweise als Abbildung.** Für jede endliche Menge $X = \{x_1, x_2, \dots, x_n\}$ können wir jede Abbildung $\sigma\colon X \to X$ schreiben als Abbildungstafel

$$\left[\begin{smallmatrix} x_1 & x_2 & \dots & x_n \\ \sigma(x_1) & \sigma(x_2) & \dots & \sigma(x_n) \end{smallmatrix}\right].$$

Wir nehmen hierbei an, dass die Elemente $x_1,\dots,x_n$ verschieden sind, und somit tritt jedes in der ersten Zeile genau einmal auf. Ist σ eine Permutation, dann tritt jedes Element $x_1, x_2, \dots, x_n$ auch in der zweiten Zeile genau einmal auf.

Zur Vereinfachung der Notation betrachten wir zumeist die Menge $X = \{1,2,3,\dots,n\}$. Jede Abbildung $\sigma\colon X \to X$ lässt sich dann schreiben als

$$\left[\begin{smallmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{smallmatrix}\right].$$

Zum Beispiel ist $\sigma = \left[\begin{smallmatrix} 1&2&3&4&5&6&7&8 \\ 4&6&8&3&5&2&1&7 \end{smallmatrix}\right]$ die Permutation $1 \mapsto 4$, $2 \mapsto 6$, $3 \mapsto 8$, $4 \mapsto 3$, $5 \mapsto 5$, $6 \mapsto 2$, $7 \mapsto 1$, $8 \mapsto 7$. Die erste Zeile zählt lediglich die Punkte $1,2,\dots,n$ auf, und kann auch weggelassen werden. Man erhält so die Schreibweise als Liste $\sigma = [4,6,8,3,5,2,1,7]$.

Die Zykelschreibweise für Permutationen, die wir in §10B kennenlernen werden, ist meist noch effizienter und für viele Zwecke praktischer.

§**10Ad. Das Zentrum von S_X.** Sei X eine Menge. Für $i, j \in X$ bezeichnen wir mit $\tau = (i,j)$ die Permutation von X, für die $\tau(i) = \tau(j)$ und $\tau(j) = \tau(i)$ gilt sowie $\tau(k) = \tau(k)$ für alle $k \notin \{i,j\}$. Für $i \neq j$ ist dies die *Transposition* $i \leftrightarrow j$, für $i = j$ ist τ die Identität.

Satz 10A6. *Für jede Menge X mit $|X| \geq 3$ hat die symmetrische Gruppe S_X triviales Zentrum, $Z(S_X) = \{\mathrm{id}_X\}$. Gleiches gilt im Falle einer unendlichen Menge X auch für $S_{(X)}$.*

BEWEIS. Für jedes $\sigma \in S_X$ mit $\sigma \neq \mathrm{id}_X$ existiert $i \in X$ mit $\sigma(i) \neq i$. Sei $j := \sigma(i)$ und $k \in X \smallsetminus \{i,j\}$. Für $\tau = (j,k)$ gilt $\tau\sigma\tau^{-1} \neq \sigma$, denn $(\tau\sigma\tau^{-1})(i) = k$. □

Wie so oft bilden die kleinen Gruppen Ausnahmen: Die Gruppe S_2 ist von Ordnung 2, also isomorph zu $\mathbb{Z}/2\mathbb{Z}$. Insbesondere ist das Zentrum $Z(S_2) = S_2$ nicht trivial.

§**10Ae. Ordnung der Gruppe S_n.** Für jede endliche Menge X ist auch die symmetrische Gruppe S_X endlich, und es ist nicht schwer, ihre Ordnung zu bestimmen.

Hierzu dient folgende nützliche Beobachtung:

Proposition 10A7. *Jede Permutation $\sigma \in \mathrm{S}_n$ schreibt sich eindeutig als Produkt*

$$\sigma = (n,i_n)(n-1,i_{n-1})\cdots(3,i_3)(2,i_2)(1,i_1) \qquad \textit{mit } 1 \le i_k \le k \textit{ für alle } k.$$

BEWEIS. *Existenz:* Wir führen Induktion über n. Für $n = 1$ ist die Aussage klar. Sei nun $n \ge 2$. Für $\sigma \in \mathrm{S}_n$ sei $i_n = \sigma(n)$ mit $1 \le i_n \le n$. Für $\sigma' = (n,i_n)\sigma$ gilt dann $\sigma'(n) = n$, also $\mathrm{supp}(\sigma') \subset \{1,\dots,n-1\}$. Für $\sigma' \in \mathrm{S}_{n-1}$ gilt nach Induktionsvoraussetzung gilt

$$\sigma' = (n-1,i_{n-1})\cdots(3,i_3)(2,i_2)(1,i_1),$$

mit $1 \le i_k \le k$ für alle k. Daraus erhalten wir schließlich

$$\sigma = (n,i_n)(n-1,i_{n-1})\cdots(3,i_3)(2,i_2)(1,i_1).$$

Eindeutigkeit: Für $n = 1$ ist die Aussage klar. Sei nun $n \ge 2$. Angenommen es gilt

$$(n,i_n)(n-1,i_{n-1})\cdots(3,i_3)(2,i_2)(1,i_1) = (n,j_n)(n-1,j_{n-1})\cdots(3,j_3)(2,j_2)(1,j_1)$$

mit $1 \le i_k, j_k \le k$ für alle k. Links gilt $n \mapsto i_n$, rechts gilt $n \mapsto j_n$, also $i_n = j_n$. Multiplikation von links mit (n,i_n) löscht links wie rechts den ersten Faktor:

$$(n-1,i_{n-1})\cdots(3,i_3)(2,i_2)(1,i_1) = (n-1,j_{n-1})\cdots(3,j_3)(2,j_2)(1,j_1)$$

Nach Induktionsvoraussetzung gilt dann $i_k = j_k$ für alle k. □

Korollar 10A8. *Für alle $n \in \mathbb{N}$ gilt $|\mathrm{S}_n| = n!$.* □

Korollar 10A9. *Die symmetrische Gruppe S_n wird von ihren Transpositionen erzeugt.* □

Die Gruppe S_n wird schon von den Transpositionen benachbarter Elemente erzeugt:

Korollar 10A10. *Es gilt $\mathrm{S}_n = \langle (1,2),(2,3),\dots,(n-1,n)\rangle$.*

Dies folgt aus obiger Proposition nach kurzer Rechnung: Für $i < j$ gilt nämlich

$$(i,j) = (i,i+1)(i+1,i+2)\cdots(j-2,j-1)(j,j-1)(j-1,j-2)\cdots(i+2,i+1)(i+1,i).$$

Übung 10A11. Es gilt $\mathrm{S}_n = \langle (1,2),(1,3),\dots,(1,n)\rangle$.

§10B. Zykelzerlegung

§**10Ba. Zykel.** Sei X eine Menge. Für $\ell \ge 2$ verschiedene Elemente $i_1,i_2,\dots,i_\ell \in X$ bezeichnen wir mit $\sigma = (i_1,i_2,\dots,i_\ell)$ die Permutation $\sigma \in \mathrm{S}_X$ definiert durch $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, …, $\sigma(i_\ell) = i_1$ sowie $\sigma(k) = k$ für alle $k \in X \smallsetminus \{i_1,i_2,\dots,i_\ell\}$. Dies nennen wir einen *Zykel der Länge ℓ* oder kurz einen *ℓ-Zykel*.

Bemerkung 10B1. Die Ordnung des ℓ-Zykels $\sigma = (i_1,i_2,\dots,i_\ell)$ ist $\mathrm{ord}(\sigma) = \ell$. Demnach gilt $\langle\sigma\rangle = \{\mathrm{id}_X,\sigma,\dots,\sigma^{\ell-1}\}$. Der Träger von σ ist die Menge $\{i_1,i_2,\dots,i_\ell\}$. Dies ist einzige nicht-triviale Bahn von X unter der Aktion von $\langle\sigma\rangle$.

Im Sonderfall $\ell = 1$ wäre i_1 ein Fixpunkt, also $\{i_1\}$ eine Bahn der Länge 1, und $\sigma = \mathrm{id}_X$. Dies betrachten wir *nicht* als einen Zykel.

Man beachte, dass für $\ell \ge 3$ der Träger den Zykel noch nicht eindeutig festlegt. Zum Beispiel ist $(1,2,3) \ne (1,3,2)$ obwohl beide Permutationen Träger $\{1,2,3\}$ haben.

Bemerkung 10B2. Wir können jeden ℓ-Zykel $(i_1, i_2, \dots, i_\ell)$ auf genau ℓ verschiedene Arten niederschreiben: diese entstehend durch zyklische Rotation

$$(i_1, i_2, \dots, i_\ell) = (i_2, \dots, i_\ell, i_1) = \cdots = (i_\ell, i_1, \dots, i_{\ell-1}).$$

Die Wahl des zuerst geschriebenen Elements i_k ist dabei willkürlich: Sie entspricht der Wahl eines Repräsentanten der Bahn $\{i_1, i_2, \dots, i_\ell\}$. Haben wir ein i aus dieser Bahn gewählt, so sind $i, \sigma(i), \sigma^2(i), \dots, \sigma^{\ell-1}(i)$ alle Elemente der Bahn und der Zykel schreibt sich als $\sigma = (i, \sigma(i), \sigma^2(i), \dots, \sigma^{\ell-1}(i))$

§**10Bb. Zykelzerlegung.** Zykel bieten sich als praktische Schreibweise für Permutationen an. Für jede endliche Permutation ist folgende Feststellung ungemein nützlich:

Satz 10B3. *Jede endliche Permutation $\sigma \in \mathrm{S}_{(X)}$ schreibt sich als Produkt $\sigma = c_1 c_2 \cdots c_k$ disjunkter Zykel $c_1, c_2, \dots, c_k$. Diese Schreibweise ist eindeutig bis auf die Reihenfolge.*

Beispiel 10B4. Es gilt

$$\left[\begin{smallmatrix} 1&2&3&4&5&6&7&8 \\ 4&6&8&3&5&2&1&7 \end{smallmatrix}\right] = (1,4,3,8,7)(2,6).$$

Der Fixpunkt $5 \mapsto 5$ wird in der Zykelschreibweise nicht explizit aufgeführt.

Ausführlicher bedeutet die Eindeutigkeit folgendes: Gilt $\sigma = c_1 c_2 \cdots c_k$ mit disjunkten Zykeln $c_1, c_2, \dots, c_k$ und auch $\sigma = c'_1 c'_2 \cdots c'_{k'}$ mit disjunkten Zykeln $c'_1, c'_2, \dots, c'_{k'}$, dann gilt $k = k'$ und $\{c_1, c_2, \dots, c_k\} = \{c'_1, c'_2, \dots, c'_{k'}\}$. Die so definierte Menge $\{c_1, c_2, \dots, c_k\}$ nennen wir die Zykelzerlegung von σ. (Etwas laxer aber kürzer nennt man auch die Produktschreibweise $\sigma = c_1 c_2 \cdots c_k$ die Zykelzerlegung von σ.) Für die Zykelzerlegung gilt

$$\operatorname{supp}(\sigma) = \operatorname{supp}(c_1) \sqcup \operatorname{supp}(c_2) \sqcup \cdots \sqcup \operatorname{supp}(c_k).$$

Hieraus ergibt sich die Bahnenzerlegung der Menge X unter der Aktion der Gruppe $\langle\sigma\rangle$:

$$X = \operatorname{Fix}(\sigma) \sqcup \operatorname{supp}(c_1) \sqcup \operatorname{supp}(c_2) \sqcup \cdots \sqcup \operatorname{supp}(c_k).$$

BEWEIS. *Existenz:* Induktion über $n = |\operatorname{supp}(\sigma)|$. Für $n = 0$ gilt $\sigma = \mathrm{id}_X$ und das leere Produkt erfüllt das Gewünschte. Für $n \geq 1$ existiert ein $i \in X$ mit $\sigma(i) \neq i$. Es existiert $\ell \geq 1$ mit $\sigma^\ell(i) = i$, und wir wählen ℓ minimal. Dann besteht die Bahn I von i unter der Aktion von $\langle\sigma\rangle$ aus den ℓ verschiedenen Elementen $i, \sigma(i), \dots, \sigma^{\ell-1}(i)$. Wir setzen $c_1 = (i, \sigma(i), \dots, \sigma^{\ell-1}(i))$. Dann erfüllt $\tau = c_1^{-1}\sigma$ die Bedingung $\tau|_I = \mathrm{id}_I$ und $\tau(x) = \sigma(x)$ für alle $x \in X \smallsetminus I$. Insbesondere gilt also $\operatorname{supp}(\tau) = \operatorname{supp}(\sigma) \smallsetminus I$, und nach Induktionsannahme gilt $\tau = c_2 \dots c_k$ mit disjunkten Zykeln $c_2, \dots, c_k$.

Eindeutigkeit: Seien $\sigma = c_1 c_2 \cdots c_k$ und $\sigma = c'_1 c'_2 \cdots c'_{k'}$ zwei Zerlegungen in disjunkte Zykel. Wir haben $k = k'$ und $\{c_1, c_2, \dots, c_k\} = \{c'_1, c'_2, \dots, c'_{k'}\}$ zu zeigen. Wir können $k \leq k'$ annehmen. Für $k = 0$ ist $\sigma = \mathrm{id}_X$ und die Aussage ist klar. Sei $k \geq 1$ und $i \in \operatorname{supp}(c_1)$. Dann existiert c'_ν mit $i \in \operatorname{supp}(c'_\nu)$. Nach Umordnung können wir $\nu = 1$ annehmen. Da c_1, c'_1 von den anderen Zykeln disjunkt sind, gilt $\sigma^\ell(i) = c_1^\ell(i) = {c'_1}^\ell(i)$ für alle $\ell \in \mathbb{Z}$, und somit $c_1 = c'_1$. Multiplikation mit c_1^{-1} reduziert beide Produkte um einen Faktor, und nach Induktionsvoraussetzung gilt dann $\{c_2, \dots, c_k\} = \{c'_2, \dots, c'_{k'}\}$. □

Proposition 10B5. *Jeder ℓ-Zykel schreibt sich als Produkt von $\ell - 1$ Transpositionen, nämlich*

$$(i_1, i_2, \dots, i_\ell) = (i_1, i_2)(i_2, i_3) \cdots (i_{\ell-1}, i_\ell).$$

Daraus folgt: Jede endliche Permutation schreibt sich als Produkt von Transpositionen. □

Bemerkung 10B6. Ist X eine unendliche Menge, dann kann man eine Zykelzerlegung für beliebige Permutationen $\sigma\colon X \to X$ definieren selbst wenn der Träger von σ nicht endlich ist. Wenn X in endlich viele nicht-triviale Bahnen zerfällt, dann gilt obiger Satz wie bisher: Man muss lediglich noch unendliche Zykel zulassen von der Form

$$(\ldots, \sigma^{-2}(i), \sigma^{-1}(i), i, \sigma(i), \sigma^2(i), \ldots).$$

Wenn X unter der Aktion von σ in unendlich viele nicht-triviale Bahnen $(X_\lambda)_{\lambda\in\Lambda}$ zerfällt, dann schreibt sich σ als ein unendliches Produkt $\prod_{\lambda\in\Lambda} c_\lambda$ disjunkter Zykel $c_\lambda \in \mathrm{S}_X$. Da die Träger disjunkt sind, ist solch ein Produkt wohldefiniert als die Abbildung $x \mapsto c_\lambda(x)$ falls es ein $\lambda \in \Lambda$ gibt mit $x \in \operatorname{supp}(c_\lambda)$, und andernfalls $x \mapsto x$.

Übung 10B7. Sei X eine unendliche Menge und sei $E \subset \mathrm{S}_X$ die Menge aller Permutationen mit nur endlich vielen nicht-trivialenen Bahnen. Ist E eine Untergruppe von S_X?

§**10Bc. Die Ordnung einer Permutation.** Sei $\sigma = c_1 c_2 \ldots c_r$ in $\mathrm{S}_{(X)}$ ein Produkt disjunkter Zykel $c_1, c_2, \ldots, c_r$ der Längen $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_r \geq 2$. (Dies können wir durch Umordnung stets erreichen.) Dann ist $(\ell_1, \ell_2, \ldots, \ell_r) \in \mathbb{N}^r$ eindeutig durch σ bestimmt und heißt die *Zykelstruktur* von σ.

Proposition 10B8. *Hat $\sigma \in \mathrm{S}_{(X)}$ die Zykelstruktur $(\ell_1, \ell_2, \ldots, \ell_r)$, dann gilt*

$$\operatorname{ord}(\sigma) = \operatorname{kgV}(\ell_1, \ell_2, \ldots, \ell_r).$$

BEWEIS. Aus der Zykelzerlegung $\sigma = c_1 \cdots c_r$ folgt $\sigma^k = c_1^k \cdots c_r^k$ für alle $k \in \mathbb{Z}$. Es gilt $\sigma^k = \mathrm{id}$ genau dann wenn $c_1^k = \cdots = c_r^k = \mathrm{id}$. Letzteres ist genau dann der Fall, wenn k ein gemeinsames Vielfaches der Ordnungen $\operatorname{ord}(c_1) = \ell_1$, …, $\operatorname{ord}(c_r) = \ell_r$ ist. □

Beispiel 10B9. Die Permutationen der Ordnung 2 sind genau von der Form

$$(i_1, j_1) \text{ oder } (i_1, j_1)(i_2, j_2) \text{ oder } (i_1, j_1)(i_2, j_2)(i_3, j_3)\ldots$$

Übung 10B10. Man beweise folgende Aussagen und setzte die Reihe fort:
In S_3 gibt es Elemente der Ordnung $1, 2, 3$, aber keine weiteren Ordnungen.
In S_4 gibt es Elemente der Ordnung $1, 2, 3, 4$, aber keine weiteren Ordnungen.
In S_5 gibt es Elemente der Ordnung $1, 2, 3, 4, 5, 6$, aber keine weiteren Ordnungen.
In S_6 gibt es Elemente der Ordnung $1, 2, 3, 4, 5, 6$, aber keine weiteren Ordnungen.
In S_7 gibt es Elemente der Ordnung $1, 2, 3, 4, 5, 6, 7, 10, 12$, aber keine weiteren Ordnungen.

§**10Bd. Konjugationsklassen.** Wir beginnen mit folgender Beobachtung:

Lemma 10B11. *Für jeden Zykel $c = (i_1, i_2, \ldots, i_\ell) \in \mathrm{S}_{(X)}$ und $\tau \in \mathrm{S}_X$ gilt*

$$\tau \circ c \circ \tau^{-1} = (\tau(i_1), \tau(i_2), \ldots, \tau(i_\ell))$$

Das bedeutet, für $\sigma \in \mathrm{S}_{(X)}$ und $\tau \in \mathrm{S}_X$ ändert die Konjugation $\sigma \mapsto \tau \circ \sigma \circ \tau$ eventuell die Zykel aber nicht die Zykelstruktur. Hiervon gilt folgende Umkehrung:

Satz 10B12. *Zwei Permutationen $\sigma, \sigma' \in \mathrm{S}_{(X)}$ sind genau dann konjugiert in $\mathrm{S}_{(X)}$ wenn sie dieselbe Zykelstruktur haben.*

BEWEIS. Wenn σ, σ' dieselbe Zykelstruktur $(\ell_1, \ell_2, \ldots, \ell_r) \in \mathbb{N}^r$ haben, dann wollen wir $\tau \in \mathrm{S}_{(X)}$ konstruieren, sodass $\tau\sigma\tau^{-1} = \sigma'$ gilt. Wir können beide Permutationen σ und

σ' wie folgt niederschreiben und in Beziehung setzen:

$$\begin{aligned}\sigma &= (i_{1,1}, i_{1,2}, \dots, i_{1,\ell_1})(i_{2,1}, i_{2,2}, \dots, i_{2,\ell_2}) \cdots (i_{r,1}, i_{r,2}, \dots, i_{r,\ell_r}) \\ \sigma' &= (i'_{1,1}, i'_{1,2}, \dots, i'_{1,\ell_1})(i'_{2,1}, i'_{2,2}, \dots, i'_{2,\ell_2}) \cdots (i'_{r,1}, i'_{r,2}, \dots, i'_{r,\ell_r})\end{aligned} \tag{10.1}$$

Die Elemente in der ersten Zeile sind untereinander verschieden, ebenso die Elemente der zweiten Zeile. Es existiert also eine Permutation $\tau \in \mathrm{S}_{(X)}$ mit $i_{1,1} \mapsto i'_{1,1}$, …, $i_{r,\ell_r} \mapsto i'_{r,\ell_r}$, da sich alles auf der endlichen Teilmenge $\{i_{1,1}, \dots, i_{r,\ell_r}, i'_{1,1}, \dots, i'_{r,\ell_r}\}$ abspielt. Nach obigem Lemma 10B11 erfüllt τ die gewünschte Bedingung $\tau\sigma\tau^{-1} = \sigma'$. □

§**10Be. Ordnung des Zentralisators.** Für den Fall einer endlichen Menge X wollen wir die bisherigen Ergebnisse präzisieren, indem wir zu $\sigma \in \mathrm{S}_X$ die Ordnung des Zentralisators und die Elementezahl der Konjugationsklassen in S_X bestimmen:

Ist $\sigma = c_1 c_2 \dots c_r$ ein Produkt disjunkter Zykel $c_1, c_2, \dots, c_r$ der Längen $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_r \geq 2$, dann nennen wir $(\ell_1, \ell_2, \dots, \ell_r) \in \mathbb{N}^r$ die *Zykelstruktur* von σ. Verlängern wir dies um die Fixpunkte durch $\ell_{r+1} = \cdots = \ell_s = 1$, so erhalten wir die *Bahnenstruktur* $(\ell_1, \ell_2, \dots, \ell_s) \in \mathbb{N}^s$. Diese ist eine Partition von $n = |X|$, das heißt es gilt

$$n = \ell_1 + \ell_2 + \cdots + \ell_s \quad \text{mit} \quad \ell_1 \geq \ell_2 \geq \cdots \geq \ell_s \geq 1.$$

Bahnen- und Zykelstruktur lassen sich leicht ineinander umrechnen wenn X endlich ist und die Anzahl $|X|$ der Elemente gegeben ist. Wir betrachten zur Vereinfachung $X = \{1, 2, \dots, n\}$.

Satz 10B13. *Sei $\sigma \in \mathrm{S}_n$. Angenommen, in der Bahnenzerlegung von σ treten m_ℓ Bahnen der Länge ℓ auf. Dann hat der Zentralisator von σ die Ordnung*

$$|Z_{\mathrm{S}_n}(\sigma)| = m_1! \cdot m_2! 2^{m_1} \cdot m_3! 3^{m_3} \cdots m_n! n^{m_n}.$$

Die Konjugationsklasse von σ hat demnach die Ordnung

$$\left|\sigma^{\mathrm{S}_n}\right| = \frac{n!}{m_1! \cdot m_2! 2^{m_1} \cdot m_3! 3^{m_3} \cdots m_n! n^{m_n}}.$$

BEWEIS. Für die Konjugation $\sigma' = \tau\sigma\tau^{-1}$ mit einer Permutation $\tau \in \mathrm{S}_n$ überführt die Zykelschreibweise von σ in die Zykelschreibweise von σ', das heißt

$$\begin{aligned}\sigma &= (i_{1,1}, i_{1,2}, \dots, i_{1,\ell_1})(i_{2,1}, i_{2,2}, \dots, i_{2,\ell_2}) \cdots (i_{s,1}, i_{s,2}, \dots, i_{s,\ell_s}), \\ \sigma' &= (i'_{1,1}, i'_{1,2}, \dots, i'_{1,\ell_1})(i'_{2,1}, i'_{2,2}, \dots, i'_{2,\ell_2}) \cdots (i'_{s,1}, i'_{s,2}, \dots, i'_{s,\ell_s}),\end{aligned} \tag{10.2}$$

mit $i'_{\mu,\nu} = \tau(i_{\mu,\nu})$. Die Zykelschreibweise denken wir uns hierbei verlängert um die Fixpunkte durch Anhängen von $(i_{r+1,1}) \cdots (i_{s,1})$ bzw. $(i'_{r+1,1}) \cdots (i'_{s,1})$. Dies hat den Vorteil, dass jedes Element von $X = \{1, \dots, n\}$ in der ersten Zeile genau einmal auftritt, und ebenso in der zweiten Zeile genau einmal auftritt. Die Korrespondenz $i_{\mu,\nu} \mapsto i'_{\mu,\nu}$ legt somit τ eindeutig fest.

Der Zentralisator $Z_{\mathrm{S}_n}(\sigma)$ besteht nun aus allen Permutationen $\tau \in \mathrm{S}_n$ mit $\tau\sigma\tau^{-1} = \sigma$. In (10.2) soll also $\sigma' = \sigma$ gelten. Aufgrund der Eindeutigkeit der Zykelzerlegung gibt es hierbei für τ nur folgende Möglichkeiten:

1. Die ℓ-Zykel können untereinander vertauscht werden, und zwar auf $m_\ell!$ Arten.
2. Jeder ℓ-Zykel kann in sich rotiert werden, auf ℓ Weisen (siehe 10B2).

Da diese Transformationen untereinander unabhängig sind, lassen sich die ℓ-Zykel von σ auf genau $m_\ell!\ell^{m_\ell}$ verschiedene Arten niederschreiben. Zykel verschiedener Länge interferieren nicht, und so sind die Wahlen für verschiedene ℓ voneinander unabhängig.

Die Anzahl der Elemente in der Konjugationsklasse ergibt sich hieraus mit Hilfe der Bahnengleichung, in diesem Fall $|S_n| = \left|\sigma^{\mathrm{S}_n}\right| \cdot |Z_{\mathrm{S}_n}(\sigma)|$. □

§10C. Die Signatur

§10Ca. Existenz und Eindeutigkeit. Wir beginnen mit einer einfachen Beobachtung:

Lemma 10C1. *Sei $(A,\cdot)$ eine abelsche Gruppe. Stimmen zwei Gruppenhomomorphismen $f,g\colon \mathrm{S}_{(X)} \to A$ auf einer Transposition überein, dann folgt $f = g$.*

BEWEIS. Für jede Permutation $\sigma \in \mathrm{S}_{(X)}$ und $i,j \in X$ gilt

$$f(\sigma\circ(i,j)\circ\sigma^{-1}) = f(\sigma)\cdot f(i,j)\cdot f(\sigma)^{-1} = f(i,j),$$
$$g(\sigma\circ(i,j)\circ\sigma^{-1}) = g(\sigma)\cdot g(i,j)\cdot g(\sigma)^{-1} = g(i,j). \quad \square$$

Da alle Transpositionen in $S_{(X)}$ konjugiert sind, stimmen f und g auf allen Transpositionen überein. Da $\mathrm{S}_{(X)}$ von den Transpositionen erzeugt wird, stimmen h und g auf S_n überein. □

Wie steht es nun mit der Existenz von Gruppenhomomorphismen $f\colon \mathrm{S}_{(X)} \to A$ in eine abelsche Gruppe A? Da die Transposition $(1,2)$ Ordnung 2 hat, muss $a = f(1,2)$ Ordnung 1 oder 2 haben, und somit liegt das Bild $f(\mathrm{S}_{(X)})$ in der zweielementigen Untergruppe $\{1,a\}$. Für abelsche gruppen reicht es demnach, zweielementige Gruppen zu betrachten.

Wir betrachten hierzu die multiplikativ geschrieben Gruppe $\mathbb{Z}^\times = \{\pm 1\}$.

Satz 10C2. *Für jede natürliche Zahl $n \geq 2$ existiert genau ein nicht-trivialer Gruppenhomomorphismus $\mathrm{S}_n \to \{\pm 1\}$. Diesen nennen wir die* Signatur*, geschrieben* $\mathrm{sign}\colon \mathrm{S}_n \to \{\pm 1\}$.

BEWEIS. *Existenz:* Für $\sigma \in \mathrm{S}_n$ definieren wir

$$\mathrm{sign}(\sigma) := \prod_{i<j} \tfrac{\sigma(j)-\sigma(i)}{j-i}.$$

Jede Differenz $j-i$ des Nenners tritt auch irgendwann im Zähler auf, eventuell mit umgekehrten Vorzeichen. Das Ergebnis ist demnach $+1$ oder -1. Offenbar gilt $\mathrm{sign}(\mathrm{id}) = 1$. Zudem gilt $\mathrm{sign}(1,2) = -1$, denn in diesem Fall hat nur der Term $\frac{1-2}{2-1}$ negatives Vorzeichen.

Es bleibt zu zeigen, dass sign ein Homomorphismus ist:

$$\mathrm{sign}(\tau\circ\sigma) = \prod_{i<j} \tfrac{\tau(\sigma(j))-\tau(\sigma(i))}{j-i} = \Big(\prod_{i<j} \tfrac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}\Big)\Big(\prod_{i<j} \tfrac{\sigma(j)-\sigma(i)}{j-i}\Big)$$

Das letzte Produkt ist $\operatorname{sign}(\sigma)$, das vorletzte ist $\operatorname{sign}(\tau)$, denn

$$\begin{aligned}\prod_{i<j}\tfrac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} &= \prod_{\substack{i<j\\ \sigma(i)<\sigma(j)}}\tfrac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}\cdot\prod_{\substack{i<j\\ \sigma(i)>\sigma(j)}}\tfrac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}\\ &= \prod_{\substack{i<j\\ \sigma(i)<\sigma(j)}}\tfrac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}\cdot\prod_{\substack{i>j\\ \sigma(i)<\sigma(j)}}\tfrac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}\\ &= \prod_{\sigma(i)<\sigma(j)}\tfrac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} = \prod_{i<j}\tfrac{\tau(j)-\tau(i)}{j-i}.\end{aligned}$$

Eindeutigkeit: Die Eindeutigkeit folgt aus dem vorangegangenen Lemma. Für jeden Gruppenhomomorphismus $f\colon \mathrm{S}_n \to \{\pm 1\}$ bestehen nämlich nur zwei Möglichkeiten: Wenn $f(1,2)=1$, dann ist f trivial. Wenn $f(1,2)=-1$, dann folgt $f=\operatorname{sign}$. □

§**10Cb. Natürlichkeit.** Statt Permutationen der Menge $X=\{1,\dots,n\}$ kann man auch Permutationen einer beliebigen Menge Y mit n Elementen betrachten. Gemäß 10A1 induziert jede Bijektion $f\colon X \xrightarrow{\sim} Y$ einen Gruppenisomorphismus $f_*\colon \mathrm{S}_X \xrightarrow{\sim} \mathrm{S}_Y$, und aus $|\operatorname{Hom}(\mathrm{S}_X,\{\pm1\})|=2$ folgt dann natürlich $|\operatorname{Hom}(\mathrm{S}_Y,\{\pm1\})|=2$.

Definition 10C3. Für jede endliche Menge X mit mindestens zwei Elementen existiert genau ein nicht-trivialer Gruppenhomomorphismus $\operatorname{sign}_X\colon \mathrm{S}_X \to \{\pm1\}$. Diesen nennen wir die *Signatur*. Für einelementige Mengen nennen wir auch $\operatorname{sign}_X\colon \mathrm{S}_X \xrightarrow{\sim} \{1\}$ die Signatur.

Wenn die Menge X aus dem Kontext klar ist, so unterlässt man ihre explizite Nennung und schreibt statt sign_X kurz sign. Dies wird durch folgende Beobachtung gerechtfertigt:

Proposition 10C4. *Die Signatur ist in folgendem Sinne natürlich:*

- *Jede Bijektion $f\colon X \xrightarrow{\sim} Y$ endlicher Mengen induziert einen Gruppenisomorphismus $f_*\colon \mathrm{S}_X \xrightarrow{\sim} \mathrm{S}_Y$ vermöge $f_*(\sigma) = f\circ\sigma\circ f^{-1}$ und es gilt $\operatorname{sign}_X = \operatorname{sign}_Y \circ f_*$.*
- *Jede Inklusion $\iota\colon Y \subset Z$ endlicher Mengen induziert einen injektiven Gruppenhomomorphismus $\iota_*\colon \mathrm{S}_Y \hookrightarrow \mathrm{S}_Z$ wie in 10A2 und es gilt $\operatorname{sign}_Y = \operatorname{sign}_Z \circ \iota_*$.* □

Dies wird durch das folgende kommutative Diagramm dargestellt:

$$X \xrightarrow[\cong]{f} Y \xhookrightarrow{\iota} Z$$

$$\begin{array}{ccccc} \mathrm{S}_X & \xrightarrow[\cong]{f_*} & \mathrm{S}_Y & \xhookrightarrow{\iota_*} & \mathrm{S}_Z \\ & \searrow^{\operatorname{sign}_X} & \downarrow{\scriptstyle \operatorname{sign}_Y} & \swarrow_{\operatorname{sign}_Z} & \\ & & \{\pm1\} & & \end{array}$$

Die Signatur erstreckt sich auch auf *endliche* Permutationen einer unendlichen Menge:

Korollar 10C5. *Für jede Menge X existiert genau ein nicht-trivialer Gruppenhomomorphismus $\mathrm{S}_{(X)} \to \{\pm1\}$. Diesen nennen wir die* Signatur, *geschrieben* $\operatorname{sign}\colon \mathrm{S}_{(X)} \to \{\pm1\}$.

BEWEIS. Die Eindeutigkeit folgt wie oben, denn $\mathrm{S}_{(X)}$ wird von Transpositionen erzeugt, und diese sind untereinander in $\mathrm{S}_{(X)}$ konjugiert. Um die Existenz nachzuweisen definiert man $\operatorname{sign}\colon \mathrm{S}_{(X)} \to \{\pm 1\}$ wie folgt: Für $\sigma \in \mathrm{S}_{(X)}$ ist $\operatorname{supp}(\sigma)$ in einer endlichen Teilmenge $Y \subset X$ enthalten, also können wir $\operatorname{sign}(\sigma) := \operatorname{sign}_Y(\sigma|_Y)$ definieren. Die Natürlichkeit stellt sicher, dass $\operatorname{sign}(\sigma)$ wohldefiniert ist, das heißt unabhängig von der Wahl von Y. Für je zwei Permutationen $\sigma, \tau \in \mathrm{S}_{(X)}$ liegen beide Träger in einer endlichen Menge Y, also gilt $\operatorname{sign}(\sigma \circ \tau) = \operatorname{sign}_Y(\sigma|_Y \circ \tau|_Y) = \operatorname{sign}_Y(\sigma|_Y)\operatorname{sign}_Y(\tau|_Y) = \operatorname{sign}(\sigma)\operatorname{sign}(\tau)$. □

§**10Cc. Effiziente Berechnung.** Sei X eine endliche Menge. Der Signaturhomomorphismus $\operatorname{sign}\colon \mathrm{S}_X \to \{\pm 1\}$ ordnet jeder Transposition $\tau = (i, j)$ den Wert $\operatorname{sign}(\tau) = -1$ zu. Wenn sich $\sigma \in \mathrm{S}_X$ als Produkt von ℓ Transpositionen schreiben lässt, dann gilt $\operatorname{sign}(\sigma) = (-1)^\ell$. Die Anzahl ℓ der hierzu verwendeten Transposition ist natürlich nicht eindeutig, lediglich die Parität $\ell \mod 2$ ist wohldefiniert.

Definition 10C6. Sei X eine endliche Menge. Permutationen $\sigma \in \mathrm{S}_X$ mit $\operatorname{sign}(\sigma) = +1$ nennt man *gerade*, Permutationen mit $\operatorname{sign}(\sigma) = -1$ nennt man *ungerade*.

Bemerkung 10C7. Jeder ℓ-Zykel $\sigma = (i_1, i_2, \ldots, i_\ell)$ schreibt sich als Produkt von $\ell - 1$ Transpositionen (10B5), also gilt $\operatorname{sign}(\sigma) = (-1)^{\ell-1}$. Damit lässt sich aus der Zykelzerlegung (10B3) die Signatur sehr effizient berechnen: Hat σ die Zykelstruktur $(\ell_1, \ldots, \ell_r)$ dann gilt $\operatorname{sign}(\sigma) = (-1)^{\ell_1 - 1} \cdots (-1)^{\ell_r - 1} = (-1)^{|\operatorname{supp}(\sigma) - r|}$.

§**10Cd. Universelle Eigenschaft.** Statt der multiplikativen Schreibweise der Gruppe $(\{\pm 1\}, \cdot)$ ist manchmal die additive Schreibweise der Gruppe $\mathbb{Z}/_2 = \{0, 1\}$ bequemer, wobei $0+0 = 1+1 = 0$ und $1+0 = 0+1 = 1$. Den Signaturhomomorphismus schreiben wir dann als $\varepsilon\colon \mathrm{S}_{(X)} \to \mathbb{Z}/_2$, sodass $\operatorname{sign}(\sigma) = (-1)^{\varepsilon(\sigma)}$. Für jede Gruppe $(A, \cdot)$ und jedes Element $a \in A$ mit $a^2 = 1$ ist die Abbildung $h_a\colon \mathrm{S}_{(X)} \to A$ mit $\sigma \mapsto a^{\varepsilon(\sigma)}$ ein Gruppenhomomorphismus.

Korollar 10C8 (Universelle Eigenschaft der Signatur)**.** *Jeder Homomorphismus $h\colon \mathrm{S}_{(X)} \to A$ in eine abelsche Gruppe A ist von der Form $h(\sigma) = a^{\varepsilon(\sigma)}$ für ein $a \in A$ mit $a^2 = 1$.* □

Übung 10C9. Sei X eine endliche Menge mit $n \geq 2$ Elementen. Dann existieren genau drei Monoidhomomorphismen $\operatorname{Abb}(X) \to (\mathbb{Z}, \cdot)$:

1. Der triviale Homomorphismus $\operatorname{Abb}(X) \to \{1\}$ mit $f \mapsto 1$ für alle $f \in \operatorname{Abb}(X)$.
2. Die Abbildung $\operatorname{Abb}(X) \to \{0, 1\}$ mit $f \mapsto 1$ für $f \in \mathrm{S}_X$ und $f \mapsto 0$ sonst.
3. Die Abbildung $\operatorname{Abb}(X) \to \{-1, 0, 1\}$ mit $f \mapsto \operatorname{sign}(f)$ für $f \in \mathrm{S}_X$ und $f \mapsto 0$ sonst.

Auch den letztgenannten Homomorphismus nennen wir Signatur $\operatorname{sign}\colon \operatorname{Abb}(X) \to \{\pm 1, 0\}$. Im Falle $X = \{1, \ldots, n\}$ lässt sie sich charakterisieren durch $\operatorname{sign}(f) = \prod_{i<j} \frac{f(j)-f(i)}{j-i}$. Hat auch diese erweiterte Signatur die oben genannten Eigenschaften?

§10D. Die alternierende Gruppe

Sei X eine endliche Menge. Wir nennen den Kern des Signaturhomomorphismus

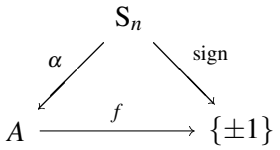
$$\mathrm{A}_X := \operatorname{Alt}(X) := \ker(\operatorname{sign}\colon \mathrm{S}_X \to \{\pm 1\})$$

die *alternierende Gruppe* auf X. Diese besteht aus allen geraden Permutationen von X. Für $n \in \mathbb{N}$ und $X = \{1, \ldots, n\}$ schreiben wir auch $\mathrm{A}_n := \mathrm{A}_X$.

Bemerkung 10D1. Für $n = 1$ ist $\mathrm{A}_1 = \mathrm{S}_1$ die triviale Gruppe. Für $n \geq 2$ ist $\mathrm{A}_n \lhd \mathrm{S}_n$ eine normale Untergruppe von Index 2, also von der Ordnung $|\mathrm{A}_n| = n!/2$. □

Satz 10D2. *Die alternierende Gruppe* A_n *ist die Kommutatorgruppe der symmetrischen Gruppe* S_n*, und die Signatur* $\mathrm{sign}\colon \mathrm{S}_n \to \{\pm 1\}$ *ist die Abelschmachung der Gruppe* S_n*.*

BEWEIS. Sei K die Kommutatoruntergruppe von S_n. Dann ist der Quotient $A = \mathrm{S}_n/K$ eine abelsche Gruppe. Der Quotientenhomomorphismus $\alpha\colon \mathrm{S}_n \twoheadrightarrow A$ bildet nach Lemma 10C1 alle Transpositionen auf dasselbe $a \in A$ Element ab, und es gilt $A = \langle a \rangle$.



Da Transpositionen Ordnung 2 haben, muss a Ordnung 1 oder 2 haben. Die universelle Eigenschaft (§9Cb) beschert uns einen Gruppenhomomorphismus $f\colon A \to \{\pm 1\}$ mit $\mathrm{sign} = f \circ \alpha$. Wegen $\mathrm{sign}(1,2) = -1$ gilt $f(a) = -1$, also hat a Ordnung 2. Damit ist f ein Isomorphismus, und $K = \ker(\alpha) = \ker(\mathrm{sign}) = \mathrm{A}_n$. □

Wie in 10C5 gesehen erstreckt sich die Signatur auch auf die Gruppe $\mathrm{S}_{(X)}$ der *endlichen* Permutationen einer unendlichen Menge X. Wir definieren hier entsprechend die alternierende Gruppe durch

$$\mathrm{A}_{(X)} := \ker(\mathrm{sign}\colon \mathrm{S}_{(X)} \to \{\pm 1\}).$$

Auch hier ist die Signatur die Abelschmachung der Gruppe $\mathrm{S}_{(X)}$, und so fällt $\mathrm{A}_{(X)}$ mit der Kommutatorgruppe von $\mathrm{S}_{(X)}$ zusammen (10C8).

§**10Da. Erzeugendensysteme von** A_n**.** Die symmetrische Gruppe S_n wird von ihren Transpositionen erzeugt. Analog hierzu erhalten wir:

Proposition 10D3. *Die alternierende Gruppe* A_n *wird von ihren* 3*-Zykeln erzeugt.*

BEWEIS. Jede Permutation $\sigma \in \mathrm{S}_n$ ist ein Produkt $\sigma = \tau_1 \cdots \tau_\ell$ von $\ell \geq 0$ Transpositionen (10A9). Es gilt $\mathrm{sign}(\sigma) = (-1)^\ell$, also $\sigma \in A_n$ genau dann, wenn ℓ gerade ist. Je zwei aufeinanderfolgende Faktoren $\tau_{2k-1}\tau_{2k}$ können wir als Produkt von 3-Zykeln schreiben: Für paarweise verschiedene a,b,c,d gilt $(a,b)(a,b) = \mathrm{id}$ und $(a,b)(b,c) = (a,b,c)$ und $(a,b)(c,d) = (a,b,c)(b,c,d)$. □

Übung 10D4. Es gilt $A_n = \langle (1,2,3), (2,3,4), \ldots, (n-2,n-1,n) \rangle$.
Ebenso gilt $A_n = \langle (1,2,3), (1,3,4), \ldots, (1,n-1,n) \rangle$.

§**10Db. Konjugationsklassen in** A_n**.** Die Konjugationsklassen von S_n haben wir in Satz 10B12 bestimmt. Eine gerade Permutation $\sigma \in \mathrm{S}_n$ hat in A_n entweder dieselbe Konjugationsklasse wie in S_n oder diese spaltet sich in zwei Konjugationsklassen:

Satz 10D5. *Für jede Permutation* $\sigma \in \mathrm{A}_n$ *gilt:*

1. *Wenn* $Z_{\mathrm{S}_n}(\sigma) \subset \mathrm{A}_n$*, dann gilt* $Z_{\mathrm{S}_n}(\sigma) = Z_{\mathrm{A}_n}(\sigma)$ *und* $\sigma^{\mathrm{S}_n} = \sigma^{\mathrm{A}_n} \sqcup \sigma^{\mathrm{A}_n(1,2)}$.
2. *Wenn* $Z_{\mathrm{S}_n}(\sigma) \not\subset \mathrm{A}_n$*, dann gilt* $|Z_{\mathrm{S}_n}(\sigma) : Z_{\mathrm{A}_n}(\sigma)| = 2$ *und* $\sigma^{A_n} = \sigma^{S_n}$.

BEWEIS. Der Zentralisator

$$Z_{\mathrm{A}_n}(\sigma) = Z_{\mathrm{S}_n}(\sigma) \cap \mathrm{A}_n = \ker(\operatorname{sign}|_{Z_{\mathrm{S}_n}(\sigma)})$$

ist vom Index 1 oder 2 in $Z_{\mathrm{S}_n}(\sigma)$, je nachdem ob $Z_{\mathrm{S}_n}(\sigma)$ nur gerade Permutationen enthält oder nicht. Wegen $\left|\sigma^{\mathrm{A}_n}\right| = |\mathrm{A}_n : Z_{\mathrm{A}_n}(\sigma)|$ folgt im ersten Fall $\left|\sigma^{A_n}\right| = \frac{1}{2}\left|\sigma^{S_n}\right|$ und im zweiten Fall $\left|\sigma^{A_n}\right| = \left|\sigma^{S_n}\right|$. □

Korollar 10D6. *Für $n \geq 5$ sind in A_n alle 3-Zykel zueinander konjugiert.*

BEWEIS. Wegen $(4,5) \in Z_{\mathrm{A}_n}((1,2,3))$ gilt Fall (2) im obigen Satz. □

Übung 10D7. In A_3 und A_4 sind nicht alle 3-Zykel zueinander konjugiert.

Beispiel 10D8. Die Konjugationsklassen der symmetrischen Gruppe S_5 sind:

Repräsentant σ	$\lvert Z_{\mathrm{S}_5}(\sigma)\rvert$	$\left\lvert\sigma^{\mathrm{S}_5}\right\rvert$	$\operatorname{ord}(\sigma)$	$\operatorname{sign}(\sigma)$
id	$\lvert\mathrm{S}_5\rvert = 120$	1	1	$+1$
(12)	$3!\cdot 2 = 12$	10	2	-1
(123)	$2!\cdot 3 = 6$	20	3	$+1$
(1234)	4	30	4	-1
(12345)	5	24	5	$+1$
$(12)(34)$	$2!2^2 = 8$	15	2	$+1$
$(123)(45)$	$3\cdot 2 = 6$	20	6	-1

Wie man sieht, summiert sich die Gesamtzahl der Elemente zu $120 = 5!$. Die Gruppe S_5 operiert durch Konjugation auf der normalen Untergruppe $\mathrm{A}_5 \lhd \mathrm{S}_5$. Diese zerfällt in die obigen S_n-Bahnen, die Signatur $+1$ haben. Ihre Elementezahl summiert sich zu $60 = 5!/2$.

Die Konjugationsklassen in der alternierenden Gruppe A_5 sind:

Repräsentant σ	$\lvert Z_{\mathrm{A}_5}(\sigma)\rvert$	$\left\lvert\sigma^{\mathrm{A}_5}\right\rvert$	$\operatorname{ord}(\sigma)$	$\operatorname{sign}(\sigma)$
id	$\lvert\mathrm{S}_5\rvert = 60$	1	1	$+1$
(123)	3	20	3	$+1$
(12345)	5	12	5	$+1$
(12354)	5	12	5	$+1$
$(12)(34)$	4	15	2	$+1$

Ausführlicher bedeutet dies:

- Alle 3-Zykel sind in A_5 konjugiert: Zu $\sigma = (a,b,c)$ und $\sigma' = (a',b',c')$ existiert $\tau \in \mathrm{S}_5$ mit $\tau\sigma\tau^{-1} = \sigma'$. Sei $\mathrm{Fix}(\sigma) = \{d,e\}$. Wenn $\tau \neq A_5$, dann leistet $\tau(d,e) \in \mathrm{A}_5$ das Gewünschte.
- Alle 5-Zykel liegen zwar in einer S_5-Konjugationsklasse, aber sie zerfallen in zwei A_5-Konjugationsklassen: Für $\sigma = (1,2,3,4,5)$ gilt nämlich $Z_{\mathrm{S}_5}(\sigma) = \langle\sigma\rangle < A_5$. Also $\left|\sigma^{\mathrm{S}_5}\right| = 120/5 = 24$ und $\left|\sigma^{\mathrm{A}_5}\right| = 60/5 = 12$.
- Alle Produkte von zwei disjunkten 2-Zykeln sind in A_5 konjugiert.

§10E. Einfache Gruppen

Definition 10E1. Eine Gruppe G heißt *einfach*, wenn sie nur zwei normale Untergruppen hat, das heißt aus $K \lhd G$ folgt entweder $\{1\}$ oder G.

Bemerkung 10E2. Da normale Untergruppen die Kerne von Gruppenhomomorphismen sind, lässt sich diese Definition wie folgt umformulieren: Eine Gruppe G ist genau dann einfach, wenn jeder Gruppenhomomorphismus $G \to H$ entweder trivial oder injektiv ist.

Proposition 10E3. *Jede Gruppe von Primzahlordnung ist einfach (isomorph zu $\mathbb{Z}/p\mathbb{Z}$). Eine abelsche Gruppe A ist genau dann einfach, wenn sie von Primzahlordnung ist.*

BEWEIS. Die erste Aussage folgt aus dem Satz von Lagrange: Ist G eine Gruppe von Primzahlordnung, dann hat sie nur die Untergruppen $\{1\}$ und G.

Sei A eine abelsche einfache Gruppe. Wegen $A \neq \{1\}$ existiert $a \in A$ mit $a \neq 1$. Es muss dann $\langle a \rangle = A$ gelten, denn sonst wäre $\langle a \rangle$ eine normale Untergruppe mit $\{1\} \subsetneq \langle a \rangle \subsetneq A$. Also ist A zyklisch. Die Gruppe $A \cong \mathbb{Z}/n\mathbb{Z}$ ist genau dann einfach, wenn n eine Primzahl ist: Andernfalls wäre für $n = ab$ mit $a, b > 1$ die Untergruppe $a\mathbb{Z}/n\mathbb{Z}$ eine normale Untergruppe mit $\{1\} \subsetneq a\mathbb{Z}/n\mathbb{Z} \subsetneq \mathbb{Z}/n\mathbb{Z}$. □

Beispiel 10E4. Die symmetrische Gruppe S_n ist genau dann einfach wenn $n = 2$ gilt. Denn S_1 ist trivial und für $n \geq 3$ hat S_n die nicht-triviale normale Untergruppe $\mathrm{A}_n \lhd S_n$.

Beispiel 10E5. Ist X eine unendliche Menge, dann ist die symmetrische Gruppe S_X nicht einfach, denn sie enthält die normale Untergruppe $\mathrm{S}_{(X)}$ der endlichen Permutationen.

Beispiel 10E6. Die alternierende Gruppen A_1 und A_2 sind trivial und daher nicht einfach, A_3 ist abelsch von Ordnung 3 und daher einfach. Hingegen ist A_4 nicht einfach, denn

$$V = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \lhd \mathrm{A}_4 \quad (\text{sogar } V \lhd \mathrm{S}_4).$$

§10Ea. Die alternierende Gruppe A_n für $n \geq 5$ ist einfach. Bislang kennen wir als einfache Gruppen nur $\mathbb{Z}/p\mathbb{Z}$ von Primzahlordnung. Wir wollen nun zeigen, dass die alternierenden Gruppen A_n mit $n \geq 5$ alle einfach sind.

Zunächst ein besonders kurzer Beweis für A_5:

Satz 10E7. *Die Gruppe A_5 ist einfach.*

BEWEIS. Sei $K \lhd \mathrm{A}_5$ eine normale Untergruppe. Nach dem Satz von Lagrange muss dann $|K| \mid |A_5| = 60$ gelten. Außerdem muss K die Vereinigung von Konjugationsklassen in A_5 sein. Diese haben wir in Beispiel 10D8 bestimmt: sie haben jeweils $1, 20, 12, 12, 15$ Elemente. Aber keine der möglichen Summen teilt 60, bis auf 1 und $1+20+12+12+15 = 60$, und diese entsprechen den trivialen Untergruppen $\{1\}$ und A_5. □

Der allgemeine Fall ist kaum schwieriger, aber wir müssen systematischer vorgehen:

Satz 10E8. *Für $n \geq 5$ ist die alternierende Gruppe A_n einfach.*

BEWEIS. Sei $\{1\} \subsetneq K \lhd \mathrm{A}_n$ eine normale Untergruppe. Es reicht zu zeigen, dass K einen 3-Zykel σ enthält. Dann enthält nämlich K die gesamte Konjugationsklasse σ^{A_n}. Nach 10D6 sind alle 3-Zykel in A_n konjugiert, und nach 10D3 erzeugen sie die Gruppe A_n.

Sei $\sigma \neq \mathrm{id}$ ein Element von K. Wir betrachten die Zerlegung $\sigma = z_1 z_2 \cdots z_r$ in disjunkte Zykel $z_1, z_2, \ldots, z_r$ der Länge $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_r \geq 2$. Wir unterscheiden fünf Fälle:

1. Für $\ell_1 \geq 4$ gilt $\sigma = (a,b,c,d,\ldots)z_2 \cdots z_r$. Für $\tau = (a,b,c)$ finden wir
$$\tau\sigma\tau^{-1} \cdot \sigma = (b,c,a,d,\ldots) \cdot (a,b,c,d,\ldots)^{-1} = (a,b,d).$$
2. Wenn $\ell_1 = 3$ und $r = 1$, dann gilt $\sigma = (a,b,c)$ und es ist nichts mehr zu zeigen.
3. Für $\ell_1 = \ell_2 = 3$ gilt $\sigma = (a,b,c)(d,e,f)z_3 \cdots z_r$. Für $\tau = (b,c,d)$ finden wir
$$\tau\sigma\tau^{-1} \cdot \sigma = (a,c,d)(b,e,f) \cdot (a,b,c)^{-1}(d,e,f)^{-1} = (a,d,b,c,e).$$
Wir können nun Fall (1) anwenden.
4. Wenn $\ell_1 = \ell_2 = 2$ und $r = 2$, dann gilt $\sigma = (a,b)(c,d)$. Wegen $n \geq 5$ können wir noch ein fünftes Element $e \in X \smallsetminus \{a,b,c,d\}$ wählen. Für $\tau = (e,d,c)$ finden wir
$$\tau\sigma\tau^{-1} \cdot \sigma = (a,b)(e,c) \cdot (a,b)(c,d) = (c,d,e).$$
5. Für $\ell_1 = \ell_2 = 2$ gilt $\sigma = (a,b)(c,d)z_3 \cdots z_r$. Für $\tau = (a,b,c)$ finden wir
$$\tau\sigma\tau^{-1} \cdot \sigma = (b,c)(a,d) \cdot (a,b)(c,d) = (a,c)(b,d).$$
Wir können nun Fall (4) anwenden.

In allen Fällen enthält die gegebene normale Untergruppe $K \lhd \mathrm{A}_n$ mit $K \neq \{1\}$ einen 3-Zykel, und somit alle 3-Zykel. Folglich gilt $K = \mathrm{A}_n$. □

Bemerkung 10E9. Das Ergebnis erstreckt sich auch auf endliche Permutationen einer unendlichen Menge X: Die Gruppe $\mathrm{S}_{(X)}$ der endlichen Permutationen von X enthält als normale Untergruppe die alternierende Gruppe $\mathrm{A}_{(X)}$ der endlichen Permutationen von X mit Signatur $+1$. Der obige Beweis zeigt, dass $\mathrm{A}_{(X)}$ einfach ist für alle X mit $|X| \geq 5$.

Proposition 10E10. *Jede einfache Gruppe G mit einer Untergruppe $H < G$ vom Index $n \geq 2$ kann in die symmetrische Gruppe S_n eingebettet werden. Für $G \ncong \mathbb{Z}/2$ gilt dann $|G| \leq n!/2$.*

BEWEIS. Die Gruppe G operiert transitiv auf der Menge $X = G/H$ der Linksnebenklassen mittels Linksmultiplikation, $\alpha\colon G \times G/H \to G/H$ mit $(g, aH) \mapsto gaH$. Dies induziert einen nicht-trivialen Gruppenhomomorphismus $\tilde{\alpha}\colon G \to \mathrm{S}_X$ (9F7). Ist G einfach, dann muss $\tilde{\alpha}$ injektiv sein.

Wäre $|G| = n!$, dann wäre $G \cong \mathrm{S}_n$ nicht einfach. (Die einzige Ausnahme besteht für $n = 2$ also $G \cong \mathbb{Z}/2$.) Also hat das Bild von G in S_n mindestens Index 2, das heißt $2|G| \leq n!$. □

Korollar 10E11. *Eine unendliche einfache Gruppe hat keine Untergruppen von endlichem Index.* □

Korollar 10E12. *Für $n \geq 5$ enthält A_n keine Untergruppe vom Index $2, 3, \ldots, n-1$.* □

Hingegen ist $A_{n-1} < A_n$ eine Untergruppe vom Index n.

Übung 10E13. Die alternierende Gruppe A_5 der Ordnung 60 enthält keine Untergruppen der Ordnung 30, 20, 15, wohl aber Untergruppen der Ordnung 2, 3, 4, 5, 6, 10, 12.

§10F. Semidirekte Produkte

§10Fa. Internes semidirektes Produkt. Zur Erinnerung (§9Cc): Ein internes direktes Produkt $G = H \times K$ besteht aus zwei normalen Untergruppen $H \lhd G$ und $K \lhd G$ für die $HK = G$ und $H \cap K = \{1\}$ gilt. In diesem Fall kommutieren H und K, und G ist isomorph zum externen Produkt $H \times K$ mit komponentenweiser Verknüpfung. In Anlehnung an das direkte Produkt definieren wir nun das (zunächst interne) semidirekte Produkt wie folgt:

Definition 10F1. Eine Gruppe G ist das *interne semidirekte Produkt* einer normalen Untergruppe $K \lhd G$ mit einer Untergruppe $H < G$ wenn $KH = G$ und $K \cap H = \{1\}$ gilt.

In diesem Fall schreiben wir $G = K \rtimes H = H \ltimes K$. Die Situation ist nicht symmetrisch, und das Zeichen "$\rtimes$" bzw. "$\ltimes$" zeigt an, dass K normal in G ist.

Bemerkung 10F2. Die Bedingungen $KH = G$ und $K \cap H = \{1\}$ bedeuten, dass sich jedes Element $g \in G$ eindeutig als Produkt $g = kh$ mit $k \in K$ und $h \in H$ schreiben lässt (§9Cc).

Wegen $KH = HK$ (9B12) lässt sich jedes Element $g \in G$ auch eindeutig als Produkt $g = h'k'$ mit $h' \in H$ und $k' \in K$ schreiben. Es muss hierbei nicht $(h,k) = (h',k')$ gelten: Aus $kh = h(h^{-1}kh)$ folgt zwar $h' = h$, aber $k' = h^{-1}kh$ ist im Allgemeinen von k verschieden.

Beispiel 10F3. Die symmerische Gruppe S_n ist das semidirekte Produkt $\mathrm{S}_n = \mathrm{A}_n \rtimes \langle (1,2) \rangle$ aus der normalen Untergruppe $\mathrm{A}_n \lhd \mathrm{S}_n$ der geraden Permutationen und einer Untergruppe $H = \{\mathrm{id}, (1,2)\}$ der Ordnung 2. Es gilt nämlich $\mathrm{A}_n \cap H = \{\mathrm{id}\}$ und $\mathrm{A}_n H = \mathrm{S}_n$.

Statt $(1,2)$ kann man hierbei auch jede andere Transposition (a,b) wählen, oder jede ungerade Permutation $\sigma \in \mathrm{S}_n$ der Ordnung 2, also $(a,b)(c,d)(d,e)$ für $n \geq 6$ oder $(a,b)(c,d)(d,e)(f,g)(h,i)$ für $n \geq 10$, etc.

Beispiel 10F4. Sei R ein Ring. Die *affine Gruppe* des Rings R ist

$$\mathrm{Aff}(R) = \{\, f \colon R \to R, f(x) = a + bx \mid a \in R, b \in R^\times \,\}.$$

Man rechnet leicht nach, dass dies eine Gruppe ist. Hierin die Menge der *Translationen*

$$T = \{\, f \colon x \mapsto a + x \mid a \in R \,\} \lhd \mathrm{Aff}(R)$$

eine normale Untergruppe und die Menge der *Streckungen*

$$S = \{\, f \colon x \mapsto bx \mid b \in R^\times \,\} < \mathrm{Aff}(R)$$

eine Untergruppe (und im Allgemeinen nicht normal). Nach Konstruktion gilt $\mathrm{Aff}(R) = TS$. Zudem gilt $T \cap S = \{\mathrm{id}\}$. Wir haben also ein semidirektes Produkt. Dies schreiben wir

$$\mathrm{Aff}(R) = T \rtimes S = S \ltimes T.$$

Offenbar gilt $(T, \circ) \cong (R, +)$ und $(S, \circ) \cong (R^\times, \cdot)$. Statt der präzisen aber schwerfälligen Bezeichnung $\mathrm{Aff}(R) = T \rtimes S$ schreibt man daher auch kurzerhand $\mathrm{Aff}(R) = R \rtimes R^\times$.

Etwas allgemeiner erhält man zu $S < R^\times$ die affine Untergruppe

$$\mathrm{Aff}(R;S) = \{\, f \colon R \to R, f(x) = a + bx \mid a \in R, b \in S \,\}.$$

Dies ist wie zuvor ein semidirektes Produkt, das wir kurz $R \rtimes S$ schreiben.

Beispiel 10F5. Die Diedergruppe D_n ist die Isometriegruppe des regelmäßigen n-Ecks.

[Bild]

Wir betrachten hierzu das regelmäßige n-Eck in der Ebene $\mathbb{R}^2$ mit den Eckpunkten $P_k = (\cos(2\pi k/n), \sin(2\pi k/n))$ wobei $k \in \mathbb{Z}$. Wegen der Periodizität reicht es $k = 1, 2, \ldots, n$ zu betrachten. Besser noch ist eine Nummerierung modulo n durch $\mathbb{Z}/n$, $\bar{k} \mapsto P_k$.

Darstellung als Matrizengruppe: Die Diedergruppe D_n lässt sich wie folgt als Matrixgruppe darstellen. Hierzu sei r_k die Drehung um den Winkel $2\pi k/n$ und s_k die Spiegelung an der Achse, die im Winkel $\pi k/n$ geneigt ist. Es gilt dann

$$D_n = \{\, r_0, \ldots, r_{n-1}, s_0, \ldots, s_{n-1} \,\} \quad \text{mit}$$

$$r_k = \begin{pmatrix} \cos(2\pi k/n) & -\sin(2\pi k/n) \\ \sin(2\pi k/n) & \cos(2\pi k/n) \end{pmatrix} \quad \text{und} \quad s_k = \begin{pmatrix} \cos(2\pi k/n) & \sin(2\pi k/n) \\ \sin(2\pi k/n) & -\cos(2\pi k/n) \end{pmatrix}.$$

Auch hier ist es vorteilhaft die Indizes zyklisch modulo n zu rechnen. Hierbei fallen folgende Relationen auf:

- r_0 ist die Identität, hier gesehen als Drehung um den Winkel 0.
- r_1 ist die Drehung um den Winkel $2\pi/n$ und es gilt $r_k = r_1^k$ für alle k.
- s_0 ist die Spiegelung an der horizontalen Achse und es gilt $s_k = r_k s_0$ für alle k.
- Es gilt $s_0 r_k s_0 = r_{-k}$ und allgemein $s_\ell r_k s_\ell = r_{2\ell-k}$.

Somit enthält D_n die normale Untergruppe der Rotationen:

$$R = \{r_0, \ldots, r_{n-1}\} \lhd D_n.$$

Dies ist eine zyklische Gruppe der Ordnung n. Zu der Spiegelung s_0 ist

$$S = \{\mathrm{id}, s_0\} < D_n$$

eine Untergruppe der Ordnung 2. Dies ist wegen $r_1 s_0 r_{-1} = r_1 s_0 r_{-1} s_0 s_0 = r_1 r_1 s_0 = s_2$ nicht normal für $n \geq 2$. Offenbar gilt $R \cap S = \{\mathrm{id}\}$ sowie $D_n = RS$. Somit ist die Diedergruppe das semidirekte Produkt von R und S. Dies schreiben wir kurz als

$$D_n = R \rtimes S$$

Darstellung als Permutationsgruppe: Wir numerieren die n Eckpunkte zyklisch mit den Elementen $\bar{0}, \bar{1}, \ldots, \overline{n-1} \in \mathbb{Z}/n$. Die Operation von D_n induziert dann einen injektiven Gruppenhomomorphismus $\varphi\colon D_n \hookrightarrow \mathrm{Sym}(\mathbb{Z}/n)$. Die Rotation r_k entspricht der Translation $\varphi(r_k)\colon x \mapsto k + x$. Die Spiegelung s_0 enspricht der Abbildung $\varphi(s_0)\colon x \mapsto -x$, und allgemein entspricht s_k der Abbildung $\varphi(s_k)\colon x \mapsto 2k - x$. Somit erhalten wir den Gruppenisomorphismus

$$\varphi\colon D_n \xrightarrow{\sim} \mathbb{Z}/n \rtimes \{\pm 1\}.$$

Beispiel 10F6. Sei V ein Vektorraum über einem Körper K. Die *K-affine Gruppe* von V ist

$$\mathrm{Aff}_K(V) = \{\, f\colon V \to V, f(x) = a + b(x) \mid a \in V, b \in \mathrm{Aut}_K(V) \,\}.$$

Hierin liegt die normale Untergruppe $T = \{\, f\colon x \mapsto a + x \mid a \in V \,\}$ der *Translationen* sowie die Gruppe $\mathrm{Aut}_K(V)$ der *K-linearen Automorphismen*, so dass $\mathrm{Aff}_K(V) = T \rtimes \mathrm{Aut}_K(V)$.

Offenbar gilt $(T, \circ) \cong (V, +)$, sodass man statt $T \rtimes \mathrm{Aut}_K(V)$ kurz $\mathrm{Aff}_K(V) = V \rtimes \mathrm{Aut}_K(V)$ schreibt. Gleiches gilt sinngemäß für jeden Modul V über einem beliebigen Ring K.

Auch hier ist es manchmal nützlich, eine Untergruppe $S < R^\times$ zu betrachten. Man erhält so entsprechend wie zuvor ein semidirektes Produkt $V \rtimes S$.

Diese und viele ähnliche Beispiele fassen wir wie folgt zusammen:

Definition 10F7. Sei A eine Gruppe und sei $S < \mathrm{Aut}(A)$. Die *affine Gruppe* von A über S ist

$$\mathrm{Aff}(A;S) := \{\, f\colon A \to A, f(x) = a \cdot b(x) \mid a \in A, b \in S \,\}.$$

Lemma 10F8. *Mit der Komposition von Abbildungen ist* $\mathrm{Aff}(A,S)$ *eine Gruppe.*

BEWEIS. Für $a = 1$ und $b = \mathrm{id}$ erhalten wir $f = \mathrm{id}$. Für $f_1\colon x \mapsto a_1 \cdot b_1(x)$ und $f_2\colon x \mapsto a_2 \cdot b_2(x)$ gilt

$$(f_1 \circ f_2)\colon x \mapsto a_1 \cdot b_1(a_2 \cdot b_2(x)) = (a_1 b_1(a_2)) \cdot (b_1 b_2)(x).$$

Zu $f\colon x \mapsto a \cdot b(x)$ ist das Inverse $f^{-1}\colon x \mapsto b^{-1}(a^{-1}) \cdot b^{-1}(x)$. □

Die vorgegebene Gruppe $S < \mathrm{Aut}(A)$ ist insbesondere eine Untergruppe der symmetrischen Gruppe $\mathrm{Sym}(A)$. Ebenso bilden die Linkstranslationen $\lambda_a\colon x \to ax$ eine Untergruppe $T = \{\, \lambda_a \mid a \in K \,\} < \mathrm{Sym}(A)$. Die Zuordnung $a \mapsto \lambda_a$ stiftet einen Gruppenisomorphismus $\lambda\colon A \xrightarrow{\sim} T$, und wir können die Gruppen A und T mittels λ identifizieren.

Die von T und S erzeugte Untergruppe in $\mathrm{Sym}(A)$ ist gerade die affine Gruppe $\mathrm{Aff}(A;S)$ von A über S. Es gilt $T \lhd \mathrm{Aff}(A;S)$, denn $b(a \cdot b^{-1}(x)) = b(a) \cdot x$. Nach Konstruktion haben wir $TS = ST = \mathrm{Aff}(A;S)$. Zudem gilt $T \cap S = \{1\}$, denn $b(1) = 1$ für alle $b \in S$, aber $a1 = 1$ nur für $a = 1$. Damit haben wir $G = T \rtimes S$ gezeigt.

Notation. Statt $\mathrm{Aff}(A;S)$ schreiben wir kurzerhand $A \rtimes S$. Hierbei identifiziert man die Gruppe A mit der Gruppe T der Linkstranslationen mittels $a \mapsto \lambda_a$.

§**10Fb. Operation durch Konjugation.** In einem semidirekten Produkt $G = K \rtimes H$ schreibt sich jedes Element $g \in G$ eindeutig als Produkt $g = kh$ mit $k \in K$ und $h \in H$. Mit anderen Worten, wegen $K \cap H = \{1\}$ und $KH = G$ ist die Abbildung

$$K \times H \to G, \quad (k,h) \mapsto kh$$

ist bijektiv. Für die Verknüpfung von $g_1 = k_1 h_1$ und $g_2 = k_2 h_2$ in G gilt dann

$$(k_1 h_1)(k_2 h_2) = (k_1 \cdot h_1 k_2 h_1^{-1})(h_1 h_2). \tag{10.3}$$

Um also in einem semidirekten Produkt $G = K \rtimes H$ rechnen zu können, brauchen wir neben der Verknüpfung in K und in H auch die Konjugation von H auf K:

Ist $G = K \rtimes H$ ein semidirektes Produkt, dann operiert G auf $K \lhd G$ durch Konjugation

$$\alpha\colon G \times K \to K \quad \text{wobei} \quad (g,k) \mapsto gkg^{-1}$$

und somit operiert auch $H < G$ auf K. Dies entspricht dem Gruppenhomomorphismus

$$\tilde{\alpha}\colon H \to \mathrm{Aut}(K) \quad \text{mit} \quad \tilde{\alpha}(h)(k) = hkh^{-1}. \tag{10.4}$$

Beide Sichtweisen, die Operation α und der Homomorphismus $\tilde{\alpha}$, entsprechen einander eindeutig. Der Kürze willen betrachten wir im Folgenden meist nur den Gruppenhomomorphismus $H \to \mathrm{Aut}(K)$.

Ein wichtiger Spezialfall soll gleich erwähnt werden: Ist $\tilde{\alpha}\colon H \to \mathrm{Aut}(K)$ der triviale Homomorphismus, mit $\tilde{\alpha}(h) = \mathrm{id}_K$ für alle $h \in H$, dann gilt in obiger Formel (10.3)

$$(k_1 h_1)(k_2 h_2) = (k_1 k_2)(h_1 h_2)$$

und wir erhalten das direkte Produkt. Der Homomorphismus $\tilde{\alpha}\colon H \to \mathrm{Aut}(K)$ bestimmt also, wie das direkte Produkt zu einem semi-direkten Produkt "deformiert" wird.

§**10Fc. Externes semidirektes Produkt.** Jedes interne semidirekte Produkt $G = K \rtimes H$ zerlegt die Gruppe G in eine normale Untergruppe $K \lhd G$ und ein Komplement $H < G$. Dabei operiert H auf K mittels $\alpha\colon H \to \mathrm{Aut}(K)$. Wir wollen nun den umgekehrten Standpunkt einnehmen, und G aus den Daten (K,H,α) zusammenbauen:

Satz 10F9. *Seien H,K Gruppen und $\alpha\colon H \to \mathrm{Aut}(K)$ ein Gruppenhomomorphismus. Zu dem Tripel (K,H,α) existiert genau eine Gruppe G mit Untergruppen $K \lhd G$ und $H < G$ sodass $G = K \rtimes H$ ein semidirektes Produkt ist, und die Operation von H auf K durch α gegeben ist.*

Die *Eindeutigkeit* folgt sofort aus obiger Multiplikationsformel (10.3). Die *Existenz* verlangt eine Konstruktion. Hierzu kann man auf der Menge $G = K \times H$ die Verknüpfung

$$(k_1h_1)\cdot(k_2h_2) := (k_1\alpha(h_1)(k_2))(h_1h_2)$$

definieren und direkt nachrechnen, dass alle Bedingungen erfüllt sind: $(G,\cdot)$ ist eine Gruppe, $\bar{K} = K \times 1$ ist eine normale Untergruppe, $\bar{H} = \{1\} \times H$ ist eine Untergruppe, sodass $G = \bar{K} \rtimes \bar{H}$ ein semidirektes Produkt ist mit der vorgegebenen Operation von $\bar{H}$ auf $\bar{K}$. Dieser Weg ist allerdings länglich, insbesondere der Nachweis der Assoziativität. (Übung!)

Der Satz von Cayley weist uns einen leichteren Weg:

BEWEIS. Wir betrachten die Menge $X = K \times H$ und die symmetrische Gruppe S_X. Hierin betten wir K und H ein durch $\lambda\colon K \to \mathrm{S}_X$, $\lambda(a)(k,h) = (ak,h)$, und $\delta\colon H \to \mathrm{S}_X$, $\delta(b) = (\alpha(b)(k),bh)$. Die von $\bar{K} = \lambda(K)$ und $\bar{H} = \delta(H)$ erzeugte Untergruppe von S_X ist dann

$$G = \langle \bar{K},\bar{H}\rangle = \{\, f\colon X \to X, f(k,h) = (a\cdot\alpha(b)(k),bh) \mid a \in K, b \in H \,\}$$

Dass die Menge auf der rechten Seite tatsächlich eine Gruppe ist, haben wir in 10F8 bereits nachgerechnet. Es gilt $\bar{K} \lhd G$ und $\bar{H} < G$ sowie $G = \bar{K}\bar{H}$ und $\bar{K} \cap \bar{H} = \mathrm{id}_X$. Somit haben wir $G = \bar{K} \rtimes \bar{H}$ und auch die Operation von $\bar{H}$ auf $\bar{K}$ entspricht dem vorgegebenen Homomorphismus $\alpha\colon H \to \mathrm{Aut}(K)$. □

Definition 10F10. Die so definierte Gruppe schreiben wir $G = K \overset{\alpha}{\rtimes} H = H \overset{\alpha}{\ltimes} K$, und nennen sie das *externe semidirekte Produkt* von K und H zu der vorgebenen Konjugation α. Die Situation ist nicht symmetrisch, und das Zeichen "$\rtimes$" bzw. "$\ltimes$" zeigt an, dass H auf K mittels α durch Konjugation operiert.

Man beachte, dass für ein *externes* semidirektes Produkt die Gruppen $(K,\cdot)$ und $(H,\cdot)$ noch nicht ausreichen, um $K \rtimes H$ eindeutig zu beschreiben. Dies gelingt erst durch die zusätzliche Angabe der Konjugation α. Hat man die Gruppe $(G,\cdot)$ damit konstruiert, dann ist $G = \bar{K} \rtimes \bar{H}$ ein *internes* semidirektes Produkt, und die Konjugation α ergibt sich aus der Gruppenstruktur von G.

Beispiel 10F11. Das semidirekte Produkt $G = K \overset{\alpha}{\rtimes} H$ ist ein direktes Produkt genau dann wenn $\alpha\colon H \to \mathrm{Aut}(K)$ der triviale Homomorphismus ist, mit $\alpha(h) = \mathrm{id}_K$ für alle $h \in H$.

Beispiel 10F12. Die Diedergruppe $D_n = \mathbb{Z}/n \overset{\alpha}{\rtimes} \mathbb{Z}/2$ wobei $\alpha\colon \mathbb{Z}/2 \to \mathrm{Aut}(\mathbb{Z}/n)$ gegeben ist durch $\bar{n} \mapsto (-1)^n$.

Manchmal lässt man in der Notation die explizite Erwähnung von α weg. Dies ist nur dann statthaft, wenn α aus dem Kontext unmissverständlich hervorgeht oder alle (nicht-trivialen) Wahlen von α diesselbe Gruppe liefern (bis auf Isomorphie). Im Zweifelsfalle ist es jedenfalls besser, die Operation von H auf K zu präzisieren.

§10Fd. Semi-direkte Produkte $\mathbb{Z}/_p \ltimes \mathbb{Z}/_q$.

Proposition 10F13. *Seien $p < q$ zwei Primzahlen. Wenn $p \nmid q-1$ gilt, dann existiert nur ein semi-direktes Produkte der Form $\mathbb{Z}/_p \ltimes \mathbb{Z}/_q$, nämlich das direkte Produkte $\mathbb{Z}/_p \times \mathbb{Z}/_q$.*

Gilt hingegen $p \mid q-1$, dann existiert neben $\mathbb{Z}/_p \times \mathbb{Z}/_q$ ein nicht-triviales semi-direktes Produkte $\mathbb{Z}/_p \ltimes \mathbb{Z}/_q$. Dieses ist bis auf Isomorphie eindeutig.

BEWEIS. Um die möglichen semi-direkten Produkte $G = \mathbb{Z}/_p \overset{\alpha}{\ltimes} \mathbb{Z}/_q$ zu bestimmen, müssen wir die möglichen Gruppenhomomorphismen $\alpha\colon \mathbb{Z}/_p \to (\mathbb{Z}/_q)^\times$ kennen. Nun ist $(\mathbb{Z}/_q)^\times$ eine zyklische Gruppe der Ordnung $q-1$ (9D21). Für $p \nmid q-1$ ist demnach α trivial, also $G = \mathbb{Z}/_p \times \mathbb{Z}/_q$. Für $p \mid q-1$ gibt es daneben noch Isomorphismen auf die eindeutige Untergruppe $H < (\mathbb{Z}/_q)^\times$ der Ordnung p, also $G = \mathbb{Z}/_p \rtimes H$. □

Notation. Die durch $\mathbb{Z}/_q \rtimes H$ eindeutig bestimmte affine Untergruppe schreiben wir kurzerhand $\mathbb{Z}/_q \rtimes \mathbb{Z}/_p$ oder $\mathbb{Z}/_p \ltimes \mathbb{Z}/_q$. (Diese Schreibweise soll aussagen, dass wir hier das *nicht-triviale* semi-direkte Produkt betrachten, und davon gibt es wie gesehen nur eines.)

§10Fe. Spaltende Gruppenhomomorphismen.

Das externe semidirekte Produkt $G = K \overset{\alpha}{\rtimes} H$ sagt uns, wie man die Gruppe G aus K und H und α zusammenbaut. Das interne semidirekte Produkt $G = K \rtimes H$ sagt uns, wie man die Gruppe G in K und H zerlegt. Wir kommen schließlich zu der Frage, wie man zu einer gegebenen normalen Untergruppe $K < G$ ein passendes Komplement $H < G$ findet.

Sei G eine Gruppe und $K \lhd G$ eine normale Untergruppe. Für jede Untergruppe $H < G$ ist dann $HK = KH = \langle H, K\rangle$ die von H und K erzeugte Untergruppe in G und es gilt $K \lhd HK$ und $HK/K \cong H/(H \cap K)$ (9B13).

Definition 10F14. Ein *Komplement* zu $K \lhd G$ ist eine Untergruppe $H < G$, sodass $H \cap K = \{1\}$ und $HK = G$ gilt. In diesem Fall gilt demnach $G = K \rtimes H$.

Die trivialen Fälle sind klar: $\{1\} \lhd G$ hat G als Komplement, und $G \lhd G$ hat $\{1\}$ als Komplement. Im Allgemeinen muss jedoch kein Komplement existieren:

Beispiel 10F15. In $\mathbb{Z}/4\mathbb{Z}$ hat die Untergruppe $2\mathbb{Z}/4\mathbb{Z}$ kein Komplement.
In $\mathbb{Z}/6\mathbb{Z}$ hat die Untergruppe $3\mathbb{Z}/6\mathbb{Z}$ genau ein Komplement, nämlich $2\mathbb{Z}/6\mathbb{Z}$.

Wenn ein Komplement existiert, ist es im Allgemeinen nicht eindeutig:

Beispiel 10F16. Für $\mathrm{A}_n \lhd \mathrm{S}_n$ ist jede Untergruppe der Form $\{\mathrm{id}, (i,j)\}$ ein Komplement.

Wegen $K \lhd G$ können wir den Quotientenhomomorphismus $\pi\colon G \to G/K$ betrachten. Wenn $H < G$ die Bedingungen $H \cap K = \{1\}$ und $HK = G$ erfüllt, daher induziert π einen Isomorpmismus $\pi|_H\colon H \xrightarrow{\sim} G/K$. Die Umkehrabbildung $\iota\colon G/K \xrightarrow{\sim} H$ ist dann ein Gruppenhomomorphismus $\iota\colon G/K \to G$ mit $\pi \circ \iota = \mathrm{id}_{G/K}$.

Ist ein surjektiver Gruppenhomomorphismus $p\colon G \to Q$ gegeben, so können wir jedem $a \in Q$ ein Urbild $s(a) \in G$ zuordnen. Somit erhalten wir eine Abbildung $s\colon Q \to G$ mit $p \circ s = \mathrm{id}_Q$. Im Allgemeinen wird s aber kein Gruppenhomomorphismus sein.

Definition 10F17. Sei $p\colon G \to Q$ ein surjektiver Gruppenhomomorphismus. Wir sagen, dass *p spaltet* wenn es einen Gruppenhomomorphismus $s\colon Q \to G$ mit $p \circ s = \mathrm{id}_Q$ gibt.

Der triviale Homomorphismus $G \to \{1\}$ spaltet und jeder Isomorphismus $G \xrightarrow{\sim} Q$ spaltet. Im Allgemeinen muss jedoch ein surjektiver Gruppenhomomorphismus nicht spalten:

Beispiel 10F18. Der Homomorphismus $\mathbb{Z}/4 \to \mathbb{Z}/2$ spaltet nicht.
Der Homomorphismus $\mathbb{Z}/6 \to \mathbb{Z}/2$ spaltet.

Wenn $p\colon G \to Q$ spaltet, dass im Allgemeinen nicht eindeutig:

Beispiel 10F19. Der Homomorphismus $\mathrm{sign}\colon \mathrm{S}_n \to \{\pm 1\}$ ist surjektiv für $n \geq 2$. Dieser spaltet mittels $s\colon 1 \mapsto \mathrm{id}, -1 \mapsto \sigma$, wobei $\sigma \in \mathrm{S}_n$ von der Ordnung 2 sein und zudem $\mathrm{sign}(\sigma) = -1$ erfüllen muss. Dies ist zum Beispiel für jede Transposition $\sigma = (i, j)$ der Fall.

Proposition 10F20. *Ein surjektiver Gruppenhomomorphismus $p\colon G \to Q$ spaltet genau dann wenn der Kern $K = \ker(p)$ ein Komplement in H erlaubt.*

BEWEIS. Wenn K ein Komplement $H < G$ erlaubt, dann induziert p einen Gruppenisomorphismus $p|_H\colon H \xrightarrow{\sim} Q$: Surjektivität folgt aus $HK = G$ und Injektivität aus $H \cap K = \{1\}$.

Wenn umgekehrt $p\colon G \to Q$ spaltet mittels eines Gruppenhomomorphismus $s\colon Q \to G$, dann $H = s(Q)$ eine Untergruppe von G. Die Einschränkung $p|_H\colon H \to Q$ ist ein Isomorphismus, denn $p|_H \circ s = \mathrm{id}_Q$ und $s \circ p|_H = \mathrm{id}_H$. Für $a \in H \cap K$ gilt $p(a) = 1$ und somit $a = 1$. Zudem gilt $G = HK$, das heißt, jedes Element $g \in G$ lässt sich schreiben als $g = ab$ mit $a \in K$ und $b \in H$, nämlich $b = s(p(g))$ und $a = gb^{-1}$. □

Korollar 10F21. *Für eine normale Untergruppe $K \lhd G$ sind äquivalent:*

- *$K \lhd G$ hat ein Komplement $H < G$, und damit gilt $G = K \rtimes H$.*
- *Der Quotientenhomomorphismus $\pi\colon G \to G/K$ spaltet.* □

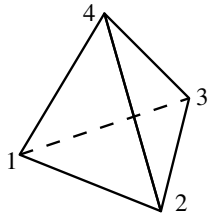
§10G. Übungen und Ergänzungen

§10Ga. Konjugationsklassen in S_4 und A_4.

Übung 10G1. Man bestimme die Konjugationsklassen in S_4 und A_4: Für jede finde man einen Repräsentanten, die Ordnung des Zentralisators, und die Größe der Konjugationsklasse.

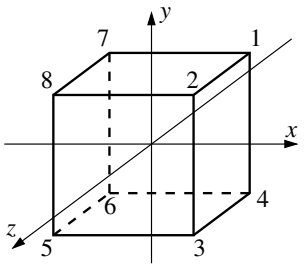
Sei T die die Isometriegruppe des Tetraeders (Drehungen und Spiegelungen) und sei T^+ die Untergruppe der orientierungstreuen Isometrien (Drehungen).

Übung 10G2. Die Operation auf den 4 Ecken induziert einen Gruppenhomomorphismus $T \to S_4$. Ist dies ein Isomorphismus? Was ist das Bild von T^+?



Übung 10G3. Man zeige, dass die Drehungen in T eine einzige Konjugationsklasse bilden, in T^+ aber in zwei Konjugationsklassen zerfallen. Wie kann man dies geometrisch interpretieren?

§**10Gb. Symmetriegruppe des Würfels.** Sei O die Isometriegruppe des Würfels (Drehungen und Spiegelungen) und sei O^+ die Untergruppe der orientierungstreuen Isometrien (Drehungen). Seien α,β,γ die Drehungen um den Winkel $+\frac{\pi}{2}$ um die Achsen x,y,z, und sei σ die Punktspiegelung am Ursprung. (Ist dies eine Drehung oder eine Spiegelung?)



Übung 10G4. Wir betrachten die Operation von O^+ auf den 8 Ecken. Für eine gegebene Ecke, was ist die Bahn, was die Standgruppe? Man bestimme hieraus die Ordnung der Gruppe O^+. Was gilt für O? Die Operation induziert einen Gruppenhomomorphismus $O \to S_8$. Ist dieser injektiv? surjektiv? Man zerlege die Aktion von $\alpha,\beta,\gamma,\sigma$ in disjunkte Zykel.

Übung 10G5. Man untersuche ebenso die Operation von O^+ bzw. O auf den 6 Seiten $F_1=\{1,2,3,4\}$, $F_2=\{5,6,7,8\}$, $F_3=\{1,2,7,8\}$, $F_4=\{3,4,5,6\}$, $F_5=\{2,3,5,8\}$, $F_6=\{1,4,6,7\}$.

Übung 10G6. Man untersuche ebenso die Operation von O^+ bzw. O auf den 4 Diagonalen $D_1=\{1,5\}$, $D_2=\{2,6\}$, $D_3=\{3,7\}$, $D_4=\{4,8\}$. Was kann man über $O^+ \to S_4$ sagen? Was kann man über $O \to S_4$ sagen? Ist die Untergruppe $\langle\sigma\rangle$ normal in O? Ist sie zentral?

Übung 10G7. Man berechne $\alpha\beta\alpha^{-1}$ und $\alpha^{-1}\beta\alpha$ in einer der vorhergehenden Darstellungen. Was ist die geometrische Interpretation? Gilt $O^+=\langle\alpha,\beta\rangle$? Gilt $O=\langle\alpha,\beta,\sigma\rangle$? Gilt gar $O=\langle\alpha,\beta\sigma\rangle$?

§**10Gc. Eine Bemerkung zu Kommutatoren.** Die Kommutatorgruppe besteht nach Definition (§9Ca) aus allen Produkten von Kommutatoren. Für die alternierende Gruppe vermerken wir folgende Verschärfung, die auf Oystein Ore (1951) zurückgeht:

Satz 10G8. *Jede Permutation $\sigma \in \mathrm{A}_n$ ist ein Kommutator $\sigma=\rho\tau\rho^{-1}\tau^{-1}$ mit $\rho,\tau \in \mathrm{S}_n$.*

BEWEIS. In der Zykelzerlegung von σ treten eine gewisse Anzahl von Zykeln ungerader Länge auf (mit Signatur $+1$) sowie eine gerade Anzahl von Zykeln gerader Länge (mit Signatur -1). Es genügt die Aussage zu beweisen auf dem Träger jedes Zykels ungerader Länge bzw. auf dem Träger von je zwei disjunkten Zykeln gerader Länge. Dass dies möglich ist, zeigen die beiden folgenden modellhaften Beispiele. □

Beispiel 10G9. Für jedes $n \geq 2$ ist der Zykel $\sigma = (1,\dots,2n-1)$ ein Kommutator in S_{2n-1}. Wir wählen hierzu $\rho = (1,\dots,n)$ und $\tau\colon k \mapsto 2n-k$ für alle $k = 1,\dots,2n-1$. Dann gilt

$$\tau\cdot\rho\tau^{-1}\rho^{-1} = (1,\dots,n)(n,\dots,2n-1) = \sigma.$$

Kleinste Beispiele: Für $n=2$ erhalten wir $\tau = (1,3)$ und

$$(1,2)\cdot\tau(2,1)\tau^{-1} = (1,2)(2,3) = (1,2,3).$$

Für $n=3$ erhalten wir $\tau = (1,5)(2,4)$ und

$$(1,2,3)\cdot\tau(3,2,1)\tau^{-1} = (1,2,3)(3,4,5) = (1,2,3,4,5).$$

Beispiel 10G10. Für $n \geq m \geq 1$ ist $\sigma = (1,\dots,2m)(2m+1,\dots,2m+2n)$ ein Kommutator in S_{2m+2n}. Wir wählen hierzu $\rho = (1,2,\dots,m+n+1)$ und $\tau_0\colon k \mapsto 2m+2n+1-k$ für alle $k = 1,\dots,2m+2n$ sowie $\tau = (m+n,2m)\circ\tau_0$. Dann gilt

$$\tau\cdot\rho\tau^{-1}\rho^{-1} = (1,2,\dots,m+n+1)(2m,m+n+1,m+n+2,\dots,2m+2n) = \sigma$$

Kleinste Beispiele: Für $n=m=1$ erhalten wir $\tau = (1,4)(2,3)$ und

$$(1,2,3)\cdot\tau(3,2,1)\tau^{-1} = (1,2,3)(2,3,4) = (1,2)(3,4).$$

Für $n=2, m=1$ erhalten wir $\tau = (1,6)(2,5,3,4)$ und

$$(1,2,3,4)\cdot\tau(4,3,2,1)\tau^{-1} = (1,2,3,4)(2,4,5,6) = (1,2)(3,4,5,6).$$

§**10Gd. Permutationen auf unendlichen Mengen.** Dass die Existenz der Signatur alles andere als selbstverständlich ist, zeigt folgendes gegenläufige Ergebnis:

Satz 10G11. *Sei X eine unendliche Menge. Dann ist die Kommutatorgruppe der symmetrischen Gruppe S_X wieder S_X. Anders gesagt, jeder Gruppenhomomorphismus $S_X \to A$ in eine abelsche Gruppe A ist trivial.*

Insbesondere gibt es keinen Signaturhomomorphismus $S_X \twoheadrightarrow \{\pm 1\}$.

Bevor wir dies allgemein beweisen, ist ein Beispiel erhellend. Für endliches X enthält die Kommutatorgruppe von S_X keine Transposition. Im unendlichen Fall ist dies anders. Wir betrachten hierzu die Menge $X = \mathbb{Z}$. Sei $\tau\colon k \mapsto k+2$ und $\rho = (1,2)(3,4)(5,6)\cdots$. Es gilt $\tau\rho^{-1}\tau^{-1} = (3,4)(5,6)(7,8)\cdots$ und somit ist $\rho\tau\rho^{-1}\tau^{-1} = (1,2)$ ein Kommutator.

Das folgende Beispiel verallgemeinert diesen Trick:

Beispiel 10G12. Jeder Zykel $\sigma = (1,\dots,n)$ ist ein Kommutator in $S_{\mathbb{Z}}$:

Hierzu wählen wir $\rho \in S_{\mathbb{Z}}$ als $\rho = (1,\dots,n)(n+1,\dots,2n)(2n+1,\dots,3n)\cdots$, das heißt

$$\rho(x) = \begin{cases} x & \text{für } x \leq 0, \\ x+1 & \text{für } x > 0 \text{ und } n \nmid x, \\ x-n+1 & \text{für } x > 0 \text{ und } n \mid x. \end{cases}$$

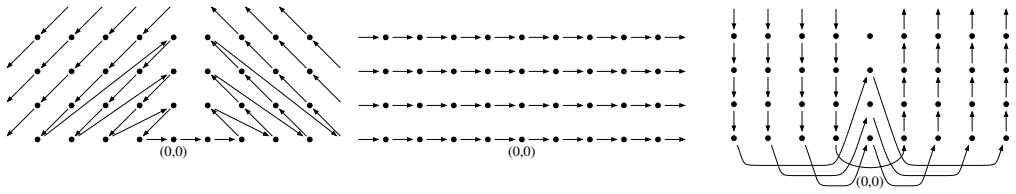
Für $\tau\colon \mathbb{Z} \to \mathbb{Z}$ mit $\tau(x) = x+n$ gilt dann $\rho\cdot\tau\rho^{-1}\tau^{-1} = \sigma$.

BEWEIS DES SATZES. Sei X eine unendliche Menge und sei $\sigma \in \mathrm{S}_X$ eine Permutation. Wir zerlegen $X = \bigsqcup_{\lambda\in\Lambda} X_\lambda$ in die Bahnen X_λ unter der Aktion von σ. Dann ist jedes $\sigma_\lambda = \sigma|_{X_\lambda} : X_\lambda \to X_\lambda$ ein Zykel, entweder endlicher Länge oder unendlicher Länge.

Jeder Zykel σ_λ unendlicher Länge ist ein Kommutator auf seinem Träger X_λ gemäß dem nachfolgenden Lemma 10G13. Die Zykel endlicher Länge haben wir schon abgehandelt: Bei ungerader Länge ist σ_λ ein Kommutator in S_{X_λ} gemäß 10G9. Zykel gerader Länge fassen wir in Paaren $\sigma_\mu \sqcup \sigma_\nu$ zusammen, und jedes solche Paar ist ein Kommutator in $\mathrm{S}_{X_\mu \sqcup X_\nu}$ gemäß 10G10. Sollte die Anzahl gerader Zykel ungerade sein, so können wir einen verbleibenden Zykel wie in 10G12 als Kommutator erzeugen. □

Ein einziger Punkt in diesem Beweis erfordert technische Virtuosität: Wie stellt man einen unendlichen Zykel als Kommutator dar, und zwar nur auf seinem Träger? Die folgende Konstruktion hierzu hat sich Oystein Ore (1951) ausgedacht:

Lemma 10G13. *Der unendliche Zykel $\zeta : \mathbb{Z} \to \mathbb{Z}$, $k \mapsto k+1$, ist ein Kommutator in $\mathrm{S}_\mathbb{Z}$.*



(a) Die Permutation σ (b) Die Permutation ρ (c) Die Permutation $\bar\rho$

ABBILDUNG 1. Drei Permutationen der Menge $X = \mathbb{Z} \times \mathbb{N}$

BEWEIS. Statt $\mathbb{Z}$ betrachten wir die Menge $X = \mathbb{Z} \times \mathbb{N}$ und hierauf die Permutation $\sigma : X \to X$ aus Abbildung 1(a). Diese lässt sich wie folgt in Formeln fassen:

$$\sigma(x,y) = \begin{cases} (x-1,y-1) & \text{für } x \le 0,\ y > 0, \\ (0,-x-1) & \text{für } x < 0,\ y = 0, \\ (1,0) & \text{für } x = 0,\ y = 0, \\ (x-1,y+1) & \text{für } x > 1, \\ (y+1,0) & \text{für } x = 1. \end{cases}$$

Die Menge X ist eine Bahn unter σ, also stiftet $f : \mathbb{Z} \to X$, $k \mapsto \sigma^k(0,0)$ eine Bijektion. Der Gruppenisomorphismus $f_* : \mathrm{S}_\mathbb{Z} \xrightarrow{\sim} \mathrm{S}_X$ bildet ζ auf σ ab. Es genügt also zu zeigen, dass σ ein Kommutator in S_X ist. Hierzu definieren wir $\rho, \bar\rho : X \to X$ durch $\rho(x,y) = (x+1,y)$ und

$$\bar\rho(x,y) = \begin{cases} (x,y-1) & \text{für } x < 0,\ y > 0, \\ (0,-x-1) & \text{für } x < -1,\ y = 0, \\ (1,0) & \text{für } x = -1,\ y = 0, \\ (y+2,0) & \text{für } x = 0, \\ (x,y+1) & \text{für } x > 0. \end{cases}$$

Diese sind in Abbildung 1(b,c) dargestellt. Wie man sieht haben ρ und $\bar{\rho}$ dieselbe Bahnenstruktur und sind daher konjugiert. Ausführlicher definieren wir $\tau\colon X \to X$ durch $\tau(x,y) = \bar{\rho}^x(y+1,0)$. Da $\{\ (y+1,0) \mid y \in \mathbb{N}\ \}$ ein Repräsentantensystem der Bahnen von $\bar{\rho}$ ist und jede Bahn unendliche Länge hat, ist τ eine Bijektion. Nach Konstruktion gilt $\tau\rho = \bar{\rho}\tau$, also $\bar{\rho} = \tau\rho\tau^{-1}$. Für den Kommutator rechnet man nach, dass $\tau\rho\tau^{-1}\rho^{-1} = \bar{\rho}\rho^{-1} = \sigma$ gilt. □

KAPITEL 11

Sylow–Sätze und Anwendungen

§11A. Einführung und Überblick

In diesem Kapitel widmen wir uns ausschließlich *endlichen* Gruppen.

Der Satz von Lagrange besagt, das für jede Untergruppe $H < G$ die Ordnung $|H|$ ein Teiler von $|G|$ ist. Umgekehrt muss allerdings für einen Teiler n von $|G|$ nicht unbedingt eine Untergruppe der Ordnung n in G existieren. Zum Beispiel enthält die alternierende Gruppe A_5 der Ordnung 60 keine Untergruppen der Ordnung 30, 20, 15 (siehe 10E12), wohl aber Untergruppen der Ordnung 2, 3, 4, 5, 6, 10, 12.

Der Satz von Cauchy bietet nun eine sehr nützliche, wenn auch notwendigerweise eingeschränkte Umkehrung des Satzes von Lagrange:

Satz 11A1 (Cauchy)**.** *Teilt eine Primzahl p die Ordnung der Gruppe G, dann existiert ein Element $x \in G$ der Ordnung p, und damit eine Untergruppe $\langle x \rangle < G$ der Ordnung p.*

Der norwegische Mathematiker Peter Ludwig SYLOW (1832–1918) hat die Bedeutung dieses Satzes erkannt und erheblich ausgebaut. Die Grundidee ist, von p zu möglichst hohen Potenzen p^e übergehen. Das Beste, das man hierbei erhoffen kann, ist in einer Gruppe G der Ordnung $|G| = p^e a$ mit $p \nmid a$ eine Untergruppe $P < G$ der Ordnung p^e zu finden.

Definition 11A2. Sei $p \in \mathbb{N}$ eine Primzahl. Sei G eine Gruppe der Ordnung $|G| = p^e a$ wobei $e, a \in \mathbb{N}$ und $p \nmid a$. Eine *p-Sylow-Untergruppe* von G ist eine Untergruppe $P < G$ der Ordnung $|P| = p^e$. Die Menge p-Sylow-Untergruppen von G bezeichnen wir mit $\mathrm{Syl}_p(G)$

Statt *p-Sylow-Untergruppe* sagen wir kurz *p-Sylow-Gruppe* von G. A priori könnte die Menge $\mathrm{Syl}_p(G)$ leer sein. Der Satz von Sylow klärt dies sehr zufriedenstellend auf:

Satz 11A3 (Sylow)**.** *Sei $p \in \mathbb{N}$ eine Primzahl. Sei G eine Gruppe der Ordnung $|G| = p^e a$ wobei $e, a \in \mathbb{N}$ und $p \nmid a$. Dann gilt:*

1. *Jede p-Untergruppe von G liegt in einer p-Sylow-Untergruppe von G.*
   Insbesondere existiert mindestens eine p-Sylow-Gruppe in G, also $\mathrm{Syl}_p(G) \neq \emptyset$.
2. *Je zwei p-Sylow-Untergruppen sind in G konjugiert.*
3. *Ihre Anzahl $m_p = \left|\mathrm{Syl}_p(G)\right|$ erfüllt $m_p \mid a$ und $m_p = 1 + kp$ mit $k \in \mathbb{N}$.*

Diese Sylow-Sätze sind ein erstes, mächtiges Werkzeug zur Strukturuntersuchung endlicher Gruppen. Dies werden wir durch vielfältige Anwendungen und Übungen illustrieren.

Als wichtigen Spezialfall halten wir fest:

Korollar 11A4. *Eine p-Sylow-Gruppe $P \in \mathrm{Syl}_p(G)$ ist einzig genau dann wenn $P \lhd G$.* □

§11B. Die Sylow-Sätze

§11Ba. Beweis des Satzes von Cauchy. Wir beginnen mit dem Satz von Cauchy:

BEWEIS. Wir betrachten die Menge

$$X = \{\, (a_1,\dots,a_p) \in G^p \mid a_1 \cdots a_p = 1 \,\}.$$

Diese hat $|G|^{p-1}$ Elemente, wie man anhand folgender Bijektion $X \cong G^{p-1}$ sieht:

$$\begin{aligned} X \to G^{p-1}, &\qquad (a_1,\dots,a_{p-1},a_p) \mapsto (a_1,\dots,a_{p-1}),\\ G^{p-1} \to X, &\qquad (a_1,\dots,a_{p-1}) \mapsto (a_1,\dots,a_{p-1},(a_1\cdots a_{p-1})^{-1}). \end{aligned}$$

Für jedes $(a_1,a_2,\dots,a_p) \in X$ gilt $a_2\cdots a_p a_1 = a_1^{-1}(a_1a_2\cdots a_p)a_1 = 1$, also liegt auch $(a_2,\dots,a_p,a_1)$ in X. Wir können daher auf X eine Abbildung $\sigma\colon X \to X$ definieren durch

$$\sigma(a_1,a_2,\dots,a_p) = (a_2,\dots,a_p,a_1).$$

Diese Abbildung erfüllt $\sigma^p = \mathrm{id}$, also operiert die Gruppe $\mathbb{Z}/p\mathbb{Z}$ mittels $\bar{n} \mapsto \sigma^n$. Jede Bahn hat Länge 1 oder p. Wegen $p \mid |X|$ impliziert die Bahnengleichung $p \mid |\mathrm{Fix}\,\sigma|$. Dabei ist $(a_1,\dots,a_p)$ genau dann ein Fixpunkt von σ, wenn $a_1 = \cdots = a_p$ gilt. Ein solcher Fixpunkt ist $(1,\dots,1)$, also gilt $|\mathrm{Fix}(\sigma)| \geq 1$, und damit $|\mathrm{Fix}(\sigma)| \geq p$. Also existiert ein weiterer Fixpunkt $(x,\dots,x) \in \mathrm{Fix}(\sigma)$ mit $x \neq 1$ und $x^p = 1$. □

Definition 11B1. Wir nennen $x \in G$ ein *p-Element*, wenn $\mathrm{ord}(x) = p^k$ für ein $k \in \mathbb{N}$.

Der Satz von Cauchy besagt demnach: Aus der Teilbarkeit $p \mid |G|$ folgt, dass G ein nicht-triviales p-Element enthält. Als unmittelbare Folgerung halten wir fest:

Korollar 11B2. *Eine endliche Gruppe G ist genau dann eine p-Gruppe, wenn jedes Element $x \in G$ ein p-Element ist.*

BEWEIS. "$\Rightarrow$" folgt mit Lagrange. "$\Leftarrow$" folgt mit Cauchy. □

§11Bb. Beweis der Sylow-Sätze. Sei $p \in N$ eine Primzahl und sei G eine Gruppe der Ordnung $|G| = p^e a$ wobei $e, a \in \mathbb{N}$ und $p \nmid a$. Die Sylow-Sätze sind trivialerweise erfüllt für $a = 1$: In diesem Fall gilt $\mathrm{Syl}_p(G) = \{G\}$ und $\mathrm{Syl}_q(G) = \{\{1\}\}$ für jede Primzahl $q \neq p$.

Wir können also im Folgenden $a > 1$ annehmen. Wir nennen eine p-Untergruppe $P < G$ *maximal*, wenn es keine p-Untergruppe $H < G$ mit $P \subsetneq H$ gibt.

Bemerkung 11B3. Ist $P < G$ eine p-Sylow-Gruppe, also $|P| = p^e$, dann ist P offenbar maximal. Bislang wissen wir aber noch nicht, ob es in G überhaupt p-Sylow-Gruppen gibt. Maximale p-Untergruppen $P < G$ gibt es hingegen immer, so dass dieser Anfang leicht gemacht ist. Im Folgenden werden wir zeigen, dass jede maximale p-Untergruppe $P < G$ tatsächlich $|P| = p^e$ erfüllt, also eine p-Sylow-Gruppe von G ist.

Lemma 11B4. *Sei $P < G$ eine maximale p-Untergruppe.*

1. *Der Index $|N_G(P) : P|$ ist teilerfremd zu p.*
2. *Ist a ein p-Element mit $aPa^{-1} = P$, dann gilt $a \in P$.*

BEWEIS. Nach Definition des Normalisators

$$N_G(P) = \{\, a \in G \mid aPa^{-1} = P \,\}$$

gilt $P \lhd N_G(P)$, und somit ist der Quotient $N_G(P)/P$ eine Gruppe. Sei

$$\pi\colon N_G(P) \to Q := N_G(P)/P$$

der Quotientenhomomorphismus.

(1) Teilt p den Index $|N_G(P) : P| = |Q|$, dann existiert nach dem Satz von Cauchy ein Element $\bar{a} \in Q$ der Ordnung p. Somit ist $\langle \bar{a} \rangle < Q$ eine Untergruppe der Ordnung p und ihr Urbild $\pi^{-1}(\langle \bar{a} \rangle) < N_G(P) < G$ ist eine Untergruppe der Ordnung $p \cdot |P|$, die P enthält. Dies widerspräche der Annahme, dass P eine maximale p-Untergruppe von G ist.

(2) Aus $aPa^{-1} = P$ folgt $a \in N_G(P)$. Wäre $a \notin P$, dann wäre $\pi(a) \in Q$ ein nicht-triviales p-Element, also teilte p die Ordnung $|Q| = |N_G(P) : P|$. Das aber widerspricht Teil (1). □

Lemma 11B5. *Sei P eine maximale p-Untergruppe von G.*

1. *Die Anzahl m der zu P konjugierten Untergruppen erfüllt $m \equiv 1 \mod p$.*
2. *Alle maximalen p-Untergruppen von G sind zu P konjugiert.*

BEWEIS. Sei $X = \{\, gPg^{-1} \mid g \in G \,\} = \{P_1, P_2, \ldots, P_m\}$ die Menge der zu P konjugierten Untergruppen in G. Jede von ihnen ist eine maximale p-Untergruppe. Die Gruppe G operiert auf X durch Konjugation, $G \times X \to X$, $(g, P_k) \mapsto gP_kg^{-1}$.

Sei $Q < G$ eine maximale p-Untergruppe. Auch Q operiert auf X durch Konjugation, und jede Bahn hat Länge p^ℓ für ein $\ell \in \mathbb{N}$. Was wäre eine Bahn der Länge 1? Für jedes $a \in Q$ gilt hier $aP_ka^{-1} = P_k$ und folglich $a \in P_k$ nach 11B4. Das bedeutet $Q < P_k$, und da auch Q eine maximale p-Gruppe ist, folgt $Q = P_k$.

Angewendet auf $Q = P$ bedeutet das: X zerfällt in den Fixpunkt P und nicht-triviale Bahnen, deren Länge durch p teilbar ist. Daher gilt $m \equiv 1 \mod p$.

Angewendet auf jede andere maximale p-Gruppe Q bedeutet dies: Wegen $m \equiv 1 \mod p$ muss Q mindestens einen Fixpunkt P_k haben, also $Q = P_k$. □

Lemma 11B6. *Jede maximale p-Untergruppe von G ist eine p-Sylow-Gruppe von G.*

Ausführlicher bedeutet dies: Sei G eine Gruppe der Ordnung $|G| = p^e a$ wobei $e, a \in \mathbb{N}$ und $p \nmid a$. Dann hat jede maximale p-Untergruppe $P < G$ die Ordnung $|P| = p^e$.

BEWEIS. Nach dem Satz von Lagrange gilt $|G| = |G : P| \cdot |P|$. Wir haben also zu zeigen, dass der Index $|G : P|$ teilerfremd zu p ist. Für $N = N_G(P)$ gilt $|G : P| = |G : N| \cdot |N : P|$. Hierbei ist $|N : P|$ teilerfremd zu p nach 11B4. Andererseits ist $m = |G : N|$ die Anzahl der zu P konjugierten Untergruppen in G (9F14), also $m \equiv 1 \mod p$ nach 11B5. □

Da jede p-Untergruppe von G in einer maximalen p-Untergruppe liegt, ist Lemma 11B6 zu folgender Aussage äquivalent: Jede p-Untergruppe von G liegt in einer p-Sylow-Gruppe von G. Insbesondere gibt es p-Sylow-Gruppen, also $\mathrm{Syl}_p(G) \neq \emptyset$.

§11C. Einfache Klassifikationssätze

Wir kennen bereits die Struktur jeder Gruppe G von Primzahlordnung $|G| = p$: Nach Lagrange ist G zyklisch (9A4), also $G \cong \mathbb{Z}/p\mathbb{Z}$. Auch die Struktur jeder Gruppe G der Ordnung $|G| = p^2$ ist uns bekannt: G ist abelsch (9F23), also gilt nach dem Klassifikationssatz (9D14) entweder $G \cong \mathbb{Z}/p^2$ oder $G \cong \mathbb{Z}/p \times \mathbb{Z}/p$.

Mit Hilfe der Sylow-Sätze können wir nun die Struktur weiterer Gruppen klären.

§11Ca. Gruppen der Ordnung pq. Hier eine erste schöne Anwendung:

Proposition 11C1. *Seien $p < q$ zwei Primzahlen.*

1. *Für $p \nmid q-1$ ist jede Gruppe G der Ordnung pq abelsch, und demnach $G \cong \mathbb{Z}/pq$.*
2. *Für $p \nmid q-1$ gibt es genau zwei Gruppen der Ordnung pq, nämlich die abelsche Gruppe $\mathbb{Z}/pq$ und die nicht-abelsche Gruppe $\mathbb{Z}/p \ltimes \mathbb{Z}/q$.*

BEWEIS. Sei $K \in \mathrm{Syl}_q(G)$. Wegen $m_q = 1 + kq \mid p$ und $q > p$ bleibt nur $m_q = 1$, also $K \lhd G$. Sei $H \in \mathrm{Syl}_p(G)$. Wegen $m_p = 1 + hp \mid q$ bleiben nur $m_p \in \{1, q\}$. In beiden Fällen gilt $H \cap K = \{1\}$ und $HK = G$ nach Lagrange.

Im Fall $p \nmid q-1$ gilt $m_p = 1$, also $H \lhd G$. Mit 9C8 folgt $G = H \times K$. Für Gruppen von Primzahlordnung wissen wir $H \cong \mathbb{Z}/p$ und $K \cong \mathbb{Z}/q$. Mit dem chinesischen Restsatz 9D7 schließen wir $G \cong \mathbb{Z}/pq$.

Im Fall $p \mid q-1$ gibt es die zusätzliche Möglichkeit $m_p = q$. In diesem Fall kommutieren H und K nicht. Die Konjugation von H auf K definiert eine Operation $H \times K \to K$ durch $(h,k) \mapsto hkh^{-1}$. Dies entspricht einem nicht-trivialen Gruppenhomomorphismus $H \to \mathrm{Aut}(K)$. Da H zyklisch von Primzahlordnung ist, muss dieser injektiv sein. Da K zyklisch von Primzahlordnung q ist, wissen wir $\mathrm{Aut}(K) \cong (\mathbb{Z}/q)^\times$. Das Bild ist also die eindeutige Untergruppe in $\mathrm{Aut}(K)$ der Ordnung p. Es folgt $G = K \rtimes H$. □

Beispiel 11C2. Ist $p \geq 3$ eine Primzahl, dann existieren genau zwei nicht-isomorphe Gruppen der Ordnung $2p$, nämlich

- die zyklische Gruppe $\mathbb{Z}/2p \cong \mathbb{Z}/p \times \mathbb{Z}/2$
- sowie die Diedergruppe $D_n \cong \mathbb{Z}/p \rtimes \mathbb{Z}/2$.

Beispiel 11C3. Jede Gruppe der Ordnung $15, 33, 35, 51, \ldots$ ist zyklisch.
Es gibt je genau zwei nicht-isomorphe Gruppen der Ordnung $21, 39, 55, 57, \ldots$.

§11Cb. Einfache Gruppen der Ordnung 60. Wir wollen das folgende schöne Ergebnis zeigen:

Satz 11C4. *Jede einfache Gruppe G der Ordnung $|G| = 60$ ist isomorph zu A_5.*

Zum Beweis schlagen wir eine Folge von Übungen vor:

Übung 11C5. Wenn $K < \mathrm{S}_n$ eine Untergruppe vom Index 2 ist, dann gilt $K = \mathrm{A}_n$.

Übung 11C6. Sei G eine endliche Gruppe und $m > 1$ die Anzahl der p-Sylow-Gruppen.

1. Es gibt dann einen nicht-trivialen Homomorphismus $\varphi\colon G \to \mathrm{S}_m$.
2. Ist G einfach, so ist φ injektiv, also ist $|G|$ ein Teiler von $m!$.

Übung 11C7. Sei G eine einfache Gruppe der Ordnung $|G| = 60$

1. In G gibt es genau zehn 3-Sylow-Gruppen.
2. In G gibt es genau sechs 5-Sylow-Gruppen.
3. In G gibt es genau fünf 2-Sylow-Gruppen.
4. Es existiert ein nicht-trivialer Gruppenhomomorphismus $G \to \mathrm{S}_5$.

Folgern Sie hieraus, dass $G \cong \mathrm{A}_5$ gilt.

§11D. Auflösbare Gruppen

§**11Da. Auflösbarkeit.** Eine endliche Gruppe G heißt *auflösbar* wenn es eine Folge

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = \{1\}$$

von Untergruppen gibt, so dass jeweils $G_{i+1} \lhd G_i$ normal ist von Primzahlindex.

Die sukzessiven Quotientengruppen G_i/G_{i+1} sind dann zyklisch von Primzahlordnung.

Beispiel 11D1. Jede zyklische Gruppe $\mathbb{Z}/n$ ist auflösbar.

Aus der Primfaktorzerlegung $n = p_1 p_2 \cdots p_r$ erhalten wir nämlich die Auflösung

$$\mathbb{Z}/n\mathbb{Z} \quad \rhd \quad p_1\mathbb{Z}/n\mathbb{Z} \quad \rhd \quad p_1p_2\mathbb{Z}/n\mathbb{Z} \quad \rhd \quad \ldots \quad \rhd \quad p_1p_2\cdots p_r\mathbb{Z}/n\mathbb{Z} = \{0\}.$$

Beispiel 11D2. Jede endliche abelsche Gruppe A ist auflösbar.

Nach dem Klassifikationssatz gilt nämlich $A \cong \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_s$, und die hier auftretenden zyklischen Gruppen können wir sukzessive auflösen.

Beispiel 11D3. Jede p-Gruppe ist auflösbar (Satz 9F26). Dies war in Kapitel 9 eine erste Anwendung der Bahnengleichung. In diesem Fall gilt sogar stärker $G_i \lhd G$ für alle i. Für Auflösbarkeit wie oben definiert reicht die schwächere Bedingung $G_i \lhd G_{i-1}$.

Beispiel 11D4. Ist G eine nicht-abelsche einfache Gruppe, wie zum Beispiel die alternierende Gruppe A_n für $n \geq 5$, dann ist G nicht auflösbar.

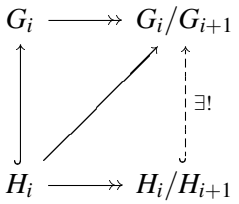
§**11Db. Untergruppen und Quotienten.** Zur Untersuchung der Auflösbarkeit endlicher Gruppen ist folgendes Kriterium sehr nützlich:

Satz 11D5. *Sei G eine endliche Gruppe.*

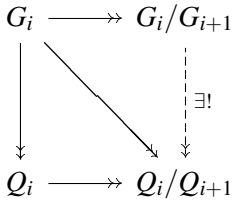
1. *Ist G auflösbar, dann ist auch jede Untergruppe $H < G$ und jede Quotientengruppe G/K auflösbar.*
2. *Sind die normale Untergruppe $K \lhd G$ und die Quotientengruppe G/K auflösbar, dann ist auch G auflösbar.*

BEWEIS. Sei G auflösbar durch $G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = \{1\}$. Für jedes Untergruppe $H < G$ ist dann $H_i = H \cap G_i$ eine Untergruppe von H. Es gilt $H_i < G_i$ und $H_{i+1} = H_i \cap G_{i+1}$ und somit $H_{i+1} \lhd H_i$. Der Index $|H_i : H_{i+1}|$ ist entweder gleich 1 oder

eine Primzahl, wie man aus folgendem Diagramm abliest:



Sei $K \lhd G$ eine normale Untergruppe und sei $\pi\colon G \to Q$ der Quotientenhomomorphismus. Die Untergruppen $Q_i = \pi(G_i)$ erfüllen $Q_{i+1} \lhd Q_i$ gemäß der Korrespondenz normaler Untergruppen (9B15). Der Index $|Q_i : Q_{i+1}|$ ist entweder gleich 1 oder eine Primzahl, wie man aus folgendem Diagramm abliest:



Sei nun umgekehrt $Q = G/K$ auflösbar durch $Q = Q_0 \rhd \ldots \rhd Q_s = \{1\}$. Wir erhalten durch $G_k = \pi^{-1}(Q_k)$ eine Kette $G = G_0 \rhd \ldots \rhd G_s = K$. Die sukzessiven Indizes bleiben dabei erhalten (9B15). Ist zudem K auflösbar durch $K = G_s \rhd \ldots \rhd G_r = \{1\}$, dann ist G auflösbar durch die Zusammensetzung $G = G_0 \rhd \ldots \rhd G_s \rhd \ldots \rhd G_r$. □

Beispiel 11D6. Die symmetrische Gruppe S_n mit $n \geq 5$ ist nicht auflösbar: Hier gilt $\mathrm{A}_n \lhd \mathrm{S}_n$. Zwar ist die Quotientengruppe $\mathrm{S}_n/\mathrm{A}_n \cong \{\pm 1\}$ auflösbar, aber A_n ist es nicht.

§**11Dc. Abgeleitete Gruppen.** Aus jeder Gruppe G leiten wir *Kommutatorgruppe* ab:

$$D(G) := [G,G] = \langle\, [a,b] \mid a,b \in G \,\rangle\,.$$

Dies ist eine normale Untergruppe in G und die Quotientengruppe $G/[G,G]$ ist die Abelschmachung von G (§9Cb). Induktiv definieren wir die *abgeleiteten Gruppen* durch $D^0(G) = G$, $D^1(G) = D(G)$ und $D^{k+1}(G) = D(D^k(G))$ für alle $k \in \mathbb{N}$.

Satz 11D7. *Für jede endliche Gruppe sind äquivalent:*

1. *Die Gruppe G ist auflösbar, das heißt:*
   Es existiert eine Kette $G = G_0 \rhd \ldots \rhd G_n = \{1\}$ mit G_i/G_{i+1} von Primzahlordnung.
2. *Es existiert eine Kette $G = G_0 \rhd \ldots \rhd G_n = \{1\}$ mit G_i/G_{i+1} zyklisch.*
3. *Es existiert eine Kette $G = G_0 \rhd \ldots \rhd G_n = \{1\}$ mit G_i/G_{i+1} abelsch.*
4. *Die Kette $G = D^0(G) \rhd D^1(G) \rhd \ldots$ endet mit $D^n(G) = \{1\}$ für ein $n \in \mathbb{N}$.* □

BEWEIS. Die Implikationen "(1) ⇒ (2) ⇒ (3)" sind klar, denn jedesmal wird die Bedingung abgeschwächt. Für "(3) ⇒ (4)" betrachten wir eine Kette $G = G_0 \rhd \ldots \rhd G_n = \{1\}$, für die G_k/G_{k+1} abelsch ist, und beweisen $D^k(G) < G_k$ durch Induktion über k. Zunächst gilt $D^0(G) < G$. Da G_k/G_{k+1} abelsch ist, gilt $[G_k,G_k] < G_{k+1}$. Aus $D^k(G) < G_k$ folgt dann $D^{k+1}(G) = [D^k(G),D^k(G)] < [G_k,G_k] < G_{k+1}$. Damit haben wir $D^k(G) < G_k$ für alle k gezeigt. Aus $G_n = \{1\}$ folgt $D^n(G) = \{1\}$.

Die Umkehrung "(4) $\Rightarrow$ (3)" ist klar, denn $D^k(G) \rhd D^{k+1}(G)$ und die Quotientengruppe $D^k(G)/D^{k+1}(G)$ ist abelsch. Die Verschärfungen "(3) $\Rightarrow$ (2) $\Rightarrow$ (1)" zeigt man wie in den einführenden Beispielen 11D1 und 11D2. □

Der Satz gibt eine etwas größere Flexibilität zum Nachweis der Auflösbarkeit. Die ersten drei Kriterien "Es existiert eine Kette…" lassen die Wahl der Kette offen, was manchmal ein Vorteil ist, aber keinen konkreten Hinweis zur Suche gibt. Das vierte Kriterium gibt eine konkrete Kette vor, nämlich die abgeleiteten Untergruppen.

Beispiel 11D8. Die symmetrische Gruppe S_n mit $n \geq 5$ ist nicht auflösbar: Hier gilt $D(\mathrm{S}_n) = \mathrm{A}_n$ und $D(\mathrm{A}_n) = \mathrm{A}_n$. Die Kette der abgeleiteten Gruppe wird also bei $\mathrm{A}_n \neq \{1\}$ stationär.

§**11Dd. Gruppen der Ordnung ≤ 60.** Wir schließen mit folgendem schönen Ergebnis, dass die Auflösbarkeit von Gruppen bis zur Ordnung ≤ 60 klärt:

Satz 11D9. *Jede Gruppe G der Ordnung $|G| < 60$ ist auflösbar. Mit Ordnung 60 gibt es genau eine nicht-auflösbare Gruppe, nämlich die alternierende Gruppe A_5.*

Diesen Satz zeigt man durch geduldige Anwendung der Sylow-Sätze:

Übung 11D10. Gruppen der Ordnung pqr sind auflösbar (mit $p < q < r$ prim).

Übung 11D11. Gruppen der Ordnung p^2q sind auflösbar.

Übung 11D12. Gruppen der Ordnung $24, 36, 40, 48, 54, 56$ sind auflösbar.

Übung 11D13. Warum muss eine nicht-auflösbare Gruppe der Ordnung 60 einfach sein?

§11E. Übungen und Ergänzungen

§11Ea. Weitere Klassifikationen kleiner Gruppen.

Übung 11E1. Man bestimme alle Gruppen der Ordnung $45 = 3^2 \cdot 5$ bis auf Isomorphie.

Übung 11E2. Man bestimme alle Gruppen der Ordnung $665 = 5 \cdot 7 \cdot 19$ bis auf Isomorphie.

Übung 11E3. Man bestimme alle Gruppen der Ordnung $1105 = 5 \cdot 13 \cdot 17$ bis auf Isomorphie.

Übung 11E4. Sei G eine Gruppe der Ordnung 30. Für $p = 2, 3, 5$ sei m_p die Anzahl der p-Sylow-Gruppen in G. Zudem sei H_p eine p-Sylow-Gruppe von G.

1. Man zeige, dass G genau $m_5 \cdot 4$ Elemente der Ordnung 5 enthält sowie $m_3 \cdot 2$ Elemente der Ordnung 3. Man folgere hieraus $m_5 = 1$ oder $m_3 = 1$.
2. $K = H_5H_3$ ist eine Untergruppe der Ordnung 15. Sie ist zyklisch und normal in G.
3. Es gilt $G = K \rtimes H_2$ und für $H_2 \to \mathrm{Aut}(K)$ gibt es vier Möglichkeiten.

Man schließe hieraus, dass $G \cong \mathbb{Z}/30$ oder $G \cong D_{15}$ oder $G \cong D_5 \times \mathbb{Z}/3$ oder $G \cong \mathbb{Z}/5 \times D_3$.

Übung 11E5. Sei G eine Gruppe der Ordnung 255. Für $p = 3, 5, 17$ sei m_p die Anzahl der p-Sylow-Gruppen in G. Zudem sei H_p eine p-Sylow-Untergruppe von G.

1. Man zeige, dass H_{17} normal ist in G, und somit ist $K = H_{17}H_5$ eine Untergruppe.
2. Man zeige, dass $K = H_{17} \rtimes H_5$ ein direktes Produkt ist. Somit ist K zyklisch.

3. Man benutze $K < N_G(H_5)$ um $m_5 = |G : N_G(H_5)| \leq 3$ zu zeigen.
4. Man folgere $m_5 = 1$, also ist auch H_5 normal in G.
5. Man zeige, dass $G = K \rtimes H_3$ ein direktes Produkt ist, also ist G zyklisch.

Die Technik der letzten Übung funktioniert ebenso für Gruppen der Ordnung $3 \cdot 5 \cdot 17 \cdot 257$ und $3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$. Der folgende Abschnitt liefert das allgemeine Kriterium.

§**11Eb. Für welche Ordnungen n sind alle Gruppen zyklisch?** Zu jeder Ordnung $n \in \mathbb{N}_{\geq 1}$ gibt es mindestens eine Gruppe der Ordnung n, nämlich die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$. Bei der Klassifikation kleiner Gruppen stößt man gelegentlich auf Ordnungen n, sodass bis auf Isomorphie alle Gruppen der Ordnung n zyklisch sind.

Der folgende Satz erlaubt eine vollständige Beschreibung dieses Phänomens:

Satz 11E6. *Sei $n \in \mathbb{N}_{\geq 1}$. Genau dann gibt es bis auf Isomorphie nur eine Gruppe der Ordnung n wenn $\mathrm{ggT}(n, \varphi(n)) = 1$ gilt. (Hierbei ist φ die Eulersche φ-Funktion.)*

Übung 11E7. Für $n \in \mathbb{N}$ gilt $\mathrm{ggT}(n, \varphi(n)) = 1$ genau dann, wenn die Primfaktorzerlegung $n = p_1 p_2 \dots p_k$ sowohl $p_1 < p_2 < \dots < p_k$ als auch $p_i \nmid p_j - 1$ für alle i, j erfüllt.

Übung 11E8. Man zeige den obigen Satz:

1. Wenn $\mathrm{ggT}(n, \varphi(n)) = 1$ gilt, dann ist jede Gruppe der Ordnung n zyklisch.
2. Wenn alle Gruppen der Ordnung n zyklisch sind, dann gilt $\mathrm{ggT}(n, \varphi(n)) = 1$.

Übung 11E9. Man bestimme alle Gruppen der Ordnung 595 bis auf Isomorphie.

§**11Ec. Matrixgruppen.**

Übung 11E10. Sei p eine Primzahl. Man konstruiere einen Gruppenisomorphismus

$$\mathrm{Aut}((\mathbb{Z}/_p)^n, +) \cong \mathrm{GL}_n(\mathbb{Z}/_p).$$

Übung 11E11. Sei $\mathbb{F}_q$ ein Körper mit q Elementen, zum Beispiel $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p. Man zeige, die Gruppe $\mathrm{GL}_n(\mathbb{F}_q)$ hat Ordnung

$$\left|\mathrm{GL}_n(\mathbb{F}_q)\right| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

Was ist die Ordnung von $\mathrm{SL}_n(\mathbb{F}_q)$?

Übung 11E12. Man konstruiere einen Gruppenisomorphismus $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) \cong S_3$. *Hinweis:* Man lasse $GL_2(\mathbb{F}_2)$ auf den drei Geraden des $\mathbb{F}_2$-Vektorraums $\mathbb{F}_2^2$ operieren.

Wenden wir die Sylow-Sätze auf $G = \mathrm{GL}_n(\mathbb{F}_p)$ an. Es gilt $|G| = p^e a$ mit $e = \frac{1}{2}n(n-1)$. Wie sieht eine Untergruppe $P < \mathrm{GL}_n(\mathbb{F}_p)$ mit der maximal möglichen Ordnung p^e aus?

Übung 11E13. Man zeige, dass die oberen Dreiecksmatrizen

$$P = \left\{ \begin{pmatrix} 1 & * & * & * & * \\ 0 & 1 & * & * & * \\ 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \right\}$$

eine Untergruppe bilden, und zwar der Ordnung $p^{n(n-1)/2}$.

Wir wissen aus dem Satz von Cayley, dass man jede Gruppe als Untergruppe einer symmetrischen Gruppe darstellen kann. Nun lassen sich symmetrische Gruppen ihrerseits als Matrixgruppen realisieren:

Übung 11E14. Sei K ein Körper. Für eine Permutation $\sigma \in \mathrm{S}_n$ sei $A_\sigma \in K^{n\times n}$ die Matrix mit den Spalten $e_{\sigma(i)}$. Man zeige, dass die Abbildung $\varphi\colon S_n \to \mathrm{GL}_n K$, $\sigma \mapsto A_\sigma$, ein injektiver Gruppenhomomorphismus ist. Was ist $\det A_\sigma$?

Hieraus folgt, dass jede endliche Gruppe G als Matrixgruppe darstellbar ist.

Übung 11E15. Jede endliche p-Gruppe lässt sich als eine Gruppe von oberen Dreiecksmatrizen über $\mathbb{F}_p$ realisieren.

§**11Ed. Symmetrische Gruppen.** Wir wollen die Sylow-Sätze anhand der symmetrische Gruppe S_n illustrieren und zu jeder Primzahl p eine konkrete p-Sylow-Gruppe in S_n konstruieren. Zunächst gilt es, deren Größe zu bestimmen:

Übung 11E16. Wir zerlegen $n! = p^e a$ mit $e, a \in \mathbb{N}$ sodass $p \nmid a$. Dann gilt

$$e = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \dots$$

Nach den Sylow-Sätzen gibt es nun eine Untergruppe $P < \mathrm{S}_n$ der maximal möglichen Ordnung p^e. Wie sieht eine solche Gruppe aus? Betrachten wir zum Beispiel $p = 3$ und kleine Grade $n = 1,2,3,4,\dots$:

Für $n = 3,4,5$ gilt $e = 1$. Eine 3-Sylow-Gruppe ist zum Beispiel

$$P = \big\langle (1,2,3) \big\rangle .$$

Für $n = 6,7,8$ gilt $e = 2$. Eine 3-Sylow-Gruppe ist

$$P = \big\langle (1,2,3), (4,5,6) \big\rangle .$$

Für $n = 9,10,11$ gilt $e = 4$. Eine 3-Sylow-Gruppe ist

$$P = \left\langle \begin{matrix} (1,2,3), (4,5,6), (7,8,9), \\ (1,4,7)(2,5,8)(3,6,9) \end{matrix} \right\rangle .$$

Für $n = 12,13,14$ gilt $e = 5$. Eine 3-Sylow-Gruppe ist

$$P = \left\langle \begin{matrix} (1,2,3), (4,5,6), (7,8,9), \quad (10,11,12), \\ (1,4,7)(2,5,8)(3,6,9) \end{matrix} \right\rangle .$$

Für $n = 15,16,17$ gilt $e = 6$. Eine 3-Sylow-Gruppe ist

$$P = \left\langle \begin{matrix} (1,2,3), (4,5,6), (7,8,9), \quad (10,11,12), (13,14,15), \\ (1,4,7)(2,5,8)(3,6,9) \end{matrix} \right\rangle .$$

Für $n = 18,19,20$ gilt $e = 8$. Eine 3-Sylow-Gruppe ist

$$P = \left\langle \begin{matrix} (1,2,3), (4,5,6), (7,8,9), \quad (10,11,12), (13,14,15), (16,17,18), \\ (1,4,7)(2,5,8)(3,6,9), \qquad (10,13,16)(11,14,17)(12,15,18) \end{matrix} \right\rangle .$$

Übung 11E17. Man setze diese Folge fort. Wie sieht eine 3-Sylow-Gruppe von S_{27} aus?

§**11Ee. Sätze von Sylow und Cayley.** Für jede endliche Gruppe G existiert ein injektiver Gruppenhomomorphismus $G \hookrightarrow \mathrm{S}_n$ für gewisse n. Man kann sich fragen, welches für G das kleinste n ist. Sicherlich ist $n = |G|$ immer möglich, aber meist zu groß:

Übung 11E18. Betrachten wir die Diedergruppe D_4 der Ordnung 8.

1. Man zeige $D_4 \hookrightarrow \mathrm{S}_4$ indem man eine zu D_4 isomorphe Untergruppe $H < \mathrm{S}_4$ angibt. Gibt es solche Gruppen auch in S_n mit $n < 4$?

Betrachten wir nun die Quaternionengruppe Q, ebenfalls der Ordnung 8.

1. Man erläutere zunächst $Q \ncong D_4$.
2. Ist H eine 2-Sylow-Gruppe in S_4? in S_5?
   Gibt es eine Untergruppe in S_5 isomorph zu Q?
3. Man finde $K < \mathrm{S}_6$ isomorph zu $D_4 \times \mathbb{Z}/2\mathbb{Z}$. Ist K eine 2-Sylow-Gruppe in S_6? in S_7? Gibt es eine Untergruppe in S_7 isomorph zu Q?

Welches ist demnach der minimale Grad n für eine Einbettung $Q \hookrightarrow \mathrm{S}_n$?

TEIL III

Grundlagen der Körpertheorie

KAPITEL 12

Körpererweiterungen

§12A. Einleitung und Überblick

Zerfällung von Polynomen über den komplexen Zahlen. Der Hauptsatz der Algebra der komplexen Zahlen besagt, dass der Körper $\mathbb{C}$ der komplexen Zahlen *algebraisch abgeschlossen* ist. Ausführlicher bedeutet dies: Zu jedem Polynom

$$P = X^n + c_1 X^{n-1} + \cdots + c_{n-1} X + c_n$$

in $\mathbb{C}[X]$ existieren Nullstellen $a_1, \ldots, a_n \in \mathbb{C}$ sodass gilt

$$P = (X - a_1) \cdots (X - a_n).$$

Ist P ein Polynom über einem Teilkörper K von $\mathbb{C}$, zum Beispiel $K = \mathbb{Q}$, dann nennen wir den von den Nullstellen $a_1, \ldots, a_n$ über K erzeugten Teilkörper $E = K(a_1, \ldots, a_n)$ den *Zerfällungskörper* von P über K. Anders gesagt, E ist der kleinste Teilkörper von $\mathbb{C}$, der K umfasst und über dem das Polynom P zerfällt. In der Galois-Theorie werden wir die Struktur solcher Zerfällungskörper nutzen zum Studium der Auflösbarkeit der Gleichung

$$X^n + c_1 X^{n-1} + \cdots + c_{n-1} X + c_n = 0.$$

Bemerkung. Der Körper $\mathbb{R}$ der reellen Zahlen ist nicht algebraisch abgeschlossen, wie das Polynom $X^2 + 1$ und andere Beispiele zeigen. Die Frage nach der Existenz komplexer Nullstellen entstand im 17. Jahrhundert und führte nach einer wechselvollen Geschichte im 18. Jahrhundert zu der obigen präzisen Formulierung und den ersten Beweisversuchen von d'Alembert (1746), Euler (1749), Lagrange (1772), Laplace (1795) und anderen. Gauß kritisierte in seiner Dissertation (1799) die Unzulänglichkeiten aller bisherigen Beweise und entwickelte seinen eigenen Beweis, der allgemein als erster Beweis dieses Satzes anerkannt wird. (Auch Gauß' geometrisches Argument bedurfte allerdings einer Vervollständigung durch Ostrowski 1920.) Seit Gauß' Dissertation wurden zahlreiche Beweise entwickelt, wahlweise mit Methoden der Analysis, der Algebra, oder der Topologie.

Der von Gauß eingeführte Name "Fundamentalsatz der Algebra" stammt aus der Kindheit der Algebra, als diese sich noch hauptsächlich mit reellen und komplexen Zahlen beschäftigte. Heute ist der Name eher irreführend: Der Satz ist wenig fundamental und handelt kaum von Algebra. Der Hauptgegenstand sind die komplexen Zahlen, und diese sind neben ihren algebraischen vor allem durch ihre analytischen/metrischen/topologischen Eigenschaften charakterisiert. Aus heutiger Sicht nennt man diesen Satz daher besser den "Hauptsatz der Algebra der komplexen Zahlen", aber der traditionelle Name besteht natürlich fort.

Verallgemeinerung auf beliebige Körper. Zwar ist $\mathbb{C}$ ein äußerst wichtiger Körper, aber bei weitem nicht der einzige interessante. Zudem sind nicht alle Körper Teilkörper von $\mathbb{C}$. Wir lösen daher in diesem Kapitel die grundlegende Frage, wie man zu einem Polynom über einem beliebigen Körper K einen Zerfällungskörper konstruiert.

Den ersten Schritt in diese Richtung unternahm Leopold KRONECKER:

Satz (Kronecker)**.** *Sei K ein Körper. Zu jedem Polynom $P \in K[X]$ vom Grad $\deg P \geq 1$ existiert ein Erweiterungskörper E über K in dem P eine Nullstelle hat.*

Durch wiederholte Adjunktion von Wurzeln erhalten wir so alle Nullstellen:

Satz. *Zu jedem Polynom $P \in K[X]^*$ über K existiert ein Zerfällungskörper E über K.*
Je zwei Zerfällungskörper E und E' von P über K sind isomorph über K.

Schließlich werden wir hieraus einen algebraischen Abschluss herstellen:

Satz. *Zu jedem Körper K existiert ein algebraischer Abschluss C über K.*
Je zwei algebraische Abschlüsse C und C' über K sind isomorph über K.

Vorgehensweise. Der Hauptsatz der Algebra der komplexen Zahlen dient für die Entwicklung dieses Kapitels nicht als Voraussetzung sondern als leuchtendes Vorbild. (Wir werden ihn allenfalls in Beispielen und Anwendungen benutzen.)

Die angekündigten Ergebnisse über beliebigen Körpern gewinnen wir bequem mit den Werkzeugen, die wir in den vorangegangenen Kapitel entwickelt haben, nämlich den Grundzügen der Ringtheorie (Polynomringe, Primfaktorzerlegung, Ideale, Quotienten, ...) sowie der linearen Algebra (Vektorräume, Basen, Dimensionsformel 8F5). Die Entwicklung ist weitestgehend elementar, braucht aber etwas Sorgfalt. Ich habe daher nicht vor detaillierten Beweisen zurückgeschreckt. Die hier bereitgestellten Begriffe und Techniken werden uns auch in den folgenden Kapiteln gute Dienste leisten.

§12B. Körpererweiterungen

§12Ba. Körpererweiterungen. Sei E ein Körper. Ist $K \subset E$ ein Teilkörper, dann schreiben wir abkürzend $K < E$. Umgekehrt nennen wir dann E einen *Erweiterungskörper* von K oder kurz eine *Erweiterung* des Körpers K. Das Paar $E|K$ nennen wir eine *Körpererweiterung*. In Diagrammen schreiben wir

$$\text{statt} \quad \begin{array}{c} E \\ \uparrow \\ K \end{array} \qquad \text{kurz} \quad \begin{array}{c} E \\ | \\ K \end{array} .$$

Beispiel 12B1. Die Körper $\mathbb{Q} < \mathbb{R} < \mathbb{C}$ werden durch sukzessive Erweiterung konstruiert: Der Körper $\mathbb{R}$ der reellen Zahlen ist eine Erweiterung des Körpers $\mathbb{Q}$ der rationalen Zahlen. Der Körper $\mathbb{C}$ der komplexen Zahlen ist eine Erweiterung des Körpers $\mathbb{R}$ der reellen Zahlen. (Ebenso ist der Körper $\mathbb{C}$ auch eine Erweiterung von $\mathbb{Q}$.)

Beispiel 12B2. Bei Konstruktionen mit Zirkel und Lineal haben wir in Kapitel 1 zu $c \in \mathbb{Q}_{>0}$ die Körpererweiterung $\mathbb{Q}[\sqrt{c}] = \{\, a+b\sqrt{c} \mid a,b \in \mathbb{Q} \,\}$ von $\mathbb{Q}$ betrachtet (§1Bb). Allgemeiner: Für alle $\xi \in \mathbb{C}$ mit $\xi^2 \in \mathbb{Q}$ ist $\mathbb{Q}[\xi] = \{\, a+b\xi \mid a,b \in \mathbb{Q} \,\}$ ein Körper mit $\mathbb{Q} < \mathbb{Q}[\xi] < \mathbb{C}$.

Beispiel 12B3. Zu jedem Körper K enthält der Polynomring $K[X]$ den Körper K als Unterring. Dies gilt auch für den Bruchkörper $K(X) = \{\, P/Q \mid P,Q \in K[X], Q \neq 0 \,\}$ der rationalen Funktionen in X. Wegen $K \subset K[X] < K(X)$ ist $K(X)$ eine Körpererweiterung von K.

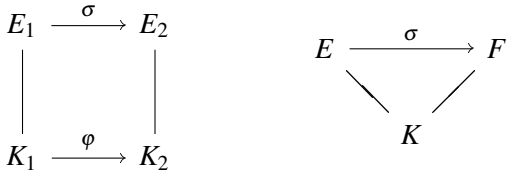
Beispiel 12B4. Ist K ein Körper und $P \in K[X]$ ein irreduzibles Polynom über K, dann ist das Ideal (P) maximal und der Quotient $E = K[X]/(P)$ demnach ein Körper. Die Quotientenabbildung $\pi\colon K[X] \to E$ ist injektiv auf K, denn $K \cap (P) = \{0\}$. Wir können also K mit seinem Bild $\pi(K) < E$ identifizieren, und somit $E|K$ als Erweiterungskörper betrachten.

Dieses einfache aber sehr flexible Beispiel wird für algebraische Körpererweiterungen im Folgenden eine fundamentale Rolle spielen.

§**12Bb. Homomorphismen.** Wie zu jedem mathematischen Objekt stellt sich auch für Körpererweiterungen die natürliche Frage, welche Homomorphismen wir betrachten. Dies wird uns Klarheit und die sprachlichen Mittel für die weiteren Untersuchungen verschaffen.

Der Homomorphismusbegriff von Ringen überträgt sich auf die Unterkategorie der Körper. Wir erinnern daran, dass jeder Homomorphismus $\varphi\colon K \to R$ eines Körpers K in einen Ring R mit $1 \neq 0$ injektiv ist (3B8). Insbesondere sind Homomorphismen zwischen Körpern stets injektiv. Für Körpererweiterungen vereinbaren wir folgenden Sprachgebrauch:

Definition 12B5. Seien K_1 und K_2 Körper und sei $\varphi\colon K_1 \to K_2$ ein Homomorphismus. Ein *Homomorphismus über* φ zwischen zwei Körpererweiterungen $E_1|K_1$ und $E_2|K_2$ ist ein Körperhomomorphismus $\sigma\colon E_1 \to E_2$ mit $\sigma|_{K_1} = \varphi$. Anders gesagt, σ setzt φ fort.



Wir halten den Spezialfall $K_1 = K_2 = K$ und $\varphi = \mathrm{id}_K$ gesondert fest:

Definition 12B6. Ein *Homomorphismus* zwischen zwei Körpererweiterungen $E|K$ und $F|K$ über K ist ein Körperhomomorphismus $\sigma\colon E \to F$ mit $\sigma|_K = \mathrm{id}_K$. Die Menge dieser Homomorphismen bezeichnen wir mit $\mathrm{Hom}(E|K, F|K)$.

Körpererweiterungen über K und ihre Homomorphismen bilden eine *Kategorie*: Für jede Erweiterung $E|K$ ist die Identität $\mathrm{id}_E\colon E \to E$ ein Homomorphismus über K. Sind $f\colon E|K \to F|K$ und $g\colon F|K \to G|K$ Körperhomomorphismen über K, so ist auch ihre Komposition $g \circ f\colon E|K \to G|K$ ein Körperhomomorphismus über K.

Wir vereinbaren den in jeder Kategorie üblichen Sprachgebrauch:

- Ein bijektiver Homomorphismus $\sigma\colon E \xrightarrow{\sim} F$ mit $\sigma|_K = \mathrm{id}_K$ heißt *Isomorphismus über* K. In diesem Fall ist auch $\sigma^{-1}\colon F \xrightarrow{\sim} E$ ein Isomorphismus über K.

- Ein *Endomorphismus* von $E|K$ ist ein Homomorphismus $\sigma\colon E \to E$ mit $\sigma|_K = \mathrm{id}_K$. Die Menge aller Endomorphismen von R bezeichnen wir mit $\mathrm{End}(E|K)$.
- Ein *Automorphismus* von $E|K$ ist ein Isomorphismus $\sigma\colon E \xrightarrow{\sim} E$ mit $\sigma|_K = \mathrm{id}_K$. Die Menge aller Automorphismen von R bezeichnen wir mit $\mathrm{Aut}(E|K) = \mathrm{Gal}(E|K)$.

Beispiel 12B7. Die Körpererweiterung $\mathbb{C} = \{\, a+bi \mid a,b \in \mathbb{R} \,\}$ über $\mathbb{R}$ erlaubt neben der Identität $\mathrm{id}_\mathbb{C}$ noch die Konjugation $\mathrm{conj}\colon \mathbb{C} \to \mathbb{C}$ mit $a+bi \mapsto a-bi$ als Automorphismus über $\mathbb{R}$. Weitere Automorphismen gibt es nicht, also gilt $\mathrm{Aut}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}, \mathrm{conj}\}$.

Beispiel 12B8. Die Erweiterung $\mathbb{R}|\mathbb{Q}$ erlaubt außer der Identität keine Automorphismen, also $\mathrm{Aut}(\mathbb{R}|\mathbb{Q}) = \{\mathrm{id}_\mathbb{R}\}$. (Übung 12F21 führt dies aus.)

Beispiel 12B9. Es gilt $\mathbb{Q} < \mathbb{Q}[i] < \mathbb{C}$. Die Erweiterung $\mathbb{Q}[i]$ über $\mathbb{Q}$ erlaubt neben der Identität noch die Konjugation $\sigma\colon a+bi \mapsto a-bi$ als Automorphismus über $\mathbb{Q}$. Weitere Automorphismen gibt es nicht, also gilt $\mathrm{Aut}(\mathbb{Q}[i]|\mathbb{Q}) = \{\mathrm{id}, \sigma\}$.

Beispiel 12B10. Sei $c \in \mathbb{Q}_{>0}$ sodass $\mathbb{Q} < \mathbb{Q}[\sqrt{c}] < \mathbb{R}$. Falls $\sqrt{c} \notin \mathbb{Q}$, dann erlaubt $\mathbb{Q}[\sqrt{c}]$ über $\mathbb{Q}$ neben der Identität noch die Konjugation $\sigma\colon a+b\sqrt{c} \mapsto a-b\sqrt{c}$ als Automorphismus über $\mathbb{Q}$. Weitere Automorphismen gibt es nicht, also gilt $\mathrm{Aut}(\mathbb{Q}[\sqrt{c}]|\mathbb{Q}) = \{\mathrm{id}, \sigma\}$.

§**12Bc. Grad einer Erweiterung.** Ist $E|K$ eine Körpererweiterung, dann ist E ein Vektorraum über K: Die abelsche Gruppe $(E,+)$ statten wir mit der Operation $K \times E \to E$ aus, die durch durch Einschränkung der Multiplikation $\cdot\colon E \times E \to E$ entsteht. Die Körperaxiome von $(E,+,\cdot)$ implizieren dann die Vektorraumaxiome über K. Jeder K-Vektorraum ist frei, das heißt er besitzt eine Basis (8F3). Je zwei Basen haben dieselbe Kardinalität, und so ist die Dimension $\dim_K(E)$ als Länge einer Basis von E über K definiert.

Definition 12B11. Die Dimension $|E:K| := \dim_K(E)$ heißt der *Grad* der Erweiterung $E|K$. Die Erweiterung $E|K$ heißt *endlich* wenn der Grad $|E:K|$ endlich ist.

Beispiel 12B12. Die Erweiterung $\mathbb{R}|\mathbb{Q}$ ist von unendlichem Grad, geschrieben $|\mathbb{R}:\mathbb{Q}| = \infty$. Die Erweiterung $\mathbb{C}|\mathbb{R}$ ist vom Grad $|\mathbb{C}:\mathbb{R}| = 2$. Ebenso gilt $|\mathbb{Q}[i]:\mathbb{Q}| = |\mathbb{Q}[\sqrt{c}]:\mathbb{Q}| = 2$.

Übung 12B13. Sei $\mathcal{P} = \{2,3,5,7,\dots\}$ die Menge der Primzahlen in $\mathbb{N}$. Man beweise zunächst, dass diese Menge unendlich ist. Man zeige, dass die Familien der reellen Zahlen $\log p$ mit $p \in \mathcal{P}$ linear unabhängig über $\mathbb{Q}$ ist. Das bedeutet insbesondere $\dim_\mathbb{Q}(\mathbb{R}) = \infty$.

Beispiel 12B14. Für den Polynomring $K[X]$ über einem Körper K gilt $\dim_K K[X] = \infty$, denn nach Definition bilden die Monome $1, X, X^2, X^3, \dots$ eine Basis von $K[X]$ über K. Für den Körper $K(X)$ der rationalen Funktionen über K gilt demnach $|K(X):K| = \infty$.

Beispiel 12B15. Ist $P \in K[X]$ ein irreduzibles Polynom über K, dann ist $E = K[X]/(P)$ eine Körpererweiterung vom Grad $|E:K| = \deg P$ (4B9).

Die Dimensionsformel (§8Fc) besagt nun:

Satz 12B16 (Gradformel)**.** *Für alle Körpererweiterungen $K < E < F$ gilt*

$$|F:K| = |F:E| \cdot |E:K|\,.$$

Diese Gleichung gilt auch im Falle unendlicher Erweiterungen. Wir werden Sie jedoch hauptsächlich für endliche Erweiterungen einsetzen. Hier besagt sie: Wenn zwei der Grade endlich sind dann auch der dritte und es gilt die obige Formel.

Proposition 12B17. *Sei K ein Körper und seien $E|K$ und $F|K$ zwei Körpererweiterungen. Für jeden Körperhomomorphismus $\sigma\colon E \to F$ über K gilt:*

1. *Die Abbildung σ ist injektiv, wie jeder Körperhomomorphismus.*
2. *Das Bild $\sigma(E)$ ist ein Unterkörper von F und isomorph zu E.*
3. *Die Abbildung σ ist K-linear zwischen den Vektorräumen E und F über K.*

Gilt $\dim_K(E) = \dim_K(F) < \infty$*, dann ist jeder Körperhomomorphismus $\sigma\colon E \to F$ über K ein Isomorphismus. Aus* $\dim_K(E) < \infty$ *folgt insbesondere* $\mathrm{End}(E|K) = \mathrm{Aut}(E|K)$. □

§**12Bd. Erzeugter Teilring und Teilkörper.** Die Schnittmenge von Teilringen in E ist wieder ein Teilring von E. Ebenso ist die Schnittmenge von Teilkörpern in E wieder ein Teilkörper in E. Wir erinnern an die Notation für erzeugte Teilringe und Teilkörper (§3Bb):

Definition 12B18. Sei $K < E$ ein Teilkörper und $S \subset E$ eine Teilmenge. Der von S über K erzeugte Teilring $K[S]$ ist der kleinste Teilring, der K und S enthält:

$$K[S] := \bigcap \{\, F \subset E \text{ Teilring} \mid K \subset F, S \subset F \,\}.$$

Der von S über K erzeugte Teilkörper $K(S)$ ist der kleinste Teilkörper, der K und S enthält:

$$K(S) := \bigcap \{\, F \subset E \text{ Teilkörper} \mid K \subset F, S \subset F \,\}.$$

Ist $S = \{a_1, \ldots, a_n\} \subset E$ eine endliche Menge so schreiben wir kurz $K[a_1, \ldots, a_n]$ für den erzeugten Teilring $K[S]$, und entsprechend $K(a_1, \ldots, a_n)$ für den erzeugten Teilkörper $K(S)$.

Übung 12B19. Für alle $a_1, \ldots, a_n \in E$ gilt $K[a_1, \ldots, a_n] = K[a_1, \ldots, a_m][a_{m+1}, \ldots, a_n]$ sowie $K(a_1, \ldots, a_n) = K(a_1, \ldots, a_m)(a_{m+1}, \ldots, a_n)$, wobei $n > m > 0$.

Bemerkung 12B20. Als Gegenstück zur obigen "extrinsischen" Definition ist gelegentlich eine intrinsische Beschreibung des Rings $K[S]$ nützlich:

$$K[S] = \{\, P(a_1, \ldots, a_n) \mid n \geq 0,\ P \in K[X_1, \ldots, X_n],\ a_1, \ldots, a_n \in S \,\}$$

Offenbar gilt "$\supset$", denn der Ring $K[S]$ enthält K und S. Die Umkehrung "$\subset$" gilt, denn auch die rechte Seite ist ein Teilring von E, der K und S enthält.

Ebenso gewinnt man eine intrinsische Beschreibung des Körpers $K(S)$:

$$K(S) = \left\{ \frac{P(a_1, \ldots, a_n)}{Q(a_1, \ldots, a_n)} \;\middle|\; \begin{array}{c} n \geq 0,\ P, Q \in K[X_1, \ldots, X_n], \\ a_1, \ldots, a_n \in S,\ Q(a_1, \ldots, a_n) \neq 0 \end{array} \right\}$$

Offenbar gilt "$\supset$", denn der Körper $K(S)$ enthält K und S. Die Umkehrung "$\subset$" gilt, denn auch die rechte Seite ist ein Teilkörper von E, der K und S enthält.

Proposition 12B21. *Sei K ein Körper, seien $E|K$ und $F|K$ zwei Körpererweiterungen, und sei $\sigma\colon E \to F$ ein Körperhomomorphismus über K. Im Falle $E = K(a_1, \ldots, a_n)$ ist σ bereits durch die Bilder $\sigma(a_1), \ldots, \sigma(a_n) \in F$ eindeutig festgelegt.*

BEWEIS. Sind $\sigma, \tau\colon E \to F$ zwei Körperhomomorphismus über K, dann gilt zunächst $\sigma|_K = \tau|_K = \mathrm{id}_K$. Gilt zudem $\sigma(a_i) = \tau(a_i)$ für $i = 1, \ldots, n$, dann folgt $\sigma = \tau$ auf $K[a_1, \ldots, a_n]$: Da σ und τ Ringhomomorphismen sind, gilt für jedes Polynom $P \in K[X_1, \ldots, X_n]$ dann

$$\sigma P(a_1, \ldots, a_n) = P(\sigma a_1, \ldots, \sigma a_n) = P(\tau a_1, \ldots, \tau a_n) = \tau P(a_1, \ldots, a_n).$$

Ebenso folgt $\sigma = \tau$ auf dem Körper $K(a_1,\dots,a_n)$:

$$\sigma\left(\frac{P(a_1,\dots,a_n)}{Q(a_1,\dots,a_n)}\right) = \frac{\sigma P(a_1,\dots,a_n)}{\sigma Q(a_1,\dots,a_n)} = \frac{\tau P(a_1,\dots,a_n)}{\tau Q(a_1,\dots,a_n)} = \tau\left(\frac{P(a_1,\dots,a_n)}{Q(a_1,\dots,a_n)}\right). \qquad \square$$

§12C. Algebraische Erweiterungen

§12Ca. Einfache Erweiterungen. Wir nennen $E|K$ eine *einfache Erweiterung*, wenn es ein Element $a \in E$ gibt, sodass $E = K(a)$ gilt. In diesem Fall nennen wir a ein *primitives Element* der Körpererweiterung $E|K$.

Beispiel 12C1. Die Erweiterung $\mathbb{C}|\mathbb{R}$ ist einfach, denn $\mathbb{C} = \mathbb{R}[i]$.
Die Erweiterung $\mathbb{R}|\mathbb{Q}$ ist nicht einfach (schon aus Kardinalitätsgründen, siehe §12Ff).

Für jede einfache Körpererweiterung $K(a)$ über K haben wir vom Polynomring $K[X]$ ausgehend einen surjektiven Ringhomomorphismus

$$f\colon K[X] \twoheadrightarrow K[a] \quad \text{mit} \quad f(X) = a \quad \text{und} \quad f|_K = \mathrm{id}_K.$$

Da $K[X]$ ein Hauptidealring ist, gilt $\ker(f) = (P)$ für ein $P \in K[X]$. Nach dem Isomorphiesatz induziert f einen Ringisomorphismus

$$\bar{f}\colon K[X]/(P) \xrightarrow{\sim} K[a].$$

Da $K[a]$ als Teilring eines Körpers ein Integritätsring ist, muss (P) ein Primideal sein (§5G). Zwei Fälle sind möglich:

1. Gilt $\ker(f) = (0)$, dann ist $f\colon K[X] \xrightarrow{\sim} K[a]$ ein Ringisomorphismus und setzt sich zu einem Körperisomorphismus $K(X) \xrightarrow{\sim} K(a)$ fort. Hier gilt $\dim_K(K[a]) = \infty$.
2. Gilt $\ker(f) = (P)$ mit $P \neq 0$, dann ist (P) maximal (5G8). Der Quotient $K[X]/(P)$ ist dann ein Körper und somit $K[a] = K(a)$. Hierbei gilt $\dim_K(K[a]) = \deg P$.

Übung 12C2. Man bestimme den Grad der Körpererweiterung $|\mathbb{Q}[\sqrt[n]{2}] : \mathbb{Q}|$ für $n \in \mathbb{N}_{\geq 1}$. Für die Erweiterung $\mathbb{R}|\mathbb{Q}$ leite man hieraus erneut ab, dass $|\mathbb{R} : \mathbb{Q}| = \infty$ gilt.

§12Cb. Algebraische und transzendente Elemente. Sei $E|K$ eine Körpererweiterung. Ein Element $a \in E$ heißt *algebraisch* über K, oder kurz *K-algebraisch*, wenn es ein Polynom $P \in K[X]^*$ gibt mit $P(a) = 0$. Andernfalls heißt *a transzendent* über K.

Bemerkung 12C3. Ein Element $a \in E$ ist genau dann algebraisch, wenn die Potenzen $1, a, a^2, a^3, \dots$ über K linear abhängig sind. Dann gibt es nämlich eine nicht-triviale Linearkombination

$$c_0 + c_1 a + c_2 a^2 + \cdots + c_n a^n = 0$$

mit $c_0, c_1, c_2, \dots, c_n \in K$. Wir können n minimal und $c_n = 1$ annehmen. Dann ist

$$P = c_0 + c_1 X + c_2 X^2 + \cdots + X^n$$

das Minimalpolynom von a über K. Umgekehrt ist $a \in E$ genau dann transzendent über K, wenn die Potenzen $1, a, a^2, a^3, \dots$ über K linear unabhängig sind. Das bedeutet, für alle $P \in K[X]$ folgt aus $P(a) = 0$ notwendigerweise $P = 0$.

Beispiel 12C4. Das Element $X \in K(X)$ ist transzendent über K, denn es erfüllt keine polynomielle Relation über K: Aus $P(X) = c_0 + c_1 X + \cdots + c_n X^n = 0$ folgt $P = 0$.

Beispiel 12C5. Das Element $\sqrt[n]{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, denn es ist eine Nullstelle des Polynoms $X^n - 2$ über $\mathbb{Q}$.

Beispiel 12C6. Die Eulersche Zahl $e = \sum_{k=0}^{\infty} \frac{1}{k!}$ und die Kreiszahl π sind transzendent über $\mathbb{Q}$. (Das ist allerdings nicht leicht zu beweisen.) Aus Abzählunsgründen sind die meisten reellen Zahlen $x \in \mathbb{R}$ transzendent über $\mathbb{Q}$ (siehe §12Ff). Interessanterweise ist es dennoch nicht leicht, eine konkrete transzendente Zahl anzugeben.

Bemerkung 12C7. Die Begriffe "algebraisch" und "transzendent" sind nur bezüglich des Grundkörpers K definiert: Ohne Angabe des Grundkörpers haben sie keinen Sinn. Zum Beispiel ist $e \in \mathbb{R}$ transzendent über $\mathbb{Q}$, aber algebraisch über $\mathbb{R}$. Nur wenn der in Rede stehende Grundkörper aus dem Kontext eindeutig hervorgeht kann man seine explizite Nennung weglassen.

Satz 12C8. *Sei $E|K$ eine Körpererweiterung. Für jedes Element $a \in E$ sind äquivalent:*

1. *Das Element a ist algebraisch über K.*
2. *Die Erweiterung $K(a)$ ist endlich über K.*
3. *Der erzeugte Teilring $K[a]$ ist ein Körper, also $K[a] = K(a)$.*

In diesem Fall existiert genau ein normiertes Polynom $P \in K[X]^*$ minimalen Grades mit $P(a) = 0$. Dieses nennen wir das Minimalpolynom *von a.*

Das Minimalpolynom P von a ist das einzige normierte irreduzible Polynom $P \in K[X]$ mit $P(a) = 0$. Wir schreiben daher $\operatorname{Irr}_K^X(a) := P$.

Die Dimension $\deg_K(a) := |K(a) : K| = \deg P$ heißt der Grad *des Elements a über K.*

BEWEIS. Die Äquivalenz der drei Bedingungen folgt sofort aus obigen Vorüberlegungen zu einfachen Erweiterungen.

Die Polynome $Q \in K[X]$ mit $Q(a) = 0$ sind gerade der Kern des Ringhomomorphismus $f\colon K[X] \twoheadrightarrow K[a]$ mit $X \mapsto a$, und nach Voraussetzung gilt $\ker(f) \neq \{0\}$. Jedes Polynom $P \in \ker(f) \smallsetminus \{0\}$ minimalem Grades erfüllt $\ker(f) = (P)$. Dieses Polynom wird eindeutig, wenn wir zusätzlich P normiert annehmen, also mit Leitkoeffizient $\operatorname{lc} P = 1$.

Da $K[X]/(P) \cong K[a] = K(a)$ nullteilerfrei ist, ist P irreduzibel. Jedes andere Polynom $Q \in K[X]$ mit $Q(a) = 0$ ist ein Vielfaches von P. Ist auch Q irreduzibel, dann gilt $P \sim Q$, und ist zudem auch Q normiert, dann gilt $P = Q$. □

Beispiel 12C9. Jedes Element $a \in K$ ist algebraisch über K mit $\operatorname{Irr}_K^X(a) = X - a$.

Beispiel 12C10. Das Element $\mathbb{Q}[\sqrt[n]{2}] \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$ mit $\operatorname{Irr}_{\mathbb{Q}}^X(\sqrt[n]{2}) = X^n - 2$.

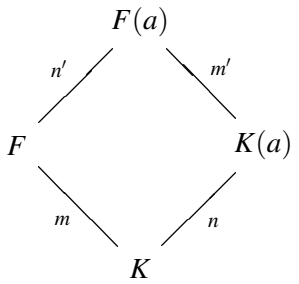
§**12Cc. Algebraische Erweiterungen.** Eine Körpererweiterung $E|K$ heißt *algebraisch* wenn jedes Element $a \in E$ algebraisch über K ist.

Proposition 12C11. *Jede endliche Erweiterung ist algebraisch.* □

Die Umkehrung gilt nicht, wie das untenstehende Beispiel 12C16 zeigt.

Lemma 12C12. *Seien $K < F < E$ Körper, wobei die Erweiterung $F|K$ endlich sei. Ist $a \in E$ algebraisch über K, also $K(a)|K$ endlich, dann ist auch $F(a)|K$ endlich.*

BEWEIS. Wir betrachten das folgende Diagramm:



Die Erweiterung $F|K$ ist endlich, vom Grad $|F:K| = m$. Da a als algebraisch über K vorausgesetzt wird, ist die Erweiterung $K(a)|K$ endlich, vom Grad $\deg_K(a) = n$. Dann ist a erst recht algebraisch über F, vom Grad $n' = \deg_F(a) \leq n$. Nach der Dimensionsformel gilt $|F(a):K| = mn' < \infty$. □

Satz 12C13. *Sind $a_1,\dots,a_n \in E$ algebraische Elemente über K, dann ist die Erweiterung $K(a_1,\dots,a_n)$ endlich und damit algebraisch über K.*

BEWEIS. Dies folgt per Induktion aus dem vorangegangenen Lemma. □

Das bedeutet: Sind $a,b \in E$ algebraisch über K, Also $A(a) = 0$ und $B(b) = 0$ für gewisse $A,B \in K[X]^*$, dann sind auch Summe $a+b$ und Produkt ab algebraisch über K, das heißt es existieren $S,P \in K[X]^*$ mit $S(a+b) = 0$ und $P(ab) = 0$. Die Gradformel (12B16) liefert diese Existenzaussage auf wundersam einfache Weise. Man beachte jedoch, dass wir auf diesem Wege noch keine Handhabe bekommen, die Polynome S und P auch konkret auszurechnen.

Satz 12C14. *Enthält die Teilmenge $S \subset E$ nur algebraische Elemente über K, dann ist der erzeugte Teilkörper $K(S)$ algebraisch über K.*

BEWEIS. Jedes Element $a \in K(S)$ liegt in einem Teilkörper $K(a_1,\dots,a_n)$ für geeignete $a_1,\dots,a_n \in S$ (12B20). Nach Satz 12C13 ist a damit algebraisch. □

Korollar 12C15. *Sei $E|K$ eine Körpererweiterung. Dann ist die Menge $\bar{K} \subset E$ aller K-algebraischen Elemente von E ein Teilkörper von E, und $\bar{K}|K$ ist algebraisch.* □

Beispiel 12C16. In $\mathbb{C}|\mathbb{Q}$ sei $\mathbb{Q}^a$ die Menge aller $\mathbb{Q}$-algebraischen Elemente von $\mathbb{C}$. Dies ist ein algebraischer Erweiterungskörper von $\mathbb{Q}$, aber nicht endlich, wie die Teilkörper $\mathbb{Q}[\sqrt[n]{2}]$ der Dimension n über $\mathbb{Q}$ belegen.

§12D. Zerfällungskörper

§12Da. Adjunktion einer Wurzel. Nachdem wir über das Grundvokabular algebraischer Körpererweiterungen verfügen, wollen wir damit beginnen, solche Erweiterungen zu konstruieren. Am Anfang steht die folgende grundlegende Feststellung:

Satz 12D1 (Kronecker)**.** *Sei K ein Körper. Zu jedem Polynom $P \in K[X]$ vom Grad $\deg P \geq 1$ existiert ein algebraischer Erweiterungskörper $E|K$ in dem P eine Nullstelle hat.*

BEWEIS. Wir zerlegen $P = P_1 \cdots P_r$ in $r \geq 1$ irreduzible Polynome $P_1, \ldots, P_r \in K[X]$. Der Quotient $E := K[X]/(P_1)$ ist ein Körper (12B4). Wir können K mit seinem Bild $\pi(K) < E$ identifizieren, und somit $E|K$ als Erweiterungskörper betrachten. Da π ein Ringhomomorphismus ist, erfüllt $x = \pi(X)$ die Bedingung $P_1(x) = P_1(\pi(X)) = \pi(P_1(X)) = 0$. □

Definition 12D2. Sei K ein Körper und $P \in K[X]^*$. Wir sagen die Körpererweiterung $E|K$ entsteht durch *Adjunktion* einer Wurzel von P wenn es ein Element $a \in E$ gibt mit $P(a) = 0$ und $E = K(a)$. Ist zudem P irreduzibel, dann gilt $\deg_K(a) = |K(a) : K| = \deg P$ und das Minimalpolynom von a über K ist $\mathrm{Irr}_K^X(a) = P/\mathrm{lc}(P)$.

Beispiel 12D3. Das Polynom $P = X^2 - 2$ ist irreduzibel über $\mathbb{Q}$. Der Quotient $E = \mathbb{Q}[X]/(P)$ entsteht aus $\mathbb{Q}$ durch Adjunktion des Elements $x = \pi(X)$, also $E = \mathbb{Q}(x)$. Wegen $x^2 = 2$ gilt

$$\mathbb{Q}(x) = \{\, a + bx \mid a, b \in \mathbb{Q} \,\}$$

mit der Addition

$$(a + bx) + (a' + b'x) = (a + a') + (b + b')x$$

und der Multiplikation

$$(a + bx) \cdot (a' + b'x) = (aa' + 2bb') + (ab' + a'b)x.$$

Das entspricht offenbar dem Teilkörper $\mathbb{Q}[\sqrt{2}]$ in $\mathbb{R}$. Beide Erweiterungen sind isomorph: $\mathbb{Q}[X]/(P) \cong \mathbb{Q}[\sqrt{2}]$ im Sinne der folgenden Erläuterung. Man beachte, dass man in $\mathbb{Q}[X]/(P)$ bequem rechnen kann (4B9). Die obigen Operationen lassen sich unmittelbar auf einem Computer implementieren, und zwar exakt, ohne jede Rundung.

Beispiel 12D4. Sei $K < \mathbb{C}$ ein Teilkörper, zum Beispiel $K = \mathbb{Q}$. Jedes Polynom $P \in K[X]^*$ zerfällt über $\mathbb{C}$, das heißt es existieren Nullstellen $a_1, \ldots, a_n \in \mathbb{C}$ sodass $P = c(X - a_1) \cdots (X - a_n)$ gilt. Für jede Nullstelle a_k entsteht der Teilkörper $K(a_k) < \mathbb{C}$ durch Adjunktion einer Wurzel von P. Die Teilkörper $K(a_1), \ldots, K(a_n)$ können verschieden sein.

Das Polynom $X^2 - 2$ über $\mathbb{Q}$ zerfällt in $(X - \sqrt{2})(X + \sqrt{2})$ über $\mathbb{C}$, und somit stimmen die von jeweils einer Wurzel erzeugten Teilkörper $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$ überein.

Das Polynom $X^3 - 2$ über $\mathbb{Q}$ zerfällt in $(X - \sqrt[3]{2})(X - j\sqrt[3]{2})(X - j^2\sqrt[3]{2})$ über $\mathbb{C}$, wobei $j = e^{2\pi i/3}$. Hier sind die Teilkörper $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$, $\mathbb{Q}(j^2\sqrt[3]{2})$ untereinander verschieden.

Dieses Phänomen hängt vom Grundkörper ab. Über $K = \mathbb{Q}(j)$ zerfällt $X^3 - 2$ ebenso in $(X - \sqrt[3]{2})(X - j\sqrt[3]{2})(X - j^2\sqrt[3]{2})$, aber hier gilt $K(\sqrt[3]{2}) = K(j\sqrt[3]{2}) = K(j^2\sqrt[3]{2})$.

§12Db. Fortsetzung von Körperhomomorphismen.

Bemerkung 12D5. Jeder Körperhomomorphismus $\sigma\colon E \to F$ über K induziert einen Ringhomomorphismus $\tilde{\sigma}\colon E[X] \to F[X]$ vermöge der offensichtlichen Fortsetzung

$$\tilde{\sigma}(c_0 + c_1X + \ldots c_nX^n) = \sigma(c_0) + \sigma(c_1)X + \cdots + \sigma(c_n)X^n.$$

Häufig bezeichnen wir diese Fortsetzung der Kürze halber einfach mit σ.

Für $P = c_0 + c_1X + \ldots c_nX^n$ in $K[X]$ und $x \in E$ haben wir $P(x) \in E$ und

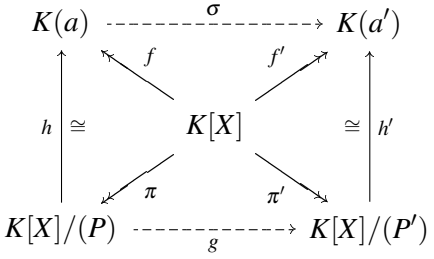
$$\begin{aligned}\sigma(P(x)) &= \sigma(c_0 + c_1x + \ldots c_nx^n)\\ &= c_0 + c_1\sigma(x) + \ldots c_n\sigma(x)^n = P(\sigma(x)),\end{aligned}$$

da σ ein Körperhomomorphismus ist mit $\sigma|_K = \mathrm{id}_K$. Gilt insbesondere $P(x) = 0$, dann gilt $P(\sigma(x)) = \sigma(P(x)) = \sigma(0) = 0$. Das bedeutet, $\sigma\colon E \to F$ über K bildet Nullstellen von $P \in K[X]$ in E auf Nullstellen von P in F ab.

Der folgende Satz besagt, dass eine einfache algebraisch Erweiterung $K(a)|K$ durch das Minimalpolynom $\mathrm{Irr}_K^X(a) \in K[X]$ eindeutig beschrieben wird. Anders gesagt, alle einfachen algebraischen Erweiterungen werden durch durch die irreduziblen Polynome $P \in K[X]$ parametrisiert.

Satz 12D6. *Seien $K(a)$ und $K(a')$ einfache algebraische Erweiterungen über K. Genau dann existiert ein Körperisomorphismus $\sigma\colon K(a) \xrightarrow{\sim} K(a')$ mit $\sigma|_K = \mathrm{id}_K$ und $\sigma(a) = a'$, wenn $\mathrm{Irr}_K^X(a) = \mathrm{Irr}_K^X(a')$ gilt.*

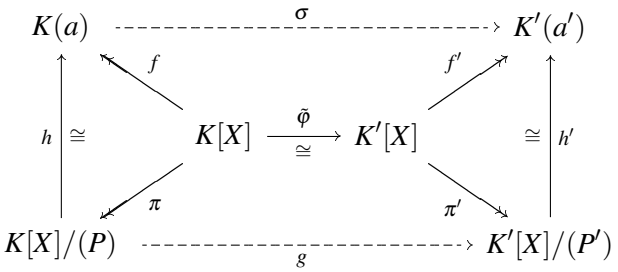
Der Beweis wird sich durch Betrachtung des folgenden Diagramms ergeben:



Für spätere Anwendungen lohnt es sich jedoch, diesen Satz leicht zu verallgemeinern:

Satz 12D7. *Sei $\varphi\colon K \xrightarrow{\sim} K'$ ein Körperisomorphismus. Seien $K(a)|K$ und $K'(a')|K'$ einfache algebraische Erweiterungen. Genau dann existiert ein Körperisomorphismus $\sigma\colon K(a) \xrightarrow{\sim} K'(a')$ mit $\sigma|_K = \varphi$ und $\sigma(a) = a'$, wenn $\tilde{\varphi}(\mathrm{Irr}_K^X(a)) = \mathrm{Irr}_{K'}^X(a')$ gilt.*

BEWEIS. Der Ringhomomorphismus $f\colon K[X] \to K(a)$ mit $f(X) = a$ ist surjektiv. Sein Kern $\ker(f) = (P)$ wird erzeugt vom Minimalpolynomen $P = \mathrm{Irr}_K^X(a)$. Dies induziert den Isomorphismus $h\colon K[X]/(P) \xrightarrow{\sim} K(a)$ über K wie in folgendem Diagramm:



Entsprechend hat $f'\colon K'[X] \to K'(a')$ den Kern $\ker(f') = (P')$ mit $P' = \mathrm{Irr}_{K'}^X(a')$ und induziert einen Isomorphismus $h'\colon K'[X]/(P') \xrightarrow{\sim} K'(a')$ über K.

Ist $\sigma\colon K(a) \xrightarrow{\sim} K(a')$ ein Isomorphismus mit $\sigma|_K = \varphi$ und $\sigma(a) = a'$, dann gilt $f' \circ \tilde{\varphi} = \sigma \circ f$ und somit $\ker(f') = \tilde{\varphi}(\ker(f))$. Aufgrund der Normierung folgt dann $P' = \tilde{\varphi}(P)$.

Ist $P' = \tilde{\varphi}(P)$, dann induziert dies einen Isomorphismus $g\colon K[X]/(P) \xrightarrow{\sim} K'[X]/(P')$, und wir erhalten den Isomorphismus $\sigma = h_2 \circ g \circ h_1^{-1}\colon K(a_1) \xrightarrow{\sim} K(a_2)$. □

§**12Dc. Zerfällungskörper.** Sei $E|K$ eine Körpererweiterung und $P \in K[X]^*$ ein Polynom über K. Wir sagen P *zerfällt* über E, wenn es Elemente $a_1,\dots,a_n \in E$ gibt, sodass $P = c(X-a_1)\cdots(X-a_n)$ gilt. (Hierbei ist $c = \operatorname{lc} P$ der Leitkoeffizient.) Gilt zudem $E = K(a_1,\dots,a_n)$, so nennen wir E einen *Zerfällungskörper* von P über K. (Etwas laxer gesagt, E entsteht aus K durch Adjunktion aller Wurzeln von P: Wir adjungieren sowenig wie möglich und soviel wie nötig, damit P zerfällt.)

Beispiel 12D8. Ist $K < \mathbb{C}$ ein Teilkörper, zum Beispiel $K = \mathbb{Q}$, dann zerfällt jedes Polynom $P \in K[X]^*$ über $\mathbb{C}$, das heißt es existieren Nullstellen $a_1,\dots,a_n \in \mathbb{C}$ sodass $P = c(X-a_1)\cdots(X-a_n)$ gilt. Dann ist der erzeugte Teilkörper $E = \mathbb{C}(a_1,\dots,a_n) < \mathbb{C}$ ein Zerfällungskörper von P über K.

Beispiel 12D9. Zu $P = X^2 - 2$ über $\mathbb{Q}$ entsteht der Körper $\mathbb{Q}[\sqrt{2}]$ durch Adjunktion der Wurzel $\sqrt{2} \in \mathbb{R}$. Wegen $P = (X-\sqrt{2})(X+\sqrt{2})$ ist $\mathbb{Q}[\sqrt{2}]$ ein Zerfällungskörper von P.

Beispiel 12D10. Zu $P = X^3 - 2$ über $\mathbb{Q}$ entsteht der Körper $\mathbb{Q}[\sqrt[3]{2}]$ durch Adjunktion der Wurzel $\sqrt[3]{2} \in \mathbb{R}$. Die weiteren Wurzeln $j\sqrt[3]{2}$ und $j^2\sqrt[3]{2}$ mit $j = e^{2\pi i/3} \in \mathbb{C}$ liegen jedoch nicht in $\mathbb{Q}[\sqrt[3]{2}]$: Hier gilt $P = (X-\sqrt[3]{2})(X^2+\sqrt[3]{2}X+\sqrt[3]{2}^2)$ und der quadratische Faktor zerfällt nicht über $\mathbb{Q}[\sqrt[3]{2}]$. Der Zerfällungskörper von P entsteht erst durch weitere Adjunktion:

$$\mathbb{Q}[\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}] = \mathbb{Q}[\sqrt[3]{2}, j\sqrt[3]{2}] = \mathbb{Q}[\sqrt[3]{2}, j].$$

Satz 12D11. *Zu jedem Polynom $P \in K[X]^*$ über K existiert ein Zerfällungskörper E über K. Je zwei Zerfällungskörper E und E' von P über K sind isomorph über K.*

BEWEIS. Wir können P als normiert annehmen, also mit Leitkoeffizient $\operatorname{lc} P = 1$. Sei $n = \deg P$ der Grad von P und sei $P = P_1 \cdots P_r$ die Zerlegung von P in normierte irreduzible Polynome $P_1,\dots,P_r$ in $K[X]$. Nach Umordnung können wir $\deg P_1 \geq \cdots \geq \deg P_r \geq 1$ annehmen. Es gilt $\deg P_1 + \cdots + \deg P_r = n$, und daher $1 \leq r \leq n$.

Zum Beweis der Existenz führen wir Induktion über die Differenz $d = d_K(P) := n - r$. Dies ist der "Defekt" von P und misst, wie weit P über K davon entfernt ist zu zerfallen: Der Grad n gibt an, wie viele Linearfaktoren nötig wären, die Anzahl r der irreduziblen Faktoren sagt uns, welche Zerlegung über K bestenfalls möglich ist.

Für $d = 0$ gilt $r = n$: Das heißt P zerfällt über K in Linearfaktoren und wir sind fertig.

Für $d \geq 1$ gilt $\deg P_1 \geq 2$ und nach dem Satz von Kronecker (12D1) existiert eine Körpererweiterung $E_1 = K(a_1)$ mit $P_1(a_1) = 0$. Demnach spaltet P_1 über E_1 (mindestens) den Linearfaktor $(X-a_1)$ ab, also gilt $d_{E_1}(P) < d_K(P)$. Nach Induktionsvoraussetzung existiert ein Körper $E = E_1(a_1,\dots,a_n)$ mit $P = (X-a_1)\cdots(X-a_n)$. Wegen $E_1 = K(a_1)$ gilt schließlich $E = K(a_1,\dots,a_n)$.

$$\begin{array}{c} E = K(a_1,\dots,a_n) \\ | \\ E_1 = K(a_1) \\ | \\ K \end{array}$$

Die Eindeutigkeit bis auf Isomorphie folgt aus dem folgenden Satz, angewendet auf den Spezialfall $K = K'$ und $\varphi = \mathrm{id}_K$. □

§**12Dd. Fortsetzung von Körperhomomorphismen.** Auch für Zerfällungskörper stellen wir die Fortsetzung von Körperhommorphismen sicher:

Satz 12D12. *Sei $\varphi\colon K \xrightarrow{\sim} K'$ ein Körperisomorphismus. Sei $P \in K[X]$ ein Polynom über K und sei E ein Zerfällungskörper von P über K. Sei $P' = \tilde{\varphi}(P)$ das entsprechende Polynom über K' und sei E' ein Zerfällungskörper von P' über K'. Dann existiert ein Körperisomorphismus $\sigma\colon E \xrightarrow{\sim} E'$ mit $\sigma|_K = \varphi$.*

Als Diagramm können wir die Situation wie folgt darstellen:

$$\begin{array}{ccc} E & \overset{\exists\sigma}{\underset{\cong}{\dashrightarrow}} & E' \\ | & & | \\ K & \underset{\cong}{\xrightarrow{\varphi}} & K' \end{array}$$

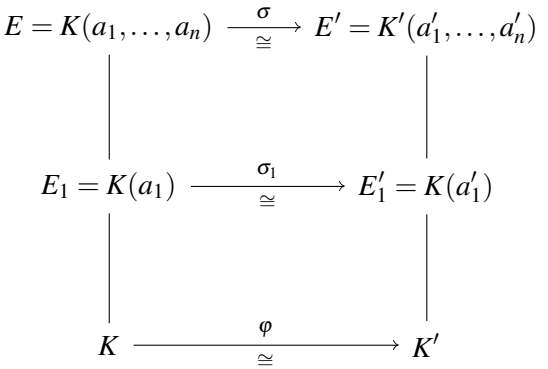
BEWEIS. Sei $E = K(a_1,\dots,a_n)$ mit $P = (X-a_1)\cdots(X-a_n)$ und $E' = K'(a'_1,\dots,a'_n)$ mit $P' = (X-a'_1)\cdots(X-a'_n)$. Wir wollen $E \cong E'$ über K zeigen.

Wie zuvor können wir P als normiert annehmen, also mit Leitkoeffizient $\operatorname{lc} P = 1$. Sei $n = \deg P$ der Grad von P und sei $P = P_1 \cdots P_r$ die Zerlegung von P in normierte irreduzible Polynome $P_1,\dots,P_r$ in $K[X]$. Nach Umordnung können wir $\deg P_1 \geq \cdots \geq \deg P_r \geq 1$ annehmen. Es gilt $\deg P_1 + \cdots + \deg P_r = n$, und daher $1 \leq r \leq n$.

Entsprechendes gilt für $P' = P'_1 \cdots P'_r$ wobei $P'_k = \tilde{\varphi}(P_k)$ für $k = 1,\dots,r$.

Wir führen Induktion über die Differenz $d = d_K(P) := n - r$.

Wenn $d = 0$, dann zerfällt P bereits über K in Linearfaktoren. Somit gilt $E = K$ und entsprechend $E' = K'$, und $\sigma = \varphi$ ist der gewünschte Isomorphismus.



Für $d \geq 1$ gilt $\deg P_1 \geq 2$. Da P_1 ein Teiler von P ist, sind die Nullstellen von P_1 eine Teilmenge der Nullstellen $a_1,\dots,a_n$ von P. Nach Umordnung der Elemente $a_1,\dots,a_n$ können wir $P_1(a_1) = 0$ annehmen. Durch Umordnung der Elemente $a'_1,\dots,a'_n$ erreichen wir entsprechend $P'_1(a'_1) = 0$. Nach 12D7 existiert ein Isomorphismus $\sigma_1 \colon K(a_1) \xrightarrow{\sim} K'(a'_1)$ mit $\sigma_1|_K = \varphi$ und $\sigma_1(a_1) = a'_1$. Ferner ist E ein Zerfällungskörper von P über $E_1 = K(a_1)$, und E' ist ein Zerfällungskörper von P' über $E'_1 = K(a'_1)$. Über E_1 spaltet P_1 (mindestens) den Linearfaktor $(X - a_1)$ ab, also gilt $d_{E_1}(P) < d_K(P)$. Nach Induktionsvoraussetzung existiert ein Isomorphismus $\sigma \colon E \xrightarrow{\sim} E'$, der σ_1 fortsetzt und somit auch $\sigma|_K = \varphi$ erfüllt. □

§12E. Algebraischer Abschluss

§**12Ea. Algebraisch abgeschlossene Körper.** Ein Körper C heißt *algebraisch abgeschlossen*, wenn jedes Polynom $P \in C[X]^*$ über C zerfällt, das heißt es existieren $a_1,\dots,a_n \in C$, sodass $P = c(X - a_1)\cdots(X - a_n)$ gilt. (Hierbei ist $c = \operatorname{lc} P$ der Leitkoeffizient.)

Beispiel 12E1. Der Körper $\mathbb{Q}$ der rationalen Zahlen ist nicht algebraisch abgeschlossen, denn für $n \geq 2$ ist das Polynom $X^n - 2$ irreduzibel und zerfällt daher nicht über $\mathbb{Q}$.

Beispiel 12E2. Auch der Körper $\mathbb{R}$ der reellen Zahlen ist nicht algebraisch abgeschlossen, denn das Polynom $X^2 + 1$ zerfällt nicht über $\mathbb{R}$. Gleiches gilt für alle quadratischen Polynome $aX^2 + bX + c$ über $\mathbb{R}$ mit negativer Diskriminante $b^2 - 4ac < 0$.

Beispiel 12E3. Der Hauptsatz der Algebra der komplexen Zahlen besagt, dass der Körper $\mathbb{C}$ der komplexen Zahlen algebraisch abgeschlossen ist.

Proposition 12E4. *Für jeden Körper C sind äquivalent:*

1. *Jedes Polynom $P \in C[X]$ mit $\deg P \geq 1$ hat eine Nullstelle in C.*
2. *Der Körper C ist algebraisch abgeschlossen.*
3. *Jedes irreduzible Polynom in $C[X]$ hat Grad 1.*
4. *Für jede algebraische Erweiterung $E|C$ gilt $E = C$.*

BEWEIS. "(1) ⇒ (2)" folgt per Induktion über den Grad durch Faktorisierung der Nullstellen: Jedes Polynom $P \in C[X]$ vom Grad 0 zerfällt wie angegeben, denn $P = c$ mit $c \in C$. Für $\deg P \geq 1$ existiert nach (1) eine Nullstelle $a_n \in C$. Aus $P(a_n) = 0$ folgt $P = Q \cdot (X - a_n)$ und nach Induktionsvoraussetzung $Q = c(X - a_1)\cdots(X - a_{n-1})$.

"(2) ⇒ (3)" ist klar, denn Polynome $P \in C[X]$ vom Grad $\deg P \geq 2$ zerfallen nach (2).

"(3) $\Rightarrow$ (4)" Da $E|C$ algebraisch ist, können wir für $a \in E$ das Minimalpolynom $P = \mathrm{Irr}_C^X(a)$ betrachten. Nach (3) gilt $\deg P = 1$, somit $P = X - a$. Hieraus folgt $a \in C$.

"(4) $\Rightarrow$ (1)" Sei $P \in C[X]$ ein Polynom mit $\deg P \geq 1$. Nach dem Satz von Kronecker (12D1) existiert ein algebraischer Erweiterungskörper $E|C$ in dem P eine Nullstelle hat. Wegen (4) gilt aber $E = C$, also hat P eine Nullstelle in C. □

§**12Eb. Algebraischer Abschluss.** Eine Körpererweiterung $C|K$ heißt *algebraischer Abschluss* des Körpers K, wenn $C|K$ algebraisch und C algebraisch abgeschlossen ist.

Beispiel 12E5. Die Erweiterung $\mathbb{C}|\mathbb{R}$ ist ein algebraischer Abschluss von $\mathbb{R}$, denn wegen $i^2 + 1 = 0$ ist $\mathbb{C} = \mathbb{R}[i]$ algebraisch über $\mathbb{R}$ und nach dem Hauptsatz der Algebra der komplexen Zahlen ist $\mathbb{C}$ algebraisch abgeschlossen.

Beispiel 12E6. Die Erweiterung $\mathbb{Q}[i]|\mathbb{Q}$ ist kein algebraischer Abschluss von $\mathbb{Q}$. Zwar ist $\mathbb{Q}[i]|\mathbb{Q}$ algebraisch, aber $\mathbb{Q}[i]$ ist nicht algebraisch abgeschlossen. Zum Beispiel hat $X^2 - 2$ keine Nullstelle in $\mathbb{Q}[i]$. (Übung: Warum nicht?)

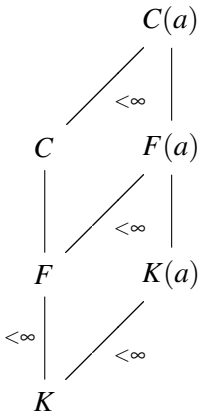
Beispiel 12E7. Die Erweiterung $\mathbb{C}|\mathbb{Q}$ ist kein algebraischer Abschluss von $\mathbb{Q}$. Zwar ist der Körper $\mathbb{C}$ algebraisch abgeschlossen, aber $\mathbb{C}|\mathbb{Q}$ ist nicht algebraisch (§12Ff). Zum algebraischen Abschluss $\mathbb{Q}^a|\mathbb{Q}$ siehe unten, Beispiel 12E10.

Satz 12E8. *Sei $C|K$ eine algebraische Körpererweiterung. Dann sind äquivalent:*

1. *Jedes Polynom $P \in C[X]^*$ zerfällt über C.*
2. *Jedes Polynom $P \in K[X]^*$ zerfällt über C.*

In diesem Fall ist C algebraisch abgeschlossen und $C|K$ ein algebraischer Abschluss.

BEWEIS. "(1) $\Rightarrow$ (2)" ist trivial. Für "(2) $\Rightarrow$ (1)" nehmen wir an, jedes Polynom in $K[X]^*$ zerfällt über C. Wir müssen zeigen, dass jedes Polynom $P \in C[X]^*$ über C zerfällt. Nach 12E4 reicht es zu zeigen, dass P eine Nullstelle in C hat.



Nach dem Satz von Kronecker (12D1) existiert eine Körpererweiterung $C(a)$ sodass $P(a) = 0$. Das Polynom $P = c_0 + c_1X + \cdots + c_nX^n$ hat Koeffizienten $c_0, c_1, \ldots, c_n \in C$, und diese sind nach Voraussetzung algebraisch über K. Daher ist $F = K(c_0, c_1, \ldots, c_n)$ endlich über K (12C13). Wegen $P(a) = 0$ mit $P \in F[X]^*$ ist auch $F(a)$ endlich über F. Nach der Gradformel 12B16 ist $F(a)$ auch endlich über K. Damit ist auch $K(a) < F(a)$ endlich über

K, insbesondere ist a dann K-algebraisch und wir können das Minimalpolynom $\operatorname{Irr}_K^X(a) \in K[X]^*$ betrachten. Nach Voraussetzung zerfällt $\operatorname{Irr}_K^X(a)$ über C. Folglich gilt $a \in C$. □

Korollar 12E9. *Sei C ein algebraisch abgeschlossener Körper. Ist $K < C$ ein Teilkörper, so betrachten wir den Körper K^a aller K-algebraischen Elemente in C. Dann ist K^a algebraisch abgeschlossen, und somit ist $K^a|K$ ein algebraischer Abschluss von K.*

BEWEIS. Nach Satz 12C14 ist K^a ein Körper, und nach Konstruktion ist $K^a|K$ eine algebraische Erweiterung. Jedes Polynom $P \in K[X]^*$ zerfällt in C. Die Nullstellen von P sind aber sämtlich algebraisch über K, also liegen sie in K^a. Damit zerfällt P über K^a. Nach dem vorangegangenen Satz ist dann K^a algebraisch abgeschlossen. □

Beispiel 12E10. Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen. Sei $\mathbb{Q}^a$ der Unterkörper der $\mathbb{Q}$-algebraischen Zahlen. Dann ist $\mathbb{Q}^a$ algebraisch abgeschlossen und somit ein algebraischer Abschluss von $\mathbb{Q}$.

§**12Ec. Existenz des algebraischen Abschlusses.** Zu je *endlich* vielen (normierten) Polynomen $f_1, \dots, f_r \in K[X]^*$ existiert ein gemeinsamer Zerfällungskörper $E|K$ sodass

$$\begin{aligned} f_1 &= (X - a_{1,1}) \cdots (X - a_{1,n_1}) \\ &\vdots \\ f_r &= (X - a_{r,1}) \cdots (X - a_{r,n_r}) \end{aligned}$$

mit $a_{1,1}, \dots, a_{1,n_1}, \dots, a_{r,1}, \dots, a_{r,n_r} \in E$ gilt sowie $E = K(a_{1,1}, \dots, a_{1,n_1}, \dots, a_{r,1}, \dots, a_{r,n_r})$. Die technische Schwierigkeit besteht nun allein darin, dies für *unendlich* viele Polynome gleichzeitig auszuführen. Wir vereinbaren folgende Sprechweise:

Definition 12E11. Sei $\mathcal{P} \subset K[X]^*$ eine Menge Polynome. Wir sagen $\mathcal{P}$ *zerfällt* über E, wenn jedes Polynom $f \in \mathcal{P}$ über E zerfällt. Wir nennen $E|K$ einen *Zerfällungskörper* von $\mathcal{P}$ über K wenn zudem $E = K(S)$ gilt für $S = \{\, a \in E \mid f(a) = 0 \text{ für ein } f \in \mathcal{P} \,\}$.

Nach 12C14 ist solch ein Zerfällungskörper E von P über K algebraisch.

Beispiel 12E12. Besteht $\mathcal{P}_0 = \{f_1, \dots, f_r\}$ aus endlich vielen Polynomen in $K[X]^*$, dann entsteht ein Zerfällungskörper E von P über K wie oben angegeben durch sukzessive Konstruktion von Zerfällungskörpern bezüglich $f_1, \dots, f_r$.

Satz 12E13. *Für jede Menge $\mathcal{P} \subset K[X]^*$ von Polynomen über K existiert ein Zerfällungskörper.*

BEWEIS. Wir können die Polynome $f \in \mathcal{P}$ als normiert annehmen, also mit Leitkoeffizient $\operatorname{lc} f = 1$. Wir betrachten die Indexmenge $\mathscr{X} = \{\, (f,k) \in \mathcal{P} \times \mathbb{N} \mid 1 \le k \le \deg f \,\}$. Der Monoidring $R = K[\mathbb{N}^{(\mathscr{X})}]$ ist ein Polynomring in den Variablen $A_{f,k}$, indiziert durch $(f,k) \in \mathscr{X}$. Für jedes Polynom

$$f = X^n + c_1 X^{n-1} + \cdots + c_{n-1} X + c_n$$

in $\mathcal{P}$ betrachten wir die ersehnte Zerfällung in $(X - A_{f,1}) \cdots (X - A_{f,n})$ als Relation

$$r_f := f - (X - A_{f,1}) \cdots (X - A_{f,n}).$$

Im Grad $n-k$ für $1 \leq k \leq \deg f$ entspricht dies einer Relation

$$r_{f,k} := c_k - (-1)^k \sum_{i_1<\cdots<i_k} A_{f,i_1} \cdots A_{f,i_k}.$$

Diese Relationen $r_{f,k} \in R$ erzeugen ein Ideal $\mathfrak{a} := \{\, r_{f,k} \mid (f,k) \in \mathscr{X} \,\}$ in R.

Wir stellen zunächst sicher, dass $\mathfrak{a} \neq R$ gilt.

Wäre $1 \in \mathfrak{a}$, dann hätten wir $1 = g_1 r_1 + \cdots + g_n r_n$ mit gewissen Relationen $r_1, \ldots, r_n$ wie oben und $g_1, \ldots, g_n \in R$. An dieser Gleichung sind nur endlich viele $f \in \mathcal{P}$ beteiligt, diese bilden eine endliche Teilmenge $\mathcal{P}_0 \subset \mathcal{P}$. Hierzu sei $\mathscr{X}_0 = \{\, (f,k) \in \mathcal{P}_0 \times \mathbb{N} \mid 1 \leq k \leq \deg f \,\}$. Die Relation liegt demnach in einem gewissen Teilring $R_0 = K[\mathbb{N}^{\mathscr{X}_0}]$. Für endlich viele Polynome können wir wie oben gesehen einen Zerfällungskörper $E_0|K$ konstruieren. Sei $\pi\colon R_0 \to E_0$ der Ringhomomorphismus über K, der die Variablen $A_{f,1}, \ldots, A_{f,\deg f}$ mit $f \in \mathcal{P}_0$ auf die Nullstellen von f in E_0 abbilden. In E_0 sind dann alle Relationen $r_1, \ldots, r_n$ erfüllt, das heißt $\pi(r_1) = \cdots = \pi(r_n) = 0$. Aus $1 = g_1 r_1 + \cdots + g_n r_n$ in R wird dann $1 = 0$ in E_0, was der Tatsache widerspricht, dass E_0 ein Körper ist.

Somit ist die Annahme $1 \in \mathfrak{a}$ widerlegt, und es gilt $\mathfrak{a} \neq R$.

Sei $\mathfrak{m} \lhd R$ ein maximales Ideal, das $\mathfrak{a}$ enthält. Dass ein solches existiert, folgt aus dem Zornschen Lemma (5G12). Aufgrund der Maximalität von $\mathfrak{m}$ ist $E = R/\mathfrak{m}$ ein Körper. Es gilt $K < R$, und wegen $K \cap \mathfrak{m} = \{0\}$ ist die Quotientenabbildung $\pi\colon R \to E$ injektiv auf K. Wir können also K mit dem Bild $\pi(K)$ in E identifizieren. Das Bild von $A_{f,k}$ in E bezeichnen wir mit $a_{f,k} = \pi(A_{f,k})$. In $E[X]$ gilt nach Konstruktion für jedes $f \in \mathcal{P}$ die Gleichung

$$f = (X - a_{f,1}) \cdots (X - a_{f,n}).$$

Wie der Polynomring $R = K[\, A_{f,k} \mid (f,k) \in \mathscr{X} \,]$ wird auch der Quotient $E = R/\mathfrak{m}$ von von den Elementen $a_{f,k}$ über erzeugt, das heißt $E = K[\, a_{f,k} \mid (f,k) \in \mathscr{X} \,]$. Somit ist E wie gewünscht ein Zerfällungskörper von $\mathcal{P}$ über K. □

Hieraus erhalten wir nun mühelos folgenden wichtigen Spezialfall:

Satz 12E14. *Zu jedem Körper K existiert ein algebraischer Abschluss $C|K$.*
Je zwei algebraische Abschlüsse $C|K$ und $C'|K$ sind isomorph über K.

BEWEIS. Sei $\mathcal{P} \subset K[X]^*$ die Menge der normierten irreduziblen Polynome über K, oder gleich $\mathcal{P} = K[X]^*$. Sei C der Zerfällungskörper von $\mathcal{P}$ über K. Dann ist $C|K$ algebraisch und jedes Polynom $P \in K[X]$ zerfällt über C . Nach 12E8 ist C algebraisch abgeschlossen.

Die Eindeutigkeit bis auf Isomorphie folgt aus dem nachfolgenden Satz 12E15. □

§12Ed. Fortsetzung von Körperhomomorphismen.

Satz 12E15. *Sei $\varphi\colon K \xrightarrow{\sim} K'$ ein Körperisomorphismus. Sei $E|K$ eine algebraische Erweiterung und $C|K'$ ein algebraischer Abschluss. Dann existiert ein Körperhomomorphismus $\sigma\colon E \to C$ mit $\sigma|_K = \varphi$.*

$$\begin{array}{ccc} E & \overset{\sigma}{\dashrightarrow} & C \\ | & & | \\ K & \underset{\cong}{\xrightarrow{\varphi}} & K' \end{array}$$

Ist zudem E algebraisch abgeschlossen und $C|K'$ algebraisch, dann ist jeder Körperhomomorphismus $\sigma\colon E \to C$ über K ein Isomorphismus.

BEWEIS. Wir betrachten die Menge M aller Paare (F,f) wobei F ein Teilkörper ist mit $K < F < E$ und $f\colon F \to C$ ein Homomorphismus mit $f|_K = \varphi$.

$$\begin{array}{ccc} E & \overset{\sigma}{\dashrightarrow} & C \\ | & & | \\ F & \underset{\cong}{\overset{f}{\longrightarrow}} & F' \\ | & & | \\ K & \underset{\cong}{\overset{\varphi}{\longrightarrow}} & K' \end{array}$$

Wegen $(K,\varphi) \in M$ ist diese Menge nicht leer. Die Menge M ist durch Inklusion geordnet, mittels $(F,f) \le (F',f')$ genau dann wenn $F < F'$ und $f'|_F = f$. Zu jeder Kette $T \subset M$ ist $G := \bigcup_{(F,f)\in T} F$ ein Teilkörper mit $K < G < E$ und $g := \bigcup_{(F,f)\in T} f$ ist ein Homomorphismus $g\colon G \to C$ mit $g|_K = \varphi$. Nach dem Lemma von Zorn existiert ein maximales Element (F,σ) in M.

Wir behaupten, dass $F = E$ gilt. Um $E \subset F$ zu zeigen, sei $a \in E$. Da $E|K$ algebraisch ist, können wir $P = \operatorname{Irr}_K^X(a)$ betrachten. Da C algebraisch abgeschlossen ist, zerfällt $P' = \tilde{\varphi}(P)$ über C, es gibt also $a' \in C$ sodass $P'(a') = 0$. Nach Satz 12D7 existieren Erweiterungen $F < F(a) < E$ über F und $F' < F'(a') < C$ über $F' = \sigma(F)$ und eine Fortsetzung von σ zu $\bar{\sigma}\colon F(a) \to F'(a')$. Wegen der Maximalität von (F,σ) muss hierbei also $F(a) = F$ gelten, und somit $a \in F$. Somit ist $\sigma\colon E \to C$ ein Homomorphismus mit $\sigma|_K = \varphi$.

Das isomorphe Bild $E' = \sigma(E)$ ist eine Körpererweiterung von K'. Ist E algebraisch abgeschlossen, dann ist auch E' algebraisch abgeschlossen. Ist zudem $C|K'$ algebraisch, dann gilt $C < E'$: In diesem Fall erhalten wir $\sigma(E) = C$ und $\sigma\colon E \to C$ ist ein Körperisomorphismus. □

§12F. Übungen und Ergänzungen

§12Fa. Algebraische und nicht-algebraische Erweiterungen.

Übung 12F1. Für $a = \sqrt{7}$ und $b = 1+\sqrt{7}$ zeige man $\operatorname{Irr}_{\mathbb{Q}}(a) \neq \operatorname{Irr}_{\mathbb{Q}}(b)$ aber $\mathbb{Q}(a) = \mathbb{Q}(b)$.

Übung 12F2. Für $a = \sqrt[3]{7}$ und $b = j\sqrt[3]{7}$ zeige man $\operatorname{Irr}_{\mathbb{Q}}(a) = \operatorname{Irr}_{Q}(b)$ aber $\mathbb{Q}(a) \neq \mathbb{Q}(b)$.

Übung 12F3. Sind die Erweiterungen $\mathbb{Q}(\sqrt{7})$ und $\mathbb{Q}(\sqrt{11})$ isomorph?

Übung 12F4. Jede Erweiterung $E|\mathbb{Q}$ vom Grad 2 ist von der Form $E = \mathbb{Q}(\sqrt{a})$.

Übung 12F5. Man bestimme die algebraischen Erweiterungen von $\mathbb{C}$ und von $\mathbb{R}$.
Man gebe Beispiele nicht-algebraischer Erweiterungen von $\mathbb{C}$ und von $\mathbb{R}$.

Übung 12F6. Ist jede endliche Erweiterung algebraisch? Ist jede algebraische Erweiterung endlich? Ist der algebraische Abschluss $\mathbb{Q}^a$ von $\mathbb{Q}$ endlich über $\mathbb{Q}$?

Übung 12F7. Kann ein endlicher Körper F algebraisch abgeschlossen sein? *Hinweis:* Jeder endliche Körper F hat eine Primzahl p als Charakteristik (§3De). Für $P = X^{p^n} - X$ berechne man $\mathrm{ggT}(P, P')$ und leite hieraus die Anzahl der verschiedenen Nullstellen von P ab.

Übung 12F8. Angenommen $e \in \mathbb{R}$ sei transzendent über $\mathbb{Q}$. Ist e dann auch transzendent über jeder algebraischen Erweiterung von $\mathbb{Q}$?

§12Fb. Zerfällungskörper.

Übung 12F9. Für $(X^2-2)(X^2-3)$ über $\mathbb{Q}$ bestimme man alle Körper, die aus $\mathbb{Q}$ durch Adjunktion einer Wurzel entstehen. Sind diese Körper untereinander isomorph? Für den Zerfällungskörper E über $\mathbb{Q}$ bestimme man den Grad $|E:\mathbb{Q}|$ und finde eine Basis über $\mathbb{Q}$.

Übung 12F10. Für X^3-2 über $\mathbb{Q}$ bestimme man den Zerfällungskörper E über $\mathbb{Q}$ in $\mathbb{C}$. Man ermittle den Grad $|E:\mathbb{Q}|$ und finde eine Basis über $\mathbb{Q}$.

Übung 12F11. Man zeige, dass $P = X^3 - 3X - 1$ irreduzibel über $\mathbb{Q}$ ist und drei reelle Wurzeln besitzt. Sei $a \in \mathbb{R}$ eine Wurzel, also $P(a) = 0$. Über $\mathbb{Q}(a)$ prüfe man die Zerlegung

$$P = (X-a)(X^2+aX+a^2-3) = (X-a)(X+\tfrac{a+1}{a})(X+\tfrac{1}{a+1}).$$

Ist $\mathbb{Q}(a)$ ein Zerfällungskörper von P über $\mathbb{Q}$?

Übung 12F12. Man zeige, dass $E = \mathbb{Q}(i, \sqrt[4]{2})$ ein Zerfällungskörper von X^4+2 über $\mathbb{Q}$ ist. Ist E auch ein Zerfällungskörper von X^4-2 über $\mathbb{Q}$? Man bestimme den Grad $|E:\mathbb{Q}|$ und finde eine Basis von E über $\mathbb{Q}$.

§12Fc. Irreduzibilität bei Körpererweiterungen.

Übung 12F13. Sei $E|K$ eine endliche Erweiterung vom Grad m und sei $P \in K[X]$ ein irreduzibles Polynom vom Grad n. Wenn $\mathrm{ggT}(m,n) = 1$, dann ist P auch irreduzibel in $E[X]$.

Übung 12F14. Ist X^3+3 irreduzibel in $\mathbb{Q}(\sqrt{3})[X]$?
Ist X^5+3X^3-9X+6 irreduzibel in $\mathbb{Q}(\sqrt{2},\sqrt{3})[X]$?
Ist X^2+2 irreduzibel in $\mathbb{Q}(\sqrt{2})[X]$?

§12Fd. Körpererweiterungen und Automorphismen.

Übung 12F15. Man bestimme $\mathrm{Aut}(\mathbb{C}|\mathbb{R})$ und $\mathrm{Aut}(\mathbb{Q}(i)|\mathbb{Q})$ sowie $\mathrm{Aut}(\mathbb{Q}(j)|\mathbb{Q})$.

Übung 12F16. Man bestimme $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q})$.

Übung 12F17. Man bestimme $\mathrm{Aut}(\mathbb{Q}(j, \sqrt[3]{2})|\mathbb{Q})$.

Übung 12F18. Man bestimme $\mathrm{Aut}(\mathbb{Q}(i, \sqrt[4]{2})|\mathbb{Q})$.

Übung 12F19. Man bestimme $G = \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})$.
Gilt hier $|G| < |\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}|$? Das ist nicht normal...

§12Fe. Automorphismen von $\mathbb{R}$.

Wir wollen zeigen, dass der Körper $\mathbb{R}$ außer der Identität keine Automorphismen erlaubt. Genauer gilt folgendes Ergebnis:

Satz 12F20. *Jeder Körperhomomorphismus $\mathbb{R} \to \mathbb{R}$ ist die Identität.*

Übung 12F21. Sei $\varphi\colon \mathbb{R} \to \mathbb{R}$ ein Körperhomomorphismus

1. Es gilt $\varphi|_{\mathbb{N}} = \mathrm{id}_{\mathbb{N}}$ und somit $\varphi|_{\mathbb{Z}} = \mathrm{id}_{\mathbb{Z}}$ und schließlich $\varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$.
2. Für jede reelle Zahl $x \in \mathbb{R}$ gilt $x \geq 0$ genau dann wenn $x = a^2$ für ein $a \in \mathbb{R}$.
3. Der Endomorphismus φ erhält die positiven Zahlen, also $\varphi(\mathbb{R}_{\geq 0}) \subset \mathbb{R}_{\geq 0}$.
4. Für alle $a \leq b$ in $\mathbb{R}$ gilt $\varphi(a) \leq \varphi(b)$. Hieraus folgt $\varphi = \mathrm{id}_{\mathbb{R}}$.

Warnung. — Wir wissen nun, dass $\mathrm{Aut}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}, \mathrm{conj}\}$ und $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}\}$ gilt. Man könnte versucht sein, hieraus $\mathrm{Aut}(\mathbb{C}) = \{\mathrm{id}, \mathrm{conj}\}$ zu schließen. Das Problem hierbei ist, dass ein Körperautomorphismus von $\mathbb{C}$ nicht unbedingt den Teilkörper $\mathbb{R}$ festlässt. — Das ist unglaublich aber wahr! In der Tat ist die Gruppe $\mathrm{Aut}(\mathbb{C})$ unendlich, gar überabzählbar. Das ist allerdings nur eine Existenzaussage, fußend auf dem Auswahlaxiom. Niemand hat jemals einen anderen Automorphismus von $\mathbb{C}$ gesehen als die Identität und die Konjugation.

Übung 12F22. Zum Vergleich eine algebraische Variante dieses Phänomens. Für $n \in \mathbb{N}_{\geq 1}$ sei $\sqrt[n]{3}$ die positive reelle Wurzel von $X^n - 3$. Man zeige, dass $K = \bigcup_{n \geq 1} \mathbb{Q}(\sqrt[n]{3})$ ein Teilkörper von $\mathbb{R}$ ist. Ist die Erweiterung $K|\mathbb{Q}$ algebraisch? (endlich?) Man bestimme $\mathrm{Aut}(K)$.

Die Moral von der Geschicht: Für eine Erweiterung $K < E < F$ kann es passieren, dass F größer ist als E, aber $\mathrm{Aut}(F|K)$ kleiner ist als $\mathrm{Aut}(E|K)$. Trösten wir uns: Jede *Galois-Erweiterung* $E|K$ hat die sympathische Eigenschaft $|\mathrm{Aut}(E|K)| = |E : K|$. Alles wird gut.

§**12Ff. Abzählbarkeit.** Die $\mathbb{Q}$-algebraischen Zahlen sind nur ein "kleiner" Teil aller reellen Zahlen; die überwiegende "Mehrheit" aller reellen Zahlen ist transzendent über $\mathbb{Q}$:

Übung 12F23. Die Körper $\mathbb{R}$ und $\mathbb{C}$ sind überabzählbar.
Der Körper $\mathbb{Q}$ und sein algebraischer Abschluss $\mathbb{Q}^a$ in $\mathbb{C}$ sind hingegen abzählbar.

Wenn man also "zufällig" eine reelle Zahl $x \in [0,1]$ wählt, dann ist diese transzendent mit Wahrscheinlichkeit 1 und algebraisch mit Wahrscheinlichkeit 0. Dennoch ist es nicht leicht, eine konkrete transzendente Zahl anzugeben und ihre Transzendenz nachzuweisen!

KAPITEL 13

Endliche Körper

§13A. Einführung und Überblick

Die endlichen Körper gehören zu den schönsten und nützlichsten Strukturen der Algebra. Bemerkenswerterweise erlauben sie eine vollständige und übersichtliche Klassifikation, die auf Évariste GALOIS zurückgeht und der wir uns in diesem Kapitel widmen wollen.

§**13Aa. Klassifikation.** Bei einem Körper K nennen wir die Elementezahl $|K|$ auch die *Ordnung* von K, in Anlehnung an die Sprechweise bei endlichen Gruppen. Der Körper $\mathbb{Q}$ der rationalen Zahlen hat unendliche Ordnung. Für jede Primzahl $p \in \mathbb{N}$ ist der Restklassenring $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ein endlicher Körper der Ordnung p. Weder $\mathbb{Q}$ noch $\mathbb{F}_p$ haben echte Teilkörper, und die Automorphismengruppe ist jeweils trivial: $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}}\}$ und $\mathrm{Aut}(\mathbb{F}_p) = \{\mathrm{id}_{\mathbb{F}_p}\}$.

Jeder Körper K enthält einen kleinsten Teilkörper $P < K$, definiert als Schnittmenge aller Teilkörper von K, und diesen nennen wir den *Primkörper* von K. Gemäß 3D24 ist der Primkörper entweder isomorph zu $\mathbb{Q}$ oder zu $\mathbb{F}_p$ für eine gewisse Primzahl $p \in \mathbb{N}$. Im ersten Fall hat K die Charakteristik $\mathrm{char}(K) = 0$, im zweiten Fall hat K die Charakteristik $\mathrm{char}(K) = p$. Bei einem endlichen Körper K kann nur letzteres auftreten.

Satz (Klassifikation)**.** *Endliche Körper erlauben folgende Klassifikation:*

1. *Jeder endliche Körper hat p^n Elemente, wobei $p = \mathrm{char}(F)$ und $n \in \mathbb{N}_{\geq 1}$.*
2. *Zu jeder Primzahlpotenz p^n mit $n \in \mathbb{N}_{\geq 1}$ existieren Körper mit p^n Elementen.*
3. *Zwei endliche Körper mit gleicher Elementezahl sind isomorph.*

Auch die Teilkörper eines endlichen Körpers sind gut zu verstehen:

Satz (Teilkörper)**.** *Sei F ein Körper der Ordnung $|F| = p^n$, wobei $p \in \mathbb{N}$ prim ist und $n \in \mathbb{N}_{\geq 1}$. Dann hat jeder Teilkörper $K < F$ Ordnung $|K| = p^m$ mit $m \mid n$. Umgekehrt existiert für jeden Teiler $m \mid n$ in $\mathbb{N}$ genau ein Teilkörper $K < F$ der Ordnung $|K| = p^m$.*

Wir erinnern daran, dass für jeden kommutativen Ring R von Primzahlcharakteristik $p \geq 2$ die Abbildung $\mathfrak{f}_p \colon R \to R$ mit $x \mapsto x^p$ ein Ringhomomorphismus ist, genannt *Frobenius-Homomorphismus* (§3Df). Für endliche Körper erhalten wir insbesondere:

Satz (Automorphismen)**.** *Sei F ein Körper der Ordnung $|F| = p^n$, wobei $p \in \mathbb{N}$ prim ist und $n \in \mathbb{N}_{\geq 1}$. Dann ist $\mathrm{Aut}(F) = \langle \mathfrak{f}_p \rangle$ eine zyklische Gruppe der Ordnung n.*

Der Vergleich von Teilkörpern $K < F$ und Untergruppen $H < \mathrm{Aut}(F)$ enthüllt die Galois-Korrespondenz (§13Be): Für jeden endlichen Körper F haben wir eine natürliche Bijektion zwischen den Teilkörpern von F und den Untergruppen von $\mathrm{Aut}(F)$. Diesen fundamentalen Sachverhalt werden wir im nächsten Kapitel auf beliebige (Galois-)Erweiterungen ausdehnen und damit zum Hauptsatz der Galois-Theorie vorstoßen.

§**13Ab. Konstruktion.** Nach der Klassifikation stellt sich die praktische Frage, wie man einen endlichen Körper F der Ordnung p^n möglichst konkret und effizient konstruieren kann, um zum Beispiel Rechnungen in F auszuführen. Dies führen wir in §13C aus.

§**13Ac. Sprachgebrauch.** Der deutschen Wortwahl "endlicher Körper" entspricht auf englisch *finite field* und auf französisch *corps fini*. Galois zu Ehren nennt man einen endlichen Körper auf englisch häufig auch *Galois field*, also 'Galois-Körper', und schreibt $\mathrm{GF}(q)$ für einen Körper mit q Elementen. Die gelegentlich anzutreffende deutsche Übersetzung "Galois-Feld" halte ich für unglücklich. Ich plädiere dafür, auf deutsch der ebenso kurzen wie präzisen Bezeichnung "endlicher Körper" treu zu bleiben. Einen endlichen Körper mit q Elementen bezeichnet man üblicherweise mit dem Symbol $\mathbb{F}_q$.

§**13Ad. Eindeutigkeit bis auf Isomorphie.** Die vertrauten Objekte $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sind jeweils durch ihre definierenden Eigenschaften festgelegt bis auf *eindeutige* Isomorphie. Zum Beispiel ist der geordnete Körper $(\mathbb{R},+,\cdot,\leq)$ charakterisiert durch die Supremums-Eigenschaft, die besagt: Jede nicht-leere, nach oben beschränkte Teilmenge $A \subset \mathbb{R}$ hat ein Supremum in $\mathbb{R}$. Jeder andere angeordnete Körper mit der Supremums-Eigenschaft ist zu $\mathbb{R}$ isomorph und zwar vermöge genau eines Körperisomorphismus (§12Fe). Entsprechende Aussagen gelten für $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$. Insbesondere gilt $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}_\mathbb{Q}\}$ und $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}_\mathbb{R}\}$.

Beim Körper $\mathbb{C} = \mathbb{R}[i]$ der komplexen Zahlen begegnen wir dem Phänomen, dass die Elemente $\pm i$ algebraisch nicht zu unterscheiden sind. Die Konjugation $\mathrm{conj}\colon \mathbb{C} \to \mathbb{C}$, mit $a+bi \mapsto a-bi$ für alle $a,b \in \mathbb{R}$, drückt diese Ambivalenz als Körperautomorphismus aus, und wir wissen $\mathrm{Aut}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}, \mathrm{conj}\}$ (§12Fd). Wenn man $\mathbb{C}$ als algebraischen Abschluss von $\mathbb{R}$ definiert, oder schlicht als $\mathbb{C} = \mathbb{R}[i]$ mit $i^2 = -1$, dann ist der Körper $\mathbb{C}$ hierdurch bis auf Isomorphie festgelegt: Jede Erweiterung von $\mathbb{R}$ mit dieser Eigenschaft ist isomorph zu $\mathbb{C}$ über $\mathbb{R}$. Allerdings ist die Wahl des Isomorphismus nicht eindeutig, denn es gibt stets genau zwei Möglichkeiten, und keine ist bevorzugt.

Der obige Klassifikationssatz besagt, dass es für jede Primzahlpotenz p^n bis auf Isomorphie genau einen Körper der Ordnung p^n gibt. Diesen nennt man daher *den* Körper der Ordnung p^n. Allerdings sind zwei Körper E und F der Ordnung p^n nicht *kanonisch* isomorph: Da die Automorphismengruppe $\mathrm{Aut}(F) = \langle \mathfrak{f}_p \rangle$ Ordnung n hat, existieren genau n mögliche Isomorphismen $E \xrightarrow{\sim} F$, und je zwei Isomorphismen unterscheiden sich durch einen Automorphismus $\mathfrak{f}_p^k$ mit $0 \leq k < n$. Alle Konstruktionen und Rechnungen in E lassen sich also ebenso in F durchführen, aber die Entsprechung ist nicht eindeutig sondern "n-deutig".

Diese Subtilität liegt in der Natur endlicher Körper. Das Problem ist jedoch weniger ein mathematisches als ein grammatikalisches. Eine gewisse Eindeutigkeit lässt sich künstlich herstellen als Teilkörper eines fest gewählten algebraischen Abschlusses $\bar{\mathbb{F}}_p$ von $\mathbb{F}_p$ (§13Bf).

§13B. Klassifikation endlicher Körper

§13Ba. Charakteristik und Kardinalität. Wir beginnen mit folgender Erinnerung:

Lemma 13B1. *Sei E ein Körper.*

- *Für jeden Teilkörper $K < E$ ist E ein Vektorraum über K.*
- *Ist $\dim_K(E) = n$ endlich, dann existiert ein Isomorphismus $K^n \xrightarrow{\sim} E$ über K.*
- *Ist der Körper E endlich, dann ist $n = \dim_K(E)$ endlich und es gilt $|E| = |K|^n$.* □

Satz 13B2. *Jeder endliche Körper F enthält einen kleinsten Teilkörper*

$$P = \{\, n1_F \mid n \in \mathbb{Z} \,\}.$$

Dessen Ordnung $p := |P|$ ist eine Primzahl und es gibt einen eindeutigen Isomorphismus $\mathbb{F}_p \cong P$. Die Dimension $n = \dim_P(F)$ ist endlich. Somit gilt $F \cong P^n$ und $|F| = p^n$.

BEWEIS. Der Ringhomomorphismus $\varphi\colon \mathbb{Z} \to F$ hat als Bild

$$\operatorname{im}(\varphi) = P.$$

Dies induziert einen Ringisomorphismus

$$\bar{\varphi}\colon \mathbb{Z}/\ker(\varphi) \xrightarrow{\sim} P.$$

Da $\mathbb{Z}$ ein Hauptidealring ist, gilt $\ker(\varphi) = (p)$ für ein $p \in \mathbb{N}$. Da F endlich ist, folgt $p \neq 0$. Da F nullteilerfrei ist, muss p prim sein, somit erhalten wir den Körperisomorphismus

$$\bar{\varphi}\colon \mathbb{F}_p \xrightarrow{\sim} P.$$

Da F endlich ist, ist die Dimension $n = \dim_P(F)$ endlich. Die Wahl einer Basis stiftet einen Vektorraumisomorphismus $P^n \xrightarrow{\sim} F$, und aus diesem folgt $|F| = |P|^n = p^n$. □

Der Körper $P < F$ heißt der *Primkörper* von F. Die Primzahl $p := |P|$ heißt die *Charakteristik* (§3De) des Körpers F, geschrieben $\operatorname{char}(F) = p$.

Der Isomorphismus $\bar{\varphi}\colon \mathbb{F}_p \xrightarrow{\sim} P < F$ ist eindeutig bestimmt. Wir können mittels $\bar{\varphi}$ den Teilkörper P mit $\mathbb{F}_p$ identifizieren und im Folgenden $\mathbb{F}_p < F$ als Teilkörper auffassen, und damit F als Erweiterungskörper über $\mathbb{F}_p$ betrachten.

§13Bb. Existenz und Eindeutigkeit. Wir halten eine einfache aber nützliche Beobachtung fest, die uns im Folgenden wiederholt gute Dienste leisten wird:

Lemma 13B3. *Sei E ein Körper. Für jeden Automorphismus $f \in \operatorname{Aut}(E)$ ist die Fixpunktmenge*

$$\operatorname{Fix}(f) = \{\, a \in E \mid f(a) = a \,\}$$

ein Teilkörper von E. Ebenso definiert jede Untergruppe $G < \operatorname{Aut}(E)$ einen Teilkörper

$$\operatorname{Fix}(G) = \{\, a \in E \mid f(a) = a \text{ für alle } f \in G \,\} = \bigcap_{f \in G} \operatorname{Fix}(f).$$

BEWEIS. Wegen $f(0) = 0$ und $f(1) = 1$ gilt $0, 1 \in F$. Wenn $a, b \in F$, dann gilt

$$f(a+b) = f(a) + f(b) = a + b$$

also $a+b \in F$, und ebenso

$$f(a \cdot b) = f(a) \cdot f(b) = a \cdot b$$

also $a \cdot b \in F$. Für das additive Inverse von $a \in E$ gilt

$$0 = f(0) = f(a+(-a)) = f(a) + f(-a)$$

also $f(-a) = -f(a)$. Aus $a \in F$ folgt demnach $-a \in F$.

Für das multiplikative Inverse von $a \in E^*$ gilt entsprechend

$$1 = f(1) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$$

also $f(a^{-1}) = f(a)^{-1}$. Aus $a \in F$ folgt demnach $a^{-1} \in F$. □

Beispiel 13B4. Für jeden Körper E positiver Charakteristik p ist die Abbildung $\mathfrak{f}_p \colon E \to E$ mit $x \mapsto x^p$ ein Körperhomomorphismus, genannt Frobenius-Homomorphismus (§3Df). Für jedes $n \in \mathbb{N}$ ist die Fixpunktmenge $F = \mathrm{Fix}(\mathfrak{f}_p^n)$ ein Teilkörper von E.

Satz 13B5. *Zu jeder Primzahl $p \in \mathbb{N}$ und $n \in \mathbb{N}_{\geq 1}$ existieren Körper der Ordnung p^n. Jeder Körper der Ordnung p^n ist ein Zerfällungskörper des Polynoms $X^{p^n} - X$ über $\mathbb{F}_p$. Je zwei Körper der Ordnung p^n sind demnach isomorph.*

BEWEIS. Für $n = 1$ leistet $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ das Gewünschte. Für $n \geq 2$ betrachten wir das Polynom $f = X^{p^n} - X$ über $\mathbb{F}_p$. Nach 12D11 existiert ein Zerfällungskörper E von f über K. Aus $f' = -1$ folgt $\mathrm{ggT}(f, f') = 1$, also hat f keine mehrfachen Nullstellen. Die Nullstellenmenge $F = \{\, a \in E \mid f(a) = 0 \,\}$ hat also genau p^n Elemente. Wegen

$$F = \{\, a \in E \mid a^{p^n} = a \,\} = \mathrm{Fix}(\mathfrak{f}_p^n)$$

ist F ein Teilkörper von E. Damit ist ein Körper F der Ordnung $|F| = p^n$ gefunden.

Ist umgekehrt F ein Körper der Ordnung p^n, dann ist $F^\times = F \smallsetminus \{0\}$ eine Gruppe der Ordnung $p^n - 1$ bezüglich Multiplikation. Nach dem Satz von Lagrange gilt $x^{p^n-1} = 1$ für alle $x \in F^\times$. Damit gilt auch $x^{p^n} = x$ für alle $x \in F^\times$ und zusätzlich auch für $x = 0$. Das Polynom $X^{p^n} - X$ hat also genau p^n verschiedene Nullstellen in F, und somit gilt

$$X^{p^n} - X = \prod_{a \in F} (X - a).$$

Folglich ist jeder Körper F der Ordnung p^n ein Zerfällungskörper des Polynoms $X^{p^n} - X$ über $\mathbb{F}_p$. Nach Satz 12D11 ist F hierdurch bis auf Isomorphie eindeutig bestimmt. □

§13Bc. Teilkörper.

Lemma 13B6. *Im Polynomring $K[X]$ über jedem Körper K gilt für alle $p, m, n \in \mathbb{N}$*

$$\mathrm{ggT}(X^{p^m} - X, X^{p^n} - X) = X^{p^d} - X \quad \textit{wobei} \quad d = \mathrm{ggT}(m, n).$$

Für $p \geq 2$ gilt demnach: $X^{p^m} - X$ teilt $X^{p^n} - X$ genau dann wenn $m \mid n$.

BEWEIS. Für $n = 0$ gilt $d = m$ und die Aussage ist klar.

Für $n > 0$ sei $m = qn + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < n$. Dann gilt

$$X^{p^m} = X^{p^{qn+r}} = (((X^{p^n})^{p^n} \cdots)^{p^n})^{p^r} \equiv X^{p^r} \quad \text{modulo} \quad X^{p^n} - X.$$

Für die euklidische Division gilt demnach $(X^{p^m}-X) = Q\cdot(X^{p^n}-X)+(X^{p^r}-X)$ für ein $Q \in K[X]$. So fortfahrend berechnet man im euklidischen Algorithmus parallel zum ggT der Exponenten m und n in $\mathbb{Z}$ auch den ggT der Polynome $X^{p^m}-X$ und $X^{p^n}-X$ in $K[X]$.

Für $p \geq 2$ gilt $X^{p^m}-X = X^{p^d}-X$ genau dann wenn $m = d$, also $m \mid n$. □

Satz 13B7. *Sei F ein Körper der Ordnung $|F| = p^n$, wobei $p \in \mathbb{N}$ prim ist und $n \in \mathbb{N}$. Dann hat jeder Teilkörper $K < F$ Ordnung $|K| = p^m$ mit $m \mid n$. Umgekehrt existiert für jeden Teiler $m \mid n$ in $\mathbb{N}$ genau ein Teilkörper $K < F$ der Ordnung $|K| = p^m$.*

BEWEIS. Sei $\mathbb{F}_p < F$ der Primkörper von F. Für $\mathbb{F}_p < K < F$ gilt dann

$$|F:\mathbb{F}_p| = |F:K|\cdot|K:\mathbb{F}_p|$$

Somit ist $m = \dim_{\mathbb{F}_p}(K)$ ein Teiler von $n = \dim_{\mathbb{F}_p}(F)$, und es gilt $|K| = p^m$ sowie $F = p^n$. Ist umgekehrt $m \in \mathbb{N}$ ein Teiler von n, dann ist $X^{p^m}-X$ ein Teiler von $X^{p^n}-X$ in $\mathbb{F}_p[X]$. Daher enthält F als Zerfällungskörper von $X^{p^n}-X$ über $\mathbb{F}_p$ einen Zerfällungskörper K von $X^{p^m}-X$ über $\mathbb{F}_p$. Wie wir im Beweis von 13B5 gesehen haben, gilt dann

$$K = \{\, a \in F \mid a^{p^m} = a \,\}$$

Hierdurch wird der Teilkörper $K < F$ eindeutig festgelegt. □

§**13Bd. Automorphismen.** Aus 9D22 wissen wir:

Lemma 13B8. *Sei F ein Körper der Ordnung p^n mit Primkörper $\mathbb{F}_p < F$. Die Gruppe $F^\times$ ist zyklisch der Ordnung p^n-1, das heißt es existiert ein Element $a \in F^\times$ der Ordnung p^n-1, genannt* Primitivwurzel *von F. Somit gilt $F^\times = \langle a\rangle$ und insbesondere $F = \mathbb{F}_p[a]$.* □

Satz 13B9. *Sei F ein Körper der Ordnung p^n. Dann ist $\mathrm{Aut}(F) = \langle \mathfrak{f}_p\rangle$ eine zyklische Gruppe der Ordnung n, die vom Frobenius-Automorphismus $\mathfrak{f}_p\colon F \to F$ erzeugt wird.*

BEWEIS. Wir wissen bereits, dass $\mathfrak{f}_p\colon F \to F$ ein Körperautomorphismus ist. Jedes Element $a \in F$ erfüllt $a^{p^n} = a$, also gilt $\mathfrak{f}_p^n = \mathrm{id}_F$. Wäre $\mathfrak{f}_p^k = \mathrm{id}_F$ für $1 \leq k < n$, dann gälte $a^{p^k} = a$ für alle $a \in F$, und somit hätte $X^{p^k}-X$ mehr Nullstellen als sein Grad p^k erlaubt. Also ist $\langle \mathfrak{f}_p\rangle < \mathrm{Aut}(F)$ eine Untergruppe der Ordnung n.

Wir zeigen schließlich $\mathrm{Aut}(F) = \langle \mathfrak{f}_p\rangle$. Es existiert ein Element $a \in F$ sodass $F = \mathbb{F}_p[a]$, zum Beispiel eine Primitivwurzel von F. Sei $P = \mathrm{Irr}^X_{\mathbb{F}_p}(a)$ das Minimalpolynom in $\mathbb{F}_p[X]$. Es gilt dann $\mathbb{F}_p[X]/(P) \cong F$ und $\deg(P) = n$. Wegen $F = \mathbb{F}_p[a]$ ist jeder Automorphismus $f \in \mathrm{Aut}(F)$ bereits durch das Bild $f(a)$ festgelegt. Andererseits muss $f(a)$ eine Nullstelle von P sein, denn $P(f(a)) = f(P(a)) = f(0) = 0$. Demnach gilt $|\mathrm{Aut}(F)| \leq n$. □

§**13Be. Galois-Korrespondenz.** Sei F ein endlicher Körper der Ordnung p^n. Wir haben die Teilkörper von F und die Untergruppen von $\mathrm{Aut}(F)$ oben explizit angegeben. Den Vergleich fassen wir in folgender Beobachtung zusammen:

- Für jeden Teiler $m \mid n$ in $\mathbb{N}$ existiert genau eine Untergruppe der Ordnung n/m von $\mathrm{Aut}(\mathfrak{f}_p)$, nämlich $\langle \mathfrak{f}_p^m\rangle$. Ihr Fixkörper ist der Teilkörper $K < F$ der Ordnung p^m.
- Für jeden Teiler $m \mid n$ in $\mathbb{N}$ existiert genau ein Teilkörper $K < F$ der Ordnung p^m, und die Automorphismengruppe $\mathrm{Aut}(F|K) = \langle \mathfrak{f}_p^m\rangle$ ist zyklisch der Ordnung n/m.

Dies ist ein Parade-Beispiel für die Galois-Korrespondenz, die wir in Kapitel 14 entwickeln werden. Im Falle eines endlichen Körpers besagt sie folgendes:

Satz 13B10. *Für jeden endlichen Körper E haben wir eine natürliche Bijektion zwischen den Teilkörpern $F < E$ und den Untergruppen $G < \mathrm{Aut}(E)$:*

- *Zu jedem Teilkörper $F < E$ haben wir die Untergruppe*
$$\mathrm{Aut}(E|F) = \{\, g \in \mathrm{Aut}(E) \mid g(x) = x \text{ für alle } x \in F \,\}.$$
- *Zu jeder Untergruppe $G < \mathrm{Aut}(E)$ haben wir den Teilkörper*
$$\mathrm{Fix}(G) = \{\, x \in E \mid g(x) = x \text{ für alle } g \in G \,\}.$$

Diese Zuordnungen sind zueinander inverse Bijektionen:

- *Für jeden Teilkörper $F < E$ und $G = \mathrm{Aut}(E|F)$ gilt $\mathrm{Fix}(G) = F$.*
- *Für jede Untergruppe $G < \mathrm{Aut}(E)$ und $F = \mathrm{Fix}(G)$ gilt $\mathrm{Aut}(E|F) = G$.*

Dies fassen wir prägnant zusammen durch
$$\mathrm{Fix}(\mathrm{Aut}(E|F)) = E \qquad \text{und} \qquad \mathrm{Aut}(E|\mathrm{Fix}(G)) = G.$$

Sind $K < F < E$ Teilkörper, dann gilt $g(F) = F$ für jeden Körperautomorphismus $g \in \mathrm{Aut}(E|K)$. Die Einschränkung definiert demnach einen surjektiven Gruppenhomomorphismus $\mathrm{Aut}(E|K) \twoheadrightarrow \mathrm{Aut}(F|K)$, $g \mapsto g|_F$ mit Kern $\mathrm{Aut}(E|F)$.

Dies fassen wir prägnant zusammen durch die kurze exakte Sequenz
$$\mathrm{Aut}(E|F) \hookrightarrow \mathrm{Aut}(E|K) \twoheadrightarrow \mathrm{Aut}(F|K).$$

§**13Bf. Algebraischer Abschluss.** In §12E haben wir gesehen, dass zu jedem Körper K ein algebraischer Abschluss $C|K$ existiert. Für endliche Körper können wir nun eine besonders einfache Konstruktion des algebraischen Abschlusses angeben.

Sei $p \in \mathbb{N}$ eine Primzahl und $E_0 = \mathbb{F}_p$. Für jedes $n \in \mathbb{N}$ existiert ein endlicher Körper E_n der Ordnung $p^{n!}$ (13B5). Da $n!$ ein Teiler von $(n+1)!$ ist, enthält E_{n+1} genau einen Teilkörper isomorph zu E_n (13B7). Es gibt demnach $n!$ Körperhomomorphismen $E_n \hookrightarrow E_{n+1}$; wir wählen hiervon eine Einbettung $\sigma_n \colon E_n \hookrightarrow E_{n+1}$ und identifizieren E_n mittels σ_n mit dem Bild in E_{n+1}. Wir erhalten so eine Kette endlicher Körper
$$E_1 < E_2 < E_3 < \dots.$$

Lemma 13B11. *Die Vereinigung $\bar{\mathbb{F}}_p = \bigcup_{n\in\mathbb{N}} E_n$ ist auf natürliche Weise ein Körper.*

BEWEIS. Für je zwei Elemente $a, b \in \bar{\mathbb{F}}_p$ existiert ein Index $n \in \mathbb{N}$, für den $a, b \in E_n$ gilt. Wir definieren Summe $a+b$ und Produkt ab in $\bar{\mathbb{F}}_p$ wie in E_n. Dies ist wohldefiniert, denn $E_n < E_m$ ist ein Teilkörper für alle $n \le m$. Die Körperaxiome gelten in jedem Teilkörper E_n also auch in $\bar{\mathbb{F}}_p$. □

Lemma 13B12. *Der Körper $\bar{\mathbb{F}}_p$ enthält zu jeder natürlichen Zahl $n \in \mathbb{N}_{\ge 1}$ genau einen Teilkörper $\mathbb{F}_{p^n}$ der Ordnung p^n, nämlich $\mathbb{F}_{p^n} = \{\, a \in \bar{\mathbb{F}}_p \mid a^{p^n} = a \,\}$.*

BEWEIS. Wegen $n \mid n!$ enthält der Körper E_n der Ordnung $p^{n!}$ einen Teilkörper der Ordnung p^n. Die Eindeutigkeit beweist man wie in 13B5. □

Satz 13B13. *Der Körper $\bar{\mathbb{F}}_p$ ist ein algebraischer Abschluss des Primkörpers $\mathbb{F}_p$.*

BEWEIS. Nach Konstruktion ist jedes Element $a \in \bar{\mathbb{F}}_p$ algebraisch über $\mathbb{F}_p$, denn es gilt $a \in E_n$ für ein $n \in \mathbb{N}$ und E_n ist endlich und damit algebraisch über $\mathbb{F}_p$. Sei $P \in \mathbb{F}_p[X]^*$ ein Polynom. Der Zerfällungskörper F von P über $\mathbb{F}_p$ ist endlich über $\mathbb{F}_p$, der Dimension n. Es gilt $n \mid n!$ und somit $F \hookrightarrow E_n < \bar{\mathbb{F}}_p$. Damit zerfällt P über $\bar{\mathbb{F}}_p$. □

Bemerkung 13B14. Wenn man einen algebraischen Abschluss $\bar{\mathbb{F}}_p|\mathbb{F}_p$ vorgibt, dann kann man für jedes $n \in \mathbb{N}_{\geq 1}$ von *dem* Körper $\mathbb{F}_{p^n}$ der Ordnung p^n sprechen. Das ist eine häufig zu findende, bequeme Sprachregelung. Ohne weitere Präzisierung ist es ratsam, bescheidener von *einem* Körper F der Ordnung p^n zu sprechen: ein solcher existiert und je zwei sind isomorph. Allerdings gibt es keinen kanonischen Isomorphismus (§13Ad).

§13C. Konstruktion endlicher Körper

Wir wenden uns nun der praktischen Frage zu, wie man einen endlichen Körper F der Ordnung p^n möglichst konkret konstruieren kann, um zum Beispiel Rechnungen in F auszuführen. Dies ist mit unseren bisherigen Mitteln zwar möglich aber noch sehr umständlich. Die folgende Beobachtung weist uns den rechten Weg:

- Ist F ein Körper der Ordnung p^n, dann existiert $a \in F$ mit $F = \mathbb{F}_p[a]$ und das zugehörige Minimalpolynom $\operatorname{Irr}^X_{\mathbb{F}_p}(a)$ ist irreduzibel vom Grad n.
- Ist umgekehrt $P \in \mathbb{F}_p[X]$ ein irreduzibles Polynom vom Grad $n \geq 1$, dann ist $F = \mathbb{F}_p[X]/(P)$ ein Körper der Ordnung p^n und $F = \mathbb{F}_p[x]$ mit $x = \pi(X)$.

In diesem Sinne entspricht jedes Paar (F,a) eines endlichen Körper F der Ordnung p^n mit der Wahl eines primitiven Elements $a \in F$ einem irreduziblen Polynom $P \in \mathbb{F}_p[X]$ (12D7).

Das bedeutet insbesondere: Um einen Körper der Ordnung p^n zu konstruieren genügt es, ein irreduzibles Polynom $P \in \mathbb{F}_p[X]$ vom Grad n zu finden. Wir werden in diesem Abschnitt die nötigen Hilfsmittel entwickeln.

§**13Ca. Beispiel: Körper der Ordnung** 4. Das Polynom X^2+X+1 von Grad 2 ist irreduzibel über $\mathbb{F}_2$, denn es hat keine Nullstelle in $\mathbb{F}_2$. (Es ist das einzige irreduzible Polynom vom Grad 2 über $\mathbb{F}_2$, wie man leicht ausprobiert.) Der Quotientenring $\mathbb{F}_4 := \mathbb{F}_2[X]/(X^2+X+1)$ ist demnach ein Körper der Ordnung 4.

Als $\mathbb{F}_2$-Basis können wir $(1,x)$ wählen, wobei $x = \pi(X)$ das Bild von X in $\mathbb{F}_4$ ist. Die Verknüpfungstafeln der Addition und der Multiplikation sind dann (mit $y = 1+x$):

$+$	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

$\cdot$	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

Wegen $x^2 = x+1$ kann die Multiplikation auch wie folgt formuliert werden:

$$(\alpha+\beta x)(\alpha'+\beta' x) = (\alpha\alpha'+\beta\beta') + (\alpha\beta'+\beta\alpha'+\beta\beta')x.$$

Übung 13C1. Nach obigem Vorbild konstruiere man Körper der Ordnung 8, 9, 25, 27.

§**13Cb. Irreduzible Polynome.** Wir wollen irreduzible Polynome über $\mathbb{F}_p$ besser verstehen lernen. Dazu gehört, ihre Anzahl zu berechnen oder ihre Häufigkeit abzuschätzen.

Lemma 13C2. *Sei $P \in \mathbb{F}_p[X]$ ein irreduzibles Polynom vom Grad d.*

1. *Der Quotient $F = \mathbb{F}_p[X]/(P)$ ist ein Zerfällungskörper von P über $\mathbb{F}_p$.*
2. *Es gilt $P \mid X^{p^n} - X$ genau dann wenn $d \mid n$.*

BEWEIS. (1) Nach Konstruktion wissen wir, dass P eine Nullstelle in F hat, nämlich das Bild $x = \pi(X)$, und es gilt $F = \mathbb{F}_p[x]$. Die Automorphismengruppe $\mathrm{Aut}(F) = \langle \mathfrak{f}_p \rangle$ hat d Elemente und bildet x auf d verschiedene Elemente $x_1, \dots, x_d$ mit $x_k = \mathfrak{f}_p^k(x)$ ab: Wäre $x_i = x_j$ mit $i < j$, dann wäre $\mathfrak{f}_p^i = \mathfrak{f}_p^j$ und somit $\mathfrak{f}_p^{j-i} = \mathrm{id}_F$, im Widerspruch zur Ordnung $\mathrm{ord}(\mathfrak{f}_p) = n$. Wegen $P(\mathfrak{f}_p^k(x)) = \mathfrak{f}_p^k(P(x)) = \mathfrak{f}_p^k(0) = 0$ hat P genau d Nullstellen in F, nämlich $P = (X - x_1) \cdots (X - x_d)$.

(2) Sei E der Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{F}_p$, das heißt E ist ein Körper der Ordnung p^n und wir wissen $X^{p^n} - X = \prod_{a \in E}(X - a)$. Wenn $P \mid X^{p^n} - X$, dann enthält E einen Teilkörper isomorph zu F, also gilt $d \mid n$. Umgekehrt, wenn $d \mid n$ gilt, dann enthält E einen Teilkörper isomorph zu F, und somit $P \mid X^{p^n} - X$. □

Satz 13C3. *Sei $I_p^d \subset \mathbb{F}_p[X]$ die Menge der irreduziblen normierten Polynome vom Grad d über $\mathbb{F}_p$. In $\mathbb{F}_p[X]$ gilt dann die Zerlegung $X^{p^n} - X = \prod_{d \mid n} \prod_{P \in I_p^d} P$.*

BEWEIS. Wir wissen, dass sich $f = X^{p^n} - X$ wie jedes Polynom in $\mathbb{F}_p[X]$ eindeutig in ein Produkt irreduzibler Faktoren zerlegen lässt. Nach dem Lemma kommen als Faktoren genau die Polynome aus I_p^d mit $d \mid n$ vor. Wegen $\mathrm{ggT}(f, f') = 1$ kommt keiner dieser Faktoren mehrfach vor. □

Korollar 13C4. *Es gilt $p^n = \sum_{d \mid n} d \cdot |I_p^d|$.*

BEWEIS. Dies folgt aus $X^{p^n} - X = \prod_{d \mid n} \prod_{P \in I_p^d} P$ durch Betrachtung der Grade. □

Korollar 13C5. *Für die Anzahl $|I_p^d|$ der irreduziblen normierten Polynome vom Grad d über $\mathbb{F}_p$ gilt die Abschätzung $\frac{1}{n}\left(p^n - 2p^{n/2}\right) \leq |I_p^n| \leq \frac{1}{n} p^n$.*

BEWEIS. Die Abschätzung $n|I_p^n| \leq p^n$ ist klar. Man findet nun

$$\sum_{d \mid n, d < n} d \cdot |I_p^d| \leq \sum_{1 \leq d \leq n/2} d \cdot |I_p^d| \leq \sum_{1 \leq d \leq n/2} p^d < \frac{p^{n/2+1} - 1}{p - 1} \leq 2p^{n/2}.$$

Die beweist $n|I_p^n| = p^n - \sum_{d \mid n, d < n} d \cdot |I_p^d| \geq p^n - 2p^{n/2}$. □

Diese Abschätzung bedeutet anschaulich folgendes: In $\mathbb{F}_p[X]$ gibt es genau p^n normierte Polynome vom Grad n. Wählt man zufällig ein normiertes Polynom $P \in \mathbb{F}_p[X]$ vom Grad n aus, so liegt Wahrscheinlichkeit, dass P irreudzibel ist, knapp unter $\frac{1}{n}$.

§**13Cc. Irreduzibilitätskriterium.**

Proposition 13C6. *Ein Polynom $P \in \mathbb{F}_p[X]$ von Grad n ist genau dann irreduzibel wenn $P \mid X^{p^n} - X$ gilt sowie $\mathrm{ggT}(P, X^{p^{n/t}} - X) = 1$ für alle Primteiler t von n.*

BEWEIS. Wenn P irreduzibel vom Grad n ist, dann teilt P zwar $X^{p^n}-X$ aber keines der Polynome $X^{p^{n/t}}-X$, also gilt $\operatorname{ggT}(P, X^{p^{n/t}}-X)=1$.

Nehmen wir umgekehrt an, P teilt $X^{p^n}-X$ und es gilt $\operatorname{ggT}(P, X^{p^{n/t}}-X)=1$ für alle Primteiler t von n. Sei Q ein irreduzibler Faktor von P, vom Grad $\deg Q = d$. Wegen $Q \mid X^{p^n}-X$ gilt dann $d \mid n$. Wäre $d<n$, dann teilte Q eines der Polynome $\operatorname{ggT}(P, X^{p^{n/t}}-X)$, was wir ausgeschlossen haben. Also gilt $d=n$ und somit $P \sim Q$. □

Oft ist der Grad $n=\deg(P)$ noch relativ klein, aber der Grad p^n von $X^{p^n}-X$ unvernünftig groß. Der folgende Algorithmus berechnet daher $X^{p^n}-X$ modulo P, sodass alle Zwischenergebnisse vom Grad $\leq n$ bleiben.

Algorithmus 10 Prüfen der Irreduzibilität von $P \in \mathbb{F}_p[X]$

Eingabe: Ein Polynom $P \in \mathbb{F}_p[X]$ vom Grad n sowie die Primfaktorzerlegung $n = n_1^{e_1} \cdots n_k^{e_k}$.
Ausgabe: Die Antwort "irreduzibel" wenn P irreduzibel ist und "zerlegbar" sonst.

```
Q ← X^{p^n} rem P                          // binäres Potenzieren modulo P
if Q ≠ X then return "zerlegbar"           // denn P ∤ X^{p^n} − X
for i from 1 to k do
    m ← n/n_i
    Q ← X^{p^m} rem P                      // binäres Potenzieren modulo P
    R ← ggT(P, Q − X)                      // Euklidischer Algorithmus
    if R ≠ 1 then return "zerlegbar"       // denn ggT(P, X^{p^m} − X) ≠ 1
end for
return "irreduzibel"                       // nach der vorherigen Proposition
```

Übung 13C7. Man beweise, dass Algorithmus 10 korrekt ist und schätze seine Komplexität ab.

Algorithmus 11 Finden eines irreduziblen Polynoms $P \in \mathbb{F}_p[X]$ vom Grad n

Eingabe: Eine Primzahl $p \geq 2$ und eine natürliche Zahl $n \geq 1$.
Ausgabe: Ein irreduzibles normiertes Polynom $P \in \mathbb{F}_p[X]$ vom Grad n.

```
P ← ein zufälliges normiertes Polynom vom Grad n in F_p[X]
for m from 1 to ⌊n/2⌋ do
    Q ← X^{p^m} rem P                      // binäres Potenzieren modulo P
    R ← ggT(P, Q − X)                      // Euklidischer Algorithmus
    if R ≠ 1 then Neu anfangen mit neuer Wahl von P
end for
return P
```

Übung 13C8. Man beweise, dass Algorithmus 11 korrekt ist und schätze seine (durchschnittliche) Komplexität ab.

§13D. Übungen und Ergänzungen

§13Da. Körper der Ordnung 125. Wir haben oben einen Körper der Ordnung 4 konstruiert. Als ein etwas interessanteres Beispiel betrachten wir zwei Quotienten von $\mathbb{F}_5[X]$:

Übung 13D1. Über dem Körper $\mathbb{F}_5$ sei

$$P = X^3 + X + 1, \qquad E = \mathbb{F}_5[X]/(P), \qquad x = \pi(X),$$
$$Q = Y^3 + 2Y^2 - Y + 2, \qquad F = \mathbb{F}_5[Y]/(Q), \qquad y = \pi(Y).$$

1. Welche Ordnung haben E und F? Sind diese Ringe Körper?
2. Man beschreibe die Verknüpfungen bezüglich der $\mathbb{F}_5$-Basis $(1, x, x^2)$:
   - Wie addiert man $a = a_0 + a_1x + a_2x^2$ und $b = b_0 + b_1x + b_2x^2$ zu einem Ergebnis derselben Form $c = c_0 + c_1x + c_2x^2$?
   - Wie multipliziert man $a = a_0 + a_1x + a_2x^2$ und $b = b_0 + b_1x + b_2x^2$ zu einem Ergebnis derselben Form $c = c_0 + c_1x + c_2x^2$?
3. Man berechne $Q(x^2 - x)$ in E.
4. Man bestimme den Kern des Homomorphismus $\phi\colon \mathbb{F}_5[Y] \to E$, $Y \mapsto x^2 - x$.
5. Man konstruiere einen Isomorphismus $\mathbb{F}_5[Y]/(Q) \xrightarrow{\sim} \mathbb{F}_5[X]/(P)$.

§13Db. Irreduzible Polynome über $\mathbb{F}_p$.

Übung 13D2. Hat das Polynom $X^2 + X + 1$ eine Wurzel in $\mathbb{F}_2$? in $\mathbb{F}_4$? in $\mathbb{F}_8$? in $\mathbb{F}_{16}$? In welchen Körpern $\mathbb{F}_{2^n}$ für $n \in \mathbb{N}$?

Übung 13D3. Man bestimme die Unterkörper von $\mathbb{F}_{4096}$ mit ihren Inklusionen. Man bestimme entsprechend die Untergruppen von $\mathrm{Aut}(\mathbb{F}_{4096})$ mit ihren Inklusionen.

Übung 13D4. Sei p eine Primzahl und sei $a \in \mathbb{F}_p^\times$. Man zeige, dass $X^p - X - a$ irreduzibel über $\mathbb{F}_p$ ist. (Im Spezialfall $p = 2$ findet man $X^2 + X + 1$ wieder.)

Übung 13D5. Sei $p \in \mathbb{N}$ eine Primzahl und $n \in \mathbb{N}_{\geq 1}$. Gibt es ein irreduzibles Polynom $P \in \mathbb{F}_p[X]$ vom Grad n, sodass die multiplikative Gruppe $F^\times$ des Körpers $F = \mathbb{F}_p[X]/(P)$ erzeugt wird durch das Bild von X?

Übung 13D6. Wieviele Quadrate gibt es in $\mathbb{F}_{61}^\times$? Wieviele 3. Potenzen? 4.? 5.? 6.? 7.?

Übung 13D7. Wieviele Primitivwurzeln gibt es im Körper $\mathbb{F}_q$? In $\mathbb{F}_3$ und $\mathbb{F}_4$ zum Beispiel sind alle Elemente außer 0 und 1 Primitivwurzeln. In der Reihenfolge aufsteigender Ordnung, welches sind die nächsten Körper mit dieser bemerkenswerten Eigenschaft? Man versuche eine möglichst explizite Charakterisierung.

§13Dc. Das Polynom $X^4 + 1$.

Übung 13D8. Man zeige, dass $P = X^4 + 1$ irreduzibel über $\mathbb{Q}$ ist, aber reduzibel über $\mathbb{F}_2$.

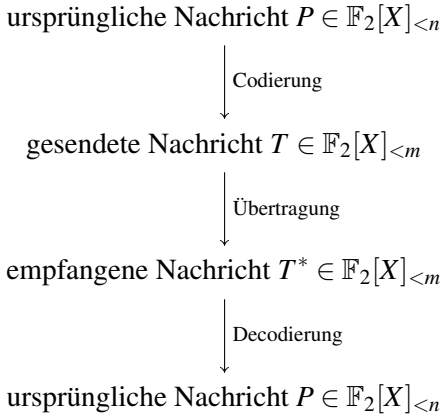
Wir wollen zeigen, dass P reduzibel über jedem endlichen Körper $\mathbb{F}_p$ für $p \geq 3$ ist.

Übung 13D9. Man zeige 8 teilt $p^2 - 1$ und folgere das es ein Element $a \in \mathbb{F}_{p^2}$ gibt mit $a^4 = -1$. Somit erlaubt P eine Wurzel in $\mathbb{F}_{p^2}$ und ist reduzibel über $\mathbb{F}_p$. Zur Illustration zerlege man $X^4 + 1$ in irreduzible Polynome in $\mathbb{F}_p[X]$ für $p = 2, 3, 5, 7, 11$.

§13Dd. Fehlererkennende und fehlerkorrigierende Codes.

Ein *Bit* ist die minimale Informationseinheit $a \in \{0, 1\}$. Wir identifizieren das Alphabet $\{0, 1\}$ mit dem Körper $\mathbb{F}_2$. Eine Folge $(a_{n-1}, \ldots, a_1, a_0)$ von n Bits betrachten wir als Polynom $\sum_{i=0}^{n-1} a_k X^k$ in $\mathbb{F}_2[X]_{<n}$.

Fehlererkennender Code. — Ein Sender möchte eine Nachricht $P \in \mathbb{F}_2[X]_{<n}$ von n Bits über einen fehlerbehafteten Kanal übermitteln. Dies soll mittels eines vorher festgelegten Protokolls geschehen, das dem Empfänger erlaubt, einen eventuell auftretenden Bitfehler *erkennen* zu können. Statt P übermittelt man hierzu eine Nachricht $T \in \mathbb{F}_2[X]_{<m}$. Die empfangene Nachricht T^* ist bei fehlerfreier Übermittlung gleich T und hieraus soll die ursprüngliche Nachricht P rekonstruierbar sein. Wird das $i$te Bit von T fehlerhaft übermittelt, dann gilt $T^* = T + X^i$ mit $0 \leq i < m$, und hieraus soll die Fehlerhaftigkeit erkennbar sein.



Übung 13D10. Eine einfache Methode besteht darin, die Nachricht $P \in \mathbb{F}_2[X]_{<n}$ zweimal nacheinander zu übermitteln. Statt P übermittelt man also die Nachricht $T = X^n P + P$ in $\mathbb{F}_2[X]_{<2n}$. (Das kostet $2n$ Bits.) Man erkläre, wie dieses Protokoll die Erkennung eines Bitfehlers ermöglicht. Ermöglicht es auch seine Korrektur?

Übung 13D11. Man kann die Nachricht $P \in \mathbb{F}_2[X]_{<n}$ mit einem *Paritätsbit* versehen: Dies ist die Quersumme $P(1) = a_{n-1} + \cdots + a_0 \in \mathbb{F}_2$. Das so ergänzte Polynom $Q = XP + P(1)$ in $\mathbb{F}_2[X]_{<n+1}$ erfüllt stets $Q(1) = 0$. Man erläutere, wie die Übermittlung dieser $n+1$ Bits die Erkennung eines Bitfehlers ermöglicht. Ermöglicht sie auch seine Korrektur?

Fehlerkorrigierender Code. — Ein Sender möchte 120 Bits über einen fehlerbehafteten Kanal übermitteln. Dies soll mittels eines vorher festgelegten Protokolls geschehen, das dem Empfänger erlaubt, ein eventuell auftretendes fehlerhaftes Bit nicht nur erkennen sondern auch *korrigieren* zu können. Wie kann man dies möglichst effizient bewerkstelligen?

Übung 13D12. Eine einfache Methode besteht darin, die Nachricht 3 mal nacheinander zu übermitteln. (Das kostet 360 Bits.) Man erkläre, wie dies die Korrektur eines Bits ermöglicht.

Übung 13D13. Eine etwas bessere Methode besteht darin, die Nachricht $P \in \mathbb{F}_2[X]_{<120}$ mit einem Paritätsbit versehen und $Q = XP + P(1)$ zweimal zu übermitteln. (Das kostet 242 Bits.) Man erkläre, wie dieses Protokoll die Korrektur eines Bitfehlers erlaubt.

Damit haben wir die Kosten bereits von 360 Bit auf 242 Bit gesenkt. Wir präsentieren schließlich eine dritte, noch raffiniertere Methode. Für dieses Protokoll wählen wir ein irreduzibles Polynom $A \in \mathbb{F}_2[X]$ vom Grad 7. Ist $P \in \mathbb{F}_2[X]_{<120}$ die zu übermittelnde Nachricht, so berechnen wir $R = X^7 P \operatorname{rem} A$ und setzen $T = X^7 P + R$ in $\mathbb{F}_2[X]_{<127}$.

Übung 13D14. Die gesendete Nachricht erfüllt die Bedingung $T \operatorname{rem} A = 0$. Sei $T^* = T + X^i$ die empfangene Nachricht, wobei $0 \leq i < 127$. Im Körper $F = \mathbb{F}_2[X]/(A)$ sei x das Bild von X. Man zeige, dass x die Gruppe $F^\times$ erzeugt. Die Abbildung $X^i \mapsto x^i$ ist also injektiv für $0 \leq i < 127$. Man erkläre, wie man die ursprüngliche Nachricht T aus der empfangenen Nachricht T^* rekonstruieren kann. (Wir nehmen wie immer an, dass höchstens ein Bitfehler vorliegt). Worin besteht der Vorteil dieser Methode?

Übung 13D15. Um das obige Protokoll wirklich zu implementieren, müssen sich Sender und Empfänger vorab auf ein irreduzibles Polynom $A \in \mathbb{F}_2[X]$ vom Grad 7 verständigen. Wir schlagen $A = X^7 + X^3 + 1$ vor. Man zeige, dass A irreduzibel ist. *Hinweis:* Man erstelle zunächst die Liste aller irreduziblen Polynome vom Grad ≤ 3 in $\mathbb{F}_2[X]$. Diese sind X, $X+1$, X^2+X+1, X^3+X^2+1, X^3+X+1.

KAPITEL 14

Der Hauptsatz der Galois-Theorie

§14A. Einleitung und Überblick

Évariste GALOIS (1811–1832) hat kurz vor seinem tragischen Tod die Korrespondenz zwischen Körpererweiterungen $E|F$ und Automorphismengruppen $\mathrm{Aut}(E|F)$ aufgedeckt. Er dachte dabei konkret an die Auflösung von Gleichungen $a_nX^n + \cdots + a_1X + a_0 = 0$ und die Permutationen ihrer Wurzeln (§14D). Die Körperstruktur wurde später von Richard DEDEKIND (1831–1916) und Emil ARTIN (1898–1962) herausgearbeitet, und so treten in heutiger Darstellung die Körpererweiterungen und ihre Automorphismen in den Vordergrund.

§14Aa. Galois-Erweiterungen. Für jeden endlichen Körper E haben wir in §13Be die Galois-Korrespondenz zwischen Teilkörpern $F < E$ und Untergruppen $G < \mathrm{Aut}(E)$ explizit angeben können. Unser Ziel ist die Verallgemeinerung dieser Korrespondenz auf eine möglichst allgemeine Klasse von Körpererweiterungen $E|K$.

Definition 14A1. Eine algebraische Körpererweiterung $E|K$ heißt *galoissch* wenn

$$\mathrm{Fix}(\mathrm{Aut}(E|K)) = K.$$

In diesem Fall nennen wir $E|K$ auch eine *Galois-Erweiterung*. Die Automorphismengruppe der Erweiterung $E|K$ heißt dann auch *Galois-Gruppe*, geschrieben $\mathrm{Gal}(E|K) = \mathrm{Aut}(E|K)$.

Für jede Körpererweiterung $E|K$ gilt trivialerweise $\mathrm{Fix}(\mathrm{Aut}(E|K)) \supset K$. Die Bedingung $\mathrm{Fix}(\mathrm{Aut}(E|K)) = K$ besagt, dass jedes Element $a \in E \smallsetminus K$ von $\mathrm{Aut}(E|K)$ bewegt wird.

Beispiel 14A2. Jede endliche Erweiterung eines endlichen Körpers ist galoissch.

- Sei E ein endlicher Körper der Ordnung p^n und sei $\mathbb{F}_p < E$ der Primkörper. Dann hat die Erweiterung $E|\mathbb{F}_p$ Grad n und die Automorphismengruppe $\mathrm{Aut}(E|\mathbb{F}_p) = \langle \mathfrak{f}_p \rangle$ hat Ordnung n und erfüllt $\mathrm{Fix}(\mathrm{Aut}(E|\mathbb{F}_p)) = \mathbb{F}_p$.
- Etwas allgemeiner, sei m ein Teiler von n und sei $K < E$ der Teilkörper der Ordnung p^m. Dann hat die Erweiterung $E|K$ Grad n/m und die Automorphismengruppe $\mathrm{Aut}(E|K) = \langle \mathfrak{f}_p^m \rangle$ hat Ordnung n/m und erfüllt $\mathrm{Fix}(\mathrm{Aut}(E|K)) = K$.

Wir werden in diesem Kapitel Kriterien entwickeln, mit deren Hilfe wir eine große Klasse von Erweiterungen $E|K$ als galoissch nachweisen werden. Die folgende Charakterisierung besagt, dass Galois-Erweiterungen $E|K$ die größtmögliche Symmetrie aufweisen:

Satz 14A3. *Für jede endliche Körpererweiterung $E|K$ gilt*

$$|\mathrm{Aut}(E|K)| \leq |E:K|$$

und $E|K$ ist genau dann galoissch wenn hierbei Gleichheit gilt, also

$$|\mathrm{Aut}(E|K)| = |E:K|.$$

§**14Ab. Galois-Korrespondenz.** Das Ziel dieses Kapitels ist der folgende Hauptsatz der Galois-Theorie, der die ersehnte Galois-Korrespondenz in epischer Breite formuliert:

Satz 14A4. *Für jede endliche Galois-Erweiterung $E|K$ besteht eine natürliche Bijektion zwischen den Zwischenkörpern der Erweiterung $E|K$ und den Untergruppen von $\mathrm{Aut}(E|K)$:*

- *Zu jedem Zwischenkörper F mit $K < F < E$ haben wir die Untergruppe*
$$G = \mathrm{Aut}(E|F) = \{\, g \in \mathrm{Aut}(E|K) \mid g(x) = x \text{ für alle } x \in F \,\}.$$
- *Zu jeder Untergruppe $G < \mathrm{Aut}(E|K)$ haben wir den Teilkörper*
$$F = \mathrm{Fix}(G) = \{\, x \in E \mid g(x) = x \text{ für alle } g \in G \,\}.$$

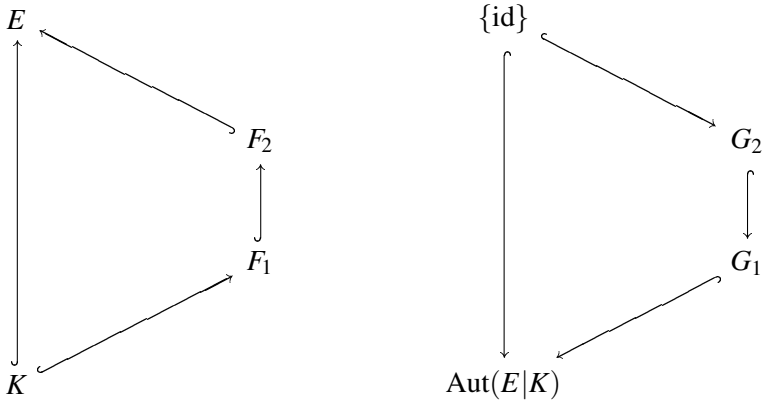
Diese Zuordnungen sind zueinander inverse Bijektionen, das heißt es gilt

$$\mathrm{Fix}(\mathrm{Aut}(E|F)) = F \qquad \text{und} \qquad \mathrm{Aut}(E|\mathrm{Fix}(G)) = G.$$

Diese Bijektion ist inklusionsumkehrend: Für alle Zwischenkörper F_1, F_2 von $E|K$ und die zugeordneten Untergruppen $G_1 = \mathrm{Aut}(E|F_1)$, $G_2 = \mathrm{Aut}(E|F_2)$ von $\mathrm{Aut}(E|K)$ gilt

$$F_1 < F_2 \qquad \Longleftrightarrow \qquad G_1 > G_2.$$

In Diagrammen kehren sich also alle Pfeile um:



Bei der Galois-Korrespondenz entsprechen sich Grad und Index:

$$|F_2 : F_1| = |G_1 : G_2|$$

Die Erweiterung $F_2|F_1$ ist genau dann galoissch, wenn G_2 normal in G_1 ist, kurz $G_2 \lhd G_1$. In diesem Fall gilt $g(F_2) = F_2$ für jeden Automorphismus $g \in Aut(E|F_1)$, und wir erhalten einen surjektiven Gruppenhomomorphismus $\mathrm{Aut}(E|F_1) \to \mathrm{Aut}(F_2|F_1)$ durch die Einschränkung $g \mapsto g|_{F_2}$, mit Kern $\mathrm{Aut}(E|F_2)$. Dies drücken wir aus durch die kurze exakte Sequenz

$$\mathrm{Aut}(E|F_2) \hookrightarrow \mathrm{Aut}(E|F_1) \twoheadrightarrow \mathrm{Aut}(F_2|F_1)$$

oder als Quotienten $\mathrm{Aut}(F|K) \cong \mathrm{Aut}(E|K)/\mathrm{Aut}(E|F)$.

§**14Ac. Erste Beispiele.** Der Beweis des Hauptsatzes und der nötigen Ausführungen wird uns das gesamte Kapitel beschäftigen. Zuvor wollen wir den Satz durch konkrete Beispiele illustrieren. Diese sind einfach genug, um (fast) alle Aussagen direkt ablesen zu können, aber zugleich hinreichend vielfältig, um einige Nuancen ausleuchten zu können.

Beispiel 14A5. Die Erweiterung $\mathbb{C}|\mathbb{R}$ ist galoissch, denn $\mathrm{Aut}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}_\mathbb{C}, \mathrm{conj}\}$ erfüllt $\mathrm{Fix}(\mathrm{Aut}(\mathbb{C}|\mathbb{R})) = \mathbb{R}$. Offensichtlich entsprechen die Untergruppen den Zwischenkörpern:

$$\begin{array}{ccc} \{\mathrm{id}\} & & \mathbb{C} \\ \Big| & & \Big| \\ 2 & & 2 \\ \Big| & & \Big| \\ \langle \mathrm{conj} \rangle & & \mathbb{R} \end{array}$$

Beispiel 14A6. Der Zerfällungskörper von X^2-2 über $\mathbb{Q}$ ist $E = \mathbb{Q}[\sqrt{2}]$. Er ist vom Grad $|E:\mathbb{Q}| = 2$ mit Basis $(1, \sqrt{2})$, denn X^2-2 ist irreduzibel über $\mathbb{Q}$ und $E \cong \mathbb{Q}[X]/(X^2-2)$. Nach 12D6 gilt $\mathrm{Aut}(E|\mathbb{Q}) = \{\mathrm{id}, \sigma\}$ wobei $\sigma\colon E \to E$ durch $a+b\sqrt{2} \mapsto a-b\sqrt{2}$ für alle $a, b \in Q$ definiert ist. Es gilt $\mathrm{Fix}(\mathrm{Aut}(E|\mathbb{Q})) = \mathbb{Q}$, also ist $E|\mathbb{Q}$ galoissch.

id	1	$\sqrt{2}$
σ	1	$-\sqrt{2}$

Die Gruppe $\mathrm{Aut}(E|\mathbb{Q})$ der Ordnung 2 hat nur zwei Untergruppen: Die triviale Gruppe $\{\mathrm{id}\}$ entspricht dem Fixkörper E, und $\mathrm{Aut}(E|\mathbb{Q}) = \langle\sigma\rangle$ entspricht dem Fixkörper $\mathbb{Q}$.

$$\begin{array}{ccc} \{\mathrm{id}\} & & \mathbb{Q}[\sqrt{2}] \\ \Big| & & \Big| \\ 2 & & 2 \\ \Big| & & \Big| \\ \langle\sigma\rangle & & \mathbb{Q} \end{array}$$

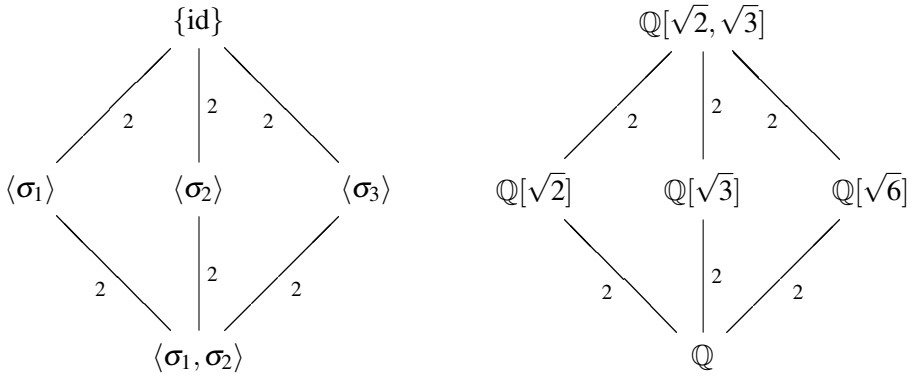
Beispiel 14A7. Der Zerfällungskörper von $P = (X^2-2)(X^2-3)$ über $\mathbb{Q}$ ist $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Wir wissen bereits $|\mathbb{Q}[\sqrt{2}]:\mathbb{Q}| = 2$ mit Basis $(1, \sqrt{2})$ über $\mathbb{Q}$. Man prüft nach, dass $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$ gilt. Somit ist X^2-3 auch irreduzibel über $\mathbb{Q}[\sqrt{2}]$, also $|E:\mathbb{Q}[\sqrt{2}]| = 2$ mit Basis $(1, \sqrt{3})$ über $\mathbb{Q}[\sqrt{2}]$. Demnach gilt $|E:\mathbb{Q}| = 4$ mit Basis $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ über $\mathbb{Q}$.

Nach 12D6 existiert $\sigma \in \mathrm{Aut}(E|\mathbb{Q}[\sqrt{2}])$ mit $\sigma(\sqrt{3}) = -\sqrt{3}$ und $\tau \in \mathrm{Aut}(E|\mathbb{Q}[\sqrt{3}])$ mit $\sigma(\sqrt{2}) = -\sqrt{2}$. Hieraus gewinnen wir die Automorphismen der Erweiterung $E|\mathbb{Q}$:

id	1	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{6}$
σ	1	$\sqrt{2}$	$-\sqrt{3}$	$-\sqrt{6}$
τ	1	$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{6}$
$\sigma\tau$	1	$-\sqrt{2}$	$-\sqrt{3}$	$\sqrt{6}$

Als $\mathbb{Q}$-lineare Abbildungen reicht es für $\sigma, \tau, \sigma\tau$, die Bilder der Basis anzugeben. Dass $\sigma, \tau, \sigma\tau$ tatsächlich Körperhomomorphismen sind, ließe sich aus diesen Daten leicht nachprüfen. Es gelingt jedoch mühelos ganz ohne Rechnung mit Satz 12D6 wie oben angegeben.

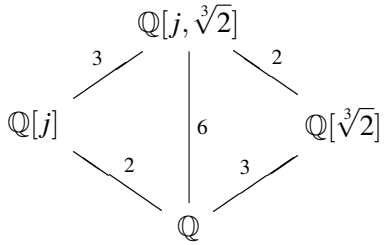
Die Gruppe $\mathrm{Aut}(E|\mathbb{Q})$ hat neben den trivialen Untergruppen genau drei nicht-triviale Untergruppen, jeweils der Ordnung 2. Diese entsprechen wie folgt den Zwischenkörpern:



Diese Zwischenkörper hätte man auch leicht ohne die Galois-Korrespondenz finden können. Aber sehen Sie ohne weitere Hilfsmittel ebenso leicht, warum es keine weiteren als die genannten Zwischenkörper geben kann? Selbst die Tatsache, dass es nur *endlich* viele Zwischenkörper gibt, ist ohne weitere Hilfsmittel nicht leicht zu zeigen (§14Bd).

Beispiel 14A8. Als Gegenbeispiel hier eine Erweiterung $E|K$, die nicht galoissch ist. Über $\mathbb{Q}$ ist $P = X^3 - 2$ irreduzibel und somit ist die Erweiterung $E = \mathbb{Q}[\sqrt[3]{2}]$ vom Grad $|E:\mathbb{Q}| = 3$. Allerdings ist $\mathrm{Aut}(E|\mathbb{Q}) = \{\mathrm{id}_E\}$: Für jeden Automorphismus $\sigma\colon E \to E$ über $\mathbb{Q}$ gilt $P(\sigma(\sqrt[3]{2})) = \sigma(P(\sqrt[3]{2})) = \sigma(0) = 0$. Aber $\sqrt[3]{2}$ ist die einzige Nullstelle von P in E: Die beiden anderen Nullstellen $j\sqrt[3]{2}$ und $j^2\sqrt[3]{2}$ liegen nicht in $\mathbb{R}$, also sicherlich nicht in E. Somit muss $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ gelten, also $\sigma = \mathrm{id}_E$. Demnach ist die Erweiterung $E|Q$ nicht galoissch, denn $\mathrm{Fix}(\mathrm{Aut}(E|\mathbb{Q})) = E \neq \mathbb{Q}$. Man sieht sofort, dass hier die Galois-Korrespondenz nicht gelten kann. Aber auch solche Körpererweiterungen sind der Galois-Theorie zugänglich, wenn man zur *normalen Hülle* wie im nächsten Beispiel übergeht.

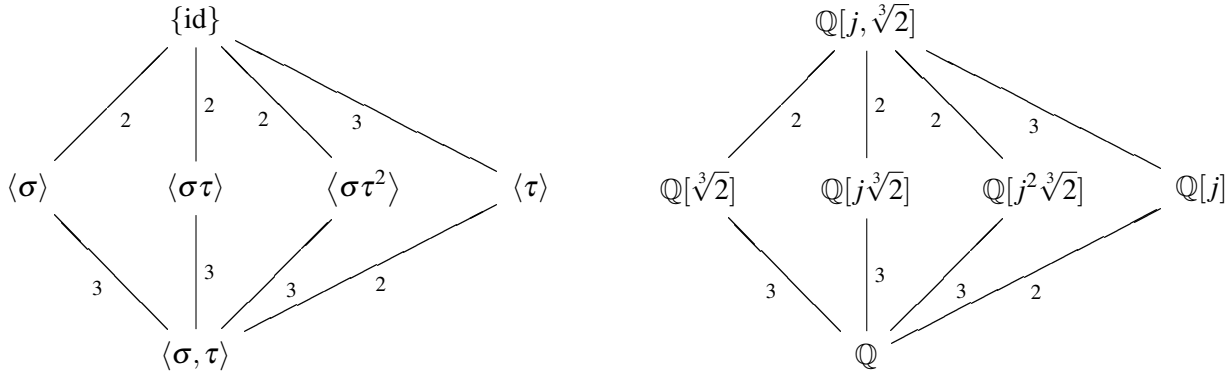
Beispiel 14A9. Der Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$ ist $E = \mathbb{Q}[j, \sqrt[3]{2}]$ mit $j = e^{2\pi i/3}$. Wegen $\mathrm{Irr}^X_{\mathbb{Q}}(j) = X^2 + X + 1$ gilt $|\mathbb{Q}[j]:\mathbb{Q}| = 2$. Das Polynom $X^3 - 2$ ist irreduzibel über $\mathbb{Q}$ wegen $\mathrm{ggT}(2,3) = 1$ bleibt es irreduzibel über $\mathbb{Q}[j]$. Also gilt $|E:\mathbb{Q}[j]| = 3$ und somit $|E:\mathbb{Q}| = 6$. Als Basis für E über $\mathbb{Q}$ wählen wir $(1, j, \sqrt[3]{2}, j\sqrt[3]{2}, \sqrt[3]{4}, j\sqrt[3]{4})$.



Nach 12D6 existiert $\tau \in \mathrm{Aut}(E|\mathbb{Q}[j])$ mit $\tau(\sqrt[3]{2}) = j\sqrt[3]{2}$ und $\sigma \in \mathrm{Aut}(E|\mathbb{Q}[\sqrt[3]{2}])$ mit $\sigma(j) = j^2$. Hieraus gewinnen wir die Automorphismen der Erweiterung $E|\mathbb{Q}$:

id	1	j	$\sqrt[3]{2}$	$j\sqrt[3]{2}$	$\sqrt[3]{4}$	$j\sqrt[3]{4}$
τ	1	j	$j\sqrt[3]{2}$	$j^2\sqrt[3]{2}$	$j^2\sqrt[3]{4}$	$\sqrt[3]{4}$
τ^2	1	j	$j^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$j\sqrt[3]{4}$	$j^2\sqrt[3]{4}$
σ	1	j^2	$\sqrt[3]{2}$	$j^2\sqrt[3]{2}$	$\sqrt[3]{4}$	$j^2\sqrt[3]{4}$
$\sigma\tau$	1	j^2	$j^2\sqrt[3]{2}$	$j\sqrt[3]{2}$	$j\sqrt[3]{4}$	$\sqrt[3]{4}$
$\sigma\tau^2$	1	j^2	$j\sqrt[3]{2}$	$\sqrt[3]{2}$	$j^2\sqrt[3]{4}$	$j\sqrt[3]{4}$

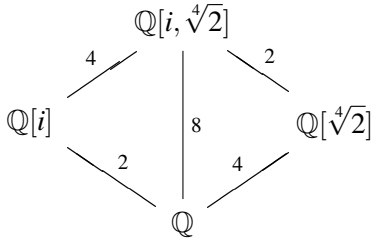
Man sieht, dass $\tau^3 = \sigma^2 = (\sigma\tau)^2 = (\sigma\tau^2)^2 = \mathrm{id}$. Die Gruppe $\mathrm{Aut}(E|\mathbb{Q})$ ist isomorph zur symmetrischen Gruppe S_3. Neben den trivialen Untergruppen hat sie eine Untergruppe $\langle\tau\rangle$ der Ordnung 3 und drei Untergruppen $\langle\sigma\rangle$, $\langle\sigma\tau\rangle$, $\langle\sigma\tau^2\rangle$ der Ordnung 2. Diese entsprechen wie folgt den Zwischenkörpern von $E|\mathbb{Q}$:



Beispiel 14A10. Der Zerfällungskörper des Polynoms $X^4 - 2$ über $\mathbb{Q}$ ist

$$E = \mathbb{Q}[\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}] = \mathbb{Q}[i, \sqrt[4]{2}].$$

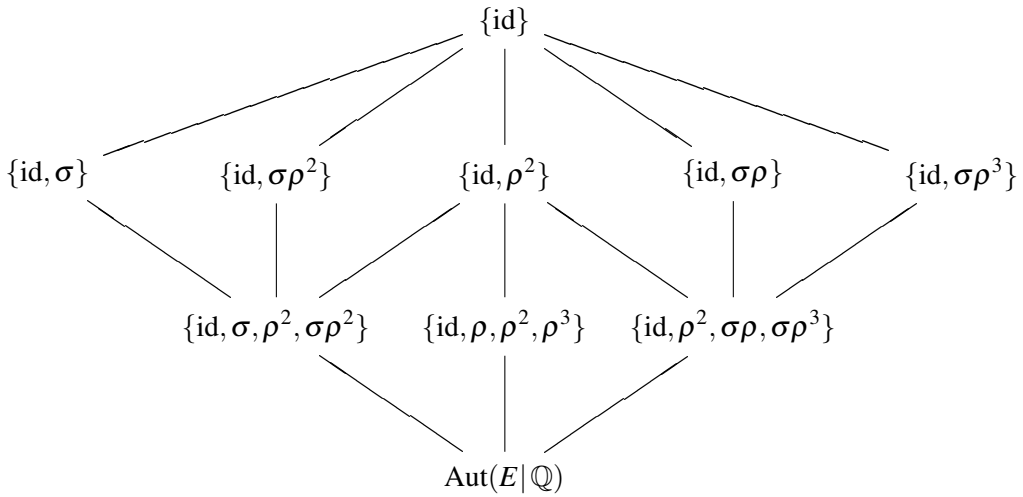
Da $X^4 - 2$ über $\mathbb{Q}$ irreduzibel ist, gilt $|\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}| = 4$. Wegen $i \notin \mathbb{Q}[\sqrt[4]{2}]$ gilt $|E : \mathbb{Q}[\sqrt[4]{2}]| = 2$, also insgesamt $|E : \mathbb{Q}| = 8$. Das folgende Diagramm veranschaulicht diese Rechnung:



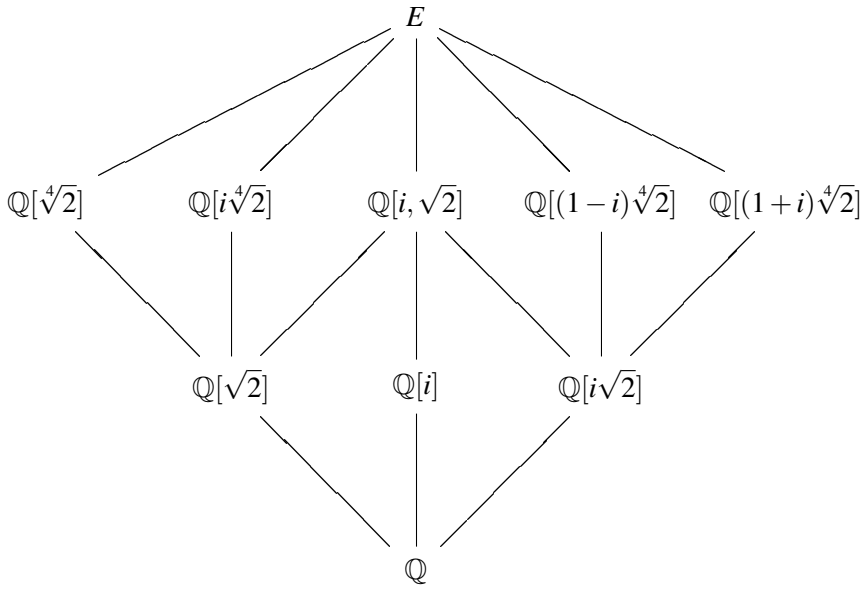
Nach 12D6 existiert $\rho \in \mathrm{Aut}(E|\mathbb{Q}[i])$ mit $\rho(\sqrt[4]{2}) = i\sqrt[4]{2}$ und $\sigma \in \mathrm{Aut}(E|\mathbb{Q}[\sqrt[4]{2}])$ mit $\sigma(i) = -i$. Hieraus gewinnen wir alle Automorphismen der Erweiterung $E|\mathbb{Q}$: Die folgende Tabelle zeigt, dass alle 8 Automorphismen in der Liste verschieden sind, weil sie alle unterschiedlich auf der Nullstellenmenge $N = \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$ von $X^4 - 2$ operieren.

id	ρ	ρ^2	ρ^3	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$
$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$
$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$\sqrt[4]{2}$
$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-i\sqrt[4]{2}$
$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$-\sqrt[4]{2}$

Betrachtet man die Menge der Nullstellen als Quadrat in $\mathbb{C}$, so operiert ρ darauf als Drehung um 90 Grad und σ als Spiegelung an einer Diagonalen. Die Gruppe ist also isomorph zur D_4. Dies sieht man aber auch daran, dass $\mathrm{Aut}(E|\mathbb{Q})$ isomorph zu einer 8-elementigen Untergruppe der symmetrischen Gruppe $\mathrm{S}_N \cong \mathrm{S}_4$ ist, welche nach Sylowsatz konjugiert zur D_4 sein muss. Für den Untergruppenverband erhält man:



Diese entsprechen wie folgt den zehn Zwischenkörper von $E|\mathbb{Q}$:



§14B. Separable Erweiterungen

§14Ba. Separable Erweiterungen. Sei K ein Körper und sei C ein algebraischer Abschluss von K. Ein Polynom $P \in K[X]$ heißt *separabel* wenn es in C lauter verschiedene Nullstellen hat, also $P = c(X-a_1)\cdots(X-a_n)$ mit paarweise verschiedenen $a_1,\ldots,a_n \in C$.

Bemerkung 14B1. Die Separabilität von P ist gleichbedeutend mit $\mathrm{ggT}(P,P') = 1$ in $C[X]$ und somit auch $\mathrm{ggT}(P,P') = 1$ in $K[X]$, denn der ggT berechnet sich nach dem euklidischen Algorithmus gänzlich in $K[X]$. Separabilität lässt sich somit bereits über K prüfen und erfordert nicht die Betrachtung eines algebraischen Abschlusses.

Der *Separabilitätsgrad* $\operatorname{sep\,deg} P$ eines Polynoms $P \in K[X]$ ist die Anzahl der verschiedenen Nullstellen von P in C. Ausführlicher: In $C[X]$ gilt $P = (X-a_1)^{m_1}\cdots(X-a_s)^{m_s}$ mit paarweisen verschiedenen Nullstellen $a_1,\ldots,a_s \in C$ von Vielfachheiten $m_1,\ldots,m_s \in \mathbb{N}_{\geq 1}$. Wir setzen $\operatorname{sep\,deg} P := s$.

Offenbar gilt $\operatorname{sep\,deg} P \leq \deg P$, und Gleichheit gilt genau dann, wenn P separabel ist.

Definition 14B2. Sei $E|K$ eine Körpererweiterung. Ein algebraisches Element $a \in E$ heißt *separabel* über K, wenn sein Minimalpolynom $\mathrm{Irr}_K^X(a) \in K[X]$ über K separabel ist, andernfalls heißt a *inseparabel* über K. Eine algebraische Erweiterung $E|K$ heißt *separabel*, wenn jedes Element $a \in E$ separabel über K ist, andernfalls heißt $E|K$ *inseparabel*.

Beispiel 14B3. Jedes Element $a \in K$ ist separabel über K, denn $\mathrm{Irr}_K^X(a) = X - a$.

Bemerkung 14B4. Seien $K < F < E$ Körper. Ist $a \in E$ separabel über K, dann ist a auch separabel über F, denn es gilt $\mathrm{Irr}_F^X(a) \mid \mathrm{Irr}_K^X(a)$ in $F[X]$.

Beispiel 14B5. Sei $p \in \mathbb{N}$ eine Primzahl. In $E = \mathbb{F}_p(T)$ sei $U = T^P$ und $K = \mathbb{F}_p(U)$. Dann ist $E|K$ algebraisch, denn $E = K(T)$ und T ist Nullstelle des Polynoms $P = X^p - U$ in $K[X]$. Dieses ist irreduzibel über K, wie man zum Beispiel mit dem Kriterium von Eisenstein für $\mathbb{F}_p[U]$ sieht. Über E gilt $P = (X-T)^p$, also hat P das Element T als p-fache Nullstelle. Somit ist P nicht separabel und das Element $T \in E$ ist inseparabel über K.

§14Bb. Vollkommene Körper. Die Separabilität von Erweiterungen ist eine wichtige aber etwas technische Bedingung. Wir wollen zunächst die Körper K charakterisieren, über denen jede algebraische Erweiterung $E|K$ separabel ist.

Satz 14B6. *Ein irreduzibles Polynom $P \in K[X]$ ist genau dann separabel, wenn $P' \neq 0$.*

Hieraus ergeben sich, je nach Charakteristik, zwei wichtige Folgerungen:

1. *Über einem Körper K der Charakteristik 0 ist jedes irreduzible Polynom separabel. Folglich ist in Charakteristik 0 jede algebraische Erweiterung separabel.*
2. *Sei K eine Körper der Charakteristik $p > 0$. Für $P \in K[X]$ gilt $P' = 0$ genau dann, wenn $P \in K[X^p]$. Ist $P \in K[X]$ irreduzibel und $P \notin K[X^p]$, dann ist P separabel.*

BEWEIS. Sei $P \in K[X]$ irreduzibel vom Grad n, also

$$P = \sum_{k=0}^{n} a_k X^k$$

mit $n \geq 1$ und $a_n \neq 0$. Das abgeleitete Polynom

$$P' = \sum_{k=1}^{n} k a_k X^{k-1}$$

erfüllt $\deg P' < \deg P$. Wenn P separabel ist, dann gilt $\mathrm{ggT}(P,P') = 1$ nach 4C10, also $P' \neq 0$. Gilt umgekehrt $P' \neq 0$, so erfüllt $Q = \mathrm{ggT}(P,P')$ dann $\deg Q < n$. Dann muss $Q = 1$ gelten, denn andernfalls wäre $Q \mid P$ ein nicht-trivialer Teiler. Also können dann P und P' keine gemeinsamen Nullstellen haben, und somit P ist separabel.

Es gilt $P' = 0$ genau dann, wenn $k a_k = 0$ für alle $k = 0, \ldots, n$.

(1) Im Fall $\mathrm{char}(K) = 0$ gilt stets $P' \neq 0$, sogar $\deg P' = n-1$, denn in K gilt $n a_n \neq 0$.

(2) Im Fall $\mathrm{char}(K) = p$ gilt $P' = 0$ genau dann, wenn $a_k = 0$ für alle $p \nmid k$. □

Definition 14B7. Ein Körper K heißt *vollkommen* wenn jede algebraische Erweiterung $E|K$ separabel ist.

Zum Beispiel ist jeder Körper der Charakteristik 0 vollkommen.

Der Körper $\mathbb{F}_p(U)$ ist nicht vollkommen, wie Beispiel 14B5 zeigt.

Satz 14B8. *Ein Körper K der Charakteristik $p > 0$ ist genau dann vollkommen, wenn der Frobenius-Homomorphismus $\mathfrak{f}_p \colon K \to K$, $x \mapsto x^p$, ein Automorphismus ist.*

Als Körperhomomorphismus ist $\mathfrak{f}_p \colon K \to K$ stets injektiv. Zur Vollkommenheit von K fehlt demnach nur die Surjektivität von $\mathfrak{f}_p$. Die Surjektivität von $\mathfrak{f}_p$ bedeutet, dass jedes Element $a \in K$ eine p-te Wurzel in K hat, also $b \in K$ existiert sodass $b^p = a$. In diesem Fall ist $\mathfrak{f}_p$ bijektiv, das heißt jedes Element in K hat genau eine p-te Wurzel.

BEWEIS. Sei K vollkommen. Für $a \in K$ sei E ein Zerfällungskörper des Polynoms $X^p - a$. Sei $b \in E$ eine Nullstelle, also $b^p - a = 0$. Da $\mathfrak{f}_p$ injektiv ist, ist b eindeutig. Somit gilt $X^p - a = (X-b)^p$. Sei $P = \mathrm{Irr}_K^X(b)$ das Minimalpolynom. Wegen $P \mid X^p - a$ kann P nur die Gestalt $P = (X-b)^k$ mit $1 \leq k \leq p$ haben. Da aber $E|K$ als separabel vorausgesetzt wird, muss $P = (X-b)$ gelten, also $b \in K$. Das bedeutet, $\mathfrak{f}_p$ ist surjektiv.

Sei umgekehrt $\mathfrak{f}_p$ surjektiv. Wir nehmen an, es gäbe ein irreduzibles Polynom $P \in K[X]$ mit $P' = 0$. Es gilt dann $P = \sum_{k=0}^{n} a_k X^{kp}$ mit $a_k \in K$. Für jedes a_k existiert $b_k \in K$ sodass $b_k^p = a_k$. Somit gilt

$$P = \sum_{k=0}^{n} a_k X^{kp} = \sum_{k=0}^{n} (b_k X^k)^p = \Big(\sum_{k=0}^{n} b_k X^k \Big)^p$$

im Widerspruch zu unserer Annahme, dass P in $K[X]$ irreduzibel ist. □

Der Satz zeigt insbesondere, dass jeder endliche Körper vollkommen ist. Das haben wir in Kapitel 13 bereits gesehen, denn $X^{p^n} - X$ über $\mathbb{F}_p$ ist separabel und alle irreduziblen Polynome vom Grad n über $\mathbb{F}_p$ sind Teiler von $X^{p^n} - X$, also selbst separabel.

Der Körper $\mathbb{F}_p(U)$ ist nicht vollkommen, wie wir aus 14B5 wissen. In der Tat ist der Frobenius-Homomorphismus hier injektiv aber nicht surjektiv.

§**14Bc. Separabilitätsgrad.** Wir erinnern an folgenden Sachverhalt:

Lemma 14B9. *Sei $E|K$ eine algebraische Erweiterung und sei $C|K$ ein algebraischer Abschluss. Für $a \in E$ und $b \in C$ sind äquivalent:*

1. *Es gibt einen Homomorphismus $\sigma\colon E \to C$ über K mit $\sigma(a) = b$.*
2. *Es gibt einen Homomorphismus $\sigma\colon K(a) \to K(b)$ über K mit $\sigma(a) = b$.*
3. *Für die Minimalpolynome über K gilt $\operatorname{Irr}^X_K(a) = \operatorname{Irr}^X_K(b)$.*

Sind diese Bedingungen erfüllt, dann nennen wir a und b konjugiert *über K. Demnach hat $a \in E$ genau $\operatorname{sep\,deg} \operatorname{Irr}^X_K(a)$ über K konjugierte Elemente in C.*

BEWEIS. "(1) $\Rightarrow$ (2)" ist klar durch Einschränkung von σ auf $K(a)$. Die Umkehrung "(2) $\Rightarrow$ (1)" folgt aus der Fortsetzung von Körperhomomorphismen (12E15). Die Äquivalenz "(2) $\Leftrightarrow$ (3)" ist die Aussage von Satz 12D6. □

Sei $E|K$ eine endliche Erweiterung und $C|K$ ein algebraischer Abschluss. In Kapitel 12 haben wir gesehen, dass es Körperhomomorphismen $E \to C$ über K gibt. Wir interessieren uns nun für die genaue Anzahl solcher Einbettungen:

Definition 14B10. Der *Separabilitätsgrad* einer endlichen Erweiterung $E|K$ ist die Anzahl der Homomorphismen $E \to C$ in einen algebraischen Abschluss C von K, geschrieben

$$|E : K|_s := |\operatorname{Hom}(E|K, C|K)|$$

Da der algebraische Abschluss $C|K$ bis auf Isomorphie eindeutig ist, hängt diese Zahl nur von $E|K$ ab, nicht aber von der Wahl eines algebraischen Abschlusses $C|K$.

Beispiel 14B11. Für eine einfache algebraische Erweiterung $K(a)|K$ gilt

$$|K(a) : K|_s = \operatorname{sep\,deg} \operatorname{Irr}^X_K(a).$$

Insbesondere gilt $|K(a) : K|_s \leq |K(a) : K|$, und Gleichheit gilt genau dann, wenn das Minimalpolynom $\operatorname{Irr}^X_K(a)$ separabel ist.

Satz 14B12. *Sind $E < F < E$ endliche Erweiterungen, dann gilt*

$$|E : K|_s = |E : F|_s \cdot |F : K|_s .$$

BEWEIS. Sei C ein algebraischer Abschluss von K und $\operatorname{Hom}(F|K, C|K) = \{\sigma_1, \ldots, \sigma_k\}$ mit $k = |F : K|_s$. Für jedes Bild $\sigma_i(F) < C$ ist C ein algebraischer Abschluss. Es gibt genau $\ell = |E : F|_s$ Einbettungen $\sigma_{i,1}, \ldots, \sigma_{i,\ell}\colon E \to C$, die σ_i fortsetzen. Alle $\sigma_{i,j}$ mit $i \in \{1, \ldots, k\}$ und $j \in \{1, \ldots, \ell\}$ sind untereinander verschieden. Umgekehrt ist jede Einbettung $\sigma\colon E \to C$ über K gleich einem $\sigma_{i,j}$, denn $\sigma|_F = \sigma_i$ für ein $i \in \{1, \ldots, k\}$ und somit $\sigma = \sigma_{i,j}$ für ein $j \in \{1, \ldots, \ell\}$. Daraus folgt die Behauptung. □

Korollar 14B13. *Für jede endliche Erweiterung $E|K$ gilt $|E : K|_s \leq |E : K|$.*
Gleichheit $|E : K|_s = |E : K|$ gilt genau dann, wenn $E|K$ separabel ist.

BEWEIS. Wir haben $E = K(a_1, \ldots, a_n)$ für geeignete Elemente $a_1, \ldots, a_n \in E$. Sowohl der Grad (12B16) als auch der Separabilitätsgrad (14B12) sind multiplikativ.

$$K < K(a_1) < K(a_1, a_2) < \ldots < K(a_1, \ldots, a_n) = E$$

Für jeden Erweiterungsschritt gilt nach 14B11

$$|K(a_1, \ldots, a_r, a_{r+1}) : K(a_1, \ldots, a_r)|_s \leq |K(a_1, \ldots, a_r, a_{r+1}) : K(a_1, \ldots, a_r)| .$$

Daraus folgt $|E:K|_s \leq |E:K|$. Sind alle $a_1,\ldots,a_n$ separabel, so gilt in jedem Schritt Gleichheit, also insgesamt $|E:K|_s = |E:K|$. Gilt umgekehrt $|E:K|_s = |E:K|$, dann ist jedes Element $a \in E$ separabel, denn $|K(a):K|_s < |K(a):K|$ und $|E:K(a)|_s \leq |E:K(a)|$ implizieren $|E:K|_s < |E:K|$ dank Multiplikativität. □

Korollar 14B14. *Sei $E|K$ eine algebraische Erweiterung. Enthält die Teilmenge $S \subset E$ nur separable Elemente über K, dann ist der erzeugte Teilkörper $K(S)$ separabel über K.*

BEWEIS. Jedes Element $a \in K(S)$ liegt in einem endlich erzeugten Teilkörper $K(a_1,\ldots,a_n)$ mit $a_1,\ldots,a_n \in S$. Jeder solche Körper ist nach 14B13 separabel. □

Definition 14B15. Sei $K^a|K$ ein algebraischer Abschluss von K und sei

$$S = \{\, a \in K^a \mid a \text{ ist separabel über } K \,\}$$

die Menge der separablen Elemente über K. Dann ist $K^s := K(S)$ die größte algebraische, separable Erweiterung, genannt *separabler Abschluss* von K in K^a.

§**14Bd. Satz vom primitiven Element.** Sei $E|K$ eine endliche Erweiterung. Wir nennen $a \in E$ ein *primitives Element* über K, wenn $E = K(a)$ gilt.

Satz 14B16 (Steinitz)**.** *Sei $E|K$ eine endliche Erweiterung. Genau dann existiert ein primitives Element $a \in E$, wenn $E|K$ nur endlich viele Zwischenkörper besitzt.*

BEWEIS. Wenn der Körper K endlich ist, dann ist auch E endlich. Wir wissen bereits, dass für jeden endlichen Körper E ein primitives Element $a \in E$ über K existiert (zum Beispiel eine Primitivwurzel $a \in E^\times$ mit $E^\times = \langle a \rangle$). Ebenso hat ein endlicher Körper offenbar nur endlich viele Teilkörper. Wir können im Folgenden also K als unendlich annehmen.

Angenommen $E|K$ hat nur endlich viele Zwischenkörper. Wir wollen zeigen, dass für jeden Zwischenkörper $F = K(a,b)$ mit $a,b \in E$ ein primitives Element $c \in F$ existiert, sodass $F = K(c)$. Hierzu betrachten wir die Abbildung $x \mapsto K(a+bx)$ für $x \in K$. Da K unendlich ist, aber $E|K$ nur endlich viele Zwischenkörper besitzt, gibt es $x_1 \neq x_2$ in K mit $K(a+bx_1) = K(a+bx_2)$. Wir wählen $c = a+bx_1$. Offenbar gilt $K(c) < K(a,b)$. Da $a+bx_1$ und $a+bx_2$ in $K(c)$ liegen, gilt dies auch für $b(x_1-x_2)$. Aus $x_1-x_2 \in K^\times$ erhalten wir $b \in K(c)$ und damit $a \in K(c)$. Hieraus schließen wir $K(a,b) < K(c)$, also $K(a,b) = K(c)$.

Da $E|K$ endlich ist, existieren Elemente $a_1,\ldots,a_n \in E$ sodass $E = K(a_1,\ldots,a_n)$. Per Induktion zeigen wir, dass es $b_k \in K(a_1,\ldots,a_k)$ gibt sodass $K(b_k) = K(a_1,\ldots,a_k)$. Für $n = 1$ können wir $b_1 = a_1$ wählen. Gilt $K(b_k) = K(a_1,\ldots,a_k)$, dann

$$K(a_1,\ldots,a_k,a_{k+1}) = K(a_1,\ldots,a_k)(a_{k+1}) = K(b_k)(a_{k+1}) = K(b_k,a_{k+1}) = K(b_{k+1})$$

für ein geeignetes Element $b_{k+1} \in K(b_k,a_{k+1})$ wie vorher gesehen. Also $E = K(b_n)$.

Nehmen wir umgekehrt an, es gelte $E = K(a)$ für ein $a \in E$. Für jeden Zwischenkörper F mit $K < F < E$ betrachten wir das Minimalpolynom

$$P_F = \operatorname{Irr}_F^X(a) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$$

und den Teilkörper $F' = K(a_1,\ldots,a_{n-1},a_n)$. Dann ist $P_F \in F'[X]$ irreduzibel über F' denn es ist sogar irreduzibel über $F > F'$. Also ist $|F'(a):F'| = |F(a):F| = n$. Wegen $E = F(a) = F'(a)$ folgt aus der Gradformel $|E:F'| = |E:F| \cdot |F:F'|$ dann $|F:F'| = 1$ und somit $F = F'$.

Das bedeutet, die Abbildung $F \mapsto P_F \in E[X]$ ist injektiv, und aus $K < F$ folgt $P_F \mid P_K$. Dank der eindeutigen Primfaktorzerlegung in $E[X]$ hat P_K nur endlich viele normierte Teiler, also kann es nur endlich viele Zwischenkörper $K < F < E$ geben. □

Man kann sich fragen, wie eine endliche Körpererweiterung $E|K$ aussieht, die unendlich viele Zwischenkörper F mit $K < F < E$ erlaubt. Hier ein einfaches Beispiel:

Übung 14B17. Sei $p \in \mathbb{N}$ eine Primzahl. Über dem Körper $\mathbb{F}_p$ der Ordnung p betrachten wir den Polynomring $\mathbb{F}_p[X,Y]$ in zwei Unbestimmten X,Y und den zugehörigen Bruchkörper $E = \mathbb{F}_p(X,Y)$. Hierin ist $K = \mathbb{F}_p(X^p,Y^p)$ ein Teilkörper und es gilt $|E:K| = p^2$. Die Erweiterung $E|K$ erlaubt kein primitives Element aber eine unendliche Anzahl von Zwischenkörpern F mit $K < F < E$.

Satz 14B18. *Ist $E|K$ endlich und separabel, dann existiert ein primitives Element $a \in E$.*

BEWEIS. Wenn der Körper K endlich ist, dann ist auch E endlich. Wir wissen bereits, dass für jeden endlichen Körper E ein primitives Element $a \in E$ über K existiert (zum Beispiel eine Primitivwurzel $a \in E^\times$ mit $E^\times = \langle a \rangle$). Wir können im Folgenden also K als unendlich annehmen.

Da die Erweiterung $E|K$ endlich ist, existieren Elemente $a_0, a_1, \ldots, a_r \in E$ sodass $E = K(a_0, a_1, \ldots, a_r)$. Sei $n = |E:K|$. Da $E|K$ separabel ist existieren n verschiedene Einbettungen $\sigma_1, \ldots, \sigma_n \colon E \to C$ in einen algebraischen Abschluss C von K. In $C[X]$ definieren wir

$$Q_i = \sigma_i(a_0) + \sigma_i(a_1)X + \cdots + \sigma_i(a_r)X^r.$$

Für $i \neq j$ gilt $Q_i \neq Q_j$, denn andernfalls wäre $\sigma_i(a_0) = \sigma_j(a_0)$, $\sigma_i(a_1) = \sigma_j(a_1)$, …, $\sigma_i(a_r) = \sigma_j(a_r)$ und somit $\sigma_i = \sigma_j$. Somit ist in $C[X]$ das Produkt

$$P = \prod_{i \neq j} (Q_i - Q_j)$$

nicht Null. Da K unendlich ist, existiert $x \in K$ mit $P(x) \neq 0$. Also sind die Elemente

$$Q_i(x) = \sigma_i(a_0) + \sigma_i(a_1)x + \cdots + \sigma_i(a_r)x^r$$

in E paarweise verschieden für $i = 1, \ldots, n$. Somit hat $a = a_0 + a_1 x + \cdots + a_r x^r$ mindestens n konjugierte Elemente in C, also $\deg \operatorname{Irr}_K^X(a) \geq n$, also $|K(a):K| \geq n$. Wegen $K(a) < E$ und $|E:K| = n$ schließen wir $E = K(a)$. □

Übung 14B19. Sei $E|K$ eine endliche Körpererweiterung. Zur Existenz eines primitiven Elements ist die Separabilität von $E|K$ hinreichend. Ist sie auch notwendig?

§14C. Normale Erweiterungen

§14Ca. Normale Erweiterungen.

Satz 14C1. *Sei $C|K$ ein algebraischer Abschluss und $K < E < C$. Dann sind äquivalent:*

1. *Für jeden Homomorphismus $\sigma \colon E \to C$ über K gilt $\sigma(E) = E$.*
2. *Zu jedem Element $a \in E$ enthält E auch alle Konjugierten von a in C über K.*
3. *Hat ein irreduzibles Polynom $P \in K[X]$ eine Nullstelle in E, so zerfällt es über E.*
4. *E ist der Zerfällungskörper einer Menge $\mathcal{P} \subset K[X]$ von Polynomen über K.*

Sind diese Bedingungen erfüllt, dann nennen wir die Erweiterung $E|K$ normal.

BEWEIS. "(1) $\Rightarrow$ (2)" Folgt aus 14B9: Ist $a \in E$ konjugiert zu $b \in C$ über K, dann existiert $\sigma\colon E \to C$ mit $\sigma(a) = b$. Wegen $\sigma(E) = E$ gilt $b \in E$.

"(2) $\Rightarrow$ (3)" Ist $P \in K[X]$ irreduzibel und $P(a) = 0$ mit $a \in E$, dann ist jede Nullstelle $b \in C$ mit $P(b) = 0$ zu a konjugiert über K. Wegen (2) gilt also $b \in E$. Das Polynom P zerfällt somit über E.

"(3) $\Rightarrow$ (4)" Sei $\mathcal{P} = \{\, \operatorname{Irr}_K^X(a) \mid a \in E \,\}$. Wegen (3) ist E der Zerfällungskörper von $\mathcal{P}$ über K.

"(4) $\Rightarrow$ (1)" Sei $\mathcal{P} \subset K[X]$ und $S = \{\, a \in E \mid P(a) = 0 \text{ für ein } P \in \mathcal{P} \,\}$, sodass $E = K(S)$. Jeder Homomorphismus $\sigma\colon E \to C$ ist injektiv. Für jedes $P \in \mathcal{P}$ wird die endliche Menge $\{\, a \in E \mid P(a) = 0 \,\}$ auf sich selbst abgebildet, also ist σ hierauf auf surjektiv. Aus $\sigma(S) = S$ folgt $\sigma(K(S)) = K(\sigma(S)) = K(S)$. □

§14Cb. Charakterisierung von Galois-Erweiterungen.

Lemma 14C2. *Sei E ein Körper und $G < \operatorname{Aut}(E)$ eine Gruppe von Automorphismen von E. Sei $K = \operatorname{Fix}(G) < E$ der Fixkörper von G. Für ein $a \in E$ sei $Ga = \{a_1, \ldots, a_n\}$ eine Bahn endlicher Länge n. Dann ist a algebraisch über K mit separablem Minimalpolynom*

$$P = \prod_{i=1}^{n} (X - a_i).$$

BEWEIS. Jeder Körperautomorphismus $\tau\colon E \to E$ setzt sich fort zu einem Ringautomorphismus $\tau\colon E[X] \to E[X]$ gemäß $\tau(\sum c_i X^i) = \sum \tau(c_i) X^i$. Für alle $g \in G$ gilt somit

$$g(P) = \prod_{i=1}^{n} (X - g(a_i)) = \prod_{i=1}^{n} (X - a_i) = P,$$

denn g permutiert die Elemente der Bahn $Ga = \{a_1, \ldots, a_n\}$. Wegen $g(P) = P$ für alle $g \in G$ liegen die Koeffizienten von P im Fixkörper K. Nach Konstruktion ist P normiert und separabel. Sei $Q = \operatorname{Irr}_K^X(a)$ das Minimalpolynom von a über K. Es gilt $Q \mid P$. Da jedes $g \in G$ den Körper K festlässt folgt aus $Q(a) = 0$ dann auch $Q(g(a)) = g(Q(a)) = g(0) = 0$, also hat Q mindestens die n verschiedenen Nullstellen $a_1, \ldots, a_n$, und somit $Q = P$. □

Satz 14C3. *Für jede algebraische Körpererweiterung $E|K$ sind äquivalent:*

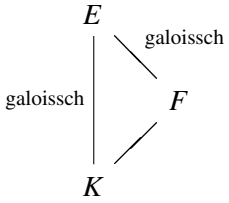
1. *$E|K$ ist galoissch.*
2. *$E|K$ ist normal und separabel.*

BEWEIS. "(1) $\Rightarrow$ (2)" Wir setzen $\operatorname{Fix}(\operatorname{Aut}(E|K)) = K$ voraus. Für $a \in E$ ist zu zeigen, dass $P = \operatorname{Irr}_K^X(a)$ separabel ist und über E zerfällt. Dies folgt mit $G = \operatorname{Aut}(E|K)$ aus 14C2: Die Bahn Ga ist endlich, denn für alle $g \in G$ gilt $P(g(a)) = 0$.

"(2) $\Rightarrow$ (1)" Für $a \in E$ mit $a \notin K$ ist zu zeigen, dass es ein $g \in \operatorname{Aut}(E|K)$ gibt mit $g(a) \neq a$. Sei C ein algebraischer Abschluss von E. Nach Voraussetzung ist a separabel über K, also $|K(a) : K|_s = |K(a) : K| > 1$. Es existiert ein Homomorphismus $h\colon K(a) \to C$ über K mit $h(a) \neq a$. Dieser setzt sich zu $g\colon E \to C$ fort mit $g|_{K(a)} = h$, also $g(a) \neq a$. Nach Voraussetzung ist $E|K$ normal, also gilt $g(E) = E$. Damit ist $g \in \operatorname{Aut}(E|K)$. □

Korollar 14C4. *Sei $E|K$ eine Galois-Erweiterung. Dann ist für jeden Zwischenkörper F mit $K < F < E$ die Erweiterung $E|F$ ebenfalls galoissch.*

Als Diagramm drückt sich dieser Sachverhalt wie folgt aus. Man beachte, dass die Erweiterung $F|K$ nicht unbedingt galoissch ist, hierzu anschließend mehr.



BEWEIS. Nach Voraussetzung ist $E|K$ galoissch, also 14C3 separabel und normal. Dann ist auch $E|F$ separabel und normal, nach 14C3 also galoissch. □

Bemerkung 14C5. Die Zuordnung $F \mapsto \mathrm{Aut}(E|F))$ von der Menge der Zwischenkörper von $E|K$ in die Menge der Untergruppen von $\mathrm{Aut}(E|K)$ ist demnach injektiv, denn nach dem Korollar gilt $F = \mathrm{Fix}(\mathrm{Aut}(E|F))$. Man beachte, dass wir hierbei die Erweiterung $E|K$ zwar als algebraisch voraussetzen, nicht aber als endlich.

§14Cc. Normale Zwischenkörper.

Satz 14C6. *Sei $E|K$ eine Galois-Erweiterung und F ein Zwischenkörper, $K < F < E$. Für jeden Automorphismus $g \in \mathrm{Aut}(E|K)$ gilt*

$$\mathrm{Aut}(E|g(F)) = g \cdot \mathrm{Aut}(E|F) \cdot g^{-1}.$$

Die folgenden Aussagen sind daher äquivalent:

1. *Die Erweiterung $F|K$ ist normal.*
2. *Es gilt $g(F) = F$ für alle $g \in \mathrm{Aut}(E|K)$.*
3. *Die Untergruppe $\mathrm{Aut}(E|F) < \mathrm{Aut}(E|K)$ ist normal.*

In diesem Fall erhalten wir einen surjektiven Gruppenhomomorphismus $\mathrm{Aut}(E|K) \to \mathrm{Aut}(F|K)$ durch die Einschränkung $g \mapsto g|_F$, mit Kern $\mathrm{Aut}(E|F)$.

Dies fassen wir prägnant zusammen durch die kurze exakte Sequenz

$$\mathrm{Aut}(E|F) \hookrightarrow \mathrm{Aut}(E|K) \twoheadrightarrow \mathrm{Aut}(F|K)$$

oder als Quotienten

$$\mathrm{Aut}(F|K) \cong \mathrm{Aut}(E|K)/\mathrm{Aut}(E|F).$$

BEWEIS. Für alle $h \in \mathrm{Aut}(E|K)$ gilt

$$\begin{aligned}
h \in \mathrm{Aut}(E|g(F)) \quad &\Leftrightarrow \quad h(g(a)) = g(a) \quad \text{für alle } a \in F \\
&\Leftrightarrow \quad (g^{-1}hg)(a) = a \quad \text{für alle } a \in F \\
&\Leftrightarrow \quad g^{-1}hg \in \mathrm{Aut}(E|F) \\
&\Leftrightarrow \quad h \in g\,\mathrm{Aut}(E|F)g^{-1}
\end{aligned}$$

Die Äquivalenz "(2) $\Leftrightarrow$ (3)" folgt hieraus mit 14C4:

$$g(F) = F \qquad \Leftrightarrow \qquad \mathrm{Aut}(E|F) = \mathrm{Aut}(E|g(F)) = g \cdot \mathrm{Aut}(E|F) \cdot g^{-1}.$$

Sei C ein algebraischer Abschluss von E (und damit auch von F und K).

"(1) $\Rightarrow$ (2)" Ist $F|K$ normal, dann gilt $h(F) = F$ für jede Einbettung $h\colon F \to C$ über K. Für alle $g \in \mathrm{Aut}(E|K)$ ist $g|_F\colon F \to C$ solch eine Einbettung, also $g(F) = F$.

"(2) $\Rightarrow$ (1)" Jede Einbettung $h\colon F \to C$ setzt sich fort zu einer Einbettung $g\colon E \to C$ mit $g|_F = h$. (§12Ed). Da E normal ist, gilt $g(E) = E$, also $g \in \mathrm{Aut}(E|K)$. Mit Voraussetzung (2) folgt nun $g(F) = h(F) = F$. □

§14Cd. Satz von Artin.

Lemma 14C7. *Für jede endliche Erweiterung $E|K$ gilt $|\mathrm{Aut}(E|K)| \leq |E:K|$, und $E|K$ ist genau dann galoissch, wenn $|\mathrm{Aut}(E|K)| = |E:K|$ gilt*

BEWEIS. Sei C ein algebraischer Abschluss von E. Es gilt $\mathrm{Aut}(E|K) \subset \mathrm{Hom}(E|K,C|K)$ und $|\mathrm{Hom}(E|K,C|K)| = |E:K|_s \leq |E:K|$, also insgesamt

$$|\mathrm{Aut}(E|K)| \leq |\mathrm{Hom}(E|K,C|K)| = |E:K|_s \leq |E:K|\,.$$

Hierbei ist $\mathrm{Aut}(E|K) = \mathrm{Hom}(E|K,C|K)$ gleichbedeutend damit, dass $E|K$ normal ist, und $|E:K|_s = |E:K|$ ist gleichbedeutend damit, dass $E|K$ separabel ist. Gilt beides, dann folgt

$$|\mathrm{Aut}(E|K)| = |\mathrm{Hom}(E|K,C|K)| = |E:K|_s = |E:K|\,.$$

Gilt umgekehrt $|\mathrm{Aut}(E|K)| = |E:K|$, dann wird die obige doppelte Ungleichung zu einer Gleichung und es folgt $\mathrm{Aut}(E|K) = \mathrm{Hom}(E|K,C|K)$ sowie $|E:K|_s = |E:K|$, also ist $E|K$ normal und separabel, nach 14C3 also galoissch. □

Satz 14C8 (Artin)**.** *Sei E ein Körper und sei $G < \mathrm{Aut}(E)$ eine endliche Gruppe von Körperautomorphismen. Über dem Fixkörper $F = \mathrm{Fix}(G)$ ist dann $E|F$ eine endliche Galois-Erweiterung vom Grad $|E:F| = |G|$ mit Automorphismengruppe $\mathrm{Aut}(E|F) = G$.*

BEWEIS. Nach 14C2 ist $E|F$ algebraisch, separabel und normal, und somit galoissch (14C3). Nach 14C2 gilt $|F(a):F| \leq |G|$ für alle $a \in E$. Es gibt also ein $a \in E$ sodass $|F(a):F|$ maximal ist. Für alle $b \in E$ gilt $F(a,b) = F(c)$ Nach dem Satz 14B18 vom primitiven Element. Es gilt $F(a) < F(c)$ und wegen $|F(a):F| = |F(c):F|$ dann $F(a) = F(c)$. Somit ist $E = F(a)$. Insbesondere ist $E|F$ endlich und $|E:F| \leq |G|$. Offenbar ist $G < \mathrm{Aut}(E|F)$, also $|G| \leq |\mathrm{Aut}(E|F)|$. Nach 14C7 gilt aber $|E:F| = |\mathrm{Aut}(E|F)|$. Aus

$$|G| \leq |\mathrm{Aut}(E|F)| = |E:F| \leq |G|$$

folgt also $|E:F| = |G|$ und $G = \mathrm{Aut}(E|F)$. □

Korollar 14C9. *Sei $E|K$ eine endliche Galois-Erweiterung. Dann ist für jede Untergruppe $G < \mathrm{Aut}(E|K)$ und $F = \mathrm{Fix}(G)$ die Erweiterung $E|F$ galoissch mit $\mathrm{Aut}(E|F) = G$.* □

Für jede endliche Galois-Erweiterung $E|K$ ist damit die Galois-Korrespondenz zwischen den Zwischenkörpern $K < F < E$ und den Untergruppen $G < \mathrm{Aut}(E|K)$ bewiesen: Korollar 14C9 besagt $\mathrm{Aut}(E|\mathrm{Fix}(G)) = G$, und Korollar 14C4 besagt $\mathrm{Fix}(\mathrm{Aut}(E|F)) = F$.

§**14Ce. Normale Hülle.** Sei $E|K$ eine algebraische Erweiterung und sei C ein algebraischer Abschluss von E (und damit auch von K). Sei

$$S = \{\, b \in C \mid b \text{ ist zu einem } a \in E \text{ über } K \text{ konjugiert} \,\}.$$

Dann ist $\bar{E} := K(S)$ eine normale Erweiterung über K, und zwar die kleinste die E enthält. Daher nennen wir $\bar{E}$ die *normale Hülle* von E über K.

Proposition 14C10. *Ist $E|K$ separabel, dann ist $\bar{E}|K$ galoissch.*

BEWEIS. Nach Konstruktion ist $\bar{E}|K$ normal über K, es bleibt nur zu zeigen, dass $\bar{E}|K$ auch separabel über K ist. Nach Voraussetzung ist $E|K$ separabel, also enthält S als konjugierte nur separable Elemente, und nach 14B14 ist dann $\bar{E} = K(S)$ separabel über K. □

Wenn die Erweiterung $E|K$ nicht separabel ist, dann kann man durch Adjunktion weiterer Elemente dieses Manko nicht beheben (höchstens verschlimmern). Für die Normalität ist dies möglich: Durch Adjunktion aller konjugierten Elemente erhält man die normale Hülle $\bar{E}|K$, und die Proposition besagt, dass man die Separabilität dabei nicht beschädigt.

Proposition 14C11. *Sei $C|K$ ein algebraischer Abschluss. Sei $S \subset C$ und*

$$\bar{S} = \{\, b \in C \mid b \text{ ist zu einem } a \in S \text{ über } K \text{ konjugiert} \,\}.$$

Dann ist $K(\bar{S})$ die normale Hülle von $K(S)$ über K.

BEWEIS. Offenbar ist $K(\bar{S})$ in der normalen Hülle von $K(S)$ über K enthalten. Es genügt also zu zeigen, dass $K(\bar{S})$ normal über K ist. Für jede Einbettung $\sigma\colon K(\bar{S}) \to C$ über K gilt $\sigma(\bar{S}) = \bar{S}$, also $\sigma(K(\bar{S})) = K(\bar{S})$. □

§14D. Galois-Gruppe einer Gleichung

Ist $E|K$ eine endliche Galois-Erweiterung, dann ist E Zerfällungskörper eines irreduziblen Polynoms über K: Da $E|K$ separabel ist existiert nach 14B18 ein primitives Element $a \in E$ sodass $E = K(a)$. Da $E|K$ normal ist, enthält E alle Nullstellen des Minimalpolynoms $\mathrm{Irr}_K^X(a)$, und damit ist E Zerfällunsgkörper von $\mathrm{Irr}_K^X(a)$.

Nach 14B14 gilt umgekehrt: Ist $P \in K[X]$ separabel, dann ist der Zerfällungskörper E über K eine endliche Galois-Erweiterung. Wir kommen damit zu folgender Begriffsbildung, die auf die ursprüngliche Betrachtung Galois zurückgeht:

Definition 14D1. Sei $P \in K[X]$ ein separables Polynom (oder zumindest sei jeder Primfaktor von P separabel). Sei E der Zerfällungskörper von P über K. Die Galois-Gruppe $\mathrm{Aut}(E|K)$ nennt man dann auch die Galois-Gruppe von P über K, geschrieben

$$\mathrm{Gal}(P|K) = \mathrm{Aut}(E|K).$$

§**14Da. Operation auf der Nullstellenmenge.** Sei $P \in K[X]$ ein Polynom wie oben und $\mathrm{Gal}(P|K) = \mathrm{Aut}(E|K)$ seine Galois-Gruppe. Für die Nullstellenmenge

$$N = N(P) := \{\, a \in E \mid P(a) = 0 \,\}$$

gilt $g(N) = N$ für alle $g \in \mathrm{Gal}(P|K)$, denn aus $P(a) = 0$ folgt $P(g(a)) = g(P(a)) = g(0) = 0$. Jeder Körperhomomorphismus g ist injektiv, und da die Menge N endlich ist, folgt aus der Injektivität die Surjektivität, $g(N) = N$, also ist $g|_N\colon N \xrightarrow{\sim} N$ eine Permutation.

Proposition 14D2. *Für jedes separable Polynom $P \in K[X]$ erhalten wir einen injektiven Gruppenhomomorphismus* $\mathrm{Gal}(P|K) \to \mathrm{S}_N$ *durch die Einschränkung $g \mapsto g|_N$ auf die Nullstellenmenge $N = N(P)$. Insbesondere gilt für den Zerfällungskörper E von P über K die Beschränkung $|E:K| \leq n!$, wobei $n = |N|$ der Grad von P ist.* □

BEWEIS. Nach Konstruktion ist die Erweiterung $E|K$ separabel und normal, also galoissch. Die Einschränkung $\mathrm{Gal}(P|K) \to \mathrm{S}_N$, $g \mapsto g|_N$, ist ein Gruppenhomomorphismus. Wegen $E = K(N)$ ist dieser injektiv: Wenn $g|_N = h|_N$, dann gilt $g = h$ auf ganz $E = K(N)$. Es gilt $|E:K| = |\mathrm{Gal}(P|K)|$, und wegen $\mathrm{Gal}(P|K) \hookrightarrow \mathrm{S}_N$ gilt $|\mathrm{Gal}(P|K)| \leq |\mathrm{S}_N| = n!$. □

Wir können uns jede endliche Galois-Gruppe als Gruppe eines (separablen) Polynoms P vorstellen, und somit als Permutationsgruppe auf der Nullstellenmenge von P. Die untenstehenden Beispiele zeigen, dass $\mathrm{Gal}(P|K) \cong \mathrm{S}_N$ durchaus möglich ist, also die obere Grenze $n!$ angenommen werden kann. Umgekehrt gilt für $P = (X-a_1)\cdots(X-a_n)$ mit $a_1,\dots,a_n \in K$ offenbar $E = K$ und somit $\mathrm{Gal}(P|K) = \{\mathrm{id}\}$. Im Allgemeinen werden die Wurzeln jedoch nicht-trivial permutiert, und zwar nach folgendem Muster:

Satz 14D3. *Sei $P = P_1^{m_1}\cdots P_r^{m_r}$ die Primfaktorzerlegung von P in $K[X]$, wobei wir $P_1,\dots,P_r$ als separabel annehmen. Sei E ein Zerfällungskörper von P über K. Unter der Operation der Galois-Gruppe* $\mathrm{Gal}(P|K)$ *hat die Nullstellenmenge die Bahnenzerlegung*

$$N(P) = N(P_1) \sqcup \cdots \sqcup N(P_r).$$

Insbesondere ist ein separables Polynom $P \in K[X]$ genau dann irreduzibel über K, wenn seine Galois-Gruppe $\mathrm{Gal}(P|K)$ *transitiv auf der Nullstellenmenge $N(P)$ operiert, das heißt für alle $a,b \in N(P)$ existiert ein $g \in \mathrm{Gal}(P|K)$ mit $g(a) = b$.*

BEWEIS. Wir nehmen $P, P_1, \dots, P_r$ als normiert an, also $\mathrm{lc}\,P = \mathrm{lc}\,P_1 = \cdots = \mathrm{lc}\,P_r = 1$. Es sei $N = N(P)$ und $N_k = N(P_k)$ für $k = 1,\dots,r$. Offenbar gilt $N = N_1 \cup \cdots \cup N_r$, und da die Polynome $P_1,\dots,P_r$ irreduzibel und paarweise verschieden sind gilt $N_i \cap N_j = \emptyset$ für $i \neq j$. Da die Polynome $P_1,\dots,P_r$ separabel sind, ist $E = K(N)$ separabel und nach Konstruktion normal, also galoissch.

Sei $a \in N_k$ und $g \in \mathrm{Gal}(P|K)$. Aus $P_k(a) = 0$ folgt $P_k(g(a)) = g(P_k(a)) = g(0) = 0$, also $g(N_k) \subset N_k$. Da P_k irreduzibel ist, dann gilt $\mathrm{Irr}_K^X(a) = P_k$ für alle $a \in N_k$. Zu jedem Paar $a,b \in N_k$ existiert demnach ein Homomorphismus $h\colon K(a) \to K(b)$ über K mit $h(a) = b$. Ist C ein algebraischer Abschluss von E, dann wird $h\colon K(a) \to K(b)$ komponiert mit der Inklusion $K(b) \hookrightarrow C$ zum Homomorphismus $h\colon K(a) \to C$. Dieser setzt sich fort zu $g\colon E \to C$ mit $g|_{K(a)} = h$, also $g|_K = \mathrm{id}_K$ und $g(a) = b$. Da $E|K$ normal ist, gilt $g(E) = E$ also $g \in \mathrm{Aut}(E|K)$. Somit ist jedes N_k eine Bahn von N unter der Aktion von $\mathrm{Gal}(P|K)$. □

Beispiel 14D4. Die folgenden Beispiele aus §14Ac illustrieren die Operation der Galois-Gruppe $\mathrm{Gal}(P|K)$ auf der Nullstellenmenge $N(P)$.

- $\mathrm{Aut}(\mathbb{C}|\mathbb{R}) = \mathrm{Gal}(X^2+1|\mathbb{Q}) \hookrightarrow \mathrm{S}_N$ mit $N = \{i,-i\}$.
- $\mathrm{Aut}(\mathbb{Q}[\sqrt{2}]|\mathbb{Q}) = \mathrm{Gal}(X^2-2|\mathbb{Q}) \hookrightarrow \mathrm{S}_N$ mit $N = \{\sqrt{2},-\sqrt{2}\}$.
- $\mathrm{Aut}(\mathbb{Q}[\sqrt{2},\sqrt{3}]|\mathbb{Q}) = \mathrm{Gal}((X^2-2)(X^2-3)|\mathbb{Q}) \hookrightarrow \mathrm{S}_N$ mit $N = \{\pm\sqrt{2},\pm\sqrt{3}\}$. Das Bild ist hierbei eine Untergruppe der Ordnung 4 isomorph zu $\mathbb{Z}/2 \times \mathbb{Z}/2$.
- $\mathrm{Aut}(\mathbb{Q}[j,\sqrt[3]{2}]|\mathbb{Q}) = \mathrm{Gal}(X^3-2|\mathbb{Q}) \hookrightarrow \mathrm{S}_N$ mit $N = \{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\}$. Wegen $|\mathbb{Q}[j,\sqrt[3]{2}]|\mathbb{Q}| = 6$ ist dies ein Isomorphismus, somit $\mathrm{Aut}(\mathbb{Q}[j,\sqrt[3]{2}]|\mathbb{Q}) \cong \mathrm{S}_3$.

- $\mathrm{Aut}(\mathbb{Q}[i,\sqrt[4]{2}]|\mathbb{Q}) = \mathrm{Gal}(X^4-2|\mathbb{Q}) \hookrightarrow \mathrm{S}_N$ mit $N = \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$.
  Wegen $|\mathbb{Q}[i,\sqrt[4]{2}]|\mathbb{Q}| = 8$ stiftet dies einen Isomorphismus $\mathrm{Aut}(\mathbb{Q}[i,\sqrt[4]{2}]|\mathbb{Q}) \cong D_4$.

§**14Db. Ein Kriterium für** $\mathrm{Gal}(P|\mathbb{Q}) = \mathrm{S}_p$**.** Wir beginnen mit einem Beispiel:

Beispiel 14D5. Das Polynom $P = X^5 - 4X + 2$ über $\mathbb{Q}$ ist irreduzibel nach Eisenstein. Der Graph von P zeigt, dass P genau drei reelle Nullstellen hat und somit zwei komplex-konjugierte Nullstellen. Sei $N = \{\, a \in \mathbb{C} \mid P(a) = 0 \,\}$ die Nullstellenmenge und $E = \mathbb{Q}(N)$ der Zerfällungskörper von P über $\mathbb{Q}$. Nach dem folgenden Kriterium ist $\mathrm{Aut}(E|\mathbb{Q}) = \mathrm{Gal}(P|\mathbb{Q})$ isomorph zur symmetrischen Gruppe S_5 aller Permutationen von N.

Satz 14D6. *Sei $P \in \mathbb{Q}[X]$ ein irreduzibles Polynom von Primzahlgrad $\deg P = p$ das $p-2$ reelle Nullstellen hat sowie zwei komplex-konjugierte Nullstellen. Dann ist $\mathrm{Gal}(P|\mathbb{Q}) \cong \mathrm{S}_p$ isomorph zur symmetrischen Gruppe auf den Nullstellen von P.*

BEWEIS. Wir können P als normiert annehmen, also $\mathrm{lc}\, P = 1$. Sei $N = \{\, a \in \mathbb{C} \mid P(a) = 0 \,\}$ die Nullstellenmenge von P und sei $E = \mathbb{Q}(N)$ der Zerfällungskörper von P über $\mathbb{Q}$. Für $P(a) = 0$ gilt $|\mathbb{Q}(a) : \mathbb{Q}| = p$, denn $\mathrm{Irr}_K^X(a) = P$. Wegen $|E : \mathbb{Q}| = |E : \mathbb{Q}(a)| \cdot |\mathbb{Q}(a) : \mathbb{Q}|$ teilt p den Grad $|E : \mathbb{Q}|$ und somit die Ordnung $|\mathrm{Aut}(E|\mathbb{Q})|$.

Sei G das Bild des injektiven Gruppenhomomorphismus $\mathrm{Aut}(E|\mathbb{Q}) \hookrightarrow \mathrm{S}_N$. Nach dem Satz von Cauchy (11A1) existiert ein Element $g \in \mathrm{Aut}(E|K)$ der Ordnung p. Die Einschränkung $\rho = g|_N$ ist ein p-Zykel in $G < \mathrm{S}_N$. Die Konjugation $\mathrm{conj}\colon \mathbb{C} \to \mathbb{C}$ induziert eine Transposition $\tau = \mathrm{conj}\,|_N$ auf N, denn $p-2$ Nullstellen bleiben fest und die zwei komplex-konjugierten werden vertauscht. Es gilt damit $G \supset \langle \rho, \tau \rangle = \mathrm{S}_N$, also $G = \mathrm{S}_N$. □

Man beachte, dass dieser Satz für beliebigen Grad nicht gilt: Zum Beispiel hat $X^4 - 2$ zwei reelle Nullstellen $\pm\sqrt[4]{2}$ und zwei komplex-konjugierte Nullstellen $\pm i\sqrt[4]{2}$. Nach 14A10 ist die Galois-Gruppe $\mathrm{Gal}(X^4-2|\mathbb{Q})$ jedoch nicht S_4 sondern D_4.

§**14Dc. Das Umkehrproblem der Galois-Theorie.** Wir halten zunächst als einfache Beobachtung fest, dass jede endliche Gruppe als Galois-Gruppe auftreten kann:

Proposition 14D7. *Für jede endliche Gruppe G existiert ein Körper K und eine endliche Galois-Erweiterung $E|K$ sodass $\mathrm{Aut}(E|K) \cong G$.*

BEWEIS. Nach dem Satz von Cayley können wir G als Untergruppe einer symmetrischen Gruppe S_n realisieren. Wir können daher $G \subset \mathrm{S}_n$ annehmen. Sei $\mathbb{Q}[X_1, \ldots, X_n]$ der Polynomring in den Unbestimmten $X_1, \ldots, X_n$ über $\mathbb{Q}$. Hierauf operiert die symmetrische Gruppe S_n durch Vertauschung der Variablen gemäß $\sigma(X_n) = X_{\sigma(n)}$. Diese Operation setzt sich auf den Bruchkörper $E = \mathbb{Q}(X_1, \ldots, X_n)$ fort. Wir erhalten so einen injektiven Gruppenhomomorphismus $h\colon \mathrm{S}_n \to \mathrm{Aut}(E)$. Sei $\bar{G} = h(G)$ die von G induzierte Gruppe von Automorphismen von E. Sei $K = \mathrm{Fix}(\bar{G})$ der Fixkörper. Nach dem Satz von Artin ist $E|K$ eine Galois-Erweiterung mit $\mathrm{Aut}(E|K) = \bar{G} \cong G$. □

In der vorhergehenden Konstruktion haben wir den Grundkörper K der Gruppe G angepasst. Es wäre noch schöner, wenn wir jede endliche Gruppe G als Galois-Gruppe *über* $\mathbb{Q}$ realisieren könnten. Dieses Problem ist jedoch ungleich schwerer:

Frage 14D8 (Umkehrproblem der Galois-Theorie)**.** Existiert für jede endliche Gruppe G eine endliche Galois-Erweiterung $E|\mathbb{Q}$, für die $\mathrm{Aut}(E|\mathbb{Q}) \cong G$ gilt?

Für kleine Beispiele kann man diese Frage durch explizite Konstruktion positiv beantworten. Wir haben zum Beispiel bereits S_2, S_3, D_4, sowie S_5 realisiert. Es ist nicht schwer zu zeigen, dass jede endliche *abelsche* Gruppe als Galois-Gruppe über $\mathbb{Q}$ realisierbar ist.

Ein berühmter und schwieriger Satz von Igor SHAFAREVICH aus dem Jahr 1954 besagt, dass jede endliche *auflösbare* Gruppe als Galois-Gruppe über $\mathbb{Q}$ realisierbar ist. Für beliebige endliche Gruppen bleibt die Frage weithin offen. Selbst nach bald zweihundertjähriger Erfolgsgeschichte hält die Galois-Theorie immer noch interessante offene Fragen bereit.

KAPITEL 15

Anwendungen der Galois-Theorie

Dieses Kapitel behandelt zwei klassische Anwendungen der Galois-Theorie: die Konstruierbarkeit mit Zirkel und Lineal sowie die Auflösbarkeit von Gleichungen.

Als erstes die Frage der Konstruierbarkeit mit Zirkel und Lineal, die wir für das regelmäßige n-Eck abschließend beantworten. (Dies führt auf die Frage nach Fermat-Primzahlen, die in voller Allgemeinheit noch offen ist.) Zusammen mit der Transzendenz von π ergibt sich zudem die Unmöglichkeit der Quadratur des Kreises.

Als zweites die Frage nach der Auflösbarkeit von Gleichungen durch Radikale, also Ausdrücke der Form $\sqrt[n]{a}$. Gleichungen mit Grad ≤ 4 wusste man seit dem 16. Jahrhundert durch solche Formeln zu lösen, aber die Suche in Grad 5 und höher bliebt die folgenden Jahrhunderte erfolglos. Hier beweisen wir den überraschenden und wunderschönen Satz von Ruffini und Abel: Gleichungen vom Grad ≥ 5 lassen sich im Allgemeinen nicht durch Radikale auflösen!

Zur Vereinfachung werden wir uns in diesem Kapitel auf Körper der Charakteristik 0 konzentrieren.

§15A. Konstruierbarkeit mit Zirkel und Lineal

§15Aa. Kreisteilungspolynome. Sei $n \in \mathbb{N}_{\geq 1}$. In der multiplikativen Gruppe $\mathbb{C}^\times$ ist das Element $\zeta = e^{2\pi i/n}$ von Ordnung n, das heißt es gilt $\zeta^k = 1$ genau dann, wenn $k \in n\mathbb{Z}$. Das Polynom $X^n - 1$ hat daher als Nullstellen in $\mathbb{C}$ genau die n verschiedenen Elemente $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$, die wir die n-ten *Einheitswurzeln* in $\mathbb{C}$ nennen. Also gilt

$$X^n - 1 = (X-1)(X-\zeta)(X-\zeta^2)\cdots(X-\zeta^{n-1}) \qquad \text{in } \mathbb{C}[X]. \tag{15.1}$$

Die Menge $W_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\} < \mathbb{C}^\times$ ist eine zyklische Gruppe der Ordnung n und es gilt $\mathbb{Z}/n \xrightarrow{\sim} W_n$ gemäß $a \mapsto \zeta^a$. Die Erzeuger von W_n sind die Elemente $\xi \in \mathbb{C}^\times$ der Ordnung n, die wir die *primitiven n-ten Einheitswurzeln* nennen und zu der Menge

$$W_n^\times = \{\ \zeta^a \mid a \in (\mathbb{Z}/n)^\times\ \}$$

zusammenfassen. Wir erinnern daran, dass für $k \in \mathbb{Z}$ genau dann $\bar{k} \in (\mathbb{Z}/n)^\times$ gilt, wenn $\mathrm{ggT}(k,n) = 1$. Die Anzahl $\varphi(n) = |(\mathbb{Z}/n)^\times|$ ist die Eulersche φ-Funktion.

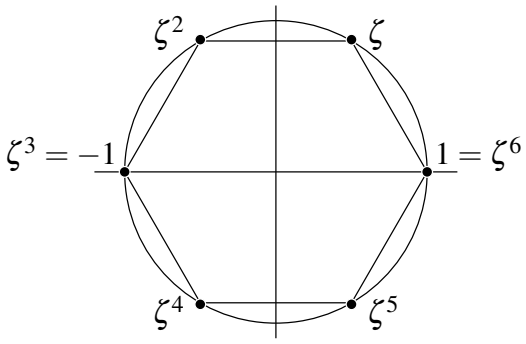


ABBILDUNG 1. Die n-ten Einheitswurzeln, hier für $n = 6$ gezeigt, liegen auf dem Einheitskreis und bilden die Ecken eines regelmäßigen n-Ecks.

Definition 15A1. Das n-te *Kreisteilungspolynom* oder *zyklotomische Polynom* ist

$$\Phi_n := \prod_{\substack{\xi\in\mathbb{C}^\times \\ \mathrm{ord}(\xi)=n}} (X-\xi). \tag{15.2}$$

Hierbei gilt $\mathrm{ord}(\xi) = n$ genau dann wenn $\xi = \zeta^a$ mit $a \in (\mathbb{Z}/n)^\times$, also $\deg \Phi_n = \varphi(n)$.

Lemma 15A2. *Für jedes $n \in \mathbb{N}_{\geq 1}$ gilt $\Phi_n \in \mathbb{Z}[X]$ und*

$$X^n - 1 = \prod_{\substack{d\in\mathbb{N} \\ d|n}} \Phi_d. \tag{15.3}$$

Mit (15.3) lassen sich zyklotomische Polynome rekursiv berechnen:

$$\begin{aligned}
\Phi_1 &= X-1 \\
\Phi_2 &= (X^2-1)/\Phi_1 = X+1 \\
\Phi_3 &= (X^3-1)/\Phi_1 = X^2+X+1 \\
\Phi_4 &= (X^4-1)/\Phi_1\Phi_2 = X^2+1 \\
\Phi_5 &= (X^5-1)/\Phi_1 = X^4+X^3+X^2+X+1 \\
\Phi_6 &= (X^5-1)/\Phi_1\Phi_2\Phi_3 = X^2-X+1 \\
&\dots
\end{aligned}$$

BEWEIS. Die Elemente $\xi \in \mathbb{C}$ mit $\xi^n = 1$ bilden die zyklische Gruppe $W_n < \mathbb{C}^\times$ der Ordnung n. Jedes Element $\xi \in W_n$ hat eine Ordnung $d = \mathrm{ord}(\xi)$ und diese teilt n (9A1). Damit folgt (15.3) aus (15.1) durch Umgruppierung gemäß (15.2). Wir zeigen per Induktion, dass Φ_n ganzzahlige Koeffizienten hat. Für Φ_1 ist dies klar. Für $n \geq 2$ folgt dies aus

$$\Phi_n = (X^n-1)/Q_n$$

mit $Q_n = \prod_{d\in\mathbb{N},d|n,d<n} \Phi_d$. Hier teilen wir das ganzzahlige Polynom $X^n - 1$ mit Leitkoeffizient 1 durch das ganzzahlige Polynom Q_n mit Leitkoeffizient 1. Die euklidische Division liefert $X^n - 1 = S_nQ_n + R_n$ mit $S_n, R_n \in \mathbb{Z}[X]$ und $\deg R_n < \deg Q_n$. Da S_n, R_n hierdurch eindeutig bestimmt sind und zudem $X^n - 1 = \Phi_nQ_n$ in $\mathbb{Q}[X]$ gilt, folgt $\Phi_n = S_n$ und $R_n = 0$. □

§**15Ab. Irreduzibilität.** Für jede Primzahl $p \in \mathbb{N}$ haben wir mit Hilfe des Eisenstein-Kriteriums (6G23) gezeigt, dass das p-te Kreisteilungspolynom

$$\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1$$

irreduzibel in $\mathbb{Z}[X]$ ist. Dies wollen wir nun wie folgt verallgemeinern:

Satz 15A3. *Für jedes $n \in \mathbb{N}_{\geq 1}$ ist Φ_n irreduzibel in $\mathbb{Z}[X]$ und somit in $\mathbb{Q}[X]$.*

Anders gesagt, für jede primitive n-te Einheitswurzel $\xi \in \mathbb{C}$ gilt $\operatorname{Irr}^X_{\mathbb{Q}}(\xi) = \Phi_n$.

BEWEIS. Wir können $\Phi_n = UV$ zerlegen in normierte Polynome $U, V \in \mathbb{Z}[X]$ wobei U irreduzibel in $\mathbb{Z}[X]$ ist. Sei $p \in \mathbb{N}$ eine Primzahl mit $p \nmid n$ und sei $\xi \in \mathbb{C}$ eine Wurzel von U. Wegen $\operatorname{ggT}(p,n) = 1$ ist mit ξ auch ξ^p eine primitive n-te Einheitswurzel, und somit eine Wurzel von Φ_n. Angenommen, ξ^p wäre keine Wurzel von U, dann müsste ξ^p eine Wurzel von V sein. Da $U(X)$ und $V(X^p)$ eine gemeinsame Wurzel ξ haben und U irreduzibel ist, gilt $U \mid V(X^p)$, also $V(X^p) = UW$ mit $W \in \mathbb{Z}[X]$.

Wegen $X^n - 1 = \Phi_n Q_n$ mit $Q_n \in \mathbb{Z}[X]$ gilt $X^n - 1 = UVQ_n$. Wir betrachten die Reduktion $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ modulo p und erhalten $X^n - 1 = \bar{U}\bar{V}\bar{Q}_n$. Wegen $V(X^p) = U(X)W(X)$ gilt hier $\bar{V}(X)^p = \bar{V}(X^p) = \bar{U}(X)\bar{W}(X)$. Demnach $\operatorname{ggT}(\bar{U}, \bar{V}) \neq 1$, und somit hätte $f = X^n - 1$ in $\mathbb{F}_p[X]$ mehrfache Faktoren. Da aber f und seine Ableitung $f' = nX^{n-1}$ die Bedingung $\operatorname{ggT}(f, f') = 1$ erfüllen, kann dieser Fall nicht eintreten. Also ist ξ^p, entgegen unserer anfänglichen Annahme, nicht Wurzel von V sondern von U.

Iteration dieses Arguments zeigt, für jedes $k \in \mathbb{N}$ mit $\operatorname{ggT}(k,n) = 1$, dass ξ^k eine Wurzel von U ist. Somit ist jede primitive n-te Einheitswurzel eine Wurzel von U, also $\deg U = \varphi(n)$. Das bedeutet $\Phi_n = U$ und $V = 1$, und somit ist Φ_n irreduzibel. □

Korollar 15A4. *Sei $\xi \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Dann ist $\mathbb{Q}(\xi)$ der Zerfällungskörper von $X^n - 1$ über $\mathbb{Q}$, es gilt $|\mathbb{Q}(\xi) : \mathbb{Q}| = \varphi(n)$ und $\operatorname{Aut}(\mathbb{Q}(\xi)|\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$.*

BEWEIS. Der Körper $\mathbb{Q}(\xi)$ enthält mit $1, \xi, \xi^2, \ldots, \xi^{n-1}$ alle Wurzeln von $X^n - 1$. Wir haben oben gesehen, dass $\operatorname{Irr}^X_{\mathbb{Q}}(\xi) = \Phi_n$ und somit $|\mathbb{Q}(\xi) : \mathbb{Q}| = \deg \Phi_n = \varphi(n)$. Für jedes Element $a \in (\mathbb{Z}/n)^\times$ ist auch ξ^a eine primitive n-te Einheitswurzel, es gilt $\mathbb{Q}(\xi) = \mathbb{Q}(\xi^a)$ und wegen $\operatorname{Irr}^X_{\mathbb{Q}}(\xi) = \operatorname{Irr}^X_{\mathbb{Q}}(\xi^a) = \Phi_n$ existiert ein Automorphismus $\sigma_a \colon \mathbb{Q}(\xi) \to \mathbb{Q}(\xi)$ mit $\sigma_a(\xi) = \xi^a$. Für $a, b \in (\mathbb{Z}/n)^\times$ gilt dann $\sigma_a(\sigma_b(\xi)) = \sigma_a(\xi^b) = (\xi^a)^b = \xi^{ab} = \sigma_{ab}(\xi)$. Das bedeutet $h \colon (\mathbb{Z}/n)^\times \to \operatorname{Aut}(\mathbb{Q}(\xi)|\mathbb{Q})$ mit $a \mapsto \sigma_a$ ist ein Gruppenhomomorphismus. Nach Konstruktion ist h injektiv, denn $\sigma_a = \sigma_b$ bedeutet $\xi^a = \xi^b$, und dies gilt nur für $a = b$. Wegen $|(\mathbb{Z}/n)^\times| = |\operatorname{Aut}(\mathbb{Q}(\xi)|\mathbb{Q})| = \varphi(n)$ ist h ein Isomorphismus. □

§**15Ac. Konstruierbarkeit mit Zirkel und Lineal.** Wir beginnen mit einer einfachen Beobachtung zu quadratischen Erweiterungen:

Lemma 15A5. *Sei K ein Körper der Charakteristik $\operatorname{char}(K) \neq 2$. Jede Erweiterung $E|K$ vom Grad $|E : K| = 2$ entsteht durch Adjunktion einer Quadratwurzel, das heißt es existiert $x \in E$ sodass $E = K(x)$ und $x^2 \in K$.*

BEWEIS. Wir wählen $b \in E$ mit $b \notin K$, sodass $E = K(b)$ gilt. Sei $\operatorname{Irr}^X_K(b) = X^2 + pX + q$. In einem Zerfällungskörper gilt $X^2 + pX + q = (X - b)(X - b')$ also $p = -b - b'$ und $q = bb'$.

Für $x := b + p/2$ gilt $b = -p/2 + x$ und $b' = -p/2 - x$ und somit

$$q = (-p/2 + x)(-p/2 - x) = p^2/4 - x^2.$$

Wir erhalten somit $E = K(x)$ und $x^2 = p^2/4 - q \in K$. □

Satz 15A6. *Seien $z, z_1, \ldots, z_r \in \mathbb{C}$ komplexe Zahlen. Dann sind äquivalent:*

1. *Der Punkt $z \in \mathbb{C}$ ist mit Zirkel und Lineal konstruierbar ausgehend von $1, z_1, \ldots, z_r$.*
2. *Ausgehend vom Grundkörper $K = \mathbb{Q}(z_1, \ldots, z_r)$ gibt es einen Turm quadratischer Erweiterungen $K = E_0 < E_1 < \ldots < E_n$ mit $z \in E_n$.*
3. *Die Zahl z ist algebraisch über $K = \mathbb{Q}(z_1, \ldots, z_r)$ und die normale Hülle E von $K(z)$ über K hat als Grad eine Zweierpotenz, also $|E : K| = 2^n$ für ein $n \in \mathbb{N}$.*

BEWEIS. Die geometrisch-algebraische Äquivalenz "(1) ⇔ (2)" haben wir in Kapitel 1 bewiesen. (Dort allerdings für reelle Erweiterungen, das heißt Teilkörper von $\mathbb{R}$. Als Übung beweise man dies erneut für Erweiterungen in $\mathbb{C}$.)

Besonders interessant für alles Weitere ist die Implikation "(3) ⇒ (2)". Sei $E|K$ eine Galois-Erweiterung vom Grad $|E : K| = 2^n$. Die Galois-Gruppe $G = \mathrm{Aut}(E|K)$ ist nach §9Fc auflösbar: Es existiert eine Kette von Untergruppen

$$\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_{n-1} \lhd G_n = G$$

der Ordnung $|G_i| = 2^i$. Die Galois-Korrespondenz beschert uns damit Zwischenkörper $E_k = \mathrm{Fix}(G_{n-k})$ sodass $|E : E_k| = 2^{n-k}$ und somit $|E_k : K| = 2^k$. Jede der sukzessiven Erweiterungen erfüllt $|E_{k+1} : E_k| = 2$, also erhalten wir einen Turm quadratischer Erweiterungen $K = E_0 < E_1 < \ldots < E_n$ mit $z \in E_n$.

Für die Implikation "(2) ⇒ (3)" beginnen wir mit einen Turm quadratischer Erweiterungen $K = E_0 < E_1 < \ldots < E_n = E$. Dann entsteht auch die normale Hülle $\bar{E}$ von E über K als Turm quadratischer Erweiterungen (15B13). □

§**15Ad. Konstruierbare n-Ecke und Fermat-Primzahlen.** Die Konstruktion des regelmäßigen n-Ecks führt uns nun auf folgende Frage: Für welche Werte $n \in \mathbb{N}_{\geq 1}$ ist $\zeta = e^{2\pi i/n}$ mit Zirkel und Lineal konstruierbar? Die Erweiterung $E = \mathbb{Q}(\zeta)$ ist galoissch vom Grad $\varphi(n)$. Nach obigem Satz glückt die Konstruktion mit Zirkel und Lineal genau dann, wenn $\varphi(n)$ eine Potenz von 2 ist. Hierzu sei $n = 2^e p_1^{e_1} \cdots p_\ell^{e_\ell}$ die Primzerlegung von n, mit Primzahlen $2 = p_0 < p_1 < \cdots < p_\ell$ und Vielfachheiten $e \geq 0$, $e_1, \ldots, e_\ell \geq 1$. Dann gilt

$$\varphi(n) = 2^{\max\{0, e-1\}} \cdot (p_1 - 1) p_1^{e_1 - 1} \cdots (p_\ell - 1) p_\ell^{e_\ell - 1}$$

Dies ist genau dann eine Zweierpotenz wenn $e_1 = \cdots = e_\ell = 1$ und jedes $p_k - 1$ eine Zweierpotenz ist. Solche Primzahlen gibt es tatsächlich, wie man leicht ausprobiert:

- $2^0 + 1 = 2$ ist prim.
- $2^1 + 1 = 3$ ist prim.
- $2^2 + 1 = 5$ ist prim.
  $2^3 + 1 = 9$ ist nicht prim.
- $2^4 + 1 = 17$ ist prim.
  $2^5 + 1 = 33$ ist nicht prim.
  $2^6 + 1 = 65$ ist nicht prim.
  $2^7 + 1 = 129$ ist nicht prim.

- $2^8+1 = 257$ ist prim.
  $2^9+1 = 513$ ist nicht prim.
  $2^{10}+1 = 1025$ ist nicht prim.
  $2^{11}+1 = 2049$ ist nicht prim.
  $2^{12}+1 = 4097$ ist nicht prim.
  $2^{13}+1 = 8193$ ist nicht prim.
  $2^{14}+1 = 16385$ ist nicht prim.
  $2^{15}+1 = 32769$ ist nicht prim.
- $2^{16}+1 = 65537$ ist prim.
  $2^{17}+1 = 131073$ ist nicht prim.
  ⋮

Lemma 15A7. *Für $m \in \mathbb{N}_{\geq 1}$ ist $p = 1+2^m$ höchstens dann eine Primzahl, wenn der Exponent m eine Zweierpotenz ist, also $m = 2^n$ für ein $n \in \mathbb{N}$ gilt, und somit $p = 1+2^{2^n}$.*

BEWEIS. Angenommen $m = ab$ mit $a > 1$ ungerade. Dann ist p zerlegbar gemäß

$$p = 1+2^{ab} = (1-2^b+2^{2b}-\cdots+2^{(a-1)b})(1+2^b).$$

Wenn also $p = 1+2^m$ eine Primzahl ist, dann kann m keinen ungeraden Faktor haben, und somit muss $m = 2^n$ für ein $n \in \mathbb{N}$ gelten. □

Zahlen der Form $F_n = 2^{2^n}+1$ nennt man *Fermat-Zahlen*, und die Primzahlen darunter nennt man *Fermat-Primzahlen*. Pierre de FERMAT (1607–1665) beobachtete, dass $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sämtlich prim sind. Er ließ sich sogar zu der Behauptung hinreißen, dass alle F_n prim seien. Doch schon Leonhard EULER (1707–1783) fand 1732 die Faktorisierung $F_5 = 1+2^{32} = 641 \cdot 6700417$. Die Faktorisierung von F_6 wurde 1880 von Landry und Le Lasseur gefunden, die Faktorisierung von F_7 gelang Morrison und Brillhart 1970 mit Hilfe von Computern.

$$\begin{aligned}
F_5 &= 2^{32}+1 = 4\,294\,967\,297 \\
&= 641 \times 6\,700\,417 \\
F_6 &= 2^{64}+1 = 18\,446\,744\,073\,709\,551\,617 \\
&= 274\,177 \cdot 67\,280\,421\,310\,721 \\
F_7 &= 2^{128}+1 = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,457 \\
&= 59\,649\,589\,127\,497\,217 \cdot 5\,704\,689\,200\,685\,129\,054\,721
\end{aligned}$$

Mit immer raffinierteren Algorithmen und massivem Computereinsatz gelang es bis zum Jahr 2010, die Fermat-Zahlen F_8, F_9, F_{10}, F_{11} vollständig zu faktorisieren. Man weiß zudem, dass auch $F_{12}, \ldots, F_{32}$ nicht prim sind, jeweils weil man einen (kleinen) Faktor von F_n gefunden hat oder F_n einen Primzahltest nicht bestanden hat. Die Natur der Fermat-Zahl F_{33} ist noch offen. Es ist nicht bekannt, ob es außer den fünf ersten Fermat-Primzahlen F_0, F_1, F_2, F_3, F_4 noch weitere Fermat-Primzahlen gibt.

Ungeachtet dieser Ungewissheit können wir als abschließenden Satz formulieren:

Satz 15A8 (Gauß)**.** *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^e p_1 \cdots p_\ell$ gilt mit $e \in \mathbb{N}$ und Fermat-Primzahlen $p_1 < \cdots < p_\ell$.*

§**15Ae. Die Quadratur des Kreises.** Die *Quadratur des Kreises* ist folgende Konstruktionsaufgabe: Zu einem gegebenen Kreis konstruiere man ein flächengleiches Quadrat. Wir nehmen hierbei an, dass der Kreis durch seinen Mittelpunkt 0 und seinen Radius 1 gegeben ist. Gesucht ist demnach ein Quadrat mit Fläche π, also mit Seitenlänge $\sqrt{\pi}$.

Die Quadratur des Kreises erreichte wie nur wenige mathematische Fragestellungen eine große Popularität außerhalb der Mathematik. Jahrhundertelang suchten daher neben Mathematikern auch immer wieder Laien vergeblich nach einer Lösung, und der Begriff "Quadratur des Kreises" wurde somit zu einer Metapher für eine unlösbare Aufgabe. Die abschließende Antwort lieferte Ferdinand von LINDEMANN (1852–1939):

Satz 15A9 (Lindeman 1882)**.** *Die Kreiszahl π ist transzendent über $\mathbb{Q}$.* □

(Der Beweis dieses Satzes wird hier ausgelassen.)

Mit π ist auch $\sqrt{\pi}$ transzendent über $\mathbb{Q}$, denn wäre $\sqrt{\pi}$ algebraisch über $\mathbb{Q}$ so auch π. Für die Konstruktion mit Zirkel und Lineal bedeutet das:

Korollar 15A10. *Sei ein Kreis mit Mittelpunkt 0 und Radius 1 gegeben. Mit Zirkel und Lineal ist die Konstruktion eines flächengleichen Quadrats nicht möglich.* □

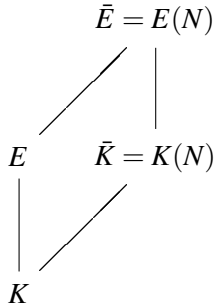
§15B. Auflösbare Erweiterungen

Eine endliche Galois-Erweiterung $E|K$ heißt *zyklisch* (oder *abelsch*, *auflösbar*, etc.) wenn die Galois-Gruppe $\mathrm{Aut}(E|K)$ *zyklisch* (oder *abelsch*, *auflösbar*, etc.) ist.

§**15Ba. Translationssatz.** Die folgende Beobachtung klärt, wie sich die Galois-Gruppe eines Polynoms P verhält, wenn man von einem Körper K zu einer Erweiterung E übergeht:

Proposition 15B1. *Sei $P \in K[X]$ ein separables Polynom über K. Zu jeder Erweiterung $E|K$ ist der natürliche Gruppenhomomorphismus $h\colon \mathrm{Gal}(P|E) \to \mathrm{Gal}(P|K)$ injektiv.*

BEWEIS. Über einem algebraischen Abschluss $C|E$ gilt $P = (X-a_1)\cdots(X-a_n)$ mit $a_1,\ldots,a_n \in C$. Durch Adjunktion der Nullstellenmenge $N = \{a_1,\ldots,a_n\}$ erhalten wir den Erweiterungskörper $\bar{E} = E(N)$ über E und ebenso $\bar{K} = K(N)$ über K.



Für jeden Automorphismus $\sigma \in \mathrm{Aut}(\bar{E}|E)$ gilt $\sigma|_K = \mathrm{id}_K$, denn $K < E$. Zudem gilt $\sigma(N) = N$, also $\sigma(\bar{K}) = \bar{K}$. Somit erhalten wir $h\colon \mathrm{Aut}(\bar{E}|E) \to \mathrm{Aut}(\bar{K}|K)$ durch $\sigma \mapsto \sigma|_{\bar{K}}$. Gilt $\sigma|_{\bar{K}} = \mathrm{id}_{\bar{K}}$, dann insbesondere $\sigma|_N = \mathrm{id}_N$ und somit $\sigma = \mathrm{id}_{\bar{E}}$. Also ist h injektiv. □

§**15Bb. Kreisteilunskörper.** In den folgenden Argumenten werden Einheitswurzeln weiter eine besondere Rolle spielen. Einen Zerfällungskörper von $X^n - 1$ über K nennen wir daher *Kreisteilungskörper* vom Exponenten n über K.

Korollar 15B2. *Es gilt* $\mathrm{Gal}(X^n - 1|\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$. *Ist K ein Körper der Charakteristik* 0*, dann gilt* $\mathrm{Gal}(X^n - 1|K) \hookrightarrow (\mathbb{Z}/n)^\times$*, und insbesondere ist* $\mathrm{Gal}(X^n - 1|K)$ *abelsch.* □

Im Allgemeinen wird $\mathrm{Aut}(X^n - 1|K)$ nicht isomorph zu $(\mathbb{Z}/n)^\times$ sein. Wenn K bereits alle n-ten Einheitswurzeln enthält, dann ist K der Zerfällungskörper von $X^n - 1$ über K und es gilt $\mathrm{Aut}(X^n - 1|K) = \{\mathrm{id}\}$. Allgemein, wenn das Polynom $X^n - 1$ in K genau m Wurzeln hat, dann gilt nach Lagrange $m \mid n$. In diesem Fall betrachten wir den natürlichen Ringhomomorphismus $\mathbb{Z}/n \to \mathbb{Z}/m$: Die Galois-Gruppe $\mathrm{Aut}(X^n - 1|K)$ ist isomorph zum Kern des induzierten Gruppenhomomorphismus $(\mathbb{Z}/n)^\times \to (\mathbb{Z}/m)^\times$.

§**15Bc. Die Gleichung $X^n - c$.** Zur Erinnerung: Die Gruppe $G = (\mathbb{Z}/n) \rtimes (\mathbb{Z}/n)^\times$ besteht aus den Abbildungen $f\colon \mathbb{Z}/n \to \mathbb{Z}/n$ mit $x \mapsto r + sx$, wobei $r \in \mathbb{Z}/n$ und $s \in (\mathbb{Z}/n)^\times$. Die Verknüpfung von f mit $g\colon x \mapsto r' + s'x$ ist dann $f \circ g\colon x \mapsto (r + sr') + (ss')x$.

Satz 15B3. *Sei K ein Körper der Charakteristik* 0*. Für $c \in K^\times$ wird der Zerfällungskörper E von $X^n - c$ über K erzeugt von einer Wurzel a von $X^n - c$ und einer primitiven n-ten Einheitswurzel ξ, und es existiert eine Einbettung $h\colon \mathrm{Aut}(E|K) \hookrightarrow (\mathbb{Z}/n) \rtimes (\mathbb{Z}/n)^\times$.*

Beweis. Sei C ein algebraischer Abschluss von K. Die Wurzeln von $X^n - c$ sind dann $a, \xi a, \ldots, \xi^{n-1}a \in C$. Offenbar gilt $K[a, \xi a, \ldots, \xi^{n-1}a] = K[a, \xi]$. Für jeden Automorphismus $\sigma \in \mathrm{Aut}(E|K)$ gilt $\sigma(a) = \xi^r a$ für ein $r \in \mathbb{Z}/n$ sowie $\sigma(\xi) = \xi^s$ für ein $s \in (\mathbb{Z}/n)^\times$. Wegen $E = K[a, \xi]$ ist σ durch das Paar (r, s) eindeutig festgelegt. Wir definieren $h\colon \mathrm{Aut}(E|K) \hookrightarrow G$ durch $h(\sigma)\colon x \mapsto r + sx$. Erfüllt $\tau \in \mathrm{Aut}(E|K)$ dann $h(\tau)\colon x \mapsto r' + s'x$, also $\tau(a) = \xi^{r'}a$ und $\tau(\xi) = \xi^{s'}$, dann gilt $\sigma(\tau(\xi)) = \sigma(\xi^{s'}) = (\xi^s)^{s'} = \xi^{ss'}$ und $\sigma(\tau(a)) = \sigma(\xi^{r'}a) = (\xi^s)^{r'}\xi^r a = \xi^{r+sr'}a$. Somit gilt $h(\sigma\tau) = h(\tau)h(\sigma)$. □

Beispiel 15B4. Wir kennen bereits zwei Fälle, in denen der obige Homomorphismus sogar ein Isomorphismus ist, nämlich

$$\mathrm{Gal}(X^3 - 2|\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/3) \rtimes (\mathbb{Z}/3)^\times \cong \mathrm{S}_3,$$
$$\mathrm{Gal}(X^4 - 2|\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/4) \rtimes (\mathbb{Z}/4)^\times \cong D_4.$$

Korollar 15B5. *Sei $p \in \mathbb{N}$ eine Primzahl und sei $P = X^p - c$ ein irreduzibles Polynom in $\mathbb{Q}[X]$. Dann gilt* $\mathrm{Gal}(P|\mathbb{Q}) \cong (\mathbb{Z}/p) \rtimes (\mathbb{Z}/p)^\times$.

Beweis. Wir benutzen die Bezeichnungen des Satzes. Die Grade $|\mathbb{Q}[a] : \mathbb{Q}| = p$ und $|\mathbb{Q}[\xi] : \mathbb{Q}| = p - 1$ sind teilerfremd. Daher hat der Zerfällungskörper $E = \mathbb{Q}[a, \xi]$ den Grad $|E : \mathbb{Q}| = p(p-1)$. Nach dem Satz gilt dann $\mathrm{Aut}(E|\mathbb{Q}) \cong (\mathbb{Z}/p) \rtimes (\mathbb{Z}/p)^\times$. □

§**15Bd. Zyklische Erweiterungen.** Wir haben oben die Galois-Gruppe $\mathrm{Gal}(X^n - c|K)$ untersucht. Die Situation wird vereinfacht, wenn K die nötigen Einheitswurzeln enthält:

Satz 15B6. *Sei $p \in \mathbb{N}$ eine Primzahl. Sei K ein Körper der Charakteristik 0, der eine primitive p-te Einheitswurzel enthält. Für jede Erweiterung $E|K$ sind dann äquivalent:*

1. *Es existiert $a \in E$, $a \notin K$, mit $E = K(a)$ und $a^p \in K$.*
2. *Die Erweiterung $E|K$ ist galoissch von Grad $|E:K| = p$.*

BEWEIS. Die Implikation "(1) $\Rightarrow$ (2)" folgt aus dem vorherigen Satz: Ist $\xi \in K$ eine primitive p-te Einheitswurzel, dann ist die Erweiterung $E = K(a)$ normal, also galoissch, denn E ist der Zerfällungskörper von $X^p - c$ über K, wobei $c = a^p$. Wir erhalten einen injektiven Gruppenhomomorphismus $h\colon \operatorname{Aut}(E|K) \to \mathbb{Z}/p$ durch $\sigma(a) = \xi^{h(\sigma)}a$, also ist $\operatorname{Aut}(E|K)$ zyklisch von Ordnung p oder trivial. Letzteres ist wegen $a \in E \smallsetminus K$ ausgeschlossen.

Die Umkehrung "(2) $\Rightarrow$ (1)" kann man wie folgt beweisen: Die Galois-Gruppe $\operatorname{Aut}(E|K)$ hat Ordnung p, und ist somit zyklisch. Sei $g \in \operatorname{Aut}(E|K)$ ein Erzeuger. Es gibt ein primitives Element $a \in E$ sodass $E = K(a)$, allerdings wird dieses im Allgemeinen nicht $a^p \in K$ erfüllen. Für $k = 0, \dots, p-1$ sei

$$b_k = a + \xi^k g(a) + \cdots + \xi^{k(p-1)} g^{p-1}(a).$$

Dann gilt $g(b_k) = \xi^{-k} b_k$, also $g(b_k^p) = (g(b_k))^p = b_k^p$. Wegen $\operatorname{Fix}(\operatorname{Aut}(E|K)) = K$ bedeutet dies $b_k^p \in K$ für alle $k = 0, \dots, p-1$. Umgekehrt lassen sich die Elemente $a, g(a), \dots, g^{p-1}(a) \in E$ als K-Linearkombinationen der Elemente $b_0, b_1, \dots, b_{p-1} \in E$ ausdrücken: Das obige Gleichungssystem hat als Matrix $A = (\xi^{kj})$ für $k, j = 0, \dots, p-1$. Dies ist eine Vandermonde-Matrix, und ihre Determinante $\det A = \prod_{i<j}(\xi^i - \xi^j)$ ist nicht Null, denn es gilt $\xi^i \neq \xi_j$ für alle $0 \leq i < j \leq p-1$. Es gilt daher $E = K(c) = K(b_1, \dots, b_n)$. Für mindestens einen Index $k \in \{0, \dots, p-1\}$ gilt folglich $b_k \notin K$ und somit $E = K(b_k)$ mit $b_k^p \in K$. □

Warnung: Für $p = 2$ ist in dem Satz die Voraussetzung der p-ten Einheitswurzeln überflüssig, denn $\pm 1 \in K$ gilt immer. Für $p \geq 3$ gelten in Abwesenheit der nötigen Einheitswurzeln die obigen Implikationen jedoch nicht mehr:

Beispiel 15B7. In $E = \mathbb{Q}[\sqrt[3]{2}]$ erfüllt $a = \sqrt[3]{2}$ zwar $a^3 \in \mathbb{Q}$, aber $E|\mathbb{Q}$ ist nicht normal, also nicht galoissch: Es fehlen die zu $\sqrt[3]{2}$ konjugierten Elemente $j\sqrt[3]{2}$ und $j^2\sqrt[3]{2}$.

Beispiel 15B8. Das Polynom $P = X^3 - 3X - 1$ ist irreduzibel über $\mathbb{Q}$ und hat drei reelle Wurzeln. Sei $a \in \mathbb{R}$ eine Wurzel, also $P(a) = 0$. Über $\mathbb{Q}(a)$ gilt dann die Zerlegung

$$P = (X-a)(X^2 + aX + a^2 - 3) = (X-a)(X + \tfrac{a+1}{a})(X + \tfrac{1}{a+1}).$$

Demnach ist $E = \mathbb{Q}(a)$ ein Zerfällungskörper von P über $\mathbb{Q}$. Insbesondere ist $E|\mathbb{Q}$ galoissch von Primzahlgrad $|E:\mathbb{Q}| = 3$. Es gibt aber kein Element $b \in E$ mit $E = \mathbb{Q}(b)$ und $b^3 \in \mathbb{Q}$. Ist $b^3 = 1$, dann $b \in \{1, j, j^2\}$ und $|\mathbb{Q}(b):\mathbb{Q}| \in \{1, 2\}$. Ist $b^3 \neq 1$, dann sind b, jb, j^2b die Konjugierten von r über $\mathbb{Q}$, und $\mathbb{Q}(b)$ ist wegen $j \notin \mathbb{Q}(b)$ nicht normal über $\mathbb{Q}$.

§**15Be. Radikalerweiterung.** Wir wollen nun definieren, was wir unter einer Radikalerweiterung "$K(\sqrt[n]{a})$" eines Körpers K verstehen. Die häufig zu findende Schreibweise "$\sqrt[n]{a}$" ist bequem aber möglicherweise irreführend: Anders als die gewohnte Wurzelfunktion $\sqrt[n]{\ }\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ gibt es im Allgemeinen keine natürliche Abbildung, die einem Element $a \in K$ (in einem beliebigen Körper) seine n-te Wurzel "$\sqrt[n]{a}$" (in einem algebraischen Abschluss) zuordnet. Wir vereinbaren also zunächst einen ebenso präzisen wie ehrlichen Sprachgebrauch.

Definition 15B9. Eine endliche Erweiterung $E|K$ heißt *Radikalerweiterung* (vom Exponenten $n \in \mathbb{N}$) wenn es ein Element $a \in E$ gibt mit $E = K(a)$ und $a^n \in K$.

Eine Folge $K = E_0 < E_1 < \ldots < E_n = E$ von Körpererweiterungen heißt *Turm von Radikalerweiterungen* wenn jede Erweiterung $E_{k+1}|E_k$ eine Radikalerweiterung ist.

Bemerkung 15B10. Ist $E|K$ eine Radikalerweiterung vom Exponenten n, also $E = K(a)$ mit $a^n \in K$ für ein geeignetes $a \in E$, dann ist a Nullstelle des Polynoms $X^n - c$ mit $c := a^n \in K$. Genau dann ist $|E : K| = n$, wenn $X^n - c$ irreduzibel über K ist; in diesem Fall gilt $\mathrm{Irr}_K^X(a) = X^n - c$. Im Allgemeinen braucht $X^n - c$ allerdings nicht irreduzibel über K zu sein. Jedenfalls ist $\mathrm{Irr}_K^X(a)$ ein Teiler von $X^n - c$, und somit $|E : K| = \deg \mathrm{Irr}_K^X(a) \leq n$.

Beispiel 15B11. Jeder Kreisteilungskörper E vom Exponenten n über K ist eine Radikalerweiterung: Ist ξ eine primitive n-te Einheitswurzel, so gilt $E = K(\xi)$ mit $\xi^n = 1$. Man beachte, dass der Exponent n und der Grad $\varphi(n) < n$ nicht übereinstimmen.

Der Zerfällungskörper E von $X^n - c$ über K, wobei $c \in K^\times$, entsteht als Turm von Radikalerweiterungen: zunächst $E_1 = K(\xi)$ durch Adjunktion einer primitiven n-ten Einheitswurzel ξ, sodann $E_2 = E_1(a)$ durch Adjunktion einer n-ten Wurzel a von c.

Man kann $E = K(\xi, a)$ auf viele verschiedene Weisen als Turm von Radikalerweiterungen erzeugen, zum Beispiel $E_1 = K(a)$ und $E_2 = E_1(\xi a)$. Auch hier gilt $a^n = (\xi a)^n = c$, aber die Erweiterungsgrade $|E_1 : K|$ und $|E_2 : E_1|$ sind im Allgemeinen kleiner als n.

Bemerkung 15B12. Jede Radikalerweiterung $E = K(a)$ mit $a^n \in K$ lässt sich verfeinern zu einem Turm $K = E_0 < E_1 < \ldots < E_r = E$ von Radikalerweiterungen mit primen Exponenten: Ist nämlich $n = p_1 p_2 \ldots p_r$ die Primfaktorzerlegung von n in $\mathbb{N}$, dann haben wir

$$K = K(a^{p_1 p_2 \cdots p_r}) < K(a^{p_2 \cdots p_r}) < \ldots < K(a^{p_r}) < K(a) = E.$$

Auf diese Weise lässt sich jeder Turm von Radikalerweiterungen verfeinern zu einem Turm von Radikalerweiterungen mit primen Exponenten.

Satz 15B6 besagt nun folgendes: Angenommen $p \in \mathbb{N}$ ist eine Primzahl und K enthält eine primitive p-te Einheitswurzel. Dann sind die echten Radikalerweiterung $E|K$ vom Exponenten p gerade die Galois-Erweiterungen vom Grad p.

Lemma 15B13. *Sei K ein Körper der Charakteristik 0. Angenommen es gibt einen Turm $K = F_0 < F_1 < \ldots < F_n = F$ von Radikalerweiterungen. Dann erlaubt die normale Hülle E von F über K ebenfalls einen Turm von Radikalerweiterungen (mit denselben Exponenten).*

BEWEIS. Wir führen Induktion über n. Für $n = 0$ ist nichts zu zeigen, denn $F = K$. Wir nehmen an, es gilt $n \geq 1$ und die Aussage ist für $n - 1$ bereits bewiesen, das heißt, die normale Hülle E_{n-1} von F_{n-1} über K lässt sich durch einen Turm von Radikalerweiterungen darstellen. Angenommen $F_n = F_{n-1}(a)$ mit $a^m \in F_{n-1}$. Dann entsteht die normale Hülle E_n von F_n über K aus E_{n-1} durch Adjunktion aller Konjugierten $a_1, \ldots, a_r$ von a über K. Hierbei sei $\mathrm{Aut}(E_n|K) = \{\sigma_1, \ldots, \sigma_r\}$ und $a_i = \sigma_i(a)$. Dann gilt

$$a_i^m = \sigma_i(a)^m = \sigma_i(a^m) \in \sigma(F_{n-1}) < E_{n-1}.$$

Demnach stiftet die sukzessive Adjunktion der Konjugierten $a_1, \ldots, a_r$ einen Turm von Radikalerweiterungen $E_{n-1} < \ldots < E_n$ vom Exponenten m. □

§**15Bf. Auflösbare Erweiterungen.** Radikalerweiterungen sind die denkbar einfachsten Körpererweiterungen. Wir werden nun sehen, dass man nicht alle Körpererweiterungen so erzeugen kann.

Definition 15B14. Eine Körpererweiterung $F|K$ heißt *durch Radikale auflösbar* wenn es eine Erweiterung $E|F$ und einen Turm von Radikalerweiterungen $K < \ldots < E$ gibt.

Ein Polynom $P \in K[X]$ heißt über K *durch Radikale auflösbar* wenn sein Zerfällungskörper über K auflösbar ist, wenn es also einen Turm $K < \ldots < E$ von Radikalerweiterungen gibt, sodass P über E zerfällt. Dies bedeutet, dass man jede Wurzel von P ausdrücken kann durch rationale Operationen und Radikale.

Beispiel 15B15. Jedes quadratisches Polynom $P = aX^2 + bX + c$ über einem Körper K (der Charakteristik $\neq 2$) ist durch Radikale auflösbar. Sei $E = K(r)$ wobei r eine Wurzel des Polynoms $X^2 - (b^2 - 4ac)$ über K ist. Dann zerfällt E über E gemäß

$$a\left(X - \frac{-b+r}{2a}\right)\left(X - \frac{-b-r}{2a}\right) = aX^2 + bX + c.$$

Ähnliche allgemeine Formeln existieren in Grad 3 (leichte Übung) und Grad 4 (etwas mühsame Übung). Allgemein gilt folgendes:

Satz 15B16. *Sei $P = a_0 + a_1X + \cdots + a_nX^n$ ein Polynom über einem Körper K der Charakteristik 0. Dann ist P genau dann über K durch Radikale auflösbar, wenn die Galois-Gruppe $\mathrm{Gal}(P|K)$ auflösbar ist.*

BEWEIS. Nehmen wir an, P sei über K durch Radikale auflösbar. Es gibt also einen Turm $K = F_0 < F_1 < \ldots < F_r = F$ von Radikalerweiterungen, sodass P über F zerfällt. Nach Lemma 15B13 können wir $F|K$ als normal annehmen. Sei $n \in \mathbb{N}$ ein gemeinsames Vielfaches aller auftretenden Exponenten und sei ξ eine n-te Einheitswurzel in einem algebraischen Abschluss von F. Dann ist $K < K(\xi)$ eine Radikalerweiterung und mittels $E_k = F_k(\xi)$ erhalten wir einen Turm

$$K < E_0 < E_1 < \ldots < E_r = E$$

von Radikalerweiterungen, sodass P über E zerfällt. Nach Konstruktion ist E normal über K, also galoissch. Nach 15B2 ist die Erweiterung $K < K(\xi)$ abelsch. Nach Satz 15B6 ist jede Erweiterung $E_0 < \ldots < E_r$ galoissch mit zyklischer Galois-Gruppe. Nach der Galois-Korrespondenz gehören hierzu die Gruppen

$$\mathrm{Aut}(E|K) \rhd \mathrm{Aut}(E|E_0) \rhd \mathrm{Aut}(E|E_1) \rhd \ldots \rhd \mathrm{Aut}(E|E_r) = \{\mathrm{id}\},$$

und die sukzessiven Quotienten sind abelsch. Die Galois-Gruppe $\mathrm{Aut}(E|K)$ ist somit auflösbar. Der Zerfällungskörper L von P über K ist ein normaler Zwischenkörper von $E|K$. Die Einschränkung definiert einen surjektiven Gruppenhomomorphismus $\mathrm{Aut}(E|K) \twoheadrightarrow \mathrm{Aut}(L|K)$. Damit ist auch $\mathrm{Gal}(P|K)$ auflösbar.

Nehmen wir umgekehrt an, dass die Galois-Gruppe $\mathrm{Gal}(P|K)$ auslösbar ist. Sei E der Zerfällungskörper von P über K, sodass $\mathrm{Aut}(E|K) = \mathrm{Gal}(P|K)$. Sei $n = |E:K|$ und sei ξ eine n-te Einheitswurzel in einem algebraischen Abschluss von E. Dann ist $F = E(\xi)$ der Zerfällungskörper von P über $K(\xi)$, sodass $\mathrm{Aut}(F|K(\xi)) = \mathrm{Gal}(P|K(\xi))$. Nach 15B1 ist der natürliche Gruppenhomomorphismus $h\colon\ \mathrm{Gal}(P|K(\xi)) \to \mathrm{Gal}(P|K)$ injektiv. Daher ist

die Gruppe $\mathrm{Gal}(P|K(\xi))$ auflösbar. Es existiert also eine Kette

$$\mathrm{Aut}(F|K(\xi)) = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{\mathrm{id}\}$$

von Untergruppen, sodass jede Quotientengruppe G_{r-1}/G_r zyklisch von Primzahlordnung ist. Mittels Galois-Korrespondenz gehören hierzu die Teilkörper

$$K(\xi) = F_0 < F_1 < \ldots < F_r = F.$$

Die sukzessiven Erweiterungen $F_k|F_{k-1}$ sind von Primzahlgrad, nach Satz 15B6 also Radikalerweiterungen. Gleiches gilt für den ersten Erweiterungsschritt $K(\xi)|K$. Demnach ist $K < \ldots < F$ ein Turm von Radikalerweiterungen sodass P über F zerfällt. □

Korollar 15B17. *Jedes Polynom $P \in K[X]$ vom Grad $n \leq 4$ über einem Körper der Charakteristik 0 ist durch Radikale auflösbar.*

BEWEIS. Wir wissen $\mathrm{Gal}(P|K) \hookrightarrow S_n$. Da S_n für $n \leq 4$ auflösbar ist, ist auch $\mathrm{Gal}(P|K)$ auflösbar. Nach dem Satz ist P durch Radikale auflösbar. □

Korollar 15B18. *Es gibt Polynome $P \in \mathbb{Q}[X]$ vom Grad ≥ 5, die nicht durch Radikale auflösbar sind.*

BEWEIS. Für das Polynom $P = X^5 - 4X + 2$ haben wir $\mathrm{Gal}(P|\mathbb{Q}) \cong \mathrm{S}_5$ gezeigt (§14Db). Da die Gruppe S_5 nicht auflösbar ist, ist P nicht durch Radikale auflösbar. □

Es gibt selbstverständlich in jedem Grad $n \geq 5$ auch Polynome, die durch Radikale auflösbar sind, zum Beispiel alle Polynome der Form $X^n - c$, die wir oben ausführlich diskutiert haben. Die Frage ob ein Polynom P über K auslösbar ist oder nicht lässt sich *nicht* allein durch den Grad entscheiden sondern nur durch die Galois-Gruppe $\mathrm{Gal}(P|K)$.

§**15Bg. Die allgemeine Gleichung vom Grad n.** Unter einer *allgemeinen* Gleichung vom Grad n über K verstehen wir eine Gleichung, deren Koeffizienten keine algebraische Relation erfüllen. Hierzu sei $K[a_1,\ldots,a_n]$ der Polynomring in den Unbestimmten $a_1,\ldots,a_n$ und sei $E = K(a_1,\ldots,a_n)$ der Bruchkörper.

Die allgemeine Gleichung vom Grad n über K ist dann die Gleichung

$$X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n.$$

Wir sagen, diese Gleichung ist durch Radikale auflösbar wenn sie durch Radikale auflösbar ist über dem Körper $E = K(a_1,\ldots,a_n)$.

Beispiel 15B19. Die allseits beliebte Formel

$$x = \frac{1}{2}a_1 \pm \frac{1}{2}\sqrt{a_1^2 - 4a_2}$$

zeigt, dass die allgemeine Gleichung zweiten Grades durch Radikale auflösbar ist (Diese kurze Schreibweise ist bequem trotz aller in §15Be formulierten Bedenken. Als Stilübung führe man die korrekte Formulierung aus.)

Satz 15B20. *Das allgemeine Polynom P vom Grad n über K hat Galois-Gruppe* $\mathrm{Gal}(P|E) \cong \mathrm{S}_n$. *Es ist daher für $n \leq 4$ auflösbar und für $n \geq 5$ nicht auflösbar.*

BEWEIS. Der Beweis gelingt leicht mit dem Hauptsatz über symmetrische Polynome. (Hier ausgelassen.) □