Algebra für Lehramt

Matthias Künzer

Universität Stuttgart

9. September 2024

Inhalt

Verzeichnis einiger Aussagen

Vorwort

Inhalt ist Algebra, im Umfang der Vorlesung aus dem Wintersemester.

Vorausgesetzt wird Lineare Algebra. Insbesondere werden die Begriffe Gruppe, abelsche Gruppe, Körper, Vektorraum als bekannt angenommen. Wir werden aber kurze Erinnerungen einbauen.

Das Skript wurde für den Online-Betrieb während der Covid-Pandemie erstellt.

Dank für Verbesserungen geht an Nora Krauß, Stefan Erbschwendner, Georg Schmid, Simon Meder, Lea Etgeton, Lara Binder, Axel Weeber, Jan Glock, Jennifer Roming, Matthias Kalmbach, Madeleine Rapp, André Kliem, Markus Engelhardt, Simon Meder, Kim Paul Schmidt und Elias Schwesig.

Von Nora Krauß stammt das Beispiel zu Sylow in §A.2 und die Ausarbeitung von Lemma 274.

Für weitere Hinweise auf Fehler und Unklarheiten bin ich dankbar.

Stuttgart, Sommer 2020 und Sommer 2021

Matthias Künzer

Konventionen

- Sei X eine Menge.

  Wir schreiben $Y \subseteq X$, um auszudrücken, daß Y eine Teilmenge von X ist.

  Wir schreiben $Y \subset X$, um auszudrücken, daß Y eine Teilmenge von X ist mit $Y \neq X$.

- Für $a, b \in \mathbb{Z}$ sei $[a,b] := \{ z \in \mathbb{Z} : a \leqslant z \leqslant b \}$ das ganzzahlige Intervall.

- Für $a \in \mathbb{Z}$ sei $\mathbb{Z}_{\geqslant a} := \{ z \in \mathbb{Z} : a \leqslant z \}$.

- Sei X eine Menge. Seien $Y, Z \subseteq X$.

  Wir schreiben $Y \sqcup Z := Y \cup Z$, um auszudrücken, daß eine disjunkte Vereinigung vorliegt, daß also $Y \cap Z = \emptyset$ ist.

- Seien X und Y Mengen. Sei $f : X \to Y$ eine Abbildung.

  Sei $X' \subseteq X$, $Y' \subseteq Y$ und $f(X') \subseteq Y'$. Wir schreiben $f|_{X'}^{Y'} : X' \to Y' : x' \longmapsto f(x')$ für die eingeschränkte Abbildung.

  Ist $Y' = Y$, so schreiben wir auch $f|_{X'} := f|_{X'}^{Y}$.

  Ist $X' = X$, so schreiben wir auch $f|^{Y'} := f|_{X}^{Y'}$.

- Sei X eine Menge. Es bezeichne $|X|$ die Anzahl der Elemente von X.

  Wir schreiben dabei $|X| = \infty$, falls diese Anzahl nicht endlich ist.

- Sei X eine Menge. Bezeichne $\mathrm{Pot}(X) := \{ Y : Y \subseteq X \}$ die Potenzmenge von X.

- Sei R ein kommutativer Ring. Seien $m, n \geqslant 0$. Seien $k \in [1,m]$ und $\ell \in [1,n]$.

  Sei $\mathrm{e}_{k,\ell} \in R^{m \times n}$ die Matrix, die an Position (k,ℓ) den Eintrag 1 an, und an allen anderen Positionen den Eintrag 0.

  Falls $n = 1$ ist, so schreiben wir auch $\mathrm{e}_k := \mathrm{e}_{k,1}$ für den Spaltenvektor, der an Position k den Eintrag 1 hat, und an allen anderen Positionen den Eintrag 0.

Kapitel 1

Ganze Zahlen und Polynome

1.1 Ringe

Definition 1 Ein *Ring* ist eine Menge R, zusammen mit Abbildungen

$$(+) \ : \ R \times R \to R \ : \ (r, s) \mapsto r + s \ ,$$

genannt *Addition*, und

$$(\cdot) \ : \ R \times R \to R \ : \ (r, s) \mapsto r \cdot s \ ,$$

genannt *Multiplikation*, derart, daß die folgenden Eigenschaften (Ring 1–7) gelten.

(Ring 1) Für $r, \, s \, \in \, R$ ist $r + s = s + r$.

(Ring 2) Für $r, \, s, \, t \, \in \, R$ ist $(r + s) + t = r + (s + t)$.

(Ring 3) Es gibt ein Element 0_R derart, daß für $r \in R$ sich $r + 0_R = r$ ergibt.

(Ring 4) Für $r \in R$ gibt es ein $s \in R$ mit $r + s = 0$.

(Ring 5) Für $r, \, s, \, t \, \in \, R$ ist $(r \cdot s) \cdot t = r \cdot (s \cdot t)$.

(Ring 6) Es gibt ein Element 1_R derart, daß für $r \in R$ sich $r \cdot 1_R = r = 1_R \cdot r$ ergibt.

(Ring 7) Für $r, \, r', \, s, \, s' \, \in \, R$ ist $(r + r') \cdot s = r \cdot s + r' \cdot s$ und $r \cdot (s + s') = r \cdot s + r \cdot s'$.

Oft schreibt man nur $R := (R, +, \cdot)$. Oft schreibt man nur $rs := r \cdot s$ für $r, \, s \, \in \, R$.

Die Eigenschaften (Ring 1–4) besagen, daß $(R, +)$ eine abelsche Gruppe ist.

(Ring 2) und (Ring 5) geben Anlaß zum Weglassen der darin auftretenden Klammern.

Das Element 0_R in (Ring 3) liegt eindeutig fest, denn für Elemente 0_R, $0'_R$ in R mit dieser Eigenschaft wird $0_R = 0_R + 0'_R = 0'_R$. Wir schreiben oft $0 := 0_R$.

Das Element s in (Ring 4) liegt eindeutig fest, denn für Elemente s, s' in R mit dieser Eigenschaft wird $s = s + r + s' = s'$. Wir schreiben $s =: -r$.

Das Element 1_R in (Ring 6) liegt eindeutig fest, denn für Elemente 1_R, $1'_R$ in R mit dieser Eigenschaft wird $1_R = 1_R \cdot 1'_R = 1'_R$. Wir schreiben oft $1 := 1_R$.

Wir schreiben $R^\times := R \smallsetminus \{0\}$.

Wir schreiben $\mathrm{U}(R) := \{\, r \in R \,:\, \text{es gibt ein } s \in R \text{ mit } r \cdot s = 1_R = s \cdot r \,\}$ für die Menge der *invertierbaren* Elemente von R. Ein invertierbares Element heißt auch eine *Einheit* ([1]).

Ist $r \in \mathrm{U}(R)$, dann liegt das Element $s \in R$ mit $r \cdot s = 1_R = s \cdot r$ eindeutig fest, denn für Elemente s, s' mit dieser Eigenschaft wird $s = s \cdot r \cdot s' = s'$. Wir schreiben $s =: r^{-1}$.

Falls $r \cdot s = s \cdot r$ gilt für r, $s \in R$, dann heißt der Ring R ein *kommutativer Ring.*

Falls $(R, +, \cdot)$ kommutativ ist, falls $0_R \neq 1_R$ ist und falls für alle $r \in R^\times$ ein $s \in R$ mit $r \cdot s = 1$ existiert, dann ist R ein Körper. Mit anderen Worten, es ist ein kommutativer Ring R ein Körper, falls $\mathrm{U}(R) = R^\times$ ist.

Das Axiom (Ring 7) kann auch äquivalent ersetzt werden, vgl. §A.1.

Definition 2 Sei R ein Ring.

Eine Teilmenge $S \subseteq R$ heißt *Teilring,* falls $0_R \in S$, falls $1_R \in S$, und falls für s, $s' \in S$ auch $s - s'$ und $s \cdot s'$ in S liegen.

Diesenfalls ist S, mit auf S von R eingeschränkter Addition und Multiplikation, wieder ein Ring.

Die Bedingung $0_R \in S$ ist dabei redundant, da aus den anderen Bedingungen bereits $0_R = 1_R - 1_R \in S$ folgt.

Definition 3 Seien R und S Ringe.

Das *direkte Produkt* $R \times S = \{\, (r, s) \;:\; r \in R,\, s \in S \,\}$ ist ein Ring mit eintragsweiser Addition und Multiplikation, d.h. mit

$$\begin{aligned} (r, s) + (r', s') &:= (r + r', s + s') \\ (r, s) \cdot (r', s') &:= (r \cdot r', s \cdot s') \end{aligned}$$

für (r, s), $(r', s') \in R \times S$.

Beispiel 4

(1) Es ist $\mathbb{Z}$ ein kommutativer Ring.

(2) Es sind $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ Körper, also auch kommutative Ringe. Es ist $\mathbb{Z} \subseteq \mathbb{Q}$ ein Teilring.

[1] Engl. unit.

(3) Sei R ein kommutativer Ring. Sei $n \in \mathbb{Z}_{\geqslant 1}$. Es ist $R^{n\times n}$ der Ring der $n \times n$-Matrizen mit Einträgen in R.

Dieser ist i.a. nicht kommutativ. Z.B. ist in $\mathbb{Q}^{2\times 2}$ zum einen $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$, aber zum anderen $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$.

(4) Sei p prim. Es ist

$$\mathbb{Z}_{(p)} \;:=\; \{\, \tfrac{a}{b} \in \mathbb{Q} \,:\, a \in \mathbb{Z},\, b \in \mathbb{Z}^\times \text{ teilerfremd, } p \text{ teilt nicht } b \,\} \;\subseteq\; \mathbb{Q}$$

ein Teilring von $\mathbb{Q}$, der $\mathbb{Z}$ als Teilring enthält.

Definition 5 Sei R ein kommutativer Ring.

Es heißt R ein *Integritätsbereich*, wenn $0_R \neq 1_R$ ist und für $x,\, y \in R^\times$ auch $x \cdot y \in R^\times$ liegt.

Beispiel 6

(1) Es ist $\mathbb{Z}$ ein Integritätsbereich.

(2) Jeder Körper und jeder Teilring eines Körpers sind Integritätsbereiche.

(3) Es ist $\mathbb{Q} \times \mathbb{Q}$ zwar ein kommutativer Ring, aber kein Integritätsbereich. Denn z.B. sind $(3,0),\, (0,7) \in (\mathbb{Q}\times\mathbb{Q})^\times$, aber $(3,0)\cdot(0,7) = (0,0) = 0_{\mathbb{Q}\times\mathbb{Q}}$.

Definition 7 Sei R ein kommutativer Ring.

Der *Polynomring* $R[X]$ ist definiert als Menge der formalen Polynome

$$\begin{aligned} R[X] \;&:=\; \{\, \textstyle\sum_{i\in[0,m]} a_i X^i \,:\, m \in \mathbb{Z}_{\geqslant 0},\, a_i \in R \text{ für } i \in [0,m] \,\} \\ &=\; \{\, a_0X^0 + a_1X^1 + \ldots + a_mX^m \,:\, m \in \mathbb{Z}_{\geqslant 0},\, a_i \in R \text{ für } i \in [0,m] \,\}\,. \end{aligned}$$

Gesprochen wird $R[X]$ als "R adjungiert X" oder kurz "$R\ X$".

Zwei Polynome seien also genau dann gleich, wenn sie bei jedem Monom denselben Koeffizienten haben. ([2])

Wir schreiben auch oft $\sum_{i\geqslant 0} a_iX^i := \sum_{i\in[0,m]} a_iX^i$, wobei bei ersterer Schreibweise schon vereinbart sei, daß es ein $m \in \mathbb{Z}_{\geqslant 0}$ gibt mit $a_i = 0$ ist für $i \geqslant m+1$.

Seien Polynome $f(X) = \sum_{i\geqslant 0} a_iX^i$ und $g(X) = \sum_{j\geqslant 0} b_jX^j$ in $R[X]$ gegeben.

Sei auf $R[X]$ die Addition definiert durch

$$f(X) + g(X) = \big(\sum_{i\geqslant 0} a_iX^i\big) + \big(\sum_{i\geqslant 0} b_iX^i\big) \;:=\; \sum_{i\geqslant 0}(a_i+b_i)X^i\,.$$

[2] Eigentlich ist also ein solches Polynom eine Abbildung von $\mathbb{Z}_{\geqslant 0}$ nach R mit endlichem Träger. Die Verwendung der formalen Variable X gibt dieser Tatsache ein angenehmeres Aussehen.

Sei auf $R[X]$ die Multiplikation definiert durch

$$f(X) \cdot g(X) \;=\; \big(\sum_{i\geqslant 0} a_i X^i\big) \cdot \big(\sum_{j\geqslant 0} b_j X^j\big) \;:=\; \sum_{k\geqslant 0} \big(\sum_{i\in[0,k]} a_i \cdot b_{k-i}\big) X^k \,.$$

Mit anderen Worten, die Multiplikation ist erklärt als distributive Fortsetzung von $aX^i bX^j = abX^{i+j}$, wobei $a,\, b \,\in\, R$ und $i,\, j \,\in\, \mathbb{Z}_{\geqslant 0}$.

Man verifiziert, daß $R[X]$ damit ein kommutativer Ring ist.

Natürlich schreibt man auch

$$a_0X^0 + a_1X^1 + a_2X^2 + \ldots + a_mX^m \;=\; a_0 + a_1X + a_2X^2 + \ldots + a_mX^m \,.$$

Für $f(X) = \sum_{i\geqslant 0} a_i X^i \in R[X]$ und $r \in R$ sei $f(r) := \sum_{i\geqslant 0} a_i r^i \in R$. Ist $f(r) = 0$, dann heißt r *Nullstelle* von $f(X)$ in R.

Beispiel 8

(1) Wir haben den Teilring $\mathbb{Z}[X] \subseteq \mathbb{Q}[X]$.

(2) Wir erinnern an den Körper $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$, mit $1 + 1 + 1 = 0$. Vgl. auch Definition 17 unten.

In $\mathbb{F}_3[X]$ ist $X^3 - X$ ungleich dem Nullpolynom 0, denn die Koeffizienten von $X^3 - X$ bei X^3 und bei X^1 unterscheiden sich von denen des Nullpolynoms.

Aber trotzdem gilt für alle $x \in \mathbb{F}_3$, daß $x^3 - x = 0$ ist.

Deswegen besteht man auf der Verwendung einer formalen Variablen X, im Unterschied zur tatsächlichen Variablen x.

(3) Ist R ein Integritätsbereich, dann ist $\mathrm{U}(R[X]) = \mathrm{U}(R)$.

Ist also z.B. K ein Körper, dann ist $\mathrm{U}(K[X]) = \mathrm{U}(K) = K^\times$.

Ferner ist z.B. $\mathrm{U}(\mathbb{Z}[X]) = \mathrm{U}(\mathbb{Z}) = \{-1, +1\}$.

Definition 9 Sei R ein kommutativer Ring. Sei $f(X) = \sum_{i\geqslant 0} a_i X^i \in R[X]$.

Ist $f(X) \neq 0$, so ist der *Grad* von $f(X)$ definiert als

$$\deg(f(X)) \;:=\; \max\{\, i \in \mathbb{Z}_{\geqslant 0} \,:\, a_i \neq 0 \,\} \qquad ([3])$$

Zusätzlich setzen wir noch $\deg(0) := -\infty$, wobei wir vereinbaren, daß $-\infty < x$ und $-\infty + x = -\infty$ sein soll für $x \in \mathbb{Z}_{\geqslant 0}$ und daß $(-\infty) + (-\infty) = -\infty$ sein soll.

[3] Engl. degree.

Dann gelten für $f(X),\, g(X) \in R[X]$ die folgenden Ungleichungen.

$$\begin{array}{rcl} \deg(f(X)+g(X)) & \leqslant & \max\{\deg(f(X)), \deg(g(X))\} \\ \deg(f(X)\cdot g(X)) & \leqslant & \deg(f(X)) + \deg(g(X)) \end{array}$$

Ist R ein Integritätsbereich, dann ist $\deg(f(X)\cdot g(X)) = \deg(f(X)) + \deg(g(X))$. Insbesondere ist dann $R[X]$ wieder ein Integritätsbereich.

Ist $f(X) = \sum_{i\geqslant 0} a_i X^i \in R[X]^\times$ und $n := \deg(f(X))$, dann heißt a_n auch der *Leitkoeffizient* von $f(X)$.

Ein Polynom in $R[X]^\times$ mit Leitkoeffizient 1 heißt *normiert*.

Satz 10 (Descartes) Sei $f(X) = a_0X^0 + a_1X^1 + \ldots + a_mX^m \in \mathbb{Z}[X]$.

Sei $a_0 \neq 0$ und $a_m \neq 0$.

Sei $\frac{u}{v} \in \mathbb{Q}$ mit $u,\, v \in \mathbb{Z}^\times$ teilerfremd und mit

$$f\big(\tfrac{u}{v}\big) \;=\; 0$$

gegeben. D.h. sei $\frac{u}{v}$ eine Nullstelle von $f(X)$, die in $\mathbb{Q}^\times$ liegt und gekürzt geschrieben ist.

Dann ist u ein Teiler von a_0 . Ferner ist v ein Teiler von a_m .

Beweis. Es ist $0 = v^m \cdot \big(\sum_{i\in[0,m]} a_i \frac{u^i}{v^i}\big) = \sum_{i\in[0,m]} a_i u^i v^{m-i}$.

Da $a_0v^m = -\sum_{i\in[1,m]} a_i u^i v^{m-i} = -u \cdot \big(\sum_{i\in[1,m]} a_i u^{i-1} v^{m-i}\big)$ durch u teilbar ist, aber u und v teilerfremd sind, muß u ein Teiler von a_0 sein.

Da $a_mu^m = -\sum_{i\in[0,m-1]} a_i u^i v^{m-i} = -v \cdot \big(\sum_{i\in[0,m-1]} a_i u^i v^{m-1-i}\big)$ durch v teilbar ist, aber u und v teilerfremd sind, muß v ein Teiler von a_m sein. ▫

Beispiel 11 Wir wollen nachweisen, daß $X^3 + X + \frac{2}{3} \in \mathbb{Q}[X]$ keine Nullstelle in $\mathbb{Q}$ hat.

Dies ist äquivalent zur Aussage, daß $f(X) := 3\cdot(X^3 + X + \frac{2}{3}) = 3X^3 + 3X + 2 \in \mathbb{Z}[X]$ keine Nullstelle in $\mathbb{Q}$ hat.

Annahme, doch. Dann gibt es $\frac{u}{v} \in \mathbb{Q}$ mit $u,\, v \in \mathbb{Z}^\times$ teilerfremd und mit $f(\frac{u}{v}) = 0$. Nach Satz 10 ist dann aber u ein Teiler von 2 und v ein Teiler von 3.

Somit ist $u \in \{1, 2, -1, -2\}$ und $v \in \{1, 3, -1, -3\}$, folglich

$$\tfrac{u}{v} \;\in\; \{1, 2, \tfrac{1}{3}, \tfrac{2}{3}, -1, -2, -\tfrac{1}{3}, -\tfrac{2}{3}\}\ .$$

Aber ein Taschenrechner gibt $f(1) = 8$, $f(2) = 32$, $f(\frac{1}{3}) = \frac{28}{9}$, $f(\frac{2}{3}) = \frac{44}{9}$, $f(-1) = -4$, $f(-2) = -28$, $f(-\frac{1}{3}) = \frac{8}{9}$, $f(-\frac{2}{3}) = -\frac{8}{9}$.

Da 0 nicht unter diesen Funktionswerten auftritt, haben wir einen *Widerspruch*.

1.2 Ringmorphismen

Definition 12 Seien R und S Ringe.

Eine Abbildung $\varphi : R \to S$ heißt *Ringmorphismus*, falls $\varphi(1_R) = 1_S$ ist und falls für $r, r' \in R$ sich

$$\begin{aligned} \varphi(r + r') &= \varphi(r) + \varphi(r') \\ \varphi(r \cdot r') &= \varphi(r) \cdot \varphi(r') \end{aligned}$$

ergibt.

Dann ist auch $\varphi(0_R) = \varphi(0_R) + \varphi(0_R) - \varphi(0_R) = \varphi(0_R + 0_R) - \varphi(0_R) = 0_S$.

Desweiteren ist $\varphi(-x) = \varphi(-x) + \varphi(x) - \varphi(x) = \varphi((-x) + x) - \varphi(x) = \varphi(0_R) - \varphi(x) = 0_S - \varphi(x) = -\varphi(x)$ für $x \in R$.

Ferner ist für $r \in \mathrm{U}(R)$ auch $\varphi(r^{-1}) \cdot \varphi(r) = \varphi(r^{-1} \cdot r) = \varphi(1_R) = 1_S$, genauso $\varphi(r) \cdot \varphi(r^{-1}) = 1_S$ und also $\varphi(r) \in \mathrm{U}(S)$ mit $\varphi(r^{-1}) = \varphi(r)^{-1}$.

Das Kompositum zweier Ringmorphismen ist ein Ringmorphismus.

Ist der Ringmorphismus φ bijektiv, so heißt φ ein *Ringisomorphismus*. Dies wird durch $\varphi : R \xrightarrow{\sim} S$ gekennzeichnet.

Ist φ ein Ringisomorphismus, dann auch φ^{-1}.

Zwei Ringe R und S heißen *isomorph*, geschrieben $R \simeq S$, wenn es einen Ringisomorphismus von R nach S gibt.

Beispiel 13 Sei $z \in \mathbb{Z}$. Wir betrachten die Abbildung

$$\begin{array}{lcl} \mathbb{Z}[X] & \xrightarrow{\varphi} & \mathbb{Z} \\ f(X) & \mapsto & \varphi(f(X)) := f(z)\,, \end{array}$$

definiert durch Einsetzen von z in das Polynom $f(X)$.

In der Tat ist $\varphi(1) = 1$, da Einsetzen von z in das konstante Polynom $1 \in \mathbb{Z}[X]$ eben $1 \in \mathbb{Z}$ ergibt.

Seien nun $f(X)$, $g(X) \in \mathbb{Z}[X]$ gegeben. Es wird

$$\begin{aligned} \varphi(f(X) + g(X)) &= f(z) + g(z) &&= \varphi(f(X)) + \varphi(g(X)) \\ \varphi(f(X) \cdot g(X)) &= f(z) \cdot g(z) &&= \varphi(f(X)) \cdot \varphi(g(X))\,. \end{aligned}$$

Also ist φ ein Ringmorphismus.

Definition 14 Sei R ein Ring.

Eine Teilmenge $I \subseteq R$ heißt *Linksideal*, falls $0 \in I$ und falls für $r, s \in R$ und $x, y \in I$ sich $r \cdot x + s \cdot y \in I$ ergibt.

Eine Teilmenge $I \subseteq R$ heißt *Rechtsideal*, falls $0 \in I$ und falls für $r, s \in R$ und $x, y \in I$ sich $x \cdot r + y \cdot s \in I$ ergibt.

Eine Teilmenge $I \subseteq R$ heißt *Ideal*, falls sie ein Links- und ein Rechtsideal ist.

Wir schreiben $I \trianglelefteq R$, um auszudrücken, daß I ein Ideal in R ist.

Wir schreiben $I \triangleleft R$, um auszudrücken, daß I ein Ideal in R ist mit $I \neq R$.

Bemerkung 15 Sei R ein Ring. Sei $I \trianglelefteq R$.

Genau dann ist $I = R$, wenn $1 \in I$ liegt.

Beispiel 16

(1) Sei R ein kommutativer Ring. Sei $x \in R$. Es ist $xR := \{ xr : r \in R \} \trianglelefteq R$.
Speziell ist $0 := 0R \trianglelefteq R$.

(2) Es ist $3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\} \triangleleft \mathbb{Z}$.

(3) Es ist $\{ \left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right) : a, b \in \mathbb{Z} \}$ ein Rechtsideal in $\mathbb{Z}^{2\times 2}$, aber kein Ideal.
Es ist $\{ \left(\begin{smallmatrix} 5a & 5b \\ 5c & 5d \end{smallmatrix}\right) : a, b, c, d \in \mathbb{Z} \}$ ein Ideal in $\mathbb{Z}^{2\times 2}$.

Definition 17 Sei R ein Ring. Sei $I \trianglelefteq R$.

Für $r \in R$ sei $r + I := \{ r + x : x \in I \}$ die *Restklasse* von r modulo I.

Umgekehrt heißt jedes Element von $r + I$ ein *Repräsentant* von $r + I$.

Seien $r, s \in R$. Es ist $r + I = s + I$ genau dann, wenn $r - s \in I$ ist. Wir schreiben $r \equiv_I s$, um dies auszudrücken. Gesprochen: r ist kongruent zu s modulo I.

Ist R kommutativ und $I = aR$ für ein $a \in R$, so kürzen wir auch noch $r \equiv_{aR} s$ zu $r \equiv_a s$ ab.

Beispiel 18 Sei $R = \mathbb{Z}$. Sei $I = 5\mathbb{Z}$.

Es ist $3 + 5\mathbb{Z} = \{ 3 + 5 \cdot z : z \in \mathbb{Z} \} = -7 + 5\mathbb{Z}$. Also ist $3 \equiv_5 -7$.

Es sind 3 und -7 zwei Repräsentanten von $28 + 5\mathbb{Z}$.

Es gibt in $\mathbb{Z}$ modulo $5\mathbb{Z}$ die Restklassen $0 + 5\mathbb{Z}$, $1 + 5\mathbb{Z}$, $2 + 5\mathbb{Z}$, $3 + 5\mathbb{Z}$ und $4 + 5\mathbb{Z}$.

Definition 19 Sei R ein Ring. Sei $I \trianglelefteq R$.

Sei

$$R/I := \{ r + I : r \in R \}$$

die Menge der Restklassen in R modulo I. Es heißt R/I der *Faktorring* von R modulo I.

Auf R/I werde eine Addition und eine Multiplikation repräsentantenweise definiert. D.h. für $r, s \in R$ sei

$$\begin{array}{lcll} (r+I) & + & (s+I) & := & (r+s)+I \\ (r+I) & \cdot & (s+I) & := & (r\cdot s)+I \end{array}$$

Wir greifen bei dieser Definition auf Repräsentanten r und s der Restklassen zu, um die Summe bzw. das Produkt zu definieren. Daher müssen wir uns noch von der Unabhängigkeit der Repräsentantenwahl überzeugen. Mit anderen Worten, wir müssen die Wohldefiniertheit der Addition und der Multiplikation nachweisen. Seien dazu r, r', s, $s' \in R$ mit $r + I = r' + I$ und mit $s + I = s' + I$ gegeben.

Es ist $(r + s) + I = (r' + s') + I$, da $(r + s) - (r' + s') = (r - r') + (s - s') \in I$ liegt.

Es ist $(r \cdot s) + I = (r' \cdot s') + I$, da $(r \cdot s) - (r' \cdot s') = (r - r') \cdot s + r' \cdot (s - s') \in I$ liegt.

Man verifiziert, daß R/I ein Ring ist: (Ring 1–7) vererben sich von R nach R/I.

Hierbei ist $0_{R/I} = 0_R + I$ und $1_{R/I} = 1_R + I$.

Ist R kommutativ, dann auch R/I.

Konvention 20 Falls aus dem Kontext hervorgeht, daß Restklassen modulo I betrachtet werden, wird auch statt $r + I$ kurz nur r geschrieben.

Beispiel 21 Es ist $\mathbb{Z}/5\mathbb{Z} = \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$.

Unter Verwendung von Konvention 20 dürfen wir auch $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ schreiben.

$(+)$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$(\cdot)$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Häufig verwendet man auch andere Repräsentanten, wie z.B. $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, -2, -1\}$. Man beachte hierbei z.B. $3 + 5\mathbb{Z} = -2 + 5\mathbb{Z}$, oder kurz $3 = -2$, in $\mathbb{Z}/5\mathbb{Z}$.

Definition 22 Sei R ein kommutativer Ring.

Ein Ideal $I \lhd R$ heißt *maximal*, wenn es kein $J \lhd R$ gibt mit $I \subset J$.

Ein maximales Ideal müßte also eigentlich maximales Ideal ungleich R heißen.

Lemma 23 *Sei R ein kommutativer Ring. Sei $I \lhd R$ ein Ideal.*

Es ist R/I ein Körper genau dann, wenn $I \lhd R$ ein maximales Ideal ist.

Beweis. Sei $I \lhd R$ maximal. Sei $r \in R \smallsetminus I$. Wir haben zu zeigen, daß es ein $s \in R$ gibt mit $(r + I) \cdot (s + I) = 1 + I$, i.e. mit $rs - 1 \in I$.

Sei $J := \{\, x + rt \,:\, x \in I,\ t \in R \,\}$. Da $I \subset J \trianglelefteq R$ und da $I \lhd R$ ein maximales Ideal ist, folgt $J = R$. Speziell gibt es $x \in I$ und $s \in R$ mit $x + rs = 1$. Es folgt $rs - 1 \in I$.

Sei umgekehrt $I \lhd R$ nicht maximal. Sei $J \lhd R$ mit $I \subset J$. Sei $x \in J \smallsetminus I$. Dann gibt es kein $y \in R$ mit $(x+I)(y+I) = 1+I$, denn dies *hätte* $1 = xy + z \in J$ zur Folge für ein $z \in I$ und also $J = R$, was *nicht* so ist. ▫

Beispiel 24 Sei $p \in \mathbb{Z}_{\geqslant 2}$ eine Primzahl. Dann ist $p\mathbb{Z} \lhd \mathbb{Z}$ ein maximales Ideal.

Annahme, es gibt ein Ideal $J \lhd \mathbb{Z}$ mit $p\mathbb{Z} \subset J$. Dann ist $J \smallsetminus p\mathbb{Z}$ nicht leer. Diese Menge enthält nicht 0. Ferner gilt für $x \in \mathbb{Z}$, daß genau dann x darin liegt, wenn $-x$ darin liegt. Also ist auch $(J \smallsetminus p\mathbb{Z}) \cap \mathbb{Z}_{\geqslant 1}$ nicht leer.

Sei $x \in (J \smallsetminus p\mathbb{Z}) \cap \mathbb{Z}_{\geqslant 1}$ minimal. Da $x \in J \lhd \mathbb{Z}$ liegt, ist $x \neq 1$. Teilen wir x durch p mit Rest: $x = ps + t$ mit $s \in \mathbb{Z}_{\geqslant 0}$ und $t \in [1, p-1]$. Dann ist auch $ps \in J$ und also $t = x - ps \in (J \smallsetminus p\mathbb{Z}) \cap \mathbb{Z}_{\geqslant 1}$. Folglich ist $s = 0$ und $t = x$. Wir folgern: $x \in [2, p-1]$.

Teilen wir nun umgekehrt p durch x mit Rest, so erhalten wir $p = xa + b$ mit $a \in \mathbb{Z}_{\geqslant 0}$ und $b \in [1, x-1] \subset [1, p-1]$. Es folgt $a \in [1, p-1]$. Da $p,\ x \in J$, folgt $b = p - xa \in (J \smallsetminus p\mathbb{Z}) \cap \mathbb{Z}_{\geqslant 1}$ und $b < x$, im *Widerspruch* zur Minimalität von x.

Definition 25 Sei eine Primzahl $p \in \mathbb{Z}_{\geqslant 2}$ gegeben.

Dann schreiben wir auch kurz $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. ([4])

Beispiel 26

(1) Die Addition und Multiplikation auf $\mathbb{F}_5$ haben wir in Beispiel 21 gesehen.

(2) Es ist $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ kein Körper.

Es darf $\mathbb{Z}/4\mathbb{Z}$ also auch nicht abgekürzt geschrieben werden.

Es ist wegen $4\mathbb{Z} \subset 2\mathbb{Z} \lhd \mathbb{Z}$ das Ideal $4\mathbb{Z} \lhd \mathbb{Z}$ auch nicht maximal.

Additions- und Multiplikationstafel ergeben sich wie folgt.

$(+)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\cdot)$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Der Multiplikationstafel entnehmen wir in der Tat, daß es kein Element x in $\mathbb{Z}/4\mathbb{Z}$ gibt mit $2 \cdot x = 1$ in $\mathbb{Z}/4\mathbb{Z}$.

Definition 27 Sei R ein Ring. Sei $I \trianglelefteqslant R$ ein Ideal.

Der Ringmorphismus

$$\begin{array}{rccc} \rho = \rho_{R,I} : & R & \to & R/I \\ & r & \mapsto & r + I \end{array}$$

heißt *Restklassenmorphismus.*

[4] Körper heißt auf englisch field, historisch bedingt.

Lemma 28 *Seien R und S Ringe. Sei $\varphi : R \to S$ ein Ringmorphismus.*

(1) *Es ist $\varphi(R) \subseteq S$ ein Teilring.*

(2) *Sei* $\mathrm{Kern}(\varphi) := \{\, x \in R : \varphi(x) = 0 \,\}$ *der* Kern *von φ.*
Es ist $\mathrm{Kern}(\varphi)$ *ein Ideal in R.*
Es ist $\mathrm{Kern}(\varphi) = 0$ *genau dann, wenn φ injektiv ist.*

Beweis. Zu (1). Es ist $1_S = \varphi(1_R) \in \varphi(R)$.

Für $r, r' \in R$ ist $\varphi(r) - \varphi(r') = \varphi(r - r') \in \varphi(R)$ und $\varphi(r) \cdot \varphi(r') = \varphi(r \cdot r') \in \varphi(R)$.

Zu (2). Es ist $\varphi(0) = 0$, also $0 \in \mathrm{Kern}(\varphi)$.

Seien $x, x' \in \mathrm{Kern}(\varphi)$, d.h. $\varphi(x) = 0 = \varphi(x')$. Seien $r, r' \in R$.

Es wird $\varphi(rx + r'x') = \varphi(r) \cdot \varphi(x) + \varphi(r') \cdot \varphi(x') = 0$, d.h. $rx + r'x' \in \mathrm{Kern}(\varphi)$.

Es wird $\varphi(xr + x'r') = \varphi(x) \cdot \varphi(r) + \varphi(x') \cdot \varphi(r') = 0$, d.h. $xr + x'r' \in \mathrm{Kern}(\varphi)$.

Also ist $\mathrm{Kern}(\varphi) \trianglelefteq R$.

Ist φ injektiv, dann ist $\mathrm{Kern}(\varphi) = 0$, da $\varphi(0) = 0$ ist und kein weiteres Element auf 0 abgebildet werden kann.

Ist umgekehrt $\mathrm{Kern}(\varphi) = 0$ und sind $r, r' \in R$ mit $\varphi(r) = \varphi(r')$ gegeben, dann ist $\varphi(r - r') = \varphi(r) - \varphi(r') = 0$ und also $r - r' = 0$. Somit ist dann φ injektiv. ▫

Beispiel 29 Sei R ein Ring. Sei $I \trianglelefteq R$ ein Ideal.

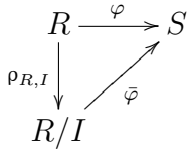
Es ist $\mathrm{Kern}(\rho_{R,I}) = I \trianglelefteq R$ und $\rho_{R,I}(R) = R/I$.

Lemma 30 *Seien R und S Ringe. Sei $\varphi : R \to S$ ein Ringmorphismus.*

Sei $I \trianglelefteq R$ ein Ideal mit $\varphi(I) = 0$, d.h. mit $\varphi(x) = 0$ für $x \in I$.

Dann gibt es den Ringmorphismus $\bar{\varphi} : R/I \to S : r + I \mapsto \bar{\varphi}(r + I) := \varphi(r)$.

Es ist $\bar{\varphi} \circ \rho_{R,I} = \varphi$.



Beweis. Zu zeigen ist die Repräsentantenunabhängigkeit der Definition von $\bar{\varphi}(r+I)$. Seien $r, r' \in R$ mit $r+I = r'+I$ gegeben. Dann ist $r-r' \in I$, also $0 = \varphi(r-r') = \varphi(r)-\varphi(r')$, also $\varphi(r) = \varphi(r')$.

Die von $\bar{\varphi}$ zu erfüllenden Verträglichkeiten ergeben sich aus denen für φ. ▫

Satz 31 (Homomorphiesatz) *Seien R und S Ringe.*

Sei $\varphi : R \to S$ ein Ringmorphismus.

Es ist $\bar{\varphi} : R/\operatorname{Kern}(\varphi) \to \varphi(R) : r + \operatorname{Kern}(\varphi) \mapsto \bar{\varphi}(r + \operatorname{Kern}(\varphi)) := \varphi(r)$ ein Ringisomorphismus.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle \rho_{R,\operatorname{Kern}(\varphi)}}\downarrow & & \uparrow \\ R/\operatorname{Kern}(\varphi) & \xrightarrow[\sim]{\bar{\varphi}} & \varphi(R) \end{array}$$

Beweis. Dank Lemma 30 genügt es zu zeigen, daß $\bar{\varphi}$ injektiv ist.

Sei $r \in R$ mit $0 = \bar{\varphi}(r + \operatorname{Kern}(\varphi)) = \varphi(r)$ gegeben. Dann ist $r \in \operatorname{Kern}(\varphi)$ und also $r + \operatorname{Kern}(\varphi) = 0$.

Somit ist $\operatorname{Kern}(\bar{\varphi}) = 0$, dank Lemma 28.(2) also $\bar{\varphi}$ injektiv. ▫

Beispiel 32 Sei R ein Ring.

Es gibt genau einen Ringmorphismus $\varphi : \mathbb{Z} \to R$. Dieser muß 0 auf 0 schicken, 1 auf 1, und infolgedessen $n = \sum_{i\in[1,n]} 1$ auf $\sum_{i\in[1,n]} 1_R$, sowie $-n = -\big(\sum_{i\in[1,n]} 1\big)$ auf $-\big(\sum_{i\in[1,n]} 1_R\big)$, wobei $n \in \mathbb{Z}_{\geqslant 1}$.

Wir werden noch sehen, daß jedes Ideal in $\mathbb{Z}$ von der Form $k\mathbb{Z}$ ist für ein eindeutiges $k \in \mathbb{Z}_{\geqslant 0}$. Vgl. Beispiel 52.(1) unten.

Insbesondere ist $\operatorname{Kern}(\varphi) = k\mathbb{Z}$ für ein $k \in \mathbb{Z}_{\geqslant 0}$.

Es heißt $\operatorname{char}(R) := k$ die *Charakteristik* von R.

Dank Satz 31 ist $\mathbb{Z}/(\operatorname{char}(R))\mathbb{Z}$ isomorph zum Teilring $\varphi(\mathbb{Z})$ in R.

Wir identifizieren entlang diesem Isomorphismus.

Z.B. ist $\operatorname{char}(\mathbb{Z}) = 0$. Z.B. ist $\operatorname{char}(\mathbb{C}) = 0$. Z.B. ist $\operatorname{char}(\mathbb{F}_5) = 5$. Z.B. ist $\operatorname{char}(\mathbb{F}_5[X]) = 5$. Z.B. ist $\operatorname{char}((\mathbb{Z}/6\mathbb{Z})^{5\times 5}) = 6$.

1.3 Chinesischer Restsatz

Sei R ein Ring.

Bemerkung 33 *Seien I, $J \trianglelefteq R$.*

(1) *Es ist $I + J := \{ a + b : a \in I, b \in J \}$ ein Ideal in R.*

(2) *Es ist $I \cap J$ ein Ideal in R.*

Beweis. Zu (1). Seien r, $r' \in R$ und a, $a' \in I$ und b, $b' \in J$. Wir betrachten die Elemente $a + b$, $a' + b' \in I + J$. Wir erhalten

$$r \cdot (a + b) + r' \cdot (a' + b') \;=\; \underbrace{r \cdot a + r' \cdot a'}_{\in I} + \underbrace{r \cdot b + r' \cdot b'}_{\in J} \;\in\; I + J \;.$$

Analog für die Multiplikation von der anderen Seite. ▫

Satz 34 (Chinesischer Restsatz) *Sei $k \geqslant 1$.*

Seien $I_1, \ldots, I_k \trianglelefteq R$ mit $I_i + I_j = R$ für $i, j \in [1, n]$ mit $i \neq j$.

Dann haben wir den surjektiven Ringmorphismus

$$\begin{array}{ccccccccc} R & \xrightarrow{\varphi} & R/I_1 & \times & R/I_2 & \times & \ldots & \times & R/I_k \\ x & \mapsto & (x + I_1 & , & x + I_2 & , & \ldots & , & x + I_k) \;. \end{array}$$

Sei $I := I_1 \cap I_2 \cap \ldots \cap I_k$. Dann haben wir den Ringisomorphismus

$$\begin{array}{ccccccccc} R/I & \xrightarrow[\sim]{\bar{\varphi}} & R/I_1 & \times & R/I_2 & \times & \ldots & \times & R/I_k \\ x + I & \mapsto & (x + I_1 & , & x + I_2 & , & \ldots & , & x + I_k) \;. \end{array}$$

Beweis. Es ist φ ein Ringmorphismus, da die Addition und Multiplikation von Restklassen repräsentantenweise definiert ist.

Zu zeigen ist, daß φ surjektiv ist.

Für $i, j \in [1, n]$ mit $i \neq j$ gibt es Elemente $a_{i,j} \in I_i$ und $b_{i,j} \in I_j$ mit $a_{i,j} + b_{i,j} = 1$. Somit ist $a_{i,j} + I_i = 0 + I_i$ und $a_{i,j} + I_j = 1 - b_{i,j} + I_j = 1 + I_j$. Es ist also $\varphi(a_{i,j})$ ein Tupel mit Eintrag $0 + I_i$ an Position i und Eintrag $1 + I_j$ an Position j.

Sei $c_j := \prod_{i \in [1,n] \smallsetminus \{j\}} a_{i,j}$ für $j \in [1, n]$. Dann ist $\varphi(c_j) = \prod_{i \in [1,n] \smallsetminus \{j\}} \varphi(a_{i,j})$ ein Tupel mit Eintrag $1 + I_j$ an Position j und Eintrag $0 + I_i$ an Position i für $i \in [1, n] \smallsetminus \{j\}$.

Sei $(d_1 + I_1, \ldots, d_k + I_k)$ ein Element der rechten Seite. Dann liegt $(d_1 + I_1, \ldots, d_k + I_k) = \varphi(d_1 c_1 + \ldots + d_k c_k)$ im Bild von φ.

Nun ist $\mathrm{Kern}(\varphi) = I$. Eine Anwendung des Homomorphiesatzes auf φ liefert also den Ringisomorphismus $\bar{\varphi}$; vgl. Satz 31. ▫

Beispiel 35 Sei $R = \mathbb{Z}$. Sei $I_1 = 3\mathbb{Z}$. Sei $I_2 = 5\mathbb{Z}$.

Es ist $3\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$, da dieses Ideal $3 \cdot 2 + 5 \cdot (-1) = 1$ enthält.

Es ist $3\mathbb{Z} \cap 5\mathbb{Z} = 15\mathbb{Z}$, da eine ganze Zahl genau dann durch 3 und durch 5 teilbar ist, wenn sie durch 15 teilbar ist.

Folglich haben wir dank Chinesischem Restsatz, Satz 34, den Ringisomorphismus

$$\begin{array}{ccccc} \mathbb{Z}/15\mathbb{Z} & \xrightarrow{\sim} & \mathbb{Z}/3\mathbb{Z} & \times & \mathbb{Z}/5\mathbb{Z} \\ z + 15\mathbb{Z} & \mapsto & (z + 3\mathbb{Z} & , & z + 5\mathbb{Z}) \, . \end{array}$$

1.4 Quotientenkörper

Sei R ein Integritätsbereich.

Definition 36 Sei die Relation $(\sim)$ auf der Menge $R \times R^\times$ folgendermaßen erklärt. Für (a, b), $(\tilde{a}, \tilde{b}) \in R \times R^\times$ sei

$$(a, b) \sim (\tilde{a}, \tilde{b}) \ :\Longleftrightarrow \ a \cdot \tilde{b} = \tilde{a} \cdot b \, .$$

Es ist $(\sim)$ eine Äquivalenzrelation.

Sei $\frac{a}{b}$ die Äquivalenzklasse von $(a, b) \in R \times R^\times$.

Sei

$$\mathrm{Quot}(R) \ := \ \{ \, \frac{a}{b} \, : \, a \in R, \ b \in R^\times \, \}$$

der *Quotientenkörper* von R. Auf diesem seien Addition und Multiplikation wie folgt definiert. Sei

$$\begin{array}{rcl} \frac{a}{b} + \frac{a'}{b'} & := & \frac{ab' + a'b}{bb'} \\ \frac{a}{b} \cdot \frac{a'}{b'} & := & \frac{aa'}{bb'} \end{array}$$

für a, $a' \in R$ und b, $b' \in R^\times$.

Wir haben einen injektiven Ringmorphismus $\iota : R \to \mathrm{Quot}(R) : a \mapsto \frac{a}{1}$.

Häufig schreibt man $a := \frac{a}{1} = \iota(a)$ für $a \in R$.

Beweis der Wohldefiniertheit der Addition und der Multiplikation.

Sei $\frac{a}{b} = \frac{\tilde{a}}{\tilde{b}}$ und $\frac{a'}{b'} = \frac{\tilde{a}'}{\tilde{b}'}$ in $\mathrm{Quot}(R)$. Seien also $a\tilde{b} = \tilde{a}b$ und $a'\tilde{b}' = \tilde{a}'b'$.

Für die Wohldefiniertheit der Addition ist $\frac{ab' + a'b}{bb'} \stackrel{!}{=} \frac{\tilde{a}\tilde{b}' + \tilde{a}'\tilde{b}}{\tilde{b}\tilde{b}'}$ zu zeigen. In der Tat wird

$$(ab' + a'b) \cdot \tilde{b}\tilde{b}' \ = \ ab'\tilde{b}\tilde{b}' + a'b\tilde{b}\tilde{b}' \ = \ \tilde{a}b'b\tilde{b}' + \tilde{a}'b\tilde{b}b' \ = \ (\tilde{a}\tilde{b}' + \tilde{a}'\tilde{b}) \cdot bb' \, .$$

Für die Wohldefiniertheit der Multiplikation ist $\frac{aa'}{bb'} \stackrel{!}{=} \frac{\tilde{a}\tilde{a}'}{\tilde{b}\tilde{b}'}$ zu zeigen. In der Tat wird

$$aa' \cdot \tilde{b}\tilde{b}' \ = \ \tilde{a}\tilde{a}' \cdot bb' \, .$$

Die Regeln (Ring 1–7) bestätigt man durch Nachrechnen. Insbesondere ist $0_{\mathrm{Quot}(R)} = \frac{0}{1}$ und $1_{\mathrm{Quot}(R)} = \frac{1}{1}$.

Nach Konstruktion ist $\mathrm{Quot}(R)$ kommutativ.

Für $\frac{a}{b} \in \mathrm{Quot}(R)$ ist schließlich genau dann $\frac{a}{b} = \frac{0}{1} = 0_{\mathrm{Quot}(R)}$, wenn $a \cdot 1 = 0 \cdot b = 0$ ist. Ist also $\frac{a}{b} \neq 0_{\mathrm{Quot}(R)}$, dann ist $a \neq 0$ und also $\frac{b}{a} \in \mathrm{Quot}(R)$. Es folgt $\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1} = 1_{\mathrm{Quot}(R)}$. Somit ist $\mathrm{Quot}(R)$ ein Körper.

Es ist ι ein Ringmorphismus. Es ist $\mathrm{Kern}(\iota) = 0$, und also ist ι injektiv. ▫

Bemerkung 37 Sei S ein kommutativer Ring.

Sei $\varphi : R \to S$ ein Ringmorphismus mit $\varphi(R^\times) \subseteq \mathrm{U}(S)$.

Dann gibt es den Ringmorphismus

$$\hat{\varphi} \ : \ \mathrm{Quot}(R) \to S \ : \ \frac{a}{b} \mapsto \varphi(a) \cdot \varphi(b)^{-1} \ .$$

Beispiel 38

(1) Es ist $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$.

(2) Sei K ein Körper. Es ist

$$K(X) \ := \ \mathrm{Quot}(K[X]) \ = \ \{ \, \frac{f(X)}{g(X)} \ : \ f(X) \in K[X], \ g(X) \in K[X]^\times \, \} \ .$$

(3) Sei K ein Körper von Charakteristik $\mathrm{char}(K) = 0$.

Nach Identifikation ist $\mathbb{Z} \subseteq K$ ein Teilring; vgl. Beispiel 32.

Dank Bemerkung 37 gibt es den Ringmorphismus $\psi : \mathbb{Q} \to K : \frac{a}{b} \mapsto a \cdot b^{-1}$.

Sein Kern ist ein Ideal in $\mathbb{Q}$, liegt also in $\{0, \mathbb{Q}\}$ und kann wegen $\psi(1) = 1$ nicht $\mathbb{Q}$ sein. Also ist $\mathrm{Kern}(\psi) = 0$. D.h. ψ ist injektiv.

Mit anderen Worten, via ψ ist $\mathbb{Q}$ isomorph zu einem Teilring von K.

Wir identifizieren entlang ψ. Dann können wir $\mathbb{Q} \subseteq K$ als Teilring ansehen.

1.5 Noethersche Ringe

Sei R ein kommutativer Ring.

Definition 39 Sei $k \geqslant 0$ und seien $x_1, x_2, \ldots, x_k \in R$ gegeben.

Das von diesen Elementen *erzeugte* Ideal ist

$$(x_1, x_2, \ldots, x_k) \ := \ \{ \, a_1 x_1 + \ldots + a_k x_k \ : \ a_1, \ldots, a_k \in R \, \} \ \trianglelefteq \ R \ .$$

Speziell können wir für $x \in R$ nun alternativ auch $(x) = xR$ schreiben.

Ein Ideal von der Form (x) für ein $x \in R$ heißt auch *Hauptideal* von R.

Es ist übrigens $(\,) = 0 = (0)$.

Definition 40 Ist jedes Ideal in R von der Form $(x_1, x_2, \ldots, x_k)$ für ein $k \geqslant 0$ und gewisse Elemente $x_1, \ldots, x_k \in R$, dann heißt R *noethersch*.

Lemma 41 *Sei R noethersch.*

Sei M eine nichtleere Teilmenge der Menge aller Ideale von R.

Dann enthält M ein bezüglich Inklusion maximales Element.

D.h. es gibt in M ein Element, das in keinem weiteren Element von M echt enthalten ist.

Beweis. Annahme, nicht. Dann finden wir für jedes Element von M ein weiteres Element von M, das jenes echt enthält.

Da $M \neq \emptyset$, gibt es ein $I_0 \in M$. Ausgehend von diesem können wir eine Kette

$$I_0 \;\subset\; I_1 \;\subset\; I_2 \;\subset\; \ldots$$

in M bilden.

Es ist $I := \bigcup_{i \geqslant 0} I_i$ ein Ideal in R. Also ist $I = (x_1, \ldots, x_k)$ für ein $k \geqslant 0$ und gewisse Elemente $x_1, \ldots, x_k \in R$. Da dies nur endlich viele Elemente sind, gibt es ein $\ell \geqslant 0$ mit $x_1, \ldots, x_k \in I_\ell$. Also ist

$$I \;=\; (x_1, \ldots, x_k) \;\subseteq\; I_\ell \;\subset\; I_{\ell+1} \;\subseteq\; I\,.$$

Wir haben einen *Widerspruch*. ▫

Folgender Satz war zu seiner Entstehungszeit um 1890 spektakulär, nicht zuletzt wegen des nichtkonstruktiven Beweises. Ein Kollege Hilberts, Gordan, soll ausgerufen haben, das sei Theologie, keine Mathematik.

Satz 42 (Hilbertscher Basissatz) *Ist R noethersch, dann ist auch $R[X]$ noethersch.*

Beweis. Annahme nicht. Dann gibt es in $R[X]$ ein Ideal I, welches nicht von endlich vielen Elementen erzeugt ist. Jedenfalls ist $I \neq 0$.

Wir wählen ein Element $f_0(X) \in I \setminus \{0\}$ von minimalem Grad. Wir wählen ein Element $f_1(X) \in I \setminus (f_0(X))$ von minimalem Grad. Wir wählen ein Element $f_2(X) \in I \setminus (f_0(X), f_1(X))$ von minimalem Grad. Usf.

Da $I \setminus \{0\} \;\supseteq\; I \setminus (f_0(X)) \;\supseteq\; I \setminus (f_0(X), f_1(X)) \;\supseteq\; \ldots$ ist, ist

$$\deg(f_0(X)) \;\leqslant\; \deg(f_1(X)) \;\leqslant\; \deg(f_2(X)) \;\leqslant\; \ldots$$

Sei a_k der Leitkoeffizient von $f_k(X)$ für $k \geqslant 0$. Die Kette von Idealen

$$(a_0) \subseteq (a_0, a_1) \subseteq (a_0, a_1, a_2) \subseteq \ldots$$

in R hat ein maximales Element, muß also stationär werden, d.h. kann ab einer Stelle nur noch Gleichheiten enthalten; vgl. Lemma 41.

Insbesondere gibt es ein $n \geqslant 1$ mit $a_n \in (a_0, a_1, \ldots, a_{n-1})$.

Wir können also $a_n = \sum_{i \in [0,n-1]} s_i a_i$ schreiben für gewisse $s_i \in R$. Setze

$$g(X) := f_n(X) - \sum_{i \in [0,n-1]} s_i \cdot X^{\deg(f_n(X)) - \deg(f_i(X))} \cdot f_i(X) \, .$$

Nach Konstruktion ist dann $\deg(g(X)) < \deg(f_n(X))$.

Da aber $f_n(X) \in I \setminus (f_0(X), \ldots, f_{n-1}(X))$ liegt und alle anderen Summanden in $(f_0(X), \ldots, f_{n-1}(X))$ liegen, liegt auch $g(X) \in I \setminus (f_0(X), \ldots, f_{n-1}(X))$.

Dies stellt aber einen *Widerspruch* zur Minimalität des Grades von $f_n(X)$ dar. ▫

Definition 43 Sei $k \geqslant 1$. Wir schreiben

$$R[X_1, \ldots, X_k] := R[X_1][X_2] \ldots [X_k]$$

für den Polynomring in den Variablen $X_1, \ldots, X_k$ mit Koeffizienten in R.

Korollar 44 *Sei Q ein Körper.*

Es ist der Polynomring $Q[X_1, \ldots, X_k]$ noethersch.

Beweis. Es ist Q noethersch.

Iterierte Anwendung von Satz 42 liefert also die gewünschte Aussage. ▫

1.6 Euklidische Ringe, Hauptidealbereiche, faktorielle Ringe

Sei R ein Integritätsbereich. Sei $K := \mathrm{Quot}(R)$ sein Quotientenkörper.

Bemerkung 45 *Seien $x, y \in R^\times$.*

Es ist genau dann $(x) = (y)$, wenn es ein $u \in \mathrm{U}(R)$ gibt mit $xu = y$.

Insbesondere ist genau dann $(x) = (1)$, wenn $x \in \mathrm{U}(R)$ liegt.

Beweis. Gebe es ein $u \in \mathrm{U}(R)$ gibt mit $xu = y$. Dann ist $y = xu \in (x)$, und also auch $(y) \subseteq (x)$. Ferner ist auch $x = yu^{-1} \in (y)$, und also auch $(x) \subseteq (y)$. Zusammen ist also $(x) = (y)$.

Sei umgekehrt $(x) = (y)$. Wegen $y \in (x)$ gibt es ein $u \in R$ mit $y = xu$. Wir haben $u \overset{!}{\in} \mathrm{U}(R)$ zu zeigen.

Wegen $x \in (y)$ gibt es ein $v \in R$ mit $x = yv$. Es folgt $x = yv = xuv$. Da R ein Integritätsbereich ist und da $x \neq 0$ ist, folgt $uv = 1$. Also ist $u \in \mathrm{U}(R)$. ▫

Definition 46 Eine Abbildung $d : R^\times \to \mathbb{Z}_{\geqslant 0}$ heißt *Gradfunktion* auf R, falls für $x \in R$ und $y \in R^\times$ Elemente $q, r \in R$ existieren mit

$$x \;=\; y \cdot q + r \;,$$

wobei $(r = 0)$ oder $(r \neq 0$ und $d(r) < d(y))$ ist.

Kurz, wobei $r = 0$ oder aber $d(r) < d(y)$ ist.

Der Integritätsbereich R, zusammen mit einer Gradfunktion d auf R, heißt dann *euklidischer Ring.*

Für $x \in R$ heißt $d(x)$ auch der *Grad* von x.

Beispiel 47

(1) Es ist $d : \mathbb{Z}^\times \to \mathbb{Z}_{\geqslant 0} : x \mapsto d(x) := |x|$ eine Gradfunktion auf $\mathbb{Z}$, wie Division mit Rest zeigt.

Insbesondere ist mit dieser Gradfunktion $\mathbb{Z}$ ein euklidischer Ring.

(2) Sei Q ein Körper.

Es ist $d : Q[X]^\times \to \mathbb{Z}_{\geqslant 0} : f(X) \mapsto d(f(X)) := \deg(f(X))$ eine Gradfunktion auf $Q[X]$, wie Polynomdivision mit Rest zeigt.

Insbesondere ist mit dieser Gradfunktion $Q[X]$ ein euklidischer Ring.

(3) Wir betrachten den Teilring $\mathbb{Z}[\mathrm{i}] := \{\, a + b\mathrm{i} \;:\; a, b \in \mathbb{Z} \,\} \subseteq \mathbb{C}$.

Wir wollen nachweisen, daß $d : \mathbb{Z}[\mathrm{i}]^\times \to \mathbb{Z}_{\geqslant 0} : z \mapsto d(z) := |z|^2$ eine Gradfunktion ist.

Für $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ ist $d(a + b\mathrm{i}) = |a + b\mathrm{i}|^2 = a^2 + b^2 \in \mathbb{Z}_{\geqslant 0}$.

Seien nun $x \in \mathbb{Z}[\mathrm{i}]$ und $y \in \mathbb{Z}[\mathrm{i}]^\times$ gegeben. Schreibe $u := x/y \in \mathbb{C}$. Schreibe $u = s + \mathrm{i}t$ mit $s, t \in \mathbb{R}$.

Durch Runden erhalten wir $s' \in \mathbb{Z}$ mit $|s - s'| \leqslant 1/2$ und $t' \in \mathbb{Z}$ mit $|t - t'| \leqslant 1/2$.

Sei $q := s' + \mathrm{i}t' \in \mathbb{Z}[\mathrm{i}]$. Es ist $|u - q|^2 = (s - s')^2 + (t - t')^2 \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$.

Es wird $r := x - yq = yu - yq = y(u - q)$. Also ist $|r|^2 = |y|^2 \cdot |u - q|^2 < |y|^2$. Falls $r \neq 0$, dann ist $d(r) = |r|^2 < |y|^2 = d(y)$, wie verlangt.

Definition 48 Der Integritätsbereich R heißt *Hauptidealbereich*, wenn jedes Ideal in R ein Hauptideal ist.

Bemerkung 49 Jeder Hauptidealbereich ist noethersch.

Beispiel 50 Ist Q ein Körper, dann hat Q nur die Ideale (0) und (1). Dann ist Q also ein Hauptidealbereich.

Lemma 51 *Sei R, zusammen mit einer Gradfunktion $d : R^\times \to \mathbb{Z}_{\geqslant 0}$, ein euklidischer Ring.*

Dann ist R ein Hauptidealbereich.

Beweis. Sei $I \trianglelefteq R$ ein Ideal. O.E. ist $I \neq 0$.

Es ist $\emptyset \neq d(I \smallsetminus \{0\}) \subseteq \mathbb{Z}_{\geqslant 0}$.

Wir können also ein Element $y \in I \smallsetminus \{0\}$ wählen mit $d(y)$ minimal.

Da $y \in I$, ist auch $(y) \subseteq I$. Wir behaupten $(y) \stackrel{!}{=} I$.

Annahme, $(y) \subset I$. Wähle $x \in I \smallsetminus (y)$. Wir finden $q,\, r \in R$ mit $x = yq + r$ und mit $r = 0$ oder aber $d(r) < d(y)$.

Da auch $r = x - yq \in I$ liegt, muß wegen der Minimalität von $d(y)$ nun $r = 0$ sein.

Dann aber ist $x = yq \in (y)$. Wir haben einen *Widerspruch.* ▫

Beispiel 52 Wir setzen Beispiel 47 fort.

(1) Es ist $\mathbb{Z}$ ein Hauptidealbereich.

(2) Ist Q ein Körper, so ist der Polynomring $Q[X]$ ein Hauptidealbereich.

(3) Es ist $\mathbb{Z}[\mathrm{i}]$ ein Hauptidealbereich.

(4) Es ist $\mathbb{Z}[\mathrm{i}\sqrt{5}] = \{\, a + b\mathrm{i}\sqrt{5} \,:\, a,\, b \in \mathbb{Z} \,\}$ kein Hauptidealbereich.

Schreibe hierzu $\gamma := \mathrm{i}\sqrt{5}$. Es ist also $\gamma^2 = -5$.

Wir behaupten, daß das Ideal $(2, 1+\gamma) \trianglelefteq \mathbb{Z}[\gamma]$ kein Hauptideal ist.

Annahme, doch. Dann gibt es ein Element $x \in \mathbb{Z}[\gamma]$ mit $(x) = (2, 1+\gamma)$.

Schreibe $x = a + b\gamma$ mit $a,\, b \in \mathbb{Z}$.

Wegen $2 \in (x)$ ist also $2 = xy$ für ein $y \in \mathbb{Z}[\gamma]$. Schreibe $y = c + d\gamma$ mit $c,\, d \in \mathbb{Z}$. Es ist auch $4 = |2|^2 = |x|^2 \cdot |y|^2 = (a^2 + 5b^2)(c^2 + 5d^2)$. Somit ist $a^2 + 5b^2$ ein Teiler von 4 in $\mathbb{Z}$. Folglich ist $b = 0$ und $a \in \{1, 2, -1, -2\}$.

Somit ist $(x) = (1)$ oder $(x) = (2)$.

Falls $(2) = (x) = (2, 1+\gamma)$ ist, dann ist $1+\gamma$ ein Vielfaches von 2 in $\mathbb{Z}[\gamma]$. Dies trifft aber nicht zu.

Falls $(1) = (x) = (2, 1+\gamma)$ ist, dann ist $1 = 2u + (1+\gamma)v$ für gewisse $u,\, v \in \mathbb{Z}[\gamma]$. Schreibe $u = e + f\gamma$ und $v = g + h\gamma$ mit $e,\, f,\, g,\, h \in \mathbb{Z}$. Es wird

$$1 \;=\; 2(e+f\gamma)+(1+\gamma)(g+h\gamma) \;=\; 2e+2f\gamma+g+h\gamma+g\gamma-5h \;=\; (2e+g-5h)+(2f+h+g)\gamma\ .$$

Koeffizientenvergleich gibt $1 = 2e + g - 5h$ und $0 = 2f + h + g$ in $\mathbb{Z}$. Modulo 2 folgt $1 \equiv_2 g + h \equiv_2 0$. Das geht nicht.

Keiner der beiden Fälle tritt also ein. Wir haben einen *Widerspruch*.

Definition 53 Seien $a,\, b \in R$.

(1) Es heißen a und b *assoziiert*, wenn $(a) = (b)$ ist, d.h. wenn es ein $u \in \mathrm{U}(R)$ gibt mit $au = b$.

(2) Es heißt a ein *Teiler* von b, wenn $(a) \supseteq (b)$ ist, d.h. wenn es ein $x \in R$ gibt mit $ax = b$.

Wir sagen diesenfalls auch, *a teilt b*, und wir schreiben $a|b$.

Definition 54 Sei $a \in R^\times \smallsetminus \mathrm{U}(R)$. Es ist also a ungleich 0 und nicht invertierbar.

(1) Es heißt *a irreduzibel*, wenn für $x,\, y \in R$ aus $(x \cdot y) = (a)$ folgt, daß $(x) = (a)$ oder $(y) = (a)$ ist.

(2) Es heißt *a prim*, wenn für $x,\, y \in R$ aus $(x \cdot y) \subseteq (a)$ folgt, daß $(x) \subseteq (a)$ oder $(y) \subseteq (a)$ ist.

Bemerkung 55 *Sei $a \in R^\times \smallsetminus \mathrm{U}(R)$.*

Wir wollen die in Definition 54 eingeführten Begriffe noch auf elementarem Wege zum Ausdruck bringen.

(1) *Seien $x,\, y \in R$. Ist $a = x \cdot y$ und ist $(a) = (x)$, dann ist $(1) = (y)$, d.h. dann ist $y \in \mathrm{U}(R)$.*

(2) *Es ist a genau dann irreduzibel, wenn alle Teiler von a von der Form u oder ua sind mit $u \in \mathrm{U}(R)$.*

(3) *Es ist a genau dann prim, wenn für $x,\, y \in R^\times$ aus $a|x \cdot y$ folgt, daß $a|x$ oder $a|y$ gilt.*

(4) *Es ist a genau dann prim, wenn $R/(a)$ ein Integritätsbereich ist.*

(5) *Ist a prim, dann ist a irreduzibel.*

Beweis. Zu (1). Aus $(a) = (x)$ folgt, daß $x = a \cdot z$ ist für ein $z \in R$. Es folgt $a = x \cdot y = a \cdot z \cdot y$. Da $a \in R^\times$ liegt und R ein Integritätsbereich ist, folgt $1 = z \cdot y$. Also ist $y \in \mathrm{U}(R)$, d.h. $(1) = (y)$.

Zu (2).

Sei zum einen a irreduzibel. Sei $a = x \cdot y$ mit $x,\ y \in R$. Dann ist $(a) = (x)$ oder $(a) = (y)$.

Falls $(a) = (x)$ ist, dann ist $x = ua$ für ein $u \in \mathrm{U}(R)$.

Falls $(a) = (y)$ ist, dann folgt aus $a = x \cdot y$ mit (1), daß $x \in \mathrm{U}(R)$ ist, wie gewünscht.

Sei zum anderen jeder Teiler von a von der Form u oder ua sind mit $u \in \mathrm{U}(R)$.

Seien $x,\ y \in R$ gegeben mit $(x \cdot y) = (a)$. Dann ist x ein Teiler von a.

Falls $x \in \mathrm{U}(R)$, dann ist $(y) = (x \cdot y) = (a)$.

Falls $x = ua$ mit $u \in \mathrm{U}(R)$, dann ist $(x) = (u \cdot a) = (a)$.

Also ist a irreduzibel.

Zu (5). Sei a prim. Seien $x,\ y \in R^\times$ mit $(x \cdot y) = (a)$ gegeben. Dann ist $(x \cdot y) \subseteq (a)$. Wegen a prim folgt $(x) \subseteq (a)$ oder $(y) \subseteq (a)$.

Falls $(x) \subseteq (a)$, dann stellen wir fest, daß $(a) = (x \cdot y) \subseteq (x)$ ist und folgern $(x) = (a)$.

Falls $(y) \subseteq (a)$, dann stellen wir fest, daß $(a) = (x \cdot y) \subseteq (y)$ ist und folgern $(y) = (a)$. ▫

Beispiel 56

(1) Sei $R = \mathbb{Z}$. Seien $a,\ b \in \mathbb{Z}^\times \smallsetminus \mathrm{U}(\mathbb{Z}) = \mathbb{Z} \smallsetminus \{-1, 0, 1\}$.

Es sind a und b genau dann assoziiert, wenn $a = b$ oder $a = -b$ ist.

Es ist a genau dann irreduzibel, wenn es prim ist. Dies ist bekannt, wird aber unten nochmal aus der Tatsache folgen, daß $\mathbb{Z}$ ein Hauptidealbereich ist; vgl. Lemma 58.

(2) Sei Q ein Körper. Sei $R = Q[X]$. Seien $f(X),\ g(X) \in Q[X]^\times \smallsetminus \mathrm{U}(Q[X])$. Mit anderen Worten, seien $f(X)$ und $g(X)$ Polynome von Grad $\geqslant 1$ mit Koeffizienten in Q.

Es sind $f(X)$ und $g(X)$ genau dann assoziiert, wenn es ein $a \in Q^\times$ gibt mit $a \cdot f(X) = g(X)$.

Es ist $f(X)$ genau dann irreduzibel, wenn es prim ist. Dies wird unten aus der Tatsache folgen, daß $Q[X]$ ein Hauptidealbereich ist; vgl. Lemma 58.

(3) Sei $R = \mathbb{Z}[\mathrm{i}\sqrt{5}]$. Darin ist 2 irreduzibel, aber nicht prim.

Schreiben wir wieder $\gamma := \mathrm{i}\sqrt{5}$.

Zunächst ist 2 weder gleich 0 noch eine Einheit in $\mathbb{Z}[\gamma]$.

Wir haben in Beispiel 52.(4) schon gesehen, daß die einzigen Teiler von 2 gegeben sind durch 1, 2, -1, -2. Also ist 2 irreduzibel.

Aber $(1+\gamma)(1-\gamma) = 1+5 = 6$ ist durch 2 teilbar, ohne daß $1+\gamma$ oder $1-\gamma$ durch 2 teilbar wäre. Also ist 2 nicht prim.

Definition 57 Es heißt der Integritätsbereich R *faktoriell*, wenn die folgenden Bedingungen $(1, 2)$ gelten.

(1) Es ist R noethersch.

(2) Sei $a \in R^\times \smallsetminus \mathrm{U}(R)$. Es ist a genau dann irreduzibel, wenn es prim ist.

Lemma 58 *Ist R ein Hauptidealbereich, dann ist R faktoriell.*

Beweis. Es genügt, die direkte Implikation in Definition 57.(2) zu zeigen; vgl. Bemerkungen 49 und 55.(5).

Sei $a \in R^\times \smallsetminus \mathrm{U}(R)$ irreduzibel. Wir haben zu zeigen, daß a prim ist.

Seien $x, y \in R$ mit $xy \in (a)$ gegeben. Es gibt also ein $d \in R$ mit $xy = ad$.

Sei $x \notin (a)$. Wir haben zu zeigen, daß $y \overset{!}{\in} (a)$ liegt.

Da R ein Hauptidealbereich ist, gibt es ein $b \in R$ mit $(a, x) = (b)$.

Da $a \in (b)$ liegt, gibt es ein $c \in R$ mit $a = b \cdot c$.

Da a irreduzibel ist, ist $(a) = (b)$ oder $(a) = (c)$.

Da $x \notin (a)$ liegt, ist aber $(a) \subset (a, x) = (b)$. Folglich muß $(a) = (c)$ sein. Wegen $a = b \cdot c$ impliziert dies $b \in \mathrm{U}(R)$ dank Bemerkung 55.(1). Dann aber ist $(a, x) = (b) = (1)$. Wähle $s, t \in R$ mit $sa + tx = 1$. Damit wird

$$y \;=\; 1 \cdot y \;=\; (sa + tx)y \;=\; say + tad \;\in\; (a)\ .$$

□

Lemma 59 *Sei R faktoriell. Sei $a \in R^\times$.*

(1) *Es gibt $k \geqslant 0$ und prime Elemente $p_1, \ldots, p_k$ in R sowie eine Einheit $u \in \mathrm{U}(R)$ mit*

$$a \;=\; u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k\ .$$

Eine solche Faktorisierung heißt auch Primfaktorzerlegung.

(2) *Seien zwei Primfaktorzerlegungen von a gegeben:*

Seien $k \geqslant 0$ und prime Elemente $p_1, \ldots, p_k$ gegeben und eine Einheit $u \in \mathrm{U}(R)$.

Seien $\ell \geqslant 0$ und prime Elemente $q_1, \ldots, q_\ell$ gegeben und eine Einheit $v \in \mathrm{U}(R)$.

Sei mit diesen

$$a \;=\; u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k \;=\; v \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_\ell\ .$$

Dann ist $k = \ell$. Ferner gibt es eine bijektive Abbildung $\sigma : \{1, \ldots, k\} \to \{1, \ldots, k\}$ mit $(p_i) = (q_{\sigma(i)})$ für $1 \leqslant i \leqslant k$.

Mit anderen Worten, bis auf Reihenfolge und Assoziiertheit ist die Primfaktorzerlegung von a eindeutig.

Beweis. Zu (1). Sei H die Menge aller Hauptideale von R.

Sei $M \subseteq H$ die Teilmenge der Hauptideale von R, die von einem Element aus $R^\times \smallsetminus \mathrm{U}(R)$ erzeugt werden, das keine Primfaktorzerlegung besitzt. Wir haben $M \stackrel{!}{=} \emptyset$ zu zeigen.

Annahme, es ist M nicht leer. Wähle ein maximales (a) in M, möglich, da R noethersch ist; vgl. Lemma 41. Da $(a) \in M$, ist a nicht prim. Da R faktoriell ist, ist a folglich auch nicht irreduzibel. Schreibe $a = xy$ mit $x,\, y \in R^\times \smallsetminus \mathrm{U}(R)$. Es ist $(a) = (xy) \subseteq (x)$ und $(a) = (xy) \subseteq (y)$. Es kann nicht $(a) = (x)$ sein, da $(y) \neq (1)$ ist; vgl. Bemerkung 55.(1). Es kann nicht $(a) = (y)$ sein, da $(x) \neq (1)$ ist; vgl. Bemerkung 55.(1).

Also ist $(a) \subset (x)$ und $(a) \subset (y)$. Folglich liegt weder (x) noch (y) in M. Somit haben sowohl x als auch y eine Primfaktorzerlegung. Dann hat aber auch $a = xy$ eine Primfaktorzerlegung. Wir haben einen *Widerspruch.*

Skizze zu (2). O.E. ist $k \leqslant \ell$.

Es ist

$$(p_1 \cdot p_2 \cdot \ldots \cdot p_k) \;=\; (q_1 \cdot q_2 \cdot \ldots \cdot q_\ell)\,.$$

Da p_k prim ist, teilt p_k das Element q_i für ein $i \in [1, \ell]$. Nach Umsortierung der Faktoren rechts teilt p_k das Element q_ℓ. Aus q_ℓ irreduzibel und $p_k \notin \mathrm{U}(R)$ folgt $(p_k) = (q_\ell)$. Ferner folgt

$$(p_1 \cdot p_2 \cdot \ldots \cdot p_{k-1}) \;=\; (q_1 \cdot q_2 \cdot \ldots \cdot q_{\ell-1})\,.$$

Nach Umsortierung teilt nun p_{k-1} das Element $q_{\ell-1}$. Aus $q_{\ell-1}$ irreduzibel und $p_{k-1} \notin \mathrm{U}(R)$ folgt $(p_{k-1}) = (q_{\ell-1})$.

Usf.

Es resultiert

$$R \;=\; (1) \;=\; (q_1 \cdot q_2 \cdot \ldots \cdot q_{\ell-k})\,.$$

Wegen $q_i \notin \mathrm{U}(R)$ für $i \in [1, \ell]$ ist schließlich auch noch $\ell = k$. ▫

Definition 60 Sei R faktoriell. Sei $p \in R$ prim.

(1) Für $a \in R^\times$ sei $\mathrm{v}_p(a) := \max\{\, k \in \mathbb{Z}_{\geqslant 0} \,:\, a \in (p^k) \,\}$ die *Bewertung* von a bei p ([5]).

(2) Sei $x \in K^\times$. Schreibe $x = \frac{a}{b}$ mit $a,\, b \in R^\times$. Sei

$$\mathrm{v}_p(x) \;:=\; \mathrm{v}_p(a) - \mathrm{v}_p(b)$$

die *Bewertung* von x bei p.

Diese hängt nicht von der gewählten Darstellung von x als Bruch ab.

[5] Engl. valuation.

(3) Sei zudem $\mathrm{v}_p(0) := \infty$. Dabei sei $\infty + z = \infty$ für $z \in \mathbb{Z}_{\geqslant 0}$ und $\infty + \infty = \infty$.

Bemerkung 61 Sei R faktoriell.

(1) Sei $P \subseteq R^\times \smallsetminus \mathrm{U}(R) \subseteq R$ eine Teilmenge, die aus Primelementen besteht, und so, daß jedes Primelement von R zu genau einem Element von P assoziiert ist.

Sei $x \in K^\times$ gegeben. Wir erhalten

$$x \;=\; u \cdot \prod_{p \in P} p^{\mathrm{v}_p(x)} \;,$$

wobei $u \in \mathrm{U}(R)$ und wobei in diesem Produkt fast alle Faktoren gleich 1 sind, wodurch es tatsächlich ein endliches Produkt ist. Dies folgt aus Lemma 59.(1).

(2) Ein Element $x \in K$ ist genau dann in R, wenn $\mathrm{v}_p(x) \geqslant 0$ ist für alle $p \in R$ prim.

(3) Ein Element $x \in K$ ist genau dann in $\mathrm{U}(R)$, wenn $\mathrm{v}_p(x) = 0$ ist für alle $p \in R$ prim.

(4) Seien $x,\, y \in K$.

Es ist $\mathrm{v}_p(x \cdot y) = \mathrm{v}_p(x) + \mathrm{v}_p(y)$.

Es ist $\mathrm{v}_p(x + y) \geqslant \min\{\mathrm{v}_p(x), \mathrm{v}_p(y)\}$, mit Gleichheit im Falle $\mathrm{v}_p(x) \neq \mathrm{v}_p(y)$.

Definition 62 Sei R faktoriell. Sei $k \geqslant 1$ und $x_1, \ldots, x_k \in R$.

Es heißt $g \in R$ ein *größter gemeinsamer Teiler* von $x_1, \ldots, x_k$, falls es die folgenden Eigenschaften (i, ii) erfüllt.

(i) Es ist g ein Teiler von x_i für $i \in [1, k]$.

(ii) Ist $y \in R$ ein Teiler von x_i für $i \in [1, k]$, dann ist y ein Teiler von g.

Sind $g,\, \tilde{g} \in R$ größte gemeinsame Teiler von $x_1, \ldots, x_k$, dann sind g und $\tilde{g}$ assoziiert.

Bemerkung 63 Sei R faktoriell. Sei $P \subseteq R$ eine Teilmenge, die aus Primelementen besteht, und so, daß jedes Primelement von R zu genau einem Element von P assoziiert ist.

Sei $k \geqslant 1$ und $x_1, \ldots, x_k \in R$, nicht alle gleich 0.

Dann ist

$$\mathrm{ggT}(x_1, \ldots, x_k) \;:=\; \prod_{p \in P} p^{\min\{\, \mathrm{v}_p(x_i) \,:\, i \in [1,k]\,\}} \;\in\; R$$

ein größter gemeinsamer Teiler von $x_1, \ldots, x_k$.

Konvention 64

(1) In $\mathbb{Z}$ wollen wir P aus positiven Primelementen wählen und also den größten gemeinsamen Teiler $\geqslant 0$ wählen.

(2) Sei Q ein Körper. In $Q[X]$ wollen wir P aus normierten Primelementen wählen und also den größten gemeinsamen Teiler normiert oder 0 wählen.

Beispiel 65 In $\mathbb{Z}$ ist $-12 = (-1) \cdot 2^2 \cdot 3^1 \cdot 5^0$ und $80 = 1 \cdot 2^4 \cdot 3^0 \cdot 5^1$.

Also ist $\mathrm{ggT}(-12, 80) = 2^{\min\{2,4\}} \cdot 3^{\min\{1,0\}} \cdot 5^{\min\{0,1\}} = 2^2 \cdot 3^0 \cdot 5^0 = 4$.

Bemerkung 66 *Sei R ein Hauptidealbereich, insbesondere also faktoriell; vgl. Lemma 58.*

Sei $k \geqslant 1$ und seien $x_1, \ldots, x_k \in R$ gegeben. Sei g ein größter gemeinsamer Teiler von $x_1, \ldots, x_k$.

Dann ist $(g) = (x_1, \ldots, x_k)$.

Beweis. Da R ein Hauptidealbereich ist, können wir $\tilde{g} \in R$ wählen mit $(\tilde{g}) = (x_1, \ldots, x_k)$.

Da g dank Eigenschaft (i) ein Teiler von x_i ist für $i \in [1, k]$, ist $(\tilde{g}) = (x_1, \ldots, x_k) \subseteq (g)$.

Da $\tilde{g}$ nach Konstruktion ein Teiler von x_i ist für $i \in [1, k]$, ist $\tilde{g}$ ein Teiler von g dank Eigenschaft (ii). Also ist $(\tilde{g}) \supseteq (g)$.

Somit ist $(g) = (\tilde{g}) = (x_1, \ldots, x_k)$. ▫

Beispiel 67 In $\mathbb{Z}$ ist $\mathrm{ggT}(-12, 80) = 4$. Als Ideale von $\mathbb{Z}$ wird also $(-12, 80) = (4)$.

Direkt betrachtet folgt $(-12, 80) \subseteq (4)$ aus $4|(-12)$ und $4|80$, und es folgt $(-12, 80) \supseteq (4)$ aus $(-12) \cdot (-7) + 80 \cdot (-1) = 4$.

Bemerkung 68 Sei R ein euklidischer Ring, mit Gradfunktion d. Dann ist R ein Hauptidealbereich, und also faktoriell. Sei $P \subseteq R$ eine Teilmenge wie in Bemerkung 61.(1).

Seien $x, y \in R^\times$ gegeben mit $d(x) \geqslant d(y)$.

Wir wollen $\mathrm{ggT}(x, y)$ bestimmen, bis auf Assoziiertheit.

Schreibe $x = yq + r$, wobei $q, r \in R$ mit $r = 0$ oder mit $d(r) < d(y)$.

Falls $r = 0$ ist, dann ist

$$(\mathrm{ggT}(x, y)) \;=\; (y)\ .$$

Falls $r \neq 0$ ist, dann ist $(x, y) = (y, x) = (y, yq + r) = (y, r)$, und also

$$(\mathrm{ggT}(x, y)) \;=\; (\mathrm{ggT}(y, r))\ ,$$

wobei $d(x) \geqslant d(y) > d(r)$.

Dieser Schritt läßt sich iterieren. Die Iteration bricht nach endlich vielen Schritten ab und heißt auch Euklidischer Algorithmus. Dieser kommt insbesondere dann zum Einsatz, wenn man nicht, oder nicht so einfach, über Primfaktorzerlegungen verfügt.

Das Ergebnis steht dann in der Form $(\mathrm{ggT}(x,y)) = (g)$ da, für ein $g \in R$. Mit anderen Worten, es ist $\mathrm{ggT}(x,y) = g \cdot u$ für ein $u \in \mathrm{U}(R)$.

Beispiel 69 Sei $R = \mathbb{Z}$. Es ist $\mathbb{Z}$ ein euklidischer Ring; vgl. Beispiel 47.(1).

Wir können $\mathrm{ggT}(60,42)$ also unter Verwendung von Bemerkung 68 bestimmen.

Es ist $60 = 42 + 18$. Also ist $\mathrm{ggT}(60,42) = \mathrm{ggT}(42,18)$.

Es ist $42 = 18 \cdot 2 + 6$. Also ist $\mathrm{ggT}(42,18) = \mathrm{ggT}(18,6)$.

Es ist $18 = 6 \cdot 3 + 0$. Also ist $\mathrm{ggT}(18,6) = \mathrm{ggT}(6,0) = 6$.

Insgesamt ist $\mathrm{ggT}(60,42) = 6$.

Mit der obigen Formel erhalten wir folgendes.

Es ist $60 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0$. Es ist also $\mathrm{v}_2(60) = 2$, $\mathrm{v}_3(60) = 1$, $\mathrm{v}_5(60) = 1$, $\mathrm{v}_7(60) = 0$ und $\mathrm{v}_p(60) = 0$ für jede andere Primzahl p.

Es ist $42 = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^1$. Es ist also $\mathrm{v}_2(42) = 1$, $\mathrm{v}_3(42) = 1$, $\mathrm{v}_5(42) = 0$, $\mathrm{v}_7(42) = 1$ und $\mathrm{v}_p(42) = 0$ für jede andere Primzahl p.

Es folgt $\mathrm{ggT}(60,42) = 2^{\min\{2,1\}} \cdot 3^{\min\{1,1\}} \cdot 5^{\min\{1,0\}} \cdot 7^{\min\{0,1\}} = 6$.

Definition 70 Sei R faktoriell. Sei $p \in R$ prim.

Sei $f(X) = \sum_{i \geqslant 0} a_i X^i \in K[X]$. Sei

$$\mathrm{v}_p(f(X)) \;:=\; \min\{\, \mathrm{v}_p(a_i) \;:\; i \geqslant 0 \,\}$$

die *Bewertung* von $f(X)$ bei p.

Es ist $\mathrm{v}_q(f(X)) \geqslant 0$ für alle primen $q \in R$ genau dann, wenn $f(X) \in R[X]$ liegt.

Es heißt $f(X)$ *primitiv*, wenn $\mathrm{v}_q(f(X)) = 0$ ist für alle primen $q \in R$.

> Wir wissen noch nicht, daß $R[X]$ faktoriell ist. Wüßten wir dies, so bräuchten wir für $\mathrm{v}_p(f(X))$ keine eigene Definition, sondern könnten Definition 60.(2) anwenden, da p auch in $R[X]$ prim ist und da $K[X] \subseteq K(X) = \mathrm{Quot}(R[X])$ liegt. Siehe auch Satz 75 unten.

Beispiel 71 Sei $R = \mathbb{Z}$ und also $K = \mathbb{Q}$.

(1) Es ist $\mathrm{v}_2(X^2 + \frac{1}{40}X - 12) = -3$.

(2) Es ist $2X^2 + 6X + 9$ primitiv.

Bemerkung 72 Sei R faktoriell. Sei $f(X) \in R[X]^\times$.

Sei $g \in R$ ein größter gemeinsamer Teiler der Koeffizienten von $f(X)$.

Dann ist $g^{-1}f(X) \in R[X]$ primitiv. Es ist $f(X) = g \cdot (g^{-1}f(X))$.

Ist insbesondere $\deg(f(X)) \geqslant 1$ und $f(X)$ irreduzibel in $R[X]$, dann ist $g \in \mathrm{U}(R)$ und also $f(X)$ primitiv.

Lemma 73 *Sei R faktoriell. Sei $p \in R$ prim.*

Seien $f(X) = \sum_{i\geqslant 0} a_i X^i$ und $g(X) = \sum_{i\geqslant 0} b_i X^i$ aus $K[X]$.

Es ist $\mathrm{v}_p(f(X) \cdot g(X)) = \mathrm{v}_p(f(X)) + \mathrm{v}_p(g(X))$.

Beweis. O.E. ist $f(X) \neq 0$ und $g(X) \neq 0$.

Da für $c,\, d \in R^\times$ zum einen $\mathrm{v}_p((c\cdot f(X))\cdot(d\cdot g(X))) = \mathrm{v}_p(f(X)\cdot g(X)) + \mathrm{v}_p(c\cdot d)$ ist und zum anderen $\mathrm{v}_p(c\cdot f(X))+\mathrm{v}_p(d\cdot g(X)) = \mathrm{v}_p(f(X))+\mathrm{v}_p(g(X))+\mathrm{v}_p(c\cdot d)$ ist, dürfen wir unter Verwendung geeigneter solcher Faktoren c und d annehmen, daß $f(X),\, g(X) \in R[X]$ liegen.

Wir schreiben $s := \mathrm{v}_p(f(X))$ und $t := \mathrm{v}_p(g(X))$.

Da p^{s+t} ein Teiler von $f(X)\cdot g(X)$ ist, folgt $\mathrm{v}_p(f(X)\cdot g(X)) \geqslant s+t$.

Wir haben $\mathrm{v}_p(f(X)\cdot g(X)) \overset{!}{\leqslant} s+t$ zu zeigen. Mit anderen Worten, wir haben zu zeigen, daß $f(X)\cdot g(X)$ einen Koeffizienten mit Bewertung $s+t$ bei p hat.

Sei $i_0 \geqslant 0$ minimal mit $\mathrm{v}_p(a_{i_0}) = s$. Dann ist $\mathrm{v}_p(a_i) > s$ für $i \in [0, i_0-1]$ und $\mathrm{v}_p(a_i) \geqslant s$ für $i \geqslant i_0+1$.

Sei $j_0 \geqslant 0$ minimal mit $\mathrm{v}_p(b_{j_0}) = t$. Dann ist $\mathrm{v}_p(b_j) > t$ für $j \in [0, j_0-1]$ und $\mathrm{v}_p(b_j) \geqslant t$ für $j \geqslant j_0+1$.

Sei $k_0 := i_0 + j_0$. Es ist der Koeffizient von $f(X)\cdot g(X) = \sum_{k\geqslant 0} c_k X^k$ bei X^{k_0} gleich

$$c_{k_0} \;=\; \left(\sum_{i\in[0,i_0-1]} a_i b_{k_0-i}\right) + a_{i_0}b_{j_0} + \left(\sum_{i\in[i_0+1,k_0]} a_i b_{k_0-i}\right)\,.$$

Dabei ist $\mathrm{v}_p\Big(\sum_{i\in[0,i_0-1]} a_i b_{k_0-i}\Big) > s+t$, zudem ist $\mathrm{v}_p(a_{i_0}b_{j_0}) = s+t$ und schließlich ist $\mathrm{v}_p\Big(\sum_{i\in[i_0+1,k_0]} a_i b_{k_0-i}\Big) > s+t$. Also ist $\mathrm{v}_p(c_{k_0}) = s+t$. ▫

Bemerkung 74 *Sei $g(X) \in R[X]$ primitiv. Sei $f(X) \in R[X]$.*

Falls das Polynom $g(X)$ das Polynom $f(X)$ in $K[X]$ teilt, dann auch in $R[X]$.

Beweis. Sei $h(X) \in K[X]$ mit $g(X)\cdot h(X) = f(X)$. Wir haben $h(X) \overset{!}{\in} R[X]$ zu zeigen.

Sei $p \in R$ prim. Wir haben $\mathrm{v}_p(h(X)) \geqslant 0$ zu zeigen. In der Tat wird

$$0 \leqslant \mathrm{v}_p(f(X)) \overset{\text{L. 73}}{=} \mathrm{v}_p(g(X)) + \mathrm{v}_p(h(X)) = \mathrm{v}_p(h(X)) .$$

□

Satz 75 (Gauß) *Ist R faktoriell, dann ist auch $R[X]$ faktoriell.*

Beweis. Dank Hilbertschem Basissatz, Satz 42, ist $R[X]$ noethersch.

Sei ein in $R[X]$ irreduzibles Element $f(X) \in R[X]$ gegeben. Wir müssen zeigen, daß $f(X)$ in $R[X]$ prim ist.

Fall $\deg(f(X)) = 0$. Dann ist $f(X) =: p \in R$. Da p in $R[X]$ irreduzibel ist, ist auch p in R irreduzibel. Da R faktoriell ist, folgt p prim in R. Seien Polynome $g(X)$, $h(X) \in R[X]$ derart gegeben, daß p in $R[X]$ zwar ein Teiler von $g(X) \cdot h(X)$ ist, aber kein Teiler von $h(X)$. Wir müssen zeigen, daß p in $R[X]$ ein Teiler von $g(X)$ ist.

Aber

$$0 < \mathrm{v}_p(g(X) \cdot h(X)) \overset{\text{L. 73}}{=} \mathrm{v}_p(g(X)) + \mathrm{v}_p(h(X)) = \mathrm{v}_p(g(X)) .$$

Fall $\deg(f(X)) \geqslant 1$. Da $f(X)$ in $R[X]$ irreduzibel ist, ist $f(X)$ primitiv; vgl. Bemerkung 72.

Behauptung: Es ist $f(X)$ irreduzibel in $K[X]$.

Es ist $f(X)$ weder 0 noch Einheit in $K[X]$.

Sei $f(X) = u(X) \cdot v(X)$ mit $u(X)$, $v(X) \in K[X]$. O.E. ist $u(X)$ primitiv, insbesondere in $R[X]$; vgl. Bemerkung 72. Dank Bemerkung 74 ist nun $v(X) \in R[X]$. Da $f(X)$ in $R[X]$ irreduzibel ist, folgt $\deg(u(X)) = 0$ oder $\deg(v(X)) = 0$. Also ist $f(X)$ auch in $K[X]$ irreduzibel. Dies zeigt die *Behauptung*.

Da $K[X]$ faktoriell ist, ist $f(X)$ auch prim in $K[X]$; vgl. Beispiel 52.(2), Lemma 58.

Wir müssen immer noch zeigen, daß $f(X)$ prim ist in $R[X]$.

Seien Polynome $g(X)$, $h(X) \in R[X]$ derart gegeben, daß $f(X)$ in $R[X]$ ein Teiler von $g(X) \cdot h(X)$ ist. Wir müssen zeigen, daß $f(X)$ in $R[X]$ ein Teiler von $g(X)$ oder von $h(X)$ ist.

Da $f(X)$ prim ist in $K[X]$, ist $f(X)$ in $K[X]$ ein Teiler von $g(X)$ oder von $h(X)$.

Da $f(X)$ primitiv ist, ist $f(X)$ in $R[X]$ ein Teiler von $g(X)$ oder von $h(X)$; vgl. Bemerkung 74. □

Korollar 76 *Sei Q ein Körper.*

Es ist der Polynomring $Q[X_1, \ldots, X_k]$ faktoriell für $k \geqslant 0$.

Beweis. Dies folgt mit iterierter Anwendung von Satz 75. □

Kapitel 2

Gruppen und Gruppenoperationen

2.1 Gruppen

Wir erinnern an den Begriff einer Gruppe:

Definition 77 Eine *Gruppe* ist eine Menge G, zusammen mit einer Abbildung

$$(\cdot) \ : \ G \times G \to G \ : \ (x, y) \mapsto x \cdot y \ ,$$

genannt *Multiplikation*, derart, daß die folgenden Eigenschaften (Gruppe 1–3) gelten.

(Gruppe 1) Für x, y, $z \in G$ ist $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

(Gruppe 2) Es gibt ein Element 1_G mit $x \cdot 1_G = x = 1_G \cdot x$ für $x \in G$.

(Gruppe 3) Für $x \in G$ gibt es ein $y \in G$ mit $x \cdot y = 1_G = y \cdot x$.

Oft schreibt man nur $G := (G, \cdot)$.

(Gruppe 1) gibt Anlaß zum Weglassen der darin auftretenden Klammern.

Dazuhin wird oft $xy := x \cdot y$ geschrieben für x, $y \in G$.

Es ist 1_G eindeutig festgelegt, denn für ein zweites Element $1'_G$ mit derselben Eigenschaft wird $1_G = 1_G \cdot 1'_G = 1'_G$. Es heißt 1_G auch das *neutrale Element* oder das *Einselement* der Gruppe.

Oft schreibt man $1 := 1_G$.

Das Element y in (Gruppe 3) liegt eindeutig fest, denn mit zwei Elementen y, y' mit dieser Eigenschaft wird $y = y \cdot x \cdot y' = y'$. Wir schreiben $y =: x^{-1}$.

Ist $x \cdot y = y \cdot x$ für x, $y \in G$, so heißt G *abelsch*.

In einer abelschen Gruppe wird manchmal $(+)$ statt $(\cdot)$, ferner $0 := 0_G$ statt 1_G und schließlich $-x$ statt x^{-1} geschrieben, sowie die Operation Addition statt Multiplikation genannt. Man sagt dann, die betrachtete abelsche Gruppe wird *additiv geschrieben*.

Definition 78 Ist G endlich, so heißt die Zahl der Elemente von G auch die *Ordnung* von G, geschrieben $|G|$.

Ist G nicht endlich, so schreiben wir $|G| = \infty$.

Beispiel 79

(1) Sei S ein Ring. Es ist $\mathrm{U}(S)$, mit der von S nach $\mathrm{U}(S)$ eingeschränkten Multiplikation, eine Gruppe. Ist S kommutativ, dann ist $\mathrm{U}(S)$ abelsch.

(2) Sei R ein kommutativer Ring. Wir haben speziell für $n \geqslant 1$ die Gruppe

$$\mathrm{GL}_n(R) \ := \ \mathrm{U}(R^{n\times n}) \quad (^6) \ .$$

Sie besteht aus den invertierbaren Matrizen der Form $n \times n$ mit Einträgen in R. Wobei invertierbar bedeutet, sie hat ein Inverses in $R^{n\times n}$.

(3) Es ist $|\,\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - p^0) \cdot (p^n - p^1) \cdot \ldots \cdot (p^n - p^{n-1})$.

(4) Sei K ein Körper. Wir haben speziell die Gruppe

$$K^\times \ = \ \mathrm{U}(K) \ .$$

Bemerkung 80 Sei X eine Menge. Sei

$$\mathrm{S}_X \ := \ \{\, X \xrightarrow{f} X \ : \ f \text{ ist bijektiv} \,\}$$

die Menge aller bijektiven Abbildungen von X nach X.

Zusammen mit der Komposition $(\circ)$ als Multiplikation ist S_X eine Gruppe, genannt die *symmetrische Gruppe* auf der Menge X.

In der Tat ist Komposition assoziativ. Das bezüglich Komposition neutrale Element ist die Identität $\mathrm{id} = \mathrm{id}_X : X \to X : x \mapsto x$. Das zu $f \in \mathrm{S}_X$ inverse Element ist die Umkehrabbildung f^{-1}.

Oft schreibt man $\mathrm{S}_n := \mathrm{S}_{[1,n]}$.

Es ist $|\mathrm{S}_n| = n!$.

Definition 81 Sei $n \geqslant 1$ gegeben.

Sei

$$\{k_{1,1}, k_{1,2}, \ldots, k_{1,\ell_1}\} \sqcup \{k_{2,1}, k_{2,2}, \ldots, k_{2,\ell_2}\} \sqcup \ldots \sqcup \{k_{m,1}, k_{m,2}, \ldots, k_{m,\ell_m}\} \ = \ [1,n] \ ,$$

für gewisse $m \geqslant 1$ und $\ell_i \geqslant 1$ für $i \in [1,m]$, wobei $\sum_{i\in[1,m]} \ell_i = n$ sei.

[6] Engl. general linear group.

Wir schreiben

$$f \;:=\; (k_{1,1}, k_{1,2}, \ldots, k_{1,\ell_1})(k_{2,1}, k_{2,2}, \ldots, k_{2,\ell_2}) \ldots (k_{m,1}, k_{m,2}, \ldots, k_{m,\ell_m}) \;:\; [1,n] \;\to\; [1,n]$$

für die bijektive Abbildung, die folgendermaßen abbildet.

$$\begin{array}{rcccl} f & : & [1,n] & \to & [1,n] \\ & & k_{i,j} & \mapsto & \begin{cases} k_{i,j+1} & \text{für } i \in [1,m] \text{ und } j \in [1, \ell_i - 1] \\ k_{i,1} & \text{für } i \in [1,m] \text{ und } j = \ell_i \end{cases} \end{array}$$

Die Bestandteile $(k_{1,1}, k_{1,2}, \ldots\ k_{1,\ell_1})$, $(k_{2,1}, k_{2,2}, \ldots, k_{2,\ell_2})$, $\ldots$, $(k_{m,1}, k_{m,2}, \ldots, k_{m,\ell_m})$ dieser Abbildung heißen ihre *Zykel*, von Längen ℓ_1 , $\ldots$, ℓ_m .

Man spricht insgesamt auch von einer *Zykeldarstellung* von $f \in \mathrm{S}_n$.

Ist $\ell_i = 1$ für ein $i \in [1,m]$, so wird der Zykel $(k_{i,1})$, der nur einen Eintrag hat, in der Notation in der Regel weggelassen.

Die Identität schreibt man aber nicht ohne jegliche Zykel, sondern als $\mathrm{id} = \mathrm{id}_{[1,n]}$ oder als $1 = 1_{\mathrm{S}_n}$.

Beispiel 82

(1) Sei $f := (4,2,5)(1,6)(3) = (4,2,5)(1,6) \in \mathrm{S}_6$.

Dann bildet f wie folgt ab.

$$\begin{array}{rcccl} f & : & [1,6] & \to & [1,6] \\ & & 4 & \mapsto & 2 \\ & & 2 & \mapsto & 5 \\ & & 5 & \mapsto & 4 \\ & & 1 & \mapsto & 6 \\ & & 6 & \mapsto & 1 \\ & & 3 & \mapsto & 3 \end{array}$$

(2) Es ist $((4,2,5)(1,6))^{-1} = (5,2,4)(6,1) = (1,6)(2,4,5)$.

(3) Es ist

$$\mathrm{S}_3 \;=\; \{\mathrm{id},\ (1,2,3),\ (1,3,2),\ (1,2),\ (2,3),\ (1,3)\} \ .$$

Bemerkung 83 Sei $n \geqslant 1$. Sei $f \in \mathrm{S}_n$. Sei $f \neq \mathrm{id}$.

Folgendermaßen erhält man eine Zykeldarstellung von f.

Sei $k_{1,1} := 1$. Man bilde den Zykel

$$(k_{1,1}, f(k_{1,1}), f^2(k_{1,1}), \ldots, f^{\ell_1 - 1}(k_{1,1})) \ ,$$

wobei $\ell_1 \geqslant 1$ minimal sei mit $f^{\ell_1}(k_{1,1}) = k_{1,1}$.

Dann sei $k_{2,1}$ minimal in den Elementen von $[1,n]$, die noch nicht im ersten Zykel auftauchen. Man bilde den Zykel

$$(k_{2,1}, f(k_{2,1}), f^2(k_{2,1}), \ldots, f^{\ell_2-1}(k_{2,1}))\ ,$$

wobei $\ell_2 \geqslant 1$ minimal sei mit $f^{\ell_2}(k_{2,1}) = k_{2,1}$.

Dann sei $k_{3,1}$ minimal in den Elementen von $[1,n]$, die noch nicht in den ersten beiden Zykeln auftauchen. Man bilde den Zykel

$$(k_{3,1}, f(k_{3,1}), f^2(k_{3,1}), \ldots, f^{\ell_3-1}(k_{3,1}))\ ,$$

wobei $\ell_3 \geqslant 1$ minimal sei mit $f^{\ell_3}(k_{3,1}) = k_{3,1}$.

Usf., bis jedes Element von $[1,n]$ in einem Zykel auftaucht.

Dann weist f in seiner Zykeldarstellung die genannten Zykel auf:

$$f \ = \ (k_{1,1}, f(k_{1,1}), \ldots, f^{\ell_1-1}(k_{1,1}))(k_{2,1}, f(k_{2,1}), \ldots, f^{\ell_2-1}(k_{2,1}))(k_{3,1}, f(k_{3,1}), \ldots, f^{\ell_3-1}(k_{3,1}))\ldots$$

Nun lasse man noch die Zykel der Länge 1 weg.

Beispiel 84 Von der Konstruktion in Bemerkung 83 macht man z.B. bei der Multiplikation von Elementen in S_n Gebrauch.

(1) In S_4 wird
$$(1,2,3) \circ (1,2)(3,4) \ = \ (1,3,4)(2) \ = \ (1,3,4)\ .$$

(2) In S_{10} wird
$$\begin{array}{rcl}(2,5,4,8)(3,6,10,9) \circ (2,5,6)(4,7,3,10,8) & = & (1)(2,4,7,6,5,10)(3,9)(8) \\ & = & (2,4,7,6,5,10)(3,9)\ .\end{array}$$

(3) In S_6 wird
$$\begin{array}{rcl}(1,2,3,4,5,6)^2 & = & (1,3,5)(2,4,6) \\ (1,2,3,4,5,6)^3 & = & (1,4)(2,5)(3,6) \\ (1,2,3,4,5)^2 & = & (1,3,5,2,4)\end{array}$$

(4) In S_{13} ist $((1,4,2)(3,5))^6 = \mathrm{id}$, und 6 ist der kleinste Exponent $\geqslant 1$ mit dieser Eigenschaft.

2.2 Untergruppen und Normalteiler

Definition 85 Sei G eine Gruppe.

Eine Teilmenge $U \subseteq G$ heißt *Untergruppe* von G, falls $1_G \in U$ und falls für $x,\ y \in U$ auch $x \cdot y^{-1} \in U$ ist.

Eine solche Untergruppe ist mit der von G nach U eingeschränkten Multiplikation wieder eine Gruppe.

Die Tatsache, daß U eine Untergruppe von G ist, wird auch $U \leqslant G$ geschrieben.

Wir schreiben auch $U < G$ für $U \leqslant G$ und $U \neq G$.

Die Untergruppe von G, die nur die 1 enthält, wird auch $1 := \{1\} \leqslant G$ geschrieben.

Beispiel 86 Es ist $U := \{\mathrm{id}, (1,2,3), (1,3,2)\}$ eine Untergruppe von S_3.

Wir können dies $U \leqslant \mathrm{S}_3$ schreiben.

Definition 87 Sei G eine endliche Gruppe.

Sei $n \geqslant 0$. Seien $x_1, \ldots, x_n \in G$.

Sei

$$U \;:=\; \langle x_1, \ldots, x_n \rangle \;:=\; \{\, x_{k_1} \cdot x_{k_2} \cdot \ldots \cdot x_{k_m} \;:\; m \geqslant 0,\, k_1, \ldots, k_m \in [1,n] \,\}$$

die Menge aller Produkte in G, die mittels der Elemente $x_1, \ldots, x_n$ in beliebiger Reihenfolge gebildet werden können. Das leere Produkt sei gleich 1_G.

Dann ist $U \leqslant G$. Es heißt U die von $x_1, \ldots, x_n$ *erzeugte* Untergruppe.

Dazu beachte man, daß für jedes x_i ein minimales $\ell_i \geqslant 1$ mit $x_i^{\ell_i} = 1_G$ existiert. Somit ist jedenfalls $x_i^{-1} = x_i^{\ell_i - 1}$ wieder in U enthalten für $i \in [1,n]$.

Also ist mit $x_{k_1} \cdot x_{k_2} \cdot \ldots \cdot x_{k_m}$ auch

$$(x_{k_1} \cdot x_{k_2} \cdot \ldots \cdot x_{k_m})^{-1} \;=\; x_{k_m}^{-1} \cdot \ldots \cdot x_{k_2}^{-1} \cdot x_{k_1}^{-1} \;\in\; U$$

enthalten. Da U nach Konstruktion unter Produkten abgeschlossen ist, folgt, daß U in der Tat eine Untergruppe von G ist.

Ist V eine Untergruppe von G mit $x_1, \ldots, x_n \in V$, dann ist $U \leqslant V \leqslant G$.

Beispiel 88 Wir setzen Beispiel 86 fort.

Es ist $U = \{\mathrm{id}, (1,2,3), (1,3,2)\} = \langle (1,2,3) \rangle = \langle (1,3,2) \rangle$.

Beispiel 89 Es ist $\mathrm{S}_3 = \langle (1,2), (1,2,3) \rangle$.
Denn sei $U := \langle (1,2), (1,2,3) \rangle$. Dann enthält U die Elemente id, $(1,2,3)$, $(1,2,3)^2 = (1,3,2)$, $(1,2)$, $(1,2) \circ (1,2,3) = (2,3)$ und $(1,2,3) \circ (1,2) = (1,3)$. Also ist $U = \mathrm{S}_3$.

Definition 90 Ist G eine nicht notwendig endliche Gruppe und sind $n \geqslant 0$ und $x_1, \ldots, x_n \in G$, dann sei ihr Untergruppenerzeugnis $\langle x_1, \ldots, x_n \rangle$ die Menge aller Produkte, die aus den Elementen $x_1, \ldots, x_n$ und ihren Inversen gebildet werden können.

Im Falle G endlich stimmt dies dem Untergruppenerzeugnis in Definition 87 überein.

Definition 91 Eine Gruppe G heißt *zyklisch*, wenn es ein $x \in G$ gibt mit $G = \langle x \rangle$.

Beispiel 92

(1) Wir betrachten die additiv geschriebene Gruppe $\mathbb{Z} = (\mathbb{Z}, +)$.

Vorsicht, das neutrale Element ist 0.

Es ist $\mathbb{Z}$ erzeugt von 1.

Alternativ ist $\mathbb{Z}$ auch erzeugt von -1.

Jedenfalls ist $\mathbb{Z}$ zyklisch.

(2) Es ist $\langle (1,2,3) \rangle$ eine zyklische Untergruppe von S_3 von Ordnung 3.

(3) Es ist $\langle (1,4,2)(3,5) \rangle$ eine zyklische Untergruppe von S_{13} von Ordnung 6; vgl. Beispiel 84.(4).

Definition 93 Sei G eine Gruppe. Sei $x \in G$.

Es heißt $|\langle x \rangle|$ die *Ordnung* des Elements x.

Bemerkung 94 *Sei G eine Gruppe. Sei $x \in G$ ein Element endlicher Ordnung.*

Es ist $|\langle x \rangle| = \min\{\, k \in \mathbb{Z}_{\geqslant 1} \,:\, x^k = 1 \,\}$.

Es ist $\{\, k \in \mathbb{Z} \,:\, x^k = 1 \,\} = |\langle x \rangle| \mathbb{Z}$.

Beweis. Da $\langle x \rangle = \{\, x^k \,:\, k \in \mathbb{Z} \,\}$ endlich ist, sind die Potenzen von x nicht alle paarweise verschieden. Also gibt es $m, n \in \mathbb{Z}$ mit $m < n$ und mit $x^m = x^n$ und also $x^{n-m} = 1$.

Sei $s := \min\{\, k \in \mathbb{Z}_{\geqslant 1} \,:\, x^k = 1 \,\}$.

Dann hat die Menge $\{\, x^k \,:\, k \in [0, s-1] \,\}$ genau s verschiedene Elemente.

Umgekehrt sind aber alle Elemente von $\langle x \rangle = \{\, x^k \,:\, k \in \mathbb{Z} \,\}$ in $\{\, x^k \,:\, k \in [0, s-1] \,\}$ enthalten, da wir $k \in \mathbb{Z}$ schreiben können als $k = su + v$ mit $u \in \mathbb{Z}$ und $v \in [0, s-1]$ und sich $x^k = x^{su+v} = x^v$ ergibt. Also ist $\langle x \rangle = \{\, x^k \,:\, k \in [0, s-1] \,\}$.

Insgesamt ist $|\langle x \rangle| = s$.

Es bleibt $\{\, k \in \mathbb{Z} \,:\, x^k = 1 \,\} \stackrel{!}{=} s\mathbb{Z}$ zu zeigen. Dafür ist nur $\{\, k \in \mathbb{Z} \,:\, x^k = 1 \,\} \stackrel{!}{\subseteq} s\mathbb{Z}$ zu zeigen. Ist $k \in \mathbb{Z}$ gegeben mit $x^k = 1$, so ist $k = sq + r$ mit $q \in \mathbb{Z}$ und $r \in [0, s-1]$. Es ist $x^r = x^{k-sq} = x^k \cdot (x^s)^{-q} = 1$. Die Minimalität von s erzwingt $r = 0$ und also $k \in s\mathbb{Z}$. ▫

Beispiel 95

(1) In S_3 hat id die Ordnung 1, es hat $(1,2)$ die Ordnung 2 und $(1,2,3)$ die Ordnung 3.

(2) Sei $n \geqslant 1$. In S_n sei f in Zykeldarstellung gegeben mit Zykeln von Längen $\ell_1, \ldots, \ell_m$. Dann hat f die Ordnung $\mathrm{kgV}(\ell_1, \ldots, \ell_m)$. Z.B. hat $(1,2,5,4)(3,6)(7,8,11,13,12,9) \in \mathrm{S}_{14}$ die Ordnung $\mathrm{kgV}(4,2,6) = 12$.

Definition 96 Sei G eine Gruppe. Sei $U \leqslant G$ eine Untergruppe.

(1) Auf G definieren wir eine Äquivalenzrelation $({}_U\sim)$ durch $(x \,{}_U\!\sim y) :\Longleftrightarrow (xy^{-1} \in U)$, für $x, y \in G$.

Die Äquivalenzklasse von $x \in G$ bezüglich $({}_U\sim)$ ist $Ux := \{\, ux \,:\, u \in U \,\}$, genannt *Rechtsnebenklasse* von x modulo U in G.

Es ist G die disjunkte Vereinigung der Rechtsnebenklassen modulo U.

Die Menge aller Rechtsnebenklassen modulo U in G wird $U\backslash G := \{\, Ux \,:\, x \in G \,\}$ geschrieben, gesprochen "G rechts modulo U".

Für $x \in G$ ist die Abbildung $U \to Ux : u \mapsto ux$ bijektiv, invertiert von der Abbildung $Ux \to U : ux \mapsto uxx^{-1} = u$.

(2) Auf G definieren wir eine Äquivalenzrelation $(\sim_U)$ durch $(x \sim_U y) :\Longleftrightarrow (x^{-1}y \in U)$, für $x, y \in G$.

Die Äquivalenzklasse von $x \in G$ bezüglich $(\sim_U)$ ist $xU := \{\, xu \,:\, u \in U \,\}$, genannt *Linksnebenklasse* von x modulo U in G.

Es ist G die disjunkte Vereinigung der Linksnebenklassen modulo U.

Die Menge aller Linksnebenklassen modulo U in G wird $G/U := \{\, xU \,:\, x \in G \,\}$ geschrieben, gesprochen "G links modulo U".

Für $x \in G$ ist die Abbildung $U \to xU : u \mapsto xu$ bijektiv, invertiert von der Abbildung $xU \to U : xu \mapsto x^{-1}xu = u$.

Satz 97 (Lagrange) *Sei G eine endliche Gruppe. Sei $U \leqslant G$.*

Es ist

$$|G| \;=\; |G/U| \cdot |U| \;=\; |U\backslash G| \cdot |U|$$

Insbesondere ist $|U|$ ein Teiler von $|G|$.

Beweis. Es ist G die disjunkte Vereinigung von $|G/U|$ Linksnebenklassen, die alle in Bijektion zu U stehen, also alle $|U|$ Elemente haben. Also ist $|G| = |G/U| \cdot |U|$.

Genauso folgt $|G| = |U\backslash G| \cdot |U|$. ▫

Korollar 98 *Sei G eine endliche Gruppe.*

Es ist für jedes $x \in G$ seine Ordnung $|\langle x\rangle|$ ein Teiler von $|G|$.

Insbesondere ist $x^{|G|} = 1$ für $x \in G$.

Beweis. Dank Satz 97 ist $k := |\langle x\rangle|$ ein Teiler von $|G|$.

Schreibe $|G| = k \cdot \ell$ für ein $\ell \in \mathbb{Z}$. Dann ist $x^{|G|} = x^{k\cdot\ell} = (x^k)^\ell = 1^\ell = 1$. ▫

Definition 99 Sei G eine endliche Gruppe. Sei $U \leqslant G$.

Man schreibt auch $[G : U] := |G/U| = |U\backslash G|$ für den *Index* von U in G.

Dann ist $|G| = |U| \cdot [G : U]$, also $[G : U] = |G/U| = |U\backslash G| = |G|/|U|$; vgl. Satz 97.

Beispiel 100 Sei $G := \mathrm{S}_3$.

(1) Sei $U := \langle (1,2) \rangle = \{\mathrm{id}, (1,2)\} \leqslant G$.

Wir erhalten die Linksnebenklassen

$$\begin{array}{rcl} \mathrm{id}\, U & = (1,2)U & = \{\mathrm{id}, (1,2)\} \\ (1,2,3)U & = (1,3)U & = \{(1,2,3), (1,3)\} \\ (1,3,2)U & = (2,3)U & = \{(1,3,2), (2,3)\} \end{array}$$

und die Rechtsnebenklassen

$$\begin{array}{rcl} U\,\mathrm{id} & = U(1,2) & = \{\mathrm{id}, (1,2)\} \\ U(1,2,3) & = U(2,3) & = \{(1,2,3), (2,3)\} \\ U(1,3,2) & = U(1,3) & = \{(1,3,2), (1,3)\}\,. \end{array}$$

Es ist $|G| = 6 = 2 \cdot 3 = |U| \cdot [G : U]$.

(2) Sei $N := \langle (1,2,3) \rangle = \{\mathrm{id}, (1,2,3), (1,3,2)\} \leqslant G$.

Wir erhalten die Linksnebenklassen

$$\begin{array}{rcccccl} \mathrm{id}\, N & = & (1,2,3)N & = & (1,3,2)N & = & \{\mathrm{id}, (1,2,3), (1,3,2)\} \\ (1,2)N & = & (2,3)N & = & (1,3)N & = & \{(1,2), (2,3), (1,3)\}\,. \end{array}$$

Es ist $fN = Nf$ für $f \in \mathrm{S}_3$. Also stimmen hier Linksnebenklassen und Rechtsnebenklassen überein.

Es ist $|G| = 6 = 3 \cdot 2 = |N| \cdot [G : N]$.

Als Anwendung betrachten wir eine Aussage, die von Pierre de Fermat stammt:

Satz 101 (Kleiner Fermatscher Satz)
Sei $p \in \mathbb{Z}_{>0}$ prim.

Für $z \in \mathbb{Z}$ ist $z^p - z$ durch p teilbar.

Beweis. Wir haben für $x \in \mathbb{F}_p$ zu zeigen, daß $x^p - x \stackrel{!}{=} 0$ ist, also $x^p \stackrel{!}{=} x$. Es genügt, $x^{p-1} \stackrel{!}{=} 1$ zu zeigen für $x \in \mathbb{F}_p^\times$. Aber $1 \stackrel{\text{Kor. } 98}{=} x^{|\mathbb{F}_p^\times|} = x^{p-1}$. □

Alternativ kann man auch anführen, daß die Abbildungen $F : \mathbb{F}_p \to \mathbb{F}_p : x \mapsto x^p$ und $\mathrm{id} : \mathbb{F}_p \to \mathbb{F}_p : x \mapsto x$ Ringmorphismen sind, es aber von $\mathbb{F}_p$ in irgendeinen Ring höchstens einen Ringmorphismus geben kann, da ein solcher bereits durch das Bild der 1 bestimmt ist. So folgt $F = \mathrm{id}$, d.h. $x^p = x$ für $x \in \mathbb{F}_p$.

Definition 102 Sei G eine Gruppe.

Eine Untergruppe $N \leqslant G$ heißt *Normalteiler* oder *normale Untergruppe* von G, falls $xN = Nx$ ist für $x \in G$.

Diesenfalls ist $N\backslash G = G/N$, nun einfach gesprochen "G modulo N".

Äquivalent hierzu ist N ein Normalteiler von G, falls $x^{-1}Nx = N$ ist für $x \in G$.

Äquivalent hierzu ist N ein Normalteiler von G, falls $xNx^{-1} = N$ ist für $x \in G$.

Die Tatsache, daß N ein Normalteiler von G ist, wird auch $N \trianglelefteq G$ geschrieben. Wir schreiben auch $(N \lhd G) :\Leftrightarrow (N \trianglelefteq G \wedge N \neq G)$.

Definition 103 Sei G eine Gruppe. Sei $N \trianglelefteq G$.

Es ist G/N mit der Multiplikation $xN \cdot yN := (x \cdot y)N$ für $x, y \in G$ wieder eine Gruppe, genannt *Faktorgruppe* von G modulo N.

Zum Nachweis der Wohldefiniertheit der Multiplikation seien $x, y, \tilde{x}, \tilde{y} \in G$ mit $xN = \tilde{x}N$ und $yN = \tilde{y}N$ gegeben. Wir haben $(x \cdot y)N \stackrel{!}{=} (\tilde{x} \cdot \tilde{y})N$ nachzurechnen. In der Tat wird

$$(\tilde{x} \cdot \tilde{y})^{-1} \cdot (x \cdot y) \;=\; \tilde{y}^{-1} \cdot \tilde{x}^{-1} \cdot x \cdot y \;=\; (\tilde{y}^{-1} \cdot y) \cdot (y^{-1} \cdot \tilde{x}^{-1} \cdot x \cdot y)\,.$$

Aber $yN = \tilde{y}N$ bedeutet $\tilde{y}^{-1} \cdot y \in N$. Und $xN = \tilde{x}N$ bedeutet $\tilde{x}^{-1} \cdot x \in N$, was wegen $N \trianglelefteq G$ auch $y^{-1} \cdot \tilde{x}^{-1} \cdot x \cdot y \in N$ nach sich zieht. Da N auch eine Untergruppe von G ist, folgt, daß das entstandene Produkt in der Tat in N liegt.

Die Gruppeneigenschaften von G/N vererben sich von denen von G. Insbesondere ist $1_{G/N} = 1_G N$.

Bemerkung 104 *Sei G eine endliche Gruppe.*

Sei $U \leqslant G$ eine Untergruppe von Index $[G : U] = 2$.

Dann ist $U \trianglelefteq G$.

Beweis. Sei $g \in G \smallsetminus U$ gewählt. Es wird $G = U \sqcup Ug$ und auch $G = U \sqcup gU$.

Sei $x \in G$. Wir haben $xU \stackrel{!}{=} Ux$ zu zeigen.

Falls $x \in U$ liegt, dann ist $xU = U = Ux$.

Falls $x \in G \smallsetminus U$ liegt, dann ist $xU = gU$ und $Ux = Ug$ mangels Auswahl, und also $xU = gU = G \smallsetminus U = Ug = Ux$. ▫

Beispiel 105 Sei $G := \mathrm{S}_3$.

(1) Sei $U := \langle (1,2) \rangle = \{\mathrm{id}, (1,2)\} \leqslant G$.

Es ist $(1,2,3)U = \{(1,2,3), (1,3)\} \neq \{(1,2,3), (2,3)\} = U(1,2,3)$; vgl. Beispiel 100.(1).

Also ist die Untergruppe U kein Normalteiler von G.

(2) Sei $N := \langle (1,2,3) \rangle = \{\mathrm{id}, (1,2,3), (1,3,2)\} \leqslant G$.

Es ist $[G : N] = 2$ und also $N \trianglelefteq G$; vgl. Bemerkung 104. Was wir auch direkt verifizieren konnten.

Es ist $G/N = \{ \mathrm{id}\, N\,,\ (1,2)N \}$.

In G/N ist $((1,2)N)^2 = (1,2)^2 N = \mathrm{id}\, N = 1_{G/N}$. Also ist G/N zyklisch von Ordnung 2.

2.3 Gruppenmorphismen

Definition 106 Seien G und H Gruppen.

Eine Abbildung $\varphi : G \to H$ heißt *Gruppenmorphismus*, falls für $x,\ y \in G$ sich

$$\varphi(x \cdot y) \ = \ \varphi(x) \cdot \varphi(y)$$

ergibt.

Dann ist auch $\varphi(1_G) = \varphi(1_G) \cdot \varphi(1_G) \cdot \varphi(1_G)^{-1} = \varphi(1_G \cdot 1_G) \cdot \varphi(1_G)^{-1} = 1_H\,.$

Ferner ist $\varphi(x^{-1}) = \varphi(x^{-1}) \cdot \varphi(x) \cdot \varphi(x)^{-1} = \varphi(x^{-1} \cdot x) \cdot \varphi(x)^{-1} = \varphi(1_G) \cdot \varphi(x)^{-1} = \varphi(x)^{-1}$ für $x \in G$.

Das Kompositum zweier Gruppenmorphismen ist ein Gruppenmorphismus.

Ist der Gruppenmorphismus φ bijektiv, so heißt φ ein *Gruppenisomorphismus*. Dies wird durch $\varphi : G \xrightarrow{\sim} H$ gekennzeichnet.

Ist φ ein Gruppenisomorphimus, dann auch φ^{-1}.

Zwei Gruppen G und H heißen *isomorph*, geschrieben $G \simeq H$, wenn es einen Gruppenisomorphismus von G nach H gibt.

Ein Gruppenisomorphismus von G nach G heißt auch *Gruppenautomorphismus* auf G.

Definition 107 Seien G und H Gruppen. Sei $\varphi : G \to H$ ein Gruppenmorphismus.

Sei $\mathrm{Kern}(\varphi) := \{\, x \in G \,:\, \varphi(x) = 1 \,\}$ der *Kern* von φ.

Bemerkung 108 *Seien G und H Gruppen. Sei $\varphi : G \to H$ ein Gruppenmorphismus.*

(1) *Es ist* $\mathrm{Kern}(\varphi) \trianglelefteq G$.

(2) *Es ist* $\mathrm{Kern}(\varphi) = 1$ *genau dann, wenn φ injektiv ist.*

(3) *Es ist* $\varphi(G) \leqslant H$.

Beweis. Zu (1). Wir zeigen $\mathrm{Kern}(\varphi) \overset{!}{\leqslant} G$. Es ist $1 \in \mathrm{Kern}(\varphi)$. Seien $k, \ell \in \mathrm{Kern}(\varphi)$. Dann ist $\varphi(k \cdot \ell^{-1}) = \varphi(k) \cdot \varphi(\ell)^{-1} = 1$. Also ist $k \cdot \ell^{-1} \in \mathrm{Kern}(\varphi)$.

Wir zeigen $\mathrm{Kern}(\varphi) \overset{!}{\trianglelefteq} G$. Sei $x \in G$. Wir zeigen $x\,\mathrm{Kern}(\varphi) \overset{!}{=} \mathrm{Kern}(\varphi)x$. Wir zeigen $\overset{!}{\subseteq}$, die umgekehrte Inklusion folgt dann analog.

Sei $k \in \mathrm{Kern}(\varphi)$. Es ist $xk = xkx^{-1}x \in \mathrm{Kern}(\varphi)x$, da $\varphi(xkx^{-1}) = \varphi(x) \cdot \varphi(k) \cdot \varphi(x^{-1}) = \varphi(x) \cdot \varphi(x)^{-1} = 1$ und also $xkx^{-1} \in \mathrm{Kern}(\varphi)$.

Zu (2). Ist φ injektiv, dann darf nur 1_G auf 1_H abgebildet werden. Es folgt $\mathrm{Kern}(\varphi) = 1$.

Sei umgekehrt $\mathrm{Kern}(\varphi) = 1$. Wir wollen die Injektivität von φ zeigen. Seien $x, y \in G$ mit $\varphi(x) = \varphi(y)$ gegeben. Dann ist $1 = \varphi(x) \cdot \varphi(y)^{-1} = \varphi(x \cdot y^{-1})$, also $x \cdot y^{-1} \in \mathrm{Kern}(\varphi) = 1$ und somit $x = y$. ▫

Beispiel 109 Sei R ein Integritätsbereich. Sei $n \geqslant 1$.

(1) Es ist $\mathrm{GL}_n(R) = \mathrm{U}(R^{n\times n})$; vgl. Beispiel 79.(2).

Es ist $\det : \mathrm{GL}_n(R) \to \mathrm{U}(R) : A \mapsto \det(A)$ ein Gruppenmorphismus, da

$$\det(A \cdot B) \;=\; \det(A) \cdot \det(B)$$

ist für $A, B \in \mathrm{GL}_n(R)$.

Wir schreiben $\mathrm{SL}_n(R) := \mathrm{Kern}(\det) \trianglelefteq \mathrm{GL}_n(R)$ ([7]).

(2) Sei $\mathrm{e}_{i,j} \in R^{n\times n}$ die Matrix, die an Position (i,j) den Eintrag 1 hat, und ansonsten überall den Eintrag 0.

Für $f \in \mathrm{S}_n$ sei $P(f) := \sum_{i\in[1,n]} \mathrm{e}_{f(i),i} \in \mathrm{GL}_n(R)$ die Permutationsmatrix zu f.

Es ist also $P(f) \cdot \mathrm{e}_i = \mathrm{e}_{f(i)}$.

Es ist $P : \mathrm{S}_n \to \mathrm{GL}_n(R) : f \mapsto P(f)$ ein injektiver Gruppenmorphismus. In der Tat wird für $f, g \in \mathrm{S}_n$

$$\begin{aligned} P(f) \cdot P(g) &= (\textstyle\sum_{i\in[1,n]} \mathrm{e}_{f(i),i}) \cdot (\sum_{j\in[1,n]} \mathrm{e}_{g(j),j}) \\ &= \textstyle\sum_{i,\,j\,\in\,[1,n]} \mathrm{e}_{f(i),i} \cdot \mathrm{e}_{g(j),j} \\ &= \textstyle\sum_{j\in[1,n]} \mathrm{e}_{f(g(j)),g(j)} \cdot \mathrm{e}_{g(j),j} \\ &= \textstyle\sum_{j\in[1,n]} \mathrm{e}_{f(g(j)),j} \\ &= P(f \circ g)\,. \end{aligned}$$

(3) Es hat $f = (1,2,3)(4,5) \in \mathrm{S}_5$ die Permutationsmatrix $P(f) = \begin{pmatrix} 0&0&1&0&0\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&0&1\\ 0&0&0&1&0 \end{pmatrix} \in \mathrm{GL}_5(R)$.

[7] Engl. special linear group.

(4) Sei $R = \mathbb{Z}$. Es ist das *Signum*

$$\operatorname{sgn} \;:=\; \det \circ P \;:\; \mathrm{S}_n \;\to\; \mathrm{U}(\mathbb{Z}) \;=\; \{-1, +1\}$$

ein Gruppenmorphismus.

Es heißt $\mathrm{A}_n := \operatorname{Kern}(\operatorname{sgn}) \trianglelefteqslant \mathrm{S}_n$ die *alternierende Gruppe*.

(5) Da $\det \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = -1$ ist und da Determinanten blockweise berechnet werden dürfen, ist $\operatorname{sgn}((a, b)) = -1$ für $1 \leqslant a < b \leqslant n$.

Seien $a_1, \ldots, a_k \in [1, n]$ paarweise verschieden. Da

$$(a_1, a_2, \ldots, a_{k-1}, a_k) \;=\; (a_1, a_2) \circ (a_2, a_3) \circ \ldots \circ (a_{k-1}, a_k)$$

ist, folgt $\operatorname{sgn}((a_1, a_2, \ldots, a_{k-1}, a_k)) = (-1)^{k-1}$.

Dies setzt sich wie folgt fort zu Elementen, die aus mehreren Zykeln bestehen.

Sei $f \in \mathrm{S}_n$ gegeben. Habe f in Zykeldarstellung Zykeln der Länge $\ell_1 \,, \ldots \,, \ell_m$. Dann ist

$$\operatorname{sgn}(f) \;=\; (-1)^{(\ell_1 - 1) + \ldots + (\ell_m - 1)} \,.$$

(6) Es ist $\operatorname{sgn}((1,7,4,9)(2,5,6)(3,10,12,17,11)) = (-1)^{3+2+4} = -1$.

(7) Kleine Beispiele alternierender Gruppen.

$$\begin{array}{lcl} \mathrm{A}_2 & = & \{\mathrm{id}\} \;\trianglelefteqslant\; \mathrm{S}_2 \\ \mathrm{A}_3 & = & \{\mathrm{id}, (1,2,3), (1,3,2)\} \;\trianglelefteqslant\; \mathrm{S}_3 \\ \mathrm{A}_4 & = & \{\mathrm{id}, (1,2,3), (1,3,2), (1,2,4), (1,4,2), (1,3,4), (1,4,3), (2,3,4), (2,4,3), \\ & & \qquad (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \;\trianglelefteqslant\; \mathrm{S}_4 \end{array}$$

Beispiel 110 Seien R und S Ringe. Sei $\varphi : R \to S$ ein Ringmorphismus.

Für $r \in \mathrm{U}(R)$ ist $\varphi(r) \in \mathrm{U}(S)$, da $\varphi(r) \cdot \varphi(r^{-1}) = \varphi(r \cdot r^{-1}) = \varphi(1_R) = 1_S$ ist, und genauso von der anderen Seite.

Folglich existiert die Einschränkung $\varphi^{\mathrm{U}} := \varphi|^{\mathrm{U}(S)}_{\mathrm{U}(R)} : \mathrm{U}(R) \to \mathrm{U}(S)$. Da $\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')$ ist für $r, r' \in R$, ist auch $\varphi^{\mathrm{U}}(r \cdot r') = \varphi(r \cdot r') = \varphi(r) \cdot \varphi(r') = \varphi^{\mathrm{U}}(r) \cdot \varphi^{\mathrm{U}}(r')$ für $r, r' \in \mathrm{U}(R)$.

Somit ist $\varphi^{\mathrm{U}} : \mathrm{U}(R) \to \mathrm{U}(S)$ ein Gruppenmorphismus.

Definition 111 Sei G eine Gruppe. Sei $x \in G$. Für $g \in G$ schreiben wir

$$^x g \;:=\; xgx^{-1} \,,$$

gesprochen "g links hoch x".

Die Abbildung von G nach G, die g nach $^x g$ schickt, heißt *Konjugation* mit x.

Ist $U \leqslant G$, so schreiben wir auch $^x U := \{\, ^x u \,:\, u \in U \,\}$.

Bemerkung 112 *Sei G eine Gruppe. Sei $x \in G$.*

Es ist die Konjugation mit x, also

$$\begin{array}{ccc} G & \to & G \\ g & \mapsto & {}^{x}g \end{array},$$

ein Gruppenautomorphismus auf G.

Gruppenautomorphismen dieser Form heißen auch *inner*.

Beweis. Wir zeigen, daß die Konjugation mit x ein Gruppenmorphismus von G nach G ist.

Seien $g, \tilde{g} \in G$. Es wird

$${}^{x}(g\tilde{g}) \;=\; xg\tilde{g}x^{-1} \;=\; xgx^{-1}x\tilde{g}x^{-1} \;=\; {}^{x}g\ {}^{x}\tilde{g}\ .$$

Wir zeigen, daß die Konjugation mit x beidseitig von der Konjugation mit x^{-1} invertiert wird.

Für $g \in G$ wird ${}^{x^{-1}}({}^{x}g) = x^{-1}xgx^{-1}x = g$.

Für $g \in G$ wird ${}^{x}({}^{x^{-1}}g) = xx^{-1}gxx^{-1} = g$.

Insbesondere ist die Konjugation mit x ein Automorphismus auf G. ▫

Bemerkung 113 *Sei $U \leqslant G$.*

Es ist $U \trianglelefteq G$ genau dann, wenn ${}^{x}U = U$ ist für $x \in G$.

Dies ist genau dann der Fall, wenn ${}^{x}u \in U$ ist für $u \in U$ und $x \in G$.

Beweis. Wir haben nur zu zeigen, daß aus ${}^{x}U \subseteq U$ für $x \in G$ folgt, daß ${}^{x}U = U$ ist für $x \in G$.

Es ist also ${}^{x}U \overset{!}{\supseteq} U$ zu zeigen. In der Tat folgt aus ${}^{x^{-1}}U \subseteq U$ auch $U = {}^{x}({}^{x^{-1}}U) \subseteq {}^{x}U$. ▫

Bemerkung 114 *Sei $n \geqslant 1$. Sei $G = \mathrm{S}_n$.*

Sei $f \in \mathrm{S}_n$ gegeben. Habe f die Zykeldarstellung

$$f \;=\; (k_{1,1}, \ldots, k_{1,\ell_1})(k_{2,1}, \ldots, k_{2,\ell_2}) \ldots (k_{m,1}, \ldots, k_{m,\ell_m})\ .$$

Sei $g \in \mathrm{S}_n$. Es wird

$${}^{g}f \;=\; (g(k_{1,1}), \ldots, g(k_{1,\ell_1}))(g(k_{2,1}), \ldots, g(k_{2,\ell_2})) \ldots (g(k_{m,1}), \ldots, g(k_{m,\ell_m}))\ .$$

Mit anderen Worten, bei Konjugation mit g werden die Zykeleinträge mit g abgebildet.

Man beachte noch, daß sich die Zykellängen bei Konjugation nicht ändern.

Beweis. Sei $k_{i,j}$ ein Zykeleintrag von f. Dieser wird unter f abgebildet auf $k_{i,j+1}$, falls $j \in [1, \ell_i - 1]$ ist, und auf $k_{i,1}$, falls $j = \ell_i$ ist.

Nun wird ${}^g f(g(k_{i,j})) = (g \circ f \circ g^{-1})(g(k_{i,j})) = g(f(k_{i,j}))$, und das ist $g(k_{i,j+1})$, falls $j \in [1, \ell_i - 1]$ ist, und $g(k_{i,1})$, falls $j = \ell_i$ ist. Das liefert die behauptete Zykeldarstellung von ${}^g f$. ▫

Beispiel 115

(1) Es ist ${}^{(1,3,2)}(1,4)(2,5,3) = (3,4)(1,5,2) = (1,5,2)(3,4)$.
Es ist ${}^{(1,3,2)}(1,4) \circ (2,5,3) = (3,4) \circ (2,5,3) = (2,5,4,3)$.

(2) Sei $V = \langle (1,2)(3,4), (1,3)(2,4) \rangle \leqslant \mathrm{S}_4$.
Es ist $V = \{ \mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \}$.
Somit enthält V genau alle Elemente der Form $(a,b)(c,d)$ aus S_4. Ferner ist noch $\mathrm{id} \in V$.
Gemäß Bemerkung 114 gilt also für $g \in \mathrm{S}_4$ und $f \in V$, daß auch ${}^g f \in V$ liegt.
Somit ist $V \trianglelefteq \mathrm{S}_4$.

Definition 116 Sei G eine Gruppe. Sei $N \trianglelefteq G$ ein Normalteiler.

Der surjektive Gruppenmorphismus

$$\begin{array}{rccc} \rho = \rho_{G,N} : & G & \to & G/N \\ & x & \mapsto & xN \end{array}$$

heißt *Nebenklassenmorphismus* oder *Restklassenmorphismus.*

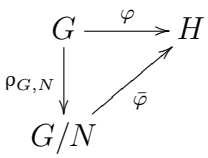
Es ist $\mathrm{Kern}(\rho_{G,N}) = N$.

Lemma 117 *Seien G und H Gruppen. Sei $\varphi : G \to H$ ein Gruppenmorphismus.*

Sei $N \trianglelefteq G$ ein Normalteiler mit $\varphi(N) = 1$, d.h. mit $\varphi(x) = 1$ für $x \in N$.

Dann gibt es den Gruppenmorphismus $\bar{\varphi} : G/N \to H : xN \mapsto \bar{\varphi}(xN) := \varphi(x)$.

Es ist $\bar{\varphi} \circ \rho_{G,N} = \varphi$.



Man nennt $\bar{\varphi}$ auch den auf G/N von φ *induzierten* Gruppenmorphismus.

Beweis. Zu zeigen ist die Repräsentantenunabhängigkeit der Definition von $\bar{\varphi}(xN)$. Seien $x, \tilde{x} \in G$ mit $xN = \tilde{x}N$ gegeben. Dann ist $\tilde{x}^{-1}x \in N$, also $1 = \varphi(\tilde{x}^{-1}x) = \varphi(\tilde{x})^{-1} \cdot \varphi(x)$, also $\varphi(\tilde{x}) = \varphi(x)$.

Die von $\bar{\varphi}$ zu erfüllende Verträglichkeit ergibt sich aus der für φ. ▫

Satz 118 (Homomorphiesatz) *Seien G und H Gruppen.*

Sei $\varphi : G \to H$ ein Gruppenmorphismus.

Es ist $\bar{\varphi} : G/\operatorname{Kern}(\varphi) \to \varphi(G) : g\operatorname{Kern}(\varphi) \mapsto \bar{\varphi}(g\operatorname{Kern}(\varphi)) := \varphi(g)$ ein Gruppenisomorphismus.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle \rho_{G,\operatorname{Kern}(\varphi)}}\downarrow & & \uparrow \\ G/\operatorname{Kern}(\varphi) & \xrightarrow[\sim]{\bar{\varphi}} & \varphi(G) \end{array}$$

Beweis. Dank Lemma 117 genügt es zu zeigen, daß $\bar{\varphi}$ injektiv ist.

Sei $x \in G$ mit $1 = \bar{\varphi}(x\operatorname{Kern}(\varphi)) = \varphi(x)$ gegeben. Dann ist $x \in \operatorname{Kern}(\varphi)$ und also $x\operatorname{Kern}(\varphi) = 1$. ▫

Bemerkung 119 *Seien G und H endliche Gruppen.*

Sei $\varphi : G \to H$ ein surjektiver Gruppenmorphismus.

Dann ist $|G| = |\operatorname{Kern}(\varphi)| \cdot |H|$.

Beweis. Es ist $H = \varphi(G) \simeq G/\operatorname{Kern}(\varphi)$ gemäß Satz 118. Also ist $|H| = |G/\operatorname{Kern}(\varphi)| = |G|/|\operatorname{Kern}(\varphi)|$. Also ist $|G| = |\operatorname{Kern}(\varphi)| \cdot |H|$. ▫

Bemerkung 120 *Sei G eine Gruppe.*

Sei $U \leqslant G$. Sei $N \trianglelefteq G$.

(1) *Es ist $U \cap N \trianglelefteq U$.*

(2) *Sei $UN := \{\, un : u \in U,\ n \in N \,\}$. Es ist $UN \leqslant G$.*

Setzt man noch $NU := \{\, nu : n \in N,\ u \in U \,\}$, dann ist noch $UN = NU$, da $N \trianglelefteq G$.

(3) *Wir haben den Gruppenisomorphismus*

$$\begin{array}{rcl} U/(U \cap N) & \xrightarrow{\sim} & UN/N \\ u(U \cap N) & \mapsto & uN\,. \end{array}$$

Falls G endlich ist, ist also insbesondere $|U|/|U \cap N| = |UN|/|N|$, d.h.

$$|UN| \;=\; \frac{|U| \cdot |N|}{|U \cap N|}\,.$$

Beweis.

Zu (1). Ist $u \in U$ und $x \in U \cap N$, dann ist ${}^u x \in U$, da $U \leqslant G$, und ${}^u x \in N$, da $N \trianglelefteqslant G$. Insgesamt ist also ${}^u x \in U \cap N$.

Zu (2). Es ist $1 = 1 \cdot 1 \in UN$.

Seien $u, \tilde{u} \in U$ und $n, \tilde{n} \in N$ gegeben. Wir haben zu zeigen, daß $(un)(\tilde{u}\tilde{n})^{-1}$ in UN liegt. In der Tat ist

$$(un)(\tilde{u}\tilde{n})^{-1} \;=\; un\tilde{n}^{-1}\tilde{u}^{-1} \;=\; u\tilde{u}^{-1}\,{}^{\tilde{u}}(n\tilde{n}^{-1}) \;\in\; UN\;.$$

Zu (3). Zunächst merken wir an, daß wegen $N \trianglelefteqslant G$ auch $N \trianglelefteqslant UN$ gilt.

Wir haben den Gruppenmorphismus $U \to UN : u \mapsto u$ und den Gruppenmorphismus $UN \to UN/N : x \mapsto xN$, welche zum Gruppenmorphismus $\varphi : U \to UN/N : u \mapsto uN$ komponieren.

Es ist φ surjektiv, denn für $u \in U$ und $n \in N$ wird $unN = uN = \varphi(u)$.

Der Kern von φ besteht aus den Elementen $u \in U$ mit $1_{UN/N} = \varphi(u) = uN$, d.h. mit $u \in N$. Folglich ist $\mathrm{Kern}(\varphi) = U \cap N$.

Dies gibt den Isomorphismus wie behauptet; vgl. Satz 118. ▫

Lemma 121 *Sei G eine endliche zyklische Gruppe. Schreibe $n := |G|$.*

Sei x ein Erzeuger von G, sei also $G = \langle x \rangle$, wobei x die Ordnung n hat.

Sei d ein Teiler von n.

Dann gibt es genau eine Untergruppe $U \leqslant G$ von Ordnung $|U| = d$, nämlich $U = \langle x^{n/d} \rangle$.

Beweis. Schreibe $m := n/d$.

Zur *Existenz* einer Untergruppe von Ordnung d. Wir wollen $|\langle x^m \rangle| \stackrel{!}{=} d$ zeigen. Wir müssen also zeigen, daß die Ordnung von x^m gleich d ist. Zum einen ist $(x^m)^d = x^{md} = x^n = 1$. Für $k \in [1, d-1]$ ist zum anderen $(x^m)^k = x^{mk} \neq 1$, da $mk \in [1, n-1]$ liegt.

Zur *Eindeutigkeit* der Untergruppe von Ordnung d. Sei $U \leqslant G$ mit $|U| = d$ gegeben. Wir betrachten die additiv geschriebene unendliche zyklische Gruppe $\mathbb{Z}$. Wir haben den surjektiven Gruppenmorphismus

$$\begin{array}{rccc} \varphi \;:\; & \mathbb{Z} & \to & G \\ & k & \mapsto & x^k\;. \end{array}$$

In der Tat ist $\varphi(k+\ell) = x^{k+\ell} = x^k \cdot x^\ell = \varphi(k) \cdot \varphi(\ell)$ für $k, \ell \in \mathbb{Z}$.

Es ist $\mathrm{Kern}(\varphi) = n\mathbb{Z}$.

Sei nun $V := \varphi^{-1}(U)$. Wegen $1 \leqslant U \leqslant G$ ist auch $n\mathbb{Z} \leqslant V \leqslant \mathbb{Z}$.

Untergruppen von $\mathbb{Z}$ sind bereits Ideale, da sich Multiplikation mit einem Element aus $\mathbb{Z}$ aus iterierter Addition und aus Negation zusammensetzen läßt. Also gibt es ein $s \in \mathbb{Z}_{\geqslant 0}$

mit $V = s\mathbb{Z}$; vgl. Beispiel 52. Da $n\mathbb{Z} \leqslant s\mathbb{Z}$, ist n ein Vielfaches von s. Insbesondere ist $s \geqslant 1$. Wir schreiben $n = st$ mit $t \in \mathbb{Z}_{\geqslant 1}$.

Es ist $U = \varphi(V)$ von Ordnung d. Auf der anderen Seite ist $\varphi(V) \simeq V/\operatorname{Kern}(\varphi|_V) = s\mathbb{Z}/n\mathbb{Z} = s\mathbb{Z}/st\mathbb{Z} \simeq \mathbb{Z}/t\mathbb{Z}$ von Ordnung t; vgl. Satz 118. Es folgt $d = t$ und $s = n/t = n/d = m$.

Somit ist $U = \varphi(V) = \varphi(m\mathbb{Z}) = \{\, x^{mz} \,:\, z \in \mathbb{Z} \,\} = \langle x^m \rangle$. ▫

Beispiel 122 Sei G eine zyklische Gruppe von Ordnung 12.

Sei x ein Erzeuger von G, sei also $G = \langle x \rangle$, wobei x die Ordnung 12 hat.

Dann hat G folgende Untergruppen, und nur diese.

$$\begin{array}{ll} \langle x^1 \rangle & \text{von Ordnung 12} \\ \langle x^2 \rangle & \text{von Ordnung 6} \\ \langle x^3 \rangle & \text{von Ordnung 4} \\ \langle x^4 \rangle & \text{von Ordnung 3} \\ \langle x^6 \rangle & \text{von Ordnung 2} \\ \langle x^{12} \rangle & \text{von Ordnung 1} \end{array}$$

Es ist die Aussage von Lemma 121 nicht mehr richtig, wenn G nicht zyklisch ist. Z.B. hat die alternierende Gruppe A_4 die Ordnung 12; in ihr liegen 3 Untergruppen von Ordnung 2, aber keine von Ordnung 6.

Folgender Satz zeigt, daß bis auf Isomorphie jede Gruppe Untergruppe einer symmetrischen Gruppe ist.

Insbesondere: Kennt man für jedes $n \geqslant 1$ die symmetrische Gruppe S_n und ihre Untergruppen, dann kennt man alle endlichen Gruppen.

Satz 123 (Cayley) *Sei G eine Gruppe.*

Wir erinnern an die symmetrische Gruppe S_G auf der Menge G, bestehend aus den bijektiven Abbildungen von G nach G.

Wir haben den injektiven Gruppenmorphismus

$$\begin{array}{rcl} \varphi \,:\, G & \to & \mathrm{S}_G \\ g & \mapsto & (\varphi(g) : G \to G : x \mapsto g \cdot x)\,. \end{array}$$

Beweis. Wir zeigen, daß φ ein Gruppenmorphismus ist. Seien $g, h \in G$ gegeben. Wir haben $\varphi(g \cdot h) \stackrel{!}{=} \varphi(g) \circ \varphi(h)$ zu zeigen.

Sei $x \in G$. Wir haben $(\varphi(g \cdot h))(x) \stackrel{!}{=} (\varphi(g) \circ \varphi(h))(x)$ zu zeigen.

In der Tat ist $(\varphi(g{\cdot}h))(x) = g{\cdot}h{\cdot}x$ und auch $(\varphi(g){\circ}\varphi(h))(x) = (\varphi(g))((\varphi(h))(x)) = g{\cdot}h{\cdot}x$.

Wir zeigen, daß φ injektiv ist. Wir haben $\operatorname{Kern}(\varphi) \stackrel{!}{=} 1$ zu zeigen.

Sei $g \in \mathrm{Kern}(\varphi)$ gegeben. Wir haben $g \stackrel{!}{=} 1_G$ zu zeigen.

Aber $g \in \mathrm{Kern}(\varphi)$ bedeutet $\varphi(g) = \mathrm{id}_G$. Also wird in der Tat $1_G = \mathrm{id}_G(1_G) = (\varphi(g))(1_G) = g \cdot 1_G = g$. ▫

2.4 Gruppenoperationen

2.4.1 Begriff der Gruppenoperation

Sei G eine Gruppe.

Definition 124

Eine *G-Menge* ist eine Menge X, zusammen mit einem Gruppenmorphismus $\varphi : G \to \mathrm{S}_X$, auch *Operationsmorphismus* genannt.

Wir schreiben dann oft

$$gx \;=\; g \cdot x \;:=\; (\varphi(g))(x)$$

und reden von der *Multiplikation* von G auf X.

Man sagt diesenfalls auch, es *operiert* G auf X.

Wir schreiben oft kurz $X := (X, \varphi)$ für diese G-Menge.

Es heißt X eine *treue* G-Menge, falls φ injektiv ist.

Bemerkung 125 *Sei X eine G-Menge.*

(1) *Es ist $1 \cdot x = x$ für $x \in X$.*

(2) *Es ist $(g \cdot \tilde{g}) \cdot x = g \cdot (\tilde{g} \cdot x)$ für $g, \tilde{g} \in G$ und $x \in X$.*

Man nimmt (2) zum Anlaß, auch $g \cdot \tilde{g} \cdot x := (g \cdot \tilde{g}) \cdot x = g \cdot (\tilde{g} \cdot x)$ zu schreiben.

Beweis. Zu (1). Es ist $1 \cdot x = (\varphi(1))(x) = \mathrm{id}_X(x) = x$.

Zu (2). Es ist $(g \cdot \tilde{g}) \cdot x = (\varphi(g \cdot \tilde{g}))(x) = (\varphi(g) \circ \varphi(\tilde{g}))(x) = (\varphi(g))((\varphi(\tilde{g}))(x)) = g \cdot (\tilde{g} \cdot x)$. ▫

Bemerkung 126 Sei X eine Menge.

Sei $(\cdot) : G \times X \to X : (g, x) \mapsto g \cdot x$ eine Abbildung, die die Eigenschaften $(1, 2)$ aus Bemerkung 125 hat.

Dann definiert $\varphi : G \to \mathrm{S}_X : g \mapsto (\varphi(g) : X \to X : x \mapsto g \cdot x)$ eine G-Menge, welche als Multiplikation von G auf X wieder die gegebene Abbildung $(\cdot)$ hat.

Kurz, um eine G-Menge zu definieren, darf man sich eine Multiplikation von G auf X mit den Eigenschaften $(1, 2)$ aus Bemerkung 125 konstruieren.

Beispiel 127

(1) Sei X eine Menge. Sei $g \cdot x := x$ für $g \in G$ und $x \in X$.

Dann ist X eine G-Menge, da die beiden Eigenschaften aus Bemerkung 125 gelten.

Wir sagen, es operiert G *trivial* auf X.

Insbesondere können wir hier auch X einelementig oder sogar leer sein lassen.

(2) Sei $X = G$.

Es ist G vermöge der Multiplikation auf G eine G-Menge.

Mit anderen Worten, um $g \cdot x$ zu bilden für $g \in G$ und $x \in G$, verwende man die vorliegende Multiplikation auf G.

In der Tat ist $1 \cdot x = x$ für $x \in G$. Ferner ist $(g \cdot \tilde{g}) \cdot x = g \cdot (\tilde{g} \cdot x)$ für $g, \tilde{g} \in G$ und $x \in G$. Vgl. Bemerkung 126.

Der zugehörige Gruppenmorphismus $\varphi : G \to \mathrm{S}_G$ ist übrigens der aus dem Satz von Cayley, er ist injektiv; vgl. Satz 123. Somit ist G via Multiplikation eine treue G-Menge.

(3) Sei $U \leqslant G$ eine Untergruppe.

Sei $X := G/U = \{\, xU \,:\, x \in G \,\}$ die Menge der Linksnebenklassen modulo U.

Es ist G/U vermöge $g \cdot xU := (gx)U$ eine G-Menge, für $g \in G$ und $x \in G$.

Zunächst ist dies wohldefiniert, denn für $x, \tilde{x} \in G$ mit $xU = \tilde{x}U$ ist $\tilde{x} = xu$ für ein $u \in U$, also auch $g\tilde{x} = gxu$ und somit $g\tilde{x}U = gxU$.

Ferner ist $1 \cdot xU = xU$. Schließlich ist $(g \cdot \tilde{g}) \cdot xU = (g \cdot \tilde{g} \cdot x)U = g \cdot (\tilde{g} \cdot x)U = g \cdot (\tilde{g} \cdot xU)$ für $g, \tilde{g} \in G$ und $x \in G$.

(4) Sei $X = G$.

Es ist G vermöge der Konjugation auf G eine G-Menge.

Mit anderen Worten, wir setzen $g \bullet x := {}^g x$. Wir verwenden die Bezeichnung $(\bullet)$, um von der Gruppenmultiplikation auf G unterscheiden zu können.

In der Tat ist $1 \bullet x = {}^1 x = 1 \cdot x \cdot 1^{-1} = x$ für $x \in G$.

Ferner ist $(g \cdot \tilde{g}) \bullet x = {}^{g \cdot \tilde{g}} x = (g \cdot \tilde{g}) \cdot x \cdot (g \cdot \tilde{g})^{-1} = g \cdot (\tilde{g} \cdot x \cdot \tilde{g}^{-1}) \cdot g^{-1} = {}^g({}^{\tilde{g}} x) = g \bullet (\tilde{g} \bullet x)$ für $g, \tilde{g} \in G$ und $x \in G$. Vgl. Bemerkung 126.

Die Bezeichnung $(\bullet)$ für diese Operation wird nur hier zwecks Erklärung verwendet. Üblicherweise verwendet man die Schreibweise ${}^g x$.

Betrachten wir einmal den zugehörigen Gruppenmorphismus

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & \mathrm{S}_G \\ g & \mapsto & (\varphi(g) : G \to G : x \mapsto {}^g x) \,. \end{array}$$

Es wird

$$\begin{aligned} \mathrm{Z}(G) &:= \mathrm{Kern}(\varphi) \\ &= \{\, g \in G \,:\, \varphi(g) = \mathrm{id}_G \,\} \\ &= \{\, g \in G \,:\, \text{es ist } {}^g x = x \text{ für } x \in G \,\} \\ &= \{\, g \in G \,:\, \text{es ist } g \cdot x = x \cdot g \text{ für } x \in G \,\} \\ &\trianglelefteq G \end{aligned}$$

auch als *Zentrum* von G bezeichnet.

Es ist die Gruppe G abelsch genau dann, wenn $\mathrm{Z}(G) = G$ ist.

Es ist z.B. $\mathrm{Z}(\mathrm{S}_3) = \{\mathrm{id}\} = 1$, wie man verifiziert. Also ist diesenfalls der Gruppenmorphismus φ injektiv und also die S_3-Menge S_3 , mit der Konjugation als Operation, treu.

(5) Sei $n \geqslant 1$. Sei $G = \mathrm{S}_n$. Sei $X = [1, n] = \{1, 2, \ldots, n\}$.

Wir haben den Gruppenmorphismus $\varphi = \mathrm{id}_{\mathrm{S}_n} : \mathrm{S}_n = G \to \mathrm{S}_{[1,n]} = \mathrm{S}_n$.

Auf diese Weise wird $[1, n]$ zu einer S_n-Menge.

Die zugehörige Multiplikationsabbildung ist also für $f \in \mathrm{S}_n$ und $x \in [1, n]$ gegeben durch

$$f \cdot x \;=\; (\mathrm{id}_{\mathrm{S}_n}(f))(x) \;=\; f(x) \,.$$

Kurz, Multiplizieren eines Elements x mit einer bijektiven Abbildung f bedeutet schlicht Anwenden von f auf x.

Da der Operationsmorphismus $\varphi = \mathrm{id}_{\mathrm{S}_n}$ injektiv ist, ist die S_n-Menge $[1, n]$ treu.

Zum Beispiel ist $[1, 4] = \{1, 2, 3, 4\}$ eine S_4-Menge. Darin wird z.B. $(1, 4, 3) \cdot 3 = (1, 4, 3)\big(3\big) = 1$. Darin wird z.B. $(1, 2) \cdot 4 = 4$.

(6) Sei $\mathcal{U}(G) := \{\, U \,:\, U \leqslant G \,\}$ die Menge der Untergruppen von G.

Es ist $\mathcal{U}(G)$ vermöge Konjugation eine G-Menge.

Mit anderen Worten, wir setzen $g \bullet U := {}^g U$ für $g \in G$ und $U \in \mathcal{U}(G)$. Man beachte, daß ${}^g U \leqslant G$, da das Bild einer Untergruppe unter dem Automorphismus auf G, der durch Konjugation mit g gegeben ist, wieder eine Untergruppe ist.

Um zu zeigen, daß G tatsächlich operiert, rechnen wir ähnlich wie in (4).

Zum einen ist $1 \bullet U = {}^1 U = U$ für $U \in \mathcal{U}(G)$.

Zum anderen ist $(g \cdot \tilde{g}) \bullet U = {}^{g \cdot \tilde{g}} U = (g \cdot \tilde{g}) \cdot U \cdot (g \cdot \tilde{g})^{-1} = g \cdot (\tilde{g} \cdot U \cdot \tilde{g}^{-1}) \cdot g^{-1} = {}^g({}^{\tilde{g}} U) = g \bullet (\tilde{g} \bullet U)$ für $g, \tilde{g} \in G$ und $U \in \mathcal{U}(G)$.

Definition 128 Sei X eine G-Menge.

Eine Teilmenge $Y \subseteq X$ heißt *G-Teilmenge*, falls $g \cdot y \in Y$ liegt für $g \in G$ und $y \in Y$.

Diesenfalls ist Y mit der von X eingeschränkten Multiplikation wieder eine G-Menge.

Beispiel 129

(1) Sei X eine G-Menge. Es sind $\emptyset$ und X jedenfalls G-Teilmengen von X.

(2) Sei $G := \langle (1,2,4)(3,6) \rangle \leqslant \mathrm{S}_6$.

Es ist $X := [1,6] = \{1,2,3,4,5,6\}$ eine G-Menge, mit Multiplikation gegeben durch Anwendung.

Die Liste aller G-Teilmengen von X ist die folgende.

$$\begin{array}{l} \emptyset, \\ \{1,2,4\},\ \{3,6\},\ \{5\}, \\ \{1,2,4,3,6\},\ \{1,2,4,5\},\ \{3,5,6\}, \\ \{1,2,3,4,5,6\} \end{array}$$

(3) Sei G eine endliche Gruppe.

Wir betrachten die G-Menge $\mathcal{U}(G)$ der Untergruppen von G, mit Multiplikation von G auf $\mathcal{U}(G)$ gegeben durch Konjugation; vgl. Beispiel 127.(6).

Sei d ein Teiler von $|G|$.

Sei $\mathcal{U}_d(G) := \{\, U \,:\, U \leqslant G,\ |U| = d \,\} \subseteq \mathcal{U}(G)$ die Teilmenge der Untergruppen von Ordnung d.

Es ist $\mathcal{U}_d(G)$ eine G-Teilmenge von $\mathcal{U}(G)$. Denn ist $|U| = d$, dann ist auch $|\,{}^g U| = d$ für $g \in G$. Dazu erinnern wir uns, daß Konjugation mit g ein Automorphismus auf G ist, insbesondere also eine bijektive Abbildung von G nach G ; vgl. Bemerkung 112.

(4) Wir betrachten das Beispiel aus (3) speziell im Fall $G = \mathrm{S}_3$.

Es ist $\mathcal{U}(\mathrm{S}_3) = \{1, \langle(1,2)\rangle, \langle(1,3)\rangle, \langle(2,3)\rangle, \langle(1,2,3)\rangle, \mathrm{S}_3\}$.

Es ist $\mathcal{U}_1(\mathrm{S}_3) = \{1\}$.

Es ist $\mathcal{U}_2(\mathrm{S}_3) = \{\langle(1,2)\rangle, \langle(1,3)\rangle, \langle(2,3)\rangle\}$. Hierin ist z.B.

$$^{(1,3,2)}\langle(1,3)\rangle \;=\; \langle(3,2)\rangle \;=\; \langle(2,3)\rangle \ .$$

Es ist $\mathcal{U}_3(\mathrm{S}_3) = \{\langle(1,2,3)\rangle\}$. Auf dieser S_3-Menge operiert S_3 trivial. Das geht bei einer einelementigen Menge auch nicht anders. Wir sehen erneut, daß $\mathrm{A}_3 = \langle(1,2,3)\rangle$ ein Normalteiler von S_3 ist.

Es ist $\mathcal{U}_6(\mathrm{S}_3) = \{\mathrm{S}_3\}$.

Definition 130 Sei X eine nichtleere G-Menge.

Es heißt X *transitiv,* wenn für jedes Paar von Elementen $(\,x\,,\,y\,)$ mit $x, y \in X$ es ein $g \in G$ gibt mit $g \cdot x = y$.

Beispiel 131

(1) Sei $n \geqslant 1$. Es ist $[1,n]$ eine transitive S_n-Menge; vgl. Beispiel 127.(5).

(2) Sei $f := (1,2,4)(3,6)$, sei $G := \langle (1,2,4)(3,6) \rangle = \langle f \rangle = \{f^0, f^1, \ldots, f^5\} \leqslant \mathrm{S}_6$ und $X := [1,6] = \{1,2,\ldots,6\}$ wie in Beispiel 129.(2).

Es ist X nicht transitiv. Denn für das Paar $(\,1\,,\,3\,)$ von Elementen von X gibt es kein $k \in [0,5]$ mit $f^k \cdot 1 = 3$. Denn es ist $f^k \cdot 1 \in \{1,2,4\}$ stets.

Dagegen ist die G-Teilmenge $Y := \{1,2,4\} \subseteq X$ transitiv. In der Tat multipliziert f^0 jedes Element auf sich selbst. Ferner ist $f \cdot 1 = 2$, $f \cdot 2 = 4$, $f \cdot 4 = 1$, $f^2 \cdot 2 = 1$, $f^2 \cdot 4 = 2$, $f^2 \cdot 1 = 4$.

(3) Sei $U \leqslant G$ eine Untergruppe.

Die G-Menge G/U der Linksnebenklassen modulo U ist transitiv.

Denn sei ein Paar $(\,xU\,,\,\tilde{x}U\,)$ von Elementen darin gegeben, wobei $x,\, \tilde{x} \in G$.

Mit $g := \tilde{x} \cdot x^{-1}$ wird $g \cdot xU = (g \cdot x)U = (\tilde{x} \cdot x^{-1} \cdot x)U = \tilde{x}U$.

> Wir wollen im weiteren Verlauf nachweisen, daß jede transitive G-Menge im wesentlichen von der Form G/U ist für eine Untergruppe $U \leqslant G$.

Definition 132 Sei X eine G-Menge.

Wir definieren eine Äquivalenzrelation $(\sim)$ auf X durch

$$x \sim \tilde{x} \qquad :\Longleftrightarrow \qquad (\text{es gibt ein } g \in G \text{ mit } g \cdot x = \tilde{x})\,.$$

Die Äquivalenzklasse von x ist

$$G \cdot x \;:=\; \{\, g \cdot x \,:\, g \in G \,\}$$

und heißt *Bahn* von x unter der Operation von G.

Nach Konstruktion ist X die disjunkte Vereinigung seiner Bahnen.

Die Schreibung der Bahn ist in der Regel der Schreibung der Operation angepaßt. Schreibt man ${}^{g}x$ für das Ergebnis der Operation von $g \in G$ auf x, so schreibt man auch ${}^{G}x$ für die Bahn von x, wobei $x \in X$.

Bemerkung 133 Sei X eine nichtleere G-Menge.

(1) Jede Bahn von X ist eine transitive G-Teilmenge von X.

(2) Jede transitive G-Teilmenge von X ist eine Bahn von X.

(3) Jede G-Teilmenge von X ist disjunkte Vereinigung gewisser Bahnen von X.

(4) Es ist X genau dann transitiv, wenn X aus nur einer Bahn besteht.

Beweis. Zu (1). Sei $x \in X$.

Wir wollen zeigen, daß $G \cdot x \subseteq X$ eine G-Teilmenge ist. Sei $g \cdot x \in G \cdot x$ gegeben, wobei $g \in G$. Sei $h \in G$ gegeben. Dann ist auch $h \cdot g \cdot x \in G \cdot x$.

Wir wollen zeigen, daß seine Bahn $G \cdot x \subseteq X$ transitiv ist. Sei das Paar $(\, g \cdot x \,,\, \tilde{g} \cdot x \,)$ von Elementen dieser Bahn betrachtet, wobei $g, \tilde{g} \in G$. Sei $h := \tilde{g} \cdot g^{-1}$. Es wird $h \cdot g \cdot x = \tilde{g} \cdot g^{-1} \cdot g \cdot x = \tilde{g} \cdot x$.

Zu (2). Sei $Y \subseteq X$ eine transitive G-Teilmenge. Da $Y \neq \emptyset$, können wir ein $y \in Y$ wählen. Wir behaupten $G \cdot y \stackrel{!}{=} Y$.

Die Inklusion $\subseteq$ folgt, da $Y \subseteq X$ eine G-Teilmenge ist. Die Inklusion $\supseteq$ folgt, da Y transitiv ist.

Zu (3). Sei $Y \subseteq X$ eine G-Teilmenge. Da nach Konstruktion X die disjunkte Vereinigung seiner Bahnen ist, ist nur zu zeigen, daß mit jedem Element $y \in Y$ auch $G \cdot y \subseteq Y$ liegt. Dies folgt aber, da Y eine G-Teilmenge von X ist.

Zu (4). Ist X transitiv, dann besteht X nur aus einer Bahn dank (2). Besteht umgekehrt X nur aus einer Bahn, dann ist X transitiv dank (1). ▫

Beispiel 134

(1) Sei $f := (1,2,4)(3,6)$, sei $G := \langle (1,2,4)(3,6) \rangle = \langle f \rangle = \{f^0, f^1, \ldots, f^5\} \leqslant \mathrm{S}_6$ und $X := [1,6] = \{1,2,\ldots,6\}$ wie in Beispiel 129.(2).

Wir haben die Bahn $G \cdot 1 = G \cdot 2 = G \cdot 4 = \{1,2,4\}$, die Bahn $G \cdot 3 = G \cdot 6 = \{3,6\}$ und die Bahn $G \cdot 5 = \{5\}$. Die disjunkte Zerlegung von X in seine Bahnen hat also folgende Form.

$$X \;=\; \{1,2,3,4,5,6\} \;=\; \{1,2,4\} \sqcup \{3,6\} \sqcup \{5\} \;.$$

(2) Operiere G via Konjugation auf $X := G$.

Die Bahn ${}^{G}x = \{\, {}^{g}x \,:\, g \in G \,\}$ von $x \in G$ heißt auch *Konjugationsklasse* von x.

Z.B. ist ${}^{\mathrm{S}_3}(1,2) = \{\, (1,2),\, (1,3),\, (2,3) \,\}$. Z.B. ist ${}^{\mathrm{S}_3}(1,2,3) = \{\, (1,2,3),\, (1,3,2) \,\}$. Insgesamt haben wir die folgende Zerlegung in Bahnen, also in Konjugationsklassen.

$$\mathrm{S}_3 \;=\; {}^{\mathrm{S}_3}\mathrm{id} \sqcup {}^{\mathrm{S}_3}(1,2) \sqcup {}^{\mathrm{S}_3}(1,2,3) \;=\; \{\, \mathrm{id} \,\} \sqcup \{\, (1,2),\, (1,3),\, (2,3) \,\} \sqcup \{\, (1,2,3),\, (1,3,2) \,\} \;.$$

2.4.2 Bahnenlemma

Sei G eine Gruppe. Seien G-Mengen X und Y gegeben.

Definition 135 Sei $x \in X$ gegeben.

Sei

$$\mathrm{Stab}_G(x) \;:=\; \{\, g \in G \,:\, g \cdot x = x \,\}$$

der *Stabilisator* von x in G.

Bemerkung 136 *Es ist* $\mathrm{Stab}_G(x) \leqslant G$.

Beweis. Es ist $1 \in \mathrm{Stab}_G(x)$.

Sind ferner $g, h \in \mathrm{Stab}_G(x)$, dann wird $g \cdot h^{-1} \cdot x = g \cdot h^{-1} \cdot h \cdot x = g \cdot x = x$ und also $g \cdot h^{-1} \in \mathrm{Stab}_G(x)$. ▫

Beispiel 137

(1) Wir betrachten die Operation von G auf G via Konjugation; vgl. Beispiel 127.(4).
Sei $x \in G$. Wir schreiben diesenfalls

$$\mathrm{C}_G(x) \;:=\; \mathrm{Stab}_G(x) \;=\; \{\, g \in G \,:\, {}^g x = x \,\} \;\leqslant\; G\,,$$

genannt *Zentralisator* von x in G.

(2) Es ist $\mathrm{C}_{\mathrm{S}_4}((1,2)) = \langle\, (1,2),\, (3,4) \,\rangle$.

(3) Wir betrachten die Operation von G auf der Menge $\mathcal{U}(G)$ der Untergruppen via Konjugation; vgl. Beispiel 127.(6).
Sei $U \leqslant G$. Wir schreiben diesenfalls

$$\mathrm{N}_G(U) \;:=\; \mathrm{Stab}_G(U) \;=\; \{\, g \in G \,:\, {}^g U = U \,\} \;\leqslant\; G\,,$$

genannt *Normalisator* von U in G.

(4) Es ist $\mathrm{N}_{\mathrm{S}_4}(\langle (1,2,3,4) \rangle) = \langle\, (1,2,3,4),\, (1,3) \,\rangle$.

Definition 138 Sei $f : X \to Y$ eine Abbildung.

Es heißt f eine *G-Abbildung*, falls

$$f(g \cdot x) \;=\; g \cdot f(x)$$

ist für $g \in G$ und $x \in X$.

Ist die G-Abbildung $f : X \to Y$ bijektiv, so heißt sie auch G-Bijektion. Diesenfalls ist auch f^{-1} eine G-Bijektion.

Existiert eine G-Bijektion $f : X \to Y$, so heißen die G-Mengen X und Y *isomorph*, geschrieben $X \simeq Y$.

Beispiel 139 Seien Untergruppen $U < V \leqslant G$ gegeben.

Wir haben die G-Mengen G/U und G/V; vgl. Beispiel 127.(3).

Wir betrachten die Abbildung $f : G/U \to G/V : xU \mapsto xV$.

Es ist f wohldefiniert, da für $x, \tilde{x} \in G$ mit $xU = \tilde{x}U$ folgt, daß $\tilde{x} = xu$ ist für ein $u \in U$, was wegen $U \leqslant V$ dann $xV = \tilde{x}V$ zur Folge hat.

Es ist f eine G-Abbildung, da $f(g \cdot xU) = f((gx)U) = (gx)V = g \cdot xV = g \cdot f(xU)$ ist für $g \in G$ und $x \in G$.

Es ist f surjektiv.

Es ist f nicht injektiv, da für ein $v \in V \setminus U$ sowohl $1U$ als auch vU auf $1V$ abgebildet werden.

Lemma 140 (Bahnenlemma) *Sei x ein Element der G-Menge X.*

Die Bahn von x ist dann eine G-Teilmenge $G \cdot x \subseteq X$; vgl. Bemerkung 133.(1).

Wir haben die G-Menge $G/\operatorname{Stab}_G(x)$; vgl. Beispiel 127.(3).

Wir haben die G-Bijektion

$$\begin{array}{rcl} G/\operatorname{Stab}_G(x) & \to & G \cdot x \\ g \operatorname{Stab}_G(x) & \mapsto & g \cdot x \end{array}$$

Ist insbesondere X transitiv, dann ist dies eine G-Bijektion von $G/\operatorname{Stab}_G(x)$ nach X.

Beweis.

Zur Wohldefiniertheit. Seien $g, \tilde{g} \in G$ mit $g \operatorname{Stab}_G(x) = \tilde{g} \operatorname{Stab}_G(x)$ gegeben. Dann ist $\tilde{g} = g \cdot h$ mit $h \in \operatorname{Stab}_G(x)$. Also ist $g \cdot x = g \cdot h \cdot x = \tilde{g} \cdot x$.

Es liegt eine G-Abbildung vor: Für $k \in G$ wird $k \cdot (g \operatorname{Stab}_G(x)) = (kg) \operatorname{Stab}_G(x)$ abgebildet auf $(kg) \cdot x = k \cdot (g \cdot x)$, wobei $g \in G$.

Zur Surjektivität. Diese folgt nach Konstruktion.

Zur Injektivität. Seien $g, \tilde{g} \in G$ mit $g \cdot x = \tilde{g} \cdot x$ gegeben. Dann ist $x = g^{-1} \cdot g \cdot x = g^{-1} \cdot \tilde{g} \cdot x$. Sei $h := g^{-1} \cdot \tilde{g}$. Es ist $h \cdot x = x$, d.h. $h \in \operatorname{Stab}_G(x)$. Also ist $g \operatorname{Stab}_G(x) = g \cdot h \operatorname{Stab}_G(x) = \tilde{g} \operatorname{Stab}_G(x)$. ▫

Korollar 141 *Sei die Gruppe G endlich.*

Sei die G-Menge X transitiv.

Dann ist $|X|$ endlich und ein Teiler von $|G|$.

Genauer gesagt ist $|X| = |G|/|\operatorname{Stab}_G(x)|$ für jedes $x \in X$.

Beweis. Wähle $x \in X$. Es ist $G/\operatorname{Stab}_G(x)$ isomorph zu $G \cdot x = X$. Insbesondere ist $|G|/|\operatorname{Stab}_G(x)| = |G/\operatorname{Stab}_G(x)| = |X|$, und dies ist ein Teiler von $|G|$. ▫

2.4.3 Fixpunktlemma

Sei G eine endliche Gruppe. Sei X eine endliche G-Menge.

Definition 142 Sei $g \in G$ gegeben. Sei

$$\mathrm{Fix}_g(X) \;:=\; \{\, x \in X \;:\; g \cdot x = x \,\} \;\subseteq\; X$$

die Menge der *Fixpunkte* von X unter g.

Lemma 143 (Fixpunktlemma)

Sei k die Anzahl der Bahnen in X unter der Operation von G.

Es ist

$$k \;=\; \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}_g(X)| \;.$$

Das Fixpunktlemma stammt von Cauchy. Es wurde von Burnside Frobenius zugesprochen. Es wird oft nach Burnside benannt.

Beweis. Seien $x_1, \ldots, x_k \in X$ Repräsentanten der Bahnen. Es ist also $X = \bigsqcup_{i \in [1,k]} G \cdot x_i$.

Es wird

$$\begin{array}{rcl}
\sum_{g \in G} |\,\mathrm{Fix}_g(X)| & = & |\{\, (g,x) \in G \times X \;:\; g \cdot x = x \,\}| \\
& = & \sum_{x \in X} |\,\mathrm{Stab}_G(x)| \\
& \overset{\text{L. } 140}{=} & \sum_{x \in X} |G|/|G \cdot x| \\
& = & \sum_{i \in [1,k]} \sum_{x \in G \cdot x_i} |G|/|G \cdot x| \\
& = & \sum_{i \in [1,k]} |G \cdot x_i| \cdot |G|/|G \cdot x_i| \\
& = & k \cdot |G| \;.
\end{array}$$

□

Beispiel 144 Sei $G := \mathrm{S}_3$. Sei $X := \{1,2,3\}$; vgl. Beispiel 127.(5).

Es ist X transitiv. D.h. die Anzahl der Bahnen ist $k = 1$.

Es ist $\mathrm{Fix}_{\mathrm{id}}(X) = \{1,2,3\}$.

Es ist $\mathrm{Fix}_{(1,2)}(X) = \{3\}$, $\mathrm{Fix}_{(1,3)}(X) = \{2\}$ und $\mathrm{Fix}_{(2,3)}(X) = \{1\}$.

Es ist $\mathrm{Fix}_{(1,2,3)}(X) = \emptyset$ und $\mathrm{Fix}_{(1,3,2)}(X) = \emptyset$.

Das Fixpunktlemma gibt nun folgendes.

$$k \;\overset{\text{L. } 143}{=}\; \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}_g(X)| \;=\; \frac{1}{6}(3+1+1+1+0+0) \;,$$

was zutrifft.

Beispiel 145 Sei $U \leqslant G$. Sei $X := G/U$; vgl. Beispiel 127.(3).

Es ist X transitiv. D.h. die Anzahl der Bahnen ist $k = 1$.

Für $g \in G$ ist

$$\begin{aligned} \mathrm{Fix}_g(X) &= \{\, x \in X \,:\, g \cdot x = x \,\} \\ &= \{\, yU \in G/U \,:\, y \in G,\ g \cdot yU = yU \,\} \\ &= \{\, yU \in G/U \,:\, y \in G,\ y^{-1} \cdot g \cdot yU = U \,\} \\ &= \{\, yU \in G/U \,:\, y \in G,\ y^{-1} \cdot g \cdot y \in U \,\} \,. \end{aligned}$$

Folglich ist

$$\begin{aligned} |\,\mathrm{Fix}_g(X)| &= |\{\, yU \in G/U \,:\, y \in G,\ y^{-1} \cdot g \cdot y \in U \,\}| \\ &= |U|^{-1} \cdot |\{\, y \in G \,:\, {}^{y^{-1}}g \in U \,\}| \,. \end{aligned}$$

Das wollen wir noch etwas weiter umformen.

Sei $u \in U$.

Falls $u \notin {}^{G}g \cap U$ liegt, ist $\{\, y \in G \,:\, {}^{y^{-1}}g = u \,\} = \emptyset$.

Falls $u \in {}^{G}g \cap U$ liegt, dann schreiben wir zunächst $u = {}^{z}g$ für ein $z \in G$. Es wird ${}^{y^{-1}}g = {}^{z}g$ genau dann, wenn $g = {}^{yz}g$ ist, d.h. wenn $yz \in \mathrm{C}_G(g)$ liegt, d.h. wenn $y \in \mathrm{C}_G(g)z^{-1}$ liegt. Dafür gibt es $|\mathrm{C}_G(g)|$ Möglichkeiten.

Also ist

$$\begin{aligned} |\{\, y \in G \,:\, {}^{y^{-1}}g \in U \,\}| &= \textstyle\sum_{u \in U} |\{\, y \in G \,:\, {}^{y^{-1}}g = u \,\}| \\ &= \textstyle\sum_{u \in {}^{G}g \cap U} |\{\, y \in G \,:\, {}^{y^{-1}}g = u \,\}| \\ &= \textstyle\sum_{u \in {}^{G}g \cap U} |\mathrm{C}_G(g)| \\ &= |\,{}^{G}g \cap U| \cdot |\mathrm{C}_G(g)| \,. \end{aligned}$$

Zusammen ist

$$|\,\mathrm{Fix}_g(X)| \;=\; |U|^{-1} \cdot |\,{}^{G}g \cap U| \cdot |\mathrm{C}_G(g)| \,.$$

Wir wählen noch Konjugationsklassenrepräsentanten $g_1, \ldots, g_m \in G$ und schreiben

$$G \;=\; \bigsqcup_{i \in [1,m]} {}^{G}g_i \,.$$

Wir beachten noch $|\mathrm{C}_G({}^{z}g_i)| = |\,{}^{z}\mathrm{C}_G(g_i)| = |\mathrm{C}_G(g_i)|$ für $z \in G$.

Das Fixpunktlemma gibt nun folgendes.

$$\begin{aligned}
k &\overset{\text{L. 143}}{=} \tfrac{1}{|G|} \textstyle\sum_{g\in G} |\operatorname{Fix}_g(X)| \\
&= \tfrac{1}{|G|} \textstyle\sum_{g\in G} |U|^{-1} \cdot |{}^G g \cap U| \cdot |\mathrm{C}_G(g)| \\
&= \tfrac{1}{|G|} \textstyle\sum_{i\in[1,m]} \sum_{g\in {}^G g_i} |U|^{-1} \cdot |{}^G g \cap U| \cdot |\mathrm{C}_G(g)| \\
&= \tfrac{1}{|G|} \textstyle\sum_{i\in[1,m]} \sum_{g\in {}^G g_i} |U|^{-1} \cdot |{}^G g_i \cap U| \cdot |\mathrm{C}_G(g_i)| \\
&= \tfrac{1}{|G|} \textstyle\sum_{i\in[1,m]} |U|^{-1} \cdot |{}^G g_i \cap U| \cdot |\mathrm{C}_G(g_i)| \cdot |{}^G g_i| \\
&\overset{\text{K. 141}}{=} \tfrac{1}{|G|} \textstyle\sum_{i\in[1,m]} |U|^{-1} \cdot |{}^G g_i \cap U| \cdot |G| \\
&= \tfrac{1}{|U|} \textstyle\sum_{i\in[1,m]} |{}^G g_i \cap U| \\
&= \tfrac{1}{|U|} |U| \\
&= 1 \, .
\end{aligned}$$

Was zutrifft.

2.5 Sylowsätze

Sei G eine endliche Gruppe. Sei $p \in \mathbb{Z}_{\geqslant 2}$ eine Primzahl.

Wir schreiben $|G| = p^a \cdot m$, mit $a \in \mathbb{Z}_{\geqslant 0}$ und $m \in \mathbb{Z}$ mit $m \not\equiv_p 0$. Es ist also $a = \mathrm{v}_p(|G|)$.

> Als Vorbereitung brauchen wir eine verallgemeinerte Version von Bemerkung 120.(3), welche wohl nicht mittels Homomorphiesatz gezeigt werden kann.

Bemerkung 146 *Seien H, $K \leqslant G$ gegeben mit $H \leqslant \mathrm{N}_G(K)$.*
Sei $HK := \{\, hk \,:\, h \in H,\ k \in K \,\}$.

(1) *Es ist $HK \leqslant G$.*

(2) *Es ist* $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

Beweis. Zu (1). Zunächst ist $1 = 1 \cdot 1 \in HK$.

Seien nun $h,\, \tilde{h} \in H$ und $k,\, \tilde{k} \in K$ gegeben. Es ist

$$(hk) \cdot (\tilde{h}\tilde{k})^{-1} = hk\tilde{k}^{-1}\tilde{h}^{-1} = h\tilde{h}^{-1}\, {}^{\tilde{h}}(k\tilde{k}^{-1}) \in HK \ ,$$

da wegen $H \leqslant \mathrm{N}_G(K)$ jedenfalls ${}^{\tilde{h}}(k\tilde{k}^{-1}) \in K$ ist.

Zu (2). Wir haben die surjektive Abbildung $\mu : H \times K \to HK : (h,k) \mapsto hk$.

Sei $h \in H$ und $k \in K$ gegeben. Es genügt, $|\mu^{-1}(\{hk\})| \stackrel{!}{=} |H \cap K|$ zu zeigen.

Nun ist $\mu^{-1}(\{hk\}) = \{\, (\tilde{h}, \tilde{k}) \in H \times K \,:\, \tilde{h}\tilde{k} = hk \,\} = \{\, (\tilde{h}, \tilde{k}) \in H \times K \,:\, \tilde{k}k^{-1} = \tilde{h}^{-1}h \,\}$.

Daher haben wir die Abbildung $H \cap K \to \mu^{-1}(\{hk\}) : x \mapsto (hx^{-1}, xk)$, die von der Abbildung $\mu^{-1}(\{hk\}) \to H \cap K : (\tilde{h}, \tilde{k}) \mapsto \tilde{k}k^{-1} = \tilde{h}^{-1}h$ beidseitig invertiert wird. □

Definition 147

(1) Eine *p-Gruppe* ist eine endliche Gruppe, deren Ordnung eine Potenz von p ist.

(2) Eine *p-Untergruppe* von G ist eine Untergruppe von G, die eine p-Gruppe ist, die also von Ordnung p^b ist für ein $b \in [0, a]$.

(3) Eine *p-Sylowuntergruppe* von G ist eine Untergruppe von G, die von Ordnung p^a ist. Wir schreiben

$$\mathrm{Syl}_p(G) \;:=\; \mathcal{U}_{p^a}(G) \;=\; \{\, U \,:\, U \leqslant G,\ |U| = p^a \,\}$$

für die Menge aller p-Sylowuntergruppen von G.

Manchmal nennt man eine p-Sylowuntergruppe auch kurz *p-Sylowgruppe*.

Definition 148 Sei H eine Gruppe. Sei X eine H-Menge. Sei

$$\mathrm{Fix}_H(X) \;:=\; \bigcap_{h \in H} \mathrm{Fix}_h(X) \;=\; \{\, x \in X \,:\, h \cdot x = x \text{ für } h \in H \,\}\,.$$

Bemerkung 149 *Sei H eine p-Gruppe. Sei X eine endliche H-Menge.*

Dann ist

$$|X| \;\equiv_p\; |\,\mathrm{Fix}_H(X)|\,.$$

Beweis. Wähle Bahnenrepräsentanten $x_1, \ldots, x_m \in X$. Es ist also $X = \bigsqcup_{i \in [1,m]} H \cdot x_i$.

Falls $|H \cdot x_i| = 1$, dann ist $x_i \in \mathrm{Fix}_H(X)$.

Falls $|H \cdot x_i| \neq 1$, dann ist $|H \cdot x_i|$ ein Teiler von $|H|$, der ungleich 1 ist, und also $|H \cdot x_i| \equiv_p 0$; vgl. Korollar 141.

Also ist

$$|X| \;=\; \sum_{i \in [1,m]} |H \cdot x_i| \;\equiv_p \sum_{\substack{i \in [1,m] \\ x_i \in \mathrm{Fix}_H(X)}} |H \cdot x_i| \;=\; |\,\mathrm{Fix}_H(X)|\,.$$

□

Beispiel 150 Sei H eine p-Gruppe.

Wir betrachten H als H-Menge bezüglich Konjugationsoperation.

Dann ist $|H| \equiv_p |\,\mathrm{Fix}_H(H)| = |\mathrm{Z}(H)|$.

Ist also $H \neq 1$, so ist auch $\mathrm{Z}(H) \neq 1$.

Als weitere Vorbereitung brauchen wir folgendes Lemma von Cauchy. Nachdem alles erledigt sein wird, wird dieses Lemma sich dann wiederum aus dem Satz von Sylow ergeben; vgl. Satz 154 unten.

Lemma 151 (Cauchy) *Sei* $|G| \equiv_p 0$.

Dann gibt es in G *ein Element der Ordnung* p.

Beweis. Sei H eine zyklische Gruppe der Ordnung p. Sei $H = \langle h \rangle$, wobei dann das Element h die Ordnung p hat.

Es operiert H auf $G^{\times p}$ via ${}^h(g_1, g_2, \ldots, g_p) := (g_2, g_3, \ldots, g_p, g_1)$.

Sei $X := \{\, (g_1, g_2, \ldots, g_p) \in G^{\times p} \,:\, g_1 \cdot g_2 \cdot \ldots \cdot g_p = 1 \,\} \subseteq G^{\times p}$.

Es ist X eine H-Teilmenge von $G^{\times p}$. In der Tat liegt ${}^h(g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1)$ wieder in X wegen

$$g_2 \cdot g_3 \cdot \ldots \cdot g_p \cdot g_1 \;=\; {}^{g_1^{-1}}(g_1 \cdot g_2 \cdot \ldots \cdot g_p) \;=\; {}^{g_1^{-1}}1 \;=\; 1\,.$$

Es ist $|X| = |G|^{p-1}$, da für ein Element aus X die Einträge g_1, …, g_{p-1} beliebig wählbar sind und sich $g_p = (g_1 \cdot g_2 \cdot \ldots \cdot g_{p-1})^{-1}$ ergibt. Wegen $|G| \equiv_p 0$ folgt daraus $|X| \equiv_p 0$.

Dank Bemerkung 149 ist nun

$$0 \;\equiv_p\; |X| \;\equiv_p\; |\operatorname{Fix}_H(X)|\,.$$

Da $(1, 1, \ldots, 1) \in \operatorname{Fix}_H(X)$, muß es noch ein weiteres Element in $\operatorname{Fix}_H(X)$ geben. Die Tatsache, daß dieses fix unter h ist, liefert, daß es von der Form $(g, g, \ldots, g)$ ist mit $g \neq 1$. Dann aber ist $g^p = 1$. Folglich hat das Element g eine Ordnung > 1, die p teilt und mithin gleich p ist. ▫

Lemma 152 *Sei* M *eine nichtleere endliche* G*-Menge.*

Gebe es für jedes $x \in M$ *eine* p*-Untergruppe* $P(x) \leqslant G$ *mit* $\operatorname{Fix}_{P(x)}(M) = \{x\}$.

Dann ist M *transitiv, und es ist* $|M| \equiv_p 1$.

Beweis. Wähle $n \in M$. Wir haben die G-Teilmengen $N := Gn$ und $N' := M \smallsetminus Gn$ von M. Es ist $M = N \sqcup N'$.

Es sind N und N' also auch $P(n)$-Teilmengen von M. Es ist $\operatorname{Fix}_{P(n)}(M) = \{n\}$. Dank Bemerkung 149 ist

$$|N| \;\equiv_p\; |\operatorname{Fix}_{P(n)}(N)| \;=\; |N \cap \{n\}| \;=\; |\{n\}| \;=\; 1$$

und

$$|N'| \;\equiv_p\; |\operatorname{Fix}_{P(n)}(N')| \;=\; |N' \cap \{n\}| \;=\; |\emptyset| \;=\; 0\,.$$

Da N eine transitive G-Menge ist, bleibt $N \overset{!}{=} M$ zu zeigen.

Wir haben also $N' \stackrel{!}{=} \emptyset$ zu zeigen. *Annahme*, nicht. Wähle $n' \in N'$. Dank Bemerkung 149 ist

$$0 \equiv_p |N'| \equiv_p |\operatorname{Fix}_{P(n')}(N')| = |N' \cap \{n'\}| = |\{n'\}| = 1 ,$$

Widerspruch. □

Lemma 153 *Sei* $\Omega := \{ U : U \text{ ist eine } p\text{-Untergruppe von } G \} = \bigsqcup_{b\in[0,a]} \mathcal{U}_{p^b}(G)$.

Es ist Ω *eine* G*-Teilmenge der Menge* $\mathcal{U}(G)$ *aller Untergruppen von* G*, auf welcher* G *via Konjugation operiert.*

Sei $\Omega_{\max} \subseteq \Omega$ *die Teilmenge der bezüglich Inklusion maximalen Elemente.*

(1) *Es ist* $\Omega_{\max} \neq \emptyset$.

(2) *Es ist* $\Omega_{\max}$ *eine* G*-Teilmenge von* Ω.

(3) *Für* $Q \in \Omega_{\max}$ *ist* $\operatorname{Fix}_Q(\Omega_{\max}) = \{Q\}$.

Beweis. Zu (1). Da $1 \in \Omega$ liegt und da Ω endlich ist, ist $\Omega_{\max} \neq \emptyset$.

Zu (2). Sei $P \in \Omega_{\max}$ gegeben. Sei $g \in G$. Dann ist $|{}^gP| = |P|$, also ${}^gP \in \Omega$.

Wir haben zu zeigen, daß ${}^gP$ in Ω ein maximales Element ist. Sei $Q \in \Omega$ mit ${}^gP \leqslant Q$ gegeben. Wir haben ${}^gP \stackrel{!}{=} Q$ zu zeigen.

Es ist $P = {}^{g^{-1}g}P \leqslant {}^{g^{-1}}Q$. Es ist $|{}^{g^{-1}}Q| = |Q|$, also ${}^{g^{-1}}Q \in \Omega$. Aus der Maximalität von P in Ω folgt $P = {}^{g^{-1}}Q$ und also auch ${}^gP = {}^{gg^{-1}}Q = Q$.

Zu (3). Zeigen wir $\supseteq$. Es ist ${}^gQ = Q$ für $g \in Q$. Also ist $Q \in \operatorname{Fix}_Q(\Omega_{\max})$.

Zeigen wir $\subseteq$. Sei $P \in \operatorname{Fix}_Q(\Omega_{\max})$ gegeben. Zu zeigen ist $P \stackrel{!}{=} Q$.

Wegen $P \in \operatorname{Fix}_Q(\Omega_{\max})$ ist ${}^gP = P$ für $g \in Q$, mithin $Q \leqslant \mathrm{N}_G(P)$. Dank Bemerkung 146.(1) folgt $PQ \leqslant G$. Dank Bemerkung 146.(2) folgt $|PQ| = \frac{|P|\cdot|Q|}{|P\cap Q|}$, was eine Potenz von p ist. Zusammen ist $PQ \in \Omega$.

Es ist $P \leqslant PQ$. Wegen der Maximalität von P folgt $P = PQ$.

Es ist $Q \leqslant PQ$. Wegen der Maximalität von Q folgt $Q = PQ$.

Zusammen ist $P = Q$. □

Satz 154 (Sylow) *Sei an die endliche Gruppe* G *und an die Primzahl* p *erinnert.*

Sei an $|G| = p^a \cdot m$ *mit* $m \not\equiv_p 0$ *erinnert.*

Sei an die Menge $\operatorname{Syl}_p(G) = \mathcal{U}_{p^a}(G)$ *der* p*-Sylowuntergruppen von* G *erinnert, d.h. an die Menge der Untergruppen von* G *von Ordnung* p^a.

(1) *Es ist* $\operatorname{Syl}_p(G) \neq \emptyset$.

(2) *Es ist* $\mathrm{Syl}_p(G)$ *eine transitive* G*-Menge unter der Konjugationsoperation.*

(3) *Es ist* $|\mathrm{Syl}_p(G)| \equiv_p 1$.
Für $P \in \mathrm{Syl}_p(G)$ *ist dabei* $|\mathrm{Syl}_p(G)| = |G|/|\mathrm{N}_G(P)|$*, was ein Teiler von* m *ist.*

(4) *Sei* $U \leqslant G$ *eine* p*-Untergruppe. Dann gibt es ein* $Q \in \mathrm{Syl}_p(G)$ *mit* $U \leqslant Q$.

Wegen der mehrteiligen Aussage spricht man von Satz 154 auch als von den Sylowsätzen.

Beweis. Sei $\Omega_{\max} \subseteq \Omega$ die Teilmenge der bezüglich Inklusion maximalen Elemente; vgl. Lemma 153. Dank Lemma 153.(1,2,3) können wir Lemma 152 anwenden und erhalten, daß $\Omega_{\max}$ eine transitive G-Menge ist und daß $|\Omega_{\max}| \equiv_p 1$ ist.

Um die Aussagen $(1, 2, 3, 4)$ des Satzes zu zeigen, genügt es nun,

$$\Omega_{\max} \stackrel{!}{=} \mathrm{Syl}_p(G)$$

zu zeigen. Man beachte, daß dann die zweite Aussage von (3) eine Folgerung aus (2), aus dem Bahnenlemma 140 und aus $P \leqslant \mathrm{N}_G(P) \leqslant G$ ist.

Zu $\supseteq$. Sei $P \in \mathrm{Syl}_p(G)$. Wir wollen $P \stackrel{!}{\in} \Omega_{\max}$ zeigen. Sei $Q \leqslant G$ eine p-Untergruppe mit $P \leqslant Q$. Wir haben $P \stackrel{!}{=} Q$ zu zeigen. Nun ist aber $|P| = p^a$ und $|Q| = p^b$ mit $b \in [0, a]$. Also ist $|P| = |Q|$. Also ist $P = Q$.

Zu $\subseteq$. *Annahme,* es gibt ein $Q \in \Omega_{\max}$ mit $|Q| = p^b$ mit $b < a$. Sei $N := \mathrm{N}_G(Q)$. Dank Bahnenlemma 140 ist $[G : N] = |\Omega_{\max}| \equiv_p 1$. Folglich teilt p^a auch $|N|$. Also teilt p^{a-b} den Index $[N : Q]$. Insbesondere ist $[N : Q] \equiv_p 0$.

Beachte $Q \trianglelefteqslant N$. Wir haben also die Faktorgruppe N/Q und den Restklassenmorphismus $\rho : N \to N/Q$.

Dank Lemma 151 von Cauchy gibt es in N/Q eine Untergruppe $U \leqslant N/Q$ von Ordnung p. Sei $V := \rho^{-1}(U) \leqslant N$. Da Q der Kern von $\rho : N \to N/Q$ ist, ist $Q \leqslant V$ und also Q auch der Kern des Gruppenmorphismus $\rho|_V^U : V \to U$, der ebenfalls surjektiv ist. Es folgt $|V| = |Q| \cdot |U| = |Q| \cdot p$; vgl. Bemerkung 119. Also ist $V \in \Omega$ und $Q < V$. Dies aber steht im *Widerspruch* zur Maximalität von Q. ▫

Korollar 155 *Sei* $P \in \mathrm{Syl}_p(G)$.

Genau dann ist $P \trianglelefteqslant G$*, wenn* $|\mathrm{Syl}_p(G)| = 1$ *ist.*

Beweis. Die Transitivität von $\mathrm{Syl}_p(G)$ bedeutet

$$\mathrm{Syl}_p(G) \;=\; \{\; {}^gP \;:\; g \in G \,\}\;;$$

vgl. Satz 154.(2).

Wenn $|\operatorname{Syl}_p(G)| = 1$ ist, dann muß ${}^gP = P$ sein für $g \in G$, da ansonsten ${}^gP$ eine weitere p-Sylowuntergruppe von G wäre. Es folgt $P \trianglelefteq G$.

Wenn umgekehrt $P \trianglelefteq G$ ist, dann ist ${}^gP = P$ für $g \in G$. Dies zieht wiederum $\operatorname{Syl}_p(G) = \{\, {}^gP \,:\, g \in G \,\} = \{P\}$ nach sich. Es folgt $|\operatorname{Syl}_p(G)| = 1$. ▫

Beispiel 156 Wir betrachten die Gruppe S_3.

Sei p prim.

(1) Falls $p \notin \{2, 3\}$ ist, dann ist $\operatorname{Syl}_p(\mathrm{S}_3) = \{1\}$. Das ist recht uninteressant.

(2) Sei $p = 3$. Wir schreiben $|\mathrm{S}_3| = 3^1 \cdot 2$. Es ist also $a = 1$ und $m = 2$.
Es ist $\operatorname{Syl}_3(\mathrm{S}_3) = \{\mathrm{A}_3\} = \{\langle(1, 2, 3)\rangle\}$.
Also ist $|\operatorname{Syl}_3(\mathrm{S}_3)| = 1$. Und in der Tat ist $\mathrm{A}_3 \trianglelefteq \mathrm{S}_3$; vgl. Korollar 155.

(3) Sei $p = 2$. Wir schreiben $|\mathrm{S}_3| = 2^1 \cdot 3$. Es ist also $a = 1$ und $m = 3$.
Es ist $\operatorname{Syl}_2(\mathrm{S}_3) = \{\langle(1, 2)\rangle, \langle(1, 3)\rangle, \langle(2, 3)\rangle\}$.
Es ist $\operatorname{Syl}_2(\mathrm{S}_3)$ eine transitive S_3-Menge unter der Konjugationsoperation, da die drei angeführten Erzeuger in einer Konjugationsklasse liegen.
Es ist $|\operatorname{Syl}_2(\mathrm{S}_3)| = 3 \equiv_2 1$. Und $|\operatorname{Syl}_2(\mathrm{S}_3)| = 3$ ist ein Teiler von $m = 3$.

2.6 Kleine Gruppen

2.6.1 Direkte Produkte

Definition 157 Seien G und H Gruppen.

Es wird $G \times H = \{\, (g, h) \,:\, g \in G,\ h \in H \,\}$ eine Gruppe vermöge

$$(g, h) \cdot (\tilde{g}, \tilde{h}) \ := \ (g \cdot \tilde{g},\ h \cdot \tilde{h})$$

für $(g, h), (\tilde{g}, \tilde{h}) \in G \times H$, genannt das *direkte Produkt* von G und H.

Bemerkung 158 *Sei G eine endliche Gruppe. Sei $M \trianglelefteq G$. Sei $N \trianglelefteq G$.*

Sei $M \cap N = 1$. Sei $|M| \cdot |N| = |G|$.

Dann haben wir den Gruppenisomorphismus $\varphi : M \times N \xrightarrow{\sim} G : (m, n) \mapsto m \cdot n$.

Beweis. Sei $m \in M$ und $n \in N$ gegeben. Wir *behaupten* $m \cdot n \stackrel{!}{=} n \cdot m$.

Es ist $m \cdot n \cdot m^{-1} \cdot n^{-1} \in N$ wegen $N \trianglelefteq G$. Es ist $m \cdot n \cdot m^{-1} \cdot n^{-1} \in M$ wegen $M \trianglelefteq G$. Also ist $m \cdot n \cdot m^{-1} \cdot n^{-1} = 1$, wie *behauptet*.

Es ist φ ein Gruppenmorphismus. Denn für $(m,n),\ (\tilde{m},\tilde{n}) \in M \times N$ ist

$$\varphi\big((m,n)\cdot(\tilde{m},\tilde{n})\big) \ = \ \varphi\big((m\cdot\tilde{m},\ n\cdot\tilde{n})\big) \ = \ m\cdot\tilde{m}\cdot n\cdot\tilde{n} \ = \ m\cdot n\cdot\tilde{m}\cdot\tilde{n} \ = \ \varphi\big((m,n)\big)\cdot\varphi\big((\tilde{m},\tilde{n})\big) \ .$$

Es ist φ injektiv. Denn ist $(m,n) \in \mathrm{Kern}(\varphi)$, dann ist $m\cdot n = 1$, also $m = n^{-1} \in M \cap N = 1$, also $m = 1$ und $n = 1$.

Es ist φ surjektiv. Denn $|\varphi(M \times N)| = |MN| = |M| \cdot |N| / |M \cap N| = |G|$; vgl. Bemerkung 120.(3).

2.6.2 Diedergruppen

Definition 159 Sei $n \in \mathbb{Z}_{\geqslant 1}$.

Sei $a := (1, 2, \ldots, n) \in \mathrm{S}_n$. Es ist $|\langle a \rangle| = n$.

Falls $n \geqslant 3$ und $n \equiv_2 0$ ist, dann schreiben wir $n = 2k$ mit $k \geqslant 2$ und setzen

$$b \ := \ (2, 2k)(3, 2k-1) \ldots (k, k+2) \ .$$

Falls $n \geqslant 3$ und $n \equiv_2 1$ ist, dann schreiben wir $n = 2k+1$ mit $k \geqslant 1$ und setzen

$$b \ := \ (2, 2k+1)(3, 2k) \ldots (k+1, k+2) \ .$$

In beiden Fällen ist $|\langle b \rangle| = 2$.

Ferner ist ${}^{b}a = a^{-1}$, d.h. $b \circ a = a^{-1} \circ b$. Also ist $\langle a, b \rangle = \{\, a^i \circ b^j \ : \ i \in [0, n-1],\ j \in [0,1] \,\}$.

(1) Wir bezeichnen mit $\mathrm{C}_n := \langle a \rangle \leqslant \mathrm{S}_n$ diese zyklische Gruppe von Ordnung $|\mathrm{C}_n| = n$.

(2) Sei $n \geqslant 3$. Wir bezeichnen mit

$$\mathrm{D}_{2n} \ := \ \langle a, b \rangle \ = \ \{\, a^i \circ b^j \ : \ i \in [0, n-1],\ j \in [0,1] \,\} \ \leqslant \ \mathrm{S}_n$$

die *Diedergruppe* von Ordnung $|\mathrm{D}_{2n}| = 2n$.

In der Tat ist $\mathrm{C}_n < \mathrm{D}_{2n}$, da $b \notin \mathrm{C}_n$ liegt. Denn falls $n \equiv_2 0$ ist, dann ist $k+1$ fix unter b, nicht aber unter $a^{n/2}$, weswegen $b \neq a^{n/2}$ ist.

Also ist n ein Teiler von $|\mathrm{D}_{2n}|$. Ferner ist $n < |\mathrm{D}_{2n}| \leqslant 2n$, wie angemerkt. Also muß $|\mathrm{D}_{2n}| = 2n$ sein.

Beispiel 160

(1) Es ist $\mathrm{D}_6 = \langle\, (1,2,3),\ (2,3) \rangle = \mathrm{S}_3$.

(2) Es ist $\mathrm{D}_8 = \langle\, (1,2,3,4),\ (2,4)\,\rangle \leqslant \mathrm{S}_4$ eine 2-Sylowgruppe von S_4 .

(3) Es ist $\mathrm{D}_{10} = \langle (1,2,3,4,5),\ (2,5)(3,4) \rangle \leqslant \mathrm{S}_5$.

Bemerkung 161 *Sei $p \geqslant 2$ eine Primzahl.*

Sei G eine Gruppe von Ordnung $|G| = p$.

Dann ist $G \simeq \mathrm{C}_p$.

Beweis. Wähle $x \in G \smallsetminus \{1\}$. Dann ist $|\langle x\rangle|$ ungleich 1 und ein Teiler von $|G| = p$. Also ist $|\langle x\rangle| = p = |G|$. Also ist $\langle x\rangle = G$.

Wir haben den Isomorphismus $\mathrm{C}_p \xrightarrow{\sim} G : a^i \mapsto x^i$ für $i \in [0, p-1]$. ▫

Bemerkung 162 *Sei $p \geqslant 3$ eine Primzahl.*

Sei G eine Gruppe von Ordnung $|G| = 2p$.

Dann ist $G \simeq \mathrm{C}_p \times \mathrm{C}_2$ oder $G \simeq \mathrm{D}_{2p}$.

Beweis. Sei N eine p-Sylowgruppe von G. Dann ist $N \trianglelefteq G$; vgl. Bemerkung 104.

Sei U eine 2-Sylowgruppe von G.

Fall: $U \trianglelefteq G$. Dann ist $|N \cap U| = 1$ und $|N| \cdot |U| = |G|$, also $G \simeq N \times U \simeq \mathrm{C}_p \times \mathrm{C}_2$; vgl. Bemerkungen 158, 161.

Fall: U nicht normal in G.

Es ist $N \simeq \mathrm{C}_p$; vgl. Bemerkung 161. Wähle $x \in N$ mit $N = \langle x\rangle$.

Es ist $U \simeq \mathrm{C}_2$; vgl. Bemerkung 161. Wähle $y \in U$ mit $U = \langle y\rangle$.

Es teilt $|U \cap N|$ sowohl $|U| = 2$ als auch $|N| = p$. Somit ist $U \cap N = 1$ und also $NU = G$; vgl. Bemerkung 120.(2, 3).

Wegen $N \trianglelefteq G$ ist ${}^y x = x^k$ für ein $k \in [0, p-1]$. Da $x = {}^{y^2}x = {}^y({}^y x) = {}^y(x^k) = (x^k)^k = x^{(k^2)}$, ist $k^2 \equiv_p 1$. Da $\mathbb{F}_p$ ein Körper ist, gibt es hierfür nur die beiden Lösungen $k \in \{-1, +1\}$.

Wäre $k = 1$, dann wäre $xy = yx$ und also $U \trianglelefteq G$, was *nicht* der Fall ist.

Also ist $k = -1$. Wir haben also $G = NU = \{\, x^i y^j \;:\; i \in [0, p-1],\ j \in [0, 1] \,\}$ erhalten, sowie ${}^y x = x^{-1}$.

Auch sind in G damit $2p$ verschiedene Elemente aufgelistet.

Wir haben also die Multiplikationsregel

$$x^i y^j \cdot x^{i'} y^{j'} \;=\; x^{i+(-1)^j \cdot i'} y^{j+j'}$$

für $i,\, i' \in [0, p-1]$ und $j,\, j' \in [0, 1]$.

In D_{2p} gilt entsprechend $a^p = \mathrm{id}$, $b^2 = \mathrm{id}$ und ${}^b a = a^{-1}$; vgl. Definition 159. Somit gilt auch

$$(a^i \circ b^j) \circ (a^{i'} \circ b^{j'}) \;=\; a^{i+(-1)^j \cdot i'} \circ b^{j+j'}$$

für $i,\, i' \in [0, p-1]$ und $j,\, j' \in [0, 1]$.

Folglich haben wir den Gruppenisomorphismus $\mathrm{D}_{2p} \xrightarrow{\sim} G : a^i \circ b^j \mapsto x^i y^j$ für $i \in [0, p-1]$ und $j \in [0, 1]$. ▫

Beispiel 163 Sei G eine Gruppe von Ordnung $|G| = 15$.

Wir wollen zeigen, daß $G \overset{!}{\simeq} \mathrm{C}_3 \times \mathrm{C}_5$ ist.

Sei M eine 3-Sylowgruppe von G. Die Anzahl der 3-Sylowgruppen ist $\equiv_3 1$ und teilt 5, sie ist also gleich 1. Folglich ist $M \trianglelefteq G$.

Sei N eine 5-Sylowgruppe von G. Die Anzahl der 5-Sylowgruppen ist $\equiv_5 1$ und teilt 3, sie ist also gleich 1. Folglich ist $N \trianglelefteq G$.

Es ist $M \simeq \mathrm{C}_3$ und $N \simeq \mathrm{C}_5$.

Es ist $M \cap N = 1$, da die Ordnungen teilerfremd sind.

Es ist $|M| \cdot |N| = 3 \cdot 5 = 15$.

Dank Bemerkung 158 folgt $G \simeq M \times N \simeq \mathrm{C}_3 \times \mathrm{C}_5$.

Es gibt also im wesentlichen nur eine Gruppe von Ordnung 15.

2.6.3 Endliche abelsche Gruppen

In diesem Abschnitt §2.6.3 werden bis Bemerkung 172 abelsche Gruppen additiv geschrieben.

Satz 164 (Elementarteilersatz) *Sei R ein euklidischer Ring, mit Gradfunktion d.*

Seien m, $n \geqslant 1$. Sei $A = (a_{i,j})_{i,j} \in R^{m \times n}$.

Dann gibt es $S \in \mathrm{GL}_m(R)$ und $T \in \mathrm{GL}_n(R)$ derart, daß

$$SAT \;=\; D$$

ist, wobei

$$D = \sum_{i \in [1,k]} x_i \, \mathrm{e}_{i,i} \ ,$$

wobei $k \in [0, \min\{m, n\}]$ und wobei $x_i \in R^\times$ für $i \in [1, k]$ mit $(x_1) \supseteq (x_2) \supseteq \ldots \supseteq (x_k)$.

Eine solche Matrix D heißt *in Elementarteilerform.*

Beweis. Die Addition eines Vielfachen einer Zeile zu einer anderen entspricht der Multiplikation mit einem Element aus $\mathrm{GL}_m(R)$ von links. Genauso die Vertauschung von Zeilen.

Entsprechend für Spalten und Multiplikation mit einem Element aus $\mathrm{GL}_n(R)$ von rechts.

Wir nennen $\{ (i,1) : i \in [2,m] \} \cup \{ (1,j) : j \in [2,n] \}$ provisorisch den *Rand* der Matrix. Der Rand ist also die Menge der Positionen in der ersten Spalte oder in der ersten Zeile, ausgenommen die Position $(1,1)$.

Falls $A \neq 0$, dann genügt es, solche Zeilen- und Spaltenoperationen anzugeben, die aus A eine Matrix machen mit Eintrag 0 im Rand und einem Eintrag ungleich 0 an Position $(1,1)$, der alle Matrixeinträge teilt.

Denn dies kann man dann in einem weiteren Schritt für den Block im Bereich $[2,m] \times [2,n]$ anwenden, falls dieser Block ungleich 0 ist. Dann für den Block im Bereich $[3,m] \times [3,n]$, falls dieser ungleich 0 ist. Usf.

Dafür gehen wir wie folgt vor.

(1) Wir tauschen einen Eintrag von A ungleich 0 und mit minimalem Grad durch Zeilen- und Spaltenvertauschungen an Position $(1,1)$.

(2) Wir verwenden, daß R ein euklidischer Ring ist, um derart Vielfache der ersten Zeile zu den weiteren Zeilen zu addieren, daß die entstehenden Einträge in der ersten Spalte gleich 0 sind oder aber kleineren Grad als der Eintrag bei $(1,1)$ haben. Ferner addieren wir derart Vielfache der ersten Spalte zu den weiteren Spalten, daß die entstehenden Einträge in der ersten Zeile gleich 0 sind oder aber kleineren Grad als der Eintrag bei $(1,1)$ haben.

(3) Falls nun im Rand ein Eintrag ungleich 0 entstanden ist, so springen wir zum Schritt (1).

(4) Nun sind die Einträge im Rand alle gleich 0.

(5) Falls der Eintrag an Position $(1,1)$ nicht alle Einträge teilt, so wählen wir eine Position (k,ℓ) mit einem Eintrag, den er nicht teilt. Wir addieren die erste Zeile zur k-ten Zeile. Wir addieren derart ein Vielfaches der ersten Spalte zur ℓ-ten Spalte, daß an Position (k,ℓ) ein Eintrag entsteht, dessen Grad kleiner ist als der Grad des Eintrags an Position $(1,1)$. Wir springen zum Schritt (1).

(6) Nun sind die Einträge im Rand alle gleich 0. Und der Eintrag an Position $(1,1)$ teilt alle Matrixeinträge.

Springt man von (3) nach (1) oder springt man von (5) nach (1), ist der minimale Grad eines nichtverschwindenden Matrixeintrags echt kleiner geworden.

Somit muß der Algorithmus nach endlich vielen Schritten sein Ende in (6) erreichen. □

Beispiel 165 Sei $A = \begin{pmatrix} 7 & 7 & -6 \\ 5 & 1 & 8 \\ -4 & -6 & 10 \end{pmatrix} \in \mathbb{Z}^{3\times 3}$.

Wir suchen $D \in \mathbb{Z}^{3\times 3}$ diagonal, mit konsekutiven Teilern auf der Diagonalen, $S \in \mathrm{GL}_3(\mathbb{Z})$ und $T \in \mathrm{GL}_3(\mathbb{Z})$ mit $SAT = D$ wie in Satz 164.

Wir rechnen, wie vom Algorithmus vorgegeben, auch wenn Abkürzungen möglich wären.

$$\begin{pmatrix} 7 & 7 & -6 \\ 5 & 1 & 8 \\ -4 & -6 & 10 \end{pmatrix} \overset{(-)\cdot\left(\begin{smallmatrix} 0&1&0\\1&0&0\\0&0&1 \end{smallmatrix}\right)}{\rightsquigarrow} \begin{pmatrix} 7 & 7 & -6 \\ 1 & 5 & 8 \\ -6 & -4 & 10 \end{pmatrix} \overset{\left(\begin{smallmatrix} 0&1&0\\1&0&0\\0&0&1 \end{smallmatrix}\right)\cdot(-)}{\rightsquigarrow} \begin{pmatrix} 1 & 5 & 8 \\ 7 & 7 & -6 \\ -6 & -4 & 10 \end{pmatrix} \overset{\left(\begin{smallmatrix} 1&0&0\\-7&1&0\\6&0&1 \end{smallmatrix}\right)\cdot(-)}{\rightsquigarrow} \begin{pmatrix} 1 & 5 & 8 \\ 0 & -28 & -62 \\ 0 & 26 & 58 \end{pmatrix} \overset{(-)\cdot\left(\begin{smallmatrix} 1&-5&-8\\0&1&0\\0&0&1 \end{smallmatrix}\right)}{\rightsquigarrow}$$

$$\begin{pmatrix}1&0&0\\0&-28&-62\\0&26&58\end{pmatrix} \overset{\left(\begin{smallmatrix}1&0&0\\0&0&1\\0&1&0\end{smallmatrix}\right)\cdot(-)}{\rightsquigarrow} \begin{pmatrix}1&0&0\\0&26&58\\0&-28&-62\end{pmatrix} \overset{\left(\begin{smallmatrix}1&0&0\\0&1&0\\0&2&1\end{smallmatrix}\right)\cdot(-)}{\rightsquigarrow} \begin{pmatrix}1&0&0\\0&26&58\\0&24&54\end{pmatrix} \overset{(-)\cdot\left(\begin{smallmatrix}1&0&0\\0&1&-2\\0&0&1\end{smallmatrix}\right)}{\rightsquigarrow} \begin{pmatrix}1&0&0\\0&26&6\\0&24&6\end{pmatrix} \overset{(-)\cdot\left(\begin{smallmatrix}1&0&0\\0&0&1\\0&1&0\end{smallmatrix}\right)}{\rightsquigarrow}$$

$$\begin{pmatrix}1&0&0\\0&6&26\\0&6&24\end{pmatrix} \overset{\left(\begin{smallmatrix}1&0&0\\0&1&0\\0&-1&1\end{smallmatrix}\right)\cdot(-)}{\rightsquigarrow} \begin{pmatrix}1&0&0\\0&6&26\\0&0&-2\end{pmatrix} \overset{(-)\cdot\left(\begin{smallmatrix}1&0&0\\0&1&-4\\0&0&1\end{smallmatrix}\right)}{\rightsquigarrow} \begin{pmatrix}1&0&0\\0&6&2\\0&0&-2\end{pmatrix} \overset{(-)\cdot\left(\begin{smallmatrix}1&0&0\\0&0&1\\0&1&0\end{smallmatrix}\right)}{\rightsquigarrow} \begin{pmatrix}1&0&0\\0&2&6\\0&-2&0\end{pmatrix} \overset{\left(\begin{smallmatrix}1&0&0\\0&1&0\\0&1&1\end{smallmatrix}\right)\cdot(-)}{\rightsquigarrow}$$

$$\begin{pmatrix}1&0&0\\0&2&6\\0&0&6\end{pmatrix} \overset{(-)\cdot\left(\begin{smallmatrix}1&0&0\\0&1&-3\\0&0&1\end{smallmatrix}\right)}{\rightsquigarrow} \begin{pmatrix}1&0&0\\0&2&0\\0&0&6\end{pmatrix} =: D\,.$$

Wir multiplizieren die operierenden Matrizen zusammen, getrennt nach links und rechts.

$$S := \begin{pmatrix}1&0&0\\0&1&0\\0&1&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&-1&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&2&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}\begin{pmatrix}1&0&0\\-7&1&0\\6&0&1\end{pmatrix}\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix} = \begin{pmatrix}0&1&0\\0&6&1\\1&5&2\end{pmatrix}$$

$$T := \begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&-5&-8\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&-2\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&-4\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&-3\\0&0&1\end{pmatrix} = \begin{pmatrix}0&9&-29\\1&-13&41\\0&-4&13\end{pmatrix}$$

In der Tat ist nun $SAT = D$.

Definition 166 Eine abelsche Gruppe A heißt *endlich erzeugt*, wenn es ein $k \geqslant 0$ und Elemente $a_1, \ldots, a_k \in A$ gibt mit $A = \langle a_1, \ldots, a_k \rangle$.

Beispiel 167

(1) Endliche abelsche Gruppen sind endlich erzeugt.

(2) Die abelsche Gruppe $\mathbb{Z} = (\mathbb{Z}, +)$ ist endlich erzeugt wegen $\mathbb{Z} = \langle 1 \rangle$. Aber $\mathbb{Z}$ ist nicht endlich.

(3) Sei $n \geqslant 1$. Die abelsche Gruppe $\mathbb{Z}^{n\times 1} = (\mathbb{Z}^{n\times 1}, +)$ ist endlich erzeugt.

Bemerkung 168 *Sei A eine abelsche Gruppe. Sei $B \leqslant A$.*

Seien B und A/B endlich erzeugt.

Dann ist A endlich erzeugt.

Beweis. Schreibe $B = \langle b_1, \ldots, b_\ell \rangle$ und $A/B = \langle a_1 + B, \ldots, a_k + B \rangle$, wobei $k, \ell \geqslant 0$ und $b_1, \ldots, b_\ell \in B$ und $a_1, \ldots, a_k \in A$.

Wir behaupten $A \overset{!}{=} \langle a_1, \ldots, a_k, b_1, \ldots, b_\ell \rangle$. Sei $x \in A$ gegeben. Wir haben zu zeigen, daß x in der rechten Seite liegt.

Schreibe $x+B = z_1(a_1+B)+\ldots+z_k(a_k+B) = (z_1a_1+\ldots+z_ka_k)+B$, mit $z_1, \ldots, z_k \in \mathbb{Z}$. Es folgt $x = z_1a_1 + \ldots + z_ka_k + b$ für ein $b \in B$. Schreibe $b = w_1b_1 + \ldots + w_\ell b_\ell$ mit $w_1, \ldots, w_\ell \in \mathbb{Z}$. Insgesamt wird $x = z_1a_1 + \ldots + z_ka_k + w_1b_1 + \ldots + w_\ell b_\ell$, was in der rechten Seite liegt. ▫

Bemerkung 169 *Sei A eine abelsche Gruppe. Sei $B \leqslant A$.*

Sei A endlich erzeugt.

Dann ist B endlich erzeugt.

Beweis. Sei o.E. $A \neq 0$.

Induktion über die Anzahl der Erzeuger.

Schreibe $A = \langle a_1 , \ldots , a_k \rangle$, wobei $k \geqslant 1$ und $a_1 , \ldots , a_k \in A$.

Fall $k = 1$ (Induktionsanfang). Es ist $A = \langle a_1 \rangle = \{ za_1 \, : \, z \in \mathbb{Z} \}$. O.E. ist $B \neq 0$. Sei $w \in \mathbb{Z}_{\geqslant 1}$ minimal mit $wa_1 \in B$. Dann ist $B = \langle wa_1 \rangle$. Denn ist $za_1 \in B$ für ein $z \in \mathbb{Z}$, dann können wir $z = wq + r$ schreiben, mit $q, r \in \mathbb{Z}$ und $r \in [0, w-1]$. Es ist auch $ra_1 = za_1 - qwa_1 \in B$. Die Minimalität von w erzwingt $r = 0$ und also $za_1 = qwa_1 \in \langle wa_1 \rangle$.

Fall $k \geqslant 2$ (Induktionsschritt).

Sei $\tilde{A} := \langle a_2 , \ldots , a_k \rangle \leqslant A$. Es ist $B \cap \tilde{A} \leqslant \tilde{A}$. Also ist $B \cap \tilde{A}$ endlich erzeugt nach Induktionsvoraussetzung.

Es ist $B \cap \tilde{A}$ der Kern des Gruppenmorphismus $\varphi : B \to A/\tilde{A} : b \mapsto b + \tilde{A}$.

Es ist $\varphi(B) \leqslant A/\tilde{A} = \langle a_1 + \tilde{A} \rangle$. Nach Fall $k = 1$ ist also $\varphi(B)$ endlich erzeugt. Nach Homomorphiesatz ist $\varphi(B) \simeq B/\operatorname{Kern}(\varphi) = B/(B \cap \tilde{A})$; vgl. Satz 118.

Somit sind $B \cap \tilde{A}$ und $B/(B \cap \tilde{A})$ endlich erzeugt. Folglich ist auch B endlich erzeugt; vgl. Bemerkung 168. ▫

Satz 170 *Sei A eine endlich erzeugte abelsche Gruppe.*

Dann gibt es $r \in \mathbb{Z}_{\geqslant 0}$ und $k \in \mathbb{Z}_{\geqslant 0}$ und $x_1 , \ldots , x_k \in \mathbb{Z}_{\geqslant 1}$ mit $(x_1) \supseteq (x_2) \supseteq \ldots \supseteq (x_k)$ und mit

$$A \simeq \mathbb{Z}/(x_1) \times \mathbb{Z}/(x_2) \times \ldots \times \mathbb{Z}/(x_k) \times \mathbb{Z}^{\times r} .$$

Beweis. Schreibe $A = \langle a_1 , \ldots , a_m \rangle$, wobei $m \geqslant 0$ und $a_1 , \ldots , a_m \in A$.

Wir haben den surjektiven Gruppenmorphismus $\varphi : \mathbb{Z}^{m \times 1} \to A : \mathrm{e}_i \mapsto a_i$ für $i \in [1, m]$. Es ist dann $\varphi((z_i)_i) = z_1 a_1 + \ldots + z_m a_m$.

Es ist $\operatorname{Kern}(\varphi)$ als Untergruppe von $\mathbb{Z}^{m \times 1}$ endlich erzeugt; vgl. Bemerkung 169. Schreibe $\operatorname{Kern}(\varphi) = \langle b_1 , \ldots , b_n \rangle$, wobei $n \geqslant 0$ und $b_1 , \ldots , b_n \in \operatorname{Kern}(\varphi) \leqslant \mathbb{Z}^{m \times 1}$.

Wir haben den surjektiven Gruppenmorphismus $\psi : \mathbb{Z}^{n \times 1} \to \operatorname{Kern}(\varphi) : \mathrm{e}_j \mapsto b_j$ für $j \in [1, n]$. Es ist dann $\psi((w_j)_j) = w_1 b_1 + \ldots + w_n b_n$.

Sei $\iota : \operatorname{Kern}(\varphi) \to \mathbb{Z}^{m \times 1}$ die Einbettung, was ein injektiver Gruppenmorphismus ist.

Sei $B \in \mathbb{Z}^{m \times n}$ die Matrix mit Spaltentupel $(b_1, \ldots, b_n)$. Es bildet $\iota \circ \psi$ das Element e_ℓ ab auf $b_\ell = B \cdot \mathrm{e}_\ell$. Daher ist $\iota \circ \psi : \mathbb{Z}^{n \times 1} \to \mathbb{Z}^{m \times 1} : x \mapsto B \cdot x$.

$$\mathbb{Z}^{n\times 1} \xrightarrow{B\cdot(-)} \mathbb{Z}^{m\times 1} \xrightarrow{\varphi} A\,.$$

Nach Homomorphiesatz ist $A \simeq \mathbb{Z}^{m\times 1}/\operatorname{Kern}(\varphi)$; vgl. Satz 31. Nun ist $\operatorname{Kern}(\varphi) = \psi(\mathbb{Z}^{m\times 1}) = \iota(\psi(\mathbb{Z}^{m\times 1})) = B\cdot\mathbb{Z}^{n\times 1}$. Also ist

$$A \simeq \mathbb{Z}^{m\times 1}/(B\cdot\mathbb{Z}^{n\times 1})\,.$$

Dank Elementarteilersatz können wir $S \in \mathrm{GL}_m(\mathbb{Z})$ und $T \in \mathrm{GL}_n(\mathbb{Z})$ wählen mit $SBT = D$, wobei $D = x_1\,\mathrm{e}_{1,1} + \ldots + x_k\,\mathrm{e}_{k,k}$, wobei $k \geqslant 0$ und $x_1, \ldots, x_k \in \mathbb{Z}^\times$ sind mit $(x_1) \supseteq (x_2) \supseteq \ldots \supseteq (x_k)$; vgl. Satz 164. Durch Multiplikation mit einer Diagonalmatrix können wir noch $x_i \geqslant 1$ erreichen für $i \in [1,k]$.

Es ist $B\cdot\mathbb{Z}^{n\times 1} = S^{-1}DT^{-1}\mathbb{Z}^{n\times 1} = S^{-1}D\mathbb{Z}^{n\times 1}$, da $T^{-1}\mathbb{Z}^{n\times 1} = \mathbb{Z}^{n\times 1}$ ist wegen T invertierbar.

Ferner haben wir den Gruppenisomorphismus

$$\begin{array}{rcl} \mathbb{Z}^{m\times 1}/(B\cdot\mathbb{Z}^{n\times 1}) = \mathbb{Z}^{m\times 1}/(S^{-1}D\cdot\mathbb{Z}^{n\times 1}) & \xrightarrow{\sim} & \mathbb{Z}^{m\times 1}/(D\cdot\mathbb{Z}^{n\times 1}) \\ y + (S^{-1}D\cdot\mathbb{Z}^{n\times 1}) & \mapsto & Sy + (D\cdot\mathbb{Z}^{n\times 1}) \\ S^{-1}y + (S^{-1}D\cdot\mathbb{Z}^{n\times 1}) & \mapsfrom & y + (D\cdot\mathbb{Z}^{n\times 1}) \end{array}$$

wofür man Lemma 117 zweimal zum Einsatz bringen kann.

Schließlich haben wir, mit $r := m - k$, den Gruppenisomorphismus

$$\begin{array}{rcl} \mathbb{Z}^{m\times 1}/(D\cdot\mathbb{Z}^{n\times 1}) & \xrightarrow{\sim} & \mathbb{Z}/(x_1)\times\mathbb{Z}/(x_2)\times\ldots\times\mathbb{Z}/(x_k)\times\mathbb{Z}^{\times r} \\ (z_i)_i + (D\cdot\mathbb{Z}^{n\times 1}) & \mapsto & (z_1+(x_1), z_2+(x_2), \ldots, z_k+(x_k), z_{k+1}, \ldots, z_m) \\ (z_i)_i + (D\cdot\mathbb{Z}^{n\times 1}) & \mapsfrom & (z_1+(x_1), z_2+(x_2), \ldots, z_k+(x_k), z_{k+1}, \ldots, z_m)\,. \end{array}$$

Zusammengesetzt ergibt dies $A \simeq \mathbb{Z}/(x_1)\times\mathbb{Z}/(x_2)\times\ldots\times\mathbb{Z}/(x_k)\times\mathbb{Z}^{\times r}$. ▫

Korollar 171 *Sei A eine endliche abelsche Gruppe.*

Dann gibt es $k \in \mathbb{Z}_{\geqslant 0}$ und $x_1, \ldots, x_k \in \mathbb{Z}_{\geqslant 2}$ mit $(x_1) \supseteq (x_2) \supseteq \ldots \supseteq (x_k)$ und mit

$$A \simeq \mathbb{Z}/(x_1)\times\mathbb{Z}/(x_2)\times\ldots\times\mathbb{Z}/(x_k)\,.$$

Dabei ist $|A| = x_1\cdot x_2\cdot\ldots\cdot x_k$.

Beweis. Dies folgt aus Satz 170, da A nur für $r = 0$ endlich sein kann. Man beachte noch, daß $\mathbb{Z}/(1)$ nur ein Element hat und daher als Faktor entfallen kann, ohne die Isomorphieklasse zu ändern. ▫

Bemerkung 172 Wir erinnern an den Chinesischen Restsatz, welchen wir nun für $\mathbb{Z}$ anwenden wollen; vgl. Satz 34.

Seien $y_1, y_2, \ldots, y_\ell \in \mathbb{Z}^\times$ paarweise teilerfremd gegeben. Dann ist $(y_i) + (y_j) = (y_i, y_j) = \mathbb{Z}$ für $i, j \in [1,\ell]$ mit $i \neq j$.

Sei $y := y_1 \cdot y_2 \cdot \ldots \cdot y_\ell$. Dann ist $(y) = (y_1) \cap (y_2) \cap \ldots \cap (y_\ell)$, da eine ganze Zahl genau dann durch y teilbar ist, wenn sie durch $y_1, \ldots, y_\ell$ teilbar ist.

Also haben wir den Ringisomorphismus

$$\begin{array}{rccccccccc} \varphi & : & \mathbb{Z}/(y) & \xrightarrow{\sim} & \mathbb{Z}/(y_1) & \times & \mathbb{Z}/(y_2) & \times & \ldots & \times & \mathbb{Z}/(y_\ell) \\ & & z+(y) & \mapsto & (z+(y_1) & , & z+(y_2) & , & \ldots & , & z+(y_\ell)) \end{array}$$

Dies ist insbesondere ein Gruppenisomorphismus der additiven Gruppen dieser Ringe.

Bemerkung 173 Sei $n \in \mathbb{Z}^\times$.

Die additiv geschriebene zyklische Gruppe $\mathbb{Z}/(n)$ ist isomorph zur multiplikativ geschriebenen zyklischen Gruppe C_n .

> Eine wirklich gute Schreibweise für zyklische und abelsche Gruppen, die in allen Lagen paßt, scheint es nicht zu geben.

Beispiel 174

(1) Wir wollen bis auf Isomorphie alle abelschen Gruppen der Ordnung 8 auflisten.

In der Bezeichnung von Korollar 171 muß das Produkt der Zahlen $x_1, \ldots, x_k$ gleich 8 sein. Wir erhalten also die folgenden Möglichkeiten in additiver Schreibweise.

$$\mathbb{Z}/(8) \ , \ \ \mathbb{Z}/(2) \times \mathbb{Z}/(4) \ , \ \ \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2) \ .$$

Jede abelsche Gruppe der Ordnung 8 ist zu einer dieser Gruppen isomorph.

Und diese drei Gruppen sind paarweise nichtisomorph. Denn die erste Gruppe enthält ein Element der Ordnung 8, die anderen beiden nicht. Und die zweite Gruppen enthält ein Element der Ordnung 4, die dritte nicht.

Dasselbe, nur multiplikativ geschrieben :

$$\mathrm{C}_8 \ , \ \ \mathrm{C}_2 \times \mathrm{C}_4 \ , \ \ \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2 \ .$$

(2) Wir wollen bis auf Isomorphie alle abelschen Gruppen der Ordnung 12 auflisten.

Unter Verwendung von Korollar 171 erhalten wir die folgenden Möglichkeiten in additiver Schreibweise.

$$\mathbb{Z}/(12) \ , \ \ \mathbb{Z}/(2) \times \mathbb{Z}/(6)$$

Unter Verwendung von Bemerkung 172 erhalten wir die folgenden Möglichkeiten in additiver Schreibweise.

$$\mathbb{Z}/(4) \times \mathbb{Z}/(3) \ , \ \ \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(3) \ .$$

Diese beiden Gruppen sind nichtisomorph, da die erste ein Element der Ordnung 4 enthält, nicht aber die zweite.

Dasselbe, nur multiplikativ geschrieben :

$$\mathrm{C}_4 \times \mathrm{C}_3 \ , \ \ \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_3 \ .$$

2.6.4 Zwei Lemmas für kleine Gruppen

Lemma 175 *Sei G eine endliche Gruppe.*

Dann kann $[G : \mathrm{Z}(G)]$ nicht prim sein.

Beweis. Annahme, $p := [G : \mathrm{Z}(G)]$ ist prim. Es ist $G/\mathrm{Z}(G)$ zyklisch. Schreibe $G/\mathrm{Z}(G) = \langle x\mathrm{Z}(G)\rangle$, wobei $x \in G$. Dann ist $G = \{\, x^i z \,:\, i \in [0, p-1],\ z \in \mathrm{Z}(G) \,\}$.

Seien nun $x^i z,\ x^j w \in G$, wobei $i,\ j \in [0, p-1]$ und $z,\ w \in \mathrm{Z}(G)$. Dann wird

$$x^i z \cdot x^j w \ = \ x^{i+j} \cdot z \cdot w \ = \ x^{j+i} \cdot w \cdot z \ = \ x^j w \cdot x^i z \ .$$

Also ist G abelsch. Also ist $G = \mathrm{Z}(G)$. Folglich ist $[G : \mathrm{Z}(G)] = 1 < p$. Wir haben einen *Widerspruch.* ▫

Beispiel 176 Sei p eine Primzahl. Sei G eine Gruppe der Ordnung p^2.

Dann ist $|\mathrm{Z}(G)| \in \{p, p^2\}$; vgl. Beispiel 150.

Dank Lemma 175 ist $[G : \mathrm{Z}(G)] \neq p$ und also $|\mathrm{Z}(G)| \neq p$.

Somit ist $|\mathrm{Z}(G)| = p^2$, mithin $\mathrm{Z}(G) = G$. Also ist G abelsch.

Folglich ist $G \simeq \mathrm{C}_p \times \mathrm{C}_p$ oder $G \simeq \mathrm{C}_{p^2}$; vgl. Korollar 171.

Lemma 177 *Sei G eine endliche Gruppe. Sei $1 < U \leqslant G$.*

Sei p der kleinste Primteiler von $|U|$.

Ist $[G : U] \leqslant p$, dann ist $U \trianglelefteq G$.

Dies ist eine Verallgemeinerung von Bemerkung 104.

Beweis. Es operiert G auf G/U durch Multiplikation von links. Also operiert auch U auf G/U durch Multiplikation von links.

Die Bahn von $1 \cdot U$ ist $\{1 \cdot U\}$. Somit hat jede andere Bahn dieser Operation eine Elementzahl $\leqslant |(G/U) \smallsetminus \{1 \cdot U\}| = [G : U] - 1 \leqslant p - 1$. Diese Elementzahl teilt aber $|U|$; vgl. Korollar 141. Der einzige Teiler von $|U|$, der $\leqslant p-1$ ist, ist 1. Also enthalten alle Bahnen dieser Operation nur ein Element.

Es folgt $u \cdot gU = gU$ für $u \in U$ und $g \in G$. Also ist ${}^{g^{-1}}u \in U$ für $g \in G$ und $u \in U$. Somit ist $U \trianglelefteq G$. ▫

2.6.5 Einfache Gruppen

Definition 178 Sei G eine Gruppe mit $G \neq 1$.

Es heißt G *einfach*, wenn G nur die Normalteiler 1 und G hat.

Beispiel 179

(1) Sei p eine Primzahl. Es ist C_p einfach.

(2) Die Gruppe A_4 ist nicht einfach.

Denn in ihr gibt es den Normalteiler $V := \langle\, (1,2)(3,4),\ (1,3)(2,4) \,\rangle$ von Ordnung 4.

Satz 180 *Sei $n \geqslant 5$. Die alternierende Gruppe A_n ist einfach.*

Beweis. Annahme, es gibt $1 < N \lhd \mathrm{A}_n$.

Wir *behaupten,* daß es $1 < M \lhd \mathrm{A}_n$ gibt mit $M \trianglelefteq \mathrm{S}_n$.

Sei $x \in {}^tN$ für $t \in \{\mathrm{id}, (1,2)\}$ und $f \in \mathrm{S}_n$. Schreibe $x = {}^t y$ mit $y \in N$. Schreibe $f = s \circ g$ mit $s \in \{\mathrm{id}, (1,2)\}$ und $g \in \mathrm{A}_n$. Dann ist

$$ {}^f x \ = \ {}^{s\circ g\circ t}y \ = \ {}^{s\circ t\circ {t}^{-1}g}y \in {}^{s\circ t}N \ . $$

Also sind $N \cap {}^{(1,2)}N \trianglelefteq \mathrm{S}_n$ und $N \circ {}^{(1,2)}N \trianglelefteq \mathrm{S}_n$.

Wir haben auszuschließen, daß $N \cap {}^{(1,2)}N = 1$ und $N \circ {}^{(1,2)}N = \mathrm{A}_n$ ist. *Annahme,* dem wäre so. Dann ist

$$ n!/2 \ = \ |\mathrm{A}_n| \ = \ |N| \cdot |\,{}^{(1,2)}N| \ = \ |N|^2 \ . $$

Dies ist für $n = 5$ und $n = 6$ nicht möglich, da 60 und 360 keine Quadratzahlen sind. Falls nun $n \geqslant 7$ ist, argumentieren wir wie folgt.

Es ist $|\mathrm{C}_{\mathrm{A}_n}((1,2))| \geqslant (n-2)!/2$. Es folgt aus $N \cap {}^{(1,2)}N = 1$, daß $N \cap \mathrm{C}_{\mathrm{A}_n}((1,2)) = 1$ ist, da für $x \in N$ mit $x \in \mathrm{C}_{\mathrm{A}_n}((1,2))$ auch $x = {}^{(1,2)}x \in {}^{(1,2)}N$ liegt. Somit wird

$$ n!/2 \ = \ |\mathrm{A}_n| \ \geqslant \ |N \circ \mathrm{C}_{\mathrm{A}_n}((1,2))| \ = \ |N| \cdot |\mathrm{C}_{\mathrm{A}_n}((1,2))| \ \geqslant \ |N| \cdot (n-2)!/2 \ . $$

Es folgt

$$ (n!/2)^2 \ \geqslant \ |N|^2 \cdot ((n-2)!/2)^2 \ , $$

also

$$ n!/2 \ \geqslant \ ((n-2)!/2)^2 \ , $$

und somit

$$ 2 \cdot n \cdot (n-1) \ \geqslant \ (n-2)! \ . $$

Für $n = 7$ ist dies falsch, da $2{\cdot}7{\cdot}(7{-}1) = 84$ und $(7{-}2)! = 120$ ist. Da $\frac{2\cdot(n+1)\cdot n}{2\cdot n\cdot(n-1)} \leqslant 2 \leqslant \frac{(n-1)!}{(n-2)!}$ für $n \geqslant 7$, bleibt es auch für $n \geqslant 7$ falsch. Wir haben einen *Widerspruch.* Dies zeigt die *Behauptung.*

Wir *behaupten*, daß M einen Zykel der Länge 3 enthält, also ein Element der Form (a, b, c).

Wähle $g \in M \smallsetminus \{\mathrm{id}\}$.

Fall 1*: Es enthält g in Zykeldarstellung wenigstens einen Zykel $(a_1, a_2, a_3, \ldots, a_k)$ mit $k \geqslant 3$.*

Dann ist $g^{-1} \circ {}^{(a_2,a_3)}g = (a_1, a_2, a_3, \ldots, a_k)^{-1} \circ (a_1, a_3, a_2, \ldots, a_k) = (a_1, a_2, a_3) \in M$.

Fall 2*: Es enthält g in Zykeldarstellung wenigstens drei Zykel der Länge* 2*.*

Seien die drei Zykel (a, b), (c, d), (e, f) in der Zykeldarstellung von g enthalten.

Dann ist auch $g^{-1} \circ {}^{(b,c)(d,e)}g = (a, b)(c, d)(e, f) \circ (a, c)(b, e)(d, f) = (a, d, e)(b, f, c) \in M$.

Das Argument aus Fall 1 zeigt nun, daß M einen Zykel der Länge 3 enthält.

Fall 3*: Es enthält g in Zykeldarstellung zwei Zykel der Länge* 2 *und keine weiteren Zykel.*

Wir schreiben $g = (a, b)(c, d)$. Wir wählen $e \in [1, n] \setminus \{a, b, c, d\}$, möglich, da $n \geqslant 5$.

Dann ist auch $g^{-1} \circ {}^{(b,e)}g = (a, b)(c, d) \circ (a, e)(c, d) = (a, e, b) \in M$.

In allen drei Fällen ist die *Behauptung* gezeigt.

Da $M \trianglelefteqslant \mathrm{S}_n$, ist nun jeder Zykel der Länge 3 in M enthalten.

Da jeder Zykel $(a_1, \ldots, a_k)$ in S_n einer Länge $k \geqslant 2$ als Produkt von Zyklen der Länge zwei darstellbar ist, namentlich als $(a_1, \ldots, a_k) = (a_1, a_2) \circ (a_2, a_3) \circ \ldots \circ (a_{k-1}, a_k)$, ist auch jedes Element von S_n als Produkt von Zyklen der Länge zwei darstellbar.

Folglich ist jedes Element von A_n als Produkt einer geraden Zahl von Zyklen der Länge 2 darstellbar.

Nun können wir aber zwei aufeinanderfolgende Zykel in einem solchen Produkt zusammenfassen in der Form $(a, b) \circ (b, c) = (a, b, c)$, wobei $|\{a, b, c\}| = 3$, oder in der Form $(a, b) \circ (c, d) = (a, b, c) \circ (b, c, d)$, wobei $|\{a, b, c, d\}| = 4$.

Also ist jedes Element von A_n als Produkt von Zyklen der Länge 3 darstellbar. Da M eine Untergruppe von A_n ist und alle Zykel der Länge 3 enthält, folgt $M = \mathrm{A}_n$. Wir haben einen Widerspruch. □

Die Klassifikation der endlichen einfachen Gruppen ist ein umfangreiches Projekt. Satz 180 ist ein erster Schritt.

Beispiel 181 Es gibt keine einfache Gruppe von Ordnung 20.

Annahme, es gibt eine einfache Gruppe G mit $|G| = 20$. Dann ist $|\operatorname{Syl}_5(G)| \equiv_5 1$ und $|\operatorname{Syl}_5(G)|$ ein Teiler von 4. Also ist $|\operatorname{Syl}_5(G)| = 1$. Folglich hat G einen Normalteiler von Ordnung 5. *Widerspruch.*

Beispiel 182 Es gibt keine einfache Gruppe von Ordnung 36.

Annahme, es gibt eine einfache Gruppe G mit $|G| = 36$. Dann ist $|\operatorname{Syl}_3(G)| \equiv_3 1$ und $|\operatorname{Syl}_3(G)|$ ein Teiler von 4. Also ist $|\operatorname{Syl}_3(G)| \in \{1, 4\}$. Da G keinen Normalteiler von Ordnung 9 hat, folgt $|\operatorname{Syl}_3(G)| = 4$.

Schreibe $X := \operatorname{Syl}_3(G)$. Es ist X eine transitive, also nichttriviale G-Menge. Folglich gibt es einen Gruppenmorphismus $\varphi : G \to \mathrm{S}_X$ mit $\operatorname{Kern}(\varphi) \neq G$. Da G einfach ist, folgt

$\mathrm{Kern}(\varphi) = 1$. Also ist φ injektiv. Da aber $|G| = 36$ größer ist als $|\mathrm{S}_X| = |\mathrm{S}_4| = 24$, haben wir einen *Widerspruch.*

Beispiel 183 Es gibt keine einfache Gruppe von Ordnung 56.

Annahme, es gibt eine einfache Gruppe G mit $|G| = 56$. Dann ist $|\operatorname{Syl}_7(G)| \equiv_7 1$ und $|\operatorname{Syl}_7(G)|$ ein Teiler von 8. Also ist $|\operatorname{Syl}_7(G)| \in \{1, 8\}$. Da G keinen Normalteiler von Ordnung 7 hat, folgt $|\operatorname{Syl}_7(G)| = 8$.

Da nun die 7-Sylowgruppen paarweise Schnitt 1 haben, gibt es $8 \cdot (7 - 1) = 48$ Elemente der Ordnung 7 in G. Folglich kann es in G höchstens $56 - 48 = 8$ Elemente geben, deren Ordnung eine Potenz von 2 ist. Somit ist $|\operatorname{Syl}_2(G)| = 1$. Daher hat G einen Normalteiler von Ordnung 8. *Widerspruch.*

Wie Feit und Thompson gezeigt haben, gibt es auch keine nichtzyklische einfache Gruppe von ungerader Ordnung.

Ein weiteres Beispiel zu p-Sylowgruppen einfacher Gruppen findet sich in §A.2.

Kapitel 3

Körpererweiterungen

3.1 Algebraische Elemente und endliche Körpererweiterungen

Wir erinnern an den Begriff eines Körpers; vgl. Definition 1. Informell gesprochen: in einem Körper gelten alle 4 Grundrechenarten.

Definition 184 Sei L ein Körper.

Ein Teilring $K \subseteq L$, der ein Körper ist, heißt *Teilkörper*.

Somit ist $K \subseteq L$ ein Teilkörper genau dann, wenn $1 \in K$, wenn für $x, y \in K$ auch $x - y \in K$ und $x \cdot y \in K$ liegen und wenn für $x \in K^\times$ auch $x^{-1} \in K$ liegt.

Beispiel 185

(1) Es ist $\mathbb{Q}$ ein Teilkörper von $\mathbb{R}$. Es ist $\mathbb{R}$ ein Teilkörper von $\mathbb{C}$.

(2) Es ist $\mathbb{Z}$ ein Teilring von $\mathbb{Q}$, aber kein Teilkörper.

Definition 186

(1) Sei K ein Körper. Sei L ein Körper.

Ist K ein Teilkörper von L, so heißt L eine *Körpererweiterung* von K.

Wir schreiben auch $L|K$ für diese Körpererweiterung.

(2) Sei $L|K$ eine Körpererweiterung. Sei Z ein Teilkörper von L, der K enthält.

Dann haben wir die Körpererweiterungen $L|Z|K$.

Es heißt Z ein *Zwischenkörper* von $L|K$.

Beispiel 187

(1) Wir haben die Körpererweiterungen $\mathbb{C}|\mathbb{R}|\mathbb{Q}$. Es ist $\mathbb{R}$ ein Zwischenkörper von $\mathbb{C}|\mathbb{Q}$.

(2) Sei $\mathbb{Q}(\mathrm{i}) := \{\, a+b\mathrm{i} \,:\, a,\, b \,\in\, \mathbb{Q} \,\} \subseteq \mathbb{C}$.

Man beachte: Ist $a+b\mathrm{i} \neq 0$, dann ist $(a+b\mathrm{i})^{-1} = \frac{a-b\mathrm{i}}{a^2+b^2} \in \mathbb{Q}(\mathrm{i})$. Also ist der Teilring $\mathbb{Q}(\mathrm{i}) \subseteq \mathbb{C}$ ein Teilkörper.

Wir haben die Körpererweiterungen $\mathbb{C}|\mathbb{Q}(\mathrm{i})$ und $\mathbb{Q}(\mathrm{i})|\mathbb{Q}$. Kurz, wir haben die Körpererweiterungen $\mathbb{C}|\mathbb{Q}(\mathrm{i})|\mathbb{Q}$.

Es ist $\mathbb{Q}(\mathrm{i})$ ein Zwischenkörper von $\mathbb{C}|\mathbb{Q}$.

Auf die Bezeichnung als $\mathbb{Q}(\mathrm{i})$ gehen wir in Beispiel 197.(1) unten nochmals ein, nachdem wir sie in größerer Allgemeinheit eingeführt haben werden.

(3) Sei K ein Körper. Wir verwenden T als Variablenbezeichnung.

Wir erinnern an $K(T) = \mathrm{Quot}(K[T]) = \{\, \frac{f(T)}{g(T)} \,:\, f(T) \in K[T],\ g(T) \in K[T]^\times \,\}$; vgl. Beispiel 38.(2).

Es ist $K(T)|K$ eine Körpererweiterung.

Sei $K(T^2) := \{\, \frac{f(T^2)}{g(T^2)} \,:\, f(T) \in K[T],\ g(T) \in K[T]^\times \,\}$.

Es ist $K(T)|K(T^2)|K$. Es ist also $K(T^2)$ ein Zwischenkörper von $K(T)|K$.

Auf die Bezeichnung als $K(T^2)$ gehen wir in Beispiel 197.(2) unten nochmals ein, nachdem wir sie in größerer Allgemeinheit eingeführt haben werden.

(4) Sei p eine Primzahl. Sei L ein Körper von Charakteristik $\mathrm{char}(L) = p$. Dann ist $\mathbb{F}_p \subseteq L$ ein Teilkörper, d.h. $L|\mathbb{F}_p$ eine Körpererweiterung. Vgl. Beispiel 32.

(5) Sei L ein Körper von Charakteristik $\mathrm{char}(L) = 0$. Dann ist $\mathbb{Q} \subseteq L$ ein Teilkörper, d.h. $L|\mathbb{Q}$ eine Körpererweiterung. Vgl. Beispiel 38.(3).

Bemerkung 188 Sei $L|K$ eine Körpererweiterung.

Dann ist L ein K-Vektorraum, wobei die skalare Multiplikation von K auf L durch die Multiplikation innerhalb L gegeben ist.

Wir schreiben auch $[L : K] := \dim_K(L) \in \mathbb{Z}_{\geqslant 1} \cup \{\infty\}$, genannt *Grad* von $L|K$.

Beispiel 189 Es ist $\mathbb{C}|\mathbb{R}$ eine Körpererweiterung.

Also ist $\mathbb{C}$ ein $\mathbb{R}$-Vektorraum, wobei die skalare Multiplikation von $\mathbb{R}$ auf $\mathbb{C}$ durch die Multiplikation innerhalb $\mathbb{C}$ gegeben ist.

Es ist $\mathbb{C}$ ein zweidimensionaler $\mathbb{R}$-Vektorraum. Als $\mathbb{R}$-lineare Basis von $\mathbb{C}$ haben wir z.B. $(1, \mathrm{i})$. Also hat die Körpererweiterung $\mathbb{C}|\mathbb{R}$ den Grad $[\mathbb{C} : \mathbb{R}] = 2$.

Definition 190 Sei $L|K$ eine Körpererweiterung. Sei $b \in L$.

(1) Sei $K[b] := \{ f(b) : f(X) \in K[X] \} \subseteq L$.

(2) Sei $K(b) := \{ \frac{f(b)}{g(b)} : f(X), g(X) \in K[X], g(b) \neq 0 \} \subseteq L$.

Bemerkung 191 *Sei $L|K$ eine Körpererweiterung. Sei $b \in L$.*

(1) *Es ist $K[b]$ ein Teilring von L, der K und b enthält.*
Jeder Teilring von L, der K und b enthält, enthält auch $K[b]$.

(2) *Es ist $K(b)$ ein Teilkörper von L, der K und b enthält.*
Jeder Teilkörper von L, der K und b enthält, enthält auch $K(b)$.

Beweis. Zu (1). Es liegt $1 \in K[b]$. Die Differenz und das Produkt zweier Elemente in $K[b]$ liegen wieder in $K[b]$. Also ist $K[b]$ ein Teilring von L. Er enthält K und b.

Sei nun $R \subseteq L$ ein Teilring mit $K \subseteq R$ und $b \in R$. Da R ein Teilring von L ist, liegt auch jedes Element der Form $a_k b^k + a_{k-1} b^{k-1} + \ldots + a_0 b^0$ in R, wobei $k \in \mathbb{Z}_{\geqslant 0}$ und $a_j \in K$ für $j \in [0, k]$. Mit anderen Worten, es ist $K[b] \subseteq R$.

Zu (2). Es liegt $1 \in K(b)$. Die Differenz und das Produkt zweier Elemente in $K(b)$ liegen wieder in $K(b)$. Also ist $K(b)$ ein Teilring von L.

Ist nun $\frac{f(b)}{g(b)} \in K(b)^\times$, dann ist $f(b) \neq 0$ und also auch $\frac{g(b)}{f(b)} \in K(b)$. Folglich ist $K(b)$ ein Teilkörper von L.

Sei nun $Z \subseteq L$ ein Teilkörper von L mit $K \subseteq Z$ und $b \in Z$. Dann ist $Z \subseteq L$ auch ein Teilring. Gemäß (1) ist also $K[b] \subseteq Z$.

Wir haben $K(b) \overset{!}{\subseteq} Z$ zu zeigen.

Seien $f(X), g(X) \in K[X]$ mit $g(b) \neq 0$ gegeben. Dann sind $f(b), g(b) \in K[b] \subseteq Z$. Da nun Z auch ein Teilkörper von L ist, ist auch $g(b)^{-1} \in Z$. Somit ist auch $\frac{f(b)}{g(b)} \in Z$. ▫

Definition 192 Sei $L|K$ eine Körpererweiterung. Sei $b \in L$.

Es heißt b *algebraisch* über K, falls es ein Polynom $f(X) \in K[X]^\times$ gibt mit $f(b) = 0$.

Diesenfalls gibt es auch ein normiertes Polynom in $K[X]$ mit Nullstelle b.

Bemerkung 193 *Sei $L|K$ eine Körpererweiterung. Sei $b \in L$.*

(1) *Sei $f(X) \in K[X]^\times$ gegeben mit $f(b) = 0$. Sei $n := \deg(f(X))$. Dann ist*

$$K[b] = {}_K\langle b^0, \ldots, b^{n-1} \rangle .$$

(2) *Es ist genau dann b algebraisch über K, wenn $K[b]$ ein endlichdimensionaler K-Vektorraum ist.*

(3) *Ist b algebraisch über K, dann ist $K[b] = K(b)$.*

Beweis. Zu (1). Zu zeigen ist nur $\overset{!}{\subseteq}$. Sei $g(X) \in K[X]$ gegeben. Wir haben zu zeigen, daß $g(b) \overset{!}{\in} {}_K\langle b^{n-1}, \ldots, b^0\rangle$ ist. Division mit Rest gibt $g(X) = f(X) \cdot q(X) + r(X)$, mit $q(X)$, $r(X) \in K[X]$ und mit $r(X) \in {}_K\langle X^{n-1}, \ldots, X^0\rangle$. Es folgt $g(b) = f(b) \cdot q(b) + r(b) = r(b) \in {}_K\langle b^{n-1}, \ldots, b^0\rangle$.

Zu (2). Sei b algebraisch über K. Sei also $f(b) = 0$ für ein Polynom $f(X) \in K[X]^\times$. Sei $n := \deg(f(X))$. Dank (1) ist $K[b] = {}_K\langle b^{n-1}, \ldots, b^0\rangle$. Insbesondere ist $K[b]$ ein endlichdimensionaler K-Vektorraum.

Sei umgekehrt $K[b]$ ein endlichdimensionaler K-Vektorraum. Sei n maximal derart, daß $(b^{n-1}, \ldots, b^0)$ ein K-linear unabhängiges Tupel in L ist. Dann ist $(b^n, b^{n-1}, \ldots, b^0)$ ein K-linear abhängiges Tupel. Beides zusammen liefert $b^n \in {}_K\langle b^{n-1}, \ldots, b^0\rangle$. Folglich ist $b^n + a_{n-1}b^{n-1} + \ldots + a_0 b^0 = 0$ für gewisse $a_0, \ldots, a_{n-1} \in K$. Mit dem normierten Polynom $f(X) := X^n + a_{n-1}X^{n-1} + \ldots + a_0 X^0$ ist also $f(b) = 0$.

Zu (3). Wir haben $K[b] \overset{!}{\supseteq} K(b)$ zu zeigen; vgl. Bemerkung 191.(1). Es genügt zu zeigen, daß $K[b]$ ein Körper ist; vgl. Bemerkung 191.(2).

Sei $x \in K[b]^\times$. Wir betrachten die K-lineare Abbildung $\varphi : K[b] \to K[b] : y \mapsto xy$. Da $K[b]$ als Teilring des Körpers L ein Integritätsbereich ist, ist $\mathrm{Kern}(\varphi) = 0$, also φ injektiv. Da b algebraisch ist über K, ist $K[b]$ ein endlichdimensionaler K-Vektorraum nach (2). Daher folgt aus φ injektiv bereits φ bijektiv. Es gibt also ein $z \in K[b]$ mit $1 = \varphi(z) = xz$. Folglich ist $K[b]$ ein Körper. ▫

Lemma 194 *Sei $L|K$ eine Körpererweiterung. Sei $b \in L$ algebraisch über K.*

Es gibt ein eindeutig bestimmtes normiertes Polynom $\mu_{b,K}(X) \in K[X]$ mit $\mu_{b,K}(b) = 0$, welches jedes Polynom $f(X) \in K[X]$ mit $f(b) = 0$ teilt.

Dieses Polynom $\mu_{b,K}(X)$ heißt Minimalpolynom *von b über K. Es ist irreduzibel in $K[X]$.*

Schreibe $n := \deg(\mu_{b,K}(X))$.

Dann ist $(b^0, \ldots, b^{n-1})$ eine K-lineare Basis von $K(b) = K[b]$.

Insbesondere ist $[K(b) : K] = \deg(\mu_{b,K}(X))$.

Beweis. Wir haben den Ringmorphismus $\varphi : K[X] \to L : f(X) \mapsto f(b)$. Es ist $\mathrm{Kern}(\varphi)$ als Ideal in $K[X]$ ein Hauptideal; vgl. Beispiel 52.(2). Da b algebraisch ist über K, ist $\mathrm{Kern}(\varphi) \neq 0$. Folglich gibt es einen eindeutigen normierten Erzeuger $\mu_{b,K}(X)$ dieses Ideals, d.h. $\mathrm{Kern}(\varphi) = (\mu_{b,K}(X))$. Dieser Erzeuger ist genau dadurch charakterisiert, daß er im Kern von φ liegt und jedes $f(X)$ mit $0 = \varphi(f(X)) = f(b)$ teilt.

Es ist $\varphi(K[X]) = K[b]$.

Wir haben den Ringisomorphismus

$$\begin{array}{rccccc} \bar{\varphi} & : & K[X]/(\mu_{b,K}(X)) & \xrightarrow{\sim} & K[b] & = & K(b) \\ & & f(X) + (\mu_{b,K}(X)) & \mapsto & f(b)\,; & & \end{array}$$

vgl. Satz 31.

Somit ist $(\mu_{b,K}(X)) \lhd K[X]$ maximal; vgl. Lemma 23. Somit ist $\mu_{b,K}(X) \in K[X]$ irreduzibel, denn ein echter Teiler von $\mu_{b,K}(X)$, weder assoziiert zu 1 noch zu $\mu_{b,K}(X)$, würde ein Ideal erzeugen, das echt zwischen $(\mu_{b,K}(X))$ und $K[X]$ liegt.

Es ist $\mu_{b,K}(X) \in K[X]^\times$ mit $\mu_{b,K}(b) = 0$. Es ist also $K[b] = {}_K\langle b^{n-1}, \ldots, b^0\rangle$ dank Bemerkung 193.(1).

Um zu wissen, daß $(b^{n-1}, \ldots, b^0)$ eine K-lineare Basis von $K[b]$ ist, müssen wir noch die K-lineare Unabhängigkeit dieses Tupels zeigen.

Sei $a_{n-1}b^{n-1} + \ldots + a_0 b^0 = 0$, wobei $a_j \in K$ für $j \in [0, n-1]$. *Annahme,* es gibt ein $k \in [0, n-1]$ mit $a_k \neq 0$. Wähle k damit maximal. Dann ist $a_k b^k + a_{k-1}b^{k-1} + \ldots + a_0 b^0 = 0$. Setzen wir

$$f(X) \ := \ a_k X^k + a_{k-1}X^{k-1} + \ldots + a_0 X^0 \ ,$$

dann ist $f(X) \in K[X]^\times$ mit $f(b) = 0$. Aber es ist $\deg(f(X)) = k < n = \deg(\mu_{b,K}(X))$, und somit kann $\mu_{b,K}(X)$ kein Teiler von $f(X)$ sein. Wir haben einen *Widerspruch.* ▫

Diese Beobachtung läßt sich umkehren:

Lemma 195 *Sei K ein Körper. Sei $m(X) \in K[X]$ ein normiertes irreduzibles Polynom.*

Sei $L := K[X]/(m(X))$. Sei $b := X + (m(X))$.

Dann ist $L|K$ eine Körpererweiterung. Es ist $L = K[b] = K(b)$.

Es ist b algebraisch über K mit Minimalpolynom $\mu_{b,K}(X) = m(X)$.

Beweis. Da $m(X) \in K[X]$ irreduzibel ist, ist $(m(X)) \lhd K[X]$ ein maximales Ideal. Denn ist $J \lhd K[X]$ mit $(m(X)) \subseteq J$ gegeben, dann können wir $J = (f(X))$ schreiben für ein normiertes Polynom $f(X) \in K[X]$. Und $(m(X)) \subseteq (f(X))$ heißt, es ist $f(X)$ ein Teiler von $m(X)$. Da $m(X)$ irreduzibel ist, folgt $f(X) = 1$ oder $f(X) = m(X)$. Ersteres kann wegen $J \lhd K[X]$ nicht sein. Also ist $(m(X)) = (f(X)) = J$.

Also ist $K[X]/(m(X))$ ein Körper, der als Teilkörper K enthält; cf. Lemma 23.

Es ist $m(b) = m(X) + (m(X)) = 0$. Und für jedes Polynom $f(X) \in K[X]$ mit $0 = f(b) = f(X + (m(X))) = f(X) + (m(X))$ ist $f(X) \in (m(X))$, also $m(X)$ ein Teiler von $f(X)$. ▫

Bemerkung 196 *Sei $L|K$ eine Körpererweiterung. Sei $b \in L$ algebraisch über K.*

Sei $f(X) \in K[X]$ ein normiertes Polynom.

Die folgenden Aussagen $(1, 2, 3)$ sind äquivalent.

(1) *Es ist $f(X) = \mu_{b,K}(X)$.*

(2) *Es ist $f(X)$ irreduzibel in $K[X]$ und es ist $f(b) = 0$.*

(3) *Es ist $f(X)$ in $K[X]^\times$ von minimalem Grad mit der Eigenschaft $f(b) = 0$.*

Beweis. Zu (1) $\Rightarrow$ (2). Dies folgt aus Lemma 194.

Zu (2) $\Rightarrow$ (1). Es ist $\mu_{b,K}(X)$ ein Teiler von $f(X)$; vgl. Lemma 194. Es ist $\deg(\mu_{b,K}(X)) \geqslant 1$. Wegen $f(X)$ irreduzibel folgt $\mu_{b,K}(X) = f(X)$.

Zu (1) $\Rightarrow$ (3). Da $\mu_{b,K}(X)$ jedes Polynom $g(X) \in K[X]^\times$ teilt, welches $g(b) = 0$ erfüllt, ist auch $\deg(\mu_{b,K}(X)) \leqslant \deg(g(X))$.

Zu (3) $\Rightarrow$ (1). Es ist $\mu_{b,K}(X)$ ein Teiler von $f(X)$. Es ist $\mu_{b,K}(b) = 0$. Wegen der vorausgesetzten Minimalität des Grades von $f(X)$ folgt $\mu_{b,K}(X) = f(X)$. ▫

Beispiel 197

(1) Es ist $\mathbb{C} = \mathbb{R}[\mathrm{i}] = \mathbb{R}(\mathrm{i})$. Es ist i algebraisch über $\mathbb{R}$, da $\mathrm{i}^2 + 1 = 0$ ist. Es ist $\mu_{\mathrm{i},\mathbb{R}}(X) = X^2 + 1 \in \mathbb{R}[X]$, da dieses Polynom Nullstelle i hat und kein normiertes Polynom kleineren Grades i als Nullstelle hat.

(2) In Beispiel 187.(1) wurde ad hoc $\mathbb{Q}(\mathrm{i})$ als $\{\, a + b\mathrm{i} \,:\, a,\, b \in \mathbb{Q} \,\}$ definiert.

Es ist i algebraisch über $\mathbb{Q}$, da $\mathrm{i}^2 + 1 = 0$ ist, d.h. da i eine Nullstelle von $X^2 + 1 \in \mathbb{Q}[X]$ ist.

Da $\mathrm{i} \notin \mathbb{Q}$ liegt, gibt es kein Polynom $\neq 0$ von Grad kleiner als $2 = \deg(X^2 + 1)$, das i als Nullstelle hat. Gemäß Bemerkung 196 ist also

$$\mu_{\mathrm{i},\mathbb{Q}}(X) \;=\; X^2 + 1 \;\in\; \mathbb{Q}[X]\,.$$

Also ist $(1, \mathrm{i})$ eine $\mathbb{Q}$-lineare Basis von $\mathbb{Q}(\mathrm{i})$.

Somit ist in der Tat $\mathbb{Q}(\mathrm{i}) = \{\, a + b\mathrm{i} \,:\, a,\, b \in \mathbb{Q} \,\}$.

Ferner ist $[\mathbb{Q}(\mathrm{i}) : \mathbb{Q}] = \dim_{\mathbb{Q}}(\mathbb{Q}(\mathrm{i})) = 2$.

(3) Es ist $K(T^2) = \{\, \frac{f(T^2)}{g(T^2)} \,:\, f(X) \in K[X],\ g(X) \in K[X]^\times \,\}$ nach Definition 190.(2), wenn man noch beachtet, daß für $g(X) \in K[X]$ genau dann $g(T^2) = 0$ ist, wenn $g(X) = 0$ ist.

Hier ist $K(T^2) \neq K[T^2]$, da z.B. $\frac{1}{T^2}$ zwar in $K(T^2)$ liegt, nicht aber in $K[T^2]$.

Es ist T^2 nicht algebraisch über K.

Ferner ist $T \notin K(T^2)$. *Annahme,* doch. Dann ist $T = \frac{f(T^2)}{g(T^2)}$ mit $f(X) \in K[X]^\times$ und $g(X) \in K[X]^\times$. Also ist $T \cdot g(T^2) = f(T^2)$. Aber $\deg(T \cdot g(T)) \equiv_2 1$, wohingegen $\deg(f(T^2)) \equiv_2 0$. *Widerspruch.*

Sei $u(X) := X^2 - T^2 \in K(T^2)[X]$. Es ist $u(T) = T^2 - T^2 = 0$, und $u(X)$ hat minimalen Grad mit dieser Eigenschaft. Also ist $\mu_{T,K(T^2)}(X) = u(X) = X^2 - T^2$; vgl. Bemerkung 196.

Also ist $(1, T)$ eine $K(T^2)$-lineare Basis von $K(T)$.

Insbesondere ist $[K(T) : K(T^2)] = \dim_{K(T^2)}(K(T)) = 2$.

(4) Wir können mit den Lemmas 195 und 194 ausgehend von einem irreduziblen Polynom eine Körpererweiterung bauen.

Wir gehen von $K := \mathbb{Q}$ aus.

Es ist z.B. $m(X) := X^5 + 2X + 2 \in \mathbb{Q}[X]$ irreduzibel, wie wir unten noch einsehen werden und für den Moment zur Kenntnis nehmen; vgl. Lemma 212 unten.

Dank Lemma 195 gibt es einen Körper $L := \mathbb{Q}(b)$ mit

$$\mu_{b,\mathbb{Q}}(X) \;=\; m(X) \;=\; X^5 + 2X + 2\;.$$

Insbesondere ist $b^5 + 2b + 2 = \mu_{b,\mathbb{Q}}(b) = 0$, d.h. $b^5 = -2b - 2$.

Dank Lemma 194 hat L die $\mathbb{Q}$-lineare Basis $(b^0, b^1, b^2, b^3, b^4)$, und also ist $[L : \mathbb{Q}] = 5$.

Das genügt als Information auch, um in L rechnen zu können. So z.B. ist

$$b^4{\cdot}(1{+}7b{-}3b^2) \;=\; b^4{+}7b^5{-}3b^6 \;=\; b^4{+}7(-2b{-}2){-}3b(-2b{-}2) \;=\; -14{-}8b{+}6b^2{+}b^4\;.$$

(5) Ausgehend von einem irreduziblen Polynom können auch endliche Körper konstruiert werden.

Sei etwa $K = \mathbb{F}_2$.

Es ist z.B. $m(X) := X^2{+}X{+}1 \in \mathbb{F}_2[X]$ irreduzibel, denn eine Zerlegung in Faktoren von Grad 1 hätte eine Nullstelle in $\mathbb{F}_2$ zur Folge, die dieses Polynom aber nicht hat.

Dank Lemma 195 gibt es einen Körper $L := \mathbb{F}_2(\alpha)$ mit $\mu_{\alpha,\mathbb{F}_2}(X) = m(X) = X^2 + X + 1$. Insbesondere ist $\alpha^2 = -\alpha - 1 = \alpha + 1$.

Dank Lemma 194 hat L die $\mathbb{F}_2$-lineare Basis (α^0, α^1). Insbesondere ist $[L : \mathbb{F}_2] = 2$ und $|L| = 2^2 = 4$. Daher nennen wir auch

$$\mathbb{F}_4 \;:=\; L \;=\; \mathbb{F}_2(\alpha)\;.$$

Es ist also

$$\mathbb{F}_4 \;=\; \{0, 1, \alpha, 1+\alpha\}\;.$$

Wir erhalten folgende Additions- und Multiplikationstafel.

$(+)$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$(\cdot)$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Vorsicht, es ist $\mathbb{F}_4$ nicht dasselbe wie $\mathbb{Z}/(4)$. Ersteres ist ein Körper, zweiteres ist kein Körper.

Wir werden die Konstruktion endlicher Körper unten noch systematischer angehen; vgl. §3.9 unten.

3.2 Körpermorphismen

Definition 198

(1) Seien L und M Körper.

Ein Ringmorphismus $\varphi : L \to M$ heißt auch *Körpermorphismus*.

Wegen $\varphi(1_L) = 1_M \neq 0_M$ ist $\varphi(L) \neq 0$. Wegen L Körper ist $\mathrm{Kern}(\varphi) \in \{0, L\}$. Also ist $\mathrm{Kern}(\varphi) = 0$.

Jeder Körpermorphismus ist mithin injektiv.

Ist φ bijektiv, so heißt $\varphi : L \to M$ ein *Körperisomorphismus*, auch $\varphi : L \xrightarrow{\sim} M$ geschrieben.

Ist $L = M$, so heißt $\varphi : L \to L$ ein *Körperendomorphismus*.

Ist φ bijektiv und $L = M$, so heißt $\varphi : L \xrightarrow{\sim} L$ ein *Körperautomorphismus*.

(2) Sei K ein Körper. Seien $L|K$ und $M|K$ Körpererweiterungen.

Ein Körpermorphismus $\varphi : L \to M$ mit $\varphi(a) = a$ für $a \in K$ heißt *Körpermorphismus über K*.

Ein Körpermorphismus über K ist auch eine K-lineare Abbildung.

Bemerkung 199 Sei $L|K$ eine Körpererweiterung.

Sei $b \in L$ algebraisch über K.

Wir haben den Körperisomorphismus über K

$$\begin{array}{rccccc} \bar{\varphi} & : & K[X]/(\mu_{b,K}(X)) & \xrightarrow{\sim} & K[b] & = & K(b) \\ & & f(X) + (\mu_{b,K}(X)) & \mapsto & f(b)\,; & & \end{array}$$

vgl. Satz 31.

Beispiel 200 Sei $p \geqslant 2$ eine Primzahl.

Sei L ein Körper von Charakteristik $\mathrm{char}(L) = p$.

Dann haben wir die Körpererweiterung $L|\mathbb{F}_p$.

Es ist

$$\begin{array}{rcccccc} \mathrm{Fr} & = & \mathrm{Fr}_L & : & L & \to & L \\ & & & & x & \mapsto & x^p \end{array}$$

ein Körpermorphismus über $\mathbb{F}_p$, genannt *Frobenius-Endomorphismus* oder kurz *Frobenius*.

Denn es ist $\mathrm{Fr}(1) = 1^p = 1$, $\mathrm{Fr}(x \cdot y) = (x \cdot y)^p = x^p \cdot y^p = \mathrm{Fr}(x) \cdot \mathrm{Fr}(y)$ und

$$\mathrm{Fr}(x+y) \;=\; (x+y)^p \;=\; \sum_{k \in [0,p]} \tbinom{p}{k}\, x^k y^{p-k} \;\overset{\mathrm{char}(L)\,=\,p}{=}\; x^p + y^p \;=\; \mathrm{Fr}(x) + \mathrm{Fr}(y)$$

für $x,\, y \in L$.

Ferner ist $\mathrm{Fr}(a) = a$ für $a \in \mathbb{F}_p$, da $\mathrm{Fr}(1) = 1$ nach sich zieht, daß $\mathrm{Fr}(\sum_{j\in[1,k]} 1) = \sum_{j\in[1,k]} 1$ ist für $k \in [0, p-1]$.

Zum Beispiel ist $\mathrm{Fr}_{\mathbb{F}_2(T)} : \mathbb{F}_2(T) \to \mathbb{F}_2(T)$ nicht surjektiv, da T nicht im Bild liegt.

Ist aber L endlich, dann ist Fr_L ein Körperautomorphismus, auch *Frobenius-Automorphismus* genannt.

Zum Beispiel ist $\mathrm{Fr}_{\mathbb{F}_4}(a_0 + a_1\alpha) = a_0 + a_1\alpha^2 = (a_0 + a_1) + a_1\alpha$, wobei $a_0\,,\, a_1 \in \mathbb{F}_2$; vgl. Beispiel 197.(5)

Lemma 201 *Sei K ein Körper.*

Sei $L|K$ eine Körpererweiterung. Sei $b \in L$ algebraisch über K.

Sei $M|K$ eine Körpererweiterung. Sei $c \in M$ gegeben mit $\mu_{b,K}(c) = 0$.

Dann gibt es den Körpermorphismus $\gamma : K(b) \to M : f(b) \mapsto f(c)$ über K, wobei $f(X) \in K[X]$.

Sein Bild ist $\gamma(K(b)) = K(c)$. Insbesondere ist $\gamma|^{K(c)} : K(b) \xrightarrow{\sim} K(c) : f(b) \mapsto f(c)$ ein Körperisomorphismus über K.

Beweis. Wir schreiben $I := (\mu_{b,K}(X)) \subseteq K[X]$. Wir haben den Körperisomorphismus über K

$$\bar{\varphi} \;:\; K[X]/I \xrightarrow{\sim} K(b) \;:\; f(X) + I \mapsto f(b)\,;$$

vgl. Bemerkung 199.

Wir haben den Ringmorphismus $\psi : K[X] \to M : f(X) \to f(c)$. Es ist $\mu_{b,K}(c) = 0$. Also ist $\psi(I) = 0$. Daher gibt es den Ringmorphismus

$$\bar{\psi} \;:\; K[X]/I \to M \;:\; f(X) + I \;\to\; f(c)\,;$$

vgl. Lemma 30. Letzterer ist ein Körpermorphismus, da $K[X]/I$ und M Körper sind. Es ist zudem ein Köpermorphismus über K.

Wir können zusammensetzen zum Körpermorphismus über K

$$\begin{array}{rcccc} \gamma \;:=\; \bar{\psi} \circ \bar{\varphi}^{-1} \;:\; & K(b) & \to & M \\ & f(b) & \mapsto & f(c)\,, \end{array}$$

wobei $f(X) \in K[X]$. ▫

Beispiel 202

(1) Wir setzen Beispiel 197.(2) fort.

Wir hatten $\mathbb{Q}(\mathrm{i}) \subseteq \mathbb{C}$ betrachtet, mit $\mu_{\mathrm{i},\mathbb{Q}}(X) = X^2 + 1$.

Nun hat $X^2 + 1$ in $\mathbb{C}$ die beiden Nullstellen i und $-\mathrm{i}$. Auf letztere wollen wir Lemma 201 anwenden.

Sei $K := \mathbb{Q}$. Sei $L := \mathbb{Q}(\mathrm{i})$. Sei $b := \mathrm{i}$. Sei $M := \mathbb{Q}(\mathrm{i})$. Sei $c := -\mathrm{i}$.

Es ist $\mu_{\mathrm{i},\mathbb{Q}}(-\mathrm{i}) = 0$. Also gibt es den Körperisomorphismus über $\mathbb{Q}$

$$\varphi \ : \ \mathbb{Q}(\mathrm{i}) \ \tilde{\to} \ \mathbb{Q}(-\mathrm{i}) = \mathbb{Q}(\mathrm{i}) \ : \ f(\mathrm{i}) \ \mapsto \ f(-\mathrm{i}) \ ,$$

wobei $f(X) \in \mathbb{Q}[X]$. Es ist also $\varphi(a_0 + a_1\mathrm{i}) = a_0 - a_1\mathrm{i}$ für $a_0 \, , \, a_1 \in \mathbb{Q}$.

Da Definitions- und Zielbereich von φ beide gleich $\mathbb{Q}(\mathrm{i})$ sind, wird φ auch als Körperautomorphismus auf $\mathbb{Q}(\mathrm{i})$ bezeichnet.

Diesen Körperautomorphismus kennen wir bereits: das ist die komplexe Konjugation, eingeschränkt auf $\mathbb{Q}(\mathrm{i})$.

(2) Wir setzen Beispiel 197.(4) fort.

Es gibt zwar keine Formel für eine Nullstelle von $m(X) = X^5 + 2X + 2 \in \mathbb{Q}[X]$ in $\mathbb{C}$. Man weiß dennoch die Existenz einer Nullstelle in $\mathbb{C}$. Im vorliegenden Fall liefert der Zwischenwertsatz mit einer Monotoniebetrachtung sogar eine eindeutige reelle Nullstelle $c \in \mathbb{R} \subseteq \mathbb{C}$.

Der Taschenrechner gibt die Näherung $c \approx -0{,}817471019$.

Jedenfalls ist $m(c) = c^5 + 2c + 2 = 0$.

Wir haben mittels Lemma 195 auf abstrakte Weise einen Körper $L := \mathbb{Q}(b)$ konstruiert, für welchen $\mu_{b,\mathbb{Q}}(X) = m(X) = X^5 + 2X + 2$ ist.

Lemma 201 erlaubt es, diesen wie folgt zu konkretisieren.

Sei $K = \mathbb{Q}$. Sei $M := \mathbb{C}$. Wir bilden den Teilkörper $\mathbb{Q}(c) \subseteq \mathbb{C}$.

Es ist $\mu_{b,\mathbb{Q}}(c) = m(c) = 0$. Also gibt es einen Körperisomorphismus über $\mathbb{Q}$

$$\gamma \ : \ \mathbb{Q}(b) \ \tilde{\to} \ \mathbb{Q}(c) \ : \ f(b) \ \mapsto \ f(c)$$

wobei $f(X) \in \mathbb{Q}[X]$. Ob man also nur die Information des Minimalpolynoms benutzt, um $\mathbb{Q}(b)$ abstrakt zu konstruieren, oder ob man die komplexe Zahl c benutzt, um $\mathbb{Q}(c)$ konkret zu konstruieren, läuft im wesentlichen auf dasselbe hinaus: es ist $\mathbb{Q}(b) \simeq \mathbb{Q}(c)$.

Insbesondere muß man sich nicht um eine Formel oder um den exakten Wert von c sorgen. Man kann auch so in $\mathbb{Q}(c)$ uneingeschränkt rechnen.

Und tatsächlich muß in $\mathbb{Q}(b)$ eben beachtet werden, daß $b^5 = -2b-2$ ist, um rechnen zu können. Und in $\mathbb{Q}(c)$ muß beachtet werden, daß $c^5 = -2c - 2$ ist, um rechnen zu können. Das läuft auch aus Sicht praktischer Rechnungen auf dasselbe hinaus.

So z.B. ist $b^{10} = (-2b-2)^2 = 4b^2+8b+4$ in $\mathbb{Q}(b)$, und $c^{10} = (-2c-2)^2 = 4c^2+8c+4$ in $\mathbb{Q}(c)$.

Ist $\tilde{c} \in \mathbb{C}$ eine andere Nullstelle von $m(X) = X^5 + 2X + 2$ in $\mathbb{C}$, dann ist übrigens ganz genauso $\mathbb{Q}(b) \simeq \mathbb{Q}(\tilde{c})$.

(3) Wir setzen Beispiel 197.(5) fort. Wir hatten $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ betrachtet, mit $\mu_{\alpha,\mathbb{F}_2}(X) = X^2 + X + 1$. Es ist also $\alpha^2 = -\alpha - 1 = \alpha + 1$.

Nun ist auch $\alpha + 1$ eine Nullstelle von $X^2 + X + 1$: $(\alpha + 1)^2 + (\alpha + 1) + 1 = (\alpha^2 + 1) + \alpha = 0$.

Auf diese wollen wir Lemma 201 anwenden.

Sei $K := \mathbb{F}_2$. Sei $L := \mathbb{F}_4$. Sei $b := \alpha$. Sei $M := \mathbb{F}_4$. Sei $c := \alpha + 1$.

Es ist $\mu_{\alpha,\mathbb{F}_2}(\alpha + 1) = 0$. Also gibt es den Körperisomorphismus über $\mathbb{F}_2$

$$\varphi \ : \ \mathbb{F}_4 \ \xrightarrow{\sim} \ \mathbb{F}_2(\alpha+1) = \mathbb{F}_2(\alpha) = \mathbb{F}_4 \ : \ f(\alpha) \ \mapsto \ f(\alpha+1) \ ,$$

wobei $f(X) \in \mathbb{F}_2[X]$. Es ist also

$$\varphi(a_0 + a_1\alpha) \ = \ a_0 + a_1(\alpha+1) \ = \ (a_0 + a_1) + a_1\alpha$$

für $a_0 \, , \, a_1 \in \mathbb{F}_2$. Diesen Automorphismus kennen wir bereits: das ist der Frobenius-Automorphismus $\mathrm{Fr}_{\mathbb{F}_4}$; vgl. Beispiel 200.

3.3 Multiplikativität der Grade

Definition 203 Sei $L|K$ eine Körpererweiterung.

Ist ihr Grad $[L : K] = \dim_K(L)$ endlich, so heißt $L|K$ eine *endliche* Körpererweiterung.

Bemerkung 204 *Sei $L|K$ eine Körpererweiterung. Sei $b \in L$.*

(1) *Genau dann ist $K(b)|K$ eine endliche Körpererweiterung, wenn b algebraisch über K ist.*

(2) *Ist $L|K$ endlich, dann ist b algebraisch über K.*

Beweis. Zu (1). Ist zum einen b algebraisch über K, dann ist $K(b) = K[b]$ endlichdimensional über K; vgl. Bemerkung 193.(3, 2).

Ist zum anderen $K(b)|K$ eine endliche Körpererweiterung, dann ist $K(b)$ endlichdimensional über K. Wegen $K[b] \subseteq K(b)$ ist auch $K[b]$ endlichdimensional über K. Also ist b algebraisch über K; cf. Bemerkung 193.(2).

Zu (2). Ist $L|K$ endlich, dann ist L ein endlichdimensionaler K-Vektorraum. Somit ist auch der K-Unterraum $K(b) \subseteq L$ ein ein endlichdimensionaler K-Vektorraum. Dank (1) ist also b algebraisch über K. ▫

Lemma 205 (Multiplikativität der Grade)

Seien $M|L|K$ Körpererweiterungen.

Sei $M|L$ eine endliche Körpererweiterung. Sei $L|K$ eine endliche Körpererweiterung.

Dann ist auch $M|K$ eine endliche Körpererweiterung. Genauer ist

$$[M:K] \;=\; [M:L]\cdot[L:K]\;.$$

Beweis. Wir schreiben $\ell := [L:K]$ und $m := [M:L]$.

Sei $(b_i : i \in [1,\ell]) = (b_1,\ldots,b_\ell)$ eine K-lineare Basis von L.

Sei $(c_j : j \in [1,m]) = (c_1,\ldots,c_m)$ eine L-lineare Basis von M.

Es genügt zu zeigen, daß $(b_i \cdot c_j : i \in [1,\ell],\, j \in [1,m])$ eine K-lineare Basis von M ist.

Wir wollen zeigen, daß ein K-lineares Erzeugendensystem von M vorliegt.

Sei $z \in M$. Schreibe $z = \sum_{j\in[1,m]} y_j c_j$, wobei $y_j \in L$ für $j \in [1,m]$. Schreibe $y_j = \sum_{i\in[1,\ell]} x_{i,j} b_i$, wobei $x_{i,j} \in K$ für $j \in [1,m]$ und $i \in [1,\ell]$. Dann ist

$$z \;=\; \sum_{j\in[1,m]} y_j c_j \;=\; \sum_{j\in[1,m]}\sum_{i\in[1,\ell]} x_{i,j} b_i c_j\;.$$

Wir wollen zeigen, daß ein K-linear unabhängiges Tupel vorliegt.

Seien $x_{i,j} \in K$ für $j \in [1,m]$ und $i \in [1,\ell]$ gegeben mit

$$0 \;=\; \sum_{j\in[1,m]}\sum_{i\in[1,\ell]} x_{i,j} b_i c_j \;=\; \sum_{j\in[1,m]} \left(\sum_{i\in[1,\ell]} x_{i,j} b_i\right) c_j\;.$$

Da $(c_1,\ldots,c_m)$ L-linear unabhängig ist, folgt $\sum_{i\in[1,\ell]} x_{i,j} b_i = 0$ für $j \in [1,m]$. Da $(b_1,\ldots,b_\ell)$ K-linear unabhängig ist, folgt $x_{i,j} = 0$ für $j \in [1,m]$ und $i \in [1,\ell]$. ▫

Beispiel 206

(1) Wir bilden den Teilkörper $\mathbb{Q}(\sqrt{2},\mathrm{i}) := \mathbb{Q}(\sqrt{2})(\mathrm{i}) \subseteq \mathbb{C}$.

Wir wollen den Grad $[\mathbb{Q}(\sqrt{2},\mathrm{i}):\mathbb{Q}]$ bestimmen.

Wir haben die Körpererweiterungen $\mathbb{Q}(\sqrt{2},\mathrm{i})|\mathbb{Q}(\sqrt{2})|\mathbb{Q}$.

Es ist schonmal $\mu_{\sqrt{2},\mathbb{Q}}(X) = X^2-2 \in \mathbb{Q}[X]$, denn dies ist ein normiertes irreduzibles Polynom mit Nullstelle $\sqrt{2}$. Folglich ist $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = \deg(\mu_{\sqrt{2},\mathbb{Q}}(X)) = 2$.

Es bleibt der Grad $[\mathbb{Q}(\sqrt{2},\mathrm{i}) : \mathbb{Q}(\sqrt{2})]$ zu bestimmen. Es ist $\mathrm{i} \notin \mathbb{R}$ und also $\mathrm{i} \notin \mathbb{Q}(\sqrt{2})$. Folglich ist X^2+1 ein normiertes Polynom minimalen Grades in $\mathbb{Q}(\sqrt{2})[X]$, das Nullstelle i hat. Somit ist

$$\mu_{\mathrm{i},\mathbb{Q}(\sqrt{2})}(X) \;=\; X^2+1 \;\in\; \mathbb{Q}(\sqrt{2})[X]\;.$$

Also ist

$$[\mathbb{Q}(\sqrt{2},\mathrm{i}):\mathbb{Q}(\sqrt{2})] \;=\; \deg(\mu_{\mathrm{i},\mathbb{Q}(\sqrt{2})}(X)) \;=\; 2\,.$$

Insgesamt ist folglich

$$[\mathbb{Q}(\sqrt{2},\mathrm{i}):\mathbb{Q}] \;=\; [\mathbb{Q}(\sqrt{2},\mathrm{i}):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] \;=\; 2\cdot 2 \;=\; 4\,.$$

Es ist $(1,\sqrt{2})$ eine $\mathbb{Q}$-lineare Basis von $\mathbb{Q}(\sqrt{2})$.

Es ist $(1,\mathrm{i})$ eine $\mathbb{Q}(\sqrt{2})$-lineare Basis von $\mathbb{Q}(\sqrt{2},\mathrm{i})$.

Gemäß Beweis zu Lemma 205 ist

$$(\,1\cdot 1,\ \sqrt{2}\cdot 1,\ 1\cdot\mathrm{i},\ \sqrt{2}\cdot\mathrm{i}\,) \;=\; (1,\sqrt{2},\mathrm{i},\mathrm{i}\sqrt{2})$$

eine $\mathbb{Q}$-lineare Basis von $\mathbb{Q}(\sqrt{2},\mathrm{i})$.

(2) Es ist $X^4+X+1\in\mathbb{F}_2[X]$ irreduzibel. Denn es hat zum einen keine Nullstelle in $\mathbb{F}_2$. Zum anderen ist es auch nicht durch X^2+X+1 teilbar, wie man mit Polynomdivision sieht, und das ist das einzige irreduzible Polynom von Grad 2 in $\mathbb{F}_2[X]$.

Folglich können wir $\mathbb{F}_{16} := \mathbb{F}_2[X]/(X^4+X+1)$ setzen. Sei $\delta := X+(X^4+X+1)$.

Es ist $\mathbb{F}_{16}=\mathbb{F}_2(\delta)$. Es ist $(1,\delta,\delta^2,\delta^3)$ eine $\mathbb{F}_2$-lineare Basis von $\mathbb{F}_{16}$. Dies bestätigt auch $|\mathbb{F}_{16}|=2^4=16$.

In $\mathbb{F}_{16}$ ist dann $\delta^4=\delta+1$ und, natürlich, $2=0$.

Wir erinnern an $\mu_{\alpha,\mathbb{F}_2}(X)=X^2+X+1$.

Sei $c:=\delta^2+\delta$. Es ist $\mu_{\alpha,\mathbb{F}_2}(c)=c^2+c+1=(\delta^4+\delta^2)+(\delta^2+\delta)+1=0$.

Wir bilden den Teilkörper $Z:=\mathbb{F}_2(c)\subseteq\mathbb{F}_{16}$.

Lemma 201 gibt den Körperisomorphismus

$$\mathbb{F}_4=\mathbb{F}_2(\alpha) \;\tilde{\to}\; \mathbb{F}_2(c)=Z \;:\; a_0+a_1\alpha \;\mapsto\; a_0+a_1c\,,$$

wobei $a_0\,,\ a_1\ \in\ \mathbb{F}_2$.

Wir haben also die Körpererweiterungen $\mathbb{F}_{16}|Z|\mathbb{F}_2$.

Nach Lemma 205 ist $[\mathbb{F}_{16}:\mathbb{F}_2]=4=[\mathbb{F}_{16}:Z]\cdot[Z:\mathbb{F}_2]=[\mathbb{F}_{16}:Z]\cdot 2$.

Es folgt $[\mathbb{F}_{16}:Z]=2$.

Wegen $\mathbb{F}_{16}=\mathbb{F}_2(\delta)$ ist erst recht $\mathbb{F}_{16}=Z(\delta)$.

Ferner ist $\deg(\mu_{\delta,Z}(X))=[Z(\delta):Z]=[\mathbb{F}_{16}:Z]=2$.

Wir wollen $\mu_{\delta,Z}(X)$ bestimmen.

Es ist $X^2+X+c\in Z[X]$ ein Polynom von Grad 2 mit δ als Nullstelle, da $\delta^2+\delta+c=0$ ist. Also ist $\mu_{\delta,Z}(X)$ ein Teiler von X^2+X+c.

Da diese beiden Polynome normiert sind und denselben Grad haben, folgt

$$\mu_{\delta,Z}(X) \;=\; X^2+X+c\,.$$

Stellen wir nochmals nebeneinander: $\mu_{\delta,\mathbb{F}_2(c)}(X) = \mu_{\delta,Z}(X) = X^2 + X + c$, aber $\mu_{\delta,\mathbb{F}_2}(X) = X^4 + X + 1$.

Da nun auch $\mu_{\delta,\mathbb{F}_2}(X) \in Z[X]$ ein Polynom ist, das δ als Nullstelle hat, muß $\mu_{\delta,Z}(X)$ in $Z[X]$ ein Teiler von $\mu_{\delta,\mathbb{F}_2}(X)$ sein. Und in der Tat ist

$$X^4 + X + 1 \;=\; (X^2 + X + c)(X^2 + X + (c+1)),$$

wie man durch Polynomdivision ermittelt und durch Multiplikation der beiden Faktoren überprüft.

3.4 Irreduzibilitätskriterien für Polynome

Bemerkung 207 *Sei K ein Körper.*

Sei $f(X) \in K[X]$ normiert und mit $\deg(f(X)) \in \{2, 3\}$.

Gebe es kein $a \in K$ mit $f(a) = 0$.

Dann ist $f(X)$ irreduzibel.

Beweis. Ansonsten hätte $f(X)$ einen Teiler von Grad 1 und also eine Nullstelle, was aber *nicht* zutrifft. ▫

Bemerkung 208 Sei $p \in \mathbb{Z}_{\geqslant 2}$ eine Primzahl.

Wir kürzen hier die Restklasse $\bar{z} := z + (p) \in \mathbb{F}_p$ ab für $z \in \mathbb{Z}$.

Wir haben also den Restklassenmorphismus $\mathbb{Z} \to \mathbb{F}_p : z \mapsto \bar{z}$.

Wir haben auch den Ringmorphismus

$$\begin{array}{rcl} \mathbb{Z}[X] & \to & \mathbb{F}_p[X] \\ f(X) = \sum_{i\geqslant 0} a_i X^i & \mapsto & \bar{f}(X) := \sum_{i\geqslant 0} \bar{a}_i X^i \end{array}$$

Bemerkung 209 Sei $f(X) \in \mathbb{Z}[X]$ normiert.

(1) Sei $g(X) \in \mathbb{Q}[X]$ ein normierter Teiler von $f(X)$ in $\mathbb{Q}[X]$.
Dann ist $g(X) \in \mathbb{Z}[X]$, und es ist $g(X)$ ein Teiler von $f(X)$ in $\mathbb{Z}[X]$.

(2) Genau dann ist $f(X)$ in $\mathbb{Q}[X]$ irreduzibel, wenn $f(X)$ in $\mathbb{Z}[X]$ irreduzibel ist.

Beweis. Zu (1). Wir finden ein $t \in \mathbb{Z}^\times$ mit $t \cdot g(X) \in \mathbb{Z}[X]$. Wir finden ein $s \in \mathbb{Q}^\times$ mit $\tilde{g}(X) := s \cdot t \cdot g(X) \in \mathbb{Z}[X]$ primitiv; vgl. Bemerkung 72. Da $g(X)$ normiert ist, ist der Leitkoeffizient von $\tilde{g}(X)$ gleich $u := s \cdot t \in \mathbb{Z}$. Mit $g(X)$ ist auch $\tilde{g}(X)$ ein Teiler von $f(X)$ in $\mathbb{Q}[X]$. Dank Bemerkung 74 gibt es ein $\tilde{h}(X) \in \mathbb{Z}[X]$ mit $f(X) = \tilde{g}(X) \cdot \tilde{h}(X) = g(X) \cdot (u \cdot \tilde{h}(X))$, wobei $u \cdot \tilde{h}(X) \in \mathbb{Z}[X]$. Folglich ist $g(X)$ ein Teiler von $f(X)$ in $\mathbb{Z}[X]$.

Zu (2). Sei $f(X)$ in $\mathbb{Z}[X]$ irreduzibel. Wir wollen zeigen, daß $f(X)$ in $\mathbb{Q}[X]$ irreduzibel ist. *Annahme,* nicht. Dann gibt es einen Teiler $g(X) \in \mathbb{Q}[X]$ von $f(X)$ mit $\deg(g(X)) \in [1, \deg(f(X)) - 1]$. Nach Division durch den Leitkoeffizienten dürfen wir annehmen, daß $g(X)$ normiert ist. Gemäß (1) ist dann aber $g(X) \in \mathbb{Z}[X]$, und es ist $g(X)$ ein Teiler von $f(X)$ in $\mathbb{Z}[X]$. Da $f(X)$ in $\mathbb{Z}[X]$ irreduzibel ist, haben wir einen *Widerspruch.*

Sei umgekehrt $f(X)$ in $\mathbb{Q}[X]$ irreduzibel. Wir wollen zeigen, daß $f(X)$ in $\mathbb{Z}[X]$ irreduzibel ist. *Annahme,* nicht. Dann gibt es eine Zerlegung $f(X) = g(X) \cdot h(X)$ mit $g(X)$, $h(X) \in \mathbb{Z}[X]^\times \smallsetminus \mathrm{U}(\mathbb{Z}[X])$ liegt. Da $f(X)$ normiert ist, sind die Leitkoeffizienten von $g(X)$ Einheiten in $\mathbb{Z}$. Da aber $g(X)$, $h(X) \notin \mathrm{U}(\mathbb{Z}[X])$, ist $\deg(g(X)) \geqslant 1$ und $\deg(h(X)) \geqslant 1$. Dann aber ist $f(X)$ auch in $\mathbb{Q}[X]$ nicht irreduzibel. Wir haben einen *Widerspruch.* ▫

Bemerkung 210 Sei $p \in \mathbb{Z}_{\geqslant 2}$ eine Primzahl.

Sei $f(X) \in \mathbb{Z}[X]$ normiert. Sei $g(X) \in \mathbb{Z}[X]$ normiert.

Sei $g(X)$ ein Teiler von $f(X)$ in $\mathbb{Z}[X]$.

Dann ist auch $\bar{g}(X)$ ein Teiler von $\bar{f}(X)$ in $\mathbb{F}_p[X]$; vgl. Bemerkung 208.

Bemerkung 211 *Sei $p \in \mathbb{Z}_{\geqslant 2}$ eine Primzahl.*

Sei $f(X) \in \mathbb{Z}[X]$ normiert. Sei $\bar{f}(X) \in \mathbb{F}_p[X]$ irreduzibel.

Dann ist $f(X)$ in $\mathbb{Z}[X]$ und also auch in $\mathbb{Q}[X]$ irreduzibel.

Beweis. Wir müssen $f(X)$ als irreduzibel in $\mathbb{Z}[X]$ nachweisen; vgl. Bemerkung 209.(2). *Annahme* nicht. Dann gibt es $g(X)$, $h(X) \in \mathbb{Z}[X]$ mit $g(X) \cdot h(X) = f(X)$ und mit $\deg(g(X))$, $\deg(h(X)) \geqslant 1$.

Betrachtung der Leitkoeffizienten liefert, daß der Leitkoeffizient von $g(X)$ in $\mathrm{U}(\mathbb{Z}) = \{-1, +1\}$ liegt. Somit sind $g(X)$ und $h(X)$ o.E. normiert.

Es folgt $\bar{g}(X) \cdot \bar{h}(X) = \bar{f}(X)$ in $\mathbb{F}_p[X]$, wobei $\deg(\bar{g}(X))$, $\deg(\bar{h}(X)) \geqslant 1$; vgl. Bemerkung 208. Wir haben einen *Widerspruch* zu $\bar{f}(X)$ irreduzibel.

Lemma 212 (Eisenstein) *Sei $p \in \mathbb{Z}_{\geqslant 2}$ eine Primzahl.*

Sei $f(X) \in \mathbb{Z}[X]$ normiert.

Sei $n := \deg(f(X))$. Schreibe $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0X^0$, wobei $a_0, \ldots, a_n \in \mathbb{Z}$.

Sei $a_i \equiv_p 0$ für $i \in [0, n-1]$. Sei $a_0 \not\equiv_{p^2} 0$.

Dann ist $f(X)$ irreduzibel in $\mathbb{Z}[X]$ und also auch in $\mathbb{Q}[X]$.

Beweis. Wir müssen $f(X)$ als irreduzibel in $\mathbb{Z}[X]$ nachweisen; vgl. Bemerkung 209.(2). *Annahme* nicht. Dann gibt es $g(X)$, $h(X) \in \mathbb{Z}[X]$ normiert mit $g(X) \cdot h(X) = f(X)$ und mit $\deg(g(X))$, $\deg(h(X)) \geqslant 1$.

Es folgt $\bar{g}(X) \cdot \bar{h}(X) = \bar{f}(X)$ in $\mathbb{F}_p[X]$, wobei $\deg(\bar{g}(X)), \deg(\bar{h}(X)) \geqslant 1$; vgl. Bemerkung 208. Nach Voraussetzung ist $\bar{f}(X) = X^n$. Also ist $\bar{g}(X) = X^k$ und $\bar{h}(X) = X^{n-k}$ für ein $k \in [1, n-1]$.

Wir können also

$$\begin{array}{rcl} g(X) & = & X^k + b_{k-1}X^{k-1} + \ldots + b_0X^0 \\ h(X) & = & X^{n-k} + c_{n-k-1}X^{n-k-1} + \ldots + c_0X^0 \end{array}$$

schreiben, wobei $b_i \in \mathbb{Z}$ mit $b_i \equiv_p 0$ für $i \in [0, k-1]$ und $c_i \in \mathbb{Z}$ mit $c_i \equiv_p 0$ für $i \in [0, n-k-1]$.

Aus $f(X) = g(X) \cdot h(X)$ folgt nun $0 \not\equiv_{p^2} a_0 = b_0 \cdot c_0 \equiv_{p^2} 0$. *Widerspruch.* ▫

Beispiel 213 Es ist $X^8 + 25X^3 + 10$ irreduzibel in $\mathbb{Q}[X]$.

Dies folgt mit Eisenstein für $p = 5$.

In der Tat ist $25 \equiv_5 0$ und $10 \equiv_5 0$. Alle weiteren Koeffizienten, ausgenommen der Leitkoeffizient, sind null.

Dagegen ist $10 \not\equiv_{5^2} 0$.

Somit sind die Bedingungen von Lemma 212 erfüllt, und wir können folgern, daß das Polynom $X^8 + 25X^3 + 10$ in $\mathbb{Q}[X]$ irreduzibel ist.

Bemerkung 214 (Translation) *Sei K ein Körper. Sei $a \in K^\times$. Sei $b \in K$.*

(1) *Wir haben den Ringisomorphismus*

$$\begin{array}{rcccl} \varphi & : & K[X] & \xrightarrow{\sim} & K[X] \\ & & f(X) & \mapsto & f(aX+b) \end{array}$$

Sein Inverses ist

$$\begin{array}{rcccl} \psi & : & K[X] & \xrightarrow{\sim} & K[X] \\ & & g(X) & \mapsto & g(a^{-1}X - a^{-1}b) \end{array}$$

(2) *Sei $f(X) \in K[X]^\times \smallsetminus \mathrm{U}(K[X])$.*
Genau dann ist $f(X)$ irreduzibel, wenn $f(aX+b)$ irreduzibel ist.

Beweis. Zu (1). Es ist φ ein Ringmorphismus.

Es ist $\psi(\varphi(f(X))) = \psi(f(aX+b)) = f(a(a^{-1}X - a^{-1}b) + b) = f(X)$ für $f(X) \in K[X]$.

Es ist $\varphi(\psi(g(X))) = \varphi(g(a^{-1}X - a^{-1}b)) = g(a^{-1}(aX+b) - a^{-1}b) = g(X)$ für $g(X) \in K[X]$.

Zu (2). Sei $f(X)$ irreduzibel. Sei $f(aX+b) = g(X) \cdot h(X)$, mit $g(X), h(X) \in K[X]$. Anwenden von ψ gibt $f(X) = g(a^{-1}X - a^{-1}b) \cdot h(a^{-1}X - a^{-1}b)$. Da $f(X)$ irreduzibel ist, folgt $g(a^{-1}X - a^{-1}b) \in \mathrm{U}(K[X])$ oder $h(a^{-1}X - a^{-1}b) \in \mathrm{U}(K[X])$. Anwenden von φ gibt $g(X) \in \mathrm{U}(K[X])$ oder $h(X) \in \mathrm{U}(K[X])$. Somit ist $f(aX+b)$ irreduzibel.

In der umgekehrten Richtung genauso, nach Ersetzung von a durch a^{-1} und von b durch $-a^{-1}b$. ▫

Beispiel 215 Sei $p \in \mathbb{Z}_{\geqslant 2}$ eine Primzahl.

Wir wollen überprüfen, daß $f(X) := \sum_{k\in[0,p-1]} X^k = X^{p-1} + X^{p-2} + \ldots + X^0$ in $\mathbb{Q}[X]$ irreduzibel ist.

Es ist

$$f(X) \cdot (X-1) \;=\; (X^p + X^{p-1} + \ldots + X^1) - (X^{p-1} + X^{p-2} + \ldots + X^0) \;=\; X^p - 1 \;.$$

Einsetzen von $X+1$ für X gibt

$$f(X+1) \cdot X \;=\; (X+1)^p - 1 \;=\; X^p + \sum_{j\in[1,p-1]} \tbinom{p}{j} X^{p-j} \;.$$

Also ist

$$f(X+1) \;=\; X^{p-1} + \sum_{j\in[1,p-1]} \tbinom{p}{j} X^{p-j-1} \;.$$

Der konstante Term ist $\binom{p}{1} = p$. Alle Koeffizienten außer dem Leitkoeffizienten sind durch p teilbar, da für $j \in [1, p-1]$ in $\binom{p}{j} = \frac{p!}{(p-j)!\cdot j!}$ der Faktor p nur im Zähler, nicht im Nenner auftritt.

Eisenstein gibt also, daß $f(X+1)$ irreduzibel ist; vgl. Lemma 212.

Bemerkung 214.(2) gibt nun, daß $f(X)$ irreduzibel ist.

Zum Beispiel ist für $p = 5$ also $X^4 + X^3 + X^2 + X + 1$ irreduzibel in $\mathbb{Q}[X]$.

Bemerkung 216 Beim Konstruieren mit Zirkel und Lineal seien gewisse Punkte in der Ebene bereits konstruiert. Ihre Koordinaten mögen im Zwischenkörper K von $\mathbb{Q}$ und $\mathbb{R}$ liegen.

Die Koordinaten eines weiteren Punktes liegen dann in $K(b)$ für ein $b \in \mathbb{R}$ mit Minimalpolynom von Grad 1 oder 2 über K. Insbesondere ist $[K(b) : K] \in \{1, 2\}$.

Geht man von Punkten mit Koordinaten in $\mathbb{Q}$ aus, so erhält man durch iteriertes Konstruieren mit Zirkel und Lineal Punkte, deren Koordinaten in einem Zwischenkörper L von $\mathbb{Q}$ und $\mathbb{R}$ liegen mit $[L : \mathbb{Q}] = 2^n$ für ein $n \in \mathbb{Z}_{\geqslant 0}$; vgl. Lemma 205.

Also ist ein Punkt, dessen Koordinaten eine Körpererweiterung von $\mathbb{Q}$ erzeugen, die einen Grad hat, der keine Potenz von 2 ist, nicht mit Zirkel und Lineal konstruierbar; vgl. Lemma 205.

So zum Beispiel ist der Punkt mit den Koordinaten $(0, \sqrt[3]{2})$ nicht mit Zirkel und Lineal konstruierbar. Denn wir haben $\mu_{\sqrt[3]{2},\mathbb{Q}}(X) = X^3 - 2$; vgl. Lemma 212 oder Bemerkung 207, Bemerkung 196. Also ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$; vgl. Lemma 194. Und das ist keine Potenz von 2.

Das Delische Problem, die Kantenlänge eines Würfels mit Volumen 2 zu konstruieren, ist also mit Zirkel und Lineal nicht lösbar.

3.5 Endliche Untergruppen der Einheitengruppe eines Körpers

Sei K ein Körper. Wir erinnern an die Einheitengruppe $\mathrm{U}(K) = K^\times$ von K.

Bemerkung 217 *Sei $f(X) \in K[X]$ normiert.*

Schreibe $N := \{\, a \in K \,:\, f(a) = 0 \,\}$ für die Menge der Nullstellen von $f(X)$ in K.

Dann ist $|N| \leqslant \deg(f(X))$.

Beweis. Induktion über $\deg(f(X))$.

Induktionsanfang. Falls $\deg(f(X)) = 0$ ist, dann ist $N = \emptyset$.

Induktionsschritt. Sei $\deg(f(X)) \geqslant 1$.

Fall $N = \emptyset$. Die Aussage trifft zu.

Fall $N \neq \emptyset$. Sei $a \in N$. Polynomdivision gibt $f(X) = (X - a) \cdot g(X) + r(X)$ mit $g(X)$, $r(X) \in K[X]$ und $\deg(r(X)) < \deg(X - a) = 1$. Also ist $r(X) = r_0 \in K$. Es folgt $0 = f(a) = (a-a)\cdot g(a)+r(a) = r_0$. Folglich ist $r(X) = 0$. Somit ist $f(X) = (X-a)\cdot g(X)$.

Es ist $g(X) \in K[X]$ normiert. Es ist $\deg(g(X)) = \deg(f(X)) - 1$.

Sei $N' := \{\, b \in K \,:\, g(b) = 0 \,\}$. Aus $(X - a) \cdot g(X) = f(X)$ folgt $\{a\} \cup N' = N$. Nach Induktionsvoraussetzung ist $|N'| \leqslant \deg(g(X))$. Folglich ist

$$|N| \;=\; |\{a\} \cup N'| \;\leqslant\; 1 + |N'| \;\leqslant\; 1 + \deg(g(X)) \;=\; \deg(f(X))\,.$$

□

Lemma 218

Sei $G \leqslant \mathrm{U}(K)$ eine Untergruppe endlicher Ordnung.

Dann ist G zyklisch.

Beweis. Da G eine endliche abelsche Gruppe ist, ist G isomorph zu einer Gruppe der Form $\mathrm{C}_{d_1} \times \mathrm{C}_{d_2} \times \ldots \times \mathrm{C}_{d_k}$ mit $k \geqslant 0$, mit $d_i \in \mathbb{Z}_{\geqslant 1}$ für $i \in [1, k]$, wobei d_i ein Teiler von d_{i+1} ist für $i \in [1, k-1]$. O.E. ist $d_1 \in \mathbb{Z}_{\geqslant 2}$. Vgl. Korollar 171, Bemerkung 173.

Annahme, es ist G nicht zyklisch. Dann ist $k \geqslant 2$. Jedes Element a in $\mathrm{C}_{d_1} \times \mathrm{C}_{d_2} \times \ldots \times \mathrm{C}_{d_k}$ erfüllt $a^{d_k} = 1$. Also gilt auch für jedes Element a in G, daß $a^{d_k} = 1$ ist.

Sei $N := \{\, a \in K \,:\, a^{d_k} - 1 = 0 \,\}$. Es ist $G \subseteq N$, also $|G| \leqslant |N|$. Es ist $|N| \leqslant d_k$; vgl. Bemerkung 217.

Es ist $|G| = d_1 \cdot d_2 \cdot \ldots \cdot d_k$.

Also folgt

$$d_1 \cdot d_2 \cdot \ldots \cdot d_k \;=\; |G| \;\leqslant\; |N| \;\leqslant\; d_k\,.$$

Somit ist $d_1 \cdot d_2 \cdot \ldots \cdot d_{k-1} \leqslant 1$. Aber $k \geqslant 2$ und $d_1 \geqslant 2$. Wir haben einen *Widerspruch.* □

Korollar 219 *Ist K ein endlicher Körper, dann ist $\mathrm{U}(K)$ zyklisch.*

Beweis. Diesenfalls können wir $G = \mathrm{U}(K)$ betrachten in Lemma 218.

Beispiel 220

(1) Es ist $\mathrm{U}(\mathbb{F}_7) = \mathbb{F}_7^\times$ zyklisch; vgl. Korollar 219. Also $\mathrm{U}(\mathbb{F}_7) \simeq \mathrm{C}_6$.

Konkret ist darin $\langle 3\rangle = \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, -1, -3, -2\} = \mathrm{U}(\mathbb{F}_7)$.

Es ist $\mathrm{U}(\mathbb{F}_7) = \langle 3\rangle = \langle -2\rangle$. Also sind 3 und auch -2 Erzeuger von $\mathrm{U}(\mathbb{F}_7)$.

Aber z.B. $|\langle 2\rangle| = 3$. Also $\langle 2\rangle < \mathrm{U}(\mathbb{F}_7)$, und 2 ist kein Erzeuger von $\mathrm{U}(\mathbb{F}_7)$.

> Sei $n \in \mathbb{Z}_{\geqslant 2}$ ohne quadratischen Teiler. Ob für unendlich viele Primzahlen p nun $\langle n\rangle = \mathrm{U}(\mathbb{F}_p)$ gilt, ist eine offene Frage. Artin vermutete dies. Er vermutete genauer, daß dies für einen gewissen Prozentsatz aller Primzahlen gilt.

(2) Es ist $\mathrm{U}(\mathbb{F}_4) = \mathbb{F}_4^\times$ zyklisch; vgl. Beispiel 197.(5), Korollar 219. Also $\mathrm{U}(\mathbb{F}_4) \simeq \mathrm{C}_3$.

Wir erinnern an $\alpha^2 = \alpha + 1$ und $2\alpha = 0$.

Es wird in $\mathbb{F}_4$ konkret $\langle\alpha\rangle = \{\alpha^0, \alpha^1, \alpha^2\} = \{1, \alpha, \alpha+1\} = \mathrm{U}(\mathbb{F}_4)$.

Ebenso ist $\langle\alpha{+}1\rangle = \{(\alpha{+}1)^0, (\alpha{+}1)^1, (\alpha{+}1)^2\} = \{1, \alpha^2, \alpha^4\} = \{1, \alpha^2, \alpha\} = \mathrm{U}(\mathbb{F}_4)$.

(3) Sei $G := \{\, z \in \mathbb{C} \,:\, z^9 = 1 \,\}$.

Es ist $G \leqslant \mathrm{U}(\mathbb{C})$, denn zum einen ist $1 \in G$, zum anderen ist für $z, w \in G$ auch $(z \cdot w^{-1})^9 = z^9 \cdot w^{-9} = 1$ und also $z \cdot w^{-1} \in G$.

Es ist $|G| \leqslant 9$ nach Bemerkung 217. Es ist G zyklisch nach Lemma 218.

Konkret, sei $\zeta_9 := \exp(2\pi\mathrm{i}/9) \in \mathbb{C}$. Dann ist $\zeta_9^9 = 1$.

Es ist $\{\, \zeta_9^j \,:\, j \in [0,8] \,\} \subseteq G$.

Es ist $\zeta_9^j = \exp(2\pi\mathrm{i}j/9)$. Also ist $\zeta_9^j \neq \zeta_9^k$ für $j, k \in [0,8]$ mit $j \neq k$.

Folglich ist $\{\, \zeta_9^j \,:\, j \in [0,8] \,\} = G$.

Insgesamt erhalten wir $G = \langle\zeta_9\rangle \simeq \mathrm{C}_9$.

Ebenso ist $\langle\zeta_9^2\rangle = G$, $\langle\zeta_9^4\rangle = G$, $\langle\zeta_9^5\rangle = G$, $\langle\zeta_9^7\rangle = G$ und $\langle\zeta_9^8\rangle = G$.

(4) Es ist $\mathrm{U}(\mathbb{Q})$ nicht zyklisch. Aber dies ist ja auch keine endliche Untergruppe der Einheitengruppe eines Körpers.

Annahme, es ist $\mathrm{U}(\mathbb{Q})$ zyklisch. Dann gibt es ein Element $x \in \mathrm{U}(\mathbb{Q})$ mit $\langle x\rangle = \mathrm{U}(\mathbb{Q})$.

Wir schreiben $x = \frac{a}{b}$ als gekürzten Bruch, wobei $a, b \in \mathbb{Z}^\times$. Dann ist

$$\langle x\rangle \;=\; \{\, a^k b^{-k} \,:\, k \in \mathbb{Z} \,\}\,.$$

Teilt eine Primzahl p also den Zähler eines Elements von $\langle x\rangle$ in gekürzter Darstellung, dann teilt sie a oder b.

Sei q eine Primzahl, die weder a noch b teilt. Eine solche existiert, da es in $\mathbb{Z}$ unendlich viele Primzahlen gibt. Dann ist $q = \frac{q}{1} \in \mathbb{Q}^\times \smallsetminus \langle x\rangle$.

3.6 Formales Ableiten und mehrfache Faktoren

Sei K ein Körper.

Definition 221 Sei $f(X) = \sum_{i \geqslant 0} a_i X^i \in K[X]$ gegeben.

Wir setzen die *formale Ableitung*

$$f'(X) \ := \ \sum_{i \geqslant 1} a_i \, i X^{i-1} \ = \ \sum_{i \geqslant 0} a_{i+1}(i+1) X^i \ \in \ K[X]$$

Die formale Ableitung heißt auch kurz Ableitung.

Das Adjektiv "formal" bezieht sich darauf, daß wir auf Differenzenquotienten und Grenzwertüberlegungen verzichtet haben, um die Ableitung zu definieren. Verzichten mußten, denn unser allgemein gewählter Körper K ließe dies wohl nicht zu.

Bemerkung 222 Die Abbildung

$$\begin{array}{ccc} K[X] & \to & K[X] \\ f(X) & \mapsto & f'(X) \end{array}$$

ist K-linear.

Beispiel 223

(1) Sei $f(X) = X^3 - 5X^2 + X - 1 \in \mathbb{Q}[X]$. Dann ist $f'(X) = 3X^2 - 10X + 1 \in \mathbb{Q}[X]$.

(2) Sei $f(X) = X^4 + X^2 \in \mathbb{F}_2[X]$. Dann ist $f'(X) = 0$.

Wir brauchen die Produktregel nun auch für das formale Ableiten:

Lemma 224 *Seien* $f(X), \, g(X) \, \in \, K[X]$.

Es ist

$$(f(X) \cdot g(X))' \ = \ f'(X) \cdot g(X) + f(X) \cdot g'(X) \ .$$

Beweis. Wir vergleichen die beiden Abbildungen

$$\begin{array}{ccc} K[X] \times K[X] & \to & K[X] \\ (u(X), v(X)) & \mapsto & (u(X) \cdot v(X))' \end{array}$$

und

$$\begin{array}{ccc} K[X] \times K[X] & \to & K[X] \\ (u(X), v(X)) & \mapsto & u'(X) \cdot v(X) + u(X) \cdot v'(X) \ . \end{array}$$

Beide sind K-bilinear. Also dürfen wir uns auf die Betrachtung von Basiselementen im ersten und im zweiten Eintrag beschränken.

Somit ist o.E. $f(X) = X^k$ und $g(X) = X^\ell$ für gewisse k, $\ell \in \mathbb{Z}_{\geqslant 0}$.

Fall $k = 0$ und $\ell = 0$. Es ist $(f(X) \cdot g(X))' = 0$ und $f'(X) \cdot g(X) + f(X) \cdot g'(X) = 0$. Das ist dasselbe.

Fall $k = 0$ und $\ell \geqslant 1$. Es ist $(f(X) \cdot g(X))' = \ell X^{\ell-1}$ und $f'(X) \cdot g(X) + f(X) \cdot g'(X) = 0 + 1 \cdot \ell X^{\ell-1}$. Das ist dasselbe.

Fall $k \geqslant 1$ und $\ell = 0$. Es ist $(f(X) \cdot g(X))' = kX^{k-1}$ und $f'(X) \cdot g(X) + f(X) \cdot g'(X) = kX^{k-1} \cdot 1 + 0$. Das ist dasselbe.

Fall $k \geqslant 1$ und $\ell \geqslant 1$. Es ist $(f(X) \cdot g(X))' = (k + \ell)X^{k+\ell-1}$.

Es ist $f'(X) \cdot g(X) + f(X) \cdot g'(X) = kX^{k-1} \cdot X^\ell + X^k \cdot \ell X^{\ell-1}$.

Das ist dasselbe. □

Definition 225 Sei $f(X) \in K[X]^\times$.

Es heißt $f(X)$ *quadratfrei*, falls es kein $u(X) \in K[X]^\times$ mit $\deg(u(X)) \geqslant 1$ so gibt, daß $u(X)^2$ ein Teiler von $f(X)$ ist.

Beispiel 226 Es ist $X^3 - X \in \mathbb{C}[X]$ quadratfrei. Es ist $X^3 - X^2 \in \mathbb{C}[X]$ nicht quadratfrei.

Lemma 227 *Sei $f(X) \in K[X]^\times$ gegeben.*

(1) *Ist* $\mathrm{ggT}(f(X), f'(X)) = 1$, *dann ist $f(X)$ quadratfrei.*

(2) *Ist* $\mathrm{char}(K) = 0$ *und $f(X)$ quadratfrei, dann ist* $\mathrm{ggT}(f(X), f'(X)) = 1$.

Beweis. Zu (1). Sei $f(X)$ nicht quadratfrei. Sei also $f(X) = u(X)^2 \cdot v(X)$, wobei $u(X) \in K[X]^\times$ mit $\deg(u(X)) \geqslant 1$ und $v(X) \in K[X]^\times$ sei.

Dann wird

$$\begin{array}{rcl} f'(X) & = & (u(X)^2 \cdot v(X))' \\ & \overset{\text{L. } 224}{=} & 2u(X) \cdot u'(X) \cdot v(X) + u(X)^2 \cdot v'(X) \\ & = & u(X) \cdot (2u'(X) \cdot v(X) + u(X) \cdot v'(X)) \, . \end{array}$$

Also ist $u(X)$ ein Teiler von $\mathrm{ggT}(f(X), f'(X))$. Also ist $\mathrm{ggT}(f(X), f'(X)) \neq 1$.

Zu (2). Sei $\mathrm{char}(K) = 0$ und $f(X)$ quadratfrei. Wir schreiben

$$f(X) \; = \; s \cdot f_1(X) \cdot f_2(X) \cdot \ldots \cdot f_k(X) \, ,$$

mit $s \in K^\times$, mit $k \geqslant 0$, mit $f_i(X) \in K[X]$ normiert und irreduzibel für $i \in [1, k]$ und mit $f_i(X) \neq f_j(X)$ für $i, j \in [1, k]$ mit $i \neq j$. Vgl. Beispiel 52.(2), Lemma 58, Lemma 59.(1).

Annahme, es ist $\mathrm{ggT}(f(X), f'(X)) \neq 1$. Dann können wir ein $i \in [1, k]$ so wählen, daß $f_i(X)$ ein Teiler von $f'(X)$ ist. Mit Lemma 224 wird aber

$$f'(X) \; = \; s \cdot \sum_{j \in [1,k]} f_j'(X) \cdot \prod_{t \in [1,k] \smallsetminus \{j\}} f_t(X) \, .$$

Es folgt, daß $f_i(X)$ auch ein Teiler von $f_i'(X) \cdot \prod_{t \in [1,k] \smallsetminus \{i\}} f_t(X)$ ist, da die anderen Summanden durch $f_i(X)$ teilbar sind.

Es folgt, daß $f_i(X)$ ein Teiler von $f_i'(X)$ ist. Wegen $\mathrm{char}(K) = 0$ ist das aber nicht möglich, und wir haben einen *Widerspruch*. ▫

Eine Spitzfindigkeit ist noch zu klären:

Bemerkung 228 *Sei $L|K$ eine Körpererweiterung.*

Seien $f(X)$, $g(X) \in K[X]^\times$ gegeben.

Sei $h(X)$ ein größter gemeinsamer Teiler von $f(X)$ und $g(X)$, gebildet in $K[X]$.

Dann ist $h(X)$ auch ein größter gemeinsamer Teiler von $f(X)$ und $g(X)$, gebildet in $L[X]$.

Man kann folgenden Beweis informell zusammenfassen zu: Die Berechnung von $\mathrm{ggT}(f(X), g(X))$ unter Verwendung des Euklidischen Algorithmus, die in $K[X]$ durchgeführt werden kann, behält in $L[X]$ ihre Gültigkeit.

Beweis. Induktion nach $\min\{\deg(f(X)), \deg(g(X))\}$.

Sei o.E. $\deg(g(X)) \leqslant \deg(f(X))$.

Polynomdivision gibt $f(X) = g(X) \cdot q(X) + r(X)$ mit $q(X), r(X) \in K[X]$ und $\deg(r(X)) < \deg(g(X))$.

Es ist $u(X) \in K[X]$ genau dann ein gemeinsamer Teiler von $f(X)$ und $g(X)$ in $K[X]$, wenn es dort ein gemeinsamer Teiler von $r(X)$ und $g(X)$ ist. Also ist $u(X)$ auch genau dann ein größter gemeinsamer Teiler von $f(X)$ und $g(X)$ in $K[X]$, wenn es dort ein größter gemeinsamer Teiler von $r(X)$ und $g(X)$ ist. Vgl. Bemerkung 61.(5).

Es ist $v(X) \in L[X]$ genau dann ein gemeinsamer Teiler von $f(X)$ und $g(X)$ in $L[X]$, wenn es dort ein gemeinsamer Teiler von $r(X)$ und $g(X)$ ist. Also ist $u(X)$ auch genau dann ein größter gemeinsamer Teiler von $f(X)$ und $g(X)$ in $L[X]$, wenn es dort ein größter gemeinsamer Teiler von $r(X)$ und $g(X)$ ist. Vgl. Bemerkung 61.(5).

Fall $r(X) = 0$. Es ist $g(X)$ ein größter gemeinsamer Teiler von $f(X)$ und $g(X)$, gebildet in $K[X]$ oder in $L[X]$. Es ist $g(X)$ assoziiert zu $h(X)$ in $K[X]$, also auch in $L[X]$. Also ist $h(X)$ auch ein größter gemeinsamer Teiler von $f(X)$ und $g(X)$, gebildet in $L[X]$.

Fall $r(X) \neq 0$. Es ist $h(X)$ auch ein größter gemeinsamer Teiler von $r(X)$ und $g(X)$, gebildet in $K[X]$. Nach Induktionsvoraussetzung ist $h(X)$ ein größter gemeinsamer Teiler von $r(X)$ und $g(X)$, gebildet in $L[X]$. Also ist $h(X)$ ein größter gemeinsamer Teiler von $f(X)$ und $g(X)$, gebildet in $L[X]$. ▫

Bemerkung 229 *Sei $\mathrm{char}(K) = 0$.*

Sei $f(X) \in K[X]^\times$ gegeben. Sei $L|K$ eine Körpererweiterung.

Es ist $f(X)$ genau dann quadratfrei in $K[X]$, wenn $f(X)$ quadratfrei in $L[X]$ ist.

Beweis. Dies folgt mit Lemma 227 unter Berücksichtigung von Bemerkung 228. ▫

3.7 Kreisteilungspolynome

Sei $n \geqslant 1$.

Definition 230

(1) Sei $\zeta_n := \exp(2\pi \mathrm{i}/n) \in \mathbb{C}$.

Da $\zeta_n^n - 1 = 0$ ist, da also ζ_n eine Nullstelle von $X^n - 1$ ist, ist ζ_n algebraisch über $\mathbb{Q}$.

(2) Sei $\Phi_n(X) := \mu_{\zeta_n,\mathbb{Q}}(X) \in \mathbb{Q}[X]$ das *n-te Kreisteilungspolynom.*

Bemerkung 231 *Es ist* $X^n - 1 = \prod_{k\in[0,n-1]}(X - \zeta_n^k)$.

Beweis. Beide Seiten sind normiert von Grad n. Die rechte Seite teilt die linke Seite in $\mathbb{C}[X]$. Also haben wir Gleichheit. ▫

Bemerkung 232 *Sei $z \in \mathbb{C}$. Sei $u(X) \in \mathbb{Z}[X]$ normiert gegeben mit $u(z) = 0$.*

Dann ist $\mu_{z,\mathbb{Q}}(X) \in \mathbb{Z}[X]$.

Beweis. Es ist $\mu_{z,\mathbb{Q}}(X)$ ein Teiler von $u(X)$ in $\mathbb{Q}[X]$. Die Aussage folgt nun mit Bemerkung 209.(1). ▫

Bemerkung 233 Es ist $\Phi_n(X) \in \mathbb{Z}[X]$. Es ist $\Phi_n(X)$ ein Teiler von $X^n - 1$ in $\mathbb{Z}[X]$.

Beweis. Da $\zeta_n^n - 1 = 0$ ist, folgt $\Phi_n(X) \in \mathbb{Z}[X]$; vgl. Bemerkung 232.

Es ist $\Phi_n(X)$ ein Teiler von $X^n - 1$ in $\mathbb{Q}[X]$; vgl. Lemma 194. Dank Polynomdivision gilt dies auch in $\mathbb{Z}[X]$. ▫

Lemma 234 *Sei $z \in \mathbb{C}$ mit $\Phi_n(z) = 0$.*

Sei p eine Primzahl, die nicht n teilt.

Dann ist $\Phi_n(z^p) = 0$.

Beweis. Für $u(X) \in \mathbb{Z}[X]$ schreiben wir wieder $\bar{u}(X) \in \mathbb{F}_p[X]$ für das Polynom, das aus $u(X)$ durch koeffizientenweise Restklassenbildung entsteht.

Wir schreiben $f(X) := \Phi_n(X) \in \mathbb{Z}[X]$; vgl. Bemerkung 233.

Annahme, $f(z^p) \neq 0$. Da $\Phi_n(z) = 0$ ist, ist auch $z^n - 1 = 0$ und also auch $(z^p)^n - 1 = 0$. Also ist z^p algebraisch über $\mathbb{Q}$. Wir schreiben $g(X) := \mu_{z^p,\mathbb{Q}}(X) \in \mathbb{Q}[X]$. Es ist $g(X) \in \mathbb{Z}[X]$; vgl. Bemerkung 232.

Wegen $f(z^p) \neq 0$ sind $f(X)$ und $g(X)$ zwei verschiedene irreduzible normierte Polynome in $\mathbb{Q}[X]$, insbesondere nicht zueinander assoziiert. Also ist $f(X) \cdot g(X)$ ein Teiler von $X^n - 1$ in $\mathbb{Q}[X]$. Sei $h(X) \in \mathbb{Q}[X]$ mit $f(X) \cdot g(X) \cdot h(X) = X^n - 1$.

Da $f(X) \cdot g(X) \in \mathbb{Z}[X]$ liegt und normiert ist, folgt dank Polynomdivision von $X^n - 1$ durch $f(X) \cdot g(X)$, daß auch $h(X)$ ein normiertes Polynom in $\mathbb{Z}[X]$ ist.

Es hat das Polynom $g(X^p)$ die Nullstelle z. Also ist $f(X)$ ein Teiler von $g(X^p)$ in $\mathbb{Z}[X]$. Also ist $\bar{f}(X)$ ein Teiler von $\bar{g}(X^p) = \bar{g}(X)^p$ in $\mathbb{F}_p[X]$.

Sei $v(X) \in \mathbb{Z}[X]$ ein normiertes Polynom derart, daß $\bar{v}(X) \in \mathbb{F}_p[X]$ ein irreduzibler Teiler von $\bar{f}(X)$ ist. Dann teilt $\bar{v}(X) \in \mathbb{F}_p[X]$ auch $\bar{g}(X)^p$ und damit auch $\bar{g}(X)$. Somit ist $X^n - 1 = \bar{f}(X) \cdot \bar{g}(X) \cdot \bar{h}(X)$ in $\mathbb{F}_p[X]$ nicht quadratfrei.

Aber in $\mathbb{F}_p[X]$ ist $(X^n - 1)' = nX^{n-1} \neq 0$, da $n \not\equiv_p 0$. Also ist $\mathrm{ggT}(X^n - 1, (X^n - 1)') = \mathrm{ggT}(X^n - 1, nX^{n-1}) = 1$. Somit ist $X^n - 1$ in $\mathbb{F}_p[X]$ quadratfrei; vgl. Lemma 227.(1).

Wir haben einen *Widerspruch*. ▫

Lemma 235 *Es ist* $\Phi_n(X) = \prod_{k \in [0,n-1],\ \mathrm{ggT}(k,n)=1} (X - \zeta_n^k)$.

Beweis. Es ist $\Phi_n(X)$ ein Teiler von $X^n - 1 = \prod_{k \in [0,n-1]} (X - \zeta_n^k)$; vgl. Bemerkungen 233, 231.

Sei $k \in \mathbb{Z}$. Es genügt, folgende *Behauptung* zu zeigen.

$$\Phi_n(\zeta_n^k) \ = \ 0 \qquad \stackrel{!}{\Longleftrightarrow} \qquad \mathrm{ggT}(k,n) \ = \ 1$$

Zu $\Leftarrow$. Man zerlege k in Primfaktoren und wende Lemma 234 für jeden Primfaktor an.

Zu $\Rightarrow$. *Annahme*, $\mathrm{ggT}(k,n) =: d > 1$. Schreibe $n' := n/d$ und $k' := k/d$. Es ist $\Phi_n(X) = \mu_{\zeta_n^k, \mathbb{Q}}(X)$, da es ein irreduzibles normiertes Polynom in $\mathbb{Q}[X]$ mit Nullstelle ζ_n^k ist; vgl. Bemerkung 196. Es ist $\zeta_n^k = \zeta_n^{d \cdot k'} = \zeta_{n'}^{k'}$ aber auch eine Nullstelle von $X^{n'} - 1$. Also ist $\Phi_n(X)$ ein Teiler von $X^{n'} - 1$; vgl. Lemma 194. Aber $\Phi_n(\zeta_n) = 0$ und $\zeta_n^{n'} - 1 \neq 0$. Dies ist ein *Widerspruch*. ▫

Lemma 236 *Es ist* $X^n - 1 = \prod_{d \in [1,n],\ d \text{ teilt } n} \Phi_d(X)$.

Beweis. Sei $k \in [0, n-1]$. Wir haben zu zeigen, daß es genau einen Teiler $d \in [1,n]$ von n gibt und genau ein $\ell \in [0, d-1]$ teilerfremd zu d mit

$$\zeta_n^k \ \stackrel{!}{=} \ \zeta_d^\ell \ = \ \zeta_n^{\ell \cdot (n/d)} \ .$$

vgl. Bemerkung 231, Lemma 235. Wir suchen also d und ℓ wie beschrieben mit $k = \ell \cdot (n/d)$. Es muß dazu n/d ein Teiler von k sein. Da ℓ teilerfremd zu d zu sein hat, muß n/d der größte gemeinsame Teiler von n und k sein.

Mit $g := \mathrm{ggT}(n,k)$ muß also $\ell = k/g$ und $d = n/g$ sein. ▫

Beispiel 237

(1) Es ist $\Phi_1(X) = X - 1$.
Wegen $X^2 - 1 = \Phi_1(X) \cdot \Phi_2(X)$ folgt $\Phi_2(X) = X + 1$.
Wegen $X^3 - 1 = \Phi_1(X) \cdot \Phi_3(X)$ folgt $\Phi_3(X) = X^2 + X + 1$.
Wegen $X^4 - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_4(X)$ folgt $\Phi_4(X) = X^2 + 1$.
Wegen $X^5 - 1 = \Phi_1(X) \cdot \Phi_5(X)$ folgt $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$.
Wegen $X^6 - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_3(X) \cdot \Phi_6(X)$ folgt $\Phi_6(X) = \frac{X^6-1}{\Phi_1(X)\Phi_2(X)\Phi_3(X)} = \frac{X^6-1}{(X+1)(X^3-1)} = \frac{X^3+1}{X+1} = X^2 - X + 1$.

(2) Sei p eine Primzahl. Wegen $X^p - 1 = \Phi_1(X) \cdot \Phi_p(X)$ folgt

$$\Phi_p(X) \;=\; X^{p-1} + X^{p-2} + \ldots + X^0 \;.$$

Wir wissen nun sowohl von Beispiel 215 als auch, unabhängig davon, von Definition 230.(2) und Lemma 194, daß $\Phi_p(X) \in \mathbb{Q}[X]$ irreduzibel ist.

Definition 238 Sei

$$\begin{array}{rcccl} \varphi & : & \mathbb{Z}_{\geqslant 1} & \to & \mathbb{Z}_{\geqslant 1} \\ & & m & \mapsto & \varphi(m) := |\{\, k \in [1,m] \,:\, \mathrm{ggT}(k,m) = 1 \,\}| \end{array}$$

die *Eulersche* φ*-Funktion.*

Bemerkung 239

(1) *Es ist* $\varphi(n) = \deg(\Phi_n(X))$ *; vgl. Lemma* 234.

(2) *Es ist* $\varphi(n) = |\mathrm{U}(\mathbb{Z}/(n))|$.

(3) *Es ist* $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$.

(4) *Sind* k *und* ℓ *aus* $\mathbb{Z}_{\geqslant 1}$ *teilerfremd, dann ist* $\varphi(k \cdot \ell) = \varphi(k) \cdot \varphi(\ell)$.

(5) *Sei* p *eine Primzahl. Sei* $a \in \mathbb{Z}_{\geqslant 1}$.
Es ist $\varphi(p^a) = (p-1) \cdot p^{a-1}$.

Beweis.

Zu (1). Nach Lemma 234 ist $\Phi_n(X) = \prod_{k \in [0,n-1],\ \mathrm{ggT}(k,n)=1} (X - \zeta_n^k)$. Also ist

$$\deg(\Phi_n(X)) \;=\; |\{\, k \in [0,n-1] \,:\, \mathrm{ggT}(k,n) = 1 \,\}| \;=\; |\{\, k \in [1,n] \,:\, \mathrm{ggT}(k,n) = 1 \,\}| \;=\; \varphi(n) \;.$$

Zu (2). Für $k \in [1,n]$ ist $k + (n) \in \mathbb{Z}/(n)$ genau dann invertierbar, wenn $\mathrm{ggT}(k,n) = 1$ ist. Denn $k + (n) \in \mathbb{Z}/(n)$ ist genau dann invertierbar, wenn $\ell \in \mathbb{Z}$ existiert mit

$(k + (n)) \cdot (\ell + (n)) = 1 + (n)$, d.h. wenn $\ell, t \in \mathbb{Z}$ existieren mit $k \cdot \ell = 1 + n \cdot t$, d.h. mit $k \cdot \ell + n \cdot (-t) = 1$. Dies trifft genau dann zu, wenn $(k, n) = (1)$ ist, d.h. wenn $\mathrm{ggT}(k, n) = 1$ ist.

Zu (3). Es ist $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \overset{\text{L. }194}{=} \deg(\mu_{\zeta_n,\mathbb{Q}}(X)) \overset{\text{D. }230.(2)}{=} \deg(\Phi_n(X)) \overset{(1)}{=} \varphi(n)$.

Zu (4). Es ist $\mathbb{Z}/(k \cdot \ell) \simeq \mathbb{Z}/(k) \times \mathbb{Z}/(\ell)$; vgl. Satz 34. Also ist auch

$$\mathrm{U}(\mathbb{Z}/(k \cdot \ell)) \simeq \mathrm{U}(\mathbb{Z}/(k) \times \mathbb{Z}/(\ell)) \simeq \mathrm{U}(\mathbb{Z}/(k)) \times \mathrm{U}(\mathbb{Z}/(\ell)) .$$

Somit ist auch

$$\varphi(k \cdot \ell) \overset{(2)}{=} |\mathrm{U}(\mathbb{Z}/(k \cdot \ell))| = |\mathrm{U}(\mathbb{Z}/(k)) \times \mathrm{U}(\mathbb{Z}/(\ell))| = |\mathrm{U}(\mathbb{Z}/(k))| \cdot |\mathrm{U}(\mathbb{Z}/(\ell))| \overset{(2)}{=} \varphi(k) \cdot \varphi(\ell) .$$

Zu (5). In $[1, p^a]$ gibt es p^{a-1} Elemente, die durch p teilbar sind, und daher $(p-1) \cdot p^{a-1}$ Elemente, die das nicht sind.

Beispiel 240 Es ist $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$ und $\varphi(6) = 2$.

Vgl. Beispiel 237.(1).

3.8 Der algebraische Abschluß

3.8.1 Begriff

Definition 241 Sei K ein Körper.

Es heißt K *algebraisch abgeschlossen*, wenn es für jedes Polynom $f(X) \in K[X]$ mit $\deg(f(X)) \geqslant 1$ wenigstens ein $a \in K$ gibt mit $f(a) = 0$.

Bemerkung 242 Sei K ein Körper. Genau dann ist K algebraisch abgeschlossen, wenn jedes irreduzible normierte Polynom in $K[X]$ von der Form $X - a$ ist für ein $a \in K$.

Dies folgt mit Abdividieren von einem zu einer Nullstelle gehörigen Polynomen von Grad 1.

Bemerkung 243 Es ist $\mathbb{C}$ algebraisch abgeschlossen, wie man mit Mitteln der Analysis zeigt.

Definition 244 Sei K ein Körper.

Eine Körpererweiterung $L|K$ heißt *algebraischer Abschluß* von K, wenn L algebraisch abgeschlossen ist und wenn jedes $y \in L$ algebraisch über K ist.

Wir wollen zeigen, daß jeder Körper einen algebraischen Abschluß hat. Dazu brauchen wir ein Hilfsmittel aus der Mengentheorie: das Lemma von Kuratowkski-Zorn; vgl. §3.8.2.

Beispiel 245

(1) Es ist $\mathbb{C}|\mathbb{R}$ ein algebraischer Abschluß von $\mathbb{R}$.

(2) Es ist $\mathbb{C}|\mathbb{C}$ ein algebraischer Abschluß von $\mathbb{C}$.

3.8.2 Lemma von Kuratowski-Zorn

Definition 246 Ein *Poset* $(X, \leqslant)$ ist eine Menge X, zusammen mit einer Teilmenge $(\leqslant) \subseteq X \times X$ derart, daß folgendes gilt. ([8])

Wir schreiben zunächst $\quad x \leqslant x' \quad :\Leftrightarrow \quad (x, x') \in (\leqslant)$.

(1) Für $x \in X$ ist $x \leqslant x$.

(2) Für $x,\, x' \in X$ mit $x \leqslant x'$ und $x' \leqslant x$ ist $x = x'$.

(3) Für $x,\, x',\, x'' \in X$ mit $x \leqslant x'$ und $x' \leqslant x''$ ist $x \leqslant x''$.

Wir schreiben oft kurz $X := (X, \leqslant)$.

Man nennt $(\leqslant)$ eine *Teilordnung* auf X. Ein Poset heißt auch eine *teilgeordnete Menge*.

Eigenschaft (1) heißt *Reflexivität*. Eigenschaft (2) heißt *Identitivität*. Eigenschaft (3) heißt *Transitivität*.

Wir sagen, es sind $x,\, x' \in X$ *vergleichbar*, wenn $x \leqslant x'$ oder $x' \leqslant x$ ist.

Ein Poset X heißt *linear geordnet*, wenn x und x' vergleichbar sind für $x,\, x' \in X$.

Wir schreiben auch $x < x'$ für ($x \leqslant x'$ und $x \neq x'$). Mit anderen Worten, es ist

$$(<) \;=\; (\leqslant) \smallsetminus \{\, (x, x) \,:\, x \in X \,\}\,.$$

Definition 247 Sei X ein Poset. Sei $x \in X$.

(1) Es heißt x *minimal* in X, falls es kein $y \in X$ gibt mit $y < x$.

(2) Es heißt x *initial* in X, falls $x \leqslant y$ gilt für $y \in X$.
Falls X ein initiales Element hat, dann ist dies eindeutig bestimmt.

(3) Es heißt x *maximal* in X, falls es kein $y \in X$ gibt mit $x < y$.

(4) Es heißt x *terminal* in X, falls $y \leqslant x$ gilt für $y \in X$.
Falls X ein terminales Element hat, dann ist dies eindeutig bestimmt.

[8] Engl. partially ordered set.

Bemerkung 248 *Sei X ein Poset. Sei $x \in X$.*

(1) *Ist x initial in X, dann ist x auch minimal in X.*

(2) *Ist x terminal in X, dann ist x auch maximal in X.*

Beweis. Zu (1). Sei x initial in X. *Annahme*, es gibt ein $y \in X$ mit $y < x$. Da x initial ist, ist $x \leqslant y$. Aus $y \leqslant x$ und $x \leqslant y$ folgt $y = x$. *Widerspruch.* Also ist x minimal in X. ▫

Bemerkung 249 *Sei X ein linear geordnetes Poset. Sei $x \in X$.*

(1) *Es ist x genau dann initial in X, wenn x minimal in X ist.*

(2) *Es ist x genau dann terminal in X, wenn x maximal in X ist.*

Beweis. Zu (1). Dank Bemerkung 248.(1) genügt es, die umgekehrte Implikation zu zeigen.

Sei x minimal in X. Wir haben zu zeigen, daß x initial in X ist. Sei $y \in X$. Wir haben zu zeigen, daß $x \overset{!}{\leqslant} y$ ist.

Annahme, es ist nicht $x \leqslant y$. Da X linear geordnet ist, ist $x \leqslant y$ oder $y \leqslant x$. Es folgt $y < x$. Dies steht aber im *Widerspruch* zur Minimalität von x. ▫

Bemerkung 250 Sei X ein Poset. Sei $Y \subseteq X$.

Es ist $Y = (Y, (\leqslant) \cap (Y \times Y))$ ein Poset.

Dies wird in der Regel kommentarlos verwendet. Z.B. kann man von einem minimalen Element von Y sprechen.

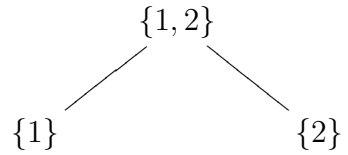
Beispiel 251

(1) Sei M eine Menge.

Die Potenzmenge $\mathrm{Pot}(M) = \{\, N : N \subseteq M \,\}$, zusammen mit $(\subseteq)$, ist ein Poset.

Jede Teilmenge von $\mathrm{Pot}(M)$ ist ein Poset.

(2) Wir betrachten das Poset $X := \{\{1\}, \{2\}, \{1,2\}\} \subseteq \mathrm{Pot}(\{1,2\})$.



Es hat X die minimalen Elemente $\{1\}$ und $\{2\}$. Es hat X kein initiales Element.

Es hat X das maximale Element $\{1,2\}$. Es hat X das terminale Element $\{1,2\}$.

(3) Es ist $\mathbb{Z}$ linear geordnet. Es hat $\mathbb{Z}$ weder ein minimales noch ein maximales Element. Es hat $\mathbb{Z}_{\geqslant 0}$ das initiale Element 0.

Definition 252 Sei $X = (X, \leqslant)$ ein Poset. Sei $K \subseteq X$.

Es heißt K eine *Kette* in X, wenn $K = (K, (\leqslant) \cap (K \times K))$ linear geordnet ist.

Eine *obere Schranke* einer Kette K ist ein Element $s \in X$ mit $k \leqslant s$ für $k \in K$.

Beispiel 253 Wir setzen Beispiel 251.(2) fort. Es ist $X = \{\{1\}, \{2\}, \{1,2\}\}$.

Schreibe $x_1 := \{1\}$, $x_2 := \{2\}$ und $x_{1,2} := \{1,2\}$.

Die Ketten in X sind:

$$\emptyset\,, \quad \{x_1\}\,, \quad \{x_2\}\,, \quad \{x_{1,2}\}\,, \quad \{x_1, x_{1,2}\}\,, \quad \{x_2, x_{1,2}\}\,.$$

Lemma 254 (Kuratowski-Zorn) *Sei $X = (X, \leqslant)$ ein Poset.*

Es habe in X jede Kette eine obere Schranke.

Sei $x \in X$. Dann gibt es ein maximales Element $m \in X$ mit $x \leqslant m$.

Beweis. Siehe Lemma A.13 im Anhang §A.3. ▫

Beispiel 255 Sei X ein nichtleeres endliches Poset.

Dann hat in X jede nichtleere Kette ein terminales Element:

Annahme, nicht. Sei $K \subseteq X$ eine Kette ohne terminales Element. Wähle $k_1 \in K$.

Es ist k_1 nicht terminal. Wähle $k_2 \in K$, für welches nicht $k_2 \leqslant k_1$ ist. Da K eine Kette ist, folgt $k_1 < k_2$.

Es ist k_2 nicht terminal. Wähle $k_3 \in K$, für welches nicht $k_3 \leqslant k_2$ ist. Da K eine Kette ist, folgt $k_2 < k_3$.

Usf.

Folglich ist K nicht endlich. Daher ist X nicht endlich. Wir haben einen *Widerspruch.*

Es hat in X jede Kette K eine obere Schranke: Falls $K = \emptyset$, so ist jedes Element von X eine obere Schranke von K. Falls $K \neq \emptyset$, so ist das terminale Element von K eine obere Schranke von K.

Dank des Lemmas von Kuratowski-Zorn 254 gibt es ein nun für jedes $x \in X$ ein maximales Element $m \in X$ mit $x \leqslant m$. Jedes Element von X liegt unter wenigstens einem maximalen Element.

3.8.3 Maximale Ideale

Lemma 256 *Sei R ein kommutativer Ring.*

Sei $I \lhd R$ ein Ideal ungleich R.

Dann gibt es ein maximales Ideal M in R mit $I \subseteq M \lhd R$.

Beweis. Sei $X := \{ J : J \lhd R \}$ die Menge der Ideale von R, die ungleich R sind.

Es ist $X = (X, \subseteq)$ ein Poset.

Wir *behaupten,* daß in X jede Kette K eine obere Schranke hat.

Ist $K = \emptyset$, dann ist I eine obere Schranke von K.

Sei nun $K \neq \emptyset$. Wir behaupten genauer, daß $\tilde{J} := \bigcup K$ eine obere Schranke von K ist.

Es ist 0 in einem Element von K enthalten, und damit auch in $\tilde{J}$.

Wir zeigen $\tilde{J} \overset{!}{\lhd} R$. Seien dazu $x, x' \in \tilde{J}$ und $r, r' \in R$ gegeben. Wir haben $rx + r'x' \overset{!}{\in} \tilde{J}$ nachzuweisen. Es gibt nun $J \in K$ mit $x \in J$ und $J' \in K$ mit $x' \in J'$. O.E. ist $J \subseteq J'$. Also sind $x, x' \in J'$. Da J' ein Ideal in R ist, folgt hieraus $rx + r'x' \in J' \subseteq \tilde{J}$.

Wir zeigen $\tilde{J} \overset{!}{\neq} R$. Dazu zeigen wir $1 \overset{!}{\notin} \tilde{J}$. *Annahme,* $1 \in \tilde{J}$. Dann gibt es ein $J \in K$ mit $1 \in J$. Da J ein Ideal in R ist, folgt hieraus $J = R$. Aber wegen $J \in K \subseteq X$ ist $J \neq R$. Wir haben einen *Widerspruch.*

Dank des Lemmas von Kuratowski-Zorn gibt es nun ein maximales Element $M \in X$ mit $I \subseteq M$; vgl. Lemma 254. Es ist M dann ein maximales Ideal in R; vgl. Definition 22. ▫

3.8.4 Große Polynomringe

Sei K ein Körper.

Sei I eine Menge, nicht notwendig endlich.

Definition 257 Sei T_i eine formale Variable für $i \in I$.

Wir kürzen auch $T := (T_i)_{i \in I}$ ab.

Sei ein *Monom* in $T = (T_i)_{i \in I}$ ein Produkt der Form

$$T_{i_1}^{e_1} \cdot T_{i_2}^{e_2} \cdot \ldots \cdot T_{i_k}^{e_k} \ ,$$

wobei $k \in \mathbb{Z}_{\geqslant 0}$, $i_j \in I$ und $e_j \in \mathbb{Z}_{\geqslant 0}$ für $j \in [1, k]$ seien, mit $i_j \neq i_{j'}$ für $j, j' \in [1, k]$ mit $j \neq j'$.

Insbesondere haben wir das Monom 1, welches aus der Wahl $k = 0$ resultiert.

Sei ein *Polynom* $f(T)$ in $T = (T_i)_{i \in I}$ mit Koeffizienten in K eine formale endliche K-Linearkombination von Monomen in $T = (T_i)_{i \in I}$.

Es ist also

$$f(T) \;=\; \sum_{t\in[1,\ell]} s_t \cdot T_{i_{t,1}}^{e_{t,1}} \cdot T_{i_{t,2}}^{e_{t,2}} \cdot \ldots \cdot T_{i_{t,k_t}}^{e_{t,k_t}}$$

für ein $\ell \in \mathbb{Z}_{\geqslant 0}$, und, für $t \in [1,\ell]$, gewisse $s_t \in K$, $k_t \in \mathbb{Z}_{\geqslant 0}$ und $i_{t,j} \in I$, $e_{t,j} \in \mathbb{Z}_{\geqslant 0}$ für $j \in [1,k_t]$.

Wir können Polynome addieren und multiplizieren.

Sei

$$\begin{array}{rcl} K[T] & = & K[T_i \,:\, i \in I] \\ & := & \{\, f(T) \,:\, \text{es ist } f(T) \text{ ein Polynom in } T=(T_i)_{i\in I} \text{ mit Koeffizienten in } K \,\} \end{array}$$

der *Polynomring* in $T = (T_i)_{i\in I}$ mit Koeffizienten in K.

Die Eigenschaften (Ring 1–7) von Definition 1 sind erfüllt.

Wir haben den injektiven Ringmorphismus $K \to K[T] : s \mapsto s \cdot 1$. Entlang diesem identifizieren wir und erhalten so den Teilring $K \subseteq K[T]$.

Beispiel 258 Sei $I := \mathbb{Z}_{\geqslant 1}$.

Es sind

$$f(T) := T_2T_3T_5^2 + \tfrac{1}{2}T_1T_3T_5\,,\;\; g(T) := T_1T_3T_5 - T_2 \;\in\; \mathbb{Q}[T] = \mathbb{Q}[T_i \,:\, i\in I]\,.$$

Es wird

$$\begin{array}{rcl} f(T)+g(T) & = & T_2T_3T_5^2 + \tfrac{3}{2}T_1T_3T_5 - T_2 \\ f(T)\cdot g(T) & = & T_1T_2T_3^2T_5^3 + \tfrac{1}{2}T_1^2T_3^2T_5^2 - T_2^2T_3T_5^2 - \tfrac{1}{2}T_1T_2T_3T_5\,. \end{array}$$

Bemerkung 259 Sei R ein kommutativer Ring, welcher $K \subseteq R$ als Teilring enthält.

Sei für $i \in I$ ein Element $r_i \in R$ gegeben. Diese bilden das Tupel $r := (r_i)_{i\in I}$.

Dann gibt es genau einen Ringmorphismus $\varphi : K[T] \to R$ mit $\varphi(T_i) = r_i$ für $i \in I$ und mit $\varphi|_K^K = \mathrm{id}_K$.

Dieser ist gegeben durch

$$\begin{array}{rcl} K[T] & \stackrel{\varphi}{\to} & R \\ f(T) \;=\; \sum_{t\in[1,\ell]} s_t \cdot T_{i_{t,1}}^{e_{t,1}} \cdot T_{i_{t,2}}^{e_{t,2}} \cdot \ldots \cdot T_{i_{t,k_t}}^{e_{t,k_t}} & \mapsto & f(r) \;:=\; \sum_{t\in[1,\ell]} s_t \cdot r_{i_{t,1}}^{e_{t,1}} \cdot r_{i_{t,2}}^{e_{t,2}} \cdot \ldots \cdot r_{i_{t,k_t}}^{e_{t,k_t}} \end{array}$$

Beispiel 260 Wir setzen Beispiel 258 fort.

Sei $R = \mathbb{Q}(\sqrt{2})$. Sei $r_i := \sqrt{2}$ für $i \in I = \mathbb{Z}_{\geqslant 1}$, unabhängig von i.

Der zugehörige Ringmorphismus φ aus Bemerkung 259 bildet z.B. wie folgt ab.

$$\begin{array}{rcl} \mathbb{Q}[T] & \stackrel{\varphi}{\to} & \mathbb{Q}(\sqrt{2}) \\ T_2T_3T_5^2 + \tfrac{1}{2}T_1T_3T_5 & \mapsto & \sqrt{2}\cdot\sqrt{2}\cdot\sqrt{2}^2 + \tfrac{1}{2}\sqrt{2}\cdot\sqrt{2}\cdot\sqrt{2} \;=\; 4+\sqrt{2} \end{array}$$

3.8.5 Konstruktion des algebraischen Abschlusses

Sei K ein Körper.

Lemma 261 *Es gibt eine Körpererweiterung $L|K$ mit der Eigenschaft, daß es für jedes irreduzible normierte Polynom $f(X) \in K[X]$ ein $y \in L$ gibt mit $f(y) = 0$.*

Kurz, jedes irreduzible normierte Polynom in $K[X]$ hat eine Nullstelle in L.

Beweis. Wir indizieren die Menge der irreduziblen normierten Polynome in $K[X]$ mit einer geeignet gewählten Menge I. Es soll also

$$\{\, f_i(X) \,:\, i \in I \,\} \;=\; \{\, g(X) \in K[X] \,:\, \text{es ist } g(X) \text{ normiert und irreduzibel} \,\}$$

sein, sowie für $i,\, j \,\in\, I$ mit $i \neq j$ auch $f_i(X) \neq f_j(X)$. ([9])

Sei $T = (T_i)_{i\in I}$. Wir betrachten den Polynomring $K[T] = K[T_i \,:\, i \in I]$.

Sei $N \subseteq K[T]$ die Teilmenge der Polynome in $T = (T_i)_{i\in I}$ der Form

$$u_1(T) \cdot f_{i_1}(T_{i_1}) + u_2(T) \cdot f_{i_2}(T_{i_2}) + \ldots + u_k(T) \cdot f_{i_k}(T_{i_k}) \;,$$

wobei $k \in \mathbb{Z}_{\geqslant 0}$, $u_j(T) \in K[T]$ und $i_j \in I$ für $j \in [1, k]$.

Es ist $N \trianglelefteqslant K[T]$.

Wir *behaupten* $N \overset{!}{\lhd} K[T]$. Dazu behaupten wir $1 \overset{!}{\notin} N$. *Annahme*, es ist $1 \in N$. Dann gibt es $k \in \mathbb{Z}_{\geqslant 0}$, $u_j(T) \in K[T]$ und $i_j \in I$ für $j \in [1, k]$ derart, daß

$$(*) \qquad u_1(T) \cdot f_{i_1}(T_{i_1}) + u_2(T) \cdot f_{i_2}(T_{i_2}) + \ldots + u_k(T) \cdot f_{i_k}(T_{i_k}) \;=\; 1$$

ist.

Sei $K_0 := K$.

Sei $K_1 := K(b_1)$ mit $\mu_{b_1,K_0}(X) = f_{i_1}(X)$; vgl. Lemma 195.

Es ist $f_{i_2}(X) \in K[X] \subseteq K_1[X]$. Wir wählen einen normierten irreduziblen Teiler $\check{f}_{i_2}(X) \in K_1[X]$ von $f_{i_2}(X)$. Sei $K_2 := K_1(b_2)$ mit $\mu_{b_2,K_1}(X) = \check{f}_{i_2}(X)$; vgl. Lemma 195.

Es ist $f_{i_3}(X) \in K[X] \subseteq K_2[X]$. Wir wählen einen normierten irreduziblen Teiler $\check{f}_{i_3}(X) \in K_2[X]$ von $f_{i_3}(X)$. Sei $K_3 := K_2(b_3)$ mit $\mu_{b_3,K_2}(X) = \check{f}_{i_3}(X)$; vgl. Lemma 195.

Usf.

Wir erhalten eine Körpererweiterung $\tilde{K} := K_k = K(b_1)(b_2)\ldots(b_k) \,|\, K$.

Sei $j \in [1, k]$. Es ist $\check{f}_{i_j}(X) \in K_{j-1}[X] \subseteq \tilde{K}[X]$ ein Teiler von $f_{i_j}(X) \in K[X] \subseteq \tilde{K}[X]$. Es ist $\check{f}_{i_j}(b_j) = 0$. Also ist auch $f_{i_j}(b_j) = 0$.

[9] Man kann z.B. als I die Menge eben dieser Polynome wählen. Die Wahl der Indexmenge I ist unwesentlich und dient nur der Schreibvereinfachung.

Wir setzen $r_{i_j} := b_j$ für $j \in [1,k]$. Wir setzen $r_i := 0$ für $i \in I \smallsetminus \{\, i_j \,:\, j \in [1,k] \,\}$.

Wir bilden das Tupel $r := (r_i)_{i \in I}$.

Wir haben den Ringmorphismus $\varphi : K[T] \to \tilde{K} : h(T) \mapsto h(r)$; vgl. Bemerkung 259.

Es schickt φ das Element 1 auf 1.

Es schickt φ das Element $u_1(T) \cdot f_{i_1}(T_{i_1}) + u_2(T) \cdot f_{i_2}(T_{i_2}) + \ldots + u_k(T) \cdot f_{i_k}(T_{i_k})$ auf

$$\begin{aligned} & u_1(r) \cdot f_{i_1}(r_{i_1}) + u_2(r) \cdot f_{i_2}(r_{i_2}) + \ldots + u_k(r) \cdot f_{i_k}(r_{i_k}) \\ = \; & u_1(r) \cdot f_{i_1}(b_1) + u_2(r) \cdot f_{i_2}(b_2) + \ldots + u_k(r) \cdot f_{i_k}(b_k) \\ = \; & 0 \,. \end{aligned}$$

Wegen $(*)$ sollte φ diese beiden Elemente aber auf dasselbe Element abbilden. Wir haben einen *Widerspruch*. Dies zeigt die *Behauptung*.

Sei $M \lhd K[T]$ ein maximales Ideal mit $N \subseteq M \lhd K[T]$, existent dank Lemma 256 unter Verwendung der vorstehenden Behauptung.

Sei $L := K[T]/M$. Es ist L ein Körper, der K als Teilkörper enthält; vgl. Lemma 23.

Sei $i \in I$. Wir haben zu zeigen, daß es ein $y \in L$ gibt mit $f_i(y) \stackrel{!}{=} 0$.

Wir setzen dazu $y := T_i + M$. Es wird $f_i(y) = f_i(T_i + M) = f_i(T_i) + M$. Aber es ist $f_i(T_i) \in N \subseteq M$. Also ist $f_i(T_i) + M = 0 + M = 0$ in L. ▫

Lemma 262 *Es gibt eine Körpererweiterung $L|K$ mit der Eigenschaft, daß L algebraisch abgeschlossen ist.*

Beweis. Sei $K_0 := K$.

Sei $K_1|K_0$ so gewählt, daß jedes irreduzible normierte Polynom in $K_0[X]$ eine Nullstelle in K_1 hat; vgl. Lemma 261.

Sei $K_2|K_1$ so gewählt, daß jedes irreduzible normierte Polynom in $K_1[X]$ eine Nullstelle in K_2 hat; vgl. Lemma 261.

Sei $K_3|K_2$ so gewählt, daß jedes irreduzible normierte Polynom in $K_2[X]$ eine Nullstelle in K_3 hat; vgl. Lemma 261.

Usf.

Sei $L := \bigcup_{i \geqslant 0} K_i$.

Für $x,\, y \in L$ definieren wir die Addition wie folgt. Es gibt ein $i \geqslant 0$ mit $x,\, y \in K_i$. Dort bilden wir $x + y \in K_i \subseteq L$. Diese Summe ist dann unabhängig von der Wahl von i.

Für $x,\, y \in L$ definieren wir die Multiplikation wie folgt. Es gibt ein $i \geqslant 0$ mit $x,\, y \in K_i$. Dort bilden wir $x \cdot y \in K_i \subseteq L$. Dieses Produkt ist dann unabhängig von der Wahl von i.

Es ist $0 \in K_0 \subseteq L$ mit $0 + x = x$ für $x \in L$.

Es ist $1 \in K_0 \subseteq L$ mit $1 \cdot x = x$ für $x \in L$.

Die Eigenschaften (Ring 1–7) von Definition 1 sind erfüllt für L. Also ist L ein Ring. Es ist zudem L ein kommutativer Ring.

Für $x \in L^\times$ ist $x \in K_i^\times$ für ein $i \geqslant 0$. Dort bilden wir x^{-1} und erhalten dort $x \cdot x^{-1} = 1$, was dann auch in L gilt.

Somit ist L ein Körper und $L|K$ eine Körpererweiterung.

Wir *behaupten,* daß L algebraisch abgeschlossen ist. Sei $g(X) \in L[X]$ mit $\deg(g(X)) \geqslant 1$. Wir müssen ein $y \in L$ mit $g(y) = 0$ finden.

Sei $f(X) \in L[X]$ ein irreduzibler normierter Teiler von $g(X)$. Es gibt ein $i \geqslant 0$ derart, daß die Koeffizienten von $f(X)$ alle in K_i liegen und folglich $f(X) \in K_i[X]$ liegt. Nach Konstruktion gibt es ein $y \in K_{i+1} \subseteq L$ mit $f(y) = 0$.

Da $f(X)$ in $L[X]$ ein Teiler von $g(X)$ ist, folgt, daß auch $g(y) = 0$ ist. ▫

Bemerkung 263 *Sei $L|K$ eine Körpererweiterung.*

Sei $n \geqslant 1$ und seien Elemente $y_1, \ldots, y_n \in L$ gegeben.

Wir schreiben $K(y_1, \ldots, y_k) := K(y_1) \ldots (y_k) \subseteq L$ für $k \in [0, n]$.

Sei nun y_k algebraisch über $K(y_1, \ldots, y_{k-1})$ für $k \in [1, n]$.

Dann ist $K(y_1, \ldots, y_n)$ ein endlichdimensionaler K-Vektorraum. Ferner ist jedes Element von $K(y_1, \ldots, y_n)$ algebraisch über K.

Beweis. Da y_k als algebraisch über $K(y_1, \ldots, y_{k-1})$ vorausgesetzt wurde, ist $K(y_1, \ldots, y_{k-1})[y_k] = K(y_1, \ldots, y_{k-1})(y_k)$ endlichdimensional über $K(y_1, \ldots, y_{k-1})$ für $k \in [1, n]$; vgl. Bemerkung 193.(2).

Somit ist $K(y_1, \ldots, y_n)$ endlichdimensional über K; vgl. Lemma 205.

Sei nun $w \in K(y_1, \ldots, y_n)$. Dann ist $K[w] \subseteq K(y_1, \ldots, y_n)$, also $K[w]$ endlichdimensional über K, also w algebraisch über K; vgl. Bemerkung 193.(2). ▫

Bemerkung 264 *Sei $L|K$ eine Körpererweiterung.*

Sei $A := \{ y \in L : y \text{ ist algebraisch über } K \}$.

(1) *Es ist A ein Zwischenkörper von K und L, d.h. $L|A|K$.*

(2) *Falls L algebraisch abgeschlossen ist, dann auch A.*

Beweis. Zu (1). Wir haben zu zeigen, daß A ein Teilkörper von L ist, der K enthält.

Es ist $K \subseteq A$, also auch $1 \in A$.

Seien $y, z \in A$. Wir haben zu zeigen, daß $y - z$, $y \cdot z$ und, falls $y \neq 0$ ist, auch y^{-1} wieder in A liegen.

Es ist y algebraisch über K. Da ferner z algebraisch ist über K, ist z auch algebraisch über $K(y)$. Mit Bemerkung 263 folgt $K(y,z) \subseteq A$.

Nun sind die genannten Elemente $y - z$, $y \cdot z$ und, falls $y \neq 0$ ist, auch y^{-1} alle in $K(y,z) \subseteq A$ enthalten.

Zu (2). Sei $f(X) = \sum_{i\in[0,n]} a_i X^i \in A[X]$ mit $\deg(f(X)) = n \geqslant 1$. Wir haben zu zeigen, daß $f(X)$ eine Nullstelle in A besitzt; vgl. Definition 241.

O.E. ist $f(X)$ normiert, also $a_n = 1$.

Da L algebraisch abgeschlossen ist, gibt es ein $y \in L$ mit $f(y) = 0$. Es genügt, $y \overset{!}{\in} A$ zu zeigen.

Es ist a_0 algebraisch über K.

Es ist a_1 algebraisch über K, also auch über $K(a_0)$.

Es ist a_2 algebraisch über K, also auch über $K(a_0, a_1)$.

Usf.

Es ist schließlich a_{n-1} algebraisch über K, also auch über $K(a_0, a_1, \ldots, a_{n-2})$.

Nun ist $f(X) \in K(a_0, a_1, \ldots, a_{n-1})[X]$. Wegen $f(y) = 0$ ist also y algebraisch über $K(a_0, a_1, \ldots, a_{n-1})$.

Dank Bemerkung 263 ist somit $K(a_0, a_1, \ldots, a_{n-1}, y) \subseteq A$. Insbesondere ist $y \in A$. ▫

Beispiel 265 Sei $A := \{\, z \in \mathbb{C} : \text{ es ist } z \text{ algebraisch über } \mathbb{Q} \,\} \subseteq \mathbb{C}$. Dann ist $\mathbb{C}|A|\mathbb{Q}$; vgl. Bemerkung 264.(1). Es ist A algebraisch abgeschlossen; vgl. Bemerkung 264.(2).

Also ist $A|\mathbb{Q}$ ein algebraischer Abschluß.

Z.B. liegen $\mathrm{i}\sqrt{5}$ und $\zeta_{11} + \zeta_7\sqrt{2}$ in A.

Satz 266 *Gegeben ist ein Körper K.*

Es existiert ein algebraischer Abschluß $A|K$.

Beweis. Nach Lemma 262 gibt es eine Körpererweiterung $L|K$ mit der Eigenschaft, daß L algebraisch abgeschlossen ist.

Wir bilden den Zwischenkörper A der über K algebraischen Elemente in L; vgl. Bemerkung 264.(1).

Dieser ist algebraisch abgeschlossen; vgl. Bemerkung 264.(2).

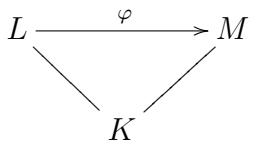
Also ist $A|K$ ein algebraischer Abschluß; vgl. Definition 244. ▫

Lemma 267

Sei $L|K$ eine Körpererweiterung, für welche jedes $y \in L$ algebraisch ist über K.

Sei $M|K$ eine Körpererweiterung, für welche M algebraisch abgeschlossen ist.

Dann gibt es einen Körpermorphismus φ von L nach M über K ; vgl. Definition 198.(2).



Wir erinnern daran, daß Körpermorphismen injektiv, aber nicht notwendig surjektiv sind; vgl. Definition 198.(1).

Beweis des Lemmas. Wir betrachten die Menge

$$\mathcal{A} \;:=\; \{\, (\psi : Z \to M) \;:\; \text{es ist } L|Z|K \text{ und } \psi \text{ ein Körpermorphismus über } K \,\}\,.$$

So etwa ist die Einbettungsabbildung $(\iota : K \to M)$ in $\mathcal{A}$ enthalten.

Wir definieren eine Teilordnung $(\leqslant)$ auf $\mathcal{A}$ wie folgt.

Seien $(\psi : Z \to M), (\tilde{\psi} : \tilde{Z} \to M) \in \mathcal{A}$. Sei $(\psi : Z \to M) \leqslant (\tilde{\psi} : \tilde{Z} \to M)$, falls $Z \subseteq \tilde{Z}$ und $\tilde{\psi}|_Z = \psi$ ist.

Es ist $(\leqslant)$ reflexiv.

Es ist $(\leqslant)$ identitiv, da für $(\psi : Z \to M), (\tilde{\psi} : \tilde{Z} \to M) \in \mathcal{A}$ mit

$$(\psi : Z \to M) \;\leqslant\; (\tilde{\psi} : \tilde{Z} \to M) \quad \text{und} \quad (\tilde{\psi} : \tilde{Z} \to M) \;\leqslant\; (\psi : Z \to M)$$

folgt, daß $Z = \tilde{Z}$ und dann auch $\psi = \tilde{\psi}$ ist.

Es ist $(\leqslant)$ transitiv, da für $(\psi : Z \to M), (\psi' : Z' \to M), (\psi'' : Z'' \to M) \in \mathcal{A}$ mit

$$(\psi : Z \to M) \;\leqslant\; (\psi' : Z' \to M) \quad \text{und} \quad (\psi' : Z' \to M) \;\leqslant\; (\psi'' : Z'' \to M)$$

folgt, daß $Z \subseteq Z' \subseteq Z''$ und also $Z \subseteq Z''$ ist, sowie daß $\psi''|_{Z'} = \psi'$ und $\psi'|_Z = \psi$ und also $\psi''|_Z = \psi''|_{Z'}|_Z = \psi'|_Z = \psi$ ist.

Sei $\mathcal{K}$ eine Kette in $\mathcal{A}$. Wir behaupten, daß $\mathcal{K}$ eine obere Schranke hat. O.E. ist $\mathcal{K} \neq \emptyset$.

Sei dazu $\hat{Z} := \bigcup_{(\psi : Z \to M) \in \mathcal{K}} Z$.

Wir *behaupten,* daß $\hat{Z}$ ein Zwischenkörper von $L|K$ ist.

Es ist $1 \in K \subseteq \hat{Z}$.

Für $y, z \in \hat{Z}$ können wir ein $(\psi : Z \to M) \in \mathcal{K}$ wählen mit $y, z \in Z$.

Es wird $y - z, y \cdot z \in Z \subseteq \hat{Z}$. Ist $y \neq 0$, dann wird auch $y^{-1} \in Z \subseteq \hat{Z}$.

Dies zeigt die *Behauptung.*

Sei nun $\hat{\psi} : \hat{Z} \to M$ für $y \in \hat{Z}$ erklärt durch $\hat{\psi}(y) := \psi(y)$, wobei $(\psi : Z \to M) \in \mathcal{K}$ gewählt wurde mit $y \in Z$. Dies ist von der Wahl von $(\psi : Z \to M)$ unabhängig, da

für Elemente $(\psi : Z \to M), (\tilde{\psi} : \tilde{Z} \to M) \in \mathcal{K}$ mit $y \in Z$ und $y \in \tilde{Z}$ sich o.E. $(\psi : Z \to M) \leqslant (\tilde{\psi} : \tilde{Z} \to M)$ ergibt und also $\tilde{\psi}(y) = (\tilde{\psi}|_Z)(y) = \psi(y)$ wird.

Wir *behaupten*, daß $\hat{\psi} : \hat{Z} \to M$ ein Körpermorphismus über K ist.

Es ist $\hat{\psi}(1) = \psi(1) = 1$, wobei ein $(\psi : Z \to M) \in \mathcal{K}$ gewählt wurde.

Es ist $\hat{\psi}(x) = \psi(x) = x$ für $x \in K$, wobei ein $(\psi : Z \to M) \in \mathcal{K}$ gewählt wurde; man beachte, daß ψ ein Körpermorphismus über K ist.

Seien $y, z \in \hat{Z}$. Wir wählen $(\psi : Z \to M) \in \mathcal{K}$ mit $y, z \in Z$. Dann ist $\hat{\psi}(y + z) = \psi(y + z) = \psi(y) + \psi(z) = \hat{\psi}(y) + \hat{\psi}(z)$ und $\hat{\psi}(y \cdot z) = \psi(y \cdot z) = \psi(y) \cdot \psi(z) = \hat{\psi}(y) \cdot \hat{\psi}(z)$.

Dies zeigt die *Behauptung*. Es ist also $(\hat{\psi} : \hat{Z} \to M) \in \mathcal{A}$.

Nach Konstruktion ist $(\psi : Z \to M) \leqslant (\hat{\psi} : \hat{Z} \to M)$ für $(\psi : Z \to M) \in \mathcal{K}$. Also ist $(\hat{\psi} : \hat{Z} \to M)$ eine obere Schranke für $\mathcal{K}$. Das zeigt die Behauptung.

Gemäß Lemma von Kuratowski-Zorn liegt die Inklusionsabbildung $(\iota : K \to M)$ in einem maximalen Element $(\psi : Z \to M)$ von $\mathcal{A}$; vgl. Lemma 254.

Wir schreiben $\tilde{Z} := \psi(Z) \subseteq M$. Es ist $\psi|^{\tilde{Z}} : Z \xrightarrow{\sim} \tilde{Z}$ ein Körperisomorphismus über K.

Wir müssen nur noch $Z \stackrel{!}{=} L$ zeigen.

Annahme, es ist $Z \subset L$. Wir wählen ein Element $y \in L \setminus Z$. Es ist y algebraisch über K, also auch algebraisch über Z. Wir schreiben $\mu(X) := \mu_{y,Z}(X) = \sum_{i \geqslant 0} a_i X^i \in Z[X]$.

Wir schreiben $\tilde{\mu}(X) := \sum_{i \geqslant 0} \psi(a_i) X^i \in \tilde{Z}[X]$. Sei $\tilde{y} \in M$ eine Nullstelle von $\tilde{\mu}(X)$, existent, da M algebraisch abgeschlossen ist.

Wir haben den Ringisomorphismus $Z[X] \xrightarrow{\sim} \tilde{Z}[X] : \sum_{i \geqslant 0} b_i X^i \mapsto \sum_{i \geqslant 0} \psi(b_i) X^i$.

Dieser liefert den Körperisomorphismus

$$Z[X]/(\mu(X)) \xrightarrow{\sim} \tilde{Z}[X]/(\tilde{\mu}(X)) : \sum_{i \geqslant 0} b_i X^i + (\mu(X)) \mapsto \sum_{i \geqslant 0} \psi(b_i) X^i + (\tilde{\mu}(X))$$

über K. Insgesamt haben folgende Körpermorphismen über K; vgl. Lemma 194.

$$\begin{array}{rcccccccc} Z(y) & \xrightarrow{\sim} & Z[X]/(\mu(X)) & \xrightarrow{\sim} & \tilde{Z}[X]/(\tilde{\mu}(X)) & \xrightarrow{\sim} & \tilde{Z}(\tilde{y}) & \to & M \\ y & \mapsto & X + (\mu(X)) & \mapsto & X + (\tilde{\mu}(X)) & \mapsto & \tilde{y} & \mapsto & \tilde{y} \\ Z \ni z & \mapsto & z + (\mu(X)) & \mapsto & \psi(z) + (\tilde{\mu}(X)) & \mapsto & \psi(z) & \mapsto & \psi(z)\,. \end{array}$$

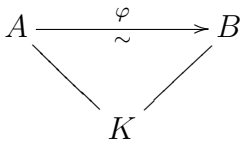
Diese liefern den zusammengesetzten Körpermorphismus $\gamma : Z(y) \to M$ über K, also $(\gamma : Z \to M) \in \mathcal{A}$. Es ist $\gamma|_Z = \psi$.

Da $Z \subset Z(y)$ ist, folgt $(\psi : Z \to M) < (\gamma : Z(y) \to M)$, im *Widerspruch* zur Maximalität von $(\psi : Z \to M)$. ▫

Satz 268 *Gegeben ist ein Körper K.*

Sei $A|K$ ein algebraischer Abschluß. Sei $B|K$ ein algebraischer Abschluß.

Dann gibt es einen Körperisomorphismus φ von A nach B über K ; vgl. Definition 198.(2).



Insbesondere ist $A \simeq B$.

Beweis. Nach Lemma 267 gibt es einen Körpermorphismus $\varphi : A \to B$ über K.

Es bleibt zu zeigen, daß φ surjektiv ist.

Wir schreiben $\tilde{A} := \varphi(A)$. Es ist $B|\tilde{A}|K$. Es ist $\varphi|^{\tilde{A}} : A \xrightarrow{\sim} \tilde{A}$ ein Isomorphismus über K.

Da A algebraisch abgeschlossen ist und da $A \simeq \tilde{A}$, ist auch $\tilde{A}$ algebraisch abgeschlossen.

Zu zeigen ist $\tilde{A} \stackrel{!}{=} B$.

Sei $y \in B$. Es ist y algebraisch über K. Dann ist y auch algebraisch über $\tilde{A}$. Das Minimalpolynom $\mu_{y,\tilde{A}}(X) \in \tilde{A}[X]$ ist irreduzibel; vgl. Lemma 194. Da $\tilde{A}$ algebraisch abgeschlossen ist, folgt $\deg(\mu_{y,\tilde{A}}(X)) = 1$; vgl. Bemerkung 242. Also ist $\mu_{y,\tilde{A}}(X) = X - y$. Somit ist $y \in \tilde{A}$. ▫

Für einen Körper K schreibt man manchmal auch $\bar{K}$ für einen irgendwie ausgewählten algebraischen Abschluß $\bar{K}|K$, gerne unter Berufung auf die Aussage von Satz 268.

3.9 Existenz und Eindeutigkeit endlicher Körper

Wir wissen von endlichen Körpern:

Ist p eine Primzahl, dann ist $\mathbb{F}_p := \mathbb{Z}/(p)$ ein Körper mit $|\mathbb{F}_p| = p$.

Ist weiter $m(X) \in \mathbb{F}_p[X]$ ein irreduzibles normiertes Polynom, dann ist $\mathbb{F}_p[X]/(m(X))$ ein Körper mit $|\mathbb{F}_p[X]/(m(X))| = p^{\deg(m(X))}$.

Wir haben in einem Beispiel auch abgekürzt und $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$ sowie darin $\alpha := X + (X^2 + X + 1)$ geschrieben. In $\mathbb{F}_4$ ist so $2 = 0$ und $\alpha^2 = \alpha + 1$.

Diese Konstruktion von $\mathbb{F}_p[X]/(m(X))$ hing daran, daß es uns gelang, ein irreduzibles normiertes Polynom $m(X)$ von gewünschtem Grad zu finden. Wir wollen nun unter anderem klären, daß das immer möglich ist.

Sei p eine Primzahl. Sei $A|\mathbb{F}_p$ ein algebraischer Abschluß; vgl. Satz 266.

Da $\mathrm{char}(A) = p$, haben wir den Frobenius-Endomorphismus $\mathrm{Fr} = \mathrm{Fr}_A : A \to A : y \mapsto y^p$; vgl. Beispiel 200.

Bemerkung 269 *Es ist* $\mathrm{Fr} : A \to A : y \mapsto y^p$ *ein Automorphismus.*

Beweis. Zu zeigen ist die Surjektivität. Sei $z \in A$. Das normierte Polynom $X^p - z \in A[X]$ von Grad $p \geqslant 1$ hat im algebraisch abgeschlossenen Körper A eine Nullstelle y. Es ist also $y^p - z = 0$. In anderen Worten, es ist $\mathrm{Fr}(y) = y^p = z$. ▫

Lemma 270 *Sei $n \geqslant 1$.*

Sei $K := \{\, y \in A : \mathrm{Fr}^n(y) = y \,\}$.

Dann ist $A|K|\mathbb{F}_p$ mit $|K| = p^n$, also mit $[K : \mathbb{F}_p] = n$.

Insbesondere existiert ein Körper mit p^n Elementen.

In $K[X]$ zerfällt das Polynom $X^{p^n} - X$ in p^n paarweise verschiedene normierte Faktoren von Grad 1.

Wir schreiben auch $\mathbb{F}_{p^n} := K$; vgl. auch Lemma 273 unten.

Beweis. Sei $f(X) := X^{p^n} - X \in \mathbb{F}_p[X]$.

Es ist $f'(X) = p^n X^{p^n-1} - 1 = -1$. Also ist $\mathrm{ggT}(f(X), f'(X)) = 1$. Somit ist $f(X)$ in $A[X]$ quadratfrei; vgl. Lemma 227.(1). Da A algebraisch abgeschlossen ist, erhalten wir

$$f(X) \;=\; (X - y_1) \cdot \ldots \cdot (X - y_{p^n})$$

mit $y_1, \ldots, y_{p^n} \in A$, wobei $y_i \neq y_j$ für $i, j \in [1, p^n]$ mit $i \neq j$. Es ist

$$\{y_1, \ldots, y_{p^n}\} \;=\; \{\, y \in A : f(y) = 0 \,\} \;=\; \{\, y \in A : \mathrm{Fr}^n(y) = y \,\} \;=\; K\,.$$

Wir haben eben $|K| = p^n$ gesehen.

Es ist $\mathbb{F}_p = \{\, x \in A : x^p = x \,\}$. Aus $x^p = x$ folgt $x^{p^n} = x$. Folglich ist $\mathbb{F}_p \subseteq K$.

Es ist $K \subseteq A$ ein Teilkörper. Denn zum einen ist $1 \in K$. Ferner ist für $y, z \in K$ auch $\mathrm{Fr}^n(y - z) = \mathrm{Fr}^n(y) - \mathrm{Fr}^n(z) = y - z$ und $\mathrm{Fr}^n(y \cdot z) = \mathrm{Fr}^n(y) \cdot \mathrm{Fr}^n(z) = y \cdot z$ und somit $y - z, y \cdot z \in K$. Schließlich ist für $y \in K^\times$ auch $\mathrm{Fr}^n(y^{-1}) = \mathrm{Fr}^n(y)^{-1} = y^{-1}$ und somit $y^{-1} \in K$.

Im Ergebnis ist also $A|K|\mathbb{F}_p$ mit $|K| = p^n$. Ferner ist

$$f(X) \;=\; (X - y_1) \cdot \ldots \cdot (X - y_{p^n})$$

eine Zerlegung in Faktoren in $K[X]$.

Da K zugleich ein $\mathbb{F}_p$-Vektorraum mit $p^{[K:\mathbb{F}_p]}$ Elementen ist, folgt schließlich $n = [K : \mathbb{F}_p]$. ▫

Korollar 271 *Sei $n \geqslant 1$.*

Es gibt ein irreduzibles normiertes Polynom $m(X) \in \mathbb{F}_p[X]$ von Grad $\deg(m(X)) = n$.

Beweis. Sei $K|\mathbb{F}_p$ eine Körpererweiterung mit $|K| = p^n$; vgl. Lemma 270.

Es ist $\mathrm{U}(K)$ eine zyklische Gruppe; vgl. Lemma 218. Sei $y \in \mathrm{U}(K) = K^\times$ mit $\langle y \rangle = \mathrm{U}(K)$ gewählt.

Dann ist auch $K = \mathbb{F}_p(y)$. In der Tat ist jedes Element von $K^\times$ sogar eine Potenz von y.

Es ist $\mu_{y,K}(X) \in \mathbb{F}_p[X]$ irreduzibel und normiert, von Grad $\deg(\mu_{y,K}(X)) = [K : \mathbb{F}_p] = n$; vgl. Lemma 194. ▫

Beispiel 272 Im allgemeinen gibt es in $\mathbb{F}_p[X]$ zu einem gegebenen Grad mehrere irreduzible normierte Polynome.

Z.B. erhalten wir in $\mathbb{F}_2[X]$ folgende Liste irreduzibler normierter Polynome von Grad $\leqslant 5$.

Grad	Irreduzible normierte Polynome
1	X, $X+1$
2	X^2+X+1
3	X^3+X+1, X^3+X^2+1
4	X^4+X+1, X^4+X^3+1, $X^4+X^3+X^2+X+1$
5	X^5+X^3+1, X^5+X^2+1, $X^5+X^4+X^3+X^2+1$, $X^5+X^4+X^3+X+1$, $X^5+X^4+X^2+X+1$, $X^5+X^3+X^2+X+1$

Lemma 273 *Sei $n \geqslant 1$. Sei L ein Körper mit $|L| = p^n$.*

Dann ist L isomorph zu $\mathbb{F}_{p^n} = \{\, y \in A : \mathrm{Fr}^n(y) = y \,\}$; vgl. Lemma 270.

Insbesondere sind zwei Körper mit p^n Elementen zueinander isomorph.

> Es ist also im wesentlichen egal, welches irreduzible normierte Polynom von Grad n in $\mathbb{F}_p[X]$ wir zur Konstruktion eines Körpers L mit $|L| = p^n$ verwenden.

Beweis. Sei $q := \mathrm{char}(L)$. Dann ist $\mathbb{Z}/(q)$ ein Teilring von L; vgl. Beispiel 32. Als Teilring eines Körpers ist $\mathbb{Z}/(q)$ ein Integritätsbereich. Für $x \in (\mathbb{Z}/(q))^\times$ ist somit die Abbildung $\mathbb{Z}/(q) \to \mathbb{Z}/(q) : y \mapsto xy$ injektiv, mithin bijektiv. Also gibt es ein $y \in (\mathbb{Z}/(q))^\times$ mit $xy = 1$. Also ist $\mathbb{Z}/(q)$ ein Körper. Also ist $(q) \lhd \mathbb{Z}$ maximal. Also ist q eine Primzahl und $\mathbb{Z}/(q) = \mathbb{F}_q$. Also ist $p^n = |L| = q^{[L:\mathbb{F}_q]}$. Also ist $p = q$. Also ist $L|\mathbb{F}_p$.

Wir haben einen Körpermorphismus $\varphi : L \to A$ über $\mathbb{F}_p$; vgl. Lemma 267. Wir schreiben $\tilde{L} := \varphi(L)$. Da φ injektiv ist, ist $\varphi|^{\tilde{L}} : L \xrightarrow{\sim} \tilde{L}$ ein Körperisomorphismus; vgl. Definition 198.(1).

Es bleibt $\tilde{L} \stackrel{!}{=} \mathbb{F}_{p^n} = \{\, y \in A : \mathrm{Fr}^n(y) = y \,\} = \{\, y \in A : y^{p^n} = y \,\}$ zu zeigen.

Da $|\tilde{L}| = |L| = p^n = |\mathbb{F}_{p^n}|$ ist, genügt es, $\tilde{L} \stackrel{!}{\subseteq} \mathbb{F}_{p^n}$ zu zeigen.

Sei $y \in \tilde{L}^\times$. Wir haben $y \stackrel{!}{\in} \mathbb{F}_{p^n}$ zu zeigen. Wir haben also $y^{p^n} \stackrel{!}{=} y$ zu zeigen. Wir haben also $y^{p^n-1} \stackrel{!}{=} 1$ zu zeigen. Aber $y \in \tilde{L}^\times = \mathrm{U}(\tilde{L})$, und $\mathrm{U}(\tilde{L})$ ist eine Gruppe von Ordnung $|\mathrm{U}(\tilde{L})| = p^n - 1$. Also ist $y^{p^n-1} = 1$; vgl. Korollar 98. ▫

Lemma 274 *Sei $n \in \mathbb{Z}_{\geqslant 1}$. Seien K und L Körper mit $|K| = |L| = p^n$ Elementen.*

(1) *Sei $a \in K$ mit $K = \mathbb{F}_p(a)$. Es gibt ein $b \in L$ mit*

$$\mu_{b,\mathbb{F}_p}(X) = \mu_{a,\mathbb{F}_p}(X) \ .$$

(2) *Sei $f(X) \in \mathbb{F}_p[X]$ normiert und irreduzibel von Grad n. Dann gibt es ein $b \in L$ mit*

$$\mu_{b,\mathbb{F}_p}(X) = f(X) \ .$$

(3) *Es ist*

$$X^{p^n} - X = \prod_{\substack{f(X) \in \mathbb{F}_p[X] \\ \text{normiert und irreduzibel, mit} \\ \deg(f(X)) \,|\, n}} f(X) \ .$$

Beweis.

Zu (1). Nach Lemma 273 gibt es einen Körperisomorphismus $\alpha : K \xrightarrow{\sim} L$. Da $\alpha(\lambda \cdot a^k) = \lambda(\alpha(a))^k$ für $k \in [0, n]$ und $\lambda \in \mathbb{F}_p$ ist und da α sich mit Summen verträgt, ist $\alpha(a) \in L$ eine Nullstelle des Minimalpolynoms $\mu_{a,\mathbb{F}_p}(X)$. Da $\mu_{a,\mathbb{F}_p}(X) \in \mathbb{F}_p[X]$ normiert und irreduzibel ist, folgt

$$\mu_{\alpha(a),\mathbb{F}_p}(X) \ = \ \mu_{a,\mathbb{F}_p}(X) \ .$$

vgl. Bemerkung 196.$(1 \Leftrightarrow 2)$. Wir können also $b = \alpha(a) \in L$ wählen.

Zu (2). Nach Lemmas 195, 194 ist $K := \mathbb{F}_p[X]/(f(X))$ ein Körpererweiterung von $\mathbb{F}_p$, mit $a := X + (f(X))$ ist $K = \mathbb{F}_p(a)$, es ist $f(X) = \mu_{a,\mathbb{F}_p}(X)$ und es ist $[K : \mathbb{F}_p] = n$, also $|K| = p^n$. Nun folgt die Aussage mit (1).

Zu (3). Es ist $(X^{p^n} - X)' = p^n X^{p^n - 1} - 1 = -1$ und daher

$$\mathrm{ggT}(X^{p^n} - X, (X^{p^n} - X)') = \mathrm{ggT}(X^{p^n} - X, -1) = 1 \ .$$

Nach Lemma 227.(1) ist das Polynom $X^{p^n} - X$ quadratfrei in $\mathbb{F}_p[X]$.

Sei $f(X) \in \mathbb{F}_p[X]$ ein irreduzibles normiertes Polynom. Sei $d := \deg(f(X))$.

Es genügt zu zeigen, daß $f(X)$ das Polynom $X^{p^n} - X$ genau dann teilt, wenn d ein Teiler von n ist.

Zu $\Rightarrow$. Sei $f(X)$ ein Teiler von $X^{p^n} - X$.

Es zerfällt $X^{p^n} - X$ in $\mathbb{F}_{p^n}[X]$ in paarweise verschiedene normierte Faktoren von Grad 1; vgl. Lemma 270. Also zerfällt auch sein Teiler $f(X)$ in $\mathbb{F}_{p^n}[X]$ in paarweise verschiedene normierte Faktoren von Grad 1. Daher können wir eine Nullstelle $z \in \mathbb{F}_{p^n}$ von $f(X)$ wählen.

Mit $Z := \mathbb{F}_p(z)$ ist dann $\mathbb{F}_{p^n} | Z | \mathbb{F}_p$. Es ist $[Z : \mathbb{F}_p] = \deg(\mu_{z,\mathbb{F}_p}(X)) = \deg(f(X)) = d$; vgl. Bemerkung 196, Lemma 194. Damit wird

$$n \ = \ [\mathbb{F}_{p^n} : \mathbb{F}_p] \ = \ [\mathbb{F}_{p^n} : Z] \cdot [Z : \mathbb{F}_p] \ = \ [\mathbb{F}_{p^n} : Z] \cdot d$$

nach Lemma 205. Also ist d ein Teiler von n.

Zu $\Leftarrow$. Nach (2) gibt es ein Element $b \in \mathbb{F}_{p^d}$ mit $f(X) = \mu_{b,\mathbb{F}_p}(X)$ und $\mathbb{F}_p(b) = \mathbb{F}_{p^d}$.

Da b in $\mathbb{F}_{p^d}$ lieft, gilt $b^{p^d} = b$, also auch b. Da $f(X) = \mu_{b,\mathbb{F}_p}(X)$ ist und da $X^{p^d} - X$ in $\mathbb{F}_p[X]$ liegt und b als Nullstelle hat, ist $f(X)$ ein Teiler $X^{p^d} - X$; vgl. Lemma 194.

Da d ein Teiler von n ist, gibt es ein $k \in \mathbb{Z}$ mit $n = k \cdot d$. Es ist $p^d - 1$ ein Teiler von $p^n - 1$, da $p^n - 1 = (p^d)^k - 1 = (p^d - 1)\left(\sum_{i\in[0,k-1]} p^{id}\right)$ ist.

Wir wählen ein $c \in \mathrm{U}(\mathbb{F}_{p^n})$ mit $\mathrm{U}(\mathbb{F}_{p^n}) = \langle c\rangle$; vgl. Korollar 219. Es hat c also die Ordnung $|\langle c\rangle| = |\mathrm{U}(\mathbb{F}_{p^n})| = p^n - 1$.

Somit hat $a := c^{\frac{(p^n-1)}{(p^d-1)}}$ Ordnung $|\langle a\rangle| = p^d - 1$, und alle Elemente $x \in \langle a\rangle$ erfüllen $x^{p^d-1} = 1$. Folglich hat das Polynom $X^{p^d} - X$ genau p^d Nullstellen in $\mathbb{F}_{p^n}$, nämlich die Elemente von $\langle a\rangle$ und die 0. Insbesondere zerfällt $X^{p^d} - X$ in $\mathbb{F}_{p^n}[X]$ in paarweise verschiedene normierte Faktoren von Grad 1.

Die Nullstellen von $X^{p^n} - X$ in $\mathbb{F}_{p^n}$ sind gerade alle Elemente von $\mathbb{F}_{p^n}$; vgl. Lemma 270. Insbesondere ist jede Nullstelle von $X^{p^d} - X$ in $\mathbb{F}_{p^n}$ auch Nullstelle von $X^{p^n} - X$. Somit ist $X^{p^d} - X$ ein Teiler von $X^{p^n} - X$.

Insgesamt ist $f(X)$ somit ein Teiler von $X^{p^n} - X$. ▫

Anhang A

Anhang

A.1 Eine Bemerkung zur Distributivität

Man kann in Definition 1 das Axiom

(Ring 7) Für $r,\, r',\, s,\, s' \in R$ ist $(r + r') \cdot s = r \cdot s + r' \cdot s$ und $r \cdot (s + s') = r \cdot s + r \cdot s'$.

äquivalent ersetzen durch das Axiom

(Ring 7′) Für $r,\, r',\, s,\, s' \in R$ ist $(r + r') \cdot (s + s') = (r \cdot s + r' \cdot s) + (r \cdot s' + r' \cdot s')$.

Zu $(\text{Ring}\, 1, 2, 3, 4, 5, 6, 7) \Rightarrow (\text{Ring}\, 1, 2, 3, 4, 5, 6, 7')$.
Für $r,\, r',\, s,\, s' \in R$ wird

$$(r + r') \cdot (s + s') \overset{(\text{Ring}\, 7)}{=} (r + r') \cdot s + (r + r') \cdot s' \overset{(\text{Ring}\, 7)}{=} (r \cdot s + r' \cdot s) + (r \cdot s' + r' \cdot s') \,.$$

Zu $(\text{Ring}\, 1, 2, 3, 4, 5, 6, 7') \Rightarrow (\text{Ring}\, 1, 2, 3, 4, 5, 6, 7)$.
Wir schreiben $1 := 1_R$ und $0 := 0_R$.
Zunächst ist

$$\begin{aligned} 0 &\overset{(\text{Ring}\, 6)}{=} 1 \cdot 0 \\ &\overset{(\text{Ring}\, 3)}{=} (1 + 0) \cdot (0 + 0) \\ &\overset{(\text{Ring}\, 7')}{=} (1 \cdot 0 + 0 \cdot 0) + (1 \cdot 0 + 0 \cdot 0) \\ &\overset{(\text{Ring}\, 6)}{=} (0 + 0 \cdot 0) + (0 + 0 \cdot 0) \\ &\overset{(\text{Ring}\, 1, 3)}{=} 0 \cdot 0 + 0 \cdot 0 \,. \end{aligned}$$

Für $x \in R$ wird also

$$\begin{aligned} x \cdot 0 &\overset{(\text{Ring}\,3)}{=} (x+0)\cdot(0+0) \\ &\overset{(\text{Ring}\,7')}{=} (x\cdot 0 + 0\cdot 0) + (x\cdot 0 + 0\cdot 0) \\ &\overset{(\text{Ring}\,1,2)}{=} (x\cdot 0 + x\cdot 0) + (0\cdot 0 + 0\cdot 0) \\ &= (x\cdot 0 + x\cdot 0) + 0 \\ &\overset{(\text{Ring}\,3)}{=} x\cdot 0 + x\cdot 0\ , \end{aligned}$$

dank (Ring $4, 2, 3$) also $0 = x \cdot 0$.

Für r, r', $s \in R$ wird mithin

$$\begin{aligned} (r+r')\cdot s &\overset{(\text{Ring}\,3)}{=} (r+r')\cdot(s+0) \\ &\overset{(\text{Ring}\,7')}{=} (r\cdot s + r'\cdot s) + (r\cdot 0 + r'\cdot 0) \\ &= (r\cdot s + r'\cdot s) + (0+0) \\ &\overset{(\text{Ring}\,3)}{=} r\cdot s + r'\cdot s\ . \end{aligned}$$

Genauso folgt die andere Gleichung in (Ring 7).

> So sympathisch (Ring $1, 2, 3, 4, 5, 6, 7'$) auch aussieht, die Konsequenzen sind also etwas unangenehm. Denn die Eigenschaft (Ring 7) will man jedenfalls zur Verfügung haben, ob sie in der Liste der Axiome steht oder nicht.

A.2 Ein Beispiel zu Sylow

> Folgende Argumentationsweise kenne ich von Nora Krauß.

Sei G eine einfache Gruppe der Ordnung $|G| = 168 = 2^3 \cdot 3 \cdot 7$.

Wir wollen die Anzahl der 2-, 3- und 7-Sylowgruppen in G bestimmen. Wir verwenden dazu Satz 154 und Korollar 155, ohne laufend darauf zu verweisen.

Da G einfach ist, besitzt G nur die Normalteiler 1 und G. Also ist $|\operatorname{Syl}_p(G)| > 1$ für $p \in \{2, 3, 7\}$.

Es ist $|\operatorname{Syl}_2(G)|$ ein Teiler von $3 \cdot 7$. Somit ist $|\operatorname{Syl}_2(G)| \in \{3, 7, 21\}$.

Es ist $|\operatorname{Syl}_3(G)| \equiv_3 1$ und $|\operatorname{Syl}_3(G)|$ ein Teiler von $2^3 \cdot 7$. Somit ist $|\operatorname{Syl}_3(G)| \in \{4, 7, 28\}$.

Es ist $|\operatorname{Syl}_7(G)| \equiv_7 1$ und $|\operatorname{Syl}_7(G)|$ ein Teiler von $2^3 \cdot 3$. Somit ist $|\operatorname{Syl}_7(G)| \in \{8\}$.

Für eine p-Sylowgruppe P werden wir vom Normalisator $\mathrm{N}_G(P)$ Gebrauch machen, welcher in G eine Untergruppe von Index $|\operatorname{Syl}_p(G)|$ ist.

Behauptung 1. *In G gibt es keine Untergruppe U von Index k mit $2 \leqslant k \leqslant 6$. Insbesondere gibt es in G kein Element von Ordnung $\geqslant 28$.*

Angenommen doch. Es operiert G transitiv auf der G-Menge G/U mit $|G/U| \in [2,6]$.

Wir haben den Operationsmorphismus $\varphi : G \to \mathrm{S}_{G/U}$. Es ist $\mathrm{Kern}(\varphi) \lhd G$. Da G einfach ist, folgt $\mathrm{Kern}(\varphi) = 1$ und also $G \simeq \varphi(G)$.

Da $[G : U] = k$ ist, ist $\mathrm{S}_{G/U} \simeq \mathrm{S}_k$. Also ist G isomorph zu einer Untergruppe von S_k . Da wegen $k \leqslant 6$ die Ordnung $|G| = 168$ kein Teiler von $k!$ ist, ist dies nicht möglich. *Widerspruch.* Dies zeigt *Behauptung* 1.

Zwischenstand. Es ist

$$\begin{array}{rcl} |\operatorname{Syl}_2(G)| & \in & \{7, 21\} \\ |\operatorname{Syl}_3(G)| & \in & \{7, 28\} \\ |\operatorname{Syl}_7(G)| & = & 8 \ . \end{array}$$

Für $P_2 \in \operatorname{Syl}_2(G)$, $P_3 \in \operatorname{Syl}_3(G)$ und $P_7 \in \operatorname{Syl}_7(G)$ ist also

$$\begin{array}{rcl} |\mathrm{N}_G(P_2)| & \in & \{8, 24\} \\ |\mathrm{N}_G(P_3)| & \in & \{6, 24\} \\ |\mathrm{N}_G(P_7)| & = & 21 \ . \end{array}$$

Behauptung 2. *Für* $P_7 \in \operatorname{Syl}_7(G)$ *ist* $|\operatorname{Syl}_3(\mathrm{N}_G(P_7))| = 7$.

Es ist $|\operatorname{Syl}_3(\mathrm{N}_G(P_7))|$ ein Teiler von 7, also $|\operatorname{Syl}_3(\mathrm{N}_G(P_7))| \in \{1, 7\}$.

Angenommen, $|\operatorname{Syl}_3(\mathrm{N}_G(P_7))| = 1$. Sei $Q \in \operatorname{Syl}_3(\mathrm{N}_G(P_7))$.

Nach Korollar 155 ist $Q \trianglelefteq \mathrm{N}_G(P_7)$ und daher $\mathrm{N}_G(P_7) \leqslant \mathrm{N}_G(Q)$.

Es ist Q eine Gruppe von Ordnung 3 und also ist $Q \in \operatorname{Syl}_3(G)$.

Nach obigem ist $|\mathrm{N}_G(Q)| \in \{6, 24\}$. Da $|\mathrm{N}_G(P_7)| = 21$ ist, und dies weder 6 noch 24 teilt, ist $\mathrm{N}_G(P_7) \leqslant \mathrm{N}_G(Q)$ nicht möglich. *Widerspruch.*

Somit ist $|\operatorname{Syl}_3(\mathrm{N}_G(P_7))| = 7$. Dies zeigt *Behauptung* 2.

Behauptung 3. *Es ist* $|\operatorname{Syl}_3(G)| = 28$.

Angenommen, $|\operatorname{Syl}_3(G)| = 7$. Sei $P_7 \in \operatorname{Syl}_7(G)$. Es enthält $\mathrm{N}_G(P_7)$ dank Behauptung 2 alle 3-Sylowgruppen von G. Folglich ist $\langle \operatorname{Syl}_3(G) \rangle \leqslant \mathrm{N}_G(P_7)$.

Da $|\operatorname{Syl}_3(G)| = 7$ ist, gibt es $7 \cdot 2 = 14$ Elemente von Ordnung 3 in G. Die Untergruppe $\langle \operatorname{Syl}_3(G) \rangle$ enthält also mindestens 15 Elemente. Da $|\mathrm{N}_G(P_7)| = 21$ ist und $|\langle \operatorname{Syl}_3(G) \rangle|$ ein Teiler hiervon, folgt $\langle \operatorname{Syl}_3(G) \rangle = \mathrm{N}_G(P_7)$. Da die 3-Sylowgruppen von G konjugiert zueinander sind, ist $\mathrm{N}_G(P_7) = \langle \operatorname{Syl}_3(G) \rangle \trianglelefteq G$. *Widerspruch* zu G einfach. Dies zeigt *Behauptung* 3.

Zwischenstand. Es ist

$$\begin{array}{rcl} |\operatorname{Syl}_2(G)| & \in & \{7, 21\} \\ |\operatorname{Syl}_3(G)| & = & 28 \\ |\operatorname{Syl}_7(G)| & = & 8 \end{array}$$

Für $P_2 \in \mathrm{Syl}_2(G)$, $P_3 \in \mathrm{Syl}_3(G)$ und $P_7 \in \mathrm{Syl}_7(G)$ ist also

$$\begin{array}{rcl} |\mathrm{N}_G(P_2)| & \in & \{8, 24\} \\ |\mathrm{N}_G(P_3)| & = & 6 \\ |\mathrm{N}_G(P_7)| & = & 21\ . \end{array}$$

In G gibt es $28 \cdot 2 = 56$ Elemente der Ordnung 3 und $8 \cdot 6 = 48$ Elemente der Ordnung 7, sowie ein Element der Ordnung 1.

Die verbleibenden $168 - 56 - 48 - 1 = 63$ Elemente haben Ordnung 2, 4, 6, 8, 12, 14, 21 oder 24.

Behauptung 4. *Es gibt in G nur Elemente der Ordnung* 1, 3, 7, 2, 4 *oder* 8.

Wir müssen ausschließen, daß es in G Elemente der Ordnung 6, 14 oder 21 gibt. Daraus folgt dann, daß es in G keine Elemente der Ordnung 12 oder 24 gibt.

Angenommen, es gibt in G ein Element w der Ordnung 6.

Dann ist $\langle w^2 \rangle \in \mathrm{Syl}_3(G)$ und $w \in \mathrm{N}_G(\langle w^2 \rangle)$. Da $|\mathrm{N}_G(\langle w^2 \rangle)| = 6$ ist, folgt $\mathrm{N}_G(\langle w^2 \rangle) = \langle w \rangle$. Da alle 3-Sylowgruppen konjugiert sind, sind auch ihre Normalisatoren in G konjugiert und zyklisch von Ordnung 6. Verschiedene 3-Sylowgruppen haben verschiedene Normalisatoren, da eine zyklische Gruppe von Ordnung 6 genau eine Untergruppe von Ordnung 3 hat. Also gibt es in G wenigstens 28 zyklische Untergruppen von Ordnung 6.

Die Abbildung, die jedem Element von Ordnung 6 sein Untergruppenerzeugnis zuordnet, hat zweielementige Urbilder von jeder zyklischen Untergruppe von Ordnung 6. Somit gibt es in G wenigstens 56 Elemente von Ordnung 6.

In G gibt es also 56 Elemente von Ordnung 3, mindestens 56 Elemente von Ordnung 6 und 48 Elemente von Ordnung 7. Es bleiben höchstens $168 - 2 \cdot 56 - 48 = 8$ Elemente übrig. Folglich ist $|\mathrm{Syl}_2(G)| \leqslant 1$ und damit $|\mathrm{Syl}_2(G)| = 1$. Also gibt es in G eine normale 2-Sylowgruppe. *Widerspruch* zu G einfach.

Angenommen, es gibt in G ein Element x der Ordnung 14.

Dann ist $\langle x^2 \rangle \in \mathrm{Syl}_7(G)$. Ferner ist $x \in \mathrm{N}_G(\langle x^2 \rangle)$. Aber $|\langle x \rangle| = 14$ teilt nicht $|\mathrm{N}_G(\langle x^2 \rangle)| = 21$. *Widerspruch.*

Angenommen, es gibt in G ein Element y der Ordnung 21.

Dann ist $\langle y^7 \rangle \in \mathrm{Syl}_3(G)$. Ferner ist $y \in \mathrm{N}_G(\langle y^7 \rangle)$. Aber $|\langle y \rangle| = 21$ ist kein Teiler von $|\mathrm{N}_G(\langle y^7 \rangle)| = 6$. *Widerspruch.*

Dies zeigt *Behauptung* 4.

Behauptung 5. *Es ist* $|\mathrm{Syl}_2(G)| = 21$.

Angenommen, $|\mathrm{Syl}_2(G)| = 7$. Dann gibt es in G höchstens $7 \cdot (8 - 1) = 49$ Elemente von Ordnung 2, 4 oder 8. Da es 56 Elemente der Ordnung 3 und 48 Elemente der Ordnung 7 in G gibt, sowie ein Element der Ordnung 1, hat G dank Behauptung 4 höchstens $49 + 56 + 48 + 1 = 154$ Elemente. *Widerspruch* zu $|G| = 168$. Dies zeigt *Behauptung* 5.

Endstand. Es ist

$$\begin{aligned} |\operatorname{Syl}_2(G)| &= 21 \\ |\operatorname{Syl}_3(G)| &= 28 \\ |\operatorname{Syl}_7(G)| &= 8 \end{aligned}$$

Ferner gibt es in G nur Elemente der Ordnung 1, 3, 7, 2, 4 oder 8.

A.3 Das Lemma von Kuratowksi-Zorn

Es sollen nun das Lemma von Kuratowski-Zorn gezeigt werden, wie in §3.8.2 angekündigt.

Wir folgen hier im wesentlichen Grayson, D.R., *Zorn's Lemma*, 2007, welcher seinerseits Kneser, H., *Eine direkte Ableitung des Zornschen Lemmas aus dem Auswahlaxiom,* Math. Z. 53, p. 110–113, folgt.

Sei $X = (X, \leqslant)$ ein Poset; vgl. Definition 246.

Erinnerung A.1 Das *Auswahlaxiom* besagt, daß es für jede surjektive Abbildung

$$U \xrightarrow{f} V$$

zwischen Mengen U und V eine Abbildung $U \xleftarrow{s} V$ mit $f \circ s = \mathrm{id}_V$ gibt.

Bemerkung A.2 *Seien A und B Mengen.*

Sei $R \subseteq A \times B$ derart gegeben, daß für jedes $a \in A$ ein $b \in B$ existiert mit $(a, b) \in R$.

Dann gibt es eine Abbildung $f : A \to B$ mit $(a, f(a)) \in R$ für $a \in A$.

Mit anderen Worten, jede linkstotale Relation enthält eine linkstotale und rechtseindeutige Relation.

Beweis. Nach Voraussetzung an R ist $p : R \to A : (a, b) \mapsto a$ surjektiv.

Wir wählen eine Abbildung $i : A \to R$ mit $p \circ i = \mathrm{id}_A$, vgl. Erinnerung A.1.

Wir schreiben $i(a) =: (i_1(a), i_2(a)) \in R \subseteq A \times B$ für $a \in A$.

Es ist $a = p(i(a)) = p\big((i_1(a), i_2(a))\big) = i_1(a)$ für $a \in A$.

Sei $f(a) = i_2(a)$ für $a \in A$. Dann ist $f : A \to B$ eine Abbildung mit $(a, f(a)) = (i_1(a), i_2(a)) \in R$ für $a \in A$. ▫

Definition A.3 Seien Y, $Z \in \operatorname{Pot}(X)$ gegeben.

Es heißt Y eine *abgeschlossene Teilmenge* von Z, geschrieben $Y \leqslant Z$, falls $Y \subseteq Z$ und falls für $y \in Y$ und $z \in Z$ aus $z \leqslant y$ bereits $z \in Y$ folgt.

Mit anderen Worten, es ist $Y \leqslant Z$ genau dann, wenn $Y \subseteq Z$ ist und

$$\{\, z \in Z \,:\, z < y \,\} \;=\; \{\, z \in Y \,:\, z < y \,\}$$

ist für $y \in Y$.

Wir schreiben $Y < Z$, falls $Y \leqslant Z$ und $Y \neq Z$ ist.

Bemerkung A.4 *Auf* $\mathrm{Pot}(X)$ *ist* $(\leqslant)$ *eine Teilordnung.*

Es ist also $\mathrm{Pot}(X) = (\mathrm{Pot}(X), \leqslant)$ *ein Poset.*

Beweis. Zur Reflexivität. Für $Y \in \mathrm{Pot}(X)$ ist $Y \leqslant Y$, da $Y \subseteq Y$ und da für $z \in Y$ und $y \in Y$ aus $z \leqslant y$ bereits $z \in Y$ folgt.

Zur Identitivität. Seien Y, $Z \in \mathrm{Pot}(X)$. Aus $Y \leqslant Z$ und $Z \leqslant Y$ folgt $Y \subseteq Z$ und $Z \subseteq Y$, also $Y = Z$.

Zur Transitivität. Seien Y, Z, $W \in \mathrm{Pot}(X)$. Seien $Y \leqslant Z$ und $Z \leqslant W$.

Aus $Y \subseteq Z$ und $Z \subseteq W$ folgt $Y \subseteq W$.

Seien $y \in Y$ und $w \in W$ mit $w \leqslant y$ gegeben. Wir haben $w \overset{!}{\in} Y$ zu zeigen.

Da $y \in Z$ und $w \in W$ und $w \leqslant y$, folgt aus $Z \leqslant W$, daß $w \in Z$ liegt.

Da $y \in Y$ und $w \in Z$ und $w \leqslant y$, folgt aus $Y \leqslant Z$, daß $w \in Y$ liegt. ▫

Definition A.5 Seien $Z \in \mathrm{Pot}(X)$ gegeben.

(1) Wir erinnern daran, daß Z *linear geordnet* heißt, falls für z, $z' \in Z$ gilt, daß $z \leqslant z'$ oder $z' \leqslant z$ ist, d.h. daß z und z' vergleichbar sind; vgl. Definition 246.

Ist Z linear geordnet und $Y \subseteq Z$, dann ist auch Y linear geordnet.

(2) Es heißt Z *wohlgeordnet,* falls Z linear geordnet ist und falls jede nichtleere Teilmenge $Y \subseteq Z$ ein minimales Element besitzt.

Minimal und initial sind hier gleichbedeutend; vgl. Bemerkung 249.(1).

Gilt für $y_0\,,\, y_0' \in Y$, daß $y_0 \leqslant y$ und $y_0' \leqslant y$ für $y \in Y$, dann folgt $y_0 \leqslant y_0'$ und $y_0' \leqslant y_0$, also $y_0 = y_0'$.

Wegen dieser Eindeutigkeit können wir also $y_0 =: \min(Y)$ schreiben.

Bemerkung A.6 *Sei* $Z \in \mathrm{Pot}(X)$ *wohlgeordnet. Sei* $Y < Z$. *Sei* $z_0 := \min(Z \smallsetminus Y)$. *Dann ist*

$$Y \;=\; \{\, z \in Z \,:\, z < z_0 \,\}\,.$$

Beweis.

Zu $\subseteq$. *Annahme*, es kann ein $y \in Y$ gewählt werden mit $y \notin \{\, z \in Z \,:\, z < z_0 \,\}$. Da Z linear geordnet ist, folgt $z_0 \leqslant y$. Da Y eine abgeschlossene Teilmenge von Z ist, erhalten wir $z_0 \in Y$, im *Widerspruch* zu $z_0 \in Z \setminus Y$.

Zu $\supseteq$. *Annahme*, es kann ein $z_1 \in \{\, z \in Z \,:\, z < z_0 \,\}$ gewählt werden mit $z_1 \notin Y$. Es liegt $z_1 \in Z \setminus Y$. Da $z_0 = \min(Z \setminus Y)$, folgt $z_0 \leqslant z_1$. Aus $z_1 \leqslant z_0$ und $z_0 \leqslant z_1$ folgt $z_1 = z_0$. Aber es ist $z_1 < z_0$, *Widerspruch.* ▫

Bemerkung A.7 *Sei $Y \subseteq X$. Sei $F \subseteq \mathrm{Pot}(Y)$ derart, daß für $Z \in F$ stets $Z \leqslant Y$ ist.*

Sei $W := \bigcup_{Z \in F} Z \subseteq Y$. Dann ist $W \leqslant Y$.

Beweis. Sei $w \in W$ und $y \in Y$ gegeben mit $y \leqslant w$. Es ist $y \overset{!}{\in} W$ zu zeigen.

Wir wählen $Z \in F$ mit $w \in Z$. Dann ist $w \in Z$ und $y \in Y$ und $y \leqslant w$. Da $Z \leqslant Y$, folgt $y \in Z \subseteq W$. ▫

Lemma A.8 *Wir betrachten das Poset $\mathrm{Pot}(X) = (\mathrm{Pot}(X), \leqslant)$; cf. Bemerkung* A.4.

Sei $F \subseteq \mathrm{Pot}(X)$ eine linear geordnete Teilmenge derart, daß für $Z \in F$ stets Z eine wohlgeordnete Teilmenge von X ist.

Sei

$$W := \bigcup_{Z \in F} Z \subseteq X .$$

(1) *Es ist W wohlgeordnet.*

(2) *Für $Z \in F$ ist $Z \leqslant W$.*

Beweis.

Zu (1). Wir haben zu zeigen, daß W linear geordnet ist. Seien $x_1, x_2 \in W$.

Wähle $Z_1 \in F$ mit $x_1 \in Z_1$. Wähle $Z_2 \in F$ mit $x_2 \in Z_2$. Da F linear geordnet ist, ist o.E. $Z_1 \leqslant Z_2$, insbesondere $Z_1 \subseteq Z_2$

Also sind $x_1, x_2 \in Z_2$. Da Z_2 linear geordnet ist, ist $x_1 \leqslant x_2$ oder $x_2 \leqslant x_1$.

Wir haben zu zeigen, daß für jede nichtleere Teilmenge $U \subseteq W$ ein $u_0 \in U$ existiert, für welches $u_0 \leqslant u$ gilt für $u \in U$.

Da $U \neq \emptyset$, kann ein $u_1 \in U$ gewählt werden. Da $u_1 \in U \subseteq W$, kann ein $Z_0 \in F$ gewählt werden mit $u_1 \in Z_0$. Es ist $u_1 \in Z_0 \cap U$ und somit $Z_0 \cap U \neq \emptyset$. Da Z_0 wohlgeordnet ist, können wir $u_0 := \min(Z_0 \cap U) \in Z_0 \cap U$ bilden.

Sei $u \in U$. Wir haben $u_0 \overset{!}{\leqslant} u$ zu zeigen.

Es ist $u \in U \subseteq W$. Wir wählen ein $Z \in F$ mit $u \in Z$. Da $u \in U \cap Z$ liegt, ist $U \cap Z \neq \emptyset$. Da Z wohlgeordnet ist, können wir $u' := \min(Z \cap U) \in Z \cap U$ bilden. Es ist $u' \leqslant u$.

Da F linear geordnet ist, ist $Z_0 \leqslant Z$ oder $Z \leqslant Z_0$.

Fall $Z_0 \leqslant Z$. Es ist $u_0 \in Z_0 \cap U \subseteq Z \cap U$. Also ist $u' \leqslant u_0$. Da $Z_0 \leqslant Z$, folgt $u' \in Z_0$. Insgesamt ist $u' \in Z_0 \cap U$ und also $u_0 \leqslant u'$. Es folgt $u_0 = u' \leqslant u$.

Fall $Z \leqslant Z_0$. Es ist $u' \in Z \cap U \subseteq Z_0 \cap U$. Also ist $u_0 \leqslant u'$. Da $Z \leqslant Z_0$, folgt $u_0 \in Z$. Insgesamt ist $u_0 \in Z \cap U$ und also $u' \leqslant u_0$. Es folgt $u_0 = u' \leqslant u$.

Zu (2). Sei $Z \in F$. Es ist $Z \subseteq W$. Zu zeigen ist $Z \overset{!}{\leqslant} W$.

Sei $z \in Z$. Sei $w \in W$. Sei $w \leqslant z$. Zu zeigen ist $w \overset{!}{\in} Z$.

Wir wählen $Z' \in F$ mit $w \in Z'$. Da F linear geordnet ist, ist $Z \leqslant Z'$ oder $Z' \leqslant Z$.

Fall $Z' \leqslant Z$. Es ist $w \in Z' \subseteq Z$.

Fall $Z \leqslant Z'$. Da $z \in Z$ und $w \in Z'$ und $w \leqslant z$, folgt aus $Z \leqslant Z'$, daß $w \in Z$ liegt. ▫

Definition A.9 Wir schreiben

$$\mathrm{Wohl}(X) \;:=\; \{\, Z \in \mathrm{Pot}(X) \,:\, Z \text{ ist wohlgeordnet} \,\} \;\subseteq\; \mathrm{Pot}(X)\,.$$

Eine Abbildung

$$\begin{array}{ccc} \mathrm{Wohl}(X) & \overset{g}{\to} & X \\ Z & \mapsto & g(Z) \end{array}$$

derart, daß für $Z \in \mathrm{Wohl}(X)$ für $z \in Z$ stets $z < g(Z)$ ist, heißt *Schrankenabbildung*.

Sei g eine Schrankenabbildung. Sei $Y \in \mathrm{Pot}(X)$. Es heißt Y dann *g-wohlgeordnet*, wenn Y wohlgeordnet ist und wenn

$$g(\{\, y' \in Y \,:\, y' < y \,\}) \;=\; y$$

ist für $y \in Y$. Wir schreiben

$$g\text{-}\mathrm{Wohl}(X) \;:=\; \{\, Z \in \mathrm{Pot}(X) \,:\, Z \text{ ist } g\text{-wohlgeordnet} \,\} \;\subseteq\; \mathrm{Wohl}(X) \;\subseteq\; \mathrm{Pot}(X)\,.$$

Bemerkung A.10 *Sei g eine Schrankenabbildung.*

Sei $Z \in g$-$\mathrm{Wohl}(X)$. Sei $Z' := Z \cup \{g(Z)\}$.

Dann ist $Z \subset Z'$ und $Z' \in g$-$\mathrm{Wohl}(X)$.

Beweis. Es ist $Z \subset Z'$, da $g(Z)$ nicht in Z liegt, da nicht $g(Z) < g(Z)$ ist.

Wir haben zu zeigen, daß Z' linear geordnet ist.

Seien $z'_1, z'_2 \in Z'$ gegeben. Falls $z'_1 = g(Z)$ ist, dann ist $z'_2 \leqslant z'_1$. Falls $z'_2 = g(Z)$ ist, dann ist $z'_1 \leqslant z'_2$. Falls $z'_1, z'_2 \in Z$ liegen, dann sind z'_1 und z'_2 vergleichbar, da Z linear geordnet ist.

Wir haben zu zeigen, daß Z' wohlgeordnet ist.

Sei $\emptyset \subset Y \subseteq Z'$. Wir haben zu zeigen, daß Y ein minimales Element besitzt.

Falls $Y \cap Z = \emptyset$ ist, dann ist $Y = \{g(Z)\}$ und $\min(Y) = g(Z)$.

Falls $Y \cap Z \neq \emptyset$ ist, dann verfügen wir über $m := \min(Y \cap Z) \in Y \cap Z \subseteq Y$, da $Z \in \mathrm{Wohl}(X)$.

Behauptung. Es ist m minimal in Y. Es ist $Y = (Y \cap Z) \cup (Y \cap \{g(Y)\})$. Sei $y \in Y$. Falls $y \in Y \cap Z$, dann ist $m \leqslant y$. Falls $y \in Y \cap \{g(Y)\}$, dann ist $m \leqslant g(Y) = y$. Dies zeigt die *Behauptung.*

Wir haben zu zeigen, daß Z' insgesamt g-wohlgeordnet ist.

Sei $z_1' \in Z'$. Wir haben $g(\{\, z' \in Z' \,:\, z' < z_1' \,\}) \stackrel{!}{=} z_1'$ zu zeigen.

Da $g(Z)$ eine obere Schranke von Z ist, ist nicht $g(Z) < z_1'$ und also

$$\{\, z' \in Z' \,:\, z' < z_1' \,\} \;=\; \{\, z \in Z \,:\, z < z_1' \,\}\,.$$

Falls $z_1' \in Z$, dann ist $g(\{\, z' \in Z' \,:\, z' < z_1' \,\}) = g(\{\, z \in Z \,:\, z < z_1' \,\}) = z_1'$, da $Z \in g\text{-}\mathrm{Wohl}(X)$.

Falls $z_1' = g(Z)$, dann ist $\{\, z' \in Z' \,:\, z' < z_1' \,\} = \{\, z \in Z \,:\, z < z_1' \,\} = Z$ und also $g(\{\, z' \in Z' \,:\, z' < z_1' \,\}) = g(Z) = z_1'$. ▫

Lemma A.11 *Sei g eine Schrankenabbildung.*

Wir betrachten das Poset $\mathrm{Pot}(X) = (\mathrm{Pot}(X), \leqslant)$.

Darin ist g-$\mathrm{Wohl}(X)$ *eine linear geordnete Teilmenge, d.h. eine Kette.*

Beweis. Seien Y, $Z \in g\text{-}\mathrm{Wohl}(X)$. Wir haben zu zeigen, daß $Y \stackrel{!}{\leqslant} Z$ oder $Z \stackrel{!}{\leqslant} Y$ ist.

Sei

$$W \;:=\; \bigcup_{\substack{U \in \mathrm{Pot}(X) \\ U \leqslant Y \text{ und } U \leqslant Z}} U\,.$$

Dank Bemerkung A.7 ist $W \leqslant Y$ und $W \leqslant Z$.

Es genügt zu zeigen, daß $W \stackrel{!}{=} Y$ oder $W \stackrel{!}{=} Z$ ist.

Annahme, es ist im Gegenteil $W < Y$ und $W < Z$.

Da Y wohlgeordnet ist, können wir $y_1 := \min(Y \setminus W)$ bilden.

Da Z wohlgeordnet ist, können wir $z_1 := \min(Z \setminus W)$ bilden.

Dank Bemerkung A.6 ist $W = \{\, y \in Y \,:\, y < y_1 \,\}$ und $W = \{\, z \in Z \,:\, z < z_1 \,\}$.

Da Y eine g-wohlgeordnete Menge ist, folgt $g(W) = g(\{\, y \in Y \,:\, y < y_1 \,\}) = y_1\,.$

Da Z eine g-wohlgeordnete Menge ist, folgt $g(W) = g(\{\, z \in Z \,:\, z < z_1 \,\}) = z_1$.

Wir schreiben $w' := y_1 = g(W) = z_1$.

Sei

$$W' \;:=\; W \cup \{w'\} \;.$$

Da $W = \{\, y \in Y \,:\, y < w' \,\}$, ist $w' \notin W$. Insbesondere ist $W \subset W'$.

Behauptung. Es ist $W' \overset{!}{\leqslant} Y$ und $W' \overset{!}{\leqslant} Z$.

Wegen der Symmetrie der Situation genügt es, $W' \overset{!}{\leqslant} Y$ zu zeigen.

Da $W \leqslant Y$ und da $w' = y_1 \in Y$, ist $W' \subseteq Y$. Wir haben zu zeigen, daß W' eine abgeschlossene Teilmenge von Y ist.

Sei $x \in W'$. Sei $y \in Y$. Sei $y \leqslant x$. Wir haben $y \overset{!}{\in} W'$ zu zeigen.

Fall $x \in W$. Wegen $W \leqslant Y$ folgt aus $y \leqslant x$, daß $y \in W \subseteq W'$ liegt.

Fall $x = w'$. Es ist $y \leqslant w'$.

Subfall $y = w'$. Dann ist $y \in W'$.

Subfall $y < w' = y_1$. Dann ist $y \in \{\, \tilde{y} \in Y \,:\, \tilde{y} < y_1 \,\} = W \subseteq W'$.

Dies zeigt die *Behauptung*.

Da $W = \bigcup\limits_{\substack{U \in \mathrm{Pot}(X) \\ U \leqslant Y \text{ und } U \leqslant Z}} U$, folgt aus der Behauptung nun $W' \subseteq W$.

Dies steht im *Widerspruch* zu $W \subset W'$. □

Lemma A.12 *Es habe jede wohlgeordnete Teilmenge von X eine obere Schranke.*

Dann gibt es in X ein maximales Element m, d.h. ein Element $m \in X$ mit

$$\{\, x \in X \,:\, m < x \,\} \;=\; \emptyset \;.$$

Beweis. Annahme, es ist $\{\, x \in X \,:\, m < x \,\} \neq \emptyset$ für $m \in X$.

Für jedes $m \in X$ gibt es also ein $x \in X$ mit $m < x$.

Wir wählen eine Abbildung $s : X \to X$ mit $x < s(x)$ für $x \in X$; vgl. Bemerkung A.2, anzuwenden mit $R = (<)$.

Nach Voraussetzung an X gibt es für jedes $Y \in \mathrm{Wohl}(X)$ ein $x \in X$, für welches x eine obere Schranke von Y ist.

Wir wählen eine Abbildung $\check{g} : \mathrm{Wohl}(X) \to X$ mit $\check{g}(Y)$ obere Schranke von Y für $Y \in \mathrm{Wohl}(X)$; vgl. Bemerkung A.2, anzuwenden mit

$$R \;=\; \{\, (Y, x) \in \mathrm{Wohl}(X) \times X \,:\, x \text{ ist obere Schranke von } Y \,\} \;.$$

Sei $g := s \circ \check{g} : \mathrm{Wohl}(X) \to X$.

Für $Y \in \mathrm{Wohl}(X)$ und $y \in Y$ ist also $y \leqslant \check{g}(Y)$, da $\check{g}(Y)$ eine obere Schranke für Y ist. Ferner ist $\check{g}(Y) < s(\check{g}(Y)) = g(Y)$. Insgesamt ist $y < g(Y)$ für $y \in Y$. Mithin ist g eine Schrankenabbildung; vgl. Definition A.9.

Wir betrachten die linear geordnete Teilmenge $g\text{-Wohl}(X) \subseteq \mathrm{Pot}(X)$; vgl. Lemma A.11. Sei

$$W \;:=\; \bigcup_{U \,\in\, g\text{-Wohl}(X)} U \;\subseteq\; X\,.$$

Gemäß Lemma A.8.(1) ist W wohlgeordnet.

Gemäß Lemma A.8.(2) ist $U \leqslant W$ für $U \in g\text{-Wohl}(X)$.

Behauptung. Es ist $W \in g\text{-Wohl}(X)$.

Sei $w \in W$. Wir haben $w \stackrel{!}{=} g(\{\, x \in W \,:\, x < w \,\})$ zu zeigen.

Wir wählen $U \in g\text{-Wohl}(X)$ mit $w \in U$. Es ist $U \leqslant W$. Folglich ist

$$\{\, x \in W \,:\, x < w \,\} \;=\; \{\, x \in U \,:\, x < w \,\}\,;$$

vgl. Definition A.3. Da $U \in g\text{-Wohl}(X)$ liegt, erhalten wir

$$g(\{\, x \in W \,:\, x < w \,\}) \;=\; g(\{\, x \in U \,:\, x < w \,\}) \;=\; w\,.$$

Dies zeigt die *Behauptung*.

Sei $W' := W \cup \{g(W)\}$. Dank Bemerkung A.10 ist $W \subset W'$ und $W' \in g\text{-Wohl}(X)$.

Letzteres hat aber $W' \subseteq W$ zur Folge, im *Widerspruch* zu $W \subset W'$. ▫

Lemma A.13 (Kuratowski-Zorn) *Wir erinnern an das Poset $X = (X, \leqslant)$.*

Wir erinnern daran, daß eine Kette in X eine linear geordnete Teilmenge von X bedeutet.

Es habe jede Kette in X eine obere Schranke.

Sei $x \in X$. Dann gibt es ein maximales Element $m \in X$ mit $x \leqslant m$.

Beweis. Sei $\tilde{X} := \{\, \tilde{x} \in X \,:\, x \leqslant \tilde{x} \,\}$.

Sei K eine wohlgeordnete Teilmenge von $\tilde{X}$.

Falls $K = \emptyset$ ist, dann ist x eine obere Schranke von K. Es ist $x \in \tilde{X}$.

Falls $K \neq \emptyset$ ist, dann wählen wir uns ein Element $k \in K$. Da $k \in K \subseteq \tilde{X}$, ist $x \leqslant k$.

Ferner ist K eine Kette in X. Nach Voraussetzung an X können wir nun eine obere Schranke $s \in X$ von K wählen. Es ist $x \leqslant k \leqslant s$ und daher $s \in \tilde{X}$.

Somit hat K in beiden Fällen eine obere Schranke in $\tilde{X}$.

Dank Lemma A.12 können wir in $\tilde{X}$ ein maximales Element m wählen. Da $m \in \tilde{X}$, ist $x \leqslant m$.

Behauptung. Es ist m maximal in X. *Annahme*, es kann ein $x' \in X$ mit $m < x'$ gewählt werden. Da $x \leqslant m < x'$, ist $x' \in \tilde{X}$. Nun ist m in $\tilde{X}$ maximal, $x' \in \tilde{X}$ und $m < x'$. Wir haben einen *Widerspruch*. ▫