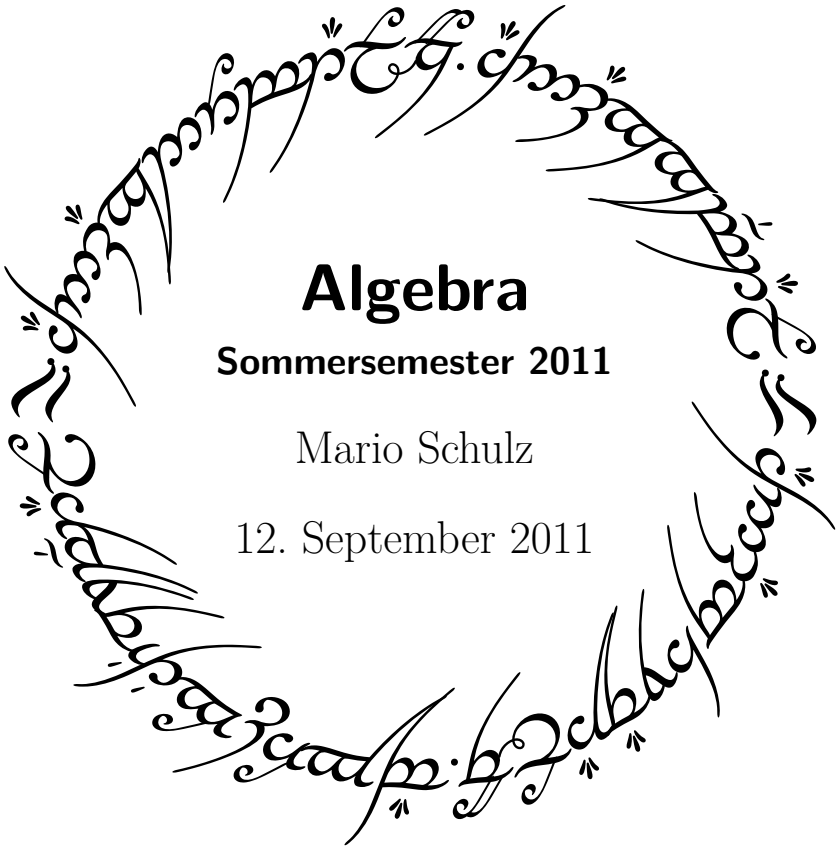


Algebra

Sommersemester 2011

Mario Schulz

12. September 2011

Inhaltsverzeichnis

Vorwort

Dieses Skript entstand im Rahmen der Vorlesung Algebra bei Herrn Prof. Dr. Steffen König an der Universität Stuttgart. Der Autor übernimmt für Schäden jeglicher Art, die durch dieses Dokument entstehen können, keine Haftung. Insbesondere kann nicht garantiert werden, dass die Inhalte fehlerfrei sind. Es handelt sich um eine Vorlesungsmitschrift und nicht um ein offizielles Dokument der Universität, weswegen Mitarbeiter eben dieser keine Verantwortung daran tragen.

Falls Sie Fragen haben oder Fehler finden, können Sie mir gerne eine Nachricht an folgende E-Mailadresse zukommen lassen:

`mario.schulz@stud.mathematik.uni-stuttgart.de`

Mein besonderer Dank gilt folgenden Personen:

- Nico Stein, Sebastian Krieg und Eric Wien
  für besonders sorgfältiges Korrekturlesen sowie zahlreiche wertvolle Verbesserungsvorschläge.
- Jim Magiera
  dessen Werk mich beim Design der LaTeX-Skriptvorlage, auf deren Basis dieses Skript geschrieben ist, inspiriert hat.

Stuttgart, im September 2011 *Mario Schulz*

Anmerkung: Diese Version vom 12. September 2011 ist eine Rohfassung. Gelegentliche Aktualisierungen können Änderungen an allen Stellen des Skripts mit sich bringen.

Organisation

Übungen

Übungen finden Mittwochs um 8.00 Uhr und um 11.30 Uhr statt. Die Scheinbedingungen sind wie gewöhnlich 50% der schriftlichen und der zu votierenden Aufgaben.

Sprechstunden

König	dienstags	10 Uhr – 11 Uhr	7.519
Liu	donnerstags	10 Uhr – 11 Uhr	7.561

Motivation Algebra: Lösen von Gleichungen

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

Gibt es für $n \geq 3$ eine Lösungsformel? Im Allgemeinen nein. Wie sieht der Beweis aus?

Geometrische Probleme mit Zirkel und Lineal:

- Winkeldreiteilung? Im Allgemeinen nicht möglich. Der Beweis wird mithilfe algebraischer Gleichungen geführt.
- Würfelverdopplung? Im Allgemeinen nicht möglich.

Im Rahmen dieser Vorlesung werden nacheinander folgende Strukturen betrachtet:

$$\text{Gruppen} \longrightarrow \text{Ringe} \longrightarrow \text{Körper} \; (\longrightarrow \text{Anwendungen})$$

Die Algebra bildet die Grundlage für algebraische Zahlentheorie, algebraische Topologie, algebraische Geometrie, Lie-Theorie, Darstellungstheorie, Kristallographie bis hin zur mathematischen Physik.

1 Gruppen

Definition 1.1 **Gruppe**

Eine Gruppe $(G, *)$ ist eine Menge G mit einer Abbildung

$$\begin{aligned} *\colon G \times G &\to G \\ (g_1, g_2) &\mapsto g_1 * g_2 \end{aligned}$$

sodass gilt:

(G1)	Assoziativität	$\forall_{g_1,g_2,g_3 \in G}$	$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$
(G2)	Neutrales Element	$\exists_{e \in G} \forall_{g \in G}$	$e * g = g = g * e$
(G3)	Inverses Element	$\forall_{g \in G} \exists_{h = g^{-1} \in G}$	$g * h = e = h * g$

Wenn der Kontext klar ist, wird das Symbol für die Verknüpfung mitunter weggelassen: $g_1 g_2 := g_1 * g_2$

Definition **Gruppenhomomorphismus**

Seien $(G, *_G)$ und $(H, *_H)$ Gruppen. Eine Abbildung $\varphi : G \to H$ heißt Gruppenhomomorphismus, wenn gilt:

$$\forall_{g,g' \in G} \quad \varphi(g *_G g') = \varphi(g) *_H \varphi(g')$$

Definition

Eine Gruppe heißt

- endliche Gruppe, wenn G eine endliche Menge ist,
- abelsch (oder kommutative Gruppe), wenn $g_1 * g_2 = g_2 * g_1 \quad \forall_{g_1,g_2 \in G}$
- zyklisch, wenn $\exists_{g \in G} \colon G = \{g^n \colon n \in \mathbb{Z}\}$. Dabei sei $g^n := \begin{cases} g * \ldots * g & , n > 0 \\ g^0 = e & , n = 0 \\ g^{-1} * \ldots * g^{-1} & , n < 0 \end{cases}$ wobei jeweils n-fache Verknüpfungen gemeint sind.

Satz
Das Neutrale Element e ist eindeutig. Zu jedem Gruppenelement ist das Inverse eindeutig.

Beweis :
Seien e und e' neutrale Elemente. $\Rightarrow\ e = e * e' = e'$.
Seien h, h' invers zu g. $\Rightarrow\ h = eh = h'gh = h'e = h'$. □

Beispiel: verschiedene Gruppen

- Die Gruppe mit einem Element: $G = \{e\}$ mit $ee = e$.
- Die leere Menge bildet keine Gruppe, da kein neutrales Element vorhanden ist.
- $G = (\mathbb{Z}, +)$ mit $e = 0$ und $g^{-1} = -g$ ist eine zyklische Gruppe (betrachte $g = 1$). $(\mathbb{Z}, \cdot)$ bildet dagegen keine Gruppe, da 0^{-1} nicht existiert.
- Sei X eine Menge. $S(X) := \{f \colon X \to X\,,\ f \text{ bijektiv}\}$ ist eine Gruppe mit der Komposition als Verknüpfung: $f * g := g \circ f$, sowie der Identität als neutrales Element $e = \mathrm{id}_X$. Besonders interessant ist der endliche Fall $X = \{1, \ldots, n\}$. Dann bezeichnet man $S(X) =: \Sigma_n$ als symmetrische Gruppe der Permutationen von n Elementen.
- Sei V ein Vektorraum über dem Körper K. Wir betrachten:

  $$G = \mathrm{GL}(V) := \{f \colon V \to V\,,\ f \text{ linear und invertierbar}\}$$

  Für $\dim V = n$ ist $V \simeq K^n$ und $\mathrm{GL}(V) \simeq \mathrm{GL}_n$, der Menge aller invertierbaren $n \times n$-Matritzen mit Einträgen in K. Diese Gruppe wird allgemeine lineare Gruppe genannt.
- Sei ein gleichseitiges Dreieck gegeben. Seine Symmetrien (Spiegelungen, Drehungen) bilden die Gruppe Σ_3. Auf diese Weise kommen wir von geometrischen Situationen auf Gruppen. Die Symmetriegruppe eines Quadrats ist jedoch $\lneq \Sigma_4$.

Definition 1.2 Untergruppe
Sei $(G, *)$ eine Gruppe. Eine Teilmenge $H \subset G$ heißt Untergruppe von $(G, *)$, wenn $(H, *_{|H})$ eine Gruppe ist, wobei mit $*_{|H}$ die Einschränkung der Abbildung $*$ auf $H \times H \to H$ gemeint ist. Das bedeutet $h_1, h_2 \in H\ \Rightarrow\ h_1 * h_2 \in H$. Ferner ist $e \in H$ sowie $h_1^{-1} \in H$.

Schreibweise: $H < G$.

Bemerkung: Die Untergruppenbildung ist transitiv: Aus $A < B$ und $B < C$ folgt sofort $A < C$.

Lemma
Sei G eine Gruppe und $H \subset G$ eine Teilmenge. Dann gilt:

$$H < G \;\Leftrightarrow\; H \neq \emptyset \;\wedge\; \forall_{a,b \in H} \colon ab^{-1} \in H$$

Es ist häufig effizienter dieses Kriterium statt den Gruppenaxiomen nachzuprüfen.

Beweis :
Siehe Aufgabenblatt 1, Votieraufgabe (3). □

Beispiel:
Sei $G = (\mathbb{Z}, +)$. Für festes $n \in \mathbb{N}$ betrachte $H = (n\mathbb{Z}, +)$. Dann gilt $g \in H \Leftrightarrow n|g$. Sei darüberhinaus $a \in \mathbb{Z}$. Division mit Rest ergibt: $a = bn + r$ mit $0 \leq |r| < n$. Für $r = 0$ ist $a \in n\mathbb{Z}$. Wie man sieht, zerfällt $\mathbb{Z}$ disjunkt in

$$\mathbb{Z} = n\mathbb{Z} \;\dot\cup\; n\mathbb{Z} + 1 \;\dot\cup\; n\mathbb{Z} + 2 \;\dot\cup\; \ldots \;\dot\cup\; n\mathbb{Z} + (n-1)$$

Dies motiviert die folgende Definition.

Definition 1.3 **Nebenklasse**
Sei $H < G \ni x$. Die Menge $xH := \{x * h \colon h \in H\}$ heißt Linksnebenklasse von x. Entsprechend werden Rechtsnebenklassen $Hx := \{h * x \colon h \in H\}$ definiert.

Im Fall $x \in H$ ist $xH = \{x * h \colon h \in H\} = H$, da $h = x^{-1}h'$ gewählt werden kann.
Im Fall $x \notin H$ gibt es eine Bijektion $xH \overset{1:1}{\longleftrightarrow} H$ mit $xh \mapsto h$.
Für $x, y \in G$ gilt entweder $xH = yH$ oder $xH \cap yH = \emptyset$. Dann zerfällt G disjunkt in

$$G = \bigcup_{\substack{\text{gewisse} \\ x_i}} x_i H \qquad \text{Partition von } G$$

Beweis :
Sei $xH \cap yH \neq \emptyset$. Wir folgern $xH = yH$.

$$xH \cap yH \ni z = xh_1 = yh_2 \qquad \Rightarrow\; x = y\overbrace{h_2 h_1^{-1}}^{\in H} \in yH$$

$$\Rightarrow\; xH = (yh_2h_1^{-1})H \subset yH$$

Die umgekehrte Inklusion $yH \subset xH$ folgt aus Symmetriegründen. □

Definiere alternativ die Äquivalenzrelation $x \sim_H y \Leftrightarrow xH = yH$. Dann bilden die Äquivalenzklassen bekanntlich eine Partition von G.

Beispiel:
Sei $G = \mathbb{Z}$ und $H = n\mathbb{Z}$. Dann gilt $x \sim_H y \Leftrightarrow x - y \in H \Leftrightarrow x = y \mod n$.

$\mathbb{Z}/n\mathbb{Z}$ bildet wieder eine Gruppe, da $(\mathbb{Z}, +)$ abelsch ist. Für $\overline{a} = a + n\mathbb{Z}$ und $\overline{b} = b + n\mathbb{Z}$ ist $(\overline{a} + \overline{b}) = (a + b) + n\mathbb{Z}$. An dieser Stelle wird die Kommutativität ausgenutzt.

Im Allgemeinen bilden die Linksnebenklassen aber keine Gruppe. Für $H < G$ bietet sich $(xH) * (yH) := (x * y)H$ an, ist aber nicht wohldefiniert, denn im Allgemeinen gilt für unterschiedliche Repräsentanten $\Big((xh_1) * (yh_2)\Big)H \neq (x * y)H$. Das nächste Beispiel illustriert das.

Beispiel:
Sei $G = \Sigma_3$ und $H = \{\mathrm{id}, (1\,2)\}$. Wir verwenden die von links nach rechts zu lesende Zykelschreibweise. Es muss 3 Linksnebenklassen geben:

$$
\begin{aligned}
H &= \mathrm{id}\, H \\
(2\,3)H &= \{(2\,3), (2\,3)(1\,2) = (2\,3\,1) = (1\,2\,3)\} \\
(1\,3)H &= \{(1\,3), (1\,3)(1\,2) = (1\,3\,2)\} \\
\Rightarrow\ \Sigma_3 &= \mathrm{id}\, H \,\dot\cup\, (2\,3)H \,\dot\cup\, (1\,3)H
\end{aligned}
$$

Was ist $(2\,3)H * (1\,3)H$? Nimmt man statt $(2\,3)$ den Repräsentant $(1\,2\,3)$ sieht man, dass veschiedene Ergebnisse herauskommen:

$$
\begin{array}{rcl}
(2\,3)(1\,3) = (1\,3\,2) & \in & (1\,3)H \\
 & & \not\in \\
(1\,2\,3)(1\,3) = (1\,2) & \in & \mathrm{id}\, H
\end{array}
$$

Die Multiplikation ist also nicht wohldefiniert, weshalb die Nebenklassen im Allgemeinen keine Gruppe bilden.

Definition 1.4
Sei G eine Gruppe und H eine Untergruppe. H heißt normale Untergruppe oder Normalteiler, wenn die Links- und Rechtsnebenklassen das Gleiche sind:

$gH = Hg \quad \forall_{g \in G}$ Schreibweise: $H \trianglelefteq G$

Eine äquivalente Bedingung ist: $gH = Hg \Leftrightarrow gHg^{-1} = H \Leftrightarrow ghg^{-1} \in H\, \forall_{h \in H}$

Bemerkung: Vorsicht: Im Gegensatz zu der Untergruppenbildung ist die Normalteilereigenschaft nicht transitiv.

Proposition 1.5

(a) Sei $N \trianglelefteq G$ ein Normalteiler und $G/N := \{gN \colon g \in G\}$ die Menge der Linksnebenklassen. Diese Menge G/N heißt Faktorgruppe oder Quotientengruppe und ist eine Gruppe mit (wohldefinierter) Multiplikation $g_1N * g_2N := (g_1 * g_2)N$.

(b) Sei $\varphi \colon G \to G'$ ein surjektiver Gruppenhomomorphismus.
Dann ist $H := \ker(\varphi) := \{g \colon \varphi(g) = e_{G'}\}$ ein Normalteiler von G und $G' \simeq G/H$.

Falls G/H eine Gruppe ist, betrachte den surjektiven Gruppenhomomorphismus

$$\begin{aligned} \varphi \colon G &\to G/H \\ g &\mapsto gH \end{aligned}$$

und seinen Kern $\ker\varphi = \{g \in G \colon gH = eH = H\} = H$. Aus Aussage (b) folgt dann sofort $H \trianglelefteq G$. Also ist G/H eine Gruppe $\Leftrightarrow$ $H \trianglelefteq G$.

Beweis :

(a) Es ist die Wohldefiniertheit von $g_1N * g_2N = (g_1g_2)N$ zu zeigen, also, dass bei der Wahl anderer Repräsentanten das Gleiche heraus kommt.

$$\text{zu zeigen:} \qquad g_1N = g_1'N \quad \wedge \quad g_2N = g_2'N \;\Rightarrow\; (g_1g_2)N = (g_1'g_2')N$$

Aufgrund der Partitionseigenschaft genügt es dazu $g_1g_2 \in (g_1'g_2')N$ nachzuweisen.

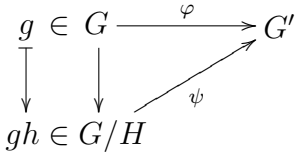
$$\begin{aligned} g_1 \in g_1N = g_1'N &\;\Rightarrow\; g_1 = g_1'n_1 \;\text{ für ein } n_1 \in N \\ g_2 \in g_2N = g_2'N &\;\Rightarrow\; g_2 = g_2'n_2 \;\text{ für ein } n_2 \in N \end{aligned}$$

$$Ng_2' = g_2'N \;\Rightarrow\; g_1g_2 = g_1'n_1g_2'n_2 = g_1'g_2'n_3n_2 \;\text{ für ein } n_3 \in N$$

Assoziativität sowie die Existenz von Einselement und Inversen sind klar. Damit ist G/H eine Gruppe.

(b) Offensichtlich ist $H := \ker(\varphi) \subset G$ eine Untergruppe. Für die Normalteilereigenschaft bleibt $ghg^{-1} \in H$ zu zeigen. Wendet man den Homomorphismus φ darauf an, ist sofort ersichtlich, dass $\varphi(ghg^{-1}) = \varphi(g)\underbrace{\varphi(h)}_{=e}\varphi(g^{-1}) = e$.

Um schließlich $G' \simeq G/H$ zu zeigen, betrachte das folgende Diagramm:



$$\begin{aligned} \psi \colon G/H &\to G' \\ gH &\mapsto \varphi(g) \end{aligned}$$

Es stellt sich die Frage nach der Wohldefiniertheit von ψ. Dazu ist zu zeigen, dass $gH = g'H \overset{!}{\Rightarrow} \varphi(g) = \varphi(g')$. Da $g = g'h$ für ein $h \in H$ gilt, folgt $\varphi(g) = \varphi(g'h) = \varphi(g')\varphi(h) = \varphi(g')$.

Die Abbildung ψ ist injektiv, denn $\underbrace{\psi(gH)}_{\varphi(g)} = e \;\Rightarrow\; g \in \ker\varphi = H$.

Sei $x \in G'$. Da φ surjektiv ist, folgt zudem wegen $\exists_{g\in G} \overbrace{\varphi(g)}^{\psi(gH)} = x$, dass ψ surjektiv und damit bijektiv ist. Für $x \in G'$ ergibt sich aus $x = \varphi(g) = \psi(gH)$ die zu ψ inverse Abbildung $\psi^{-1}\colon x \mapsto gH$. Also ist $G/H \simeq G'$.

Notiz: ψ ist nur dann surjektiv, wenn φ es ist.

□

Beispiel: Normalteiler

- Jede Untergruppe $H < G$ einer *abelschen* Gruppe G ist ein Normalteiler $H \trianglelefteq G$. Ein Beispiel ist $n\mathbb{Z} < \mathbb{Z}$.
- Gibt es zu $G \supset H$ genau zwei Nebenklassen, folgt mit $eH = H$ für $g, g' \in G \setminus H$:

  $$G = H \dot\cup gH = H \dot\cup Hg' \;\Rightarrow\; gH = Hg' = Hg$$

  Diese Situation liegt im Fall $|G| < \infty$ und $|H| = \frac{|G|}{2}$ vor. Dann gilt: $|H| = |gH|$.
- $G = \Sigma_3$ hat $|G| = 3! = 6$ Elemente. Sei $H := \{\mathrm{id}, (1\,2\,3), (1\,3\,2)\}$. Dabei bedeutet $(1\,2\,3)$, dass $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$. Dann ist $\operatorname{ord} H = |H| = 3$ und verbraucht die Hälfte der Elemente. $\frac{|G|}{|H|} = 2 \;\Rightarrow\; H \trianglelefteq G$.

  Ferner wird H erzeugt durch $H = \{g, g^2, g^3 = \mathrm{id}\}$ für $g = (1\,2\,3)$. Also ist H eine zyklische Gruppe.
- $\mathbb{Z}/3\mathbb{Z}$ ist auch zyklisch mit Ordnung $3 = |H|$. Daher stellt sich die Frage, ob diese beiden Gruppen isomorph sind. Betrachte dazu die Erzeuger und nebenstehenden Gruppenhomomorphismus.

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} &\to H \\ \overline{0} &\mapsto \mathrm{id} = g^3 \\ \overline{1} &\mapsto g \\ \overline{1} + \overline{1} = \overline{2} &\mapsto g^2 \end{aligned}$$

Es gibt also bis auf Isomorphie anscheinend gar nicht so viele zyklische Gruppen. Im nächsten Abschnitt wird das genauer untersucht.

Klassifikation zyklischer Gruppen

Eine allgemeine zyklische Gruppe $G = \{g^n \colon n \in \mathbb{Z}\}$ ist wegen $g^n \cdot g^\ell = g^{\ell+n} = g^\ell \cdot g^n$ immer abelsch. Wir wollen Folgendes zeigen:

Proposition
Die Ordnung $|G|$ einer zyklischen Gruppe G bestimmt sie bis auf Isomorphie.

Beweis :

Fall 1: $g^n \neq g^\ell$ für $n \neq \ell$, $|G| = \infty$. Dann ist G isomorph zu $\mathbb{Z}$ vermöge:

$$\begin{aligned} \mathbb{Z} &\to G \\ 0 &\mapsto e \\ 1 &\mapsto g \\ n &\mapsto g^n \\ \ell &\mapsto g^\ell \end{aligned}$$

Fall 2: $\exists_{n \gneq \ell} \colon g^n = g^\ell \;\Rightarrow\; g^{n-\ell} = e \;\Rightarrow\; \exists_{m \in \mathbb{Z}\setminus\{0\}} \colon g^m = e.$

Da dann auch $g^{-m} = e$, kann m natürlich gewählt werden: $\exists_{m \in \mathbb{N}_{>0}} \colon g^m = e.$

Wähle $m \in \mathbb{N}$ mit $g^m = e$ minimal und betrachte eine Teilmenge mit m verschiedenen Elementen $\{e, g, g^2, \ldots, g^{m-1}\} \subset G$. Sei $g^\ell \in G$ für $\ell > m$. Division mit Rest ergibt $\ell = km + r$ mit $0 \leq r \leq m$.

$$\begin{aligned} &\Rightarrow\; g^\ell = g^{km+r} = g^{km} \cdot g^r = (g^m)^k g^r = g^r \\ &\Rightarrow\; G = \{g, g^2, \ldots, g^m\} \;\Rightarrow\; |G| = m \end{aligned}$$

Folgende Abbildung ist ein entsprechender Gruppenhomomorphismus:

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\to G \\ \overline{j} &\mapsto g^j \\ \overline{1} &\mapsto g \end{aligned}$$

Also ist jede zyklische Gruppe G isomorph zu genau einer der Gruppen $\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z}$, wobei $m = |G|$. □

Bemerkung: zyklisch $\Rightarrow$ abelsch, die Umkehrung gilt nicht. Gegenbeispiel: $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ mit $(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2)$ ist nicht zyklisch. Wäre G zyklisch, müsste es wegen $|G| = 8$ isomorph zu $\mathbb{Z}/8\mathbb{Z}$ sein. Ein entsprechender Homomorphismus erzeugt jedoch einen Widerspruch:

$$\begin{aligned} \mathbb{Z}/8\mathbb{Z} &\to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ 0 &\mapsto (0,0) \\ 1 &\mapsto (a,b) \\ 2 &\mapsto (2a, 2b) \\ 4 &\mapsto (4a, 4b) = (0,0) \qquad \text{Widerspruch} \end{aligned}$$

$a \in \mathbb{Z}/4\mathbb{Z} \;\Rightarrow\; 4a = 0, \qquad b \in \mathbb{Z}/2\mathbb{Z} \;\Rightarrow\; 4b = 0.$

$\mathbb{Z}/8\mathbb{Z}$ hat Elemente der Ordnung 8, aber $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ hat keine.

Untergruppen zyklischer Gruppen

Ein Beispiel für eine Untergruppe $H < G = \mathbb{Z}$ ist $H = n\mathbb{Z}$. In diesem Fall ist n die kleinste positive Zahl in H. Ist auch eine beliebige Untergruppe $H \neq \{0\}$ von dieser Form?

Proposition
Alle Untergruppen $H < \mathbb{Z}$ sind von der Form $n\mathbb{Z}$.

Beweis :
Sei $n \in \mathbb{N} \cap H$ minimal $\Rightarrow$ $n\mathbb{Z} \subset H$.

Falls $n\mathbb{Z} \subsetneq H$ existiert ein minimales $\ell \in \mathbb{N} \cap H \setminus n\mathbb{Z}$ mit $\ell > n$. Wende wieder den Trick der Division mit Rest an: Für $\underbrace{\ell = kn}_{\in H} + r$ mit $0 \leq r < n$ ist $r = \ell - kn \in H$.

Es folgt $r = 0 \Rightarrow \ell = kn \in n\mathbb{Z}$, ein Widerspruch. Also ist $n\mathbb{Z} = H$. □

Proposition 1.6
Sei $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ eine zyklische Gruppe der Ordnung $|G| = n \in \mathbb{N} \cup \{\infty\}$. Dann gilt:

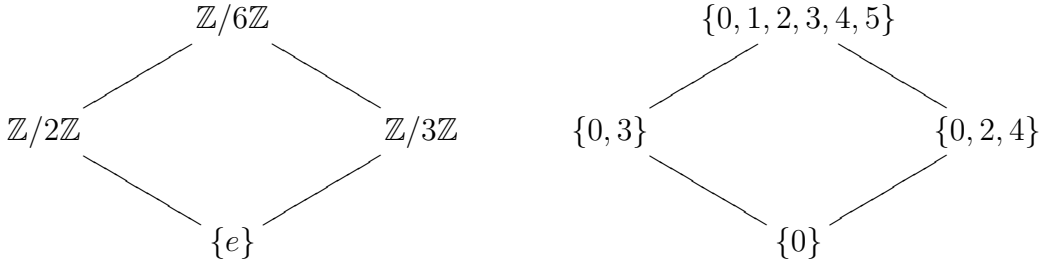
(a) $|G| = n = \inf\{\ell : g^\ell = e\}$

(b) $|G| < \infty$ und $s \in \mathbb{Z} \Rightarrow \operatorname{ord}(g^s) = \frac{n}{\operatorname{ggT}(n,s)}$

(c) Jede Untergruppe $H < G$ ist zyklisch.

(d) $|G| < \infty$ und $d|n \Rightarrow \exists! H < G$ mit $|H| = d$ und $H = \left\langle g^{\frac{n}{d}} \right\rangle$.

Beispiel: $G = \mathbb{Z}/6\mathbb{Z}$
$|G| = 6$ hat die Teiler $1, 2, 3, 6$. Wir erhalten die Untergruppen:



Beweis : Proposition 1.6

(a) Siehe oben im Beweis von „$G \simeq \mathbb{Z}$ oder $G \simeq \mathbb{Z}/n\mathbb{Z}$“.

(b) Sei $|G| < \infty$, sowie $k := \text{ord}(g^s) < \infty$, also $(g^s)^k = e$. Dann gilt:

$$sk \in n\mathbb{Z} \;\Rightarrow\; n|sk \;\Rightarrow\; \tfrac{n}{\text{ggT}(n,s)} \,|\, k$$

Umgekehrt bleibt noch $k \,|\, \frac{n}{\text{ggT}(n,s)}$ zu zeigen. Dies folgt aus:

$$(g^s)^{\frac{n}{\text{ggT}(n,s)}} = g^{\frac{sn}{\text{ggT}(n,s)}} = (g^n)^{\frac{s}{\text{ggT}(n,s)}} = e \;\Rightarrow\; \tfrac{n}{\text{ggT}(n,s)} \in k\mathbb{Z}$$

(c) Zu zeigen ist, dass Untergruppen $H < G$ zyklisch von der Form $H = \langle g^{\frac{n}{d}} \rangle$ für $d|n$ sind. Wir recyclen die Idee vom Beweis, dass alle Untergruppen von $\mathbb{Z}$ zyklisch sind.

Sei $g^s \in H$ für gewisse s. Wenn $|H| = 1 \;\Rightarrow\; H = \{g^0\}$. Sei also $|H| > 1$. Wähle kleinstes positives s mit $g^s \in H \;\Rightarrow\; \langle g^s \rangle \subset H$. Wir wollen zeigen, dass $\langle g^s \rangle = H$.

Sei $x \in H$ mit $x = g^\ell$ für $\ell > s$. Dividiere mit Rest: $\ell = ks + r$ mit $0 \leq r < s$. Wegen $g^\ell \in H$ und $g^{ks} = (g^s)^k \in H$ ist auch $g^r \in H$. Folglich ist $r = 0$ und $\ell = ks$ und damit $x \in \langle g^s \rangle$.

(d) Es gelte $d|n$. Dann ist $H = \langle g^{\frac{n}{d}} \rangle$ tatsächlich eine Untergruppe der Ordnung $|H| = d$, da $|G| = n$. Zeige noch, dass alle Untergruppen diese Form haben.

Gemäß (c) ist $H < G$ von der Form $H = \langle g^k \rangle$ für ein minimales k. Wir zeigen, dass $k|n$ gilt. Für $H \ni g^k$ und $e = g^n$ folgt wieder per Division mit Rest:

$$n = \ell k + r \text{ mit } 0 \leq r < k \;\Rightarrow\; g^r \in H \;\Rightarrow\; r = 0 \;\Rightarrow\; n = \ell k \;\Rightarrow\; k|n$$

□

Wir haben gezeigt, dass bei Untergruppen $H < G$ zyklischer Gruppen $|G|$ von $|H|$ geteilt wird. Wie wir sehen werden, ist dies bei allen Gruppen der Fall.

Definition 1.7 **Index**

Sei G eine Gruppe mit $H < G$ als Untergruppe. Die Anzahl $|G/H|$ der Linksnebenklassen heißt der Index von H in G und wird mit $[G : H]$ bezeichnet.

Satz 1.8 **Lagrange**

Sei H eine Untergruppe von G. Dann ist die Elementezahl von G gleich der Elementezahl von H multipliziert mit dem Index von H.

$$|G| = |H| \cdot [G : H]$$

Daraus folgt, dass $|H|$ ein Teiler von $|G|$ ist.

Beweis :
Wir haben gesehen, dass $|g_1H| = |g_2H|$ und $G = \dot{\bigcup} gH$. Daraus folgt sofort, dass $|G| = |H| \cdot [G : H]$ ist. □

Anwendungen

Sei p eine Primzahl. Bekanntlich ist $(G, +) = (\mathbb{Z}/p\mathbb{Z}\,, +)$ eine Gruppe. Da $|G| = p$ nur 1 und p als Teiler hat, gibt es nur zwei triviale Untergruppen: G und $\{\,\overline{0}\,\}$. Die Gruppe hat erst recht keine (nichttrivialen) Normalteiler.

Definition **einfache Gruppe**
Eine Gruppe ohne nichttriviale Normalteiler heißt einfache Gruppe.

$(\mathbb{Z}/n\mathbb{Z}\,, \cdot)$ ist keine multiplikative Gruppe, da $\overline{0}$ kein Inverses hat. Wenn $n = a \cdot b$, folgt sofort $\overline{0} = \overline{n} = \overline{a} \cdot \overline{b}$, weswegen auch $\overline{a}$ und $\overline{b}$ keine Inverse haben. Betrachtet man jedoch nur jene Elemente, die ein Inverses besitzen, liegt für $n \geq 2$ eine multiplikative Gruppe vor.

$$(\mathbb{Z}/n\mathbb{Z})^* := \{\,\text{invertierbare Elemente von } \mathbb{Z}/n\mathbb{Z}\,\}$$

Speziell gilt für eine Primzahl p:

$$(\mathbb{Z}/p\mathbb{Z})^* = \{\overline{1}, \overline{2}, \ldots \overline{p-1}\} \qquad \operatorname{ord}(\mathbb{Z}/p\mathbb{Z})^* = p - 1$$

Die Äquivalenzklasse $\overline{0}$ entspricht $p\mathbb{Z}$. Wenn p weder a noch b teilt, so ist p auch kein Teiler von $a \cdot b$.

Sei $|G| < \infty$ und $g \in G$, sodass $H := \langle g \rangle < G$. Dann folgt $|H|$ teilt $|G|$.
Wenn $\operatorname{ord}(H) = n$, ist $g^n = e$ und erst recht $g^{|G|} = e$. In einer endlichen Gruppe gilt Letzteres immer. Mithilfe dieser Identität und nachfolgendem Satz lassen sich Inverse bestimmen.

Korollar 1.9 **kleiner Satz von Fermat**
Sei $p \in \mathbb{N}$ eine Primzahl, sowie $x \in \mathbb{Z}$ sodass p kein Teiler von x ist. Dann gilt:

$$p \,|\, x^{p-1} - 1 \qquad (\Leftrightarrow \quad x^{p-1} \equiv 1 \mod p\,)$$

Die Notation $a \equiv b \mod p$ bedeutet, dass $a - b \in p\mathbb{Z}$ ist, also $p|(a-b)$ gilt. Insbesondere folgt aus $\overline{x}\,\overline{x}^{p-2} = \overline{1}$, dass $\overline{x}^{p-2}$ invers zu $\overline{x}$ ist.

Beweis :
$(\mathbb{Z}/p\mathbb{Z})^*$ ist Gruppe der Ordnung $p-1$. Aus $g^{|G|} = e$ folgt wegen $e = \overline{1}$, dass $\overline{x}^{p-1} = \overline{1}$ und somit $x^{p-1} \equiv 1 \mod p$ gilt. □

Das war ein Beispiel für die Anwendung in der Zahlentheorie. Gruppen finden sich aber auch in ganz anderen Gebieten wieder, wie zum Beispiel in der Kodierungstheorie:

Beispiel: ISBN $a_1 - a_2a_3a_4 - a_5a_7a_8a_9 - a_{10}$

Für $i \leq 9$ sind die $a_i \in \{0, \ldots, 9\}$. Die Prüfziffer $a_{10} \in \{0, \ldots, 9, x\}$ kann sogenannte einfache Fehler in der Nummer aufzeigen, das heißt ISBN erkennt, wenn ein a_i falsch ist und ist imstande unlesbare a_i zu korrigieren.

Wie funktioniert das? Wir sollten in $\mathbb{Z}/11\mathbb{Z}$ rechnen und $x = \overline{10}$ setzen, sodass die a_i für die Restklassen stehen. Man gebe $a_1, \ldots, a_9$ ein und bestimme a_{10}, sodass folgende Gleichung erfüllt ist:

$$\sum_{k=1}^{10}(11-k)a_k \equiv 0 \mod 11$$

$$\overset{\text{mod } 11}{\Longrightarrow} \quad -\sum_{k=1}^{9}\underbrace{(11-k)}_{-k}a_k = (11-10)a_{10} \qquad \Rightarrow\ a_{10} = \sum_{k=1}^{9} ka_k$$

Falls ein a_i falsch war, ist zu zeigen, dass $\sum_{k=1}^{10}(11-k)a_k \not\equiv 0$.
In $(\mathbb{Z}/11\mathbb{Z})^* = \{\overline{1}, \ldots \overline{10}\}$ existieren multiplikative Inverse. $\overline{11-k} \in (\mathbb{Z}/11\mathbb{Z})^*$. Sei (das fehlerhafte) a_i fest. Wegen $(11-k) =: x_k \in (\mathbb{Z}/11\mathbb{Z})^*$ folgt die Existenz von Inversen x_k^{-1}. Diese Zahlen sind immer gleich, und müssen daher nur einmal bestimmt werden.
In $\sum_{k=1}^{10} x_i^{-1}(11-k)a_k \equiv 0$ wird der Koeffizient vor a_i auf 1 gesetzt.
Falls die Stelle i bekannt ist, können wir a_i auf diese Weise rekonstruieren.
Ebenso folgt $\sum_k x_k a_k \not\equiv 0$, wenn ein a_i an unbekannter Stelle i falsch ist.

Gruppen mit Operationen auf Mengen

Definition 1.10
Eine (Links-) Operation einer Gruppe G auf einer Menge M ist eine Abbildung

$$\begin{aligned} G \times M &\to M \\ (g\,, m) &\mapsto gm \end{aligned}$$

mit den Eigenschaften

(O1) $(g_1 g_2)m = g_1(g_2 m)$ $\qquad \forall_{g_1, g_2 \in G\,,\, m \in M}$

(O2) $em = m$ $\qquad \forall_{m \in M}$

Beispiel:
Ein einfaches Beispiel ist $G = M$ mit $gm := g * m$ der Multiplikation in der Gruppe G. In diesem Fall wird (O1) zum Assoziativgesetz und (O2) zum Axiom des Neutralen Elements.

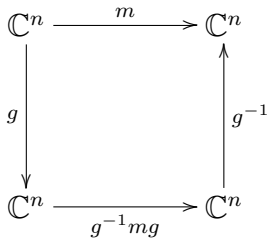
$$\begin{aligned} G \ni g\colon M &\to M \\ m &\mapsto gm \end{aligned}$$

Beispiel:
Die Linksmultiplikation mit g ist eine Abbildung $G = M \to M = G$, dazu invers ist g^{-1}. Wir finden eine Inklusion $G \subset \Sigma_{|G|} = \{\text{bij. Abb } G \to G\}$.

$G = \Sigma_n$ operiert auf $M = \{1 \dots n\}$.
Gruppenelemente g sind Abbildungen $\varphi : \{1 \dots n\} \to \{1 \dots n\}$ mit $g \cdot m = g(m)$.

Beispiel:

Sei $G = \mathrm{GL}_n(\mathbb{C})$ die Menge aller invertierbaren $n \times n$ Matrizen über $\mathbb{C}$. Ferner sei $M = \mathrm{Mat}_n(\mathbb{C})$ die Menge aller $n \times n$ Matrizen. Ein Element $m \in M$ entspricht einer linearen Abbildung $\varphi_m\colon \mathbb{C}^n \to \mathbb{C}^n$, während ein Element $g \in G$ einem Basiswechsel in $\mathbb{C}^n$ entspricht. Die Operation von G auf M schaut dann folgendermaßen aus:



$$M \ni m \mapsto g^{-1} m g \in M$$

Wir definieren hier vorläufig die Bahn $G \cdot m = \{g \cdot m\colon g \in G\}$. In der Linearen Algebra haben wir eine „Normalform“ $m' \in G \cdot m$ mit besonders einfacher Gestalt gesucht.

Beispiel:
Sei $M = \mathrm{Mat}(\ell \times m, \mathbb{C})$ und $G = \mathrm{GL}_\ell(\mathbb{C}) \times \mathrm{GL}_m(\mathbb{C})$. Wir betrachten also lineare Abbildungen $V \to U$ und jeweils einen Basiswechsel in U und V.

Elemente $(g_1, g_2) \in G$ operieren per $(g_1, g_2) \cdot m := g_1 m g_2^{-1}$ auf M. Die Normalform ist die Zeilenstufenform (vgl. Gaußelimination).

Sei M eine Menge und G eine Gruppe, welche auf M operiert. In diesem Fall schreiben wir auch $G \curvearrowright M$ und nennen M eine G-Menge. Eine typische Aufgabe ist es, die Bahnen $G \cdot m = \{gm \colon g \in G\}$ zu betrachten und deren Größe zu bestimmen. Zuvor müssen jedoch noch einige Begriffe und Definitionen festgehalten werden.

Definition 1.11 **Bahn**
Die Gruppe G operiere auf der Menge M. Für $m \in M$ heißt $G \cdot m := \{gm \colon g \in G\}$ die Bahn von m unter der Operation von G.

Definition
Die Operation einer Gruppe G auf eine Menge M heißt transitiv, wenn

$$\exists_{m \in M} \colon Gm = M \qquad \left(\Leftrightarrow \ \forall_{m_1, m_2 \in M} \exists_{g \in G} \colon gm_1 = m_2 \right)$$

Beispiel: einfachster Fall
Im Fall $G = M$ mit Operation durch *Linksmultiplikation* heißt M linksreguläre Permutationsdarstellung.

Im Fall $G = M$ mit Operation durch *Konjugation*, also $m \mapsto gmg^{-1}$ heißen die Bahnen Konjugationsklassen oder Konjugiertenklassen.

Definition
Ein $m \in M$ heißt Fixpunkt $\Leftrightarrow$ $Gm = \{m\}$ $\Leftrightarrow$ $gm = m \, \forall_{g \in G}$.

Definition **Stabilisator**
Für $m \in M$ ist der Stabilisator (auch Isotropiegruppe genannt) definiert als

$$\mathrm{Stab}_G(m) = G_m := \{g \in G \colon gm = m\}$$

Definition
Eine Operation von G auf M heißt treu, wenn die Abbildung

$$\begin{aligned} G &\to \Sigma_{|M|} \\ g &\mapsto (u_g \colon m \mapsto g(m)) \end{aligned}$$

injektiv ist. Äquivalent dazu gilt $gm = m \, \forall_{m \in M}$ nur für $g = e$.

Beispiel:
$H < G$ operiert durch Linksmultiplikation:

$$\begin{aligned} H \times G &\to G \\ (h, g) &\mapsto hg \end{aligned}$$

Die Bahnen $Hg = \{hg \colon h \in H\}$ sind Rechtsnebenklassen. Für $H \neq \{e\}$ gibt es keine Fixpunkte und keine nichttrivialen Stabilisatoren. Nach dem Satz von Lagrange 1.8 gilt $|G| = |H| \cdot [G : H]$.

Wir wollen eine ähnliche Formel für allgemeine Gruppenoperationen finden. Uns interessiert, wie groß die Bahnen sind und wie man daraus auf die Gruppenordnung schließen kann.

Proposition 1.12
Sei M eine G-Menge und $m \in M$ mit Stabilisator G_m. Dann gibt es eine Bijektion

$$p \colon G/G_m \to G \cdot m$$

Insbesondere hat die Bahn gerade so viele Elemente, wie es Linksnebenklassen gibt:

$$|G \cdot m| = [G : G_m]$$

Korollar **Klassengleichung**
Im Spezialfall $M = G$ mit Konjugationsoperation gilt:

$$|G| = |Z(G)| + \sum_{\substack{g_i \in G \\ g_i \notin Z(G)}} [G : C_G(g_i)]$$

Bemerkung: In der Klassengleichung summieren wir über ein Repräsentantensystem der nichttrivialen Bahnen von G (Länge $\neq 1$). Die Notation wird in nachfolgender Definition geklärt.

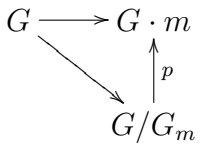
Definition
Zu einer Gruppe $G \ni g_i$ definieren wir:

$$Z(G) := \{g \colon gh = hg \,\forall_{h\in G}\} \qquad \text{das Zentrum von } G$$
$$C_G(g_i) := \{h \in G \colon hg_i = g_i h\} \qquad \text{der Zentralisator von } G$$

Für $g \in Z(G) \colon hgh^{-1} = g \;\Rightarrow\; |Gg| = 1$ einelementige Bahnen.

Beweis : Proposition 1.12
Um p zu definieren, betrachte zunächst die Abbildung

$$\begin{aligned} G &\to G \cdot m \\ g &\mapsto g \cdot m \end{aligned}$$



Es ist $g_1 m = g_2 m \;\Leftrightarrow\; g_2^{-1} g_1 m = m \;\Leftrightarrow\; g_2^{-1} g_1 \in G_m \;\Leftrightarrow\; g_1 G_m = g_2 G_m$, genau dann, wenn die Nebenklassen gleich sind. (Es kommt nicht darauf an, wo wir das g wählen.) Daher kommutiert das angegebene Diagramm, und p ist bijektiv. □

Beweis : Klassengleichung
Im Spezialfall $M = G$ mit Konjugation ist $\{ghg^{-1} \mid g \in G\}$ die Bahn von $h \in G$. Sie ist einelementig $\Leftrightarrow\; ghg^{-1} = h \,\forall_{g\in G} \;\Leftrightarrow\; gh = hg \,\forall_{g\in G} \;\Leftrightarrow\; h \in Z(G)$. Also entsprechen Elemente in $Z(G)$ den einelementigen Bahnen und G zerfällt disjunkt in $G = Z(G) \,\dot\cup\, \{\text{alle anderen Bahnen}\}$.

Wähle daher Repräsentanten $g_i \notin Z(G)$. Wie wir oben gesehen haben, gibt es eine Bijektion zwischen der Bahn von g_i und G/G_{g_i}.

Es verbleibt $G_{g_i} = C_G(g_i)$ zu zeigen. Dies folgt aus der Definition des Stabilisators:

$$G_{g_i} = \{g \in G \colon gg_i g^{-1} = g_i\} = \{g \in G \colon gg_i = g_i g\} = C_G(g_i)$$

□

Seien p, q Primzahlen und $d, e \in \mathbb{N}$. Wir stellen uns folgende Fragen:

1. $\text{ord}(G) = p \quad \Rightarrow\; G$ abelsch? Ja.
2. $\text{ord}(G) = p^2 \quad \Rightarrow\; G$ abelsch? Ja.
3. $\text{ord}(G) = p \cdot q \quad \Rightarrow\; G$ abelsch? Nein.
4. $\text{ord}(G) = d \cdot e \quad \Rightarrow\; \exists_{H<G}\, \text{ord}(H) = d$? Nein.

Zur 1. Frage:

Sei $\mathrm{ord}(G) = p$ und $g \in G \setminus \{e\}$. Sei ferner $G > H = \langle g \rangle$ zyklisch. Wegen $\overbrace{\mathrm{ord}(H)}^{\neq 1} \mid \overbrace{\mathrm{ord}(G)}^{=p}$ folgt $\mathrm{ord}(H) = p = \mathrm{ord}(G)$ und daher $H = G$. Also ist G zyklisch und damit abelsch. Wegen $\mathrm{ord}(g) = \mathrm{ord}(H) = p$ gilt zudem $G \simeq \mathbb{Z}/p\mathbb{Z}$.

Zur 3. Frage:

Als Gegenbeispiel dient die nicht abelsche Gruppe $G = \Sigma_3$, deren Ordnung dennoch Produkt zweier Primzahlen ist: $\mathrm{ord}(G) = 3! = 2 \cdot 3$

Zur 4. Frage: Betrachte die Teilmenge

$$\Sigma_4 \supset A_4 = \{\text{gerade Permutationen}\} = \{\sigma \in \Sigma_4 \colon \operatorname{sgn}(\sigma) = 1\}$$

Es ist $|A_4| = 12$, aber A_4 hat keine Untergruppe der Ordung 6.

Neue Frage: $p^\ell \,|\, \mathrm{ord}(G) \;\Rightarrow\; \exists_{H<G}$ mit $\mathrm{ord}(H) = p^\ell$? Dies werden wir im Rahmen des Sylow-Theorems 1.18 beantworten.

Die Antwort auf die 2. Frage gibt folgende Proposition:

Proposition 1.13
Sei G eine Gruppe mit $\mathrm{ord}(G) \in \{p, p^2\}$, wobei p eine Primzahl sei.
Dann ist G abelsch.

Beweis :
Sei $\mathrm{ord}(G) = p^2$. Zu zeigen ist $G = Z(G)$.

Wegen $Z(G) < G$ gilt $\mathrm{ord}(Z(G)) \in \{1, p, p^2\}$. Außerdem ist $Z(G)$ normal in G, da für $h \in Z(G)$ und $g \in G$ folgt, dass $ghg^{-1} = hgg^{-1} = h \in Z(G)$. Also ist $G/Z(G)$ eine Gruppe mit Ordnung $1, p$ oder p^2. Die Klassengleichung besagt:

$$|G| = |Z(G)| + \sum_{\substack{\text{Repräs.} \\ g_i}} [G : \underbrace{C_G(g_i)}_{\{g \colon gg_i = g_i g\} \leq G}]$$

$$\Rightarrow\; \mathrm{ord}(C_G(g_i)) \in \{1, p\} \;\Rightarrow\; [G \colon C_G(g_i)] = \tfrac{|G|}{|C_G(g_i)|} \in \{p^2, p\}.$$

Da p sowohl $|G|$ als auch alle $[G \colon C_G(g_i)]$ teilt, folgt zudem $p \,|\, \mathrm{ord}(Z(G))$ und damit $\mathrm{ord}(Z(G)) \in \{p, p^2\}$. Wenn wir $\mathrm{ord}(Z(G)) = p^2$ folgern können, sind wir fertig. Nehmen wir also an, dass $\mathrm{ord}(G/Z(G)) = p$ sei. Dann ist aber $G/Z(G) \simeq \mathbb{Z}/p\mathbb{Z}$ zyklisch von Ordnung p, also $G/Z(G) \simeq \langle \overline{g} \rangle$ für ein $g \in G$ mit $\overline{g} = gZ(G)$ und $\mathrm{ord}(\overline{g}) = p$.

Seien $a, b \in G$. Wir werden $ab = ba$ und damit einen Widerspruch zur Annahme $\mathrm{ord}(G/Z(G)) = p$ folgern. Nach obiger Überlegung existieren $k, \ell \in \mathbb{Z}$, sodass $aZ(G) = \overline{a} = g^k Z(G)$ und $bZ(G) = \overline{b} = g^\ell Z(G)$. Ferner gilt $\overline{a}\overline{b} = \overline{b}\overline{a}$, da $G/Z(G)$ abelsch ist. Aus $a \in aZ(G) = g^k Z(G)$ folgt $a = g^k z_1$ für ein $z_1 \in Z(G)$ und analog $b = g^\ell z_2$ für ein $z_2 \in Z(G)$.

$$ab = (g^k z_1)(g^\ell z_2) = g^k g^\ell z_1 z_2 = g^{k+\ell} z_1 z_2$$
$$ba = (g^\ell z_2)(g^k z_1) = g^{k+\ell} z_2 z_1$$

□

Definition 1.14
Sei G eine Gruppe mit $\text{ord}(G) = p^m$, wobei p eine Primzahl und $m \in \mathbb{N}_0$ sei.
Dann heißt G eine p-Gruppe.

Für $|G| = p^m \cdot q$ mit $\text{ggT}(p, q) = 1$ (also p, q teilerfremd) stellt sich die Frage, ob ein $H < G$ mit $\text{ord}(H) = p^m$ existiert und ob $p | \text{ord}(G)$ die Existenz eines $H < G$ mit $|H| = p$ impliziert.

Definition
Es sei G eine Gruppe mit $|G| = p^m q$, wobei $\text{ggT}(p, q) = 1$ und $H < G$ mit $|H| = p^m$ gelte. Dann heißt H eine p-Sylowuntergruppe von G.

Theorem 1.15 **Cauchy**
Sei G eine endliche Gruppe und p eine Primzahl, welche die Gruppenordnung teilt. Dann existiert ein $g \in G$ mit $\text{ord}(\langle g \rangle) = \text{ord}(g) = p$.

Also ist $H := \langle g \rangle < G$ eine Untergruppe mit Ordnung p und es gilt $H \simeq \mathbb{Z}/p\mathbb{Z}$.

Für zyklische oder abelsche Gruppen ist diese Aussage bekannt, das heißt den ersten Beweisschritt haben wir im Grunde schon gemacht. Wie oben ist auch hier der Weg über Quotientengruppen sinnvoll. Der Beweis läuft induktiv.

Beweis :
1. Fall: G zyklisch, $p | \text{ord}(G)$. Aus Proposition 1.6 folgt die Existenz einer zyklischen Untergruppe $H < G$ mit $\text{ord}\, H = p$. Also ist $H = \langle g \rangle$ mit $g \in G$ und $\text{ord}(g) = p$.

2. Fall: G abelsch. Dann ist G ein Produkt von zyklischer Gruppen, nach der Klassifikation der endlich erzeugten abelschen Gruppen. Alternativ wird der Beweis direkt per Induktion nach $|G|$ geführt:

Für $|G| = 1$ ist nichts zu zeigen, für $|G| = 2$ ist die Aussage trivial. Angenommen, die Behauptung gelte für Gruppen der Ordnung $< |G|$. Betrachte die von $e \neq h \in G$ erzeugte zyklische Untergruppe $\langle h \rangle < G$. Falls $p | \text{ord}(h)$ folgt gemäß dem 1. Fall die Existenz einer zyklischen Untergruppe $H < \langle h \rangle < G$ der Ordnung $|H| = p$. Falls $p \nmid \text{ord}(h)$ betrachte $G/\langle h \rangle$. Wegen $p | |G| = |\langle h \rangle| \cdot [G : \langle h \rangle]$ (Satz von Lagrange 1.8) gilt $p | |G/\langle h \rangle|$. Da $|G/\langle h \rangle| < |G|$, enthält $G/\langle h \rangle$ nach Induktionsannahme ein Element $\overline{g} = g\langle h \rangle$ mit $\text{ord}(\overline{g}) = p$. Wir definieren $\text{ord}(g) =: n$ und möchten $p | n$ zeigen, damit wieder der 1. Fall anwendbar wird. Da G abelsch ist, gilt tatsächlich

$$\overline{g}^n = (g\langle h \rangle)^n = g^n \langle h \rangle = \langle h \rangle = \overline{e} \;\Rightarrow\; p | n$$

3. Fall: G beliebig, also nicht notwendigerweise abelsch. Falls eine echte Untergruppe $H \lneq G$ mit $p \mid \operatorname{ord}(H)$ existiert, funktioniert die Induktion analog zum 2. Fall. Falls hingegen $\forall_{H \lneq G}\colon p \nmid \operatorname{ord}(H)$ ist die Induktion nicht anwendbar. Wir nutzten stattdessen die Klassengleichung aus: $|G| = |Z(G)| + \sum_{g_i \notin Z(G)} [G : C_G(g_i)]$

Falls $p \mid \operatorname{ord}(C_G(g_i))$ sind wir wieder fertig, da $C_G(g_i) \lneq G$. Es verbleibt der Fall $p \nmid \operatorname{ord}(C_G(g_i))\, \forall_i$. Aus $[G : C_G(g_i)] = \frac{|G|}{|C_G(g_i)|}$ folgt $p \mid [G : C_G(g_i)]$. Aus der Klassengleichung lesen wir ab, dass dann auch $|Z(G)|$ von p geteilt wird. Folglich ist $Z(G) = G$, das heißt, es liegt der oben behandelte abelsche Fall vor. □

Bemerkung: Das Interessante an diesem Satz ist, dass keine weiteren Voraussetzungen an die Gruppe gestellt werden, als dass die Ordnung von einer Primzahl geteilt wird.

Korollar 1.16

Sei G eine endliche Gruppe und p eine Primzahl. Dann ist G ist eine p-Gruppe genau dann, wenn $\forall_{g \in G}\, \exists_{n \in \mathbb{N}_0}\colon \operatorname{ord}(g) = p^n$.

Das heißt, wir können lokal an den Elementen sehen, ob eine G eine p-Gruppe ist.

Beweis :

Sei G eine p-Gruppe mit $g \in G$. Diese Richtung ist einfach: Für $H := \langle g \rangle$ ist $\operatorname{ord}(g) = \operatorname{ord}(H)$, welche bekanntlich die Gruppenordnung $\operatorname{ord}(G)$ teilt.

Sei umgekehrt $G \neq \{e\}$ keine p-Gruppe. Dann teilt eine Primzahl $q \neq p$ die Gruppenordnung. Aus dem Satz von Cauchy 1.15 folgt: $\exists_{g \in G}\colon \operatorname{ord}(g) = q$. □

Proposition 1.17

Sei p eine Primzahl und G eine p-Gruppe.

(a) Wenn G auf einer endlichen Menge X operiert, gilt: $\left|X^G\right| \equiv |X| \mod p$
Dabei steht X^G für die Menge aller Fixpunkte.

(b) $G \neq \{e\} \Rightarrow Z(G) \neq \{e\}$. Das Zentrum nichttrivialer Gruppen ist nichttrivial.

Beweis :

(a) Zu zeigen ist $p \mid \left|X \setminus X^G\right|$. Ist $x \in X \setminus X^G$, existiert ein $g \in G$ mit $gx \neq x$. Folglich gilt $[G : G_x] \neq 1$ für den Stabilisator $G_x \lneq G$. Nach dem Satz 1.8 von Lagrange gilt $p \mid [G : G_x]$, da G eine p-Gruppe ist. Außerdem ist $|G \cdot x| = [G : G_x]$. Wegen $X \setminus X^G = \dot\cup\,$(Bahnen der Nichtfixpunkte) und $p \mid |\text{Bahn}|$ folgt $p \mid \left|X \setminus X^G\right|$.

(b) Sei $X = G$ und G operiere via Konjugation. Dann gilt:
$$X^G = Z(G) \Rightarrow p \mid \operatorname{ord}(Z(G)) \Rightarrow Z(G) \neq \{e\}$$ □

Nun kommt das Hauptergebnis dieser Theorie.

Theorem 1.18 **Sylow**
Sei G eine Gruppe und p eine Primzahl. Wir schreiben die Gruppenordnung $\mathrm{ord}(G) = p^m \cdot q$ als Produkt mit $\mathrm{ggT}(p,q) = 1$.

(a) Zu allen Teilern von p^m gibt es Untergruppen entsprechender Ordnung:

$$\forall_{1\le k\le m}\, \exists_{H<G} \text{ mit } |H| = p^k$$

(b) Sei S eine p-Sylowuntergruppe von G, das heißt $|S| = p^m$. Ist $H < G$ irgendeine p-Gruppe, folgt $\exists_{g\in G}\colon H < gSg^{-1}$ (Letzteres ist auch eine Sylowuntergruppe).

(c) Sei s_0 die Anzahl aller p-Sylowuntergruppen von G. $\Rightarrow$ $s_0 | q$ und $s_0 \equiv 1 \mod p$.

Wieder überrascht, dass *keine* Voraussetzungen an die Gruppe gestellt werden, aber dennoch extrem starke Aussagen folgen. Der Beweis wird natürlich einiges an Arbeit erfordern.

Beweis :
Der Fall $m = 0$ ist uninteressant, muss aber dennoch behandelt werden. Wegen $p \nmid \mathrm{ord}(G)$ ist bei (a) nichts zu beweisen. Bei (b) ist die p-Sylowgruppe einelementig, folglich ist auch $H = \{e\}$. Aus $s_0 = 1$ folgt (c). Sei im Folgenden $m > 0$.

(a) Beweis per Induktion nach $|G|$. Sei $X = G$ mit Operation durch Konjugation. Die Klassengleichung sagt $|G| = |Z(G)| + \sum_{g_i \notin Z(G)} [G : C_G(g_i)]$.

Erster Fall: $p \nmid \mathrm{ord}(Z(G))$. Dann existiert ein g_i, sodass $p \nmid [G : C_G(g_i)]$.

Wegen $|G| = p^m q$ und $[G : C_G(g_i)] = \frac{|G|}{|C_G(g_i)|}$ folgt $p^m \,|\, |C_G(g_i)|$ und $C_G(g_i) \lneq G$. Es ist wieder Induktion anwendbar; die gesuchten H existieren schon in $C_G(g_i)$.

Zweiter Fall: $p \,|\, \mathrm{ord}(Z(G))$.

Der Satz 1.15 von Cauchy besagt die Existenz eines $g \in Z(G)$ mit $\mathrm{ord}(g) = p$. Wir betrachten die Untergruppe $H := \langle g\rangle < G$ der Ordnung p.

$H < Z(G) \Rightarrow H \trianglelefteq G \Rightarrow \forall_{x\in G}\colon xHx^{-1} = H$, denn $Z(G) \ni xgx^{-1} = g$.

Der surjektive Gruppenhomomorphismus $\pi\colon G \to G/H$ hat $\ker\pi = H$. Ferner ist $|G/H| = \frac{|G|}{|H|} = \frac{p^m q}{p} = p^{m-1}q$. Induktiv folgt $\forall_{k\le m-1}\, \exists_{J_k<G/H}$ mit $\mathrm{ord}(J_k) = p^k$. Es gilt $\pi^{-1}(J_k) < G$ und $\mathrm{ord}(\pi^{-1}(J_k)) = \underbrace{|\ker\pi|}_{=p} \cdot |J_k| = p^{k+1}$, weil $J_k = \frac{\pi(\pi^{-1}(J_k))}{\ker\pi}$.

$\Rightarrow \forall_{k\le m-1}\colon |\pi^{-1}(J_k)| = p^{k+1}$.

(b) Sei S eine p-Sylowuntergruppe (deren Existenz in (a) gezeigt wurde) und $H < G$ eine p-Gruppe. Als Menge wähle $M = G/S = \{gS\colon g \in G\}$ die Nebenklassen von S. Die Gruppe G operiere durch Linksmultiplikation auf M. Dann kann aber (erst recht) auch H auf M operieren. Der Vorteil von H ist, dass es eine p-Gruppe

ist. Der Stabilisator ist S selbst, daher ist

$$|M| = [G : S] = \frac{|G|}{|S|} = q \qquad \left|M^H\right| \overset{1.17}{\equiv} |M| \mod p$$

$$p \nmid q \;\Rightarrow\; q \not\equiv 0 \mod p \qquad \Rightarrow \qquad \left|M^H\right| \not\equiv 0 \mod p \qquad \Rightarrow \qquad M^H \neq \emptyset$$

Das klingt jetzt nicht aufregend, ist aber genau das, was wir brauchen. Es folgt die Existenz eines Fixpunktes $gS \in M^H$ mit $hgS = gS \,\forall_{h\in H} \;\Rightarrow\; g^{-1}hgS = S \,\forall_{h\in H}$. Das sieht schon besser aus, denn es folgt $g^{-1}hg \in S \,\forall_{h\in H} \;\Rightarrow\; h \in gSg^{-1} \,\forall_{h\in H}$ und damit $H < gSg^{-1}$.

Der wesentliche Trick war, sich obige Operation auf $M = G/S$ auszusuchen und zu zeigen, dass es einen Fixpunkt gibt.

S ist p-Sylow $\;\Rightarrow\;$ gSg^{-1} ist auch p-Sylow. H ist p-Sylow $\;\Rightarrow\;$ $H = gSg^{-1}$, das heißt alle p-Sylowuntergruppen sind zueinander konjugiert und alle p-Untergruppen von G sind in p-Sylowuntergruppen enthalten. Abschließend möchten wir noch eine Formel zum Zählen der p-Sylowuntergruppen haben.

(c) $s_0 := \#\{p\text{-Sylowuntergruppen von } G\}$. Sei S eine p-Sylowuntergruppe und M die Menge aller p-Sylowuntergruppen von G. Für $H \in M \;\Rightarrow\; gHg^{-1} \in M$, wir lassen G also durch Konjugation auf M operieren. Wir wissen überdies, dass es nur eine einzige Bahn gibt. Betrachte $|M| = \frac{|G|}{|G_S|}$.

Der Stabilisator $G_S = \mathrm{Stab}_G(S) = \{g \in G \colon gSg^{-1} = S\} =: N_G(S)$ heißt (hier) Normalisator von S und ist die größte Untergruppe von G, für die S normal ist.

$$S \trianglelefteq N_G(S) = G_S$$

$$s_0 := |M| = \frac{|G|}{|G_S|} = [G : G_S] \quad \text{Zu zeigen ist } s_0 | q.$$

$$S < G_S < G \qquad\qquad S \text{ hat } p^m \text{ viele Elemente, bei } G \text{ sind es } p^m q.$$

$$[G : S] = q = \underbrace{[G : G_S]}_{=\frac{|G|}{|G_S|}} \cdot \underbrace{[G_S : S]}_{\frac{|G_S|}{|S|}} \qquad \Rightarrow\; s_0 = [G : G_S] \text{ teilt } q.$$

Strategie für die zweite Aussage $s_0 \equiv 1 \mod p$:

Sei M die Menge aller p-Sylowuntergruppen von G. Auf M operiere die (feste) p-Sylowgruppe S durch Konjugation. S ist eine p-Gruppe ($|S| = p^m$), also kann Proposition 1.17 (a) angewendet werden: $s_0 = |M| \equiv \left|M^S\right| \mod p \overset{!}{=} 1$. Zu zeigen ist also $M^S = \{S\}$.

Wie man sieht, ist

$$S' \in M \;\Leftrightarrow\; \forall_{g\in S} \colon gS'g^{-1} = S' \;\Rightarrow\; S \subset N_G(S') = \{g \in G \colon gS'g^{-1} = S'\}.$$

Wir zeigen und benutzen allgemeiner das folgende Lemma:

Lemma
Wenn S' eine p-Sylow und H eine p-Gruppe mit $H \subset N_G(S')$ ist, folgt $H \subset S'$.

In unserem Fall setzen wir $H := S \;\Rightarrow\; S \subset S'$. Wegen $|S| = |S'|$ folgt dann sofort $S = S'$ und wir sind fertig.

Beweis : Lemma
Es ist $S' \subset N_G(S')$ und sogar $S' \trianglelefteq N_G(S')$. Betrachte für $H \subset N_G(S')$ die von H und S' erzeugte Untergruppe

$$\langle H, S' \rangle \ni h_1 s_1 \, h_2 s_2 \ldots h_n s_n \overset{(*)}{=} hs \qquad \text{mit } h, h_j \in H \text{ und } s, s_j \in S'$$
$$\Rightarrow\; \langle H, S' \rangle = HS' = \{hs \colon h \in H, s \in S'\}$$

Die Gleichheit $(*)$ gilt, da wegen $H \subset N_G(S')$ sofort $hS' = S'h \quad \forall_{h \in H}$ folgt. Also ist $S' < HS' \subset N_G(S') \;\Rightarrow\; S' \trianglelefteq HS'$. Aufgrund der Normalteilereigenschaft ist HS'/S' eine Gruppe. Wir wollen über deren Elementezahl die geforderte Aussage zeigen. Betrachte den wegen $hsS' = hS'$ surjektiven Gruppenhomomorphismus

$$\begin{aligned} \varphi \colon H &\to HS'/S' \\ h &\mapsto hS' \end{aligned}$$

HS'/S' ist Quotient von H. Der Kern des Homomorphismus ist

$$\ker \varphi = \{h \in H \colon hS' = eS' \;\Leftrightarrow\; h \in S'\} = H \cap S'$$

Daher gilt: $$|\langle H, S' \rangle| = \underbrace{|HS'|}_{<|G|=p^n q} = \underbrace{|S'|}_{p^n} \cdot \underbrace{\frac{|H|}{|H \cap S'|}}_{p^k \text{ für ein } k \geq 0}$$

Da jedoch p^n maximal ist, muss $k = 0$ sein, woraus schließlich $H = H \cap S' \;\Rightarrow\; H \subset S'$ folgt, was zu beweisen war.

□

Der Beweis war sehr trickreich, hat sich aber gelohnt, wie wir gleich sehen werden.

Korollar 1.19
Alle p-Sylowuntergruppen sind zueinander konjugiert.

Korollar 1.20
Seien p, q Primzahlen mit $p < q$ und $p \nmid (q-1)$. Sei ferner G eine Gruppe der Ordnung $p \cdot q$. Dann gilt

$$G \simeq \mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

G ist also insbesondere zyklisch und abelsch.

Bemerkung: Für $G = \Sigma_3$ ist $|G| = 2 \cdot 3$, aber G ist nicht abelsch. Daher ist $p \nmid (q-1)$ eine nötige Voraussetzung.

Beweis :

$$\exists P \quad p\text{-Sylow}, |P| = p \quad \Rightarrow \; P \simeq \mathbb{Z}/p\mathbb{Z}. \qquad s := \#\{p\text{-Sylow}\} \; \Rightarrow \; s|q, s = 1 \mod p$$
$$\exists Q \quad q\text{-Sylow}, |Q| = q \quad \Rightarrow \; Q \simeq \mathbb{Z}/q\mathbb{Z}. \qquad r := \#\{q\text{-Sylow}\} \; \Rightarrow \; r|p, r = 1 \mod q$$

Zum einen gilt $s \in \{1, q\}$ und zum anderen $s \in \{1, p+1, 2p+1, \ldots\}$. Angenommen, $q = \ell p + 1 \;\Rightarrow\; q - 1 = \ell p \;\Rightarrow\; p|(q-1)$, ein Widerspruch zur Voraussetzung. $\Rightarrow\; s = 1$.

Analog gilt $r \in \{1, p\}$ und $r \in \{1, q+1, 2q+1, \ldots\}$. Wegen $p < q$ folgt sofort $r = 1$.

$$P \text{ eindeutige } p\text{-Sylow} \quad \Rightarrow \; gPg^{-1} = P \;\; \forall_{g \in G}.$$
$$Q \text{ eindeutige } q\text{-Sylow} \quad \Rightarrow \; gQg^{-1} = Q \;\; \forall_{g \in G}.$$

Zu zeigen ist $P \times Q \subset G$ und $P \cap Q = \{e\}$. Mit $x := (x, 1) \in P \times Q \ni (1, y) =: y$ ist also $xy = yx$ für $x \in P, y \in Q$ zu zeigen. Für $x, y \neq e$ gilt:

$$xy = \overbrace{xyx^{-1}}^{\in xQx^{-1} = Q} x = y^a x \qquad \text{für ein } a, \text{ da die Gruppe } Q \text{ zyklisch ist.}$$
$$xy = y \underbrace{y^{-1}xy}_{\in y^{-1}Py = P} = yx^c \qquad \text{für ein } c$$

In $xy = y^a x$ ist $a = 1$ zu zeigen.

$$\begin{aligned} y^a &= xy = yx^c \\ &\Rightarrow \; y^a x = yx^{c-1} \\ \Rightarrow \; Q &\ni y^{a-1} = x^{c-1} \in P \\ &\Rightarrow \; a = 1 = c \qquad \text{,wegen } P \cap Q = \{e\} \\ &\Rightarrow \; xy = yx \end{aligned}$$

$P \times Q \subset G, |P \times Q| = pq = |G| \;\Rightarrow\; G = P \times Q.$

□

Wie man sieht, sind die Sylowsätze ein wesentliches Hilfsmittel.

2 Ringe

Definition 2.1 **Ring**

Ein Ring $(R, +, \cdot)$ ist eine Menge R mit zwei Abbildungen

$$+\colon R \times R \to R \qquad \cdot\colon R \times R \to R$$
$$(a, b) \mapsto a + b \qquad (a, b) \mapsto a \cdot b$$

sodass folgende Axiome gelten:

(R1) $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0 und Inversen $-a$ zu a.

(R2) Die Abbildung $\cdot$ ist assoziativ sowie distributiv bezüglich $+$.
Ferner existiert ein neutrales Element 1 bezüglich der Multiplikation.

$\forall_{a,b,c \in R}$	$a(bc) = (ab)c$	Assoziativität
$\forall_{a,b,c \in R}$	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$	Distributivität
$\exists_{1 \in R} \forall_{a \in R}$	$a \cdot 1 = a = 1 \cdot a$	Wir verlangen $0 \neq 1$.

Ein Ring R heißt kommutativ, wenn $\forall_{a,b \in R}\ a \cdot b = b \cdot a$ gilt.

Definition

Seien R und S Ringe. Eine Abbildung $\varphi\colon R \to S$ heißt Ringhomomorphismus, wenn $\varphi\colon (R, +) \to (S, +)$ ein Homomorphismus abelscher Gruppen ist.

$$\forall_{a,b \in R} \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$
$$\varphi(1_R) = 1_S$$

Beispiel: Ringe

- $\{0\}$ ist kein Ring, da kein Einselement vorhanden ist. $0 \cdot a$ ist tatsächlich gleich 0, denn $0 \cdot a = (0 + 0)a = 0 \cdot a + 0 \cdot a \ \Rightarrow\ 0 = 0 \cdot a$.
- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ und $\big(\mathrm{Mat}(n \times n, \mathbb{Q}), +, \cdot\big)$ sind Ringe. Letzterer ist für $n \geq 2$ nicht kommutativ.
- $\mathbb{Q}[x] = \left\{ f(x) = \sum_{i=1}^{n} a_i x^i, a_i \in \mathbb{Q} \right\}$ ist ein Ring.

  Addition und Multiplikation werden im Bild definiert. Allgemein seien für offenes $U \subset \mathbb{R}^n$ und stetiges $f\colon U \to \mathbb{R}$ die Verknüpfungen definiert als:

  $$f + g\colon x \mapsto f(x) + g(x) \qquad f \cdot g\colon x \mapsto f(x)g(x)$$

- Die Menge aller Gruppenhomomorphismen $\mathrm{Hom}(G,G)$ für eine abelsche Gruppe G bildet einen Ring.
- $R=\{0,1\}$ mit folgenden Verknüpfungen

$\cdot$	0	1
0	0	0
1	0	1

$+$	0	1
0	0	1
1	1	0

ist ein Ring, nämlich der Quotientenring $\mathbb{Z}/2\mathbb{Z}$ von $(\mathbb{Z},+,\cdot)$.

Definition 2.2
Sei $(R,+,\cdot)$ ein Ring und $I\subset R$ eine Untergruppe von $(R,+)$.

I heißt Linksideal von R $\Leftrightarrow$ $\forall_{x\in I,a\in R}\colon ax\in I$.

I heißt Rechtsideal von R $\Leftrightarrow$ $\forall_{x\in I,a\in R}\colon xa\in I$.

I heißt (zweiseitiges) Ideal $\Leftrightarrow$ I ist Links- und Rechtsideal (Analogon zum Normalteiler).

Beispiel: Ideale

- Das Nullideal $I=\{0\}$ erfüllt die Idealeigenschaften trivialerweise.
- $I=n\mathbb{Z}$ ist ein Ideal von $\mathbb{Z}$.

Proposition 2.3
Sei R ein Ring und $I\neq R$ ein Ideal. Die Faktorgruppe R/I heißt Restklassenring und ist ein Ring mit (wohldefinierter) Multiplikation

$$(x+I)(y+I):=xy+I$$

Beweis :

Es ist nur die Wohldefiniertheit zu zeigen: Für $\overbrace{x+I=x'+I}^{\Rightarrow x-x'\in I}$ und $\overbrace{y+I=y'+I}^{\Rightarrow y-y'\in I}$ muss $xy+I=x'y'+I$ folgen:

$$xy-x'y'=xy-x'y'+x'y-x'y=\underbrace{\overbrace{(x-x')}^{\in I}y}_{\Rightarrow\in I}+\underbrace{x'\overbrace{(y-y')}^{\in I}}_{\Rightarrow\in I}\in I$$

□

$\left(R\setminus\{0\},\cdot\right)$ ist im Allgemeinen keine Gruppe. Ein Gegenbeispiel ist $\mathbb{Z}/n\mathbb{Z}$, wo $n=a\cdot b$ im Allgemeinen nicht invertierbar ist.

Definition 2.4 Einheiten
Sei R ein Ring. Betrachte die Menge der invertierbaren Elemente

$$R^* := \{x \in R \colon x \text{ invertierbar bezüglich } \cdot\} = \{x \in R \colon \exists_{y \in R} : xy = 1 = yx\}$$

Die Elemente von R^* heißen Einheiten in R. Die Menge R^* heißt die Einheitengruppe von R.

Beispiel: Einheitengruppen

$$\mathbb{Z}^* = \{\pm 1\} \qquad \mathbb{Q}^* = \mathbb{Q} \setminus \{0\} \qquad \mathbb{R}^* = \mathbb{R} \setminus \{0\} \qquad (\mathbb{Z}/6\mathbb{Z})^* = \{\overline{1}, \overline{5}\}$$

Definition
Falls $R^* = R \setminus \{0\}$ ist, heißt der Ring R Schiefkörper oder Divisionsring. Ein kommutativer Schiefkörper heißt Körper.

Beispiel: Polynomring
Betrachte $R = K[x]$, wobei K ein Körper ist. Was ist dann die Einheitengruppe?
Für $f(x) \in R^* \Rightarrow \exists_{g(x)} \colon f(x)g(x) = 1$. Ausgeschrieben ist

$$\begin{aligned} f(x) &= a_0 + a_1 x + \ldots + a_n x^n & a_n \neq 0 \\ g(x) &= b_0 + b_1 x + \ldots + b_\ell x^\ell & b_\ell \neq 0 \end{aligned}$$

$$\begin{aligned} f(x)g(x) &= a_n b_\ell x^{n+\ell} + \text{ Terme kleineren Grades} \\ &\stackrel{!}{=} 1 = 1 + 0x + 0x^2 \ldots \end{aligned}$$

$$a_n b_\ell \neq 0 \Rightarrow n + \ell = 0 \Rightarrow n = \ell = 0 \Rightarrow f(x) = a_0$$
$$\Rightarrow R^* = K \setminus \{0\}$$

Wir setzen ab sofort voraus, dass R ein kommutativer Ring ist. Interessant sind dann

- Körper
- Polynomringe
- ganze Zahlen
- algebraische Geometrie: Statt $y = x^2$ betrachte $K[x, y]/\langle y - x^2 \rangle$.

Proposition 2.5
Sei R ein Ring. Dann sind äquivalent:

(a) R ist ein Körper.

(b) R hat genau zwei Ideale: $\{0\}$ und R.

(c) Für jeden Ring S ist jeder Ringhomomorphismus $R \to S$ injektiv. (Ein solcher ist niemals die Nullabbildung, da wir $1 \neq 0$ gefordert haben.)

Beweis :

(a) $\Rightarrow$ (b) Für einen Körper R und ein Ideal $\{0\} \neq I < R$ ist $I = R$ zu zeigen. Sei $0 \neq x \in I$. Da R ein Körper ist, findet sich ein multiplikatives Inverses $x^{-1} \in R$. Es folgt $x^{-1}x = 1 \in I$. Damit gilt $\forall_{y \in R}\colon y \cdot 1 = y \in I$, also $I = R$.

(b) $\Rightarrow$ (c) Sei $\varphi\colon R \to S$ ein Ringhomomorphismus. Zu zeigen ist $\ker(\varphi) = \{0\}$. Da $\ker\varphi$ ein Ideal in R ist, folgt $\ker\varphi \in \{\{0\}, R\}$. Wegen $\varphi(1_R) = 1_S$ ist $1_R \notin \ker\varphi$, folglich ist $\ker\varphi \neq R$ und damit gleich $\{0\}$.

(c) $\Rightarrow$ (a) Sei $R \ni x \neq 0$. Die Menge $Rx = \{rx\colon r \in R\} = xR = RxR \neq \{0\}$ ist ein Ideal in R. Falls $xR = R \;\Rightarrow\; 1 \in Rx \;\Rightarrow\; \exists_{r \in R}\colon 1 = rx$, also $r = x^{-1}$. Die Restklassenabbildung $R \to R/I = S$ ist ein Ringhomomorpismus, wenn $I \neq R$ ein Ideal ist. Dieser kann aber im Fall $I \neq \{0\}$ nicht injektiv sein, woraus sich für $I = Rx \neq R$ ein Widerspruch ergibt. □

Definition 2.6 **Nullteiler**
Sei R ein Ring. Ein Element $a \in R$ heißt Nullteiler $:\Leftrightarrow\; \exists_{b \in R\setminus\{0\}}\colon ab = 0$.
R heißt Integritätsbereich, wenn 0 der einzige Nullteiler in R ist.

Beispiel:
Für $R = \mathbb{Z}/6\mathbb{Z}$ sind $\overline{0}, \overline{2}, \overline{3}, \overline{4}$ Nullteiler. $\mathbb{Z}$, ein Körper K sowie der entsprechende Polynomring $K[x]$ sind Beispiele für Integritätsbereiche.

Definition 2.7
Sei R ein Ring und I ein Ideal in R.

I heißt Hauptideal $:\Leftrightarrow\; \exists_{a \in R}\colon I = Ra$.

R heißt Hauptidealring genau dann, wenn jedes Ideal ein Hauptideal ist.

I heißt Primideal $:\Leftrightarrow\; I \neq R$ und $\forall_{a,b \in R}\colon a \cdot b \in I \;\Rightarrow\; \{a, b\} \cap I \neq \emptyset$.

I heißt maximales Ideal $:\Leftrightarrow\; I \neq R$ und $\forall_{J \text{ Ideal in R}}$ mit $I \subset J \subset R \;\Rightarrow\; J \in \{I, R\}$.

- $I = \{0\} = R \cdot 0$ und $I = R = R \cdot 1$ sind Hauptideale.
- R Körper $\Rightarrow$ R Hauptidealring.
- R Körper $\Leftrightarrow$ $I = \{0\}$ maximal.
- I maximal $\Leftrightarrow$ R/I ist ein Körper:

  Mithilfe der Quotientenabbildung $R \xrightarrow{\pi} R/I$ lassen sich Ideale J von R auf Ideale J/I von R/I übertragen.

  $$I \subset J \subset R \quad \longleftrightarrow \quad \overbrace{I/I}^{\{0\}} \subset J/I \subset R/I$$

  Nach Proposition 2.5 ist die Körpereigenschaft äquivalent dazu, dass R/I nur die beiden Ideale $\{0\}$ und R/I hat.

- I ist Primideal $\Leftrightarrow$ R/I ist Integritätsbereich. Beweis:

"$\Rightarrow$" Für $\overline{a}, \overline{b} \in R/I$ ist $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{0} \Leftrightarrow a \cdot b \in I$. Da I Primideal, ist $a \in I$ oder $b \in I$. Daraus folgt $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$, also ist R/I Integritätsbereich.

"$\Leftarrow$" Für $a, b \in R$ folgt aus $a \cdot b \in I$, dass $\overline{a} \cdot \overline{b} = \overline{0}$. Da R/I Integritätsbereich ist, folgt $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$, also $a \in I$ oder $b \in I$ und damit die Primidealeigenschaft.

- I maximales Ideal $\Rightarrow$ R/I Körper $\Rightarrow$ R/I Integritätsbereich $\Rightarrow$ I Primideal.

  Die Umkehrung gilt nicht, denn $I = \{0\} \subset \mathbb{Z}$ ist Primideal, aber nicht maximal.

Beispiel: $R = \mathbb{Z}$

Die Ideale sind genau die $n\mathbb{Z}$ mit $n \in \mathbb{N}_0$. Dies sind alles Hauptideale. Welche sind Primideale und welche sind maximal? Betrachte dazu $I = n\mathbb{Z}$ und $R/I = \mathbb{Z}/n\mathbb{Z}$.

Fall 1: $n = p$ prim. Dann ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper, also auch ein Integritätsbereich. $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, also ist $p\mathbb{Z}$ ein Primideal und ein maximales Ideal.

Fall 2: n nicht prim. $\Rightarrow$ $n = a \cdot b$ mit $a, b \neq 1$. In $\mathbb{Z}/n\mathbb{Z}$ gilt dann $\overline{0} = \overline{n} = \overline{ab} = \overline{a}\overline{b}$ mit $\overline{0} \neq \overline{a}, \overline{b}$ $\Rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ ist kein Integritätsbereich und kein Körper $\Rightarrow$ $n\mathbb{Z}$ ist weder Primideal, noch maximales Ideal.

Also gilt: $n\mathbb{Z}$ Primideal $\Leftrightarrow$ $\pm n$ Primzahl.

Fall 3: $n = 0$. Dann ist $0\mathbb{Z} = \{0\}$ und $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$ ein Integritätsbereich, aber kein Körper. $\Rightarrow$ $0\mathbb{Z}$ ist Primideal aber kein maximales Ideal.

Beispiel: $R = \mathbb{Z}[x]$

Der Polynomring in einer Variablen über $\mathbb{Z}$ ist kein Hauptidealring. Betrachte dazu $I = \langle 2, x \rangle = \{a_0 + a_1 x + \ldots : a_i \in \mathbb{Z}\ ,\ 2 | a_0\}$ und zeige, dass es kein Hauptideal ist.

Gegenannahme: $\exists_{f(x) \in \mathbb{Z}[X]} \colon I = \langle f(x) \rangle = Rf(x)$

$2 \in I \Rightarrow \exists_{g(x) \in \mathbb{Z}[x]} \colon f(x)g(x) = 2$

bekanntlich gilt: $\deg(fg) = \deg(f) + \deg(g)$

$\deg(2) = 0 \Rightarrow f(x) \in \mathbb{Z}$. genauer: $f(x) \in \{\pm 1, \pm 2\}$

$x \in I \Rightarrow \exists_{h(x) \in \mathbb{Z}[x]} \colon f(x)h(x) = x \Rightarrow f(x) \neq \pm 2$

$\Rightarrow f(x) = \pm 1$, Widerspruch zu $I \neq R$

Wir möchten im Folgenden zeigen, dass $K[x]$ ein Hauptidealring ist, wenn K ein Körper ist. Dazu soll zunächst das Prinzip der Division mit Rest auf $K[x]$ übertragen werden.

Definition 2.8
Ein Integritätsbereich R heißt euklidisch $:\Leftrightarrow$ $\exists$ Gradabbildung $\lambda\colon R\setminus\{0\}\to\mathbb{N}_0$, sodass $\forall_{a\in R,b\in R\setminus\{0\}}\colon \exists_{q,r\in R}$ mit $a=qb+r$ und $r=0$ oder $\lambda(r)<\lambda(b)$.

Theorem 2.9
Sei R euklidisch. Dann ist R ein Hauptidealring.

Beweis :
Sei $\{0\}\neq I<R$ ein Ideal. Also gibt es ein $0\neq x\in I$. Damit ist die Menge der Grade $\{\lambda(x)\colon x\in I\setminus\{0\}\}$ nichtleer und besitzt ein minimales Element: $\exists_{x_0\in I}\colon \lambda(x_0)=\min\{\lambda(x)\colon x\in I\setminus\{0\}\}$. Wir zeigen, dass $I=\langle x_0\rangle=Rx_0=x_0R$ gilt, woraus folgt, dass I ein Hauptideal ist.

Sei $y\in I$. Dann ist $y=qx_0+r$ mit $r=0$ oder $\lambda(r)<\lambda(x_0)$. Da aber $\lambda(x_0)$ minimal ist, folgt aus $r=y-qx_0\in I$, dass $r=0$ und damit $y=qx_0$ gelten muss. Daraus folgt $I=Rx_0$. □

Beispiel: $R=\mathbb{Z}$, $\lambda(x):=|x|$
Division mit Rest wie üblich. Also ist $\mathbb{Z}$ ein euklidischer Ring, was nicht weiter überrascht, da die Definition gerade so gewählt war, dass $\mathbb{Z}$ ein euklidischer Ring wird.

Proposition 2.10
Sei K ein Körper. Dann ist der Polynomring in einer Variablen $K[x]$ ein euklidischer Ring, also auch ein Hauptidealring.

Um dies nachzuweisen, muss eine Gradabbildung wie oben angegeben werden. Ein Polynom hat aber bereits einen „Grad“, also probieren wir doch diesen.

Beweis :
Der Grad eines Polynoms $f(x)=a_0+a_1x+\ldots+a_nx^n$ mit $a_n\neq 0$ sei $\deg(f(x))=\lambda(f(x))=n$. Zu zeigen ist, dass die Division mit Rest $(f=q\cdot g+r)$ funktioniert.

Seien $K[X]\ni f,g\neq 0$.

Falls $\lambda(f)<\lambda(g)$, folgt $r=f$ und damit auch $\lambda(r)<\lambda(g)$.

Falls $\lambda(f)\geq\lambda(g)$, wende Induktion nach $\lambda(f)$ an. Der Fall $\lambda(f)=0$ passt, da durch

Skalare dividiert werden kann. Es verbleibt $\lambda(f) \geq 1$ zu behandeln. Betrachte dazu:

$f(x) = a_0 + a_1 x + \ldots + a_n x^n$

$g(x) = b_0 + b_1 x + \ldots + b_\ell x^\ell \qquad b_\ell \neq 0$

Wegen $n \geq \ell$ hat das Polynom $g(x) \cdot x^{n-\ell} \frac{a_n}{b_\ell}$ den Höchstkoeffizient a_n im Grad n.

Daher gilt $\deg\Big(\overbrace{f(x) - x^{n-\ell}\frac{a_n}{b_\ell} g(x)}^{h}\Big) < n = \lambda(f)$. Induktiv folgt $h = qg + r$ mit $r = 0$ oder $\lambda(r) < \lambda(g)$. Damit folgt schließlich

$$f = x^{n-\ell}\frac{a_n}{b_\ell} g + (qg + r) = \Big(x^{n-\ell}\frac{a_n}{b_\ell} + q\Big)g + r \qquad \text{mit } r = 0 \text{ oder } \lambda(r) < \lambda(g).$$

Also sind Ideale $I \neq 0$ in $K[x]$ von der Form $I = \langle f(x) \rangle$, wobei $f(x)$ ein (bis auf skalare Vielfache eindeutiges) Polynom kleinsten Grades in I ist. □

Beispiel: Der Ring der ganzen Gaußschen Zahlen

Die Menge $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ ist ein Ring mit den üblichen Verknüpfungen.

$(a + bi) + (c + di) = (a + c) + (b + d)i$

$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$

Proposition 2.11

Der Ring $\mathbb{Z}[i]$ ist ein euklidischer Ring, also ein Hauptidealring.

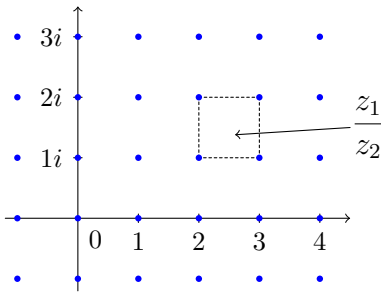
Beweis :

Wir können nicht einfach den (i.A. nicht ganzzahligen) Betrag der komplexen Zahl als Gradabbildung nehmen. Definiere stattdessen für $z \in \mathbb{C}$ die Norm $N(z)$ als $N(z) = |z|^2 = z\bar{z}$, woraus für $\mathbb{Z}[i] \ni z = a + bi$ folgt, dass $N(z) = (a + bi)(a - bi) = a^2 + b^2 \in \mathbb{N}_0$ ist. Setze also $\lambda(z) = N(z)$ für $z \neq 0$. Wir wollen damit die Division mit Rest von $z_1 = a + bi$ und $z_2 = c + di \neq 0$ durchführen.

$$\mathbb{C} \ni \frac{z_1}{z_2} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{\cdots}{c^2 + d^2}$$

hat rationale Koordinaten und liegt in einem Quadrat mit Ecken in $\mathbb{Z}[i]$. Es existiert also ein $q \in \mathbb{Z}[i]$, sodass $\left|\frac{z_1}{z_2} - q\right| \leq \frac{\sqrt{2}}{2}$.

Die Norm ist multiplikativ: $N(z_3 z_4) = N(z_3) N(z_4)$.



$$z_1 = z_2 q + \overbrace{(z_1 - z_2 q)}^{r}$$

$$N(z_1 - z_2 q) = N(z_2) \underbrace{N\Big(\frac{z_1}{z_2} - q\Big)}_{\leq \frac{1}{2}} < N(z_2) \qquad \Rightarrow \lambda(r) = N(r) < N(z_2) = \lambda(z_2)$$

oder $r = 0$

□

Definition 2.12

Sei R ein Integritätsbereich, $p \in R$, $p \neq 0$ und $p \notin R^*$.

p heißt irreduzibel: $\Leftrightarrow \ \forall_{x,y \in R}\colon p = xy \ \Rightarrow \ \{x, y\} \cap R^* \neq \emptyset$. Sonst heißt p reduzibel.

p heißt prim oder Primelement: $\Leftrightarrow \ \forall_{x,y \in R}\colon p|xy \ \Rightarrow \ p|x$ oder $p|y$

$\Leftrightarrow \ \langle p \rangle$ ist ein Primideal.

Lemma

In einem Integritätsbereich gilt die Implikation p prim $\Rightarrow$ p irreduzibel.
Die Umkehrung gilt im Allgemeinen nicht.

Beweis :

Sei $p = xy$, also $p|xy$. OBdA gelte $p|x$, woraus $x = pc$ für ein $c \in R$ folgt. Dann ist aber $p = xy = pcy$ und damit $0 = p - pcy = p(1 - cy)$. Da R ein Integritätsbereich ist, gibt es keine Nullteiler, woraus $1 - cy = 0$ also $cy = 1$ und schließlich $c, y \in R^*$ folgt. Also ist insbesondere y eine Einheit und p damit irreduzibel. □

Proposition 2.13

Sei R ein Hauptidealring (und Integritätsbereich). Sei $p \in R$, $p \notin R^*$ und $p \neq 0$. Dann sind äquivalent:

(I) p ist irreduzibel

(II) p ist prim

(III) $\langle p \rangle$ ist ein maximales Ideal

Beweis :

Wir haben gesehen, dass $\langle p \rangle$ maximal $\Rightarrow$ $\langle p \rangle$ Primideal $\Rightarrow$ p prim $\Rightarrow$ p irreduzibel gilt, also (III) $\Rightarrow$ (II) $\Rightarrow$ (I). Es verbleibt (I) $\Rightarrow$ (III) zu zeigen.

Sei $\langle p \rangle \subset I \subset R$, wobei I ein Ideal ist. Zu zeigen ist $I \in \{\langle p \rangle, R\}$. Da R ein Hauptidealring ist, folgt die Existenz eines $a \in R$ mit $I = \langle a \rangle \ \Rightarrow \ p \in \langle a \rangle \ \Rightarrow \ \exists_{b \in R}\colon p = ab$. Da p irreduzibel ist, muss einer der Faktoren eine Einheit sein. Falls $a \in R^*$ folgt $\langle a \rangle = R$. Falls $b \in R^* \ \Rightarrow \ a = pb^{-1} \ \Rightarrow \ a \in \langle p \rangle$ folgt $\langle a \rangle = \langle p \rangle$. □

Unser nächstes Ziel ist es, die Existenz und Eindeutigkeit (bis auf Reihenfolge und Einheiten) von Primfaktorzerlegungen zu zeigen.

Lemma 2.14
Sei R ein Hauptidealring. Dann ist R noethersch, das heißt für alle aufsteigenden Ketten von Idealen $\langle a_1\rangle \subset \langle a_2\rangle \subset \ldots \subset \langle a_n\rangle \ldots$ existiert ein $N \in \mathbb{N}$, sodass $\langle a_N\rangle = \langle a_{N+1}\rangle = \ldots$ gilt.

Beweis :
$I := \bigcup_n \langle a_n\rangle$ ist ein Ideal in R.
$\Rightarrow \exists_{b\in R}\colon I = \langle b\rangle \Rightarrow \exists_{N\in\mathbb{N}}\colon b \in \langle a_N\rangle \Rightarrow I = Rb = \langle a_N\rangle$ □

Theorem 2.15
Sei R ein Hauptidealring (und Integritätsbereich), $a \in R$, $a \neq 0$ und $a \notin R^*$. Dann ist a ein Produkt von Primelementen. Diese Zerlegung ist eindeutig bis auf Reihenfolge und Einheiten. Also ist R ein faktorieller Ring, das heißt, es gibt eine eindeutige Primfaktorzerlegung.

Beweis :
Falls a irreduzibel, ist a prim. Falls a reduzibel, ist $a = a_1a_2$. Falls a_1 und a_2 irreduzibel, sind wir fertig. Andernfalls ist $a = a_1'a_2'a_3'$ usw.

Nach Lemma 2.14 bricht die aufsteigende Kette $\langle a\rangle \subsetneq \left\langle \frac{a}{a_1}\right\rangle \subsetneq \left\langle \frac{a}{a_1a_2}\right\rangle \subsetneq \ldots$ ab. Folglich ist a ein endliches Produkt von irreduziblen Elementen, woraus die Existenz der Primfaktorzerlegung folgt.

Es verbleibt die Eindeutigkeit zu zeigen. Sei $a = p_1\cdots p_n = q_1\cdots q_\ell$ mit p_i, q_i prim. $q_1|a \overset{\text{z.B.}}{\Longrightarrow} q_1|p_1 \Rightarrow q_1 = p_1\varepsilon_1$ mit $\varepsilon_1 \in R^*$. $\Rightarrow p_2\cdots p_n = \varepsilon_1 q_2\cdots q_\ell$ usw. Es folgt $n = \ell$ und $p_i = \varepsilon_i q_i$ mit $\varepsilon_i \in R^*$ bis auf Anordnung. □

Beispiel: In $K[x]$ irreduzible Polynome

- $(x-\lambda)$ ist irreduzibel in $K[x]$.
- x^2+1 ist irreduzibel in $\mathbb{R}[x]$ (da $x-i$ Primfaktor in $\mathbb{C}[x]$).
- x^2-2 ist irreduzibel in $\mathbb{Q}[x]$ (da $x-\sqrt{2}$ Primfaktor in $\mathbb{R}[x]$).

Wie man sieht, hängt es wesentlich vom Körper ab, welche Polynome irreduzibel sind.

Beispiel:
Ist in $\mathbb{Z}[i]$ die Zahl 5 eine Primzahl? Nein, da $5 = (1+2i)(1-2i)$. Sind dies Primfaktoren? Ja, denn $N(1\pm 2i) = 5$. Da die Norm multiplikativ ist, würde eine weitere Faktorisierung von $(1\pm 2i)$ eine weitere Faktorisierung der Zahl 5 bedeuten.

Im Folgenden sei R immer ein kommutativer Ring und Prim(R) ein Repräsentantensystem von Primelementen (modulo Einheiten).

Definition
Ein Integritätsbereich R heißt faktorieller Ring:

$\Leftrightarrow \quad \forall_{0\neq a\in R\setminus R^*} \quad a = \prod p_i \quad$ mit p_i prim

$\Leftrightarrow \quad \forall_{0\neq a\in R\setminus R^*} \quad a = \prod f_i \quad$ eindeutig, f_i irreduzibel.

Beispiel: Ist $\mathbb{Z}[\sqrt{-5}]$ faktoriell?
Nein, denn wir finden ein Element, welches irreduzibel aber nicht prim ist. Betrachte dazu zuächst die Elemente 2, 3 und $(1\pm\sqrt{-5})$ und deren Normen 4, 9 und 6. Angenommen $2 = ab$. Wegen $N(2) = 4$ folgt $N(a)|4$ und $N(b)|4$. Sei $a = x+y\sqrt{-5}$ und $b = u+v\sqrt{-5}$. Dann ist $N(a) = x^2+5y^2$ und $N(b) = u^2+5v^2$. Daraus folgt $y = v = 0$, also ist 2 irreduzibel. Gleiches folgt auch für die anderen Zahlen analog. Andererseits ist $2\cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$. Wäre 2 prim, würde OBdA $2|(1+\sqrt{-5})$ folgen. Dann existiert aber ein $z\in\mathbb{Z}[\sqrt{-5}]$ sodass $2z = 1+\sqrt{-5} \;\Rightarrow\; z = \frac{1}{2}+\frac{1}{2}\sqrt{-5} \notin \mathbb{Z}[\sqrt{-5}]$, woraus sich ein Widerspruch ergibt.

Fragen:

- Ist $K[x]$ ein faktorieller Ring? (K sei ein Körper)
- Ist $K[x,y]$ faktoriell? Es ist kein Hauptidealring, betrachte etwa $I = \langle x, y\rangle$.
- Ist $\mathbb{Z}[x]$ faktoriell? Auch dies ist kein Hauptidealring, betrachte etwa $I = \langle 2, x\rangle$.

Alle drei Fragen werden wir bejahen.

Satz 2.16 Gauß
Sei R ein faktorieller Ring. Dann ist $R[x]$ ein faktorieller Ring.

Der Beweis benötigt einiges an Vorbereitung.

Definition Quotientenkörper
Sei R ein Integritätsbereich. Dann existiert der Körper der Brüche $Q(R)$, welcher genauso konstruiert wird, wie $\mathbb{Q}$ aus $\mathbb{Z}$ hervorgeht.

$$Q(R) := \left\{ \frac{a}{b} \,\middle|\, a,b\in R, b\neq 0 \right\}$$

Addition und Multiplikation werden wie in $\mathbb{Q}$ definiert, und es gelte die „Kürzungsrelation“ $\frac{a}{b}\sim\frac{c}{d} \;\Leftrightarrow\; ad = bc$. Dies ist eine Äquivalenzrelation, da aufgrund der Nullteilerfreiheit $\frac{a}{b} = \frac{ac}{bc}$ gilt.

$Q(R)$ ist ein Körper, $R\subseteq Q(R)$ ein Teilring.

Definition
Sei R faktoriell, $a, b \in R$ und $p_i \in \mathrm{Prim}(R)$. Dann ist

$$a = \varepsilon' \, p_1^{a_1} \cdots p_n^{a_n} \qquad \varepsilon', \varepsilon'' \in R^*$$
$$b = \varepsilon'' \, p_1^{b_1} \cdots p_n^{b_n} \qquad a_i, b_i \in \mathbb{N}_0$$
$$\frac{a}{b} = \varepsilon \, p_1^{c_1} \cdots p_n^{c_n} \qquad c_i = a_i - b_i \in \mathbb{Z}$$
$$\frac{a}{b} = \varepsilon \prod_{p \in \mathrm{Prim}(R)} p^{\nu_p} \qquad \nu_p = \nu_p(\tfrac{a}{b}) \in \mathbb{Z}$$

Setze formal $\nu_p(0) = \infty$, da $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ gelten soll.

Wir erweitern die Definition auf den Polynomring über den Quotientenkörper

$$Q(R)[x] \ni f = \sum_i a_i x^i \quad \text{mit } a_i \in Q(R) \qquad \nu_p(f) := \min(\nu_p(a_i))$$

Bemerkung: Für alle $p \in \mathrm{Prim}(R)$ gilt

$$f = 0 \Leftrightarrow \nu_p(f) = \infty \qquad f \in R[x] \Leftrightarrow \nu_p(f) \geq 0$$

Proposition 2.17 **Lemma von Gauß**
Sei R faktoriell, $p \in \mathrm{Prim}(R)$ und $f, g \in Q(R)[x]$. Dann gilt $\nu_p(fg) = \nu_p(f) + \nu_p(g)$.

Beweis :
Für $f, g \in R$ ist die Aussage klar, genauso für $f, g \in Q(R)$ beziehungsweise für $f \in Q(R)$ und $g \in Q(R)[x]$, da Polynome immer mit einer „ganzen Zahl“ aus R multipliziert werden können.

Schwieriger ist der Fall $f, g \in Q(R)[x]$. Die Koeffizienten sind hier alles Brüche in $Q(R)$. Wegen obiger Überlegung können wir mit dem Hauptnenner h der Koeffizienten durchmultiplizieren, weshalb OBdA $f, g \in R[x]$ gilt.

$$\nu_p((h_1 f)(h_2 g)) = \nu_p((h_1 h_2)(fg)) = \nu_p(h_1 h_2) + \nu_p(fg) \overset{!}{=} \nu_p(h_1 f) + \nu_p(h_2 g)$$

Da entsprechend durchmultipliziert werden kann, gilt OBdA $\nu_p(f) = \nu_p(g) = 0$.

Zu zeigen ist $\nu_p(fg) = 0$. Als faktorieller Ring ist R und damit auch R/pR ein Integritätsbereich. Daraus folgt, dass auch $(R/pR)[x]$ ein Integritätsbereich ist.

Die (kanonische) Abbildung $R[x] \to R[x]/pR[x]$ ist ein Ringhomomorphismus mit Kern $\{h \in R[x] \mid \nu_p(h) > 0\}$. Nach obiger Überlegung liegen f, g nicht im Kern. Aus $\overline{f}, \overline{g} \neq 0$ folgt $(\overline{f})(\overline{g}) \neq 0$, da wir uns in einem Integritätsbereich aufhalten. Aus $(\overline{f})(\overline{g}) = \overline{f \cdot g}$ folgt schließlich $\nu_p(fg) = 0$. □

Definition
Das Polynom $f(x) = \sum_{i=0}^{n} a_i x^i$ heißt normiert, wenn $a_n = 1$.

Für normierte Polynome in $R[x]$ ist die Primfaktorzerlegung über $R[x]$ und $Q(R)[x]$ identisch.

Korollar 2.18
Sei R ein faktorieller Ring, $h \in R[x]$ normiert und $h = fg$ mit normierten $f, g \in Q(R)[x]$. Dann ist $f, g \in R[x]$.

Beweis :
$h \in R[x]$ ist normiert, also ist $\nu_p(h(x)) = 0 \, \forall_{p \in \mathrm{Prim}(R)}$, da mindestens einer der Koeffizienten 1 ist. Für $f, g \in Q(R)[x]$ ist $\nu_p(f), \nu_p(g) \leq 0$, da Brüche als Koeffizienten auftreten können. Aus dem Lemma von Gauß 2.17 folgt:

$$0 = \nu_p(h) = \nu_p(fg) = \nu_p(f) + \nu_p(g) \;\Rightarrow\; \nu_p(f) = \nu_p(g) = 0 \;\Rightarrow\; f, g \in R[x]$$

□

Definition
Polynome $f \in R[x]$, für die $\nu_p(f) = 0$ gilt, heißen primitiv.

Normierte Polynome sind automatisch primitiv. Man überlegt sich außerdem leicht, dass ein Polynom ist genau dann primitiv ist, wenn der größte gemeinsame Teiler aller Koeffizienten eins ist.

$$g \in Q(R)[x] \;\Rightarrow\; a = \prod_{p \in \mathrm{Prim}(R)} p^{\nu_p(g)} \in Q(R) \quad \text{und } g = af \text{ mit primitivem } f \in R[x]$$

Wir beweisen jetzt den bereits formulierten Satz 2.16 von Gauß, also

$$R \text{ faktoriell} \;\Rightarrow\; R[x] \text{ faktoriell.}$$

Beweis : **Satz von Gauß**
Wir zeigen zunächst, dass ein Element $q \in R[x]$ prim in $R[x]$ ist, wenn eine der folgenden Aussagen zutrifft:

(I) q ist Primelement in R

(II) q ist Primelement in $Q(R)[x]$ und q ist primitiv in $R[x]$

Insbesondere gilt $q \in R[x]$ primitiv, q prim in $R[x] \Leftrightarrow q$ prim in $Q(R)[x]$.

Sei q wie in (I) $\Rightarrow$ R/qR ist Integritätsbereich $\Rightarrow$ $R[x]/qR[x]$ ist Integritätsbereich $\Rightarrow$ q prim in $R[x]$.

Sei q wie in (II), $f, g \in R[x] \subset Q(R)[x] \Rightarrow q$ prim in $R[x]$ mit $q|fg \Rightarrow$ OBdA $q|f$ in $Q(R)[x] \Rightarrow \exists_{h \in Q(R)[x]} f = q \cdot h$.

Aus dem Lemma von Gauß folgt: $\forall_{p \in \mathrm{Prim}(R)} 0 \leq \nu_p(f) = \overbrace{\nu_p(q)}^{=0} + \nu_p(h) \Rightarrow h \in R[x] \Rightarrow q|f$ in $R[x] \Rightarrow q$ prim in $R[x]$.

Jetzt zeigen wir, dass wenn $f \in R[x]$ ungleich Null und keine Einheit ist, es sich als Produkt von Primelementen der Form (I) oder (II) schreiben lässt. Daraus folgt, dass es keine anderen Primelemente gibt und dass jedes Element, das nicht Null und keine Einheit ist, in ein Produkt von Primelementen zerlegbar ist.

Schreibe $f = a\tilde{f}$ mit $a \in R$ und $\tilde{f} \in R[x]$ primitiv (der ggT der Koeffizienten von $\tilde{f}$ ist also eine Einheit). $a \in R$ hat nach Voraussetzung eine eindeutige Primfaktorzerlegung in R (vom Typ (I)). $Q(R)[x]$ ist faktoriell ($Q(R)$ ist ein Körper), also hat $\tilde{f}$ eine Zerlegung $\tilde{f} = \tilde{f}_1 \cdots \tilde{f}_n \, c$ mit $c \in Q(R)^*$, sodass die Faktoren $\tilde{f}_1 \cdots \tilde{f}_n$ primitiv und in $R[x]$ sind. Die $\tilde{f}_i$ sind Primelemente in $Q(R)[x]$, also vom Typ (II).

Zu zeigen ist $c \in R^*$. Berechne $\nu_p(c)$ für jedes Primelement p in R mithilfe des Lemmas von Gauß:

$$
\begin{aligned}
\nu_p(\tilde{f}) &= \nu_p(\tilde{f}_1) + \ldots + \nu_p(\tilde{f}_n) + \nu_p(c) \\
\nu_p(\tilde{f}) &= 0 \quad \text{, da } \tilde{f} \in R[x] \text{ primitiv} \\
\nu_p(\tilde{f}_i) &= 0 \quad \text{analog} \\
\Rightarrow \nu_p(c) &= 0 \Rightarrow \quad p \text{ teilt weder Zähler noch Nenner von } c, \text{ also } c \in R^*
\end{aligned}
$$

□

3 Körper

Wir betrachten polynomiale Gleichungen über K, etwa $f(x) = x^2 + 1$ für $K = \mathbb{R}$. Da die Primfaktorzerlegung in $\mathbb{C}[x]$ einerseits eindeutig ist, andererseits aber $(x \pm i) \notin \mathbb{R}[x]$ gilt, ist $f(x)$ irreduzibel in $\mathbb{R}[x]$. Genauso ist für $K = \mathbb{Q}$ die Gleichung $g(x) = x^2 - 2$ irreduzibel in $\mathbb{Q}[x]$.

Wir konstruieren $L := \mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \,\big|\, a, b \in \mathbb{Q}\}$. Diese Menge bildet einen Ring:

$$\begin{aligned}(a + b\sqrt{2}\,) + (c + d\sqrt{2}\,) &= (a + c) + (b + d)\sqrt{2} && \in \mathbb{Q}[\sqrt{2}]\\ (a + b\sqrt{2}\,)(c + d\sqrt{2}\,) &= (ac + 2bd) + (ad + bc)\sqrt{2} && \in \mathbb{Q}[\sqrt{2}]\end{aligned}$$

Existiert $0 \neq (a + b\sqrt{2})^{-1}$ in $\mathbb{Q}[\sqrt{2}]$? In folgenden Spezialfälle ist dies klar:

$$a = 0 \;\Rightarrow\; b\sqrt{2} \cdot \frac{1}{2b}\sqrt{2} = 1 \qquad\qquad b = 0 \;\Rightarrow\; a \cdot \frac{1}{a} = 1$$

Allgemein muss das Inverse $(c + d\sqrt{2}) = (a + b\sqrt{2})^{-1}$ die Gleichungen $ac + 2bd = 1$ und $ad + bc = 0$ erfüllen. Daraus folgt

$$c = -\frac{ad}{b} \;\Rightarrow\; -\frac{a^2 d}{b} + 2bd = 1 \;\Rightarrow\; -a^2 d + 2b^2 d = b \;\Rightarrow\; d = \frac{b}{2b^2 - a^2} \;\Rightarrow\; \exists_{c,d \in \mathbb{Q}}.$$

Da wir in $\mathbb{Q}$ sind, ist der Nenner $2b^2 - a^2 \neq 0$, da sonst $a^2 = 2b^2 \;\Rightarrow\; \left(\frac{a}{b}\right)^2 = 2$.

Bemerkung: $\sqrt{2} \notin \mathbb{Q}$
Angenommen $\frac{a}{b} = \frac{p}{q}$ mit $p, q \in \mathbb{Z} \;\Rightarrow\; p^2 = 2q^2$ mit $\mathrm{ggT}(p, q) = 1$. Dann gilt aber $p^2 = 2q^2 \;\Rightarrow\; 2|p^2 \;\Rightarrow\; p$ gerade $\;\Rightarrow\; 4|p^2 \;\Rightarrow\; 4|2q^2 \;\Rightarrow\; 2|q^2 \;\Rightarrow\; q$ gerade. ↯

Damit wird $\mathbb{Q}[\sqrt{2}]$ zu einem Körper. Ebenso $\mathbb{R}[i] = \mathbb{C}$ mit $i = \sqrt{-1}$.

Definition 3.1
Sei L ein Körper.

Ein Teilring $K \subset L$ heißt Teilkörper von L: $\Leftrightarrow\; \forall_{a \in K \setminus \{0\}} : a^{-1} \in K$.
L heißt dann Erweiterungskörper von K. Die Inklusion $K \subset L$ heißt Körpererweiterung.

Ein Körper K' mit $K \subset K' \subset L$ heißt Zwischenkörper der Körpererweiterung L/K.
Sei $M \subset L$ eine Teilmenge. Der kleinste Teilkörper von L, welcher M enthält, heißt der von M erzeugte Teilkörper von L und wird mit $T(M)$ bezeichnet:

$$T(M) := \bigcap_{T \supset M} T \qquad\qquad \text{wobei } T \text{ Teilkörper von } L \text{ ist.}$$

Sei $M \subset L$ eine Teilmenge und $K \subset L$ ein Teilkörper. Dann wird $T(M \cup K)$ mit $K(M)$ bezeichnet. Man sagt, dass $K(M)$ aus K durch Adjunktion von M entsteht. Im Fall $M = \{a_1, \ldots, a_n\}$ schreiben wir $K(M) = K(a_1, \ldots, a_n)$. Falls $L = K(a_1, \ldots, a_n)$ für $a_i \in L$ ist, heißt L endlich erzeugt über K. Die Körpererweiterung L/K heißt einfach oder einfache Erweiterung: $\Leftrightarrow\; \exists_{a \in L} : L = K(a)$.

Es gilt die Implikation: L/K Körpererweiterung $\Rightarrow$ L ist ein K-Vektorraum.

Definition 3.2
Sei L/K eine Körpererweiterung. Die Vektorraum-Dimension

$$\dim_K L =: [L : K]$$

heißt der Grad der Körpererweiterung. Die Erweiterung L/K heißt endlich, wenn $[L : K] < \infty$.

Beispiel:
Der Grad einer Körpererweiterung bestimmt diese keineswegs eindeutig:

$$\left[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\right] = 2 = \left[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}\right] = \left[\mathbb{C} : \mathbb{R}\right]$$

Lemma 3.3 **Gradformel**
Seien M/L und L/K Körpererweiterungen. Dann gilt für die Grade:

$$[M : K] = [M : L] \cdot [L : K]$$

Beweis :
$M \supset L \supset K$

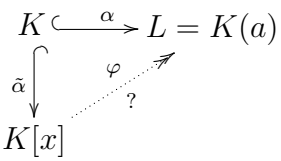
$$\begin{array}{rll} [M : L] = a & M \simeq L^a \text{ als } L\text{-Vektorraum} & \Rightarrow\ M \simeq L^a \text{ als } K\text{-VR} \\ [L : K] = b & L \simeq K^b \text{ als } K\text{-Vektorraum} & \\ \Rightarrow\ M \simeq L^a \simeq (K^b)^a & \text{als } K\text{-Vektorraum} & \end{array}$$

□

Wie konstruiert man Lösungen einer polynomialen Gleichung?

Gegeben sei ein Polynom $f(x) \in K[x]$. Lässt sich eine Körpererweiterung L/K finden, sodass $f(x)$ in L eine Nullstelle hat? Sind also polynomiale Gleichungen immer lösbar? Woher bekommen wir a im Fall $L = K(a)$?

Die Idee ist L als Quotienten von $K[x]$ zu produzieren. Sei α die Inklusionsabbildung.



Wir suchen eine Abbildung $\varphi(\overset{K}{\cup}\lambda) = \lambda$ mit $\varphi(x) \overset{!}{=} a$. Falls φ existiert, ist $K(a)$ der Quotient von $K[x]$.

Proposition 3.4
Seien R und S Ringe, $\alpha\colon R \to S$ ein Ringhomomorphismus und $a \in S$. Dann gibt es genau einen Ringhomomorphismus $\varphi\colon R[x] \to S$ mit $\varphi|_R = \alpha$ und $\varphi(x) = a$. Wir nennen φ Auswertungshomomorphismus.

Beweis :
Falls φ existiert, bildet es $R[x] \ni f(x) = \sum_{i=0}^{n} r_i x^i$ mit $r_i \in R$ ab auf

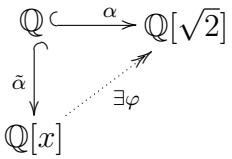
$$\varphi\Big(f(x)\Big) = \varphi\Big(\sum_{i=0}^{n} r_i x^i\Big) = \sum_{i=0}^{n} \underbrace{\varphi(r_i)}_{\alpha(r_i)} \underbrace{\varphi(x)^i}_{a^i} = \sum_{i=0}^{n} \alpha(r_i)\, a^i.$$

Ein auf diese Weise definiertes φ ist offensichtlich additiv und multiplikativ, denn $\varphi(x^i x^j) = a^{i+j} = \varphi(x^i)\varphi(x^j)$. Außerdem ist auch

$$\varphi(r) = \alpha(r) \text{ für } r \in R \quad \Rightarrow \quad \varphi(1) = \alpha(1) = 1 \quad \Rightarrow \quad \varphi(x) = a$$

□

Beispiel:



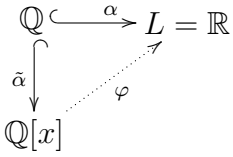
Betrachte die Ringe $\mathbb{Q}$ und $\mathbb{Q}[\sqrt{2}] = \{c + d\sqrt{2} \,|\, c, d \in \mathbb{Q}\}$. Dann existiert nach Proposition 3.4 genau ein Auswertungshomomorphismus:

$$\begin{aligned} \varphi\colon \mathbb{Q}[x] &\to \mathbb{Q}[\sqrt{2}] \\ f(x) &\mapsto f(a) && \text{wähle } a = \sqrt{2} \\ c + d\cdot x &\mapsto c + d\cdot\sqrt{2} && \Rightarrow \varphi \text{ surjektiv} \end{aligned}$$

Die wie oben definierte Abbildung φ ist ein surjektiver Ringhomomorphismus. Dann ist das Bild von φ isomorph zum Urbild modulo Kern. Nach Proposition 2.10 ist $\mathbb{Q}[x]$ ein Hauptidealring, da $\mathbb{Q}$ ein Körper ist. Der Kern ist ein Ideal und wird daher von einem Polynom $f(x) \in \ker(\varphi)$ minimalen Grades erzeugt: $\ker(\varphi) = \langle f(x)\rangle$. Offensichtlich liegt $f(x) = x^2 - 2$ im Kern, ist irreduzibel, und erzeugt daher den Kern von φ. Daraus folgt die Isomorphie $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[x]/\langle x^2 - 2\rangle$. Erstaunlicherweise existiert die rechte Seite dabei „unabhängig von $\sqrt{2}$“. Die Zahl $\sqrt{2}$ muss aber offenbar die Restklasse $\overline{x}$ von x sein, denn $\overline{x^2 - 2} = 0$.

Beispiel: $f(x) = x^2 + 1$ $\qquad \mathbb{R}[i] \simeq \mathbb{C} \simeq \mathbb{R}[x]/\langle x^2 + 1\rangle$

Beispiel: Der Auswertungshomomorphismus ist im Allgemeinen nicht surjektiv. Wähle dazu $a = \pi$ in folgendem Beispiel:



$\varphi\colon \sum r_i\, x^i \mapsto \sum r_i\, \pi^i$ ist nicht surjektiv. Wäre etwa π^{-1} im Bild, würde aus $\pi^{-1} = \varphi(f(x)) = \sum_{i=0}^{n} r_i \pi^i$ folgen, dass π die Gleichung $1 = \sum r_i x^{i+1}$ über $\mathbb{Q}$ löst, und das stimmt nicht.

Definition 3.5
Sei L/K eine Körpererweiterung mit der Inklusion $\alpha\colon K \to L$ und dem Auswertungshomomorphismus $\varphi\colon K[x] \to L$, so dass $a = \varphi(x) \in L$.

Wenn φ injektiv ist, heißt a transzendent. Sonst heißt a algebraisch (oder algebraisch abhängig) über K.

Falls a algebraisch ist, heißt das Polynom $f(x) \in K[x] \setminus \{0\}$ minimalen Grades mit $f(a) = 0$ das Minimalpolynom von a über K und wird mit $m_a = m_{a,K}$ bezeichnet.

Es gilt: a transzendent $\Leftrightarrow$ a erfüllt keine algebraische Gleichung.

Das Minimalpolynom ist als Erzeuger des Hauptideals $\ker(\varphi) = \langle m_a \rangle$ bis auf skalare Vielfache eindeutig.

Wir erinnern daran, dass für $K \subset L \ni a$ der kleinster Teilkörper von L, der $K \cup \{a\}$ enthält, mit $K(a)$ bezeichnet wird.

Das Bild von $\varphi\colon K[x] \to L$, also „Polynome ausgewertet in a“, entspricht der Menge $\mathrm{im}(\varphi) = K[a] = \{\sum r_i a^i \mid r_i \in K\}$. Dies muss im Allgemeinen kein Körper sein, lässt sich aber wenigstens explizit hinschreiben.

Proposition 3.6
Sei L/K eine Körpererweiterung und $a \in L$. Dann sind äquivalent:

(a) Es gilt $K[a] = K(a)$.

(b) Das Element $a \in L$ ist algebraisch abhängig über K.

(c) $\dim_K K(a) < \infty$

In diesem Fall gilt für den Grad des Minimalpolynoms: $\lambda(m_a) = [K(a) : K]$. Diese Zahl heißt dann Grad von a über K. Das Minimalpolynom m_a eines algebraischen Elements ist irreduzibel. Das von m_a erzeugte Ideal $\langle m_a \rangle$ ist maximal in $K[x]$.

Beweis :
(b) $\Rightarrow$ (c) Sei $a \neq 0$ algebraisch mit Minimalpolynom m_a.

$$
\begin{aligned}
m_a(x) = \sum_{i=0}^{n} r_i x^i \qquad & n > 0\ , \quad r_n = 1 \\
\Rightarrow\ & r_0 + r_1 a + r_2 a^2 + \ldots + r_{n-1} a^{n-1} + a^n = 0 \\
\Rightarrow\ & a^n = -r_0 - r_1 a - \ldots - r_{n-1} a^{n-1} \\
\Rightarrow\ & a^n \text{ ist über } K \text{ linear abhängig von } \{1, a, \ldots, a^{n-1}\} \\
\Rightarrow\ & K[a] \text{ ist } K\text{-erzeugt von } 1, a, \ldots, a^{n-1}. \text{ Dies folgt induktiv über} \\
& a^{n+1} = a a^n = a(-r_0 - r_1 a - \ldots - r_{n-1} a^{n-1}) = -r_0 a - r_1 a^2 - \ldots - r_{n-1} a^n.
\end{aligned}
$$

Falls $s_0 1 + s_1 a + \ldots + s_{n-1} a^{n-1} = 0$ mit $s_j \in K$ ergibt sich, da dann $g(x) = s_0 + s_1 x + \ldots + s_{n-1} x^{n-1}$ ein Polynom in $K[x]$ mit Nullstelle a und kleinerem Grad als m_a ist, ein Widerspruch. Also ist $\{1, a, \ldots, a^{n-1}\}$ eine Basis von $K[a]$ und $\dim_K K[x] = \lambda(m_a)$. Zusammen mit dem nächsten Beweisabschnitt folgt die Behauptung in (c).

(b) $\Rightarrow$ (a) Wir zeigen zunächst, dass $K[a]$ ein Körper ist. Dazu zeigen wir, dass $\langle m_a \rangle$ ein maximales Ideal ist, weil dann die Körpereigenschaft von $K[a] = K[x]/\langle m_a \rangle$ mithilfe von Abschnitt 2.7 folgt.

Das Bild $\mathrm{im}(\varphi) = K[x]/\langle m_a \rangle$ ist Teilmenge des Körpers L, also ein Integritätsbereich. Folglich ist auch $K[a]$ ein Integritätsbereich und damit $\langle m_a \rangle$ ein Primideal. Daraus folgt, dass m_a ein Primelement in $K[x]$, also irreduzibel ist (vgl. 2.12).

Um zu zeigen, dass $\langle m_a \rangle \neq 0$ ein maximales Ideal ist, muss aus $\langle m_a \rangle \subset I \subset K[x]$ gefolgert werden, dass $I \in \{\langle m_a \rangle, K[x]\}$. Auch $I = \langle f \rangle$ wird von einem Element erzeugt. Dann gibt es aber ein g, sodass $m_a = fg$. Da m_a irreduzibel ist, muss einer der Faktoren eine Einheit sein. Wenn f eine Einheit ist, folgt $\langle f \rangle = K[x]$. Falls g eine Einheit ist, folgt $f = \frac{1}{g} m_a$ und damit $I = \langle m_a \rangle$.

Also ist $\langle m_a \rangle$ maximal und $K[a] = K[x]/\langle m_a \rangle$ ein Körper.

$\Rightarrow$ $K[a] \supset K(a)$ (kleinster Körper mit dieser Bedingung)

$K[a] \ni \{1, a, \ldots, a^{n-1}\} \subset K(a) \Rightarrow K[a] \subset K(a) \Rightarrow K[a] = K(a)$.

$\neg$(b) $\Rightarrow$ $\neg$(a),$\neg$(c) Sei jetzt a nicht algebraisch, sondern transzendent.

Betrachte $K(a) \ni a^{-1}$ und zeige, dass $a^{-1} \notin K[a]$. Falls $a^{-1} \in K[a]$ wäre, würde sich aus $a^{-1} = r_0 + r_1 a + \ldots + r_n a^n \Rightarrow -1 + r_0 a + r_1 a^2 + \ldots + r_n a^{n+1} = 0$ ein nichttriviales Polynom mit Nullstelle a und damit ein Widerspruch zur Transzendenz von a ergeben. $\Rightarrow$ $a^{-1} \notin K[a] \Rightarrow K[a] \neq K(a)$. Nun ist aber $K[a] \subset K(a)$. φ injektiv und $K[a] = \mathrm{im}(\varphi) \simeq K[x]$, ∞-dimensional über K, da die Elemente $1, a, a^2, \ldots$ linear unabhängig sind. □

Wir haben überdies gezeigt, dass für irreduzibles $f(x) \neq 0$, das Ideal $\langle f(x) \rangle$ maximal ist. Der Körper $K[x]/\langle f(x) \rangle$ hat als K-Vektorraum die Basis $1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{n-1}$, wobei $n = \lambda(f(x))$ sei. Um feststellen zu können, dass ein Polynom $f(x)$ irreduzibel ist, schauen wir uns das folgende Kriterium an.

Theorem 3.7 **Kriterium von Eisenstein**

Sei R ein faktorieller Ring, K der Quotientenkörper von R und

$$f(x) = \sum_{i=0}^{n} a_i x^i \in R[x] \quad \text{mit} \quad n \geq 1$$

Sei ferner $p \in R$ irreduzibel mit $p | a_i$ für $i = 0, \ldots, n-1$ sowie $p \nmid a_n$ und $p^2 \nmid a_0$.

Dann ist $f(x)$ irreduzibel in $K[x]$.

Falls überdies $f(x)$ primitiv ist, dann ist $f(x)$ auch irreduzibel in $R[x]$ (vgl. Satz von Gauß 2.16).

Beweis :
Da $\deg(f(x)) = n \geq 1$ ist $f(x)$ keine Einheit. Angenommen $f(x) =: g(x)h(x)$ ist reduzibel, also $g, h \in R[x]$ mit $1 \leq \deg(g), \deg(h) < n$. Das Element p ist irreduzibel im faktoriellen Ring R, also auch prim, weswegen $R/\langle p\rangle$ ein Integritätsbereich ist. Dann hat $R/\langle p\rangle$ einen Quotientenkörper L, dessen Polynomring $L[x]$ faktoriell ist (da L ein Körper ist). Reduziere die Koeffizienten modulo p. Betrachte dazu:

$$\pi\colon R[x] \to R/\langle p\rangle\,[x] \subset L[x]$$

$$\sum_{i=0}^{n} a_i x^i = f(x) \mapsto \pi(f(x)) = \sum \underset{\cap}{\overline{a}_i} x^i = x^n \overline{a}_n \qquad \text{da } p|a_i \text{ für } i < n$$
$$R/\langle p\rangle$$

$$\overline{a}_n x^n = \pi(f(x)) = \pi(g(x))\pi(h(x)) \qquad \exists j\colon \pi(g(x)) = bx^j \ ,\ \pi(h(x)) = cx^{n-j}$$

Da $L[x]$ faktoriell, ist die Primfaktorzerlegung (und damit j) eindeutig. Folglich wird $g(0)$ und $h(0)$ von p geteilt. Damit ergibt sich aus $p^2 \mid \underbrace{g(0)h(0)}_{f(0) = a_0}$ ein Widerspruch zur Voraussetzung. □

Beispiel: Direkte Anwendung
Es sei $f(x) = x^n - pq$ mit Primzahl p, sodass $p \nmid q$. Dieses p erfüllt das Kriterium. $f(x)$ ist normiert und damit primitiv. Folglich ist $x^n - pq$ irreduzibel in $R[x]$.

Beispiel: Indirekte Anwendung
Sei p eine Primzahl und $g(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \ldots + 1$. Angenommen $g(x) =: g_1(x)g_2(x)$ ist reduzibel, also $\deg(g_1), \deg(g_2) \geq 1$. Dann gilt aber auch:

$$(*) \quad g(x+1) = g_1(x+1)g_2(x+1)$$

$$g(x+1) = \frac{(x+1)^p - 1}{x+1-1} = \frac{\sum_{j=0}^{p} \binom{p}{j} x^j - 1}{x} = \sum_{j=1}^{p} \binom{p}{j} x^{j-1}$$
$$= x^{p-1} + px^{p-2} + \ldots + p$$

Wegen $p|\binom{p}{j}\, \forall_{1\leq j<p}$ ist auf dieses Polynom das Kriterium von Eisenstein anwendbar. Also ist $g(x+1)$ irreduzibel. Nach $(*)$ muss g_1 oder g_2 eine Einheit sein. Folglich ist auch $g(x)$ irreduzibel.

Beispiele für Körpererweiterungen

Was passiert etwa bei $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$? Es ist $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, denn sonst wäre

$$\begin{aligned}
\sqrt{3} &= a + b\sqrt{2} \text{ mit } a, b \in \mathbb{Q} \\
3 &= a^2 + 2b^2 + 2ab\sqrt{2} \\
\Rightarrow \sqrt{2} &= \frac{(3 - a^2 - 2b^2)}{2ab} \Rightarrow \sqrt{2} \in \mathbb{Q} \qquad \text{Widerspruch} \\
\Rightarrow ab &= 0
\end{aligned}$$

$$\begin{aligned}
\text{falls} \quad a = 0 &\Rightarrow \frac{3}{2} = b^2 \Rightarrow \frac{3}{2} = \frac{p^2}{q^2} \Rightarrow 3q^2 = 2p^2 \Rightarrow 2|q \Rightarrow 2|p \quad \lightning \\
\text{falls} \quad b = 0 &\Rightarrow 3 = a^2
\end{aligned}$$

Also ist $\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \Rightarrow 2 < \dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))(\sqrt{3}) \leq 4$, da $x^2 - 3$ das Minimalpolynom zu $\sqrt{3}$ ist.

Falls $x^2 - 3$ über $\mathbb{Q}(\sqrt{2})$ Produkt von zwei Linearfaktoren ist, müssten diese, da $\mathbb{C}[x]$ faktoriell ist, gleich $x \pm \sqrt{3}$ sein, ein Widerspruch. Also ist $x^2 - 3$ irreduzibel über $\mathbb{Q}(\sqrt{2})$.

$$\begin{aligned}
&\mathbb{Q} \overset{2}{\subset} \mathbb{Q}(\sqrt{2}) \overset{2}{\subset} (\mathbb{Q}(\sqrt{2}))(\sqrt{3}) \\
&\Rightarrow \left[(\mathbb{Q}(\sqrt{2}))(\sqrt{3}) : \mathbb{Q}\right] = 4
\end{aligned}$$

Ist diese Erweiterung einfach? Probiere $b := \sqrt{2} + \sqrt{3}$ und versuche das Minimalpolynom zu erraten.

$$\begin{aligned}
b^2 &= (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{2}\sqrt{3} \\
b^2 - 5 &= 2\sqrt{2}\sqrt{3} \\
(b^2 - 5)^2 &= 24
\end{aligned}$$

Also ist b eine Nullstelle des Polynoms $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Falls dieses Polynom irreduzibel ist, würde $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$ folgen. Da das Kriterium von Eisenstein leider nicht direkt anwendbar ist, versuchen wir etwas anderes. Offensichtlich gilt die Inklusion $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2})(\sqrt{3})$. Zu zeigen ist also $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

$$\begin{aligned}
b^2 &= 5 + 2\sqrt{2}\sqrt{3} \qquad & b &:= \sqrt{2} + \sqrt{3} \\
b^3 &= 11\sqrt{2} + 9\sqrt{3} = 2\sqrt{2} + 9b \\
b^3 - 9b &= 2\sqrt{2} \Rightarrow \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \Rightarrow \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \\
\Rightarrow \mathbb{Q}(\sqrt{2} + \sqrt{3}) &= \mathbb{Q}(\sqrt{2})(\sqrt{3})
\end{aligned}$$

Also ist auch $x^4 - 10x^2 + 1$ das Minimaplolynom und $\left[(\mathbb{Q}(\sqrt{2}))(\sqrt{3}) : \mathbb{Q}\right] = 4$.

Definition 3.8
Eine Körpererweiterng L/K heißt algebraisch genau dann, wenn alle $a \in L$ algebraisch abhängig über K sind.

Proposition 3.9
Seien M/L und L/K Körpererweiterungen. Dann gilt:

(a) L/K endlich $\Rightarrow$ L/K algebraisch.

(b) L/K endlich erzeugt und algebraisch $\Rightarrow$ L/K endlich.

(c) M/L und L/K algebraisch $\Rightarrow$ M/K algebraisch.

Beweis :

(a) Sei $[L : K] < \infty$ und $a \in L$. Dann gilt auf jeden Fall $K(a) \subset L$ und $[K(a) : K] < \infty$, folglich können nicht alle $1, a, a^2, \ldots$ linear unabhängig über K sein. Es müssen also nichttriviale $\lambda_i \in K$ existieren, so dass $\sum_{i=0}^{n} \lambda_i a^i = 0$. Dann hat das Polynom $f(x) := \sum_{i=0}^{n} \lambda_i x^i \in K[x]$ die Nullstelle a, weshalb a algebraisch ist.

(b) Wenn L/K endlich erzeugt und algebraisch ist, existieren algebraische $a_1, \ldots, a_n \in L$, sodass $L = K(a_1, \ldots, a_n)$. Wir erhalten die Inklusionskette

$$K \subset K(a_1) \subset K(a_1, a_2) \subset \ldots \subset L = K(a_1, \ldots, a_n)$$

In jedem einzelnen Schritt haben wir nach Proposition 3.6 eine endliche Erweiterung, da jedes a_i algebraisch ist. Mit Lemma 3.3 folgt auch $[L : K] < \infty$.

(c) Sei $a \in M$. Zu zeigen ist, dass a algebraisch über K ist. Nach Voraussetzung ist a algebraisch über L, weshalb nach Definition ein $f(x) = \sum_{i=0}^{n} b_i x^i \in L[x]$ mit $f(a) = 0$ existiert.

Die Elemente $b_1, \ldots, b_n \in L$ sind nach Voraussetzung wiederum alle algebraisch abhängig über K. Aus (b) ergibt sich, dass $[K(b_1, \ldots, b_n) : K] < \infty$.

Offenbar ist $f(x) \in K(b_1, \ldots, b_n)[x]$. Also ist $[K(b_1, \ldots, b_n, a) : K(b_1, \ldots, b_n)] < \infty$ nach Proposition 3.6. Zusammen mit obigem folgt nach Lemma 3.3 insgesamt $[K(b_1, \ldots, b_n, a) : K] < \infty$ und damit auch auf jeden Fall $[K(a) : K] < \infty$, weshalb a algebraisch über K ist.

□

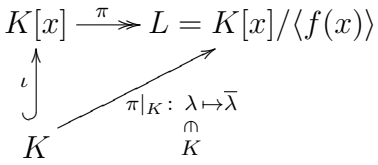
Das nächste Theorem widmet sich wieder unsererm ursprünglichen Problem algebraische Gleichungen zu lösen.

Theorem 3.10 Satz von Kronecker
Sei K ein Körper und $f(x) \in K[x]$ ein irreduzibles Polynom. Dann existiert eine einfache und algebraische Körpererweiterung L/K mit $[L : K] = \deg(f(x))$, sodass $f(x)$ in L mindestens eine Nullstelle hat.

Jede polynomiale Gleichung ist lösbar!

Der Beweis verläuft konstruktiv.

Beweis :
Das Polynom $f(x)$ ist irreduzibel, also nicht konstant und damit vom Grad ≥ 1. Nach Proposition 2.13 ist $\langle f(x)\rangle \subset K[x]$ ein maximales Ideal, also ist $L := K[x]/\langle f(x)\rangle$ ein Körper. Betrachte das folgende Diagramm:



Sei π die Restklassenabbildung. Deren Einschränkung $\pi|_K$ auf den Körper K ist ein Ringhomomorphismus und als solcher nach Proposition 2.5 injektiv. Daraus folgt die Inklusion $K \subset L$, weshalb L eine Körpererweiterung von K ist.

Nach Konstruktion gilt $\deg(f(x)) = [L : K]$. Die Behauptung, dass $f(x) = \sum a_i x^i$ in L eine Nullstelle $\overline{x} = \pi(x)$ hat, folgt aus

$$f(\pi(x)) = \sum_i a_i(\pi(x))^i = \pi\Big(\sum_i a_i x^i\Big) = \pi\Big(f(x)\Big) = 0$$

Aus der Unbestimmten wird also die Lösung der Gleichung. □

Vorgegeben sei ein Polynom $f(x) \in K[x]$, welches wir als Produkt $f(x) = f_1(x)\cdots f_n(x)$ von Irreduziblen schreiben. Wir betrachten die Körpererweiterung $L := K[x]/\langle f_1(x)\rangle$ von K. Ist $f_1(x) = a_0 + a_1x + \ldots + a_nx^n$, bildet $1, x, \ldots, x^{n-1}$ eine Basis von L über K. Modulo $\langle f_1(x)\rangle$ gilt $x^i \cdot x^j = x^{i+j}$ und $a_nx^n = -a_0 - a_1x - \ldots - a_{n-1}x^{n-1}$. Der Grad der Körpererweiterung ist $[L : K] = n = \deg(f_1(x))$. In L hat $f_1(x)$ die Nullstelle $\overline{x} = x + \langle f_1(x)\rangle$.

Betrachte anschließend $f_1(x)$ über $L[x]$ und dividiere den Linearfaktor der gefundenen Nullstelle weg. Durch wiederholte Anwendung des Satzes von Kronecker und durch die damit ggf. verbundenen Körpererweiterungen finden wir weitere Nullstellen.

Gibt es nun für beliebiges K eine Körpererweiterung, in der *alle* polynomialen Gleichungen lösbar sind? Dies ist eine stärkere Frage, denn der Satz von Kronecker garantiert nur die Lösung für *ein* Polynom.

Im Beispiel $K = \mathbb{R}$ ist nach dem Fundamentalsatz der Algebra $\mathbb{C}$ der geeignete Erweiterungskörper.

Definition 3.11
Ein Körper K heißt algebraisch abgeschlossen genau dann, wenn K eine der folgenden äquivalenten Bedingungen erfüllt:

(a) Jedes nicht-konstante Polynom $f(x) \in K[x] \setminus K$ hat eine Nullstelle in K.

(b) Jedes nicht-konstante Polynom $f(x) \in K[x] \setminus K$ zerfällt in ein Produkt von Linearfaktoren $f = f_1 \cdot f_2 \cdots f_n$ mit $f_i \in K[x]$ und $\deg(f_i) = 1$.

(c) Jedes irreduzible normierte Polynom ist von der Form $f(x) = x - a$ für ein $a \in K$.

(d) Sei L/K eine *algebraische* Körpererweiterung. Dann ist $L = K$.

Wenn K algebraisch abgeschlossen ist, schreiben wir $K = \overline{K}$.

Beweis :

(a) $\Rightarrow$ (b) Das Polynom $f(x)$ hat nach Voraussetzung die Nullstelle $a \in K$. Der Polynomring ist euklidisch, weshalb Division mit Rest anwendbar ist:

$$f(x) = q(x)(x-a) + r(x) \quad \text{mit} \quad f(x) = 0 \quad \text{oder} \quad \deg(r(x)) < \deg(x-a) = 1$$

Es folgt $\deg(r(x)) = 0$, also $r(x) = \text{const}$. Setzt man die Nullstelle a ein, folgt überdies $r(x) = 0$ wegen $0 = f(a) = q(a)(a-a) + r(a)$. Die Aussage (b) ergibt sich induktiv.

(b) $\Rightarrow$ (c) ist klar.

(c) $\Rightarrow$ (d) Sei $a \in L$. Es ist $a \in K$ zu zeigen. Da a algebraisch ist, besitzt es ein Minimalpolynom m_a über K, welches irreduzibel und normiert ist. Aus (c) ergibt sich, dass $m_a(x) = x - b$ für ein $b \in K$ gelten muss. Wegen $m_a(a) = 0$ folgt $b = a$, also $a \in K$ und damit $L = K$.

(d) $\Rightarrow$ (a) Sei $f \in K[x] \setminus K$ Produkt von irreduziblen $f = f_1 \cdots f_n$. Zu zeigen ist, dass $f_1(x)$ eine Nullstelle in K hat. Nach dem Satz von Kronecker enthält die algebraische Körpererweiterung $L := K[x]/\langle f_1(x)\rangle$ eine Nullstelle von $f_1(x)$. Nach Aussage (d) ist $L = K$, wir haben also eine Nullstelle in K gefunden. □

Definition 3.12

Sei K ein Körper und $\overline{K} \supset K$ eine algebraische Körpererweiterung, die algebraisch abgeschlossen ist. Dann heißt $\overline{K}$ algebraischer Abschluss von K.

Es stellt sich die Frage nach Existenz und Eindeutigkeit eines algebraischen Abschlusses $\overline{K}$. Wir wissen, dass $\overline{\mathbb{R}} = \mathbb{C}$ ist. Schon weniger klar ist der Fall $\overline{\mathbb{Q}}$, denn $\mathbb{C}/\mathbb{Q}$ ist nicht algebraisch. Für den Existenzbeweis wird ein Axiom der Mengenlehre gebraucht, welches unabhängig vom gewöhnlichen Zermelo-Fraenkel-Axiomensystem ist.

Auswahlaxiom

Sei $I \neq \emptyset$ eine Menge und $\{M_i : i \in I\}$ eine Familie nichtleerer Mengen, $M_i \neq \emptyset \, \forall_{i \in I}$. Dann existiert eine Funktion (Auswahlfunktion) $f : I \to \bigcup_{i \in I} M_i$ mit $f(i) \in M_i \, \forall_{i \in I}$. Es existiert also ein $(x_i)_{i \in I} \in \bigtimes_{i \in I} M_i$.

Sei M eine Menge und $\leq$ eine partielle Ordnung auf M, das heißt eine Relation mit

$\forall_{x \in M}$	$x \leq x$	Reflexivität
$\forall_{x,y,z \in M}$	$x \leq y \ \wedge \ y \leq z \ \Rightarrow \ x \leq z$	Transitivität
$\forall_{x,y \in M}$	$x \leq y \ \wedge \ y \leq x \ \Rightarrow \ x = y$	Antisymmetrie

Es müssen aber nicht alle Elemente x und y vergleichbar sein. Ein gängiges Beispiel ist die Inklusion von Mengen.

Definition

Die Ordnungsrelation $\leq$ heißt Totalordnung $:\Leftrightarrow \ \forall_{x,y}\colon x \leq y \vee y \leq x$.

Sei $N \subset M$. Ein Element $a \in M$ ist eine obere Schranke für $N :\Leftrightarrow \ \forall_{x\in N}\colon x \leq a$.

$a \in M$ ist ein maximales Element $:\Leftrightarrow \ \forall_{x\in M}\colon x \geq a \ \Rightarrow \ x = a$.

Zornsches Lemma

Sei $M \neq \emptyset$ partiell geordnet durch $\leq$, so dass $N \subseteq M$ total geordnet ist und eine obere Schranke $a \in M$ für N existiert.

Dann gibt es ein maximales Element in M.

Das Zornsche Lemma ist äquivalent zum Auswahlaxiom, eignet sich aber besser für Beweise. Das Auswahlaxiom sagt beispielsweise, dass jeder Vektorraum eine Basis besitzt, und dass es nicht messbare Mengen gibt. Auch lässt sich nur mit dem Auswahlaxiom das Banach-Tarski-Paradoxon zeigen. In der Topologie wird es verwendet um zu beweisen, dass das Produkt kompakter Mengen kompakt ist. Wir werden es für die Existenz maximaler Ideale brauchen.

Theorem 3.13

Sei R ein Ring (in dem $0 \neq 1$ gilt). Dann existiert ein maximales Ideal $I \triangleleft R$, also ein Ideal $I \neq R$, so dass für Ideale $J \triangleleft R$ mit $I \subset J \subset R$ entweder $J = I$ oder $J = R$ folgt.

Beweis :

Betrachte die Menge aller Ideale $\neq R$, also jene Ideale, die das Einselement nicht enthalten: $X := \{M_i \subset R\colon M_i \triangleleft R\,,\, 1 \notin M_i\}$. Da $1 \neq 0$ ist, befindet sich zumindest das Nullideal in X, weshalb X nichtleer ist. Diese Menge sei durch Inklusion partiell geordnet: $M_i \leq M_j \ \Leftrightarrow \ M_i \subseteq M_j$.

Sei $N \subseteq X$ total geordnet. Zu zeigen ist, dass eine obere Schranke für N existiert. Es bietet sich die Vereinigung $M_0 = \bigcup_{M_i\in N} M_i$ an, denn $M_0 \geq M_i \,\forall_{M_i\in N}$.

Zu zeigen ist, dass $M_0 \in X$ ist, also M_0 ein Ideal ungleich R ist.

Um die Idealeigenschaft nachzuweisen, ist $a + b, xa, ax \in M_0$ für $a, b \in M_0$ und $x \in R$ zu zeigen.

Offenbar existiert ein i sodass $a \in M_i$ und ein j sodass $b \in M_j$. Aus der totalen Ordnung in N folgt $M_i \leq M_j$ (oder $M_j \leq M_i$), also $a, b \in M_j$. Dies ist jedoch ein Ideal, weshalb $a + b \in M_j$ gilt. Genauso ist $xa \in M_i$ und $ax \in M_i$. Folglich ist auch M_0 ein Ideal.

Es verbleibt $M_0 \neq R$ zu zeigen. Falls $M_0 = R \ni 1$ ergibt sich aus $\exists_{M_i \in N} \colon 1 \in M_i$ sofort ein Widerspruch. Folglich ist M_0 eine obere Schranke in X für N. Wir haben damit die Voraussetzung von Zorns Lemma nachgeprüft, das heißt X ist „induktiv geordnet“. Es existiert also ein maximales Element $I_0 \in X$, also ein Ideal $I_0 \neq R$, das maximal bezüglich Inklusion ist. □

Zu jedem Ring R finden wir also ein maximales Ideal I_0 und damit auch einen Körper R/I_0.

Theorem 3.14
Jeder Körper K hat einen algebraischen Abschluss.

$K = \overline{K}$ ist nach Definition algebraisch abgeschlossen $\Leftrightarrow$ $f(x) \in K[x] \setminus K$ Nullstelle in K hat $\Leftrightarrow$ L/K algebraisch $\Rightarrow$ $L = K$. Wir beweisen folgende schwächere Aussage, aus der das Theorem folgt:

Proposition $(*)$
Sei F ein Körper. Dann existiert eine Körpererweiterung L/F, sodass jedes nichtkonstante Polynom $f(x) \in F[x] \setminus F$ eine Nullstelle in L hat.

Zunächst zeigen wir, dass daraus Theorem 3.14 induktiv folgt:

Zu $F = K = K_0$ existiert nach $(*)$ ein Erweiterungskörper $L = K_1$, sodass alle Polynome in $K_0[x] \setminus K_0$ Nullstellen in K_1 besitzen. Zu $F = K_1$ existiert wiederum ein Erweiterungskörper $L = K_2$ usw.

Sei $\overline{K} := \bigcup_{n \geq 0} K_n$. Betrachtet man $K_0 \subset K_1 \subset K_2 \subset \dots$, ergibt sich für Elemente $a \in K_i, b \in K_j$ mit $i \leq j$, dass $a, b \in K_j \ni a + b, a \cdot b$, weshalb $\overline{K}$ ein Körper ist.

Sei $f(x) = \sum_{i=0}^{n} a_i x^i \in \overline{K}[x] \setminus \overline{K}$. Da es nur endlich viele Koeffizienten sind, existiert ein $K_j \ni a_1, \dots, a_n$. Also ist $f(x) \in K_j[x] \setminus K_j$ und hat eine Nullstelle in $K_{j+1} \subset \overline{K}$.

Der Beweis dieser Aussage wird wesentlich weniger konstriktiv sein und das Zornsche Lemma benötigen.

Beweis : $(*)$
Betrachte $I := F[x] \setminus F$ als Indexmenge und mit $R := F[x_i \colon i \in I]$ einen Polynomring in I-vielen Variablen. Elemente in I sind Polynome $f(x) \in F[x]$. Es können beliebige Variablen eingesetzt werden, weshalb wir $f(x_i)$ und damit auch $f(x_f)$ bilden können.

Betrachte ferner das in R erzeugte Ideal $A := \langle f(x_f) \colon f \in F[x] \setminus F \rangle$. Die Behauptung ist, dass $A \neq R$, also $1 \notin A$ gilt und bildet den zentralen Aspekt des Beweises. Gegenannahme: $1 \in A$, also $1 = \sum_{i \in J} g_i f_i(x_{f_i})$ mit $g_i \in R$ und $|J| < \infty$. Nach dem Satz von Kronecker existiert eine algebraische Körpererweiterung F'/F, sodass in F' jedes f_i für $i \in J$ eine Nullstelle hat. Sortiere $R = F[x_i \colon i \in I] = \underbrace{\big(F[x_i \colon i \notin J]\big)}_{\text{Grundring}} \underbrace{[x_i \colon i \in J]}_{\text{endl. viele Variablen}}$. Dies ist möglich, da J endlich

ist. Aus Proposition 3.4 folgt die Existenz eines Auswertungshomomorphismus

$$\varphi\colon R = \Big(F[x_i\colon i \notin J]\Big)[x_j\colon j \in J] \to F'[x_i\colon i \notin J] \subset F'[x_i\colon i \in I]$$
$$f_j = x_j \mapsto a_j \quad \text{Nullstelle von } f_j \text{ in } F'$$

Betrachte $1 = \sum_{j\in J} g_j f_j(x_j)$. Da φ ein Ringhomomorphismus ist, ergibt sich aus

$$1 = \varphi(1) = \sum_{j\in J} \varphi(g_j)\varphi\Big(f_j(x_j)\Big) = \sum_{j\in J} \varphi(g_j)\overbrace{f_j(\underbrace{\varphi(x_j)}_{a_j})}^{0} = 0$$

ein Widerspruch zu $1 \neq 0$.

Also ist $A \neq R$. Wir betrachten den Quotientenring R/A (der nach obiger Überlegung ein echter Ring ist). Aus Theorem 3.13 folgt, dass R/A ein maximales Ideal M hat. An dieser Stelle ist der Beweis nicht mehr konstruktiv, denn es fließt Zorns Lemma ein. Sei $\pi\colon R \to R/A$ die Restklassenabbildung. Dann ist $\pi^{-1}(M) = H$ ein maximales Ideal in R und enthält A. Es gilt also $A \subset H \subset R$. Aus der Maximalität von H folgt, dass $L := R/H$ ein Körper ist.

Wir zeigen, dass L der in $(*)$ postulierte Erweiterungskörper ist.

L ist eine Körpererweiterung von F, denn $\quad F \subset R \twoheadrightarrow R/H = L$, wobei $F \to L$ injektiv nach 2.5

Sei $f \in F[x] \setminus F$. Zu zeigen ist, dass f eine Nullstelle in L hat. Aus $x_f \in A \subset H$ folgt $f(x_f) = 0$ in L, denn $f(x) = \sum a_i x^i$ impliziert formal

$$f(\pi(x_j)) = \sum \underbrace{a_i}_{\pi(a_i)} (\pi(x_f))^i = \pi(\underbrace{f(x_f)}_{\in A}) = 0.$$

Sozusagen ist x_f die Nullstelle von f in A. Der Satz stellt damit eine naheliegende Erweiterung des Satzes von Kronecker dar.

□

Also existiert zu jedem Körper ein algebraischer Abschluss. Es stellt sich die Frage nach der Eindeutigkeit. Das Beispiel

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \overset{\alpha}{\cong} \mathbb{Q}[x]/\langle x^2 - 2\rangle \supset \mathbb{Q} \qquad \alpha|_{\mathbb{Q}} = \mathrm{id}\,|_{\mathbb{Q}}$$

legt es nahe zu verlangen, dass Isomorphismen von Körpererweiterungen den Grundkörper elementweise festhalten.

Definition 3.15

Seien L_1/K und L_2/K Körpererweiterungen von K. Ein Ringhomomorphismus $\varphi\colon L_1 \to L_2$ heißt K-Homomorphismus, wenn $\forall_{x\in K}\, \varphi(x) = x$ gilt.

Falls φ zusätzlich bijektiv ist, heißt es K-Isomorphismus, und im Fall $L_1 = L_2$ K-Automorphismus.

Beispiel:

Die komplexe Konjugation ist offenbar additiv und multiplikativ (letzteres sieht man leicht an der Polardarstellung) und ist damit ein $\mathbb{R}$-Automorphismus von $\mathbb{C}$.

$$\begin{aligned}\varphi\colon \mathbb{C} &\to \mathbb{C}\\ a+bi &\mapsto a-bi\\ z=re^{i\alpha} &\mapsto \overline{z}=re^{-i\alpha}\end{aligned}$$

Analog kann man einen $\mathbb{Q}$-Automorphismus von $\mathbb{Q}[\sqrt{2}]$ konstruieren. $(a,b\in\mathbb{Q})$

$$\begin{aligned}\tilde{\varphi}\colon \mathbb{Q}[\sqrt{2}] &\to \mathbb{Q}[\sqrt{2}]\\ a+b\sqrt{2} &\mapsto a-b\sqrt{2}\end{aligned}$$

In beiden Fällen bilden die Automorphismen Nullstellen des Minimalpolynoms auf Nullstellen ab:

$$\begin{aligned} m_{i,\mathbb{R}}(x)=x^2+1 \quad &\Rightarrow \quad m_{i,\mathbb{R}}\big(\varphi(i)\big)=m_{i,\mathbb{R}}\big(-i\big)=0\\ m_{\sqrt{2},\mathbb{Q}}(x)=x^2-2 \quad &\Rightarrow \quad m_{\sqrt{2},\mathbb{Q}}\big(\tilde{\varphi}(\sqrt{2})\big)=m_{\sqrt{2},\mathbb{Q}}\big(-\sqrt{2}\big)=0\end{aligned}$$

Lemma (Nullstellen)

Sei L/K eine Körpererweiterung und $\alpha\colon L\to L$ ein K-Automorphismus. Sei ferner $f\in K[x]$ ein Polynom mit Nullstelle $x_0\in L$. Dann ist auch $\alpha(x_0)$ eine Nullstelle.

Beweis :

$\alpha(x_0)$ erfüllt die Gleichung $f(x)=\sum\lambda_j x^j=0$, denn

$$0=\alpha(0)=\alpha\left(\sum\lambda_j x_0^j\right)=\sum\underbrace{\alpha(\lambda_j)}_{=\lambda_j}(\alpha(x_0))^j$$

□

Im Spezialfall einer einfachen Körpererweiterung $L=K(a)$ bildet ein K-Automorphismus Nullstellen des Minimalpolynoms von a auf Nullstellen desselben ab.

Proposition 3.16

Seien K und K' Körper und $\sigma\colon K\to K'$ ein Isomorphismus. Es sei

$$\begin{aligned}\sigma^*\colon K[x] &\to K'[x]\\ \sum\lambda_i x^i &\mapsto \sum\sigma(\lambda_i)x^i\end{aligned}$$

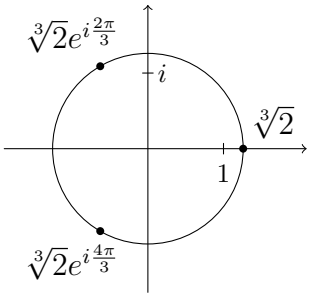
der induzierte Isomorphismus. Seien L/K und L'/K' Körpererweiterungen.

(a) Für $a\in L$ und $a'\in L'$ mit $m_{a',K'}=\sigma^*(m_{a,K})$ gibt es genau einen Isomorphismus $\varphi\colon K(a)\to K'(a')$ mit $\varphi(a)=a'$ und $\varphi|_K=\sigma$.

(b) Für $a\in L$ gilt: $\#\{\varphi\colon K(a)\to L' \text{ mit } \varphi|_K=\sigma\}=\#\{x\in L'\colon \sigma^*(m_{a,K})(x)=0\}$

Beispiel:
Sei $K = K' = \mathbb{Q}$ und $\sigma = \mathrm{id}$ sowie $m_{a,K}(x) = x^3 - 2$ für beispielsweise $a = \sqrt[3]{2} \in \mathbb{R}$.

$$\sqrt[3]{2}e^{i\frac{2\pi}{3}}, \sqrt[3]{2}e^{i\frac{4\pi}{3}} \notin \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$$
$$\sigma^*(m_{a,K}) = x^3 - 2$$
$$L' = \mathbb{C}$$
$$\left\{x \in L' \colon \sigma^*(m_{a,K})(x) = 0\right\} = \left\{\sqrt[3]{2}, \sqrt[3]{2}e^{i\frac{\pi}{3}}, \sqrt[3]{2}e^{i\frac{2\pi}{3}}\right\}$$



Aus (b) folgt, dass es *drei* Abbildungen der Gestalt

$\varphi \colon \mathbb{Q}\left(\sqrt[3]{2}\right) \to \mathbb{C}$ mit $\varphi|_{\mathbb{Q}} = \mathrm{id}$ gibt. Im Fall $L' = \mathbb{R}$ gibt es nur noch *ein* solches φ.

Beweis : **Proposition 3.16**

(a) Sei $f := m_{a,K}$ das Minimalpolynom von a. Es ist insbesondere irreduzibel. Betrachte die folgenden Isomorphismen

$$K(a) \overset{\psi}{\simeq} K[x]/\langle f\rangle \qquad K'(a') \overset{\psi'}{\simeq} K'[x]/\langle \sigma^* f\rangle$$
$$a \leftarrow\!\shortmid\ x \qquad a' \leftarrow\!\shortmid\ x$$

$$K[x] \overset{\sigma^*}{\simeq} K'[x] \qquad \Rightarrow \qquad K[x]/\langle f\rangle \overset{\overline{\sigma}^*}{\simeq} K'[x]/\langle \sigma^* f\rangle$$
$$\langle f\rangle \to \langle \sigma^* f\rangle$$
$$f \mapsto \sigma^* f$$

und definiere die gesuchte Abbildung $\varphi \colon K(a) \xrightarrow{\sim} K'(a')$ als Komposition der drei Isomorphismen $\psi' \circ \overline{\sigma}^* \circ \psi^{-1} =: \varphi$. Als solche ist φ selbst ein Isomorphismus. Nach Konstruktion gilt tatsächlich $\varphi|_K = \sigma$ und $\varphi \colon a \overset{\psi^{-1}}{\longmapsto} x \overset{\overline{\sigma}^*}{\longmapsto} x \overset{\psi'}{\longmapsto} a'$. Damit ist φ nach Proposition 3.4 zudem eindeutig.

(b) „$\geq$“ Sei $a' \in L'$ Nullstelle von $\sigma^*(m_{a,K})$. Nach (a) existiert ein $\varphi \colon K(a) \to K'(a')$ mit $\varphi|_K = \sigma$. Wir nutzen $K'(a') \subset L'$ aus und komponieren mit der Inklusionsabbildung $K(a) \to K'(a') \hookrightarrow L'$ um eine Abbildung $\phi \colon K(a) \to L'$ mit $\phi|_K = \sigma$ zu erhalten.

„$\leq$“ Sei $\varphi \colon K(a) \to L'$ mit $\varphi|_K = \sigma$ gegeben. Dann gilt $\varphi^* \colon m_{a,K} \mapsto \sigma^*(m_{a,K})$. Dabei wird eine Nullstelle von $m_{a,K}$, etwa a selbst, auf eine Nullstelle von $\sigma^*(m_{a,K})$ abgebildet, denn:

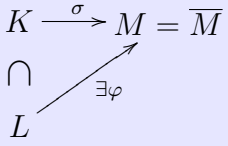
$$m_{a,K}(x) = \underbrace{\sum \lambda_j x^j}_{=0} \mapsto \underbrace{\sum \overbrace{\sigma(\lambda_j)}^{\varphi(\lambda_j)} x^j}_{=0} = \sigma^*(m_{a,K})(x) \quad \Leftrightarrow$$

Wählt man diese Nullstelle als $x \in L'$ ergibt sich die umgekehrte Inklusion.

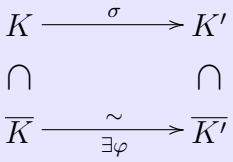
□

Theorem 3.17

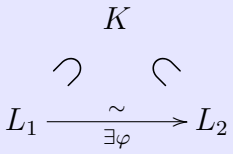
(a) Sei L/K eine algebraische Erweiterung, $M = \overline{M}$ und $\sigma\colon K \to M$ ein Homomorphismus. Dann existiert ein Homomorphismus $\varphi\colon L \to M$ mit $\varphi|_K = \sigma$, das heißt φ setzt σ fort.



(b) Sei $K \overset{\sigma}{\simeq} K'$ und sei $\overline{K}$ bzw. $\overline{K'}$ der algebraische Abschluss von K bzw. K'. Dann existiert ein Isomorphismus $\varphi\colon \overline{K} \xrightarrow{\sim} \overline{K'}$ mit $\varphi|_K = \sigma$.



(c) Seien L_1 und L_2 algebraische Abschlüsse von K. Dann existiert ein K-Isomorphismus $L_1 \simeq L_2$.



Beweis :

(a) Im Falle einer einfachen Körpererweiterung $L = K(a)$ existiert nach Proposition 3.16 eine Abbildung φ der gewünschten Form. (Nullstellen von $\sigma^*(m_{a,K})$ existieren in $M = \overline{M}$.)

Für beliebiges algebraisches $L \supset K$ verwenden wir Zorns Lemma. Wir betrachten dazu

$$X := \{(K', \tau')\colon K \subset K' \subset L, \tau'|_K = \sigma\}$$

also die in Diagramm (1) illustrierte Situation. Auf X kann eine partielle Ordnung $(K', \tau') \leq (K'', \tau'')$ definiert werden, falls Diagramm (2) und $\tau''|_{K'} = \tau'$ gilt.
Zu zeigen ist, dass jede total geordnete Teilmenge von X eine obere Schranke in X hat.

Diagramm (1)

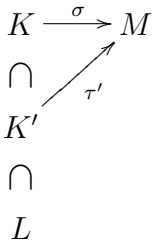
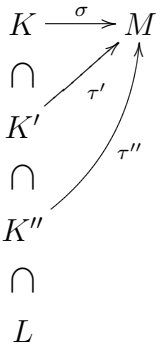


Diagramm (2)



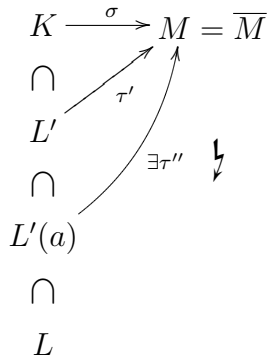
Sei $\{(K_i, \tau_i)\}_{i\in I} \subset X$ total geordnet. Für $i, j \in I$ gelte also $(K_i, \tau_i) \subseteq (K_j, \tau_j)$ oder umgekehrt. Betrachte $\left(\bigcup_{i\in I} K_i, \bigcup_{i\in I} \tau_i\right)$ als Kandidat einer oberen Schranke.

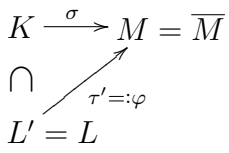
$\bigcup_{i\in I} K_i$ ist ein Körper, denn für $a, b \in \bigcup_{i\in I} K_i$ existieren i_1, i_2 mit $a \in K_{i_1}$ und $b \in K_{i_2}$. Für oBdA $i_1 \leq i_2 \Rightarrow a, b \in K_{i_2} \ni a + b, a \cdot b, \frac{1}{a}$

Von der Vereinigung $\bigcup_{i\in I} \tau_i$ können wir reden, wenn wir die Funktion f als Relation $\{(x, f(x))\}$ schreiben. Für $i \leq j$ ergibt sich, da τ_j Fortsetzung von τ_i ist, aus $(x, \tau_i(x)) = (x, \tau_j(x))$ die Wohldefiniertheit.

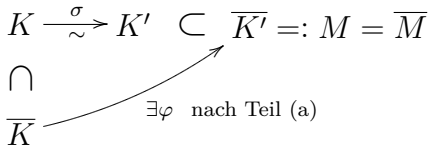
Die Voraussetzungen von Zorns Lemma sind damit erfüllt. Folglich existiert in X ein maximales Element (L', τ'). Wir behaupten, dass $L' = L$.

Aus der Gegenannahme $L' \subsetneq L$ folgt die Existenz eines $a \in L \setminus L'$. Da L/K algebraisch ist, muss dieses a algebraisch sein. Aus Proposition 3.16 ergibt sich nebenstehendes Diagramm und damit ein Widerspruch zur Maximalität von (L', τ'). Also gilt $L' = L$.



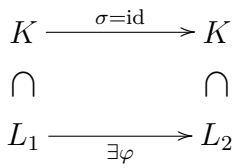


(b) Schreiben wir das Diagramm aus Teil (b) etwas um, können wir aus Teil (a) die Existenz eines Homomorphismus $\varphi\colon \overline{K} \to \overline{K'}$ mit $\varphi|_K = \sigma$ folgern:



Da $\overline{K}$ ein Körper ist, muss φ nach Propositin 2.5 injektiv sein. Wir zeigen noch dessen Surjektivität. Aus der Injektivität können wir zunächst $\varphi(\overline{K}) \simeq \overline{K}$ folgern. Gleichzeitig gilt $\varphi(\overline{K}) \supset \varphi(K) = \sigma(K) = K'$, woraus $K' \subset \varphi(\overline{K}) \subset \overline{K'}$ folgt. In dieser Inklusionskette handelt es sich ausschließlich um algebraische Erweiterungen. $\varphi(\overline{K})$ ist bereits algebraisch abgeschlossen, weswegen gemäß Definition 3.11 (d) die Gleichheit $\varphi(\overline{K}) = \overline{K'}$ folgt. Also ist φ ein Isomorphismus.

(c) Dieser Teil ist ein Spezialfall von Teil (b) für $K = K'$



$\Rightarrow$ φ ist ein K-Isomorphismus.

Wir haben damit gezeigt, dass der algebraische Abschluss $\overline{K}$ eindeutig bis auf K-Isomorphie ist. Alle algebraische Erweiterungen L/K finden also (bis auf K-Isomorphie) in $\overline{K}$ statt.

□

4 Körpererweiterungen und Galoistheorie

Wir stellen uns zunächst konkrete Fragen:

- Zu einfachen Erweiterungen: Wir haben $\Big(\mathbb{Q}(\sqrt{2})\Big)(\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ gesehen. Gilt auch allgemein $\Big(\mathbb{Q}(a_1)\Big)(a_2) \stackrel{?}{=} \mathbb{Q}(a_3)$ für ein a_3?
- Der Satz von Kronecker sagt, dass ein irreduzibles $f(x)$ mindestens eine Lösung in $K[x]/\langle f(x)\rangle$ hat. Er liefert uns also einen Körper, der *eine* Nullstelle enthält. Gibt es auch einen Körper, der *alle* Nullstellen enthält?
- Zu endlichen Körpern: $\mathbb{Z}/p\mathbb{Z}$ ist ein endlicher Körper, falls p eine Primzahl ist. Andernfalls liegt kein Körper vor, da dann Nullteiler enthalten sind. Wie sehen Körpererweiterungen von $\mathbb{Z}/p\mathbb{Z}$ aus?

Definition 4.1 **Zerfällungskörper**
Sei K ein Körper und $f(x) \in K[x]$ ein Polynom vom Grad $n \geq 1$. Sei ferner L/K eine Körpererweiterung. Dann heißt L Zerfällungskörper von $f(x)$ genau dann, wenn $a_1, \ldots, a_n \in L$ und $c \in K$ existieren, sodass

(1) $$f(x) = c\prod_{i=1}^{n}(x - a_i)$$

(2) $$L = K(a_1, \ldots, a_n)$$

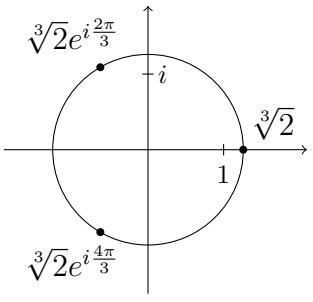
Also wird L erzeugt (über K) von den Nullstellen a_i von $f(x)$.

Ein Zerfällungskörper L existiert, da K einen algebraischen Abschluss $\overline{K}$ besitzt, der entsprechende Elemente $a_1, \ldots, a_n$ enthält.

Der Satz von Kronecker liefert nicht immer einen Zerfällungskörper. Betrachten wir $\mathbb{Q}[x] \ni f(x) = x^3 - 2$, gilt

$$\mathbb{Q}[x]/\langle x^3 - 2\rangle \simeq \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$$

Das Polynom f hat aber auch Nullstellen im Komplexen, wie nebenstehende Abbildung zeigt.



Wie lässt sich die Dimension des Zerfällungskörper beschreiben?

$$\dim \mathbb{Q}(\sqrt[3]{2}) = \deg(x^3 - 2) = 3$$
$$\dim(\text{Zerfällungskörper}) > 3$$

Zur Eindeutigkeit des Zerfällungskörpers: In $\overline{K}$ existiert ein Zerfällungskörper L. Wir erhalten also die Inklusionskette $K \subset L \subset \overline{K} \subset \overline{L}$. Andererseits ist L/K algebraisch. $K \subset L \subset \overline{L}$ sind alles algebraische Erweiterungen, weswegen nach Proposition 3.9 (c) folgt, dass $\overline{L}/K$ algebraisch ist. Also ist auch $\overline{L}/\overline{K}$ algebraisch, woraus $\overline{L} = \overline{K}$ folgt

(vgl. 3.11). Der algebraische Abschluss $\overline{K} = \overline{L}$ ist eindeutig bis auf Isomorphie. Für den Zerfällungskörper L gilt damit das Gleiche. Dagegen ist zu einem vorgegebenen Zerfällungskörper L das entsprechende Polynom $f(x)$ nicht eindeutig.

Beispiel:
Das Polynom $f_1(x) = x^2 + 1$ hat über $K = \mathbb{R}$ den Zerfällungskörper $L = \mathbb{C}$. Gleiches gilt auch für $f_2(x) = (x^2+1)(x-5)$, das Polynom f muss schließlich nicht irreduzibel sein.

Aber auch $f_3(x) = (x-(1+i))(x-(1-i)) = x^2 - 2x + 2 \in \mathbb{R}[x]$ hat über $\mathbb{R}$ den Zerfällungskörper $\mathbb{C}$ und ist nach Eisenstein irreduzibel.

Definition 4.2
Sei L/K eine Körpererweiterung und Λ eine Menge von nichtkonstanten Polynomen in $K[x]$. Dann heißt L Zerfällungskörper von Λ über K, wenn über L alle Polynome in Λ in Produkte von Linearfaktoren zerfallen und L minimal bezüglich dieser Eigenschaft ist. Minimalität bedeutet hier, dass für alle L_0 mit $K \subset L_0 \subset L$ und der Eigenschaft, dass über L_0 alle Polynome in Λ in Produkte von Linearfaktoren zerfallen, $L_0 = L$ gilt.

Eine Körpererweiterung L/K heißt normal, wenn es eine Menge Λ von nichtkonstanten Polynomen in $K[x]$ gibt, sodass L der Zerfällungskörper von Λ ist.

Proposition 4.3
Für $K \subset L \subset \overline{K}$ sind äquivalent:

(a) Alle über K irreduziblen $f \in K[x]$ mit Nullstelle in L lassen sich über L als Produkt von Linearfaktoren schreiben.

(b) L/K ist normal.

(c) Ein K-Homomorphismus $\varphi\colon L \to \overline{K}$ erfüllt $\varphi(L) = L$.

Beweis :

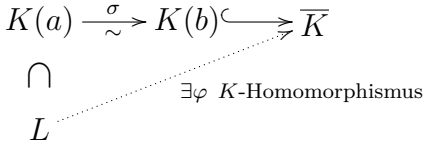
(b) $\Rightarrow$ (c) Sei L normal über K. Also existiert ein $\Lambda \subset K[x]$, sodass $L = K(N)$, wobei $N = \{\text{Nullstellen von allen } f \in \Lambda\}$. Für einen K-Homomorphismus φ ist $\varphi(L) = L$ zu zeigen. Es gilt $\varphi|_K = \mathrm{id}$, also $\varphi(K) = K$. Da φ nach Proposition 2.5 überdies injektiv ist, genügt es, die Implikation $a \in N \;\Rightarrow\; \varphi(a) \in N$ zu zeigen:

$$a \in N \;\Rightarrow\; \exists_{f\in\Lambda}\colon f(a) = 0 \qquad \varphi^*(f) = f \;\Rightarrow\; f(\varphi(a)) = 0 \;\Rightarrow\; \varphi(a) \in N$$

(c) $\Rightarrow$ (a),(b) Sei $a \in L$ und $m_{a,K}$ das Minimalpolynom. Wir zeigen über L, dass $m_{a,K}$ Produkt von Linearfaktoren ist. In $\overline{K}$ zerfällt $m_{a,K}$ bereits in Linearfaktoren. Sei b eine weitere Nullstelle von $m_{a,K}$. Es gelten die Isomorphien

$$K[x]/\langle m_{a,K}\rangle \simeq K(a) \overset{\sigma}{\simeq} K(b) \simeq K[x]/\langle m_{b,K}\rangle \qquad \text{wobei} \quad \sigma(a) = b.$$

Wir betrachten ein kommutatives Diagramm wie in Theorem 3.17 (a). Nach Voraussetzung ist $\varphi(L) = L$. Aus $\varphi(a) = \sigma(a) = b$ folgt, dass $b \in L$ ist. Alle Nullstellen von $m_{a,K}$ liegen also in L, woraus Aussage (a) folgt.



Desweiteren ist L der Zerfällungskörper von $\{m_{a,K} \colon a \in L\}$. Es folgt Aussage (b).

(a) $\Rightarrow$ (c) Sei $\varphi \colon L \to \overline{K}$ ein K-Homomorphismus. Zu zeigen ist $\varphi(L) = L$.

Sei $a \in L$. Wir zeigen, dass dann $\varphi(a) \in L$ ist. Das Minimalpolynom $m_{a,K} \in K[x]$ ist irreduzibel und hat eine Nullstelle in L. Nach Aussage (a) liegen daher alle seine Nullstellen in L. Sei x_0 eine solche Nullstelle, also $m_{a,K}(x_0) = \sum \lambda_i x_0^i = 0$.
Da φ ein K-Homomorphismus ist, ergibt sich vermöge

$$0 = \varphi(0) = \varphi\left(\sum \lambda_i x_0^i\right) = \sum \underbrace{\varphi(\lambda_i)}_{\lambda_i}(\varphi(x_0)^i) = \sum \lambda_i(\varphi(x_0)^i) \ ,$$

dass $\varphi(x_0)$ auch eine Nullstelle ist und daher in L liegt: $x_0 := a \ \Rightarrow \ \varphi(a) \in L$. $\square$

Irreduzible Polynome können dennoch mehrfache Nullstellen haben. Dieses Problem wird im Folgenden wegdefiniert.

Definition 4.4

(a) Sei $K \subset L \subset \overline{K}$. Der Separabilitätsgrad $[L : K]_s$ ist definiert als Anzahl der verschiedenen K-Homomorphismen $L \to \overline{K}$.

(b) Sei L/K endlich. L/K heißt separabel $\Leftrightarrow$ $[L : K]_s = [L : K]$.

(c) Ein Element $a \in \overline{K}$ heißt separabel über K genau dann, wenn $m_{a,K}$ in $\overline{K}$ nur einfache Nullstellen hat.

Falls L/K normal ist, gilt

$$\begin{array}{ccc} [L : K]_s & = & |\mathrm{Aut}_K(L)| \\ \| & & \| \\ |\{K\text{-Hom} \colon L \to \overline{K}\}| & = & |\{K\text{-Isom} \colon L \to L\}| \end{array}$$

Ist $\varphi \colon L \to \overline{K}$ ein K-Homomorphismus, folgt $\varphi(L) = L \ \Rightarrow \ \varphi \in \mathrm{Aut}_K(L)$.
$\mathrm{Aut}_K(L)$ kann somit als „Symmetriegruppe“ von L/K verstanden werden.

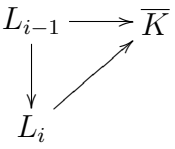
Lemma

Der Grad einer Körpererweiterung ist obere Schranke des Separabilitätsgrad.

$$[L : K] \geq [L : K]_s$$

Beweis :

Ist L/K endlich, also $L = K(a_1, \ldots, a_n)$ definiere schrittweise: $L_0 := K$ und $L_i := L_{i-1}(a_i)$. Dann ist $[L : K] = \prod[L_i : L_{i-1}]$. Ebenso gilt $[L : K]_s = \prod[L_i : L_{i-1}]_s$ nach Theorem 3.17.



Für die einfache Körpererweiterung $L_i = L_{i-1}(a_i)$ ist:

$$L_i = L_{i-1}[x]/\langle m_{a_i,L_{i-1}}\rangle$$
$$[L_i : L_{i-1}] = \deg(m_{a_i,L_{i-1}}) \geq \#\{\text{ Nullstellen von } m_{a_i,L_{i-1}}\} \overset{3.16\,(b)}{=} [L_i : L_{i-1}]_s$$

Folglich gilt immer $[L : K] \geq [L : K]_s$. □

Beispiel:
Sei $f(x) \in \mathbb{Q}[x]$ mit Nullstelle a der Vielfachheit ℓ. Wir werden damit etwas Unalgebraisches machen, nämlich ableiten:

$$\begin{aligned}
\mathbb{Q}[x] \ni f(x) &= (x-a)^\ell g(x) \\
f'(x) &= \ell(x-a)^{\ell-1} g(x) + (x-a)^\ell g'(x) \\
\ell > 1 \;\Rightarrow\; f'(a) &= 0 \\
\ell = 1 \;\Rightarrow\; f'(a) &= \underbrace{g(a)}_{\neq 0} + 0
\end{aligned}$$

Wir erkennen, dass $f(x)$ die Nullstelle a mit Vielfachheit $\ell > 1$ hat $\Leftrightarrow$ $f'(a) = 0$.

In beliebigem $K[x]$ haben wir keine Grenzwerte. Wir definieren daher $f'(x)$ über die „Ableitungen“ der Monome $(x^n)' := nx^{n-1}$, wobei $n = 1 + \ldots + 1$ als n-fache Summe des Einselements zu verstehen ist. Die so definierte Ableitung eines Polynoms ist additiv und es gelten Produkt- und Kettenregel. Damit funktioniert obiges Argument.

Man beachte allerdings, dass für $K = \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ und $f(x) = x^p$ gilt, dass $f'(x) = px^{p-1} = 0$ ist, da $p = 0$ ist, daraus aber nicht folgt, dass $f(x)$ konstant ist.

Lemma 4.5
Sei $a \in \overline{K}$. Dann ist a separabel über K genau dann, wenn $m'_{a,K} \neq 0$ ist.

Beweis :
Aus der Gegenannahme $m'_{a,K} = 0$ folgt mit $m'_{a,K}(a) = 0$, dass a eine mehrfache Nullstelle von $m_{a,K}$ und damit nicht separabel ist.

Sei umgekehrt $m'_{a,K} \neq 0$, woraus zu folgern ist, dass $m_{a,K}$ nur einfache Nullstellen hat. Das Minimalpolynom $m_{a,K}$ ist irreduzibel, weswegen $m'_{a,K}$ kein Teiler desselben sein kann. Da wegen $\deg m'_{a,K} < \deg m_{a,K}$ auch $m_{a,K} \nmid m'_{a,K}$ gilt, sind $m_{a,K}$

und $m'_{a,K}$ teilerfremd. Es existieren also Polynome α, β, sodass $1 = \alpha m_{a,K} + \beta m'_{a,K}$. Sei $m_{a,K}(b) = 0$. Wir zeigen $m'_{a,K}(b) \neq 0$. Einsetzen von b ergibt tatsächlich:

$$1 = \alpha(b) \underbrace{m_{a,K}(b)}_{=0} + \beta(b) m'_{a,K}(b) = \beta(b) m'_{a,K}(b) \qquad \Rightarrow \; m'_{a,K}(b) \neq 0$$

Nach obigem Beispiel ist b dann eine einfache Nullstelle. □

Bemerkung: $px^{p-1} = 0$ passiert über $\mathbb{F}_p$, aber nicht über $\mathbb{Q}$.

Definition 4.6
Sei K ein Körper. Die Charakteristik $\mathrm{char}(K)$ von K definieren wir als minimales $n \in \mathbb{N}$, sodass $\sum_{i=1}^{n} 1 = 0$ in K gilt. Falls kein solches $n \in \mathbb{N}$ existiert, setzen wir $\mathrm{char}(K) = 0$.

Beispiel:

$$\mathrm{char}(\mathbb{F}_p) = p \qquad \mathrm{char}(\mathbb{Q}) = 0 \qquad \mathrm{char}(K) = n \in \mathbb{N}$$

Falls $n = ab$ mit $a, b \in \mathbb{N} \setminus \{1\}$ gilt, folgt zum einen, dass $\sum_{i=1}^{n} 1 = 0$ ist und zum anderen, dass Elemente $\alpha\beta \in K \setminus \{0\}$ existieren, mit

$$K \ni \alpha := \sum_{i=1}^{a} 1 \neq 0 \neq \sum_{i=1}^{b} 1 = \beta \in K \qquad \alpha\beta = \sum_{i=1}^{ab} 1 = 0$$

Letzteres ist ein Widerspruch zur Nullteilerfreiheit von K.

Proposition 4.7

(a) L/K separabel $\Leftrightarrow$ $\forall_{a \in L}$: a separabel über K

(b) L/K separabel $\Leftrightarrow$ es existieren über K separable $a_1, \ldots, a_n$ mit $L = K(a_1, \ldots, a_n)$

(c) $\mathrm{char}(K) = 0$ und L/K endlich $\Rightarrow$ L/K separabel

(d) $\mathrm{char}(K) = p \neq 0$ und L/K endlich, sowie $p \nmid [L : K]$ $\Rightarrow$ L/K separabel

(e) Ist $K \subset M \subset L$, gilt: L/K separabel $\Leftrightarrow$ L/M und M/K separabel

Beweis :

(e) Die Gradformeln besagen

$$[L : K] = [L : M] \cdot [M : K] \qquad [L : K]_s = [L : M]_s \cdot [M : K]_s$$

Also ist $[L : K] = [L : K]_s \Leftrightarrow [M : K] = [M : K]_s$ und $[L : M] = [L : M]_s$

(a),(b) Wir zeigen die Implikationen im Uhrzeigersinn.
„⇒“ Sei L/K separabel und $a \in L$. Zu zeigen ist, dass a separabel ist.
Aus $K \subset K(a) \subset L$ folgt mit (e), dass $K(a)$ separabel über K ist.

$$\deg(m_{a,K}) = [K(a) : K] = [K(a) : K]_s \overset{3.16}{=} \#\{\text{ Nullstellen von } m_{a,K}\}$$

Folglich hat $m_{a,K}$ nur einfache Nullstellen, weshalb a separabel ist.

„⇓“ Falls alle $a \in L$ separabel sind, existieren separable $a_1, \ldots, a_n$, sodass $L = K(a_1, \ldots, a_n)$, da eine endliche Körpererweiterung vorliegt.

„⇐“ Sei $L = K(a_1, \ldots, a_n)$ mit separablen a_i. Zu zeigen ist, dass L/K separabel ist. Wir betrachten $L_0 := K$ sowie $L_i := L_{i-1}(a_i)$. Wegen (e) reicht es zu zeigen, dass L_i separabel über L_{i-1} für alle i ist.

Da a_i separabel über K ist, hat $m_{a_i,K}$ nur einfache Nullstellen. Wegen $m_{a_i,L_{i-1}} | m_{a_i,K}$ hat auch $m_{a_i,L_{i-1}}$ nur einfache Nullstellen. Es folgt (insbesondere die zweite Gleichheit):

$$[L_i : L_{i-1}] = \deg(m_{a_i,L_{i-1}}) = \#\{\text{ Nullstellen von } m_{a_i,L_{i-1}}\} \overset{3.16}{=} [L_i : L_{i-1}]_s$$

(c) Sei $\operatorname{char}(K) = 0$. Zu zeigen ist, dass L/K separabel ist. Wir können uns eine der bereits gezeigten Bedingungen aussuchen, zum Beispiel (a). Wir zeigen also, dass alle $a \in L$ separabel sind, indem wir nachweisen, dass $m_{a,K}$ nur einfache Nullstellen hat. Dazu ist $m'_{a,K} \neq 0$ zu zeigen. Da $\operatorname{char}(K) = 0$, gilt $\deg m_{a,K} = n \Rightarrow \deg m'_{a,K} = n - 1$. Daher gilt immer, dass $m'_{a,K} \neq 0$ ist, da entweder der Grad zu groß ist, oder die Ableitung konstant Eins wird.

(d) Es gilt $(x^n)' = nx^{n-1} = 0 \Leftrightarrow p | n$. Sei $a \in L$. Zu zeigen ist, dass a separabel ist. Über die Gradformel angewendet auf die Inklusionskette $K \subset K(a) \subset L$ folgt:

$$\begin{aligned} & p \nmid [L : K] = [L : K(a)] \cdot [K(a) : K] \\ \Rightarrow\ & p \nmid [K(a) : K] = \deg(m_{a,K}) \ \Rightarrow\ m'_{a,K} \neq 0; \Rightarrow\ a \text{ ist separabel} \end{aligned}$$

□

Theorem 4.8 Satz vom primitiven Element
Sei L/K endlich und separabel. Dann existiert ein $a \in L$ mit $L = K(a)$, das heißt, L ist eine einfache Körpererweiterung.

Im Beweis unterscheiden wir die beiden Fälle $|K| < \infty$ und $|K| = \infty$.

Im ersten Fall gilt $|K| < \infty \Rightarrow |L| < \infty \Rightarrow L^* = L \setminus \{0\}$ ist eine endliche multiplikative Gruppe. Wie wir sehen werden, erzwingen die Körperaxiome eine ganz spezielle Gruppenstruktur: L^* wird sich als zyklisch herausstellen. Wir zeigen sogar allgemeiner folgendes Lemma:

Lemma
Sei L irgendein Körper und $G \subset L^*$ eine endliche Gruppe. Dann ist G zyklisch.

Beweis :
Wegen $G \subset L^*$ muss G abelsch sein. Daher sind die p-Sylowuntergruppen von G eindeutig. Wir betrachten das Produkt $\prod_p \mathrm{Syl}_p(G) \subset G$.

$$|G| = p_1^{n_1} p_2^{n_2} \ldots = \left|\mathrm{Syl}_{p_1}(G)\right| \cdot \left|\mathrm{Syl}_{p_2}(G)\right| \cdots \qquad \Rightarrow\ G = \prod_p \mathrm{Syl}_p(G)$$

Zu zeigen ist, dass $\mathrm{Syl}_p(G)$ für alle p zyklisch ist. Die Gruppe ist abelsch und es gilt $\left|\mathrm{Syl}_p(G)\right| = p^n$. Zu zeigen ist daher, dass ein $x \in \mathrm{Syl}_p(G)$ mit $\mathrm{ord}(x) = p^n$ existiert. Falls kein solches x existiert, gilt $\forall_{y \in \mathrm{Syl}_p(G)} \colon \mathrm{ord}(y) \,|\, p^{n-1}$, also $y^{p^{n-1}} = 1$. Folglich sind alle (p^n-viele!) Elemente Nullstellen von $y^{p^{n-1}} - 1 = 0$. Dies widerspricht der Tatsache, dass im Körper L ein Polynom nicht mehr Nullstellen als sein Grad haben kann. $\mathrm{Syl}_p(G)$ muss also zyklisch sein.

$$\forall_{p \,|\, |G|} \ \Rightarrow\ G \simeq \prod_{p \,|\, |G|} \underbrace{\mathbb{Z}/n_p\mathbb{Z}}_{p-\mathrm{Syl}}\,, \qquad \text{wobei } n_p \text{ Potenz von } p \text{ ist}$$

$$\Rightarrow\ \mathrm{ggT}(n_p, n_{p'}) = 1 \text{ für } p \neq p' \ \Rightarrow\ G \simeq \mathbb{Z}/\prod n_p\mathbb{Z} \qquad \text{(chinesischer Restsatz)}$$

□

Beweis : **Satz vom primitiven Element**
1. Fall: $|K| < \infty$. Nach obigem Lemma ist

$$L^* = \langle a \rangle = \{a^n \colon n \in \mathbb{Z}\} \ \Rightarrow\ L = \{a^n \colon n \in \mathbb{Z}\} \cup \{0\} \ \Rightarrow\ L = K(a)$$

2. Fall: $|K| = \infty$. Hier verwenden wir, dass L/K separabel ist.

L/K endlich $\Rightarrow\ L = K(a_1, \ldots, a_n) \supset K(a_1, \ldots, a_{n-1}) \supset \ldots$ Mit Induktion genügt es zu zeigen, dass $L = K(a, b) \ \Rightarrow\ \exists_c \colon L = K(c)$.

Wir betrachten die Körper $K \subset L \subset \overline{K}$ und die verschiedenen K-Homomorphismen $\varphi_1, \ldots, \varphi_m \colon L \to \overline{K}$, wobei $m = [L : K]_s = [L : K]$ gilt, da L/K separabel ist. Sei

$$g(x) := \prod_{i<j} \Big((\varphi_i(a) - \varphi_j(a))x + \varphi_i(b) - \varphi_j(b) \Big)$$

Die Faktoren sind alle ungleich Null, da wegen $\varphi_i \neq \varphi_j$ aus $\varphi_i(a) = \varphi_j(a)$ folgt, dass $\varphi_i(b) \neq \varphi_j(b)$ ist. g ist also nicht das Nullpolynom. Da $|K| = \infty$ vorausgesetzt ist, existieren folglich unendlich viele $\lambda \in K$ mit $g(\lambda) \neq 0$. Man beachte, dass $\varphi_i(\lambda) = \lambda = \varphi_j(\lambda)$ gilt, da $\varphi_i|_K = \mathrm{id}$ ist. Wir erhalten

$$0 \neq g(\lambda) = \prod_{i<j} \Big((\varphi_i(a) - \varphi_j(a))\lambda + \varphi_i(b) - \varphi_j(b) \Big) = \prod_{i<j} \Big(\varphi_i(\lambda a + b) - \varphi_j(\lambda a + b) \Big)$$

$$\Rightarrow\ \varphi_i(\lambda a + b) \neq \varphi_j(\lambda a + b) \qquad \text{für } i \neq j$$

Wir zeigen, dass $\lambda a + b$ das gesuchte c mit $K(c) = L = K(a, b)$ ist.

Das Minimalpolynom $m_{\lambda a+b,K} \in K[x]$ hat unter anderem die Nullstelle $\lambda a + b$. Da φ_i ein K-Homomorphismus ist, gilt $\varphi_i^* m_{\lambda a+b,K} = m_{\lambda a+b,K}$. Folglich bildet φ_i Nullstellen des Minimalpolynoms auf ihresgleichen ab. $\varphi_i(\lambda a+b)$ sind also verschiedene Nullstellen für $i = 1, \ldots, m$. Wir folgern, dass $m_{\lambda a+b,K}$ mindestens vom Grad m ist und erhalten:

$$m \leq \deg(m_{\lambda a+b,K}) = [K(\lambda a + b) : K]$$
$$m = [L : K]_s = [L : K] = [L : K(\lambda a + b)] \cdot [K(\lambda a + b) : K]$$

$\Rightarrow\ [L : K(\lambda a + b)] = 1\ \Rightarrow\ L = K(\lambda a + b)$, das heißt, $c = \lambda a + b$ funktioniert. □

Theorem 4.9

(a) Sei $n \in \mathbb{N}$ und p eine Primzahl. Dann ist der Zerfällungskörper L von $f(x) = x^{p^n} - x$ ein Erweiterungskörper von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mit $[L : \mathbb{F}_p] = n$. Es gilt $|L| = p^n$ und $L = \{\text{Nullstellen von } f(x)\}$. Außerdem ist $L/\mathbb{F}_p$ algebraisch, separabel und normal.

Bezeichnung: $L =: \mathbb{F}_q$ für $q = p^n$. Man beachte aber, dass $L \ncong \mathbb{Z}/p^n\mathbb{Z}$, da letzteres für $n > 1$ kein Körper ist.

(b) $\mathbb{F}_q$ ist bis auf Isomorphie der einzige Körper mit $q = p^n$ Elementen. Jeder endliche Körper ist zu genau einem $\mathbb{F}_q$ isomorph.

(c) Die Gruppe $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$ ist zyklisch von Ordnung n und erzeugt von $Fr\colon x \mapsto x^p$, dem Frobenius-Automorphismus.

Das Theorem behauptet also, dass es für alle Primzahlen p und alle $n \in \mathbb{N}$ bis auf Isomorphie genau einen Körper $\mathbb{F}_q$ der Ordnung $q := p^n$ gibt. Dieses $\mathbb{F}_q$ ist algebraisch über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, separabel und normal. Ferner ist $\mathbb{F}_q$ gleich der Menge aller Nullstellen von $f(x) = x^{p^n} - x$. Außer diesen gibt es keine anderen endlichen Körper.

Beweis :

(a),(b) Sei K ein endlicher Körper der Charakteristik $\mathrm{char}(K) = p$ für eine Primzahl p. $\mathbb{F}_p = \{0, 1, \ldots, p-1\} \subset K\ \Rightarrow\ K$ ist Erweiterung von $\mathbb{F}_p$ vom Grad $[K : \mathbb{F}_p] =: n$. Das bedeutet, dass K ein $\mathbb{F}_p$ Vektorraum der Dimension n ist. Wir wissen dann über die Anzahl seiner Elemente, dass $|K| = p^n = q$ sowie $|K \setminus \{0\}| = |K^*| = q-1$ gilt. Wir folgern:

$$\forall_{x \in K^*}\ x^{p^n-1} = x^{|K^*|} = 1 \qquad \Rightarrow\ \forall_{x \in K}\ x^{p^n} - x = 0$$

Alle Elemente von K sind also Nullstellen des Polynoms $f(x) = x^{p^n} - x$. Sein Grad ist $\deg(f(x)) = p^n = |K|$ und wir erhalten $K = \{\text{Nullstellen von } f(x)\}$. Da deren Anzahl gleich dem Grad des Polynoms ist, müssen es lauter einfache Nullstellen sein. Folglich ist $K/\mathbb{F}_p$ separabel. Offensichtlich ist K der Zerfällungskörper von $f(x)$, also auch normal und eindeutig bis auf Isomorphie.

Es verbleibt die Existenz von K zu zeigen. Zu gegebenen p und n betrachten wir $f(x) = x^{p^n} - x$ über $\mathbb{F}_p$. In $\overline{\mathbb{F}_p}$ zerfällt $f(x)$, weshalb wir die Menge aller Nullstellen von $f(x)$ als Teilmenge von $\overline{\mathbb{F}_p}$ betrachten können. Wir zeigen, dass es sich dabei um einen Körper handelt, indem wir die Körperaxiome verifizieren. Offensichtlich sind 0 und 1 Nullstellen von $f(x)$. Sind a und b weitere Nullstellen, gilt:

$$\begin{aligned}(a+b)^q - (a+b) &= a^q + \overbrace{\sum \ldots}^{\equiv 0 \mod p} + b^q - a - b = 0\\ (ab)^q - ab &= \underbrace{(a^q - a)}_{=0} b^q + a \underbrace{(b^q - b)}_{=0} = 0\\ (a^{-1})^q - a^{-1} &= \underset{\| \\ a}{(a^q)^{-1}} - a^{-1} = 0\end{aligned}$$

Die Menge aller Nullstellen von $f(x)$ ist damit tatsächlich ein Körper über $\mathbb{F}_p$, also der Zerfällungskörper von $f(x)$. Zu zeigen ist noch, dass alle Nullstellen einfach sind. Dazu leiten wir ab:

$$f(x) = x^q - x \qquad\qquad f'(x) = \overset{\| \; p^n \equiv 0 \mod p}{q} x^{q-1} - 1 \equiv \overset{\not= \; 0}{-1} \mod p$$

Jede Nullstelle ist einfach, folglich ist deren Anzahl gleich $p^n = q$. Die Menge aller Nullstellen von $f(x)$ ist algebraisch, separabel und normal über $\mathbb{F}_p$.

(c) Der Frobeniusautomorphismus $Fr\colon x \mapsto x^p$ ist ein Körperautomorphismus (vgl. Übungspergament 5). Dieser ist injektiv, da $\mathbb{F}_p$ ein Körper ist, also surjektiv. Wir zeigen, dass tatsächlich $\langle Fr \rangle = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$ gilt.

Sei $s := \mathrm{ord}(Fr)$, also $Fr^s = \mathrm{id}$. Wegen $q = p^n$ zeigen wir, dass $n = s$ gilt.

$$\begin{aligned}&Fr^n(a) = (a^p)^{p\cdots} = a^{p^n} = a \;\Rightarrow\; s|n\\ &Fr^s(a) = a \;\Rightarrow\; a^{p^s} = a \;\Rightarrow\; a^{p^s} - a = 0\end{aligned}$$

Alle a sind also Nullstellen von $x^{p^s} - x$. Folglich hat dieses Polynom mindestens p^n Nullstellen woraus $s \geq n$ und damit $s = n$ beziehungsweise $\mathrm{ord}(Fr) = n$ folgt.

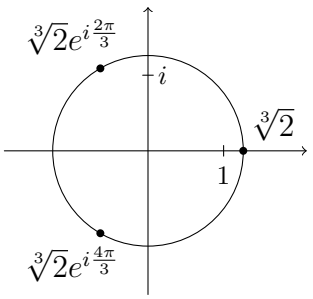
$$n = |\langle Fr \rangle| \leq \left|\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)\right| = [\mathbb{F}_q : \mathbb{F}_p]_s \leq [\mathbb{F}_q : \mathbb{F}_p] = n$$

Es gelten also lauter Gleichheiten, woraus die Behauptung $\langle Fr \rangle = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$ folgt.

□

Unser Ziel ist es, Körpererweiterungen L/K mit entsprechenden Automorphismengruppen $\mathrm{Aut}_K(L)$ (den „Symmetrien“) in Verbindung zu bringen. Allerdings kann das nicht immer funktionieren.

Als Gegenbeispiel dient wieder $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[3]{2})$. Das Polynom $x^3 - 2$ hat eine relle Nullstelle. Es gilt $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ und $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{\mathrm{id}\}$, weil der Automorphismus $\sqrt[3]{2}$ auf sich selbst abbilden muss. Um solche Fälle zu vermeiden, werden wir fordern, dass die Körpererweiterung normal sein muss.



Definition 4.10 **Galois**

Eine Körpererweiterung L/K heißt Galoiserweiterung oder galoissche Erweiterung, wenn L/K normal und separabel ist.

Die Gruppe $\mathrm{Aut}_K(L)$ heißt dann Galoisgruppe von L/K und wird mit $\mathrm{Gal}(L/K)$ oder $\mathrm{G}(L/K)$ bezeichnet.

(nach Evariste Galois, 1811-1832)

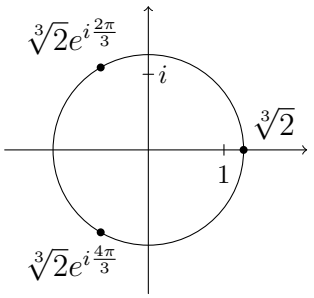
Ist L/K normal und separabel, gilt gemäß Definition 4.4:

$$|\mathrm{Aut}_K(L)| = [L:K] = [L:K]_s = \#\{K\text{-Hom}\colon L \to \overline{K}\}$$

Beispiel: Zerfällungskörper L von $f(x) = x^3 - 2$ über $\mathbb{Q} = K$

Das Polynom $f(x)$ ist vom Grad 3.

$$L \overset{\geq 1}{\supset} \mathbb{Q}(\sqrt[3]{2}) \overset{3}{\supset} \mathbb{Q}$$
$$L \ni \frac{\sqrt[3]{2}e^{i\frac{2\pi}{3}}}{\sqrt[3]{2}} = e^{i\frac{2\pi}{3}}$$



Folglich ist $L = \mathbb{Q}(\sqrt[3]{2}, e^{i\frac{2\pi}{3}})$.

$e^{i\frac{2\pi}{3}} \notin \mathbb{Q}$ ist Nullstelle von $x^3 - 1 = (x-1)(x^2+x+1)$. Sein Minimalpolynom hat Grad > 1, folglich muss es $x^2 + x + 1$ vom Grad 2 sein.

$$[\mathbb{Q}(e^{i\frac{2\pi}{3}}) : \mathbb{Q}] = 2$$
$$\Rightarrow\ [L:\mathbb{Q}] = 2 \cdot 3 = 6$$
$$6 = [L:\mathbb{Q}] = |\mathrm{Aut}_{\mathbb{Q}}(L)|$$

$$L = \mathbb{Q}\left(\sqrt[3]{2}, e^{i\frac{2\pi}{3}}\right) \overset{2}{\supset} \mathbb{Q}(\sqrt[3]{2})$$

Also gibt es 6 Automorphismen. Ein solches σ muss die Nullstellen von $x^3 - 2$ permutieren.

$$x^3 - 2 \qquad \{\sqrt[3]{2}\} \to \left\{\sqrt[3]{2}, \sqrt[3]{2}e^{i\frac{2\pi}{3}}, \sqrt[3]{2}e^{i\frac{4\pi}{3}}\right\}$$
$$x^2 + x + 1 \qquad \{e^{i\frac{2\pi}{3}}\} \to \left\{e^{i\frac{2\pi}{3}}, e^{i\frac{4\pi}{3}} = \overline{e^{i\frac{2\pi}{3}}}\right\}$$

$\sigma\colon L = \mathbb{Q}(\sqrt[3]{2}, e^{i\frac{2\pi}{3}}) \to L$ ist durch die Bilder von $\sqrt[3]{2}$ und $e^{i\frac{2\pi}{3}}$ festgelegt. Folglich gibt es für jede (unabhängige) Wahl der Bilder einen Autormorphismus.
$\Rightarrow$ $\mathrm{Aut}_K(L)$ = Gruppe der Permutationen von $\left\{\sqrt[3]{2}, \sqrt[3]{2}e^{i\frac{2\pi}{3}}, \sqrt[3]{2}e^{i\frac{4\pi}{3}}\right\}$ und damit isomorph zu Σ_3. Ein Beispiel ist

$$\sigma\colon z \mapsto \overline{z}$$
$$\sqrt[3]{2} \mapsto \sqrt[3]{2}$$
$$e^{i\frac{2\pi}{3}} \mapsto e^{i\frac{4\pi}{3}}$$

$\sigma\colon \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$ mit $a \mapsto a$ bleibt fest, $\mathbb{Q}(\sqrt[3]{2})$ sind genau die Fixpunkte von σ bzw. von $\langle\sigma\rangle = \{\sigma, \mathrm{id}\}$. Der Zwischenkörper $\mathbb{Q}(\sqrt[3]{2})$ ist die Menge der Fixpunkte einer Untergruppe von $\mathrm{Gal}(L/K)$.

Definition 4.11 **Fixkörper**

Sei L ein Körper und $G \subset \mathrm{Aut}(L)$ eine Untergruppe der Automorphismengruppe von L. Dann ist $L^G := \{a \in L\colon \varphi(a) = a\, \forall_{\varphi\in G}\}$ ein Körper und heißt Fixkörper von G.

Beweis :

Es muss verifiziert werden, dass L^G tatsächlich ein Körper ist:

$$\begin{aligned} \varphi(0) &= 0 & \varphi(ab) &= \varphi(a)\varphi(b) \\ \varphi(1) &= 1 & \varphi(a+b) &= \varphi(a) + \varphi(b) \\ \varphi(a^{-1}) &= \varphi(a)^{-1} & \Rightarrow\ & L^G \text{ ist ein Körper.} \end{aligned}$$

□

Proposition 4.12

Sei L/K eine Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L/K)$.
Dann gilt $L^G = K$, das heißt, K ist der Fixkörper der ganzen Galoisgruppe.

(Natürlich ist $L^{\{\mathrm{id}\}} = L$)

Beweis :

Wegen $G = \mathrm{Aut}_K(L)$ gilt nach Definition 3.15 $\forall_{\varphi\in G}\colon \varphi|_K = \mathrm{id}$ und wir erhalten sofort die Inklusion $K \subset L^G$. Wir zeigen daher für ein $a \in L \setminus K$, dass $a \notin L^G$ gilt, also ein $G \ni \varphi\colon a \mapsto \varphi(a) \neq a$ existiert. Wegen $a \in K(a) \supsetneq K$ ist das Minimalpolynom $m_{a,K}$ vom Grad ≥ 2 und hat damit dank Separabilität eine weitere Nullstelle $b \neq a$.

Aus Proposition 3.16 folgt, dass ein K-Automorphismus von $K(a)$ die Nullstellen von $m_{a,K}$ permutiert. Es existiert also ein $\varphi\colon a \mapsto b \neq a$. Aus Theorem 3.17 folgt die Existenz einer Fortsetzung $\varphi\colon L \to \overline{K}$ mit $a \mapsto b$. Nach Propositon 4.3 gilt dank Normalität $\mathrm{im}(\varphi) = L \ \Rightarrow\ G \ni \varphi\colon a \mapsto b \neq a$. □

Proposition 4.13

Sei L ein Körper und $H \subset \mathrm{Aut}(L)$ eine endliche Untergruppe. Dann ist L/L^H eine Galoiserweiterung mit Galoisgruppe $\mathrm{Gal}(L/L^H) = H$ und es gilt $[L : L^H] = |H|$.

Beweis :
Wir betrachten den Fixkörper $L^H = \{a \in L \colon \varphi(a) = a \,\forall_{\varphi \in H}\}$. Zu zeigen ist, dass L/L^H normal, separabel und endlich ist. Ersteres bedeutet, dass L Zerfällungskörper von Polynomen in $L^H[x]$ ist. Falls das stimmt, können wir das Minimalpolynom $m_{a,L^H} \in L^H[x]$ eines Elements $a \in L$ betrachten. a ist eine Nullstelle, außerdem auch $\varphi(a)$ für $\varphi \in H$. Dies sind endlich viele, da H endlich ist. Eventuell gibt es noch mehr Nullstellen. Ist L/L^H zudem separabel, ist jede Nullstelle einfach. Wir definieren

$$\{a = a_1, a_2, \ldots, a_n\} := \{\varphi(a) \colon \varphi \in H\} \qquad f_a(x) := \prod_{i=1}^{n} (x - a_i) \in L[x]$$

als Kandidaten für das Minimalpolynom von a. Wendet man φ^* auf f_a an, werden die Faktoren $(x - a_i)$ permutiert, denn $\varphi^*(x - a_i) = x - \varphi(a_i) = x - a_j$. Folglich ist $\varphi^* f_a = f_a$, das heißt $f_a \in L^H[x]$. Also ist L ist der Zerfällungskörper über L^H der Menge $\{f_a \colon a \in L\}$. Damit ist L/L^H normal. Die f_a haben einfache Nullstellen, folglich ist L/L^H auch separabel. Wir haben damit gezeigt, dass L/L^H tatsächlich eine Galoiserweiterung ist, falls sie endlich ist. Letzteres verbleibt noch zu zeigen. L ist zudem algebraisch über L^H, da $a \in L$ Nullstelle von $f_a \in L^H[x]$ ist.

Für $a \in L$ mit $f_a(a) = 0$ folgt $m_{a,L^H} \mid f_a$. Angenommen, es gelte $|H| \lneq [L : L^H]$. Falls $[L : L^H] < \infty$ ist, existiert eine endliche Menge $S \subset L$, sodass $L = L^H(S)$. Falls $[L : L^H] = \infty$ ist, existiert auch ein endliches $S \subset L$, sodass $L \supset L^H(S)$ und $[L^H(S) : L^H] > |H|$. Im Weiteren nennen wir $M := L^H(S)$ und betrachten M/L^H sowie $L^H \subset M \subset L$, wobei der Grad der ersten Erweiterung bereits $> |H|$ ist. Wegen $M \subset L$ haben Minimalpolynome über L^H nur einfache Nullstellen, woraus folgt, dass M/L^H separabel ist. Nach Theorem 4.8 existiert ein primitives Element c mit $M = L^H(c)$. Dieses c hat ein Minimalpolynom $m_{c,L^H} \mid f_c$. Dessen Grad ist $[M : L^H] = \deg(m_{c,L^H}) \leq \deg(f_c) \leq |H|$. Ein Widerspruch erwächst aus $[M : L^H] \leq |H| < [M : L^H]$, weshalb $|H| \geq [L : L^H]$ gelten muss und L/L^H endlich ist. Zuletzt zeigen wir die Gleichheit in dieser Ungleichung. $|H|$ darf wegen $H \subset \mathrm{Aut}(L)$ nicht zu groß sein. Nach Definition lässt H den Fixkörper L^H fest.

$$\begin{aligned}
&\Rightarrow\ H \subset \mathrm{Aut}_{L^H}(L) = \mathrm{Gal}(L/L^H) \\
&\Rightarrow\ |H| \leq |\mathrm{Aut}_{L^H}(L)| = [L : L^H] && \text{(normal, separabel)} \\
&\Rightarrow\ |H| = [L : L^H] = |\mathrm{Aut}_{L^H}(L)| && \text{(wegen } |H| \geq [L : L^H]\text{, s.o.)} \\
&\Rightarrow\ H = \mathrm{Aut}_{L^H}(L) = \mathrm{Gal}(L/L^H)
\end{aligned}$$

Damit folgt auch $\quad f_a = m_{a,L^H} = \prod_{\varphi \in \mathrm{Gal}(L/L^H)} (x - \varphi(a))$. □

Wir sind nun soweit den Hauptsatz der Galoistheorie formulieren zu können.

Theorem 4.14 **Hauptsatz der Galoistheorie**

Sei L/K eine Galoiserweiterung und $U := \{H < \mathrm{Gal}(L/K)\}$ die Menge aller Untergruppen der Galoisgruppe. Sei ferner $Z := \{M\colon K \subset M \subset L\,, M \text{ Zwischenkörper}\}$.

Dann gibt es zwei zueinander inverse Bijektionen

$$\begin{aligned} \alpha\colon Z &\to U & \qquad \beta\colon U &\to Z \\ M &\mapsto \mathrm{Gal}(L/M) & H &\mapsto L^H \end{aligned}$$

wobei L/M galoissch ist. α und β kehren Inklusionen um:

$$M \subset M' \;\Rightarrow\; \alpha(M) \supset \alpha(M') \qquad\qquad H \subset H' \;\Rightarrow\; \beta(H) \supset \beta(H')$$

Für $H \in U$ und $\varphi \in \mathrm{Gal}(L/K)$ gilt $\varphi(L^H) = L^{\varphi H \varphi^{-1}}$.

Insbesondere entspricht eine normale Untergruppe einer normalen Körpererweiterung: Für einen Zwischenkörper $M \in Z$ ist die Erweiterung M/K normal genau dann, wenn $\mathrm{Gal}(L/M) \triangleleft \mathrm{Gal}(L/K)$. In diesem Fall gibt es einen surjektiven Gruppenhomomorphismus

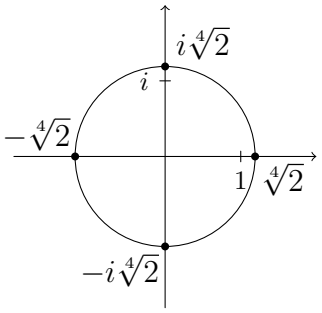
$$\gamma\colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) \qquad \text{mit } \ker(\gamma) = \mathrm{Gal}(L/M)$$

und es gilt die Kürzungsregel $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)\big/\mathrm{Gal}(L/M)$.

Wir erhalten also eine komplette Übersetzung zwischen Gruppentheorie und Körpererweiterungstheorie. Bevor wir den Hauptsatz beweisen, wollen wir ein größeres Beispiel betrachten, das uns eine Weile beschäftigen wird.

Gegeben sei $f(x) := x^4 - 2 \in \mathbb{Q}[x]$ mit Zerfällungskörper L. In $L \subset \mathbb{C}$ liegen die vier Nullstellen von f:

$$\pm\sqrt[4]{2} \in \mathbb{R} \qquad\qquad \pm i\sqrt[4]{2} \notin \mathbb{R}$$



Es gilt $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ und $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$, da $x^4 - 2$ irreduzibel und damit Minimalpolynom von $\sqrt[4]{2}$ ist. Aus $\pm i \in L \supset \mathbb{Q}(\sqrt[4]{2}\,, i) \supset L$ folgt $L = \mathbb{Q}(\sqrt[4]{2}\,, i)$. Ferner ist

$$\begin{aligned} m_{i,\mathbb{Q}}(x) = x^2 + 1 \;&\Rightarrow\; m_{i,\mathbb{Q}(\sqrt[4]{2})} \,|\, x^2 + 1 \\ i \notin \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R} \;&\Rightarrow\; \deg\Big(m_{i,\mathbb{Q}(\sqrt[4]{2})}\Big) = 2 \;\Rightarrow\; m_{i,\mathbb{Q}(\sqrt[4]{2})} = x^2 + 1 \\ L = \mathbb{Q}(\sqrt[4]{2}\,, i) \overset{2}{\supset} \mathbb{Q}(\sqrt[4]{2}) \overset{4}{\supset} \mathbb{Q} \;&\Rightarrow\; [L : \mathbb{Q}] = 8 \;\Rightarrow\; |\mathrm{Gal}(L/\mathbb{Q})| = 8 \end{aligned}$$

Von Proposition 4.7 (c) wissen wir zudem, dass $L/\mathbb{Q}$ wegen $\mathrm{char}\,\mathbb{Q} = 0$ separabel ist. Wie sehen nun die acht Automorphismen aus?

Betrachte dazu $\mathbb{Q}(\sqrt[4]{2})$ und einen Automorphismus $\varphi\colon \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$. Dieser muss $\sqrt[4]{2}$ auf eine Nullstelle von $x^4 - 2$ in $\mathbb{Q}(\sqrt[4]{2})$ abbilden, also auf $\pm\sqrt[4]{2}$.
Betrachte analog $\mathbb{Q}(i)$ und einen Automorphismus $\psi\colon \mathbb{Q}(i) \to \mathbb{Q}(i)$, der wiederum i auf Nullstellen von $x^2 + 1$ abbilden muss, also auf $\pm i$.
Allerdings bekommen wir damit noch keine 8 Abbildungen zusammen.

Für die Grade der Erweiterungen gilt $L \overset{4}{\supset} \mathbb{Q}(i) \overset{2}{\supset} \mathbb{Q}$ und $L \overset{2}{\supset} \mathbb{Q}(\sqrt[4]{2}) \overset{4}{\supset} \mathbb{Q}$.

Wegen $\mathrm{Aut}_{\mathbb{Q}(i)}(L) \subset \mathrm{Aut}_{\mathbb{Q}}(L)$ betrachten wir zunächst die Körpererweiterung $L/\mathbb{Q}(i)$. Dann ist $L = \mathbb{Q}(i)(\sqrt[4]{2})$ vom Grad 4, weshalb $x^4 - 2$ irreduzibel über $\mathbb{Q}(i)$ bleibt.

$L/\mathbb{Q}(i)$ ist normal (Zerfällungskörper von $f(x) = x^4 - 2$), separabel, endlich, einfach.

Wir betrachten eine Abbildung aus $\mathrm{Gal}(L/\mathbb{Q}(i))$. Eine solche bildet eine Nullstelle von f auf eine beliebige Nullstelle von f ab. Ein Beispiel ist etwa $\sigma \in \mathrm{Gal}(L/\mathbb{Q}(i)) \subset \mathrm{Gal}(L/\mathbb{Q})$ mit $\sigma\colon \sqrt[4]{2} \mapsto i\sqrt[4]{2}$.

Ebenso bleibt $x^2 + 1$ wegen $[L : \mathbb{Q}(\sqrt[4]{2})] = 2$ irreduzibel über $\mathbb{Q}(\sqrt[4]{2})$ und es liegt eine Galoiserweiterung vor. $\left|\mathrm{Gal}(L/\mathbb{Q}(\sqrt[4]{2}))\right| = 2 \;\Rightarrow\; \exists\tau \in \mathrm{Gal}(L/\mathbb{Q}(\sqrt[4]{2})) \subset \mathrm{Gal}(L/\mathbb{Q})$ mit $\tau\colon i \mapsto -i$

Obiges σ muss i auf i abbilden, da es in $\mathrm{Gal}(L/\mathbb{Q}(i))$ liegt. Analog gilt $\tau\colon \sqrt[4]{2} \mapsto \sqrt[4]{2}$. Folglich sind $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ und durch die Bilder von $\sqrt[4]{2}$ und i bestimmt. Bilden wir Kompositionen von σ und τ, ergibt sich zunächst:

$$\begin{aligned}
&\sigma\colon \sqrt[4]{2} \mapsto i\sqrt[4]{2} && i \mapsto i\\
&\sigma^2\colon \sqrt[4]{2} \mapsto \sigma(i)\sigma(\sqrt[4]{2}) = -\sqrt[4]{2} && i \mapsto i\\
&\sigma^3\colon \sqrt[4]{2} \mapsto -i\sqrt[4]{2} && i \mapsto i\\
&\sigma^4 = \mathrm{id} && i \mapsto i
\end{aligned}$$

Es gilt also $|\langle\sigma\rangle| = 4$. Folglich ist $H_1 := \langle\sigma\rangle$ ein Normalteiler von $\mathrm{Gal}(L/\mathbb{Q})$, da der Index von H_1 in G gleich $\frac{8}{4} = 2$ ist (vgl. Beispiel: Normalteiler).

Weitere Elemente sind $\tau \circ H_1 = \{\tau\,, \tau\circ\sigma\,, \tau\circ\sigma^2\,, \tau\circ\sigma^3\}$:

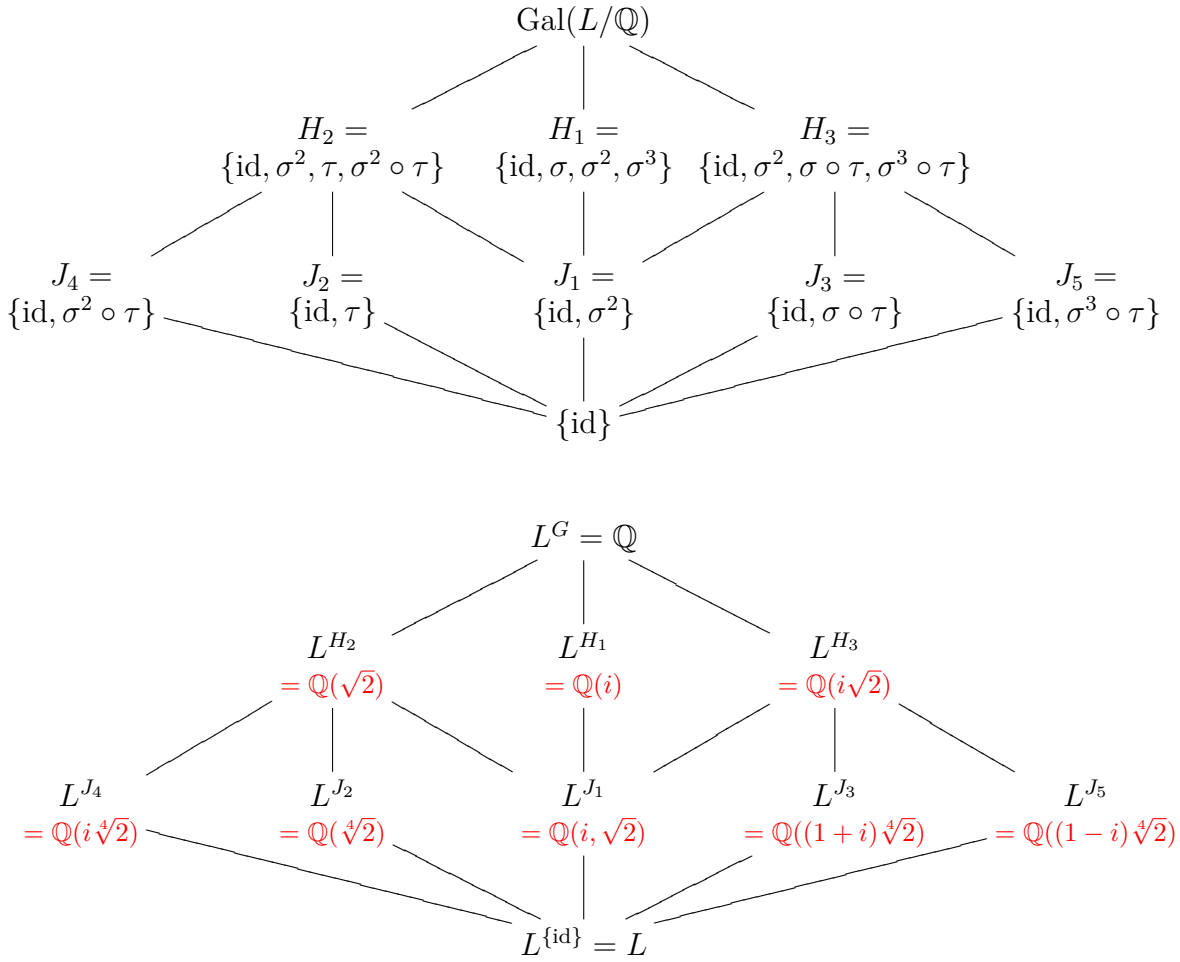
$$\begin{aligned}
\tau\colon \sqrt[4]{2} &\mapsto \sqrt[4]{2} && i \mapsto -i\\
\tau\circ\sigma = \sigma^3\circ\tau\colon \sqrt[4]{2} &\mapsto -i\sqrt[4]{2} && i \mapsto -i\\
\tau\circ\sigma^2 = \sigma^2\circ\tau\colon \sqrt[4]{2} &\mapsto -\sqrt[4]{2} && i \mapsto -i\\
\tau\circ\sigma^3 = \sigma\circ\tau\colon \sqrt[4]{2} &\mapsto i\sqrt[4]{2} && i \mapsto -i
\end{aligned}$$

Damit haben wir die 8 Elemente von $\mathrm{Gal}(L/K)$ gefunden. Wir haben oben gesehen, dass $\mathrm{Gal}(L/K) = H_1 \dot\cup (\tau \circ H_1)$ in zwei Nebenklassen zerfällt. Diese Gruppe kennen wir bereits: Es handelt sich um die Diedergruppe, also die Symmetriegruppe eines Quadrats. Dabei entspricht σ der Drehung und τ der Spiegelung. Von dieser Gruppe können wir die Untergruppen leicht bestimmen. Wegen $|\mathrm{Gal}(L/K)| = 8$ gibt es Untergruppen mit $1, 2, 4$ und 8 Elementen.

$|H| = 2$: Die zweielementigen Untergruppen sind von der Gestalt $H = \{\mathrm{id}, g\}$ mit $g^2 = \mathrm{id}$. Offenbar hat die Identität Ordnung 1. Die Elemente σ und σ^3 haben beide die

Ordnung 4. Alle anderen Elemente sind von der Ordnung 2 und kommen daher für g in Frage. Exemplarisch bestätigen wir: $(\tau \circ \sigma)^2 = \tau \circ \underbrace{\sigma \circ \tau}_{\tau \circ \sigma^3} \circ \sigma = \tau^2 \circ \sigma^4 = \mathrm{id}$

$|H| = 4$: Wir kennen bereits $H_1 = \langle \sigma \rangle = \langle \sigma^3 \rangle$ mit $|H_1| = 4$. Diese Untergruppe ist zyklisch der Ordnung 4. Gemäß Proposition 1.13 impliziert $|G| = p^2$ mit Primzahl p, dass G abelsch ist. Folglich sind alle weiteren Untergruppen der Ordnung 4 isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und werden von kommutierenden Elementen der Ordnung 2 erzeugt. Wir haben nachgerechnet, dass σ^2, τ sowie $\sigma^2, \tau \circ \sigma$ kommutieren. Insgesamt erhalten wir drei Untergruppen mit 4 Elementen.



Zuerst soll L^{H_1} bestimmt werden. $|H_1| = 4 \Rightarrow [L^{H_1} : L^G] = 2$. Nach Proposition 4.13 ist $[L : L^H] = |H|$. Wegen $H_1 = \langle \sigma \rangle$ und $\sigma(i) = i$ ist $i \in L^{H_1}$. Es folgt $L^{H_1} = \mathbb{Q}(i)$.

Bei $H_2 = \langle \tau, \sigma^2 \rangle$ sehen wir nicht wie oben sofort was L^{H_2} sein muss. Daher wird es über Gleichungen bestimmt. $\{1, i, \sqrt[4]{2}, i\sqrt[4]{2}, \sqrt{2}, i\sqrt{2}, \sqrt[4]{8}, i\sqrt[4]{8}\}$ bildet eine Basis von L/K. Ein Element in L ist daher von der Form $\lambda_1 \cdot 1 + \lambda_2 \cdot i + \lambda_3 \cdot \sqrt[4]{2} + \ldots + \lambda_8 \cdot i\sqrt[4]{8}$.
Wir wenden τ und σ an und vergleichen die Koeffizienten: $\sqrt{2}$ bleibt unter τ: $\sqrt[4]{2} \mapsto \sqrt[4]{2}$ und unter σ^2: $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$ fest. Daraus erhalten wir $L^{H_2} = \mathbb{Q}(\sqrt{2})$.

Das Element $i\sqrt{2}$ wird von $H_3 = \langle \sigma^2, \sigma \circ \tau \rangle$ festgehalten und ist wegen $(i\sqrt{2})^2 = -2$ von der Ordnung 2. Wir erhalten $L^{H_3} = \mathbb{Q}(i\sqrt{2})$.

In allen L^{J_i} muss $\mathbb{Q}(\sqrt[4]{2})$ vorkommen. Über die Inklusionsbedingung erhält man sofort $L^{J_1} = \mathbb{Q}(i, \sqrt{2})$. Genauso muss $\mathbb{Q}(\sqrt[4]{2})$ entweder L^{J_2} oder L^{J_4} sein. Wegen $J_2 = \langle\tau\rangle$ und $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$ gilt $\mathbb{Q}(\sqrt[4]{2}) \subset L^{J_2}$ und damit $\mathbb{Q}(\sqrt[4]{2}) = L^{J_2}$. Es verbleibt $L^{J_4} = \mathbb{Q}(i\sqrt[4]{2})$.

Untersucht man $J_3 = \{\mathrm{id}, \sigma\circ\tau = \tau\circ\sigma^3\}$ genauer, erkennt man, dass $\sqrt[4]{2}+i\sqrt[4]{2}$ festgehalten wird. Zu zeigen ist, dass es von der Ordnung 4 ist. Dies folgt aus $((1+i)\sqrt[4]{2})^2 = 2i\sqrt{2}$ und $(2i\sqrt{2})^2 \in \mathbb{Q}$. Folglich ist $L^{J_3} = \mathbb{Q}((1+i)\sqrt[4]{2})$.

$$\begin{aligned} \sigma\circ\tau\colon i &\mapsto -i \\ \sqrt[4]{2} &\mapsto i\sqrt[4]{2} \\ i\sqrt[4]{2} &\mapsto \sqrt[4]{2} \\ \Rightarrow\ \sqrt[4]{2}+i\sqrt[4]{2} &\mapsto \sqrt[4]{2}+i\sqrt[4]{2} \end{aligned}$$

Damit sind alle Zwischenkörper von L bestimmt.

Beweis : **Hauptsatz der Galoistheorie**

Zu zeigen ist, dass L/M galoisch, also normal und separabel ist.

$$U \underset{\beta}{\overset{\alpha}{\leftrightarrows}} Z \qquad \alpha\colon M \mapsto \mathrm{Gal}(L/M) \qquad \beta\colon H \mapsto L^H$$

Aus Proposition 4.7 (e) folgt mit $K \supset M \supset L$, dass L/K separabel ist genau dann, wenn L/M und M/K separabel sind. Hier ist L/K separabel, woraus wir schließen, dass auch L/M separabel ist. L/K ist normal, weshalb $L = K(S)$ gilt, wobei S eine Menge von Nullstellen von irgendwelchen Polynomen über K sei. Dieselben Polynome über M haben dieselben Nullstellen.Wir können also $L = M(S)$ folgern. L/M ist also auch normal und damit eine Galoiserweiterung.

Wir zeigen, dass α und β zueinander inverse Bijektionen sind. Dazu betrachten wir zunächst einen Zwischenkörper $M \in Z$. Wir erhalten:

$$M \overset{\alpha}{\longmapsto} \mathrm{Gal}(L/M) = H \overset{\beta}{\longmapsto} L^H = L^{\mathrm{Gal}(L/M)}$$

Da L/M galoissch ist, folgt $L^{\mathrm{Gal}(L/M)} = M$ gemäß Proposition 4.12. Umgekehrt sei $H \in U$. Dann erhalten wir

$$H \overset{\beta}{\longmapsto} L^H =: M \overset{\alpha}{\longmapsto} \mathrm{Gal}(L/M)$$

Im Proposition 4.13 haben wir bereits gezeigt, dass dann $H = \mathrm{Gal}(L/L^H)$ gilt. Also sind α und β zueinander inverse Bijektionen. Es verbleibt der Beweis der Zusatzeigenschaften.

Wir zeigen zuerst, dass α und β Inklusionen umkehren. Für $M_1 \subset M_2$ folgt $\alpha(M_1) \supset \alpha(M_2)$ aus

$$\begin{aligned} \alpha(M_1) &= \mathrm{Gal}(L/M_1) = \{\tau\colon L \to L, \tau|_{M_1} = \mathrm{id}\} \\ \alpha(M_2) &= \mathrm{Gal}(L/M_2) = \{\sigma\colon L \to L, \sigma|_{M_2} = \mathrm{id}\} \end{aligned}$$

Für $H_1 \subset H_2$ folgt $\beta(H_1) \supset \beta(H_2)$ über

$$\begin{aligned} \beta(H_1) = L^{H_1} &= \{x \in L\colon h(x) = x\,\forall_{h\in H_1}\} \\ \beta(H_2) = L^{H_2} &= \{y \in L\colon g(y) = y\,\forall_{g\in H_2}\} \\ \{x \in L\colon h(x) = x\,\forall_{h\in H_1}\} &\supset \{y \in L\colon g(y) = y\,\forall_{g\in H_2}\} \end{aligned}$$

Als nächstes ist für $H \in U$ und $\varphi \in \mathrm{Gal}(L/K)$ die Gleichheit $\varphi(L^H) = L^{\varphi H \varphi^{-1}}$ zu zeigen. Sei $a \in L$.

$$\begin{aligned} a \in L^H \;&\Leftrightarrow\; \sigma(a) = a \,\forall_{\sigma \in H} \;\Leftrightarrow\; (\varphi \circ \sigma)(a) = \varphi(a) \,\forall_{\sigma \in H} \qquad (\varphi \text{ ist Isomorphismus}) \\ &\Leftrightarrow\; (\varphi \circ \sigma \circ \varphi^{-1})(\varphi(a)) = \varphi(a) \,\forall_{\sigma \in H} \\ &\Leftrightarrow\; \varphi(a) \text{ fix unter } \varphi H \varphi^{-1} \end{aligned}$$

Nun zeigen wir für $M \in Z$ die Äquivalenz M/K normal $\Leftrightarrow$ $\mathrm{Gal}(L/M) \triangleleft \mathrm{Gal}(L/K)$.

„$\Rightarrow$“ Sei $M \in Z$, also $M = L^H$ für ein $H \in U$ und M/K normal. Nach Proposition 4.3 (c) bedeutet dies, dass $\forall_{\varphi\colon M \to \overline{K}} \; \varphi(M) = M$ gilt. Wir erhalten damit:

$$\begin{aligned} L^H = M = \varphi(M) = \varphi(L^H) = L^{\varphi H \varphi^{-1}} \;&\Rightarrow\; L^H = L^{\varphi H \varphi^{-1}} \,\forall_{\varphi} \\ &\Rightarrow\; H = \varphi H \varphi^{-1} \,\forall_{\varphi \in \mathrm{Gal}(M/K)} \;\Rightarrow\; H \text{ ist normal} \end{aligned}$$

„$\Leftarrow$“ Sei $H := \mathrm{Gal}(L/M) \triangleleft \mathrm{Gal}(L/K)$, also $M = L^H$ und $L/M = L/L^H$. Nach Proposition 4.13 hat L/L^H die Galoisgruppe H. Diese ist normal. Das bedeutet, dass G/H eine Gruppe ist, welche auf L^H wie folgt operiert: für $a \in L^H$ definiere $(gH)(a) := g(a)$. Es muss die Wohldefiniertheit überprüft werden. Da H normal ist, zeigen wir dazu für $g(a) \in L^H$ und $h, \tilde{h} \in H$, dass $hg(a) = g\tilde{h}(a) = g(a)$ gilt. Wegen $gH = ghH$ gilt tatsächlich $g(a) = gh(a)$. Also operiert die Gruppe G/H auf L^H. Wir erhalten die Identitäten:

$$M^{G/H} = (L^H)^{G/H} = L^G = K$$

Propostion 4.13 besagt: $M/M^{G/H}$ ist galoisch mit Galoisgruppe

$$\mathrm{Gal}(M/M^{G/H}) = G/H = \mathrm{Gal}(L^H/K) = \mathrm{Gal}(L/K) \Big/ \mathrm{Gal}(L/L^H)$$

□

5 Anwendungen

Wir betrachten zwei Klassen von Anwendungen: Zum einen geometrische Konstruktionen und zum anderen polynomiale Gleichungen.

Konstruktion mit Zirkel und Lineal

Geometrische Konstruktionen können durch Körpererweiterungen modelliert werden. Gegeben sei ein $M \subset \mathbb{R}^2 = \mathbb{C}$, sowie ein Lineal ohne Markierung nebst einem Zirkel. Ziel ist es, die Unlösbarkeit von klassischen Problemen wie der Würfelverdopplung oder Winkeldreiteilung zu zeigen. Erlaubt sind drei elementare Konstruktionen zu folgenden Daten:

Definition

Für $p, q \in M$ mit $p \neq q$ sei $p \vee q$ die Gerade durch p und q.

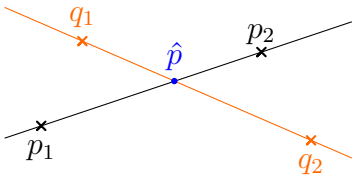
Für $p, q_1, q_2 \in M$ sei $K(p, \rho)$ der Kreis um p mit Radius $\rho = |q_1 - q_2|$.

Konstruktion I
Schnittpunkt zweier Geraden

Gegeben seien Punkte $p_1 \neq p_2$ und $q_1 \neq q_2$ mit

$$(p_1 \vee p_2) \neq (q_1 \vee q_2) \;\Rightarrow\; \hat{p} := (p_1 \vee p_2) \cap (q_1 \vee q_2)$$

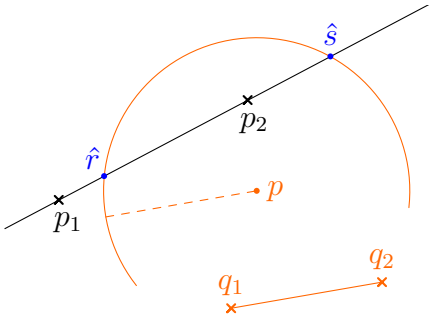
Falls existent, ist der Schnittpunkt „konstruiert“.



Konstruktion II
Schnitt einer Geraden mit einem Kreis

Gegeben seien $p_1 \neq p_2$, ein Punkt p, sowie $q_1 \neq q_2$. Dann ist

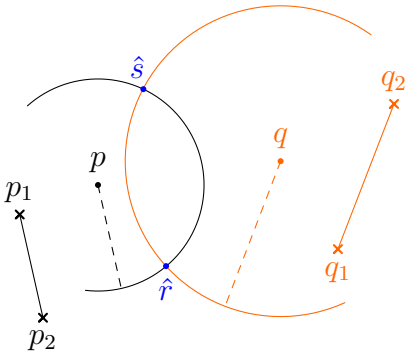
$$(p_1 \vee p_2) \cap K\Big(p, |q_1 - q_2|\Big) =: \{\hat{r}, \hat{s}\}$$



Konstruktion III
Schnitt von zwei Kreisen

Gegeben seien p und $p_1 \neq p_2$ sowie q und $q_1 \neq q_2$. Dann ist

$$K\Big(p, |p_1 - p_2|\Big) \cap K\Big(q, |q_1 - q_2|\Big) =: \{\hat{r}, \hat{s}\}$$



Definition 5.1
Sei $M \subset \mathbb{R}^2 = \mathbb{C}$. Ein Punkt $p \in \mathbb{C}$ heißt (aus M mit Zirkel und Lineal) konstruierbar genau dann, wenn eine natürliche Zahl $n \in \mathbb{N}$ und eine Kette $M = M_0 \subset M_1 \subset \ldots \subset M_n$ existieren, sodass $p \in M_n$ und jedes M_i aus M_{i-1} durch einen der obigen Konstruktionsschritte I bis III entsteht. Wir bezeichnen:

$$\mathrm{Kon}(M) := \{p \in \mathbb{R}^2 \colon p \text{ aus } M \text{ konstruierbar}\}$$

Beispiel: Würfelverdopplung
Gegeben sei ein Würfel mit Volumen beziehungsweise Kantenlänge 1. Ist daraus ein Würfel mit Volumen 2 beziehungsweise eine Würfelkante der Länge $\sqrt[3]{2}$ konstruierbar? In anderen Worten: Liegt $\sqrt[3]{2} \in \mathrm{Kon}(0,1)$?

Wir nehmen generell an, dass $|M| \geq 2$, genauer $M \supset \{0 = (0,0), 1 = (1,0)\}$ gilt.

Theorem 5.2
Sei $0, 1 \in M \subset \mathbb{C}$. Dann gilt:

(a) $\mathrm{Kon}(M)$ ist ein Teilkörper von $\mathbb{C}$.

(b) $\mathrm{Kon}(M) = \overline{\mathrm{Kon}(M)} = \{\overline{z} \colon z \in \mathrm{Kon}(M)\}$ (hier bezeichne $\overline{z}$ das komplexe Konjugat)

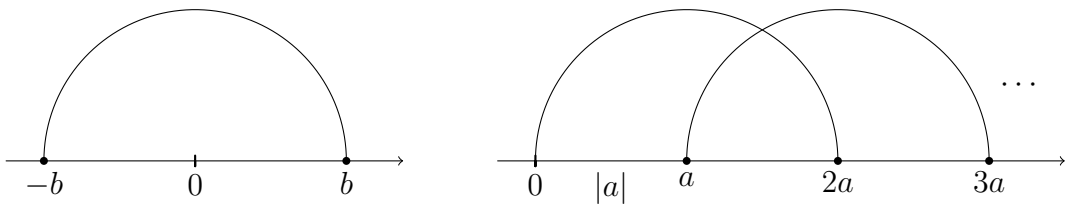
(c) $\mathbb{Q}(M \cup \overline{M})$ ist ein Teilkörper von $\mathrm{Kon}(M)$

(d) Für $b \in \mathbb{C}$ gilt: $b^2 \in \mathrm{Kon}(M) \Rightarrow b \in \mathrm{Kon}(M)$, das heißt $\mathrm{Kon}(M)$ ist quadratisch abgeschlossen (vgl. Übungsblatt 8).

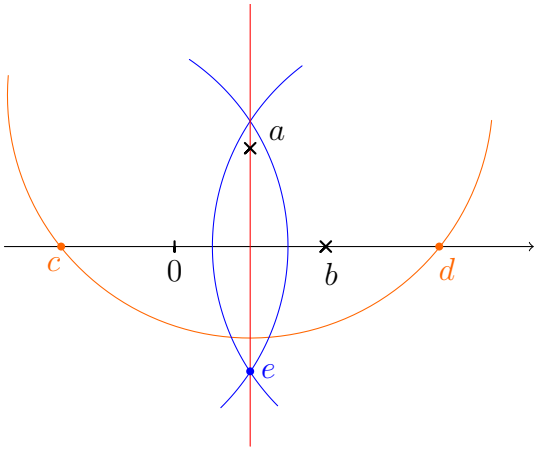
Also kann man mit Zirkel und Lineal addieren, subtrahieren, multiplizieren, dividieren, und Quadratwurzeln ziehen.

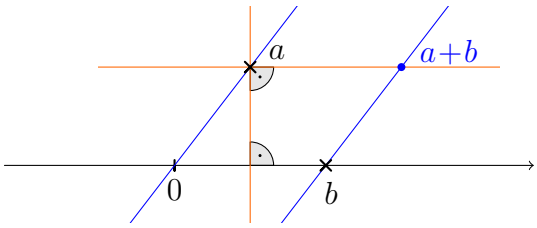
Beweis :

(a) Offensichtlich ist $-b$ zu gegebenem b konstruierbar. Ferner ist klar, dass betragsmäßig beliebig große Zahlen konstruierbar sind.

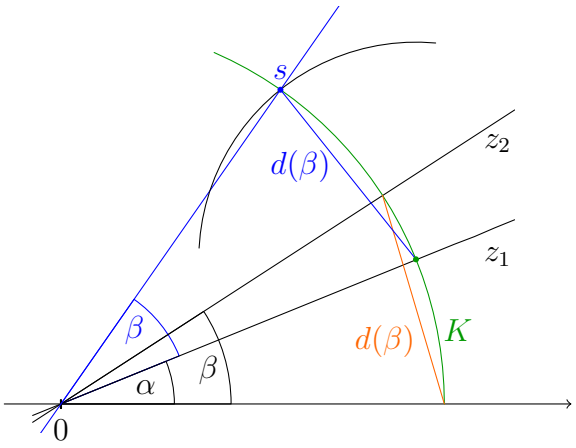


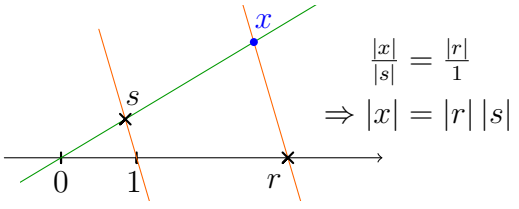
Addition: Die Konstruktion der Summe $a + b$ zweier komplexer Zahlen a und b wird über ein Parallelogramm realisiert. Dazu sei zunächst die Konstruktion einer Senkrechten durch einen Punkt zu einer Geraden gezeigt:
Gegeben seien die Punkte $0, b$ und a.
Ein großer Kreis um a schneide die Gerade $(0 \vee b)$ in c und d. Kreise um c, d mit Radius $> |a - c|$ schneiden sich in $e \neq a$. Durch die Wahl des Radius ist der Fall $a \in (0 \vee b)$ nicht ausgeschlossen.
Aus der Schule wissen wir, dass die Gerade $(a \vee e)$ senkrecht zu $(0 \vee b)$ steht. Zu gegebenem a ist also eine Senkrechte zu $(0 \vee b)$ durch a konstruierbar. Dann kann aber auch über zwei Senkrechte eine Parallele durch a zu $(0 \vee b)$ konstruiert werden. Genauso konstruieren wir eine Parallele zu $(0 \vee a)$ durch b. Diese schneidet die vorige Parallele in $a + b$.



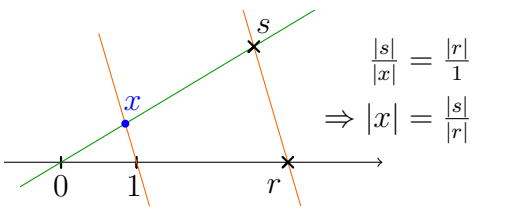


Multiplikation: Die Multiplikation komplexer Zahlen entspricht der Addition von Winkeln und der Multiplikation von Beträgen.
Gegeben seien zwei Winkel α und β, die es zu addieren gilt. Die x-Achse ist als Gerade bekannt. Man zeichne einen großen Kreis K um 0. Dann ist der Winkel β bezüglich K durch die Streckenlänge $d(\beta)$ bestimmt. Ein Kreis mit Radius $d(\beta)$ um den Punkt $(0 \vee z_1) \cap K$ schneide K in s. Dann schließt $(0 \vee s)$ mit der x-Achse den Winkel $\alpha + \beta$ ein.
Es sollen Beträge $|r|, |s| \in \mathbb{R}_+$ multipliziert werden. OBdA liege $r \in (0 \vee 1)$ und $s \notin (0 \vee r)$. Die Konstruktion paralleler Geraden ermöglicht die Anwendung des Strahlensatzes.

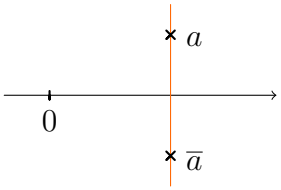




Division/Inverse werden über Subtraktion von Winkeln und Division positiver reeller Zahlen verwirklicht. Letzteres gelingt wieder mithilfe des Strahlensatzes, wobei die Rollen der Punkte vertauscht werden.
$\Rightarrow$ Kon(M) ist ein Teilkörper von $\mathbb{C}$.



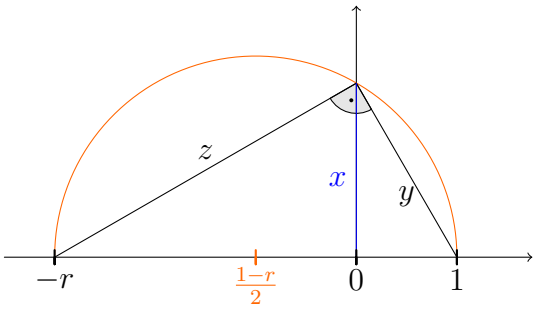
(b) **komplexe Konjugation:**
Zu einer komplexen Zahl a kann über eine Senkrechte stets die komplex konjugierte Zahl $\overline{a}$ konstruiert werden.



(d) Das Argument α einer komplexen Zahl $w = |w|\, e^{i\alpha}$ soll halbiert und $\sqrt{|w|}$ in $\mathbb{R}$ konstruiert werden. Über eine Mittelsenkrechte durch 0 und 1 ist $\frac{1}{2}$ und damit auch $\alpha \cdot \frac{1}{2}$ konstruierbar.

reelle Quadratwurzel: Die Mittelsenkrechte von $-r$ und 1 schneidet die x-Achse im Punkt $\frac{1-r}{2}$. Nach dem Satz von Thales schneidet der Kreis um $\frac{1-r}{2}$ durch 1 (und $-r$) die y-Achse in der Spize eines rechtwinkligen Dreiecks. Vielfache Anwendung des Satzes von Pythagoras ergibt:

$$\begin{aligned} y^2 &= x^2 + 1^2 \\ z^2 &= x^2 + r^2 \\ (r+1)^2 &= z^2 + y^2 \\ &= r^2 + 2r + 1 \\ z^2 - y^2 &= r^2 - 1 \\ z^2 + y^2 &= r^2 + 2r + 1 \\ \Rightarrow\ 2z^2 &= 2r^2 + 2r \\ \Rightarrow\ z^2 &= r^2 + r \ \Rightarrow\ z = \sqrt{r^2 + r} \\ \Rightarrow\ y &= \sqrt{r+1} \ \Rightarrow\ x = \sqrt{r} \end{aligned}$$



Folglich sind reelle Quadratwurzeln konstruierbar.

□

$0, 1 \in \mathrm{Kon}(M) \ \Rightarrow\ \mathbb{Q} \subset \mathrm{Kon}(M)$ Teilkörper $\ \Rightarrow\ \mathrm{Kon}(\{0,1\}) = \mathrm{Kon}(\mathbb{Q})$

$\mathrm{Kon}(\mathbb{Q})$ ist echt kleiner als $\mathbb{C}$, hat aber unendlichen Grad über $\mathbb{Q} \not\ni \sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots$

Theorem 5.3
Sei $0, 1 \in M \subset \mathbb{C}$. Dann gilt:

(a) $\mathrm{Kon}(M) \big/ \mathbb{Q}(M \cup \overline{M})$ ist eine algebraische Körpererweiterung.

(b) Ein $z \in \mathbb{C}$ ist genau dann aus M konstruierbar, wenn eine Kette

$$\mathbb{Q}(M \cup \overline{M}) = L_0 \subset L_1 \subset \ldots \subset L_r$$

existiert, sodass $z \in L_r$ und $\forall_j \colon [L_j : L_{j-1}] \leq 2$.

Den Beweis des Theorems folgt im Anschluss an einige Anwendungen. Wir können nämlich folgern: Falls $z \in \mathrm{Kon}(M \cup \overline{M})$, ist $[L_0(z) : L_0]$ eine Zweierpotenz. Wenn also $[L_0(z) : L_0]$ keine Potenz von 2 ist, kann z nicht konstruktiv sein.

Unmöglichkeitsbeweise

1. Delisches Problem (Würfelverdopplung): Es ist unmöglich die Seitenlänge eines Würfels vom Volumen 2 zu konstruieren. $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \;\Rightarrow\; \sqrt[3]{2}$ ist nicht aus $\{0, 1\}$ konstruierbar.

2. Dreiteilung eines Winkels: Zu gegebenem $z = e^{i\alpha}$ soll $e^{i\frac{\alpha}{3}}$ konstruiert werden. Wir wählen $\alpha = \frac{2\pi}{3} = 120°$. Also ist $z = e^{i\frac{2\pi}{3}} = -\frac{1}{2} + \frac{i}{2}\sqrt{3}$. Zu konstruieren ist $\xi = e^{i\frac{2\pi}{9}}$, das heißt $\xi^3 = z$. Wir bestimmen die Grade in $\mathbb{Q} \subset \mathbb{Q}(z) \subset \mathbb{Q}(z, \xi) = \mathbb{Q}(\xi)$.

z ist Nullstelle von $\frac{x^3-1}{x-1} = x^2 + x + 1$ letzteres ist irreduzibel, folglich gilt

$$2 = [\mathbb{Q}(z) : \mathbb{Q}] \,\Big|\, [\mathbb{Q}(\xi) : \mathbb{Q}] \qquad \text{(Anwendung der Gradformel)}$$

ξ ist Nullstelle von x^9-1. Das Minimalpolynom von ξ teilt x^9-1, sogar $\frac{x^9-1}{x^3-1} = x^6+x^3+1$. Wir erhalten $2 < [\mathbb{Q}(\xi) : \mathbb{Q}] \leq 6$ und möchten die Gleichheit $[\mathbb{Q}(\xi) : \mathbb{Q}] = 6$ zeigen. Dann folgt über $[\mathbb{Q}(\xi) : \mathbb{Q}(z)] = 3$, dass ξ nicht aus z konstruierbar ist.

Wir betrachten einen $\mathbb{Q}$-Automorphismus $\sigma\colon \mathbb{Q}(\xi) \to \mathbb{Q}(\xi)$. Dieser schickt $\xi = e^{i\frac{2\pi}{9}}$ auf eine Nullstelle $e^{i\frac{2\pi\ell}{9}}$ von $x^9 - 1$, sogar von $x^6 + x^3 + 1$, das heißt $3 \nmid \ell$. Ferner ist er bereits durch das Bild $\sigma(\xi) = e^{i\frac{2\pi\ell}{9}}$ bestimmt, das heißt durch die Zahl $\ell \in (\mathbb{Z}/9\mathbb{Z})^*$. Diese Zuordnung definiert einen injektiven Gruppenhomomorphismus

$$\begin{aligned} \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi)) &\to (\mathbb{Z}/9\mathbb{Z})^* \\ \sigma &\mapsto \ell \end{aligned}$$

Also ist $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi))$ bis auf Isomorphie eine Untergruppe von $(\mathbb{Z}/9\mathbb{Z})^*$. Daher teilt $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi))|$ die Zahl 6.

$\mathbb{Q}(\xi)/\mathbb{Q}$ ist separabel (wegen $\mathrm{char}\,\mathbb{Q} = 0$) und normal (Zerfällungskörper von $x^9 - 1$).

$$\begin{aligned} \Rightarrow\; & \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi)) \\ & [\mathbb{Q}(\xi) : \mathbb{Q}] \overset{4.13}{=} |\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi))| \,\Big|\, 6 \end{aligned}$$

Zusammenfassend gilt:

$$\left.\begin{array}{c} 2 \,|\, [\mathbb{Q}(\xi) : \mathbb{Q}] \\ 2 < [\mathbb{Q}(\xi) : \mathbb{Q}] \leq 6 \\ [\mathbb{Q}(\xi) : \mathbb{Q}] \,|\, 6 \end{array}\right\} \;\Rightarrow\; [\mathbb{Q}(\xi) : \mathbb{Q}] = 6$$

Beweis : **Theorem 5.3**

Wir zeigen, dass die Konstruktionen I, II und III in jedem Schritt Elemente im vorgegebenen Körper liefern, oder in einem quadratischen Erweiterungskörper. Da Realteil $\mathrm{Re}(z) = \frac{1}{2}(z+\overline{z})$ und Imaginärteil $\mathrm{Im}(z) = \frac{2}{2i}(z-\overline{z})$ einer komplexen Zahl $\mathbb{C} \ni z = a + bi$ aus z konstruierbar sind, dürfen wir in $\mathbb{R}^2$ statt in $\mathbb{C}$ rechnen.

I. Der Schnitt zweier Geraden gibt ein inhomogenes Gleichungssystem in λ und μ:

$$\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} + \lambda \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} = \begin{pmatrix} p_1' \\ p_2' \end{pmatrix} + \mu \begin{pmatrix} q_1' \\ q_2' \end{pmatrix}$$

Falls existent, liegen die Lösungen im gegebenen Körper (in dem die Koeffizienten liegen). Eine entsprechende Körpererweiterung ist vom Grad 1.

II. Der Schnitt von Gerade und Kreis

$$\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} + \lambda \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \qquad \left| \begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} \right| \stackrel{!}{=} r$$

ergibt eine quadratische Gleichung für λ, die in einer quadratischen Körpererweiterung lösbar ist. (Grad ≤ 2).

III. Der Schnitt zweier Kreise mit Mittelpunkten p und q sowie Radien r_1 und r_2 ergibt sich aus den Gleichungen

$$\left| \begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \right| = r_1 \qquad \left| \begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} \right| = r_2$$
$$(x-p_1)^2 + (y-p_2)^2 = r_1^2 \qquad (x-q_1)^2 + (y-q_2)^2 = r_2^2$$

Die Differenz ist linear in x und y und liefert die Gleichung der Geraden durch die beiden Schnittpunkte. Die Koeffizeinten liegen im vorgegebenen Körper. Die gesuchten Schnittpunkte sind die Schnittpunkte dieser Geraden mit einem Kreis, wie in II. Also ist die entsprechende Körpererweiterung vom Grad ≤ 2.

Eine Kette solcher Konstruktionen ergibt eine Kette von Körpererweiterungen vom Grad ≤ 2. Wegen $L_0 \subset L_0(z) \subset L_r$ teilt $[L_0(z) : L_0]$ mit $[L_r : L_0]$ eine Zweierpotenz.

□

Weitere Konstruktionsaufgaben:

Zur Quadratur des Kreises: Gegeben sei der Einheitskreis. Gesucht ist ein Quadrat mit derselben Fläche. Zu konstruieren ist also $\sqrt{\pi}$ oder π. Aus der Zahlentheorie wissen wir, dass π transzendent, also nicht konstruierbar ist.

Zur Konstruktion von regelmäßigen n-Ecken: Zu konstruieren sind also n-te Einheitswurzeln $\xi = e^{i\frac{2\pi}{n}}$. Das Minimalpolynom von ξ ist ein Teiler von $x^n - 1$ und vom Grad $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ (eulersche φ-Funktion). Wenn ξ konstruierbar ist, bedeutet dies, dass $\varphi(n)$ eine Zweierpotenz ist. Die Zahlentheorie besagt, dass dies äquivalent ist zu $n = 2^\ell \cdot p_1 p_2 \cdots p_r$, wobei $p_j = 2^{2^{a_j}} + 1$ paarweise verschiedene Fermatsche Primzahlen sind. Die Zahlentheoretiker kennen fünf davon:

a_j	0	1	2	3	4
p_j	3	5	17	267	65337

Für $a = 5$ erhält man wegen $641 | 4294967297$ keine Primzahl.

Polynomiale Gleichungen

Sei K ein Körper und $f(x)$ ein Polynom vom Grad n. Gesucht ist eine Formel für dessen Nullstellen. Für $n = 2$ und $\mathrm{char}(K) \neq 2$ sowie für $n = 3$ und $\mathrm{char}(K) \neq 2, 3$ kann man solche Formeln aufschreiben:

$$f(x) = x^2 + ax + b \qquad \rightsquigarrow -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$$

$$\begin{aligned} f(x) &= x^3 + ax^2 + bx + c \\ &= x^3 + px + q \end{aligned} \qquad \rightsquigarrow \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}$$

Es werden also verschiedene (iterierte) Wurzeln benötigt. Unser Ziel ist es zu zeigen, dass es für $n \geq 5$ keine solche allgemeine Formel gibt, die Lösungen aus Koeffizienten mithilfe von $\{+, -, \cdot, /\}$ und beliebigen Wurzeln berechnet. Strategie: Wir vergrößern Körpererweiterungen $K(\sqrt[n]{a})/K$ zu Galoiserweiterungen und zeigen, dass die zugehörige Galoisgruppen spezielle Eigenschaften haben. Anschließend werden wir ein $f(x)$ finden, dessen Zerfällungskörper diese Eigenschaft *nicht* hat. Generell gelte $\mathrm{char}(K) = 0$ (bzw. sogar $K = \mathbb{Q}$). Dann ist Separabilität automatisch erfüllt.

Definition 5.4 **Radikal**

Sei K ein Körper ($\mathbb{Q} \subset K$), $n \in \mathbb{N}$ und $a \in K$. Sei ferner E/K eine Körpererweiterung, sodass ein $b \in E$ existiert mit $b^n = a$. Dann heißt b ein Radikal von a über K und wird mit $b = \sqrt[n]{a}$ bezeichnet. Das Radikal ist bis auf Multiplikation mit Einheitswurzeln eindeutig.

Eine Körpererweiterung L/K heißt durch Radikale auflösbar genau dann, wenn eine Kette von Körpererweiterungen $K_0 = K \subset K_1 \subset \ldots \subset K_\ell$ mit $L \subset K_\ell$, $\ell \in \mathbb{N}$ und $K_{j+1} = K_j(b_j)$ existiert, wobei $b_j = \sqrt[n_j]{a_j}$ für ein $a_j \in K_j \, \forall_j$.

Ein Polynom heißt durch Radikale auflösbar genau dann, wenn sein Zerfällungskörper L über K durch Radikale auflösbar ist, also $K_0 \subset \ldots \subset K_\ell$ existierten, mit $L \subset K_\ell$, wobei K_ℓ durch iterierte Adjunktion von Radikalen aus $K_0 = K$ entsteht.

Wir betrachten die Galoisgruppe $\mathrm{Gal}(L/K)$ und zeigen, dass sie spezielle Eigenschaften hat, wenn $f(x)$ durch Radikale auflösbar ist. Dies erfolgt in zwei Schritten: Wir betrachten zunächst die Galoisgruppe von $K(\sqrt[n]{1}) =: K_n$ und dann die von $K_n(\sqrt[n]{a})$.

Sei K_n also der Zerfällungskörper von $x^n - 1$ über K. Es gilt $\mathbb{Q} \subset K$ und $\mathbb{C} \supset \overline{\mathbb{Q}} \subset \overline{K}$, das heißt, die Einheitswurzeln $\sqrt[n]{1}$ sind komplexe Zahlen $e^{i\frac{2\pi j}{n}}$ für $j = 1, \ldots, n$.

Lemma 5.5

Es gibt einen injektiven Gruppenhomomorphismus $\mathrm{Gal}(K_n/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$.

Das bedeutet insbesondere, dass $\mathrm{Gal}(K_n/K)$ isomorph zu einer Untergruppe der multiplikativen Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$, also abelsch ist.

Beweis :
Betrachte eine Abbildung $\mathrm{Gal}(K_n/K) \ni \sigma\colon K_n = K(e^{i\frac{2\pi}{n}}) \to K_n$. Diese ist bestimmt durch $\sigma(e^{i\frac{2\pi}{n}})$. Ferner bildet σ Nullstellen von $x^n - 1 = \sigma^*(x^n - 1)$ auf Nullstellen von $x^n - 1$ ab. Analoges gilt einem zweitem Homomorphismus τ. Wir erhalten:

$$\sigma\colon e^{i\frac{2\pi}{n}} \mapsto e^{i\frac{2\pi\ell}{n}} \qquad \tau\colon e^{i\frac{2\pi}{n}} \mapsto e^{i\frac{2\pi m}{n}} \qquad \ell, m \in \mathbb{Z}/n\mathbb{Z}$$

Wir betrachten $\tau \circ \sigma\colon e^{i\frac{2\pi}{n}} \mapsto \tau(e^{i\frac{2\pi\ell}{n}}) = \tau(e^{i\frac{2\pi}{n}})^\ell = (e^{i\frac{2\pi m}{n}})^\ell = e^{i\frac{2\pi(m\ell)}{n}}$ und erkennen einen multiplikativen Gruppenhomomorphismus

$$\begin{aligned} \mathrm{Gal}(K_n/K) &\to \mathbb{Z}/n\mathbb{Z} \\ \sigma &\mapsto \ell \\ \mathrm{id} = \sigma \circ \sigma^{-1} &\mapsto 1 \\ \sigma^{-1} &\mapsto \ell' \;\Rightarrow\; \ell \cdot \ell' = 1 \;\Rightarrow\; \ell \in (\mathbb{Z}/n\mathbb{Z})^* \\ \Rightarrow\; \mathrm{Gal}(K_n/K) &\to (\mathbb{Z}/n\mathbb{Z})^* \end{aligned}$$

Dieser Gruppenhomomorphismus ist injektiv, da σ durch $\sigma(e^{i\frac{2\pi}{n}})$ bestimmt ist. □

Es sei an $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n) = |\{j\colon 1 \le j \le n, \mathrm{ggT}(j,n) = 1\}| < n$ erinnert. Ein Beispiel ist $x^9 - 1$ mit $\varphi(9) = 6$. Der nächste Schritt ist $K_n(\sqrt[n]{a})$ zu untersuchen.

Lemma 5.6
Sei $e^{i\frac{2\pi}{n}} \in K$ und $L = K(\sqrt[n]{a})$ für ein $a \in K$. Dann ist L/K eine Galoiserweiterung und $\mathrm{Gal}(L/K)$ ist zyklisch mit $\mathrm{ord}\big(\mathrm{Gal}(L/K)\big) \,|\, n$.

Bemerkung: Es gilt auch die folgende Umkehrung (ohne Beweis):

Sei L/K eine endliche Galoiserweiterung mit $[L : K] = n$ und zyklischem $\mathrm{Gal}(L/K)$. Dann ist L der Zerfällungskörper eines Polynoms $x^n - a$ für ein $a \in K$.

Beweis :
Wir zeigen zunächst, dass L/K eine Galoiserweiterung ist. Separabilität gilt, da $\mathrm{char}(K) = 0$ vorausgesetzt war. Betrachtet man die n Nullstellen von $x^n - a$, erkennt man, dass alle in L liegen:

$$\sqrt[n]{a}\,,\quad \sqrt[n]{a}\underbrace{e^{i\frac{2\pi}{n}}}_{\in K},\quad \sqrt[n]{a}\underbrace{e^{i\frac{2\pi 2}{n}}}_{\in K}, \ldots \in L$$

Folglich ist L ist der Zerfällunskörper von $x^n - a$ über K und L/K ist auch eine normale Körpererweiterung.

$\sigma \in \mathrm{Gal}(L/K)$ schickt wie immer Nullstellen von $x^n - a$ wieder auf solche Nullstellen. Die Zuordnungen sehen genauso aus wie vorher:

$$\sigma\colon \sqrt[n]{a} \mapsto \sqrt[n]{a}\, e^{i\frac{2\pi\ell}{n}} \qquad \tau\colon \sqrt[n]{a} \mapsto \sqrt[n]{a}\, e^{i\frac{2\pi m}{n}} \qquad \ell, m \in \mathbb{Z}/n\mathbb{Z}$$

$$\Rightarrow\ \mathrm{Gal}(L/K) \to \mathbb{Z}/n\mathbb{Z} \qquad \text{injektiv}$$
$$\sigma \mapsto \ell$$
$$\tau \mapsto m$$

Betrachtet man wieder die Verkettung, ergibt sich

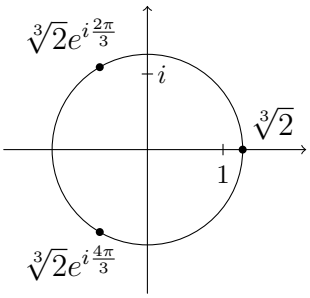
$$\tau \circ \sigma\colon \sqrt[n]{a} \overset{\sigma}{\longmapsto} \sqrt[n]{a} \cdot e^{i\frac{2\pi\ell}{n}} \overset{\tau}{\longmapsto} \tau(\sqrt[n]{a})\, e^{i\frac{2\pi\ell}{n}} = \left(\sqrt[n]{a}\, e^{i\frac{2\pi m}{n}}\right) e^{i\frac{2\pi\ell}{n}} = \sqrt[n]{a}\, e^{i\frac{2\pi(\ell+m)}{n}}$$
$$\Rightarrow\ \tau \circ \sigma \mapsto \ell + m$$

Folglich definiert $\mathrm{Gal}(L/K) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$ einen additiven Gruppenhomomorphismus. $\mathrm{Gal}(L/K)$ ist damit eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z}, +)$ und als solche gemäß Proposition 1.6 (c) zyklisch. Außerdem folgt aus Proposition 1.6 die Behauptung, dass $|\mathrm{Gal}(L/K)|$ ein Teiler von n ist.

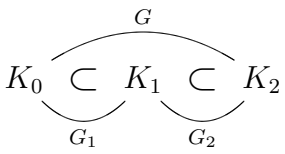
□

Also erhalten wir in beiden Fällen abelsche Gruppen. Was passiert, wenn wir iterieren?

Beispiel: Zerfällungskörper L von $x^3 - 2$



$$\frac{x^3 - 1}{x - 1} = x^2 + x + 1$$



Es ist $G_1 = \mathbb{Z}/2\mathbb{Z}$. Im Gegensatz dazu permutiert $G = \Sigma_3$ die drei Nullstellen von $x^3 - 2$ beliebig und ist damit nicht abelsch. Dieses Beispiel zeigt, dass beim Iterieren die Eigenschaft „abelsch“ verloren geht.

Definition 5.7 Normalreihe

Sei G eine Gruppe und $G_0 = \{1\} \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_n = G$ eine endliche Kette von Untergruppen mit $G_j \trianglelefteq G_{j+1}\ \forall_{j=0,\ldots,n-1}$. Eine solche Kette heißt Normalreihe.

Eine Normalreihe heißt abelsch: $\Leftrightarrow\ \forall_{j=0,\ldots,n-1}\colon G_{j+1}/G_j$ ist abelsch.

G heißt auflösbar, wenn G eine abelsche Normalreihe besitzt.

Unser nächstes Ziel ist es, zu zeigen, dass ein Polynom genau dann durch Radikale auflösbar ist, wenn sein Zerfällungskörper eine auflösbare Galoisgruppe hat. Um die Bedeutung dieser Eigenschaft zu unterstreichen, werden wir außerdem Galoisgruppen angeben, die nicht auflösbar sind.

Beispiel: auflösbare Gruppen

- Abelsche Gruppen sind auflösbar.
- Die symmetrische Gruppe Σ_3 ist auflösbar. Eine Normalreihe erhalten wir über $\Sigma_3 \supset H = \langle(1\,2\,3)\rangle$. Wegen $|H| = 3$, $|\Sigma_3| = 6$ und $[G : H] = 2$ ist H normal. Wegen $|G/H| = 2$ bekommen wir die abelsche Normalreihe $\{(1)\} \triangleleft \langle(1\,2\,3)\rangle \triangleleft \Sigma_3$.
- p-Gruppen sind auflösbar. Sei $|G| = p^n$ mit Primzahl p. Nach Proposition 1.17 (b) ist für $n > 0$ das Zentrum $\{e\} \neq Z(G) \trianglelefteq G$ nichttrivial. Es ist $|G/Z(G)| = p^\ell$ für ein $\ell < n$. Induktiv folgt, dass G auflösbar ist.

Definition 5.8
Sei G eine Gruppe und $a, b \in G$. Dann heißt $[a, b] := aba^{-1}b^{-1}$ der Kommutator von a und b.

Ferner ist die Kommutatoruntergruppe oder derivierte Gruppe von G definiert als die von allen Kommutatoren erzeugte Untergruppe $D(G) := \langle [a, b] \colon a, b \in G\rangle$.

Es gilt $[a, b] = 1 \;\Leftrightarrow\; ab = ba$. Die Menge $\{[a, b] \colon a, b \in G\}$ muss keine Gruppe sein. $D(G)$ ist normal in G, denn

$$g[a, b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \quad \text{ist ein Kommutator.}$$

Offenbar ist G abelsch $\Leftrightarrow$ $D(G) = \{1\}$.

Wir versuchen eine Normalreihe $G > D(G) > D(D(G))$. Betrachten wir Elemente $a, b \in G$ ist $[a, b] \in D(G)$. In der Quotientengruppe $G/D(G)$ ist $\overline{1} = \overline{[a, b]} = \overline{a}\overline{b}\overline{a}^{-1}\overline{b}^{-1}$. Folglich gilt $\overline{a}\overline{b} = \overline{b}\overline{a}$ für $\overline{a}, \overline{b} \in G/D(G)$, weshalb $G/D(G)$ abelsch ist.

Demnach sind $G \trianglerighteq D(G) \trianglerighteq D^2(G) \trianglerighteq D^3(G) \trianglerighteq \ldots$ lauter abelsche Quotienten, wobei $D^2(G) = D(D(G))$ sei. Es liegt eine abelsche Normalreihe vor, falls $\exists_{n\in\mathbb{N}} \colon D^n(G) = \{1\}$.

Wenn G einfach und nicht abelsch ist, hat G keine Normalteiler außer G und $\{1\}$. Für nicht-abelsches G ist $D(G) \neq \{1\}$, aber $D(G) \trianglelefteq G$. Also folgt $G = D(G) = D^2(G) = \ldots$

Es kann also passieren, dass die Reihe bei $D^i(G) = D^{i+1}(G) = \ldots$ stehen bleibt. Wir zeigen im Folgenden, dass G dann nicht auflösbar ist. Diese Reihe eignet sich also tatsächlich als Test: entweder sie liefert die abelsche Normalreihe, oder es gibt keine.

Proposition 5.9
G ist auflösbar $\Leftrightarrow$ $\exists_{n\in\mathbb{N}} \colon D^n(G) = \{1\}$

Beweis :

„⇐“ gilt nach Definition.

„⇒“ Sei G auflösbar und $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ eine abelsche Normalreihe, also G_{i+1}/G_i abelsch für jedes i. Wir zeigen mit Induktion nach i, dass $D^i(G) \subseteq G_{n-i}\, \forall_i$. Insbesondere folgt dann über $D^n(G) \subseteq G_0 = \{1\}$ die Behauptung.

Der Induktionsanfang $n = 0$ ist mit $D^0(G) = G \subseteq G_{n-0} = G$ trivial. Zusätzlich weisen wir für $n = 1$ explizit $D^1(G) = D(G) \subseteq G_{n-1}$ nach:

Da G_n/G_{n-1} abelsch ist, gilt $\overline{a}\overline{b} = \overline{b}\overline{a}$ in G_n/G_{n-1} für Elemente $a, b \in G$. Folglich ist $[a, b] = [\overline{a}, \overline{b}] = \overline{1}$ in G_n/G_{n-1}. Daraus folgt über $[a, b] \in G_{n-1}$ die Behauptung $D(G) = \langle [a, b] \rangle \subset G_{n-1}$.

Induktionsschritt: Es gelte $D^i(G) \subseteq G_{n-i}$ und $D^{i+1}(G) \subseteq G_{n-i-1}$ ist zu zeigen.

$$D^{i+1}(G) = \left\langle [D^i(G), D^i(G)] \right\rangle \subseteq \left\langle \left[G_{n-i}, G_{n-i} \right] \right\rangle \subseteq G_{n-i-1}$$

denn G_{n-i}/G_{n-i-1} ist abelsch. □

Wir haben gezeigt, dass G auflösbar ist, also eine auflösbare Normalreihe hat genau dann, wenn

$$G \supset \underset{\substack{\| \\ \langle ghg^{-1}h^{-1} \rangle}}{D(G)} \supset D^2(G) \supset \ldots \supset D^n(G) = \{e\} \qquad \text{für ein } n \in \mathbb{N}$$

Damit zeigen wir, dass beispielsweise Σ_n für $n \geq 5$ nicht auflösbar ist.

Proposition 5.10
Sei $n \geq 5$. Dann gilt $D(\Sigma_n) = D(A_n) = A_n$ (Menge aller geraden Permutationen). Also sind Σ_n und A_n nicht auflösbar. (A_n ist für $n \geq 5$ sogar einfach.)

Beweis :

Wir betrachten das Vorzeichen

$$\begin{aligned} \operatorname{sgn}\colon \Sigma_n &\to \{\pm 1\} \\ \sigma &\mapsto (-1)^k \qquad k = \#\{\text{Fehlstände in } \sigma\} = |\{i < j \colon \sigma(i) > \sigma(j)\}| \\ A_n &= \ker(\operatorname{sgn}) = \{\text{gerade Permutationen}\} \end{aligned}$$

A_n hat Index 2 in Σ_n, also ist $A_n \triangleleft \Sigma_n$ ein Normalteiler.

Elemente der Gestalt $(a\,b) \circ (c\,d) \in A_n$ erzeugen A_n. Wir sollten solche Elemente als Produkte von Kommutatoren schreiben. Wir zeigen zunächst, dass $(a\,b) \circ (c\,d)$ Produkt von 3-Zyklen $(e\,f\,g)$ ist und anschließend, dass 3-Zyklen Produkte von Kommutatoren (für $n \geq 5$) sind. Dann folgt $A_n \subset D(A_n)$, also $A_n = D(A_n)$.

Um $(a\,b)\circ(c\,d)$ als Produkt von 3-Zyklen zu schreiben, unterscheiden wir die Fälle

$$\begin{aligned}
&\{a,b\}=\{c,d\} && \Rightarrow\ (a\,b)\circ(c\,d)=\mathrm{id}\\
&\{a,b\}\cap\{c,d\}=\{a\}=\{c\} && \Rightarrow\ (a\,b)\circ(c\,d)=(a\,d\,b)\\
&\{a,b\}\cap\{c,d\}=\emptyset && \Rightarrow\ (a\,b)\circ(c\,d)=(a\,c\,b)\circ(a\,c\,d)
\end{aligned}$$

Wegen $n\geq 5$ finden sich paarweise verschiedene a,b,c,d.
Dann ist $(a\,b\,c)=(a\,b\,d)\circ(a\,c\,e)\circ(a\,d\,b)^{-1}\circ(a\,c\,e)^{-1}$ ein Kommutator. Also ist $A_n=D(A_n)$. Aus $A_n\subset\Sigma_n$ folgt $D(A_n)\subset D(\Sigma_n)$.

$$\begin{array}{ccc} \| & & \cap \\ A_n & & \Sigma_n \end{array}$$

Kommutatoren sind von der Form $ghg^{-1}h^{-1}$. Genau dann, wenn g gerade ist, ist auch g^{-1} gerade. Folglich sind Kommutatoren $[g,h]$ immer gerade. Es folgt $D(\Sigma_n)\subset A_n$ und damit $D(\Sigma_n)=A_n$. □

Theorem 5.11
Sei L/K eine endliche Körpererweiterung und $\mathrm{char}(K)=0$. Dann sind äquivalent:

(a) L/K ist durch Radikale auflösbar

(b) Es existiert eine endliche Galoiserweiterung M/K mit $M\supset L$, sodass $\mathrm{Gal}(M/K)$ auflösbar ist.

Wir benötigen (und zeigen weiter unten) lediglich die Implikation (a) ⇒ (b). Der Beweis der umgekehrten Implikation benötigt die Umkehrung von Lemma 5.6.

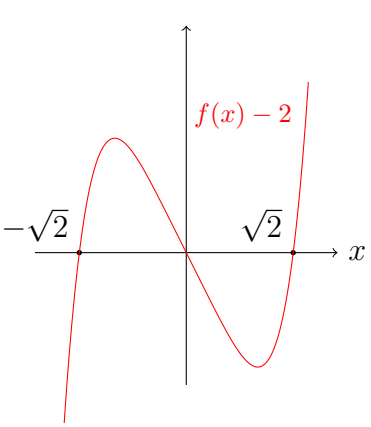
Wie wendet man Theorem 5.11 bei unbekanntem M an? Gegeben seien $f(x)\in K[x]$ und sein Zerfällungskörper $L\subset\overline{K}$. Wegen $\mathrm{char}(K)=0$ ist L/K separabel. Ferner ist L/K normal, da L Zerfällungskörper ist. L/K ist also eine Galoiserweiterung. Gemäß dem Hauptsatz ist $\mathrm{Gal}(L/K)=\mathrm{Gal}(M/K)\big/\mathrm{Gal}(M/L)$. Wenn $\mathrm{Gal}(M/K)$ auflösbar ist, ist auch $\mathrm{Gal}(L/K)$ auflösbar. Allgemein gilt die Implikation

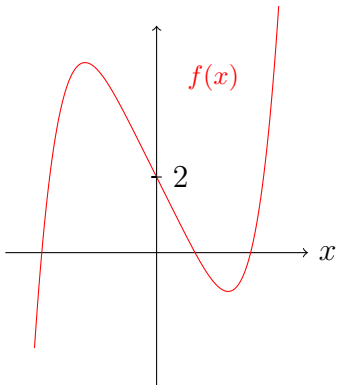
$$G \text{ auflösbar und } G\twoheadrightarrow\overline{G}\ \Rightarrow\ \overline{G} \text{ auflösbar} \qquad \text{(wobei } \overline{G} \text{ die Restklassengruppe sei)}$$

$$[\overline{g},\overline{h}]=\overline{[g,h]}\ \Rightarrow\ D^n(G)=\{e\}\ \Rightarrow\ D^n(\overline{G})=\{\overline{e}\}$$

Wenn also L/K durch Radikale auflösbar ist, muss $\mathrm{Gal}(L/K)$ eine auflösbare Gruppe sein. Das heißt eine Gleichung mit *nicht* auflösbarer Galoisgruppe kann nicht durch Radikale auflösbar sein.

Beispiel: nicht auflösbares Polynom über $\mathbb{Q}$
Das Polynom $f(x)=x^5-4x+2\in\mathbb{Q}[x]$ ist nach Eisenstein ($p=2$) irreduzibel. Ferner besitzt $f(x)-2=x^5-4x=x(x^4-4)=x(x^2-2)(x^2+2)$ drei reelle Nullstellen 0 und $\pm\sqrt{2}$. Folgende Graphen veranschaulichen die Situation, wobei zu beachten ist, dass die Achsen hier im Verhältnis 1 : 2 skaliert sind.





Wir zeigen, dass $f(x)$ auch drei relle (und zwei komplexe) Nullstellen besitzt, indem wir die Position der lokalen Extrema abschätzen.

$$f'(x) = 5x^4 - 4 = 0 \;\Leftrightarrow\; 5x^4 - 4 = 0 \;\Leftrightarrow\; x = \pm\sqrt[4]{\tfrac{4}{5}}$$

Grob geschätzt liegen die Extrema von $f(x) - 2$ bei ± 3, sodass $f(x)$ ebenfalls drei reelle Nullstellen hat.

Proposition 5.12
Sei $f(x) \in \mathbb{Q}[x]$ irreduzibel vom Grad 5, sodass $f(x)$ in $\mathbb{C}$ genau drei reelle Nullstellen hat. Dann ist die Galoisgruppe von f, das heißt die Galoisgruppe des Zerfällungskörpers von f über $\mathbb{Q}$, nicht auflösbar. Also ist f nicht durch Radikale auflösbar.

Beweis :
Wir zeigen, dass $\mathrm{Gal}(f) \cong \Sigma_5$, also nicht auflösbar ist. Hier ist $\mathrm{Gal}(f) = \mathrm{Gal}(L/\mathbb{Q})$, wobei L der Zerfällungskörper von f ist. Wegen Separabilität hat das irreduzibele Polynom f fünf einfache Nullstellen $x_1, x_2, x_3 \in \mathbb{R} \setminus \mathbb{Q}$ und $x_4, x_5 \in \mathbb{C} \setminus \mathbb{R}$.

Es ist $\mathbb{R} \supset \mathbb{Q}(x_1) \subset L$. Das Minimalpolynom $m_{x_1}(x) = f(x)$ hat Grad 5. Folglich ist $[\mathbb{Q}(x_1) : \mathbb{Q}] = 5 \,|\, [L : \mathbb{Q}]$.

Komplexe Konjugation lässt $f(x)$ fest, da es rationale Koeffizienten hat. Ebenso lässt sie die reellen x_1, x_2, x_3 fest, vertauscht aber $x_4 \neq \overline{x_4}$ und $x_5 = \overline{x_4}$. Folglich existiert ein $\tau \in \mathrm{Gal}(L/\mathbb{Q})$, das wie die komplexe Konjugation eingeschränkt auf L wirkt, also x_4 und x_5 vertauscht.

Es ist $\mathrm{Gal}(L/\mathbb{Q}) \subset \Sigma_5$ (Automorphismen permutieren die 5 Wurzeln). Ferner ist $\tau = (4, 5) \in \mathrm{Gal}(L/\mathbb{Q}) \supset \mathrm{Gal}(\mathbb{Q}(x_1)/\mathbb{Q})$ von der Ordnung 5 und in Σ_5 eine Transposition. Folgendes allgemeineres Lemma zeigt, dass dann $\mathrm{Gal}(L/\mathbb{Q}) = \Sigma_5$ gilt.

Also sind die Nullstellen von $f(x)$ nicht durch (iterierte) Radikale beschreibbar. □

Lemma

Sei p eine Primzahl. Sei ferner $G < \Sigma_p$, sodass $p \,|\, \mathrm{ord}(G)$ und eine Transposition $\Sigma_p \ni \tau$ in G enthalten ist.

Dann ist $G = \Sigma_p$.

Beweis :

Gemäß des Satzes von Cauchy 1.15 folgt aus $p \,|\, \mathrm{ord}(G)$ die Existenz eines $g \in G$ mit $\mathrm{ord}(g) = p$. Zunächst soll gezeigt werden, dass dieses g ein p-Zyklus ist.

$g \in \Sigma_p$ operiert auf $\{1, \ldots, p\} =: X$. Angenommen, $X = X_1 \dot\cup X_2$ zerfällt in zwei nichtleere Bahnen X_1 und X_2 von g. Dann ist $g|_{X_1} \in \Sigma_{|X_1|}$ und $g|_{X_2} \in \Sigma_{|X_2|}$. Es sei an $|\Sigma_{|x_1|}| = |X_1|!$ erinnert. Aus $X_1 \subsetneq X$ folgt $|X_1| < p$ und damit $p \nmid |X_1|!$ beziehungsweise analog $p \nmid |X_2|!$. Da andererseits $|\Sigma_{|X_1|}|$ von $\mathrm{ord}(g|_{X_1})$ geteilt wird, folgt $p \nmid \mathrm{ord}(g|_{X_1})$ sowie analog $p \nmid \mathrm{ord}(g|_{X_2})$. Wegen $\mathrm{ord}(g) = \mathrm{kgV}\{\mathrm{ord}(g_1), \mathrm{ord}(g_2)\}$ erwächst aus der Folgerung $p \nmid \mathrm{ord}(g)$ ein Widerspruch. Es gilt also $X_1 = X$ oder $X_2 = X$, das heißt g hat nur eine Bahn auf X nämlich X selbst.

Folglich ist $X = \{1, g(1), g^2(1), \ldots, g^{p-1}(1)\}$, weshalb g ein p-Zyklus ist, der oBdA als $g = (1\,2\,3 \ldots p)$ geschrieben werden kann.

Die Untergruppe G enthält also einen p-Zyklus $g = (1\,2 \ldots p) = (2\,3 \ldots p\,1)$ und nach Voraussetzung eine Transposition τ, die oBdA von der Form $\tau = (1\,a)$ für ein $a \in \{2, \ldots, p\}$ ist.

Da p eine Primzahl ist, können wir g durch $g^{a-1} = (1\,a \ldots)$ ersetzen. Wegen $g^{a-1}(1) = a$ genügt es schließlich oBdA den Fall $g = (1\,2 \ldots p)$ und $\tau = (1\,2)$ zu betrachten.
Wegen $\tau, g \in G$ sind auch Verkettungen $g \circ \tau \circ g^{-1} \in G$.

$$\begin{aligned} g &: 1 \mapsto 2 \\ g^2 &: 1 \mapsto 3 \\ g^3 &: 1 \mapsto 4 \\ &\vdots \\ g^{a-1} &: 1 \mapsto a \end{aligned}$$

Iterativ folgt:
$$\begin{aligned} (2\,3) &= g \circ (1\,2) \circ g^{-1} \in G \\ (3\,4) &= g \circ (2\,3) \circ g^{-1} \in G \\ &\ldots \Rightarrow (i, i+1) \in G \,\forall_i \end{aligned}$$

Desweiteren ist:
$$\begin{aligned} (1\,3) &= (1\,2) \circ (2\,3) \circ (1\,2) \in G \\ (1\,4) &= (1\,3) \circ (3\,4) \circ (1\,3) \in G \\ (i\;j) &= (1\;i) \circ (1\;j) \circ (1\;i) \in G \\ \Rightarrow (x_1\,x_2 \ldots x_m) &= (x_1\,x_m) \circ (x_1\,x_{m-1}) \circ \ldots \circ (x_1\,x_2) \in G \end{aligned}$$

Folglich ist $G = \Sigma_p$. □

Beweis : **Theorem 5.11** (a) $\Rightarrow$ (b)

Wir zeigen zuerst, dass es eine Erweiterung $M' \supset L \supset K$ gibt, sodass M'/K galoissch ist und gleichzeitig M' durch Radikale auflösbar ist. Nach Voraussetzung existiert gemäß Definition 5.4 (Auflösbarkeit durch Radikale) ein $M \supset L \supset K$, wobei dieses M durch iterierte Adjunktion von Radikalen entsteht. Das Problem ist, dass M vielleicht nicht normal ist, also gegebenfalls vergrößert werden muss und dabei auflösbar bleiben soll.

Wir wenden Induktion nach $[M : K]$ an. Der Induktionsanfang $[M : K] = 1$ impliziert $M = K$ und ist damit klar (Zerfällungskörper eines linearen Polynoms).

Im Fall $[M : K] > 1$, gilt:

$$M = K(\underbrace{a_1, \ldots, a_\ell}_{\text{Radikale}}) \supset K \qquad M \supsetneq K(a_1, \ldots, a_{\ell-1}) = M_0 \qquad M = M_0(a_\ell)$$

Nach Induktionsannahme existiert zu M_0/K ein normales und durch Radikale auflösbares $M_0' \supset M_0$. Wir möchten ein normales und durch Radikale auflösbares $M' \supset M$ konstruieren.

$$\begin{array}{ccccc} M' & \supset & M_0' & & \\ \cup & & \cup & & \\ M & \supset & M_0 & \supset & K \end{array}$$

Sei m der Exponent, sodass $a_\ell^m \in M_0$. Wir schreiben im Folgenden kurz $a := a_\ell$ und definieren

$$f(x) = \prod_{\varphi \in \mathrm{Gal}(M_0'/K)} (x^m - \varphi(a^m))$$

Alle Nullstellen von f sind Radikale. Folglich ist der Zerfällungskörper von f eine Radikalerweiterung. Es ist $f \in K[x]$, da

$$\varphi^* f(x) = f(x), \qquad \text{denn } \varphi^* \text{ permutiert die Faktoren:}$$
$$\varphi^*(x^m - \psi(a^m)) = \left(x^m - (\varphi^*\psi)(a^m)\right) \qquad \text{beachte: } \varphi^*\psi \in \mathrm{Gal}(M_0'/L)$$

Nach Induktionsannahme ist M_0' Zerfällungskörper eines Polynoms $g(x) \in K[x]$, sodass alle Nullstellen Radikale sind. Wir definieren M' als den Zerfällungskörper von $f \cdot g \in K[x]$. Alle Nullstellen sind Radikale. Es gilt $M' \supset M \supset L$ wie gefordert.

Es verbleibt damit die Behauptung des Theorems zu zeigen, nämlich dass die Galoisgruppe $\mathrm{Gal}(M'/K)$ auflösbar ist. Wir haben eine Körperkette

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = M' \qquad K_{j+1} = K_j(u_{j+1}) \qquad u_{j+1}^{m_{j+1}} \in K_j$$

Wir definieren $m := \mathrm{kgV}(m_1, \ldots, m_r)$ und ξ als primitive m-te Einheitswurzel, beispielsweise $e^{i\frac{2\pi}{m}}$. Nach Lemma 5.5 ist $K_0 \subset K_0(\xi)$ galoissch mit abelscher Galoisgruppe. Wir betrachten

$$M'' := M'(\xi) \qquad K = K_0 \subset K_0(\xi) \subset K_1(\xi) \subset \ldots \subset K_r(\xi) = M''$$

Die m_i-te Einheitswurzel ist überall enthalten, also ist Lemma 5.6 anwendbar.

$K_j(\xi)$ ist separabel und normal nach Konstruktion. Gemäß dem Hauptsatz der Galoistheorie haben wir normale Untergruppen von $\mathrm{Gal}(M'/K)$ und Quotienten $\mathrm{Gal}(K_{j+1}(\xi)/K_j(\xi))$. Diese sind nach den Lemmata 5.5 und 5.6 abelsch. (Das, was zu zeigen war, bekommt man am Schluss sozusagen geschenkt.) $\square$

Theorem 5.13 Fundamentalsatz der Algebra
Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.

Beweis :
Wir definieren $\mathbb{C} = \mathbb{R}[i]$ und verwenden die Definition von $\mathbb{R}$ (über Cauchy-Folgen) aus der Analysis. Außerdem benötigen wir folgende Folgerungen aus dem Zwischenwertsatz:

(1) $f(x) \in \mathbb{R}[x]$ mit ungeradem Grad hat eine Nullstelle in $\mathbb{R}$ (Vollständigkeit von $\mathbb{R}$).

(2) Jede Positive reelle Zahl hat eine Quadratwurzel: Das Bild von $f(x) = x^2$ ist $\mathbb{R}_{\geq 0}$.

Zu zeigen ist die Implikation $L/\mathbb{C}$ algebraisch $\Rightarrow$ $L = \mathbb{C}$ oder äquivalent dazu $L/\mathbb{C}$ endlich $\Rightarrow$ $L = \mathbb{C}$. Wir können annehmen, dass L normal ist, ansonsten vergrößern wir es entsprechend. Wir schreiben:

$$[L : \mathbb{C}] = 2^\ell m \qquad \text{mit ungeradem } m$$
$$[L : \mathbb{R}] = 2^k m \qquad \text{mit ungeradem } m \text{ und } k \geq 1$$
$$G := \mathrm{Gal}(L/\mathbb{R}) \qquad \text{mit } |G| = 2^k m$$

Nach den Sylowsätzen existiert eine Untergruppe $H < G$ mit $|H| = 2^k$. Die Galoiskorrespondenz schickt H auf den Fixkörper L^H mit $\mathbb{R} \subset L^H \subset L$.

$$[L : L^H] = |H| = 2^k \qquad [L^H : \mathbb{R}] = m$$

Wegen $\mathrm{char}(L^H) = 0$ ist L^H separabel. Gemäß Satz 4.8 vom primitiven Element existiert dann ein a, sodass $L^H = \mathbb{R}(a)$. Sei $f(x) := m_{a,\mathbb{R}}(x)$ das Minimalpolynom von a. Es ist von ungeradem Grad $m = [L^H : \mathbb{R}] = \deg(f)$ und irreduzibel. Nach (1) hat f dann eine Nullstelle in $\mathbb{R}$ und ist folglich linear. Also ist $m = 1$ und $L^H = \mathbb{R}$.

Es verbleibt $k = 1$ in $\mathbb{R} \overset{m=1}{\subset} L^H \overset{2^k}{\subset} L$ zu zeigen. Wir beweisen mithilfe von (2), dass in $\mathbb{C}$ Quadratwurzeln $a+bi$ mit $a, b \in \mathbb{R}$ existieren, also eine beliebige komplexe Zahl $z = x + iy$ mit $x, y \in \mathbb{R}$ geschrieben werden kann als $z = (a+bi)^2 = a^2 - b^2 + 2abi$. Die Forderungen $x \overset{!}{=} a^2 - b^2$ und $y \overset{!}{=} 2ab$ ergeben Gleichungen für die reellen Zahlen a und b. Diese sind demnach Lösungen von

$$a^2 = \frac{1}{2}x \pm \frac{1}{2}\sqrt{x^2 + y^2} \qquad b^2 = -\frac{1}{2} \pm \frac{1}{2}\sqrt{x^2 + y^2}$$

Nach (2) existieren die Wurzeln. Dann ist $x = a^2 - b^2$ und $y^2 = 4a^2b^2$ Folglich existieren in $\mathbb{C}$ Quadratwurzeln. Es gibt also keine Grad 2-Erweiterungen von $\mathbb{C}$. Aus $[M : \mathbb{C}] \leq 2$ folgt $M = \mathbb{C}$, denn falls $[M : \mathbb{C}] = 2$, ist das Minimalpolynom $m_{a,\mathbb{C}}(x)$ von $a \in M \setminus \mathbb{C}$ vom Grad 2, hat aber nach obiger Überlegung Nullstellen in $\mathbb{C}$ – ein Widerspruch zu seiner Irreduzibilität. Wir erinnern an

$$[L : \mathbb{R}] = 2^k \qquad L \supset \mathbb{C} \supset \mathbb{R} \qquad [L : \mathbb{C}] = 2^{k-1}$$

Nach dem Satz von Sylow 1.18 existiert für jeden Teiler von 2^{k-1} eine Untergruppe dieser Ordung (Primzahlpotenz). Für $2^{k-2} \mid 2^{k-1}$ findet sich also ein $H' < \mathrm{Gal}(L/\mathbb{C})$ mit $|H'| = 2^{k-2}$. Wir betrachten folgende Körperkette mit eingezeichneten Graden:

$$\mathbb{R} \overset{2}{\subset} \mathbb{C} \overset{d}{\subset} L^{H'} \overset{2^{k-2}}{\subset} L$$

Da insgesamt der Grad $[L : \mathbb{R}] = 2^k$ vorliegt, muss in der Mitte Grad $d = 2$ herrschen. Es folgt also $[L^{H'} : \mathbb{C}] = 2$. Ein solches $L^{H'}$ kann es aber nicht geben, da $\mathbb{C}$ keine Erweiterungen vom Grad 2 hat.

Folglich ist $\mathbb{C}/\mathbb{C}$ die einzige endliche Körpererweiterung von $\mathbb{C}$. Daraus folgt die Behauptung $\mathbb{C} = \overline{\mathbb{C}}$.

□

Damit haben wir den Fundamentalsatz der Algebra mit einem Minimum an Analysis und einem Maximum an Algebra bewiesen.

Stichwortverzeichnis