Algebra

Markus Junker

Wintersemester 2014/15

Inhaltsverzeichnis

1 Gruppen

1.1 Grundlagen

Definition 1.1.1 *$(G, \cdot, {}^{-1}, e)$ ist eine **Gruppe**, falls*

- *G eine nicht–leere Menge,*
- *$\cdot$ eine assoziative zweistellige Verknüpfung auf G,*
- *e ein neutrales Element für $\cdot$*
- *und g^{-1} ein inverses Element zu g bezüglich $\cdot$ ist, für jedes $g \in G$.*

*G heißt **kommutativ** oder **abelsch**, falls $g \cdot h = h \cdot g$ für alle $g, h \in G$ gilt.*

*Die Anzahl der Elemente von G heißt die **Ordnung von** G (eine natürliche Zahl oder ∞).*

Erläuterungen:
„Neutrales Element“ bedeutet $g \cdot e = e \cdot g = g$ für alle $g \in G$.
„Inverses Element“ bedeutet $g \cdot g^{-1} = g^{-1} \cdot g = e$ für alle $g \in G$.

Bemerkung:

Eine nicht-leere Menge G mit einer assoziativen zweistelligen Verknüpfung $\cdot$ heißt **Halbgruppe**); gibt es zusätzlich ein neutrales Element, so heißt die Struktur $(G, \cdot, e)$ **Monoïd**).

Schreibweisen:

- Kommutative Gruppen werden oft additiv als $(G, +, -, 0)$ geschrieben. Dann schreibt man auch $g - h$ für $g + (-h)$.
- In der allgemeinen Schreibweise lässt man den Punkt $\cdot$ oft weg; statt e steht oft 1. Wegen der Uneindeutigkeit ist eine Bruchschreibweise $\frac{g}{h}$ für gh^{-1} oder $h^{-1}g$ nicht üblich.
- Natürlich können in konkreten Situationen die Operationen und das neutrale Element anders bezeichnet sein.

Lemma 1.1.2 *Das neutrale Element und die inversen Elemente sind in einer Gruppe durch die Gruppenoperation $\cdot$ eindeutig bestimmt. Es gibt also höchstens eine Art, aus einer Halbgruppe eine Gruppe zu machen.*

Gruppen werden daher oft nur als $(G, \cdot)$ angegeben, bzw. nur als G, falls die Verknüpfung aus dem Kontext ersichtlich ist.

Beweis: Sind e_1, e_2 zwei neutrale Elemente, so $e_1 = e_1 e_2 = e_2$.
Gilt $gh = gh' = e$, so $h = g^{-1}gh = g^{-1}gh' = h'$. □

Es gelten in Gruppen also die **Kürzungsregeln**, d. h. aus $gh = gh'$ wie auch aus $hg = h'g$ folgt $h = h'$. Anders ausgedrückt: Die Linkgs- und Rechtsmultiplikationen mit festen Elementen, also die Abbildungen $G \to G$, $x \mapsto gx$ und $x \mapsto xg$ sind injektiv (und da die entsprechende Multiplikation mit g^{-1} eine Umkehrabbildung ist, auch bijektiv).

Man kann den Beweis noch genauer analysieren, wenn man „rechtsneutrale“ und ein „linksneutrale“ Elemente betrachtet. Dabei heißt e_r „rechtsneutral“ und e_l „linksneutral“, falls $g \cdot e_r = g$ bzw. $e_l \cdot g = g$ für alle $g \in G$ ist. Man sieht dann: (1) Wenn es in einer Halbgruppe ein rechtsneutrales und ein linksneutrales Element gibt, dann stimmen beide überein, sind also ein neutrales Element und die Halbgruppe ist ein Monoid. (2) In einer Guppe gibt es genau ein linksneutrales und genau ein rechtsneutrales Element, nämlich das neutrale Element.

Es gilt aber nicht, dass ein linksneutrales Element in einer Halbgruppe bereits ein neutrales Element wäre, denn es kann sein, dass es ein linksneutrales, aber kein rechtsneutrales element gibt.

Analoge Überlegungen gelten für inverse Elemente. Insbesondere folgt in einer Gruppe aus $gh = e$ bereits, dass $h = g^{-1}$ und $g = h^{-1}$.

Folgerung 1.1.3 *In einer Gruppe gilt* $(gh)^{-1} = h^{-1}g^{-1}$ *und* $(g^{-1})^{-1} = g$ *und* $e^{-1} = e$

BEWEIS: Es gilt $(gh)h^{-1}g^{-1} = h^{-1}g^{-1}(gh) = e$ und $gg^{-1} = g^{-1}g = e$ und $e \cdot e = e$, und die Behauptungen folgen aus der Eindeutigkeit des inversen Elements. □

Damit gibt es in einer Gruppe „Rechenregeln" für alle Fälle, in denen zwei Operationen aufeinandertreffen:

$$g(hj) = (gh)j \qquad ge = eg = g \qquad (gh)^{-1} = h^{-1}g^{-1} \qquad e^{-1} = e \qquad (g^{-1})^{-1} = g$$

Beispiel 1.1.4 [**Beispiele für Gruppen**]

- Die **triviale Gruppe** $\{e\}$.
- Die **zyklischen Gruppen** $\mathbb{Z} = (\mathbb{Z}, +)$ und $\mathbb{Z}_n := (\{0, \ldots, n-1\}, +_n)$ für $n > 0$. Dabei ist die Addition $a +_n b$ definiert als „der Rest von $a+b$ bei der Division durch n", d. .h. die eindeutige Zahl $r \in \mathbb{Z}_n$ mit $m \mid a + b - r$.
- Die additive Gruppe $(K, +)$ eines Körpers K (z. B. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$); die multiplikative Gruppe des Körpers $K^\times := (K \setminus \{0\}, \cdot)$; die multiplikative Gruppe der echt positiven Elemente $K^{>0}$ eines angeordneten Körpers K (z. B. $K = \mathbb{Q}, \mathbb{R}$).
- Die Matrixgruppe $\mathrm{GL}(n, K)$ mit der Matrizenmultiplikation.
- Allgemein: Automorphismengruppen von Strukturen, darunter die **symmetrische Gruppe** S_n (Automorphismen der n-elementigen Menge), die **Diëdergruppe** D_n (Symmetriegruppe des regelmäßigen n-Ecks)

S_n für $n \geqslant 3$ und $\mathrm{GL}(n, K)$ für $n \geqslant 2$ sind Beispiele nicht-kommutativer Gruppen.

Endliche Gruppen kann man durch die **Gruppentafel**, also die Verknüpfungstafel der Gruppenmultiplikation, angeben, wobei man sich über die Reihenfolge der Operation im Klaren sein muss.

Lemma 1.1.5 *Ist* $(M, \cdot, e)$ *ein Monoid, so bildet die Menge der* ***invertierbaren Elemente***

$$M^* := \{m \in M \mid \text{es gibt } m^{-1} \in M \text{ mit } m^{-1}m = mm^{-1} = e\}$$

eine Gruppe.

BEWEIS: Die Beweise von Lemma 1.1.2 und Folgerung 1.1.3 funktionieren auch für die invertierbaren Elemente eines Monoids; also ist wegen $m_1^{-1}m_2^{-1} = (m_2m_1)^{-1}$ die Menge der invertierbaren Elemente unter Produkten und wegen $(m^{-1})^{-1} = m$ unter Inversen abgeschlossen. Zudem gilt offensichtlich $e \in M^*$. □

Definition 1.1.6 *Seien* G, H *Gruppen. Eine Abbildung* $\varphi : G \to H$ *heißt Gruppenhomomorphismus, falls* $\varphi(e_G) = e_H$, $\varphi(g \cdot_G h) = \varphi(g) \cdot_H \varphi(h)$ *und* $\varphi(g^{-1_G}) = (\varphi(g))^{-1_H}$ *für alle* $g, h \in G$ *gilt.*
(Zur besseren Unterscheidung sind hier die Verknüpfungen mit der Struktur indiziert, in der man sich gerade befindet.)

Allgemeiner: Sind G, H algebraische Strukturen gleichen Typs, also z. B. zwei Gruppen, zwei Ringe, zwei Vektorräume, dann heißt eine Abbildung $\varphi : G \to H$ **Homomorphismus** für diesen Typ, falls φ mit allen Konstanten und Verknüpfungen, welche für die Definition der Struktur wesentlich sind, vertauscht.

Definition 1.1.7 *Ein injektiver Homomorphismus heißt **Monomorphismus**, ein surjektiver **Epimorphismus**. Ein bijektiver Homomorphismus, dessen Umkehrabbildung ebenfalls ein Homomorphismus ist, heißt **Isomorphismus**. Ein Homomorphismus von einer Struktur in sich selbst wird **Endomorphismus** genannt. Ein **Automorphismus** ist ein Isomorphismus einer Struktur auf sich selbst.*

Lemma 1.1.8 *Ein Halbgruppenhomomorphismus zwischen Gruppen ist bereits ein Gruppenhomomorphismus. Ein bijektiver Gruppenhomomorphismus ist bereits ein Gruppenisomorphismus.*

Achtung: Für Monoide ist der erste Teil falsch: Ein Halbgruppenhomomorphismus zwischen Monoiden muss kein Monoidhomomorphismus sein!

Beweis: Sei $\varphi : G \to H$ Halbgruppenhomomorphismus. Wegen $e \cdot e = e$ in G folgt $\varphi(e)\varphi(e) = \varphi(e)$, also $\varphi(e) = e$ nach Multiplikation beider Seiten mit $\varphi(e)^{-1}$. Wegen $e = \varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$ folgt auch $\varphi(g^{-1}) = \varphi(g)^{-1}$. Also ist φ Gruppenhomomorphismus. Sei nun φ bijektiv, und sei $h_i = \varphi(g_i) \in H$. Dann $\varphi^{-1}(h_1h_2) = \varphi^{-1}(\varphi(g_1)\varphi(g_2)) = \varphi^{-1}(\varphi(g_1g_2)) = g_1g_2 = \varphi^{-1}(h_1)\varphi^{-1}(h_2)$, d.h. φ^{-1} ist ebenso Halbgruppen– und somit Gruppenhomomorphismus. □

Beispiel 1.1.9 [**Beispiele für Homomorphismen**]

- „Rechnen modulo n“: $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \cong Z_n$
- Determinante $\det : \mathrm{GL}(n, K) \to K^\times$
- Signum $\mathrm{sgn} : S_n \to (\{+1, -1\}, \cdot) \cong Z_2$
- Auswertungshomomorphismen $\mathrm{eval}_a : K[X] \to K$, $P(X) \mapsto P(a)$

Definition 1.1.10 *Eine Unterstruktur einer Struktur ist eine (nicht leere) Teilmenge, die alle Konstanten enthält und unter den Verknüpfungen der Struktur abgeschlossen ist.*

*Im Spezialfall der Gruppen: Eine **Untergruppe** einer Gruppe G ist also eine Teilmenge U, für die gilt: $e \in U$, und falls $u, u' \in U$, so sind auch $uu' \in U$ und $u^{-1} \in U$. Notation: $U \leqslant G$.*

Beispiel 1.1.11

- Untergruppen der S_3 sind $\{e\}$, drei zwei-elementige Untergruppen, die aus $\{e\}$ und jeweils einer Transposition bestehen, die dreielementige Untergruppe A_3, die aus $\{e\}$ und den beiden 3-Zykeln besteht, sowie die ganze S_3.
- $\mathbb{Z}$ ist Untergruppe von $\mathbb{Q}$.
- Z_4 ist isomorph zu der Untergruppe $\{1, -1, i, -i\}$ von $\mathbb{C}^\times$.

Bemerkung 1.1.12
Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, dann ist $\mathrm{Bild}(\varphi)$ eine Untergruppe von H.
Umgekehrt: ist $U \leqslant G$, so ist die Inklusionsabbildung $U \to G$ ein Gruppenhomomorphismus.
Untergruppen sind also genau die Bilder von Gruppenhomomorphismen.

Notation: Man setzt die Verknüpfungen auf Teilmengen von G fort durch elementweise Definition, also $X^{-1} := \{x^{-1} \mid x \in X\}$ und $X \cdot Y := \{xy \mid x \in X, y \in Y\}$, und gemischt zwischen

Elementen und Teilmengen: $g \cdot Y := \{g\} \cdot Y = \{gy \mid y \in Y\}$ und $Y \cdot g := Y \cdot \{g\} = \{yg \mid y \in Y\}$. Ferner definiert man $x^g := g^{-1} \cdot x \cdot g$ und $X^g := \{g^{-1} \cdot x \cdot g \mid x \in X\}$. Die Multiplikationspunkte werden zumeist weggelassen.

Die Multiplikation $\cdot$ ist auch auf Teilmengen assoziativ; insbesondere folgt $g^{-1}(gY) = Y$.

Bemerkung: Die Abbildung $x \mapsto x^g$ heißt **Konjugation mit** g und ist ein Automorphismus von G. Elemente x^g bzw. Teilmengen X^g heißen **Konjugierte** von x bzw. X.

Definition 1.1.13 *Eine Untergruppe $U \leqslant G$ induziert zwei Äquivalenzrelationen auf G:*

$g_1 \sim_l g_2 :\iff g_2^{-1} g_1 \in U$ *und* $g_1 \sim_r g_2 :\iff g_1 g_2^{-1} \in U$. *Die Äquivalenzklassen sind die* ***Linksnebenklassen*** $\{gU \mid g \in G\}$ *bzw. die* ***Rechtsnebenklassen*** $\{Ug \mid g \in G\}$.

Links– und Rechtsnebenklassen gehen durch $x \mapsto x^{-1}$ ineinander über. Also ist die Anzahl der Rechtsnebenklassen gleich der Anzahl der Linksnebenklassen. Sie heißt der ***Index von*** U ***in*** G, *in Zeichen* $(G : U)$.

Außerdem stehen je zwei Nebenklassen in Bijektion zueinander, z.B. ist $gU \to hU$, $x \mapsto hg^{-1}x$ eine Bijektion mit Umkehrabbildung $x \mapsto gh^{-1}x$. Daraus folgt der

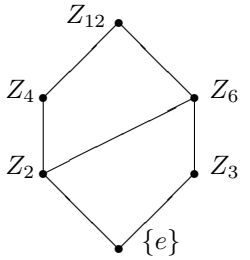
Satz 1.1.14 (Satz von Lagrange) *Ist $U \leqslant G$, so gilt $|G| = |U| \cdot (G : U)$.*

Bemerkung 1.1.15

- Ist $U \leqslant V \leqslant G$, so $U \leqslant G$.
- Ein beliebiger Schnitt von Untergruppen ist wieder eine Untergruppe. Also existiert zu $X \subseteq G$ die **von X erzeugte Untergruppe** $\langle X \rangle$.
- $\langle X \rangle$ besteht aus allen Produkten von Elementen aus X und deren Inversen:

$$\langle X \rangle = \left\{ x_1^{\pm 1} \cdot \ldots \cdot x_k^{\pm 1} \;\middle|\; k \in \mathbb{N}, x_i \in X \right\}$$

- Der Schnitt zweier Untergruppen U, V ist die größte in beiden enthaltene Untergruppen; das Erzeugnis von $U \cup V$ ist die kleinste U und V enthaltende Untergruppe. Also bilden die Untergruppen einer Gruppe einen Verband, den man als sogenanntes Hasse–Diagramm darstellen kann (Beispiel rechts).



Definition und Lemma 1.1.16 *Eine Untergruppe N von G heißt* ***normale Untergruppe*** *oder* ***Normalteiler*** *von G, falls $gN = Ng$ für alle $g \in G$ gilt (äquivalent: $N^g = N$ für alle $g \in G$). Notation: $N \trianglelefteq G$.*

Die Menge der Nebenklassen von N in G wird mit G/N bezeichnet und wird durch $gN \cdot hN := ghN$ so zu einer Gruppe, dass $G \to G/N$, $g \mapsto gN$ ein Gruppenepimorphismus wird. Dieser Homomorphismus heißt der ***natürliche*** *oder* ***kanonische Homomorphismus*** $G \to G/N$.

G/N heißt ***Faktor–*** *oder* ***Quotientengruppe*** *von G.*

Beweis: Wohldefiniertheit: Seien $g_1 N = g_2 N$, $h_1 N = h_2 N$. Dann $g_1 = g_2 n$ mit $n \in N$ und $g_1 h_1 N = g_2 n h_2 N = g_2 n N h_2 = g_2 N h_2 = g_2 h_2 N$.

Neutrales Element ist N, da $gNN = gN$, $NgN = NNg = Ng = gN$.

Inverses Element zu gN ist $g^{-1}N$, denn z.B. $gNg^{-1}N = Ngg^{-1}N = NeN = N$. □

Satz 1.1.17 (Homomorphiesatz) *Wenn $\varphi : G \to H$ ein Gruppenhomomorphismus ist, so ist der **Kern** von φ,* $\mathrm{Kern}(\varphi) := \varphi^{-1}(e) = \{g \in G \mid \varphi(g) = e\}$*, ein Normalteiler von G, und φ zerlegt sich in eine Folge von Homomorphismen*

$$\begin{array}{ccccccc} G & \xrightarrow{\text{surj.}} & G/\varphi^{-1}(e) & \xrightarrow{\cong} & \mathrm{Bild}(\varphi) & \xrightarrow{\text{inj.}} & H \\ g & \mapsto & g\mathrm{Kern}(\varphi) & \mapsto & \varphi(g) & \mapsto & \varphi(g) \end{array}$$

BEWEIS: Seien $n_1, n_2 \in \mathrm{Kern}(\varphi) =: N$. Dann: $\varphi(e) = e$, $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2) = ee = e$, $\varphi(n^{-1}) = \varphi(n)^{-1} = e^{-1} = e$ und $\varphi(g^{-1}ng) = \varphi(g)^{-1}\varphi(n)\varphi(g) = \varphi(g)^{-1}e\varphi(g) = e$. Also ist N Normalteiler.

Sei $G/N \to \mathrm{Bild}(\varphi)$, $gN \mapsto \varphi(g)$. Wegen $gN = hN \iff g^{-1}hN = N \iff g^{-1}h \in N \iff e = \varphi(g^{-1}h) = \varphi(g)^{-1}\varphi(h) \iff \varphi(g) = \varphi(h)$ ist diese Abbildung wohldefiniert und injektiv. Surjektiv ist sie per Definition des Bildes! □

Bemerkung: Normalteiler sind also genau die Kerne von Gruppenhomomorphismen. Jeder Normalteiler ist eine Untergruppe, aber nicht umgekehrt. Bei Vektorräumen sind dagegen sowohl die Bilder als auch die Kerne von Homomorphismen gerade die Unterräume. Bei anderen Arten von Strukturen muss es zwischen Bildern und Kernen gar keinen Zusammenhang geben.

Allgemeiner lässt sich auf den Äquivalenzklassen einer Struktur genau dann eine Struktur gleichen Typs so definieren, dass die natürliche Surjektion zu einem Homomorphismus wird, wenn es sich um eine **Kongruenzrelation** handelt, also eine mit den Verknüpfungen verträgliche Äquivalenzrelation. Bei Gruppen (und einigen anderen Strukturen) ist solch eine Kongruenzrelation bereits durch die Äquivalenzklasse des neutralen Elementes, also den Kern, bestimmt.

Beispiel 1.1.18 • $n\mathbb{Z}$ ist der Kern von „modulo n“, also $\mathbb{Z}/n\mathbb{Z} \cong Z_n$.
• $\mathrm{SL}(n, K)$ ist der Kern der Determinante, also $\mathrm{GL}(n, K)/\mathrm{SL}(n, K) \cong K^\times$.
• A_n ist der Kern des Signums, also $S_n/A_n \cong Z_2$.
• $G/G \cong \{e\}$ und $G/\{e\} \cong G$.

Bemerkung 1.1.19 **(a)** In kommutativen Gruppen sind alle Untergruppen Normalteiler

(b) Normalteiler von Normalteilern sind nicht unbedingt Normalteiler der großen Gruppe.

Die Umkehrung von (a) gilt nicht (siehe die Quaternionengruppe Q_8). Ein Beispiel für (b) findet man in der D_4, und damit auch ein Beispiel einer Untergruppe, die kein Normalteiler ist. Solche Beispiele sind auch die zweielementigen Untergruppen der S_3.

Lemma 1.1.20 **(a)** *Der Schnitt von Normalteilern ist wieder normal. Also gibt es zu $X \subseteq G$ den von X erzeugten Normalteiler*

$$\langle X \rangle^G = \left\langle \{ g^{-1}xg \mid g \in G, x \in X \} \right\rangle$$

(b) *Sei $U \leqslant G$. Dann ist $N_G(U) := \{g \in G \mid U^g = U\}$ eine Untergruppe, der **Normalisator von U in G**, und die größte Untergruppe von G, in der U normale Untergruppe ist.*

(c) *Sei $U \leqslant G$, $N_1, N_2 \trianglelefteq G$. Dann ist $UN_1 \leqslant G$ und $N_1N_2 \trianglelefteq G$.*

BEWEIS: (a) Sind N_i Normalteiler, so $g(\bigcap_{i\in I} N_i) = \bigcap_{i\in I} gN_i = \bigcap_{i\in I} N_i g = (\bigcap_{i\in I} N_i)g$, also ist auch $\bigcap_{i\in I} N_i$ normal. Der erzeugte Normalteiler muss alle Konjugierte von X enthalten,

also enthält er die rechte Seite. Man rechnet leicht nach, dass dies ein Normalteiler ist, der X enthält.

(b) Untergruppe: nachrechnen. Die Maximalität ist dann klar.

(c) Für $u, u' \in U$ und $n, n' \in N_1$ gibt es $n'', n''' \in N_1$ mit $unu'n' = uu'n''n' \in UN_1$ und $(un)^{-1} = n^{-1}u^{-1} = u^{-1}n''' \in UN_1$, also ist UN_1 Untergruppe. Da für $n_i \in N_i$ und $g \in G$ gilt: $g^{-1}n_1n_2g = g^{-1}n_1gg^{-1}n_2g \in N_1^g N_2^g = N_1N_2$ ist N_1N_2 sogar normal. □

Für $U, V \leqslant G$ ist UV nur dann eine Untergruppe, wenn $UV = VU$ (Übung). Achtung: Manche Autoren schreiben UV für die von den Produkten erzeugte Untergruppe!

Bemerkung 1.1.21

- Die Untergruppen von G, die $N \trianglelefteq G$ enthalten, sind von der Form UN für $U \leqslant G$.
- Die Untergruppen von G/N sind von der Form UN/N für $U \leqslant G$. Ist $\pi : G \to G/N$ der natürliche Gruppenepimorphismus, so gilt $UN = \pi^{-1}[\pi[U]]$.

Satz 1.1.22 (Noethersche Isomorphiesätze)

(a) *Sei $U \leqslant G, N \trianglelefteq G$. Dann ist $U \to UN/N$, $u \mapsto uN$ ein Gruppenepimorphismus mit Kern $U \cap N$. Es gilt also*

$$U \cap N \trianglelefteq U \quad \textit{und} \quad U/(U \cap N) \cong UN/N.$$

(b) *Sei $N \trianglelefteq G$ und $N \leqslant M \trianglelefteq G$. Dann ist $G/N \to G/M$, $gN \mapsto gM$ ein Gruppenepimorphismus mit Kern M/N. Es gilt also*

$$M/N \trianglelefteq G/N \quad \textit{und} \quad (G/N)/(M/N) \cong G/M.$$

Beweis: Nachrechnen, dass die Abbildungen wohldefiniert und surjektiv sind und den angegebenen Kern haben. □

In der Folge ist mit „Homomorphismus“ stets „Gruppenhomomorphismus“ gemeint, sofern nicht Gegenteiliges angegeben ist.

Bemerkung: Eine Untergruppe einer Gruppe G heißt **charakteristisch**, falls sie als Menge invariant unter allen Automorphismen ist. Charakteristische Untergruppen sind Normalteiler, charakteristische Untergruppen charakteristischer Untergruppen sind selbst charakteristisch in der großen Gruppe, und charakteristische Untergruppen von Normalteilern sind normal in der großen Gruppe (Übung).

1.2 Zyklische Gruppen

Definition und Lemma 1.2.1 *Eine Gruppe heißt **zyklisch**, falls sie von einem einzigen Element erzeugt wird.*

Sei $g \in G$ und $n \in \mathbb{N}$. Definiere $g^0 := e$ und induktiv $g^{n+1} := gg^n$, sowie $g^{-n} := (g^n)^{-1}$. Dadurch wird die Abbildung $g^{\sqcup} : (\mathbb{Z}, +) \to (G, \cdot)$, $n \mapsto g^n$ zu einem Homomorphismus. Außerdem gilt $(g^n)^m = g^{nm}$ (alles mit Induktion nachrechnen!)

Das Bild dieses Homomorphismus' ist die von g erzeugte zyklische Untergruppe $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.

*Die Ordnung von $\langle g \rangle$ heißt auch die **Ordnung von** g, $\operatorname{ord}(g)$, und ist das kleinste $n \in \mathbb{N} \setminus \{0\}$, für das $g^n = e$ gilt, falls es existiert (dies wird aus dem Beweis von 1.2.4(b) folgen.)*

Das kleinste gemeinsame Vielfache aller Ordnungen von Elementen in G heißt, sofern es existiert, der ***Exponent von*** *G.*

Bei additiv geschriebene Gruppen schreibt man ng statt g^n. Abelsche Gruppen werden dadurch zu $\mathbb{Z}$-Moduln (kommt später — dies sind gewissermaßen „Vektorräume über $\mathbb{Z}$“).

Lemma 1.2.2 *Sei G endlich, $g \in G$. Dann gilt, dass die Ordnung von g die Ordnung von G teilt und dass $g^{|G|} = e$ ist.*

Beweis: Folgt direkt aus dem Satz von Lagrange. □

Lemma 1.2.3 *Die Untergruppen von $\mathbb{Z}$ sind von der Form $m\mathbb{Z}$ für $m \in \mathbb{N}$.*

Beweis: Wegen $mz_1 + mz_2 = m(z_1 + z_2)$, $0 = m0$ und $-(mz) = m(-z)$ ist $m\mathbb{Z}$ Untergruppe. Sei nun $\{0\} \neq U \leqslant \mathbb{Z}$. Wähle minimales $m \in U \cap (\mathbb{N} \setminus \{0\})$ (existiert, da $u \in U \iff -u \in U$). Sei nun $u \in U \setminus m\mathbb{Z}$. Dann ist der Rest von u modulo m von der Form $u + km$ für ein $k \in \mathbb{Z}$, also in U, andererseits kleiner als m, somit gleich 0, d.h. $m|u$ bzw. $u \in m\mathbb{Z}$. □

Satz 1.2.4 **(a)** *Zyklische Gruppen sind kommutativ.*

(b) *Zu jeder Ordnung gibt es bis auf Isomorphie genau eine zyklische Gruppe, nämlich $\mathbb{Z}$ bzw. $\mathbb{Z}/m\mathbb{Z}$.*

(c) *Untergruppen und homomorphe Bilder zyklischer Gruppen sind zyklisch.*

Beweis: (a) Klar, da alle Potenzen von g untereinander kommutieren.

(b) Existenz: $\mathbb{Z}$ für unendliche Ordnung, Z_m für Ordnung m, jeweils zyklisch, da von 1 erzeugt.

Sei g Erzeuger von G. Dann ist der Homomorphismus $g^{\sqsubset} : \mathbb{Z} \to G$ entweder ein Isomorphismus oder es gibt einen Kern. Mit Lemma 1.2.3 und Homomorphiesatz: $G \cong \mathbb{Z}/m\mathbb{Z}$ für ein $m \in \mathbb{N}$.

(c) Homomorphe Bilder: Mit dem zweiten Isomorphiesatz und (b) folgt, dass jedes homomorphe Bild einer zyklischen Gruppe ein homomorphes Bild von $\mathbb{Z}$ ist, also wegen Lemma 1.2.3 selbst zyklisch. (Oder man rechne allgemeiner nach, dass Bilder von Erzeugern Erzeuger des Bildes sind!)

Untergruppen: Nach (b) kann man $V \leqslant \mathbb{Z}/N$ annehmen. Dann ist nach Bemerkung 1.1.21 $V = U/N$ mit $U \leqslant \mathbb{Z}$. Nach Lemma 1.2.3 ist U zyklisch, also ist auch V als homomorphes Bild von U zyklisch. □

Folgerung: Für eine Primzahl p gibt es bis auf Isomorphie nur eine Gruppe der Ordnung p, nämlich $\mathbb{Z}/p\mathbb{Z}$, da solch eine Gruppe zyklisch sein muss.

Bemerkung 1.2.5 Ein Homomorphismus $\alpha : \langle g \rangle \to H$ ist durch das Bild eines Erzeugers eindeutig bestimmt, da $\alpha(g^n) = \alpha(g)^n$. Insbesondere gibt es ebensoviele Automorphismen einer zyklischen Gruppe wie Erzeuger.

1.2.6 [Untergruppenverband und Automorphismengruppe zyklischer Gruppen]

(1) Die Untergruppen von $\mathbb{Z}$ sind von der Form $m\mathbb{Z}$ für $m \in \mathbb{N}$. Es gilt $m\mathbb{Z} \subseteq n\mathbb{Z} \iff n|m$. Somit ist der Untergruppenverband zum dualen (= „umgedrehten“) Teilbarkeitsverband von $\mathbb{N}$ isomorph.

$\mathbb{Z}$ hat zwei Erzeuger: $+1$ und -1, also ist $\mathrm{Aut}(\mathbb{Z}) \cong Z_2$.

(2) In $\mathbb{Z}/m\mathbb{Z}$ gilt $\mathrm{ord}(j + m\mathbb{Z}) = \frac{m}{\mathrm{ggT}(j,m)}$. Also gibt es $\varphi(m) := |\{1 \leq j \leq m \mid \mathrm{ggT}(j, m) = 1\}|$ viele Erzeuger und $\varphi(k)$ viele Elemente der Ordnung k.[1]

Der Untergruppenverband von $\mathbb{Z}/m\mathbb{Z}$ entspricht wegen Bemerkung 1.1.21 dem Teil des Untergruppenverbands von $\mathbb{Z}$, der oberhalb von $m\mathbb{Z}$ liegt (einschließlich $m\mathbb{Z}$), d.h. für jedes $k|m$ gibt es eine Untergruppe $k\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/\frac{m}{k}\mathbb{Z}$. Da der Teilbarkeitsverband von m durch $k \mapsto \frac{m}{k}$ zu seinem dualen Verband isomorph ist, gibt es zu jedem Teiler k von m genau eine Untergruppe der Ordnung k (vgl. das Beispiel in Bemerkung 1.1.15).

Es gilt also $|\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})| = \varphi(m)$. Für $\mathrm{ggT}(k, m) = 1$ ist die Abbildung $x \mapsto kx$ ein Automorphismus (Homomorphismus wegen dem Distributivgesetz; bijektiv, da der Erzeuger 1 auf den Erzeuger k abgebildet wird). Also ist $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) = \{x \mapsto kx \mid \mathrm{ggT}(k, m) = 1\}$.

Falls eine Gruppe zu jedem Teiler der Gruppenordnung genau eine Untergruppe besitzt, so ist diese Gruppe zyklisch (Übung).

Fakt 1.2.7 *Sind $n_1, n_2 \in \mathbb{N} \setminus \{0\}$, so lässt sich $\mathrm{ggT}(n_1, n_2)$ als $\mathbb{Z}$-Linearkombination von n_1 und n_2 schreiben, d.h. es gibt $\zeta_1, \zeta_2 \in \mathbb{Z}$ mit $\zeta_1 n_1 + \zeta_2 n_2 = \mathrm{ggT}(n_1, n_2)$. (Ergibt sich aus dem euklidischen Algorithmus.)*

Lemma 1.2.8 *$(Z_m^*, \cdot \bmod m) := \{k \in Z_m \mid k$ hat multiplikatives Inverses$\}$ ist Gruppe, und es gilt $Z_m^* = \{k \in Z_m \mid \mathrm{ggT}(k, m) = 1\}$.*

Folgerung: $\mathrm{Aut}(\mathbb{Z}/mZ) \cong Z_m^* \cong (\mathbb{Z}/m\mathbb{Z})^*$, da $(x \mapsto kx) \circ (x \mapsto lx) = (x \mapsto klx)$.

Beweis: $1 \in Z_m^*$, da $1 \cdot 1 = 1$. Mit $k \in Z_m^*$ ist $k^{-1} \in Z_m^*$ per Definition. Falls $k, l \in Z_m^*$, so $kl \in Z_m^*$, da $(kl)^{-1} = l^{-1}k^{-1}$. Also ist Z_m^* Gruppe.

Sei nun $\mathrm{ggT}(k, m) = l \neq 1$. Dann $m|kl$ in $\mathbb{Z}$, also $kl = 0$ in Z_m. Falls $xk = 1$, so $l = (xk)l = x0 = 0$: Widerspruch. Sei umgekehrt $\mathrm{ggT}(k, m) = 1$, dann $\zeta_1 k + \zeta_2 m = 1$ für geeignete $\zeta_i \in \mathbb{Z}$ (Fakt 1.2.7). Also gilt $\zeta_1' \cdot k = 1$ in Z_m für den Rest ζ_1' von ζ_1 modulo m. □

Bemerkung 1.2.9 [ohne Beweis] Für Primzahlpotenzen m mit $8 \nmid m$ ist $(\mathbb{Z}/m\mathbb{Z})^*$ selbst zyklisch.

Definition 1.2.10 **(a)** *Seien G, H Gruppen, dann wird die Menge $G \times H$ durch die komponentenweise Verknüpfung $(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2)$ zu einer Gruppe, dem (äußeren) **direkten Produkt** von G und H.*

(b) *Ist G eine Gruppe und $U, V \leqslant G$ mit $U \cap V = \{e\}$, $UV = G$ und $uv = vu$ für alle $u \in U, v \in V$, so ist $U \times V \cong G$ durch die Abbildung $(u, v) \mapsto uv$. Man nennt G dann (inneres) direktes Produkt von U und V und schreibt einfach $G = U \times V$ (Übung).*

Definition 1.2.11 *Seien G_i für $i \in I$ Gruppen. Dann ist das **direkte Produkt** dieser Gruppen die Gruppe $\prod_{i \in I} G_i := \{(g_i)_{i \in I} \mid g_i \in G_i\}$ mit der komponentenweisen Verknüpfung $(g_i)_{i \in I} \cdot$*

[1] φ heißt Eulersche φ-Funktion. Es folgt insbesondere $\sum_{k|n} \varphi(k) = n$.

$(h_i)_{i\in I} = (g_i h_i)_{i\in I}$. *Die* ***direkte Summe*** $\bigoplus_{i\in I} G_i$ *ist die Untergruppe* $\{(g_i)_{i\in I} \in \prod_{i\in I} G_i \mid g_i = e$ *für fast alle* $i \in I\}$.

Bemerkung: Für endliche Indexmengen I stimmen direktes Produkt und direkte Summe überein!

Satz 1.2.12 *Genau dann ist* $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *zyklisch und also isomorph zu* $\mathbb{Z}/mn\mathbb{Z}$*, wenn* $\mathrm{ggT}(m,n) = 1$ *gilt.*

Beweis: Offenbar ist $\mathrm{ord}(g,h) = \mathrm{kgV}\big(\mathrm{ord}(g), \mathrm{ord}(h)\big)$. Im teilerfremden Fall erzeugt also $(1 + m\mathbb{Z}, 1 + n\mathbb{Z})$ die ganze Gruppe; im nicht teilerfremden Fall gibt es kein Element mit Ordnung mn. □

Folgerung 1.2.13 (Chinesischer Restsatz, Gruppenversion) *Seien* $n_1, \ldots, n_k$ *paarweise teilerfremde Zahlen. Dann gilt*

$$\begin{aligned} \mathbb{Z}/(n_1 \cdot \ldots \cdot n_k)\mathbb{Z} &\cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \\ x + n_1 \cdot \ldots \cdot n_k\mathbb{Z} &\mapsto (x + n_1\mathbb{Z}, \ldots, x + n_k\mathbb{Z}) \end{aligned}$$

Beweis: Induktion über k. □

Definition 1.2.14 *Eine Gruppe* G *heißt* ***einfach****, wenn sie nicht trivial ist und außer* $\{e\}$ *und* G *keine weiteren Normalteiler enthält.*

Satz 1.2.15 *Die abelschen einfachen Gruppen sind gerade die zyklischen Gruppen von Primzahlordnung.*

Beweis: Hat G Primzahlordnung, so ist G einfach nach dem Satz von Lagrange. Sei umgekehrt G abelsch und einfach. Dann ist jede Untergruppe normal. Für $e \neq g \in G$ ist also $\langle g\rangle = G$, d.h. G ist zyklisch. Aus den Bestimmungen der Untergruppen zyklischer Gruppen in 1.2.6 folgt dann die Aussage. □

Bemerkung: A_5 ist die kleinste nicht-kommutative einfache Gruppe.

1.3 Abelsche Gruppen

In diesem Abschnitt seien Gruppen stets kommutativ und werden daher additiv geschrieben!

Definition und Bemerkung 1.3.1

- Wegen $n(g+h) = ng + nh$ für $n \in \mathbb{Z}$ und $g, h \in G$ gilt $\mathrm{ord}(g+h) \;\big|\; \mathrm{kgV}\big(\mathrm{ord}(g), \mathrm{ord}(h)\big)$. In beliebigen Gruppen gilt natürlich $\mathrm{ord}(g^{-1}) = \mathrm{ord}(g)$. Also ist

  $$G[n] \;:=\; \{g \in G \mid ng = 0\} \;=\; \{g \in G \mid \mathrm{ord}(g) \text{ teilt } n\} \quad \text{eine Untergruppe von } G.$$

  (Für nicht kommutativen Gruppen i.a. falsch, etwa $S_3[2] \neq \langle S_3[2]\rangle = S_3$.)
- Für eine Primzahl p definiert man außerdem die p**-Komponente von** G

  $$G_p := \{g \in G \mid p^n g = 0 \text{ für ein } n \in \mathbb{N}\} = \bigcup_{n\in\mathbb{N}} G[p^n],$$

  die eine Untergruppe von G ist. G heißt p**-Gruppe**, falls $G = G_p$.

- Elemente endlicher Ordnung heißen auch **Torsionselemente**; sie bilden die **Torsionsgruppe**

$$\mathrm{Tor}(G) := \{g \in G \mid ng = 0 \text{ für ein } n > 0\} = \bigcup_{n>1} G[n] = \bigcup_{p \text{ prim}} G_p.$$

  G heißt **Torsionsgruppe**, falls $G = \mathrm{Tor}(G)$, und **torsionsfrei**, falls $\mathrm{Tor}(G) = \{e\}$.

- Alle hier definierten Untergruppen sind charakteristisch.

Beispiele:

- $\mathbb{Z}$ und $\mathbb{C}$ sind torsionsfrei. $\mathrm{Tor}(\mathbb{R}^\times) = \{+1, -1\}$, $\mathrm{Tor}(\mathbb{C}^\times)$ besteht aus den Einheitswurzeln.
- $\{e\}$ ist die einzige torsionsfreie Torsionsgruppe.
- Sei G die Gruppe der Bijektionen von $\mathbb{Z}$. Die Elemente $\alpha : x \mapsto 1 - x$ und $\beta : x \mapsto -x$ haben beide Ordnung 2, $\alpha \circ \beta : x \mapsto x + 1$ hat Ordnung ∞. Also bilden hier die Torsionselemente keine Untergruppe.

Bemerkung 1.3.2 $G[p]$ ist eine Gruppe vom Exponenten p. Jede solche Gruppe ist auf natürliche Weise ein $\mathbb{F}_p$-Vektorraum. Insbesondere ist jede Untergruppe auch ein Unterraum, jeder Gruppenautomorphismus auch ein Vektorraumautomorphismus (Übung).

Lemma 1.3.3 **(a)** *$G/\mathrm{Tor}(G)$ ist torsionsfrei und maximaler torsionsfreier Quotient von G.*

(b) *$(G/G_p)_p = \{e\}$ und G_p ist minimal mit dieser Eigenschaft unter den Untergruppen von G.*

Beweis: In G/N ist $k(x + N) = kx + N$ und genau dann gleich dem neutralen Element N von G/N, wenn $kx \in N$ gilt. Mit $N = \mathrm{Tor}(G)$ folgt also, dass $x + \mathrm{Tor}(G)$ genau dann Ordnung k in $G/\mathrm{Tor}(G)$ hat, wenn kx endliche Ordnung in G hat, was genau dann der Fall ist, wenn x endliche Ordnung in G hat. Das beweist (a). Mit $N = G_p$ und $k = p^n$ folgt Teil (b) ganz analog. □

Satz 1.3.4 *Sei G abelsche Torsionsgruppe. Dann gilt $G = \bigoplus_{p \text{ prim}} G_p$.*

Beweis: Es ist klar, dass $G_p \cap G_q = \{e\}$ für verschiedene Primzahlen p, q gilt. Außerdem ist die ganze Gruppe kommutativ. Somit ist das Erzeugnis V der G_p in G einer innere direkte Summe der G_p. Zu zeigen ist also noch $V = G$.

Sei $g \in G$ und $\mathrm{ord}(g) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ die Primfaktorzerlegung. Setze $n_i := \frac{\mathrm{ord}(g)}{p_i^{\alpha_i}}$. Dann ist $g_i := n_i g \in G_{p_i}$, da $\mathrm{ord}(g_i) = p_i^{\alpha_i}$.

Nun gilt $\mathrm{ggT}(n_1, \ldots, n_k) = 1$, also gibt es $a_1, \ldots, a_k$ mit $a_1 n_1 + \cdots + a_k n_k = 1$ (per Induktion aus Fakt 1.2.7). Dann ist aber $g = (a_1 n_1 + \cdots + a_k n_k)g = a_1 g_1 + \cdots + a_k g_k \in \bigoplus_{p \text{ prim}} G_p$. □

Lemma 1.3.5 *Die endlich erzeugten abelschen Torsionsgruppen sind gerade die endlichen abelschen Gruppen.*

Beweis: „⇐“ ist klar.

„⇒“: Sei $G = \langle g_1, \ldots, g_k \rangle$ abelsch und alle $\mathrm{ord}(g_i)$ endlich. Dann schreibt sich $g \in G$ als $n_1 g_1 + \cdots + n_k g_k$ mit $0 \le n_i \le \mathrm{ord}(g_i)$: Dies sind nur endlich viele Möglichkeiten. □

Es ist also eine von Torsionselementen erzeugte abelsche Gruppe bereits eine Torsionsgruppe. Im nicht-abelschen Fall stimmt das nicht: Endlich viele Elemente endlicher Ordnung können eine unendliche Gruppe erzeugen; siehe das Beispiel der Bijektionen von $\mathbb{Z}$ oben!

Lemma 1.3.6 *Sei G abelsche Gruppe vom Exponenten p^m für eine Primzahl p, und sei $g \in G$ ein Element maximaler Ordnung p^m. Dann gibt es eine Untergruppe U mit $G = U \times \langle g \rangle$.*

BEWEIS: Sei U eine Untergruppe, die maximal bezüglich der Eigenschaft $U \cap \langle g \rangle = \{e\}$ ist. (Solch eine Untergruppe existiert z.B. nach dem Lemma von Zorn.) Zu zeigen ist nun, dass $G = U + \langle g \rangle$ gilt, denn dann ist es eine direkte Summe und der Satz ist bewiesen.

Angenommen also $G \neq U + \langle g \rangle$. Wähle ein $x \in G \setminus (U + \langle g \rangle)$ von minimaler Ordnung. Da $\mathrm{ord}(px) = \frac{\mathrm{ord}(x)}{p}$, ist $px \in U + \langle g \rangle$, also $px = u + lg$ mit $u \in U$ und $l \in \mathbb{N}$. Es gilt nun

$$0 = p^m x = \underbrace{p^{m-1}u}_{\in U} + \underbrace{p^{m-1}lg}_{\in \langle g \rangle},$$

also $p^{m-1}lg = -p^{m-1}u \in U \cap \langle g \rangle = \{e\}$. Aus $p^{m-1}lg = e$ und $\mathrm{ord}(g) = p^m$ folgt nun $p^m \mid p^{m-1}l$ und $p \mid l$.

Sei nun $l = pj$, also $p(x - jg) = u \in U$. Andererseits ist $x - jg \notin U$, da $x \notin U + \langle g \rangle$. Aus der Maximalitätsbedingung an U erhält man $\langle x - jg, U \rangle \cap \langle g \rangle \neq \{e\}$. Es gibt also k, k' und $u' \in U$ mit $e \neq kg = k'(x - jg) + u'$, d.h. $k'x = -u' + (k + k'j)g \in U + \langle g \rangle$.

Nun gibt es zwei Fälle: Wenn $p \mid k'$, dann gilt wegen $p(x - jg) \in U$ auch $k'(x - jg) \in U$, und wegen $u' \in U$ dann auch $kg \in U$, also $kg = e$: Widerspruch. Ween dagegen p und k' teilerfremd sind, so ist, da px und $k'x$ beide in $U + \langle g \rangle$ liegen, nach Fakt 1.2.7 auch $x \in U + \langle g \rangle$: ebenfalls Widerspruch! □

Folgerung 1.3.7 *Die endlichen abelschen Gruppen sind gerade die direkten Summen endlicher zyklischer Gruppen von Primzahlpotenzordnung.*

BEWEIS: „⇐“ ist klar.

„⇒“ gilt mit Satz 1.3.4 und Lemma 1.3.5, wobei man die Torsionskomponenten G_p anschließend mit Lemma 1.3.6 induktiv in eine direkte Summe zyklischer Gruppen erlegen kann. □

Beispiel: Alle abelschen Gruppen der Ordnung 12 sind bis auf Isomorphie: $Z_2 \times Z_2 \times Z_3$ und $Z_4 \times Z_3$; der Ordnung 8: $Z_2 \times Z_2 \times Z_2$, $Z_2 \times Z_4$ und Z_8.

Folgerung 1.3.8 *Sei K ein Körper und G eine endliche Untergruppe von $K^\times$. Dann ist G zyklisch.*

BEWEIS: Nach Satz 1.3.4 ist G von der Form $G_{p_1} \oplus \cdots \oplus G_{p_n}$ für paarweise verschiedene Primzahlen $p_1, \ldots, p_n$. Wegen dem chinesischen Restsatz reicht es zu zeigen, dass jedes G_{p_i} zyklisch ist. Nun ist solch ein G_p wiederum von der Form $Z_{p^{\alpha_1}} \oplus \cdots \oplus Z_{p^{\alpha_k}}$, es gilt also $|G_p[p]| = p^k$. Da die Elemente von $G[p]$ aber die Lösungen der Gleichung $X^p = 1$ in dem Körper K sind, gibt es höchstens p viele. Somit ist $k = 1$. □

Das nächste Ziel ist nun

Satz 1.3.9 *Sei G eine endlich erzeugte torsionsfreie abelsche Gruppe. Dann ist G isomorph zu einem $\mathbb{Z}^k := \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{k \text{ mal}}$.*

Bemerkung 1.3.10 Die $\mathbb{Z}^k$ sind die sogenannten **freien abelschen Gruppen**. Dies bedeutet: Wenn $\mathbb{Z}^k = \langle g_1 \rangle \times \cdots \times \langle g_k \rangle$ mit $\langle g_i \rangle \cong \mathbb{Z}$, wenn H eine abelsche Gruppe ist und $h_1, \ldots, h_k \in H$,

dann gibt es genau einen Homomorphismus $\varphi : \mathbb{Z}^k \to H$ mit $\varphi(g_i) = h_i$ (nämlich $n_1 g_1 + \cdots + n_k g_k \mapsto n_1 h_1 + \cdots + n_k h_k$).

Lemma 1.3.11 *Falls G abelsch ist, $H \leqslant G$ und $G/H \cong \mathbb{Z}^k$, dann gibt es eine Untergruppe $K \leqslant G$, so dass $K \cong \mathbb{Z}^k$ und $G = H \times K$.*

Beweis: Sei $\pi : G \to G/H = \langle g_1 + H\rangle \oplus \cdots \oplus \langle g_k + H\rangle$ mit $\langle g_i + H\rangle \cong \mathbb{Z}$ der natürliche Epimorphismus. Setze $K := \langle g_1, \ldots, g_k\rangle \leqslant G$.

Nun ist zum einen $G = H + K$, denn für $g \in G$ ist $\pi(g) = n_1 g_1 + \cdots + n_k g_k + H = \pi(n_1 g_1 + \cdots + n_k g_k)$ für geeignete $n_i \in \mathbb{Z}$, also $g - (n_1 g_1 + \cdots + n_k g_k) \in H$, somit $g \in H + K$.

Zum andern ist $H \cap K = \{e\}$, denn falls $n_1 g_1 + \cdots + n_k g_k \in H$, so ist $H = \pi(n_1 g_1 + \cdots + n_k g_k) = n_1 g_1 + \cdots + n_k g_k + H$, mithin müssen alle $n_i = 0$ sein.

Schließlich ist $K \cong (H \oplus K)/H = G/H \cong \mathbb{Z}^k$ □

Beweis von Satz 1.3.9: Sei $G = \langle g_1, \ldots, g_k\rangle$ torsionsfrei. Zeige: $G \cong \mathbb{Z}^l$ für ein $l \leqslant k$ per Induktion nach k.

Fall $k = 0$ ist klar: $G \cong \mathbb{Z}^0 = \{e\}$.

Fall $k > 0$: Setze $H := \{g \in G \mid \text{es gibt } n \in \mathbb{N} \text{ mit } ng \in \langle g_k\rangle\} \leqslant G$. Nun ist G/H torsionsfrei, denn $m(g+H) = H$ impliziert $mg \in H$, also $nmg \in \langle g_k\rangle$ für ein n, mithin $g \in H$. Per Induktion gilt nun $G/H = \langle g_1 + H, \ldots, g_{k-1}H\rangle \cong \mathbb{Z}^{l'}$ für ein $l' \leqslant k-1$. Nach Lemma 1.3.11 ist daher $G = K \oplus H$ mit $K \cong \mathbb{Z}^{l'}$.

Nun ist $H \cong G/K = \langle g_1 + K, \ldots, g_k + K\rangle$ endlich erzeugt. Außerdem ist $H/\langle g_k\rangle$ eine Torsionsgruppe, also endlich der Ordnung m. Es gilt also $mH \leqslant \langle g_k\rangle$. Die Abbildung $h \mapsto mh$ definiert somit einen Homomorphismus $H \to \langle g_k\rangle$, der wegen der Torsionsfreiheit von H injektiv ist. H ist also eine nicht-triviale Untergruppe von $\langle g_k\rangle \cong \mathbb{Z}$, also ist $H \cong \mathbb{Z}$ und insgesamt $G \cong K \oplus H \cong \mathbb{Z}^{l'} \oplus \mathbb{Z} = \mathbb{Z}^{l'+1}$.

Die Eindeutigkeit folgt daraus, dass $\mathbb{Z}^l/2\mathbb{Z}^l$ eine Gruppe vom Exponenten 2 ist, also ein $\mathbb{F}_2$-Vektorraum der Dimension l, und die Dimension ist eindeutig bestimmt. □

Satz 1.3.12 (Hauptsatz über endlich erzeugte abelsche Gruppen)
Die endlich erzeugten abelschen Gruppen sind genau die endlichen direkten Summen zyklischer Gruppen. Die Summanden sind bis auf Isomorphie und Reihenfolge eindeutig bestimmt.

Beweis: Sei G endlich erzeugt und abelsch. Dann ist $G/\mathrm{Tor}(G)$ endlich erzeugt, abelsch und torsionsfrei, also nach Satz 1.3.9 isomorph zu einem $\mathbb{Z}^l$. Mit Lemma 1.3.11 ist dann $G \cong \mathrm{Tor}(G) \oplus \mathbb{Z}^l$ mit eindeutig bestimmtem l. Wie oben sieht man, dass auch $\mathrm{Tor}(G)$ endlich erzeugt ist, also nach Folgerung 1.3.7 direkte Summe endlicher zyklischer Gruppen.

Eindeutigkeit: Es reicht zu sehen, dass sich $H := \mathrm{Tor}(G)_p$ eindeutig zerlegen lässt. Für jeden n ist nun $(p^n H)[p]$ eine abelsche Gruppe vom Exponenten p, also eine $\mathbb{F}_p$-Vektorraum einer festen Dimension. Aus diesen Dimensionen errechnet sich die Anzahl der Summanden $\mathbb{Z}/p^i\mathbb{Z}$. □

Beispiel: $\mathbb{Q}$ ist eine torsionsfreie abelsche Gruppe, aber nicht endlich erzeugt. Keine zyklische Untergruppe ist ein direkter Summand.

1.4 Gruppenoperationen

Definition 1.4.1 *Zu jeder Gruppe $(G, \cdot, {}^{-1}, e)$ gibt es die **opponierte Gruppe** G^{op} mit $G^{\mathrm{op}} = (G, \cdot^{\mathrm{op}}, {}^{-1}, e)$, wobei $g \cdot^{\mathrm{op}} h := h \cdot g$.*

Klar ist aus der Definition: $(G^{\mathrm{op}})^{\mathrm{op}} = G$

Lemma 1.4.2 *Stets ist $G \cong G^{\mathrm{op}}$, und genau dann $G = G^{\mathrm{op}}$ wenn G abelsch ist.*

Beweis: $G \to G^{\mathrm{op}}$, $x \mapsto x^{-1}$ ist Isomorphismus, und $G = G^{\mathrm{op}} \iff g \cdot h = g \cdot^{\mathrm{op}} h = h \cdot g$ für alle $g, h \in G \iff G$ abelsch. □

Bemerkung 1.4.3 **(a)** Beispiel von Funktionengruppen: Entscheidung zwischen Verknüpfung von rechts oder von links bedeutet Wahl zwischen G oder G^{op}.

(b) Wie verknüpft man Permutationen? Interpretiert man $\binom{123}{231}$ als „das Element 1 wird dorthin gestellt, wo sich bislang das Element 2 befindet“ oder als „das Element auf Platz 1 wird auf Platz 2 gestellt“? Die eine Interpretation liefert das Opponierte der zweiten!

(c) Konjugation liefert einen Homomorphismus von G in die opponierte Automorphismengruppe von G, also $G \to \mathrm{Aut}(G)^{\mathrm{op}}$, $g \mapsto (x \mapsto x^g = g^{-1}xg)$. Der Kern ist das **Zentrum** $Z(G) = \{g \in G \mid gh = hg \text{ für alle } h \in G\}$, das Bild heißt die Gruppe der **inneren Automorphismen** $\mathrm{Inn}(G)$ (Übung).

Definition 1.4.4 *Sei G Gruppe, $\Omega \neq \emptyset$ eine Menge. G **operiert (von links) auf** Ω, falls es zu jedem $g \in G$ und $\omega \in \Omega$ ein $g.\omega \in \Omega$ gibt, so dass gilt:*

— $g.(h.\omega) = (g \cdot h).\omega$ *für alle* $g, h \in G, \omega \in \Omega$
— $e.\omega = \omega$ *für alle* $\omega \in \Omega$.

*Ω heißt dann G-**Menge**.*

*Eine **Rechtsoperation von** G **auf** Ω ist eine Linksoperation von G^{op} auf Ω. Man schreibt dann $\omega.g$ für $g^{-1}.\omega$.*

Lemma 1.4.5 *Eine Linksoperation von G auf Ω „ist dasselbe wie“ ein Homomorphismus $\varphi : G \to \mathrm{Sym}(\Omega) := \{\alpha : \Omega \to \Omega \mid \alpha \text{ bijektiv.}\}$. Eine Rechtsoperation ist dasselbe wie ein Homomorphismus $\varphi : G \to \mathrm{Sym}(\Omega)^{\mathrm{op}}$ bzw. $\varphi : G^{\mathrm{op}} \to \mathrm{Sym}(\Omega)$.*

Beweis: Definiere φ aus der Gruppenoperation bzw. umgekehrt durch $g.\omega = \varphi(g)(\omega)$. Dann alle Eigenschaften nachrechnen! □

Beispiel 1.4.6 **(a)** Jede Gruppe operiert auf jeder nicht-leeren Menge auf triviale Weise durch $g.\omega = \omega$ für alle ω.

(b) Die Drehgruppe des Würfels operiert auf den drei Mittelsenkrechten, den vier Raumdiagonalen, den sechs Seitenflächen, den acht Ecken und den zwölf Kanten.

(c) S_n operiert auf $\{1, \ldots, n\}$ durch $\sigma.i = \sigma(i)$, aber z.B. auch durch $\sigma.i = \sigma(n + 1 - i)$.

Bemerkung: Ein K-Vektorraum V ist so etwas wie eine Operation des Körpers K auf der additiven Gruppe von V.

Definition 1.4.7 • *Eine Abbildung $\alpha : \Omega \to \Omega'$ zwischen G-Mengen heißt* ***G-äquivariant****, falls $\alpha(g.\omega) = g.\alpha(\omega)$ für alle $g \in G$ und $\omega \in \Omega$.*

- *Zwei Operationen von G auf Ω bzw. Ω' heißen* ***äquivalent****, falls es eine G-äquivariante Bijektion $\alpha : \Omega \to \Omega'$ gibt (Anschaulich: Die Operationen von G auf Ω und Ω' unterscheiden sich nur durch Umbenennen der Elemente von Ω.)*
- *Sei nun $\varphi : G \to \mathrm{Sym}(\Omega)$ eine Operation. Dann definiert $\omega \sim \omega'$, falls es ein $g \in G$ gibt mit $g.\omega = \omega'$, eine Äquivalenzrelation auf Ω. Die Äquivalenzklassen $\omega^G = \{g.\omega \mid g \in G\}$ heißen* ***Bahnen****.*
  $G_\omega := \{g \in G \mid g.\omega = \omega\}$ heißt der ***Stabilisator*** *von $\omega \in \Omega$ und ist eine Untergruppe von G.*
- *Die Operation heißt*
  - ***transitiv****, falls es nur eine Bahn gibt;*
  - ***treu****, falls $\mathrm{Kern}(\varphi) = \bigcap_{\omega\in\Omega} G_\omega = \{g \in G \mid g.\omega = \omega$ für alle $\omega \in \Omega\}$ trivial ist;*
  - ***semi-regulär****, falls $G_{\{e\}}$ für alle $\omega \in \Omega$ ist;*
  - *und* ***regulär****, falls sie transitiv und semi-regulär ist.*

Der Kern der Operation, also der Schnitt über alle Stabilisatoren, ist stets ein Normalteiler. Im Falle einer treuen Operation ist bis auf Isomorphie G eine Untergruppe von $\mathrm{Sym}(\Omega)$. Man nennt G dann auch **Permutationsgruppe** auf Ω, falls G als Untergruppe von $\mathrm{Sym}(\Omega)$ gegeben ist.

Beispiel 1.4.8 G operiert regulär auf $\Omega = G$ durch Linksmultiplikation, d.h. $g.\omega = g \cdot \omega$. Rechtsmultiplikation $\omega.g = \omega \cdot g$ kann man entweder als reguläre Operation von G^{op} auf $\Omega = G$ oder als Rechtsoperation von G auf $\Omega = G$ auffassen. Rechtsmultiplikation mit dem Inversen liefert also wieder eine reguläre Operation von G auf $\Omega = G$.

Es folgt der

Satz 1.4.9 (Satz von Cayley) *Jede Gruppe lässt sich als Permutationsgruppe darstellen, d.h. jede Gruppe ist Untergruppe einer Gruppe der Form* $\mathrm{Sym}(\Omega)$.

Sei nun $\lambda_G : G \to \mathrm{Sym}(G)$, $g \mapsto (x \mapsto gx)$ die Linksmultiplikation, $\varrho_G : G \to \mathrm{Sym}(G)$, $g \mapsto (x \mapsto xg)$ die Rechtsmultiplikation, und $\iota : G \to G$, $g \mapsto g^{-1}$ die Inversenabbildung. (Achtung: im allgemeinen ist nur λ_G ein Homomorphismus!)

Lemma 1.4.10 **(a)** *Die Operationen λ_G und $\varrho_G \circ \iota$ von G auf G sind äquivalent vermöge ι. Also sind die Untergruppen $\lambda_G(G)$ und $\varrho_G(G)$ von $\mathrm{Sym}(G)$ durch ι konjugiert, d.h. $\iota^{-1} \circ \varrho_G(G) \circ \iota = \lambda_G(G)$.*

(b) *$\lambda_G(G) = \varrho_G(G) \iff G$ ist abelsch.*

(c) *$\varrho_G(G) = \{\alpha \in \mathrm{Sym}(G) \mid \alpha$ ist „λ_G-äquivariant“$\}$. Dies nennt man auch die opponierte Gruppe G^{op} der Permutationsgruppe G, wenn diese mit $\lambda_G(G)$ gleichgesetzt wird.*

Beweis: (a) $\iota(\lambda_G(g)(\omega)) = (g\omega)^{-1} = \omega^{-1}g^{-1} = \varrho_G(g^{-1})(\omega^{-1}) = (\varrho_G \circ \iota)(g)(\iota(\omega))$. Es gilt also $\lambda_G(g) = \iota^{-1} \circ \varrho_G(g^{-1}) \circ \iota$ (wobei natürlich $\iota = \iota^{-1}$ gilt, die Konjugation also auch andersherum geschrieben werden kann).

(b) Ist G kommutativ, so ist $\{x \mapsto gx \mid g \in G\} = \{x \mapsto xg \mid g \in G\} = \{x \mapsto xg^{-1} \mid g \in G\}$. Sind umgekehrt die Abbildungen $x \mapsto gx$ und $x \mapsto xh^{-1}$ gleich, so folgt ($x = e$ einsetzen!) $g = h^{-1}$, also $gx = xh^{-1} = xg$ für alle x.

(c) $\{\alpha \in \mathrm{Sym}(G) \mid \alpha\ \lambda_G\text{-invariant}\} = \{\alpha : G \to G \mid \alpha(g.\omega) = g.\alpha(\omega) \text{ für alle } \omega \in G\}$ soll gleich sein $\{\omega \mapsto \omega h \mid h \in G\}$.

„$\supseteq$“ gilt offensichtlich, denn $(g.\omega).h = g.(\omega.h)$.

„$\subseteq$“: Sei $\omega_0 \in G$ fest und α λ_G-invariant. Sei $h \in G$ so, dass $\alpha(\omega_0) = \omega_0 h$. Dann ist $\alpha(\omega) = \alpha(\omega\omega_0^{-1}\omega_0) = \omega\omega_0^{-1}\alpha(\omega_0) = \omega\omega_0^{-1}\omega_0 h = \omega h$. □

Beispiel 1.4.11 [**Typische Beispiele für Gruppenoperationen**]

- Sei $U \leqslant G$. Dann operiert U durch Linksmultiplikation auf $\Omega = G$. Die Operation ist treu, aber nicht transitiv, es sei denn $U = G$. Die Bahnen sind die Rechtsnebenklassen von U in G.
- G operiert durch Linksmultiplikation auf den Linksnebenklassen von U in G (als Menge geschrieben $G : U$) durch $g.hU = (gh)U$. Die Operation ist transitiv, ihr Kern ist der größte in U enthaltene Normalteiler von G (auch U_G geschrieben). Die Operation ist genau dann regulär, wenn $U = \{e\}$.
- G operiert von rechts auf $\Omega = G$ durch Konjugation, d.h. $\omega.g = \omega^g$ $(= g^{-1}\omega g)$. Der Kern ist das Zentrum $Z(G)$, die Bahnen sind die Konjugationsklassen $h^G = \{h^g \mid g \in G\}$. Im Unterschied zu den vorherigen Beispielen sind diese i.a. unterschiedlich groß! Der Stabilisator $G_\omega = \{g \in G \mid \omega^g = \omega\} = \{g \in G \mid \omega g = g\omega\}$ heißt der **Zentralisator** $C_G(\omega)$ **von** ω **in** G.

Satz 1.4.12 *G operiere von links auf Ω. (Die analogen Aussagen gelten für Rechtsoperationen.)*

(a) *Die Bahn ω^G steht in Bijektion mit den Linksnebenklassen $G : G_\omega$ vermöge $g.\omega \mapsto gG_\omega$. Also gilt $|\omega^G| = (G : G_\omega)$. Im Falle einer endlichen Gruppe gilt also, dass die Größe der Bahn die Gruppenordnung teilt.*

(b) *Ist $\omega' \in \omega^G$, etwa $\omega' = g.\omega$, so gilt $G_{\omega'} = gG_\omega g^{-1} = G_\omega^{(g^{-1})}$.*

(c) *Operiert G transitiv, so gilt $|G| = |\Omega| \cdot |G_\omega|$ für jedes $\omega \in \Omega$.*

(d) *Operiert G regulär, so gilt $|G| = |\Omega|$.*

Beweis: (a) Die Abbildung $\omega^G \to G : G_\omega$, $g.\omega \mapsto gG_\omega$ ist wohldefiniert und injektiv, denn $g.\omega = g'.\omega \Leftrightarrow (g^{-1}g').\omega = \omega \Leftrightarrow g^{-1}g' \in G_\omega \Leftrightarrow g'G_\omega = gG_\omega$, und klarerweise surjektiv.

(b) $h \in G_{\omega'} \Leftrightarrow h.\omega' = \omega' \Leftrightarrow hg.\omega = g.\omega \Leftrightarrow g^{-1}hg.\omega = \omega \Leftrightarrow g^{-1}hg \in G_\omega \Leftrightarrow h \in gG_\omega g^{-1}$.

(c) Mit (a) gilt $|\Omega| = |\omega^G| = (G : G_\omega)$, also ist $|\Omega| \cdot |G_\omega| = (G : G_\omega) \cdot |G_\omega| = |G|$.

(d) G regulär impliziert $G_\omega = \{e\}$, also $|G_\omega| = 1$. □

Folgerung 1.4.13 (1. Folgerung aus Satz 1.4.12) **(a)** *Jede transitive Operation von G ist äquivalent zur Linksmultiplikation von G auf $G : G_\omega$ für beliebiges $\omega \in \Omega$.*

(b) *Jede reguläre Operation von G ist äquivalent zur Linksmultiplikation von G auf sich selbst.*

(c) *Falls G kommutativ ist, so ist jede treue transitive Operation regulär.*

Beweis: (a) folgt sofort aus Satz 1.4.12 (a) mit der G-äquivarianten Bijektion

$$\Omega = \omega^G \to G : G_\omega, g.\omega \mapsto gG_\omega.$$

(b) Folgt wegen „regulär = transitiv + $G_\omega = \{e\}$“ aus (a).

(c) Seien $\omega, \omega' \in \Omega$. Dann existiert wegen der Transitivität ein $g \in G$ mit $g.\omega = \omega'$. Also ist mit Satz 1.4.12 (b) und da G kommutativ $G_{\omega'} = (G_\omega)^{g^{-1}} = G_\omega$. Da die Opertaion treu ist, folgt $\{e\} = \bigcap_{\omega\in\Omega} G_\omega = G_\omega$ für jedes $\omega \in \Omega$. □

Lemma 1.4.14 *G operiere durch Linksmultiplikation auf $G : U$ und auf $G : V$ für zwei Untergruppen U und V. Beide Operationen sind genau dann äquivalent, wenn U und V zueinander konjugiert sind.*

Beweis: „⇐“: Ist $V = U^h$, so ist $G : U \to G : U^h, gU \mapsto gh^{-1}U$ die G-äquivariante Bijektion.

„⇒“: Sie eine G-äquivariante Bijektion $\alpha : G : U \to G : V$ gegeben, uns sei $h \in G$ so, dass $\alpha(U) = hV$. Dann gilt

$$g \in U \iff ghV = g\alpha(U) = \alpha(gU) = \alpha(U) = hV \iff h^{-1}gh \in V \iff g \in V^{h^{-1}}.$$

□

Folgerung 1.4.15 (2. Folgerung aus Satz 1.4.12) *Operiert G auf Ω, so gilt*

$$|\Omega| = \sum_{i\in I} (G : G_{\omega_i}),$$

wobei $\{\omega_i \mid i \in I\}$ ein Repräsentantensystem der Bahnen ist.

1.4.16 [Spezialfall „Klassengleichung“]

$$|G| = |Z(G)| + \sum_{i\in I} (G : C_G(g_i)),$$

wobei $\{g_i \mid i \in I\}$ ein Repräsentantensystem der nicht-einelementigen Konjugationsklassen von G ist.

Satz 1.4.17 *Sei p eine Primzahl.*

(a) *Ist G nicht-triviale endliche p-Gruppe, so ist $Z(G) \neq \{e\}$.*

(b) *Gilt $|G| = p^2$, so ist G kommutativ.*

Beweis: (a) Da p sowohl die Gruppenordnung als auch die Indizes der Zentralisatoren teilt, muss p nach der Klassengleichung auch die Ordnung des Zentrums teilen. Das Zentrum hat also mindestens p Elemente.

(b) Falls G nicht kommutativ ist, so ist das Zentrum eine echte und nach (a) nicht-triviale Untergruppe, hat also p Elemente. Dann ist auch $|G/Z(G)| = p$, also ist $G/Z(G)$ zyklisch $= \langle gZ(G)\rangle$. Es folgt $G = \langle g, Z(G)\rangle$. Somit ist G aus miteinander kommutierenden Elementen erzeugt und also kommutativ: Widerspruch. □

1.4.18 [Semi-direkte Produkte]

Äußeres semi-direktes Produkt: Gegeben seien Gruppen H und N, H operiere als Automorphismengruppe auf N, d.h. es gebe einen Homomorphismus $\alpha : H \to \mathrm{Aut}(N)$. Dann wird die Menge $H \times N$ durch die Operation

$$(h_1, n_1) \cdot (h_2, n_2) := (h_1h_2, n_1 \cdot \alpha(h_1)(n_2))$$

zu einer Gruppe, dem **semi-direkten Produkt** von H mit N (gemäß α), geschrieben: $H \ltimes_\alpha N$ bzw. $N \rtimes_\alpha H$. Es sind dann $h \mapsto (h, e)$ und $n \mapsto (e, n)$ Einbettungen von H und N in das semi-direkte Produkt. Dadurch wird H zur Untergruppe, N zum Normalteiler und α zur Konjugation mit dem Inversen.

Inneres semi-direktes Produkt: Sei $N \trianglelefteqslant G$ und $H \leqslant G$ so, dass $HN = G$ und $H \cap N = \{e\}$ gilt. Dann operiert H auf N durch Konjugation mit dem Inversen, und mit dem Homomorphismus $\alpha : H \to \mathrm{Aut}(N)$, $h \mapsto (n \mapsto n^{(h^{-1})})$ wird G isomorph zu $H \ltimes_\alpha N$. Man nennt dann G das semi-direkte Produkt von H und N und schreibt $G = H \ltimes N$ bzw. $G = N \rtimes H$.

Bemerkung: Ein semi-direktes Produkt ist genau dann ein direktes Produkt, wenn der Homomorphismus α trivial ist. (Trotzdem kann, wie im Falle der Symmetriegruppe des Würfels, ein nicht-direktes semi-direktes Produkt zu einem direkten Produkt isomorph sein!)

Beispiel 1.4.19 $S_n = Z_2 \ltimes A_n$ für $n \geqslant 2$. $D_n = Z_2 \ltimes Z_n$ für $n \geqslant 3$. Man definiert daher $D_1 = Z_2$ und $D_2 = Z_2 \times Z_2$.

Da $\mathrm{Aut}(Z_3) \cong Z_2$ gibt es kein echtes semi-direktes Produkt $Z_3 \ltimes Z_3$, nur das direkte Produkt!

1.5 Die Sylow–Sätze

G sei in diesem Abschnitt stets eine endliche Gruppe, p eine Primzahl, welche die Gruppenordnung teilt. Genauer sei $|G| = p^a \cdot n$, wobei p kein Teiler mehr von n ist.

Definition 1.5.1 *Eine Untergruppe von G heißt p–**Sylow–Gruppe** von G, falls sie die Ordnung p^a hat (d.h. sie ist eine p-Gruppe und p teilt nicht ihren Index).* $\mathrm{Syl}_p(G)$ *bezeichne die Menge der p–Sylow–Gruppen von G und $N_p(G)$ sei ihre Anzahl.*

Satz 1.5.2 (Sylowsche Sätze) **(a)** *Falls p^b die Ordnung von G teilt und $\#(p^b)$ die Anzahl der Untergruppen von G der Ordnung p^b bezeichnet, so gilt $\#(p^b) \equiv 1 \pmod n$. Insbesondere existieren immer p–Sylow–Gruppen.*

(b) *Je zwei p–Sylow–Gruppen einer Gruppe G sind zueinander konjugiert. Für jede p–Sylow–Gruppe P gilt: $N_p(G) = (G : N_G(P)) \equiv 1 \pmod p$. Insbesondere teilt $N_p(G)$ die Zahl n.*

(c) *Jede p-Untergruppe von G ist in einer p–Sylow–Gruppe enthalten.*

Folgerung 1.5.3 (Satz von Cauchy) *Falls die Primzahl p die Ordnung einer Gruppe G teilt, so besitzt G Elemente der Ordnung p.*

Beweis der Sylow–Sätze: (a) $\Omega := \left\{ M \subseteq G \;\middle|\; |M| = p^b \right\}$ wird durch Linksmultiplikation zu einer G-Menge; die Bahnen seien $\Omega_j = \{gM_j \mid g \in G\}$ für $j = 1, \ldots, k$. Schließlich sei $U_j := \{g \in G \mid gM_j = M_j\}$ der Stabilisator von M_j.

Es gilt somit $M_j = U_j \cdot M_j = \bigcup_{g \in M_j} U_j g$, also ist $|U_j|$ ein Teiler von $|M_j| = p^b$, d.h. U_j ist eine p-Gruppe. Mit Satz 1.4.12 (c) gilt $|\Omega_j| = (G : U_j)$, d.h. mit $m = \frac{|G|}{p^b}$ gilt:

$$|U_j| < p^b \iff pm \text{ teilt } |\Omega_j|.$$

Außerdem gilt

$$\begin{aligned} |U_j| = m &\iff |\Omega_j| = m \\ &\iff M_j = U_j g_j \text{ für ein } g_j \in G \\ &\iff \Omega_j = \{gU_j g_j \mid g \in G\} = \{g g_j g_j^{-1} U_j g_j \mid g \in G\} = \{h U_j^{g_j} \mid h \in G\} = U_j^{g_j} : G \end{aligned}$$

Betrachtet man die Bahnen modulo pm, bleiben also nur noch solche übrig, deren Stabilisatoren die Ordnung p^b haben:

$$|\Omega| \;=\; \binom{mp^b}{p^b} \;\equiv\; \sum_{|\Omega_j|=m} |\Omega_j| \;=\; \#(p^b) \cdot m \pmod{pm}$$

Im Spezialfall „G zyklisch“ ist $\#(p^b) = 1$ nach 1.2.6; es gilt also $\binom{mp^b}{p^b} \equiv m \pmod{pm}$. Für nun wieder beliebiges G erhält man also $m \equiv \#(p^b) \cdot m \pmod{pm}$ und daraus $1 \equiv \#(p^b) \pmod{p}$.

(b),(c) Sei P eine p-Sylowgruppe und Q eine beliebige p-Untergruppe von G. Dann operiert Q auf $\{P^g \mid g \in G\}$ durch Konjugation, und nach Satz 1.4.12 (c) ist die Mächtigkeit jeder Bahn ein Teiler von $|Q|$, also eine p-Potenz.

Falls es eine einelementige Bahn $\{P^g\}$ gibt, so ist Q eine Untergruppe des Stabilisators von P^g unter Konjugation, also des Normalisators $N_G(P^g)$. Es ist dann $P^g \trianglelefteq \langle P^g, Q\rangle$ und daher $\langle P^g, Q\rangle = Q \cdot P^g$. Wegen $|Q \cdot P^g| = \frac{|Q| \cdot |P^g|}{|Q \cap P^g|}$ ist $Q \cdot P^g$ eine p-Gruppe. Da aber P^g maximale p-Untergruppe von g ist, folgt $Q \leqslant P^g$.

Betrachte nun den Spezialfall $P = Q$: Dann ist $\{P\}$ offenbar eine einelementige Bahn, und nach den gerade angestellten Überlegungen auch die einzige (da $P \leqslant P^g$ für jede weitere einelementige Bahn $\{P^g\}$ gelten würde). Also gilt für die transivite Opertaion von G auf den Konjugierten von P:

$$(G : N_G(P^g)) = |\{P^g \mid g \in G\}| \equiv 1 \pmod{p}.$$

Sei Q nun wieder beliebig wie oben. Da die Bahnen p-Potenzmächtigkeit haben, muss es hier auch mindestens eine einelementige Bahn $\{P^g\}$ geben. Es folgt also $Q \leqslant P^g \in \mathrm{Syl}_p(G)$ und $Q = P^g$, falls $Q \in \mathrm{Syl}_p(G)$. □

Bemerkung 1.5.4 Ist $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ die Primfaktorzerlegung und $P_i \in \mathrm{Syl}_{p_i}(G)$, so gilt: $P_i \cap P_j = \{e\}$ für $i \neq j$ (da der Schnitt sowohl p_i- als auch p_j-Gruppe ist) und $G = \langle P_1, \ldots, P_k\rangle$ (denn da $P_i \leqslant \langle P_1, \ldots, P_k\rangle$ teilt $p_i^{\alpha_i}$ die Ordnung dieser Gruppe, folglich hat $\langle P_1, \ldots, P_k\rangle$ die gleiche Ordnung wie G).

Satz 1.5.5 *Sind alle Sylowgruppen $P_1, \ldots, P_k$ Normalteiler von G, so gilt $G = P_1 \times \cdots \times P_k$.*

Solche Gruppen, die direktes Produkt ihrer Sylow–Gruppen sind, heißen **nilpotent**.

Beweis: Da Sylow–Gruppen zur gleichen Primzahl konjugiert sind, folgt aus der Normalität $N_p(G) = 1$ für alle p. Per Induktion nach k zeigt man nun

$$\begin{aligned} &(a_k) \quad |P_1 \cdot \ldots \cdot P_k| = |P_1| \cdot \ldots \cdot |P_k| \\ &(b_k) \quad (P_1 \cdot \ldots \cdot P_k) \cap P_{k+1} = \{e\}. \end{aligned}$$

(b_1) is klar, und aus (a_k) folgt (b_k), da P_{k+1} eine Sylow–Gruppe zu einer neuen Primzahl ist. Schließlich folgt (a_{k+1}) aus (b_k), da

$$|P_1 \cdot \ldots \cdot P_{k+1}| = \frac{|P_1 \cdot \ldots \cdot P_k| \cdot |P_{k+1}|}{|(P_1 \cdot \ldots \cdot P_k) \cap P_{k+1}|}.$$

Zu zeigen ist nun nur noch, dass die P_i untereinander kommutieren. Sei $g \in P_i, h \in P_j$. Dann ist $g^{-1}h^{-1}gh \in P_i P_i^h = P_i P_i = P_i$, aber andererseits auch in $P_j^g P_j = P_j$. Somit ist $g^{-1}h^{-1}gh \in P_i \cap P_j = \{e\}$, oder $gh = hg$ □

Satz 1.5.6 *Sei $N \trianglelefteq G$ und $P \in \mathrm{Syl}_p(G)$. Dann ist $P \cap N \in \mathrm{Syl}_p(G)$ und $PN/N \in \mathrm{Syl}_p(G/N)$.*

Beweis: Klar ist, dass $P \cap N$ und PN/N p-Gruppen sind. Zu zeigen ist noch, dass es maximale p-Untergruppen sind. Dies folgt aus „verallgemeinerten Isomorphiesätzen“. Z.B. ist

$$NP : P \to N : (P \cap N),\ nP \mapsto n(P \cap N)$$

eine Bijektion, also hat

$$(N : P \cap N) = \frac{|NP|}{|P|} \mid \frac{|G|}{|P|}$$

keinen p-Anteil mehr. Ähnlich sieht man $(G/N : PN/N) = (G : PN) \mid (G : P)$. □

1.5.7 [Klassifikation der Gruppen der Ordnung 12]
Sei $|G| = 12$, $P \in \mathrm{Syl}_2(G)$ und $Q \in \mathrm{Syl}_3(G)$. Also ist $P \cong Z_4$ oder $\cong Z_2 \times Z_2$ und $Q \cong Z_3$.
Außerdem gilt $N_2(G) \equiv 1 \pmod 2$ und $N_2(G) \mid 3$, also ist $N_2(G) = 1$ oder $= 3$.
Ebenso $N_3(G) \equiv 1 \pmod 3$ und $N_3(G) \mid 4$, also ist $N_2(G) = 1$ oder $= 4$.

Angenommen $N_3(G) = 4$. Dann ist $|\{g \in G \mid \mathrm{ord}(g) \text{ teilt } 4\}| = 12 - 2 \cdot N_3(G) = 4$, also $N_2(G) = 1$. Somit ist mindestens eine der Sylow–Gruppen normal, und mit Bemerkung 1.5.4 folgt, dass G ein semi-direktes Produkt von P und Q ist.

1. Fall: $N_2(G) = N_3(G) = 1$.
(a) Falls $P \cong Z_4$, so $G \cong Z_4 \times Z_3$.
(b) Falls $P \cong Z_2 \times Z_2$, so $G \cong Z_2 \times Z_2 \times Z_3$.

2. Fall: $N_2(G) = 1$ und $N_3(G) = 4$
(a) Falls $P \cong Z_4$, so gibt es keinen nicht-trivialen Homomorphismus $Q \cong Z_3 \to \mathrm{Aut}(P) \cong Z_2$.
(b) Falls $P \cong Z_2 \times Z_2$, so gibt es zwei nicht-triviale, zueinander konjugierte Automorphismen $Q \to \mathrm{Aut}(P) \cong S_3$; also $G \cong (Z_2 \times Z_2) \rtimes Z_3 \cong A_4$.

3. Fall: $N_2(G) = 3$ und $N_3(G) = 1$
(a) Falls $P \cong Z_4$, so gibt es einen einzigen nicht-trivialen Homomorphismus $P \to \mathrm{Aut}(Q) \cong Z_2$; also $G \cong Z_4 \ltimes Z_3$.
(b) Falls $P \cong Z_2 \times Z_2$, so gibt es drei nicht-triviale, zueinander konjugierte Automorphismen $P \to \mathrm{Aut}(Q) \cong Z_2$; also $G \cong (Z_2 \times Z_2) \ltimes Z_3 \cong D_6$.

1.6 Auflösbare Gruppen

Definition 1.6.1 *Eine **Kompositionsreihe** einer Gruppe G ist eine Folge von Untergruppen $N_0, \ldots, N_k$ von G mit $\{e\} = N_k \trianglelefteq N_{k-1} \trianglelefteq \ldots \trianglelefteq N_1 \trianglelefteq N_0 = G$ und einfachen Faktorgruppen N_i/N_{i+1}.*

*Die Gruppen N_i/N_{i+1} heißen **Kompositionsfaktoren** von G, die Zahl k heißt **Länge der Reihe**.*

Bemerkung 1.6.2 Falls G endlich ist, so gibt es stets Kompositionsreihen, denn jede „Subnormalreihe“ $N_k \trianglelefteq N_{k-1} \trianglelefteq \ldots \trianglelefteq N_0$ lässt sich zu einer Kompositionsreihe verfeinern. (Wenn

N_i/N_{i+1} nicht einfach ist, existiert ein echter, nicht-trivialer Normalteiler, der die Form M/N_{i+1} hat mit $N_{i+1} \trianglelefteq M \trianglelefteq N_i$.)

Beispiel 1.6.3 Kompositionsreihen in $G = Z_4 \ltimes Z_3$: $\{e\} \trianglelefteq Z_2 \trianglelefteq Z_6 \trianglelefteq G$; $\{e\} \trianglelefteq Z_3 \trianglelefteq Z_6 \trianglelefteq G$.
Kompositionsreihen in Z_{12}: $\{e\} \trianglelefteq Z_2 \trianglelefteq Z_4 \trianglelefteq Z_{12}$; $\{e\} \trianglelefteq Z_2 \trianglelefteq Z_6 \trianglelefteq Z_{12}$; $\{e\} \trianglelefteq Z_3 \trianglelefteq Z_6 \trianglelefteq Z_{12}$.

Zwei Kompositionsreihen heißen äquivalent ($\sim$), falls sie die gleiche Länge haben und, bis auf Permutation, die gleichen Kompositionsfaktoren, jeweils gleich häufig.

Satz 1.6.4 (Satz von Jordan und Hölder) *Je zwei Kompositionsreihen einer endlichen Gruppe sind äquivalent.*

Beweis: Beweis per Induktion nach $|G|$; für $|G| = 1$ gilt der Satz trivialerweise; sei also $|G| > 1$ und seien $M_0 \trianglelefteq \ldots \trianglelefteq M_m \trianglelefteq G$ und $N_0 \trianglelefteq \ldots \trianglelefteq N_n \trianglelefteq G$ zwei Kompositionreihen. Falls $M_m = N_n$, so ist man fertig nach Induktion; ebenso, falls $M_m N_n \neq G$ (weil man dann beide Kompositionsreihen durch $M_m N_n$ verfeinern kann, bis wohin sie per Indutkion äquivalent sind). Sei also $M_m N_n = G$; dann gilt $G/M_m \cong N_n/(M_m \cap N_n)$ und $G/N_n \cong M_m/(M_m \cap N_n)$, d.h. die beiden Reihen $M_m \cap N_n \trianglelefteq M_m \trianglelefteq G$ und $M_m \cap N_n \trianglelefteq N_n \trianglelefteq G$ sind sozusagen „äquivalente Kompositionsreihenstücke“ oberhalb $M_m \cap N_n$. Sei außerdem $L_0 \trianglelefteq \ldots \trianglelefteq L_l = M_m \cap N_n$ eine Kompositionreihe von $M_m \cap N_n$. Dann gilt per Induktion (alles sind Kompositionsreihen!)

$$M_0 \trianglelefteq \ldots \trianglelefteq M_m \sim L_0 \trianglelefteq \ldots \trianglelefteq L_l \trianglelefteq M_n \quad \text{und} \quad L_0 \trianglelefteq \ldots \trianglelefteq L_l \trianglelefteq N_n \sim N_0 \trianglelefteq \ldots \trianglelefteq N_n.$$

Alle vier Kompositionsreihen können nun durch Anfügen von G zu Kompositionsreihen G erweitert werden; dadruch werden die mittleren beiden auch äquivalent; per Transitivität sind es also die beiden Ausgangssreihen (man zeichen sich am besten ein Diagramm)! □

Beispiel 1.6.5 Ein unendlicher Vektorraum über $\mathbb{F}_p$ ist ein Beispiel einer unendlichen Gruppe ohne (endliche) Kompositionsreihe.

Definition 1.6.6 *Eine endliche Gruppe heißt **auflösbar**, falls alle Kompositionsfaktoren abelsch sind.*

Beispiel 1.6.7 Auflösbar sind:

- alle abelschen Gruppen (klar);
- die Diedergruppen D_n (hat Normalteiler Z_n mit Quotient Z_2);
- alle p-Gruppen für Primzahlen p (folgt aus Satz 1.4.17);
- alle Gruppen der Ordnung pq für Primzahlen p und q.
  Beweis: Falls $p = q$ so ist G nach Satz 1.4.17 (b) abelsch. Falls $p < q$, so ist $N_q(G) = 1 \bmod q$ und $N_q(G) \mid p$, also $N_q(G) = 1$. Mit der einzigen q–Sylow–Gruppe Q hat man dann eine Kompositionsreihe $\{e\} \trianglelefteq Q \trianglelefteq G$ mit zyklischen Faktoren. □
- Die kleinste nicht-auflösbare Gruppe ist A_5.

Definition 1.6.8 *Der **Kommutator** von g und h ist das Element $[g,h] := g^{-1}h^{-1}gh$. Genau dann kommutieren die Elemente g und h von G miteinander, wenn $[g,h] = e$.*

*Die **Kommutatorgruppe** von G ist die Untergruppe $G' = [G,G] := \langle [g,h] \mid g,h \in G \rangle$. Definiere die n-ten Kommutatorgruppen durch $G^{(0)} := G$ und induktiv $G^{(n+1)} := (G^{(n)})'$. Schreibweise: $G'' = G^{(2)}$ etc. Alle $G^{(n)}$ sind charakteristische Untergruppen von G.*

*Die Reihe $\ldots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)}$ heißt **Kommutatorreihe** von G.*

Lemma 1.6.9 *Für $N \trianglelefteq G$ ist G/N genau dann abelsch, wenn $G' \leqslant N$.*

BEWEIS: G/N abelsch $\iff$ $[gN, hN] = [g,h]N = N$ für alle $g, h \in G$ $\iff$ $[g,h] \in N$ für alle $g, h \in G$ $\iff$ $G' \leqslant N$. □

Satz 1.6.10 *Äquivalent sind:*

(a) *G ist auflösbar.*

(b) *Es gibt eine Subnormalreihe $\{e\} = N_k \trianglelefteq \ldots \trianglelefteq N_0 = G$ mit abelschen Faktoren N_i/N_{i+1}.*

(c) *Es gibt ein l mit $G^{(l)} = \{e\}$.*

BEWEIS: (a)⇒(b): die Kompositionsreihe, gemäß der die Gruppe auflösbar ist (und nach dem Satz von Jordan–Hölder dann jede Kompositionsreihe).

(c)⇒(b): die Kommutatorreihe!

(b)⇒(a): Verfeinere die gegebene Subnormalreihe zu einer Kompositionsreihe; die Faktoren bleiben (als Untergruppen und Quotienten abelscher Gruppen) abelsch.

(b)⇒(c): Per Induktion zeigt man $G^{(i)} \leqslant N_i$. Dies ist klar für $i = 0$. Im Schritt $i \to i+1$ hat man $G^{(i+1)} = (G^{(i)})' \leqslant N_i' \leqslant N_{i+1}$ mit Lemma 1.6.9, da N_i/N_{i+1} abelsch ist. □

Definition 1.6.11 *Eine beliebige Gruppe G heißt auflösbar, falls $G^{(l)} = \{e\}$ für ein $l \in \mathbb{N}$. Das kleinste solche l heißt die **Auflösbarkeitsstufe** von G.*

Satz 1.6.12 **(a)** *Untergruppen und homomorphe Bilder auflösbarer Gruppen sind auflösbar.*

(b) *Sind $N \trianglelefteq G$ und G/N auflösbar, so auch G.*

BEWEIS: (a) Ist $U \leqslant G$, so $U^{(n)} \leqslant G^{(n)}$, und ist $N \trianglelefteq G$, so $(G/N)^{(n)} = G^{(n)}N/N$.

(b) Sei $N^{(k)} = \{e\}$ und $(G/N)^{(l)} = G^{(l)}N/N = N$, also $G^{(l)} \leqslant N$. Dann ist $G^{(l+k)} = (G^{(l)})^{(k)} \leqslant N^{(k)} = \{e\}$. □

Satz 1.6.13 *Alle Gruppen der Ordnung pqr für Primzahlen $p > q > r$ sind auflösbar.*

BEWEIS: 1. Fall: G hat eine normale Sylow–Gruppe N. Dann ist N auflösbar, da zyklisch, und G/N auflösbar nach Beispiel 1.6.7 (d), also ist G auflösbar nach Satz 1.6.12.

2. Fall: G hat keine normale Sylow–Gruppe. Dann gilt

$$\begin{aligned} 1 + p \leqslant N_p(G) = 1 + kp \mid qr \quad &\Rightarrow \quad N_p = qr \\ 1 + q \leqslant N_q(G) = 1 + lq \mid pr \quad &\Rightarrow \quad N_p \geqslant p \\ 1 + r \leqslant N_r(G) = 1 + mr \mid pq \quad &\Rightarrow \quad N_p \geqslant q \end{aligned}$$

Es folgt daraus

$$\begin{aligned} pqr = |G| &\geqslant 1 + |\{g \in G \mid \mathrm{ord}(g) = p\}| + |\{g \in G \mid \mathrm{ord}(g) = q\}| + |\{g \in G \mid \mathrm{ord}(g) = r\}| \\ &= 1 + N_p(G)(p-1) + N_q(G)(q-1) + N_r(G)(r-1) \\ &\geqslant 1 + qr(p-1) + p(q-1) + q(r-1) \;=\; 1 + pqr + \underbrace{pq - p - q}_{>0} \end{aligned}$$

Widerspruch! □

Bemerkung 1.6.14 **(a)** Satz von Burnside: alle Gruppen der Ordnung $p^a q^b$ für Primzahlen p und q sind auflösbar.

(b) Satz von Feit und Thompson (sehr schwer): alle Gruppen ungerader Ordnung sind auflösbar.

1.6.15 Endliche einfache Gruppen sind:

- Die einfachen abelschen Gruppen $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p.
- Die alternierenden Gruppen A_n für $n \geqslant 5$.
- Die Gruppen $\mathrm{PSL}(n, F) := \mathrm{SL}(n, F)/Z(\mathrm{PSL}(n, F))$ für endliche Körper F und $n \geqslant 2$, nicht jedoch $\mathrm{PSL}(2, \mathbb{F}_2)$.
- Weitere (endlich viele) unendliche Familien endlicher Gruppen.
- 26 sporadische endliche Gruppen: kleinste ist die Mathieu–Gruppe M_{11} der Ordnung 7 920, größte ist das „Monster“ mit ungefähr $8 \cdot 10^{53}$ Elementen.
- Beispiel einer unendlichen einfachen Gruppe:

$$A_\infty := \big\{\alpha : \mathbb{N} \to \mathbb{N} \mid T(\alpha) := \{i \mid \alpha(i) \neq i\} \text{ endlich}, \alpha\restriction_{T(\alpha)} \in A_{|T(\alpha)|}\big\}.$$

1.7 Symmetrische Gruppen

Notation: In diesem Abschnitt soll streng unterschieden werden zwischen der Permutationsgruppe $\mathrm{Sym}(n) = \big\{\alpha : \{1, \ldots, n\} \to \{1, \ldots, n\} \mid \alpha \text{ bijektiv}\big\}$, auf $\{1, \ldots, n\}$ und ihrer zugrundeliegenden abstrakten Gruppe S_n.

Bemerkung 1.7.1 Für $n \neq 6$ gibt es bis auf Äquivalenz nur eine treue Operation von S_n auf $\{1, \ldots, n\}$, d.h. es gibt bis auf Umbenennung von $\{1, \ldots, n\}$ nur eine Möglichkeit, aus S_n eine Permutationsgruppe zu machen. Für $n = 6$ gibt es zwei Möglichkeiten (ohne Beweis, aber vergleiche Bemerkung 1.7.11 (a) und Übung auf Blatt 8).

Satz 1.7.2 *Das Signum*

$$\mathrm{sgn}(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

ist ein Epimorphismus $\mathrm{Sym}(n) \to \big(\{+1, -1\}, \cdot\big) \cong Z_2$.

Beweis: Einerseits ist $|\mathrm{sgn}(\sigma)| = 1$, da jeder Faktor im Nenner bis auf Vorzeichen auch im Zähler auftaucht, und umgekehrt. Ferner ist sgn wegen

$$\mathrm{sgn}(\tau \circ \sigma) = \prod_{i<j} \Big(\frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\sigma(j) - \sigma(i)} \cdot \frac{\sigma(j) - \sigma(i)}{j - i}\Big) = \mathrm{sgn}(\tau) \cdot \mathrm{sgn}(\sigma)$$

ein Homomorphismus. □

Der Kern des Signums ist die **alternierende Gruppe**, die $\mathrm{Alt}(n)$ als Permutationsgruppe und A_n als abstrakte Gruppe geschrieben werden soll. Elemente von A_n heißen **gerade Permutationen**, alle anderen **ungerade**.

1.7.3 **[Zykelzerlegung in** $\mathrm{Sym}(n)$**]** Ein k**-Zykel** ist eine Permutation $\zeta \in \mathrm{Sym}(n)$ mit den Eigenschaften:

— $\zeta^k(i_0) = i_0 \neq \zeta^j(i_0)$ für ein $i_0 \in \{1, \ldots, n\}$ und alle $1 \leqslant j < k$;

— $\zeta(j) = j$ für alle $j \notin \{i_0, \zeta(i_0), \ldots, \zeta^{k-1}(i_0)\}$.

Ein k-Zykel entspricht also einer Bahn der Größe k von der induzierten Operation von $\langle\zeta\rangle$ auf $\{1, \ldots, n\}$. Man schreibt solch einen k-Zykel $(i_0, \zeta(i_0), \ldots, \zeta^{k-1}(i_0))$. 2-Zykel heißen auch **Transpositionen**. Offensichtlich ist die Ordnung eines k-Zykels gerade k. Ferner sieht man $(i_0, \zeta(i_0), \ldots, \zeta^{k-1}(i_0))^{-1} = (\zeta^{k-1}(i_0), \ldots, \zeta(i_0), i_0)$.

Jede Permutation lässt sich offenbar als Produkt von Zykeln schreiben, und zwar so, dass jedes Element aus $\{1, \ldots, n\}$ in genau einem Zykel vorkommt. Diese Darstellung ist eindeutig bis auf Reihenfolge der Zykel und zyklische Vertauschung innerhalb der Zykel, und heißt **Zykelzerlegung** der Permutation.

Beispiel: $\binom{1234567}{3527164} = (1,3,2,5)(6)(4,7) = (6)(2,5,1,3)(7,4)$

Der **Typ einer Permutation** gibt die Anzahl der k-Zykel für jedes k in der Zykelzerlegung an, im Beispiel kann er z.B. als $(1,1,0,1)$ angegeben werden oder durch (....)(..)(.). Die Ordnung einer Permutation ist das kleinste gemeinsame Vielfache aller Längen von Zyklen in der Zykelzerlegung.

Lemma 1.7.4 *Zwei Permutationen sind genau dann in* $\mathrm{Sym}(n)$ *konjugiert, wenn sie den gleichen Typ haben.*

In $\mathrm{Alt}(n)$ ist dies im allgemeinen falsch!

Beweis: $\tau \circ \sigma \circ \tau^{-1}$ ist die „gleiche“ Permutation wie σ nach Umbenennen der Elemente $1, \ldots, n$ in $\tau(1), \ldots, \tau(n)$. Es ist also $\big(i, \sigma(i), \ldots, \sigma^{k-1}(i)\big)$ genau dann ein k-Zykel von σ, wenn $\big(\tau(i), \sigma(\tau(i)), \ldots, \sigma^{k-1}(\tau(i))\big)$ ein k-Zykel von $\tau \circ \sigma \circ \tau^{-1}$ ist. □

Lemma 1.7.5 **(a)** $\mathrm{Sym}(n)$ *wird von den Transpositionen erzeugt.*

(b) $\mathrm{Alt}(n)$ *wird von den* 3*-Zykeln erzeugt.*

Beweis: (a) Es reicht zu zeigen,d ass jeder Zykel von Transpositionen erzeugt wird, und es gilt $\big(i, \sigma(i), \ldots, \sigma^{k-1}(i)\big) = \big(i, \sigma^{k-1}(i)\big) \circ \cdots \circ \big(i, \sigma^2(i)\big) \circ \big(i, \sigma(i)\big)$.

(b) Per Definition ist klar, dass das Signum einer Transposition -1 ist. Also besteht $\mathrm{Alt}(n)$ nach Definition und (a) aus den Permutationen, die sich als Produkt geradzahlig vieler Transpositionen schreiben lassen. Wegen $(ac) \circ (ab) = (abc)$ und $(ab) \circ (cd) = (adc) \circ (abc)$ sind dies auch produkte von 3-Zykeln. □

Satz 1.7.6 *Für* $n \geqslant 2$ *gibt es genau einen Epimorphismus* $S_n \to Z_2$*. Insbesondere ist das Signum unabhängig von der Realisierung von* S_n *als Permutationsgruppe* $\mathrm{Sym}(n)$*.*

Beweis: Realisiere S_n als Permutationsgruppe $\mathrm{Sym}(n)$, und sei $\alpha : S_n \to \{\pm 1, \cdot\}$ ein Homomorphismus. Wegen $\alpha(\tau^{-1} \circ \sigma \circ \tau) = \alpha(\tau^{-1}) \circ \alpha(\sigma) \circ \alpha(\tau)) = \alpha(\sigma)$ (Z_2 ist abelsch!), haben alle Transpositionen gleiches Bild. Falls dies 1 ist, so ist α trivial wegen Lemma 1.7.5 (a). Falls es -1 ist, so ist $\alpha = \mathrm{sgn}$. □

1.7.7 Die S_3 hat die Normalteiler $\{e\}, A_3, S_3$ und keine weiteren. Die einzige Kompositionsreihe ist daher $\{e\} \trianglelefteqslant A_3 \trianglelefteqslant S_3$ mit Kompositionsfaktoren Z_2 und Z_3. Die S_3 ist daher auflösbar.

Die S_4 hat fünf Konjugationsklassen: Die Identität bildet eine einelementige Konjugationsklasse, die weiteren bestehen aus den sechs Transpositionen, den acht 3-Zykeln, den sechs 4-Zykeln, und den drei Doppeltranspositionen vom Typ (..)(..) bzw. $(0,2)$.

Die **Kleinsche Vierergruppe** V besteht aus der Identität und den Doppeltransformationen und ist ein Normalteiler, da Untergruppe, die aus vollständigen Konjugationsklassen besteht. Man überprüft leicht anhand der Zahlen, dass es keine weiteren Normalteiler außer $\{e\}, V, A_4, S_4$ geben kann. Es gibt drei Kompositionsreihen, die alle die Form $\{e\} \trianglelefteq Z_2 \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4$ mit Faktoren Z_2, Z_2, Z_3, Z_2 haben. Also ist S_4 auflösbar.

Satz 1.7.8 *Für $n \geqslant 5$ ist A_n nicht auflösbar und sogar einfach.*

Beweis: Realisiere A_n als Alt(n) und wähle einen 5-Zykel $(edcba)$. Dann ist $[(cba), (edcba)] = (abc) \circ (abcde) \circ (cba) \circ (edcba) = (abd)$. Also sind alle 3-Zykel in A_n'. Wegen Lemma 1.7.5 (b) gilt daher $A_n = A_n'$, mithin ist A_n nicht auflösbar.

(b) Spezialfall $n = 5$ (der allgemeine Fall geht ähnlich elementar, siehe z.B. bei Robinson):

Zwei 3-Zykel $(abc), (a'b'c')$ sind in Sym(5) durch eine Permutation π konjugiert. Falls $\pi \notin$ Alt(5), so wähle e, f die beiden restlichen Elemente zu a', b', c'. Es gilt dann

$$(f, e) \circ \underbrace{\pi^{-1} \circ (abc) \circ \pi}_{=(a'b'c')} \circ (ef) = (a'b'c'),$$

wegen $(f, e) \circ \pi^{-1} = (\pi \circ (e, f))^{-1}$ sind je zwei 3-Zykel also auch in Alt(n) konjugiert.

Wegen $(abe) \circ (ab)(cd) \circ (eba) = (be)(cd)$ kann man durch Konjugation in Alt(5) jede Doppeltransposition sukzessive in jede andere überführen. Und mit $(abc) \circ (abcde) \circ (cba) = (adebc)$ kann man sich davon überzeugen, dass eine Konjugationsklasse von 5-Zykeln mindestens acht Elemente enthält.

Alt(n) besteht aus der Identität, 20 3-Zykeln, 15 Doppeltranspositionen und 24 5-Zykeln. Ein echter, nicht trivialer Normalteiler von Alt(5) kann keinen 3-Zykel enthalten, entweder keine oder alle Doppeltranspositionen, und entweder keine, 8, 12 oder 24 5-Zykel. Keine Kombination davon ergibt einen Teiler von 60. □

Folgerung 1.7.9 *Für $n \geqslant 5$ sind $\{e\}, A_n, S_n$ die einzigen Normalteiler von S_n.*

Beweis: Sei $N \trianglelefteq S_n$. Dann ist $N \cap A_n \trianglelefteq A_n$.
1. Fall: $N \cap A_n = A_n$. Dann ist entweder $N = A_n$ oder $N = S_n$, da A_n bereits Index 2 in S_n hat.
2. Fall: $N \cap A_n = \{e\}$. Dann ist entweder $N = \{e\}$, oder $|N| = 2$. Da aber kein Element der Ordnung 2 eine eigene Konjugationsklasse bildet, kann dieser Fall nicht auftreten. □

Folgerung 1.7.10 *Die Drehgruppe des regelmäßigen Ikosaeders/Dodekaeders ist A_5.*

Beweis: Das Ikosaeder lässt sich als Schnitt von fünf regulären Tetraedern schreiben, die Drehgruppe operiert treu darauf, also ist sie Untergruppe der S_5. Da sie 60 Elemente hat (nachzählen!), hat sie Index 2 in der S_n, ist also ein Normalteiler, also A_n. □

Übersicht über die Polyedergruppen

	Drehgruppe	Symmetriegruppe
reguläres Tetraeder	A_4	S_4
Würfel/reguläres Oktaeder	S_4	$S_4 \times Z_2$
reguläres Ikosaeder/reguläres Dodekaeder	A_5	$A_5 \times Z_2 \quad (\ncong S_5)$

Bemerkung 1.7.11 **(a)** Ist τ eine ungerade Permutation der Ordnung 2, z.B. eine Transposition, so gilt $S_n = A_n \rtimes \langle\tau\rangle$.

(b) Die Anzahl der Transpositionen in $\mathrm{Sym}(n)$ ist $\binom{n}{2}$. Die Anzahl der k-fachen Transpositionen ist $\frac{1}{k!}\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2(k-1)}{2}$. Gleichheit für $k > 1$ gibt es nur für $n = 6$ und $k = 3$. In allen S_n bis auf $n = 6$ sind die Transpositionen also identifizierbar!

(c) $\mathrm{Aut}(S_1) = \mathrm{Aut}(S_2) = \{e\}$. Für $n \geqslant 3$ und $n \neq 6$ ist $\mathrm{Aut}(S_n) \cong S_n$ (sogenannte **vollständige Gruppe**). Für $n \geqslant 4$ und $n \neq 6$ gilt auch $\mathrm{Aut}(A_n) \cong S_n$.

2 Ringe

2.1 Definitionen und Beispiele

Definition 2.1.1 **(a)** *Ein **Ring** $R = (R, +, \cdot, -, 0)$ besteht aus*

- *einer abelschen Gruppe $(R, +, -, 0)$ und*
- *einer Halbgruppe $(R, \cdot)$,*

so dass die Distributivgesetzte $r \cdot (s + t) = (r \cdot s) + (r \cdot t)$ und $(s + t) \cdot r = (s \cdot r) + (t \cdot r)$ für alle $r, s, t \in R$ gelten (d.h. die Multiplikation ist bilinear).

***Notationen:** Der Multiplikationspunkt wird meist weggelassen, Klammern werden durch die übliche Regel „Multiplikation vor Addition“ eingespart. Wegen Lemma 1.1.2 reicht es, einen Ring als $(R, +, \cdot)$ zu beschreiben, d.h. nur durch Angabe der Addition und Multiplikation.*

(b) *Ein Ring heißt **kommutativ**, falls die Multiplikation kommutativ ist, d.h. falls $rs = sr$ für alle $r, s \in R$ gilt.*

(c) *Ein **Ring mit Eins** oder **unitärer Ring** ist eine Struktur $(R+, \cdot, -, 0, 1)$, wobei*

- *$(R+, \cdot, -, 0)$ ein Ring ist und*
- *1 neutrales Element der Multiplikation, d.h. $1 \cdot r = r \cdot 1 = r$ für alle $r \in R$ gilt.*

Bemerkung 2.1.2 Wegen $r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0$ gilt $r \cdot 0 = 0$ für alle $r \in R$. Ebenso $0 \cdot r = 0$ für alle $r \in R$.

Beispiel 2.1.3 • $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins.

- Wenn $0 = 1$ in einem Ring mit Eins gilt, so ist $0 = 0 \cdot r = 1 \cdot r = r$ für jedes $r \in R$, also ist $R = \{0\}$ der sogenannte **triviale Ring**.
- Jeder Körper ist ein Ring.
- Die $(n \times n)$-Matrizen über einem Körper K bilden unter der Matrizenaddition und –multiplikation einen Ring mit Eins $\mathrm{Mat}_{n\times n}(K)$, der für $n \geqslant 2$ nicht kommutativ ist.
- Ist R ein Ring, so bilden die Polynome mit Koeffizienten in R den **Polynomring über** R, $R[X]$ (kommutativ/unitär, falls R kommutativ bzw. unitär).
- Ist R ein Ring und X eine Menge, so ist die Menge der Abbildungen von X nach R mit komponentenweiser Addition und Multiplikation ein Ring ${}^X R$ (kommutativ/unitär, falls R kommutativ bzw. unitär).
- Ist G eine kommutative Gruppe oder ein Vektorraum, so ist der **Endomorphismenring** $(\mathrm{End}(G), \text{komponentenweise Addition}, \circ)$ ein unitärer Ring (i.a. nicht kommutativ).
- Die Folgen ganzer Zahlen mit endlichem Träger und komponentenweiser Addition und Multiplikation bilden einen Ring ohne Eins.

Definition 2.1.4 **(a)** *Eine Abbildung $\varphi : R \to S$ zwischen zwei Ringen heißt* ***Ringhomomorphismus****, falls $\varphi(r + r') = \varphi(r) + \varphi(r')$, $\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')$, $\varphi(-r) = -\varphi(r)$ und $\varphi(0) = 0$ für alle $r, r' \in R$ gilt.*
(Wegen Lemma 1.1.8 reicht es, die beiden ersten Bedinungen zu überprüfen.)

(b) *Eine Abbildung $\varphi : R \to S$ zwischen zwei Ringen mit Eins heißt* ***unitärer Ringhomomorphismus*** *oder* ***Homomorphismus von Ringen mit Eins****, falls zusätzlich $\varphi(1) = 1$ gilt.*
Achtung: nicht jeder Ringhomomorphismus zwischen Ringen mit Eins ist unitär!

Definition 2.1.5 *Ein* ***Unterring*** *bzw. ein* ***unitärer Unterring*** *eines (unitären) Ringes ist eine Teilmenge, die bezüglich der eingeschränkten Operationen wieder ein Ring ist (also eine bezüglich Multiplikation abgeschlossene Untergruppe) und im Falle eines unitären Unterrings die Eins enthält.*

Schreibweise für Unterringe ist üblicherweise nur das Teilmengenzeichen $R \subseteq S$.

Ähnlich wir bei Gruppen überlegt man sich leicht, dass die (unitären) Unterringe gerade die Bilder von (unitären) Ringhomomorphismen sind.

Definition 2.1.6 *Eine additive Untergruppe I eines Ringes R heißt*

- ***Linksideal****, falls $R \cdot I \subseteq I$, d.h. falls $r \cdot i \in I$ für alle $r \in R$ und $i \in I$;*
- ***Rechtssideal****, falls $I \cdot R \subseteq I$;*
- ***(beidseitiges) Ideal****, falls I Rechts– und Linksideal ist.*

Schreibweise: $I \trianglelefteq R$ für „I ist Ideal von R“.

Lemma 2.1.7 *Ideale sind genau die Kerne von Ringhomomorphismen.*

Beweis: (a) Ist $\varphi : R \to S$ ein Ringhomomorphismus, so auch ein Gruppenhomomorphismus, also ist $I := \mathrm{Kern}(\varphi) = \varphi^{-1}(0)$ eine additive Untergruppe. Ist $r \in R$ und $i \in I$, so $\varphi(ri) = \varphi(r)\varphi(i) = \varphi(r)0 = 0$, und ebenso $\varphi(ir) = 0$, also ist I ein Ideal.

(b) Ist $I \trianglelefteq R$, dann definiert man durch $(r + I) \cdot (r' + I) = rr' + I$ eine Multiplikation, welche die Gruppe R/I zu einem Ring macht: Wohldefiniertheit der Multiplikation: ist $r + I = s + I$ und $r' + I = s' + I$, so $rr' - ss' = (r - s)r' + s(r' - s') \in Ir' + sI \subseteq I$, also $rr' + I = ss' + I$. Assoziativität und Distributivgesetze werden von R vererbt.

Die natürliche Surjektion $R \to R/I$ wird durch diese Definition zu einem Ringhomomorphismus mit Kern I. □

Bemerkung: Falls R ein Ring mit Eins ist, so auch R/I mit Eins $1 + I$.

Bemerkung 2.1.8 **(a)** Sei R ein Ring mit Eins und I ein Ideal. Dann gilt $I \neq R \iff 1 \notin I$ (denn $1 \in I \Rightarrow r = r \cdot 1 \in I$ für alle $r \in R$; die Umkehrung ist klar).

(b) Ideale sind Unterringe, aber im unitären Fall keine unitären Unterringe (außer R selbst).

Satz 2.1.9 (Homomorphiesatz) *Sei $\varphi : R \to S$ ein Ringhomomorphismus. Dann zerlegt sich φ in eine Folge von Homorphismen*

$$\begin{array}{ccccccc} R & \xrightarrow{\text{surj.}} & R/\mathrm{Kern}(\varphi) & \xrightarrow{\cong} & \mathrm{Bild}(\varphi) & \xrightarrow{\text{inj.}} & S \\ r & \mapsto & r + \mathrm{Kern}(\varphi) & \mapsto & \varphi(r) & \mapsto & \varphi(r) \end{array}$$

Sind R, S und φ unitär, so auch alle Zwischenhomomorphismen.

BEWEIS: Wie im Fall der Gruppen. □

Beispiel 2.1.10

- $\{0\}$ und R sind stets Ideale. Ein Ring heißt **einfach**, falls er keine weiteren Ideale besitzt.
- $m\mathbb{Z}$ ist ein Ideal in $\mathbb{Z}$, also ist $\mathbb{Z}/m\mathbb{Z} \cong Z_m$ ein Ring.
- In $\mathbb{R}[X]$ ist für jedes Polynom $f \in \mathbb{R}[X]$ die Menge $f \cdot \mathbb{R}[X] = \{fg \mid g \in \mathbb{R}[X]\} = \{h \in \mathbb{R}[X] \mid f \text{ teilt } h\}$ ein Ideal.
- Allgemeiner: in jedem kommutativen Ring R ist für $r \in R$ die Menge $r \cdot R$ ein Ideal, auch (r) geschrieben. Solche Ideale heißen **Hauptideale**.
- Sei V ein endlich-dimensionaler Vektorraum, $R = \mathrm{End}(V)$ und W ein Unterraum von V. Dann ist $\{f \in R \mid W \subseteq \mathrm{Kern}(f)\}$ ein Linksideal und $\{f \in R \mid \mathrm{Bild}(f) \subseteq W\}$ ein Rechtsideal. Alle Links– bzw. Rechtsideale sind von dieser Form, und $\mathrm{End}(V)$ ist ein einfacher Ring.
- Sind Ringe R_i für $i \in I$ gegeben, so werden durch komponentenweise Multiplikation die direkte Summe und das direkte Produkt der zugrundeliegenden Gruppen zu Ringen. $\bigoplus_{i\in\mathbb{N}} \mathbb{Z}$ (das war das Beispiel eines Ringes ohne Eins in Beispiel 2.1.3!) ist ein Ideal in $\prod_{i\in\mathbb{N}} \mathbb{Z} = {}^{\mathbb{N}}\mathbb{Z}$, aber kein Hauptideal.

Bemerkung 2.1.11 Seien R, S (unitäre) Ringe. Dann ist $R \times S$ mit komponenterweiser Addition und Multiplikation wieder ein (unitärer) Ring (mit Eins $(1, 1)$). Die Einbettungen $R \to R \times S$, $r \mapsto (r, 0)$ und $S \to R \times S$, $s \mapsto (0, s)$ sind Ringhomomorphismen, aber im unitären Fall keine unitären!

2.2 Rechnen mit Idealen

Ab sofort ist mit „Ring“ kommutativer Ring mit Eins gemeint, falls nichts anderes angegeben ist.

Bemerkung 2.2.1 Es gilt $(-1) \cdot r = -r$ und $-(rs) = (-r)s = r(-s)$ für alle $r, s \in R$ (denn z.B. $(-r)s + rs = (-r + r)s = 0 \cdot s = 0$).

Definition und Lemma 2.2.2 *Seien I_1, I_2 Ideale im Ring R. Dann sind auch Ideale:*

$$I_1 + I_2 := \big\{r_1 + r_2 \mid r_i \in I_i\big\} \quad \textit{und} \quad I_1 \cap I_2 \quad \textit{und} \quad I_1 \cdot I_2 := \Big\{ \sum_{j=1}^{n} r_{1j} r_{2j} \mid n \in \mathbb{N}, r_{ij} \in I_i\Big\}.$$

$I_1 \cap I_2$ ist das größte in I_1 und I_2 enthaltene Ideal, $I_1 + I_2$ das kleinste I_1 und I_2 enthaltende Ideal. Es gilt

$$I_1 \cdot I_2 \ \subseteq\ I_1 \cap I_2 \ \subseteq\ I_i \ \subseteq\ I_1 + I_2.$$

Achtung: Die Schreibweise $I_1 \cdot I_2$ wiederspricht der allgemeinen Konvention aus dem Kapitel 1, wonach es für die Menge der Produkte stehen müsste. Diese ist jedoch kein Ideal, weshalb sich hier die kürzere Schreibweise für das wichtigere Objekt, nämlich das erzeugte Ideal, eingebürgert hat. (Beachte, dass dies z.B. mit der Forderung $R \cdot I \subseteq I$ für ein Linksideal, womit zunächst die Menge der Produkte gemeint war, veträglich ist!)

BEWEIS: Nachrechnen, dass alles Ideale sind!

$I_1 \cdot I_2 \subseteq I_1 \cap I_2$ gilt, da sogar $R \cdot I_2 \subseteq I_2$ und $I_1 \cdot R \subseteq I_1$. Die anderen Inklusionen und Behauptungen sind dann klar. □

Lemma 2.2.3 *Es gelten die folgenden Rechenregeln für Ideale I_i eines Ringes R:*

- *$+$ ist kommutativ und assoziativ auf Idealen und idempotent, d.h. $I_i + I_i = I_i$. Das Nullideal $\{0\}$ ist neutrales Element.*
- *Multiplikation $\cdot$ ist kommutativ und assoziativ, R ist neutrales Element.*
- *Es gilt das Distributivgesetz $I_1 \cdot (I_2 + I_3) = I_1 \cdot I_2 + I_1 \cdot I_3$.*

Beweis: Alles ist einfach oder sogar klar von den Definitionen her, außer dem Distributivgesetz. Sei also $r \in I_1 \cdot (I_2 + I_3)$, $r = \sum_{j=1}^{k} r_{1j}(r_{2j} + r_{3j}) = \sum_{j=1}^{k} r_{1j}r_{2j} + \sum_{j=1}^{k} r_{1j}r_{3j} \in I_1 \cdot I_2 + I_1 \cdot I_3$.

Umgekehrt ist $I_2 \subseteq I_2 + I_3$, also $I_1 \cdot I_2 \subseteq I_1 \cdot (I_2 + I_3)$; ebenso $I_1 \cdot I_3 \subseteq I_1 \cdot (I_2 + I_3)$. Also ist auch $I_1 \cdot I_2 + I_1 \cdot I_3 \subseteq I_1 \cdot (I_2 + I_3)$. □

Definition 2.2.4 *Sei $I \trianglelefteq R$. Man schreibt $r_1 \equiv r_2 \pmod{I}$ für $r_1 - r_2 \in I$.*

Zur Erinnerung: äquivalent bedeutet dies $r_1 + I = r_2 + I$ oder: r_1, r_2 liegen in derselben Nebenklasse von I, oder: $\varphi(r_1) = \varphi(r_2)$ für den natürliche Homomorphismus $\varphi : R \to R/I$.

In $\mathbb{Z}$ gilt $n_1 \equiv n_2 \pmod{m}$ genau dann, wenn $n_1 \equiv n_2 \pmod{m\mathbb{Z}}$.

Satz 2.2.5 (Chinesischer Restsatz) *Sei R ein kommutativer Ring mit Eins, $I_1, \ldots, I_n$ Ideale von R mit $I_i + I_j = R$ für $i \neq j$. Dann ist $\varphi : R \to R/I_1 \times \cdots \times R/I_n$, $r \mapsto (r + I_1, \ldots, r + I_n)$ ein unitärer Ringepimorphismus mit Kern $I_1 \cap \cdots \cap I_n = I_1 \cdot \ldots \cdot I_n$.*

Insbesondere existiert zu gegebenen $r_1, \ldots, r_n \in R$ ein $r \in R$ mit $r \equiv r_j \pmod{I_j}$ für $j = 1, \ldots, n$.

Beweis: Alles ist klar bis auf die Surjektivität und die Beschreibung des Kerns. Zeige zunächst $I_1 \cap \cdots \cap I_n = I_1 \cdot \ldots \cdot I_n$ per Induktion über n.

Für $n = 1$ ist dies klar; für $n = 2$ gilt

$$I_1 \cap I_2 = R(I_1 \cap I_2) = (I_1 + I_2)(I_1 \cap I_2) = I_1(I_1 \cap I_2) + I_2(I_1 \cap I_2) \subseteq I_1I_2 + I_1I_2 = I_1I_2$$

Die andere Inklusion $I_1I_2 \subseteq I_1 \cap I_2$ gilt allgemein.

Wegen

$$R = (I_1 + I_n)(I_2 + I_n) \cdot \ldots \cdot (I_{n-1} + I_n) = I_1I_2 \cdot \ldots \cdot I_{n-1} + (\ldots)I_n \subseteq I_1I_2 \cdot \ldots \cdot I_{n-1} + I_n$$

gilt (*) $I_1I_2 \cdot \ldots \cdot I_{n-1} + I_n = R$. Damit gelingt der Induktionsschritt $n - 1 \to n$, denn

$$I_1 \cdot \ldots \cdot I_n \overset{IV}{=} (I_1 \cap \cdots \cap I_{n-1}) \cdot I_n \overset{\text{Fall } n=2}{=} I_1 \cap \cdots \cap I_{n-1} \cap I_n.$$

Die Surjektivität ist ebenfalls klar für $n = 1$. Für $n = 2$ gibt es $a_i \in I_i$ mit $a_1 + a_2 = 1$, da $I_1 + I_2 = R$. Setze $r := r_1a_2 + r_2a_1$. Dann gilt $r - r_1 = r_1(a_2 - 1) + r_2a_1 = r_1(-a_1) + r_2a_1 = (r_2 - r_1)a_1 \in I_1$. Ebenso $r - r_2 \in I_2$.

Per Induktion kann man wieder von $n - 1$ auf n schließen: nach Induktionsvoraussetzung gibt es ein $r' \in R$ mit $r' \equiv r_j \pmod{I_j}$ für $j = 1, \ldots, n - 1$. Nach dem Fall $n = 2$ und wegen (*) gibt es ein $r \in R$ mit $r \equiv r_n \pmod{I_n}$ und $r \equiv r' \pmod{I_1 \cap \cdots \cap I_{n-1}}$. Dann gilt $r - r_j = (r - r') + (r' - r_j) \in (I_1 \cap \cdots \cap I_{n-1}) + I_j \subseteq I_j + I_j = I_j$. □

Beispiel 2.2.6 **(a)** Sei $R = \mathbb{Z}$ und $m_1, \ldots, m_n$ paarweise teilerfremde Zahlen. Setze $I_j = m_j\mathbb{Z}$. Dann gilt $I_i + I_j = m_i\mathbb{Z} + m_j\mathbb{Z} = \mathbb{Z}$ nach Fakt 1.2.7 für $i \neq j$. Also ist

$$m_1\mathbb{Z} \cap \cdots \cap m_n\mathbb{Z} \;=\; m_1\mathbb{Z} \cdot \ldots \cdot m_n\mathbb{Z} \;=\; (m_1 \ldots m_n)\mathbb{Z}$$

und $\mathbb{Z}/(m_1 \ldots m_n)\mathbb{Z} \;\cong\; \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$ als Ringe mit Eins!
Zu Zahlen $d_1, \ldots, d_n \in \mathbb{Z}$ gibt es also stets ein $d \in \mathbb{Z}$ mit $d \equiv d_i \pmod{m_i}$ für $i = 1, \ldots, n$.

(b) Sei $R = K[X]$ der Polynomring über dem Körper K, $a_1, \ldots, a_n \in K$ paarweise verschiedene Zahlen. Setze $I_j = (X - a_j) \cdot K[X]$. Wegen $1 = \frac{1}{a_j - a_i}((X - a_i) - (X - a_j)) \in I_i + I_j$ gilt $I_i + I_j = K[X]$ für $i \neq j$.
Zu gegebenen $b_1, \ldots, b_n \in K$ existiert also ein Polynom $f(X) \in K[X]$ mit $f(X) \equiv b_i \pmod{(X - a_i) \cdot K[X]}$, d.h. $(X - a_i)$ teilt $f(X) - b_i$, das also von der Form $g(X)(X - a_i)$ ist. Es gilt also $f(X) = g(X)(X - a_i) + b_i$ oder $f(a_i) = b_i$. Dies ist der Interpolationssatz für Polynome!

2.3 Integritätsbereiche und Körper

Definition 2.3.1 *Sei R ein kommutativer Ring mit Eins, $a, b \in R$.*

(a) *a **teilt** b, in Zeichen $a \mid b$, falls es ein $c \in R$ gibt mit $ac = b$ (d.h. $b \in aR$ bzw. $bR \subseteq aR$).*

(b) *a ist **Nullteiler**, falls $a \neq 0$ und es ein $c \neq 0$ in R gibt mit $ac = 0$. (Bemerkung: jedes Element in R teilt 0!) Ringe ohne Nullteiler heißen **nullteilerfrei**.*

(c) *a ist **Einheit** von R, falls a Teiler der Eins ist, d.h. falls a ein multiplikatives Inverses a^{-1} besitzt (das dann eindeutig bestimmt ist). $R^* := \{a \in R \mid a \text{ Einheit}\}$.*

Bemerkung 2.3.2 $(R^*, \cdot)$ ist eine Gruppe (Beweis wie in Lemma 1.2.8).

Beispiel 2.3.3 • Teilen in $\mathbb{Z}$ und in Polynomringen $K[X]$ ist der gewohnte Begriff. In Körpern teilt jedes Element $\neq 0$ jedes andere.
• Nullteiler existieren z.B. in $\mathbb{Z}/6\mathbb{Z}$, da $(2 + 6\mathbb{Z})(3 + 6\mathbb{Z}) = 0 + 6\mathbb{Z}$.
In Matrizenringen gibt es sogar sogenannte nilpotente Elemente, z.B. $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)^2 = \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$.
• Die Einheiten in $\mathbb{Z}$ sind 1 und -1.
Die Einheiten in einem Polynomring über einem Körper sind die konstanten Polynome $\neq 0$.
Die Einheiten im Matrizenring bilden die allgemeine lineare Gruppe.

Definition 2.3.4 **(a)** *R heißt **Integritätsbereich**, falls R ein nullteilerfreier kommutativer Ring mit Eins ist und $R \neq \{0\}$.*

(b) *R heißt **Körper**, falls darüberhinaus $R^* = R \setminus \{0\}$, d.h. falls $0 \neq 1$ und jedes Element $\neq 0$ ein multiplikatives Inverses besitzt.*
*(Falls R nicht-kommutativer Ring mit Eins ist und $R^* = R \setminus \{0\}$ gilt, so heißt R **Schiefkörper**.)*

In Integritätbereichen, Körpern und Schiefkörpern gilt also stets $0 \neq 1$.

Lemma 2.3.5 *Für ein Ideal I im Ring R gilt genau dann $I \neq R$ („I ist echtes Ideal von R“), wenn $I \cap R^* = \emptyset$.*

BEWEIS: Falls $a \in I \cap R^*$, so ist $1 = a^{-1}a \in I$ und dann $I = R$ nach Bemerkung 2.1.8(a). Ist umgekehrt $R = I$, so ist $1 \in I \cap R^*$. □

Lemma 2.3.6 *K ist genau dann ein Körper, wenn K ein einfacher kommutativer Ring mit Eins $\neq \{0\}$ ist.*

BEWEIS: „⇒“ ist eine direkte Folgerung aus Lemma 2.3.5.
„⇐“: für $r \neq 0$ ist rR ein Ideal $\neq \{0\}$, also $rR = R$, also existiert ein $x \in R$ mit $rx = 1$. □

Bemerkung 2.3.7 **(a)** Nicht-triviale Ringhomomorphismen zwischen Körpern sind bereits injektive Körperhomomorphismen (injektiv wegen Lemma 2.3.6, und mit multiplikativen Inversen verträglich wegen Lemma 1.1.8).

(b) Ist $\varphi : R \to S$ ein unitärer Ringhomomorphismus, dann gilt $\varphi(R^*) \subseteq S^*$ (da $\varphi(r)\cdot\varphi(r^{-1}) = \varphi(rr^{-1}) = \varphi(1) = 1$) und die Einschränkung $\varphi \restriction_{R^*}: R^* \to S^*$ ist ein multiplikativer Gruppenhomomorphismus.

Satz 2.3.8 *Endliche Integritätsbereiche sind Körper.*

BEWEIS: Sei $r \neq 0$ Die Abbildung $R \to R$, $x \mapsto rx$ ist additiver Gruppenhomomorphismus (wegen der Distributivgesetze!). Da es keine Nullteiler gibt, ist der Kern trivial, d.h. die Abbildung injektiv. Damit ist sie, da der Ring endlich ist, auch surjektiv. Das Urbild der Eins ist dann ein multiplikatives Inverses von r. □

Die Injektivität der Abbildung $x \mapsto rx$ bedeutet, dass die **Kürzungsregel** $rs = rs' \Rightarrow s = s'$ für $r \neq 0$ gilt, denn aus $r(s - s') = 0$ folgt $s - s' = 0$.

Satz 2.3.9 *Jeder Integritätsbereich R ist Unterring eines Körpers. Der minimale Oberkörper ist bis auf Isomorphie über R eindeutig bestimmt und heißt **Quotientenkörper von** R,* $\mathrm{Quot}(R)$.

BEWEIS: Auf $R \times (R \setminus \{0\})$ definiert man die Relation $(a, b) \sim (c, d) :\iff ad = bc$. Auf Integritätsbereichen ist dies eine Äquivalenzrelation: reflexiv und symmetrisch ist sie stets; aus $(a, b) \sim (c, d) \sim (e, f)$, also aus $ad = bc$ und $cf = ed$, folgt $adf = bcf = bed$ und somit $af = be$ oder $(a, b) \sim (e, f)$ mit der Kürzungsregel.

Schreibe $\frac{a}{b}$ für die Äquivalenzklasse von (a, b). Durch die üblichen Rechenregeln für Brüche wird die Menge der Äquivalenzklassen zu einem Körper, in den sich der Ring R durch $r \mapsto \frac{r}{1}$ einbettet (nachrechnen, geht genauso wie bei der Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$!).

Jeder R enthaltende Körper enthält Elemente $\frac{a}{b} = ab^{-1}$, die sich nach den Bruchrechenregeln addieren und multiplizieren. Daraus folgt die Eindeutigkeit. □

Beispiel 2.3.10 $\mathbb{Q}$ ist der Quotientenkörper von $\mathbb{Z}$.
Der Körper $K(X)$ der rationalen Funktionen über dem Körper K ist der Quotientenkörper des Polynomrings $K[X]$.
Der Körper $K((X))$ der formalen Laurent-Reihen mit endlichem Hauptteil über dem Körper K ist der Quotientenkörper des Ringes $K[[X]]$ der formalen Potenzreihen.

Definition 2.3.11 *Ein Ideal M eines (kommutativen) Ringes R heißt **maximales Ideal**, falls M maximal unter den echten Idealen von R ist, d.h. $M \neq R$ und aus $M \subsetneq I \trianglelefteq R$ folgt $I = R$.*

Satz 2.3.12 *Sei R ein kommutativer Ring mit Eins. Ein Ideal M ist genau dann ein maximales Ideal, wenn R/M ein Körper ist.*

BEWEIS: Da Körper mindestens zwei Elemente haben, ist M ein echtes Ideal von R, falls R/M ein Körper ist. Die Ideale von R/M sind von der Form J/M für Ideale $M \subseteq J \trianglelefteq R$. Der Satz folgt dann aus Lemma 2.3.6. □

2.4 Einiges über Primelemente und Primideale

Definition 2.4.1 **(a)** *Ein Element $r \in R$, $r \neq 0$ und $r \notin R^*$, heißt **irreduzibel** (in R), wenn aus $r = ab$ folgt, dass a oder b eine Einheit ist.*

(b) *Ein Element $p \in R$, $p \neq 0$ und $p \notin R^*$, heißt **Primelement** (von R), oder kurz **prim** (in R), falls aus $p \mid ab$ folgt, dass $p \mid a$ oder $p \mid b$.*

(c) *Ein Ideal $P \neq R$ heißt **Primideal**, falls R/P ein Integritätsbereich ist (also genau dann, wenn aus $ab \in P$ folgt $a \in P$ oder $b \in P$).*

Bemerkung 2.4.2
- p ist genau dann Primelement, wenn pR Primideal $\neq \{0\}$.
- $r \in R$ ist genau dann irreduzibel, wenn rR maximal unter den echten Haupidealen ist.
- Später werden wir sehen: wenn p prim ist und kein Nullteiler, dann ist p irreduzibel. Die Umkehrung gilt nur in speziellen Fällen.

Beispiel 2.4.3 In $\mathbb{Z}$ ist irreduzibel = prim, dies sind gerade $\{\pm p \mid p \text{ Primzahl}\}$. Auch in $K[X]$ ist irreduzibel und prim dasselbe. Im allgemeinen stimmt dies nicht!

In $\mathbb{C}[X]$ sind die irreduziblen Elemente gerade die linearen Polynome. In $\mathbb{R}[X]$ sind es die linearen Polynome und die quadratischen Polynome ohne Nullstellen, z.B. $X^2 + 1$ (erfordert einen Beweis!).

Lemma 2.4.4 *Sei R ein Integritätsbereich. Dann gilt $rR = sR \iff r = s \cdot e$ mit $e \in R^*$.*

BEWEIS: „⇒“: Aus $rx = s$ und $r = sy$ folgt $r = rxy$, also mit Kürzungsregel $xy = 1$, d.h. x und y sind Einheiten.

„⇐“: falls $r = se$, so $rR \subseteq sR$, und andererseits auch $re^{-1} = s$, also $sR \subseteq rR$. □

Primelemente und irreduzible Elemente sind daher idealtheoretisch nur bis auf Multiplikation mit Einheiten bestimmt. Ringelemente, die durch Multiplikation mit Einheiten ineinander übergehen, nennt man auch „assoziiert“. Bei Fragen wie z.B. nach der Eindeutigkeit von Zerlegungen in Primelemente sieht man assozierte Primelemente als das gleiche Primelement an (genauer in Satz 2.4.20).

Satz 2.4.5 **(a) Kleiner Satz von Fermat**: *Seien $a \in \mathbb{Z}$ und die Primzahl $p \in \mathbb{N}$ teilerfremd. Dann gilt*

$$a^{p-1} \equiv 1 \pmod{p}.$$

(b) Satz von Euler: *Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}, n \geqslant 1$ teilerfremd. Dann gilt*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Zur Erinnerung: $\varphi(n)$ ist die Eulersche φ-Funktion aus 1.2.6.

BEWEIS: Rechnen modulo n entspricht dem Rechnen im Ring $\mathbb{Z}/n\mathbb{Z}$. Es gilt $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ nach 1.2.6 und Lemma 1.2.8. Also gilt mit Lemma 1.2.3 (Folgerung aus dem Satz von Lagrange) $(a + n\mathbb{Z})^{\varphi(n)} = 1 + n\mathbb{Z}$, was gerade der Satz von Euler ist. (a) ist dann der Spezialfall $n = p$. □

2.4.6 [Anwendung: Primzahltests I] Ist eine gegebene Zahl $n \in \mathbb{N}$ eine Primzahl?

1. Methode: Prüfe für alle $1 < d \leqslant \sqrt{n}$, ob d ein Teiler von n ist.
Vorteil: gibt sichere Antwort. Nachteil: dauert zu lange.

2. Methode: Teste, ob der Satz von Fermat gilt, d.h. wähle $a < n$ und überprüfe, ob $a^{n-1} \equiv 1 \pmod{n}$.
Vorteil: geht schnell. Nachteil: nur bei negativer Antwort weiß man, dass n keine Primzahl ist. Bei positiver Antwort: ?

Variante: wähle mehrere „unabhängige“ $a_i < n$ als Testzahlen. Es gibt aber Zahlen, die sogenannten Carmichael–Zahlen, die keine Primzahlen sind, aber den Fermat–Test für alle $a < n$ überstehen. Die kleinste solche Zahl ist 561. Es gibt unendlich viele Carmichael–Zahlen.

2.4.7 [Anwendung: RSA–Verschlüsselung] Wie kann man Nachrichten sicher verschlüsseln, ohne vorher den Schlüssel versenden zu müssen?

Grundidee: jeder Empfänger hat einen eigenen Schlüssel, der in einen öffentlichen Teil und einen privaten Teil aufgeteilt wird. Ein Sender verschlüsselt mit dem öffentlichen Teil, der Empfänger entschlüsselt mit dem privaten Teil des Schlüssels. Ver– und Entschlüsselung müssen schnell gehen, während das Knacken des Codes viel Zeit braucht.

Dazu wählt der Empfänger E zwei große unbekannte Primzahlen $p \neq q$, bildet $n = pq$, berechnet $\varphi(n) = (p-1)(q-1)$ und wählt eine „zufällige“ zu $\varphi(n)$ teilerfremde Zahl e. Der öffentliche Schlüssel besteht dann aus n, e, der geheime Teil aus $p, q, \varphi(n)$.

Nachrichten bestehen nun aus Folgen von Elementen $a_i \in \mathbb{Z}/n\mathbb{Z}$, die verschlüsselt werden in die Folge der a_i^e, berechnet in $\mathbb{Z}/n\mathbb{Z}$. Derweil berechnet E ein Inverses $d = e^{-1} \in (\mathbb{Z}/\varphi(n)\mathbb{Z})^*$, was mit Hilfe des euklidischen Algorithmus' schnell geht (man sucht d' so, dass $d'e' \equiv 1 \pmod{\varphi(n)}$ für Urbilder d', e' von d, e, in $\mathbb{Z}$). Zur Entschlüsselung berechnet E dann $(a_i^e)^d$ in $\mathbb{Z}/n\mathbb{Z}$, was gerade a_i ist: Für zu n teilerfremde Zahlen folgt dies direkt aus dem Satz von Euler; für zu n nicht-teilerfremde Zahlen a_i gilt es aber auch, da n quadratfrei ist (a_i ist dann z.B. durch p, aber nicht durch q teilbar. Für p gilt die Kongruenz $a_i^{ed} \equiv a_i$ dann trivialerweise, für q nach dem kleinen Satz von Fermat).

Achtung: Dies ist nur die Idee einer mathematischen Umsetzung der Grundidee; die konkrete Realisierung ist schwieriger. Zum einen kann man nicht einfach einzelne Buchstaben codieren, da dann durch Buchstabenhäufigkeiten die Nachricht decodierbar würde. Zum andern muss man beachten, dass die Umsetzung in Binärzahlen eventuell besondere Eigenschaften ins Spiel bringen könnten, die den Code knackbar machen.

2.4.8 [Anwendung: Codierung] Alte ISBN–Nummer: rechne im Körper $\mathbb{Z}/11\mathbb{Z}$. Neunstellige Dezimalzahl $(a_1, \ldots, a_9)$ wird so um eine Prüfziffer a_{10} ergänzt, dass $\sum_{i=1}^{10} i \cdot (a_i + 11\mathbb{Z}) = 0 + 11\mathbb{Z}$ gilt. Die Prüfziffer erkennt einen Fehler und das Vertauschen zweier Ziffern, d.h. weicht $(b_1, \ldots, b_9)$ von $(a_1, \ldots, a_9)$ nur an einer Stelle ab oder unterscheidet sich durch Vertauschen zweier Ziffern, so ändert sich die Prüfziffer.

2.4.9 [Legendre–Symbol] Schreibe $\bar{a}$ für $a + p\mathbb{Z}$, d.h. für das Bild von $a \in \mathbb{Z}$ unter dem natürlichen Epimorphismus $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$.

$(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$, $x \mapsto x^2$ ist ein Gruppenhomomorphismus. Für Primzahlen $p > 2$ ist der Kern gerade $\{\overline{1}, \overline{-1}\} = \{\overline{1}, \overline{p-1}\}$, besteht also aus zwei Elementen. Also gilt $|\text{Bild}(x \mapsto x^2)| = \frac{p-1}{2}$, d.h. genau die Hälfte der Elemente von $(\mathbb{Z}/p\mathbb{Z})^*$ sind Quadrate.

Für $a \in \mathbb{Z}$, $p \nmid a$, definiert man nun das **Legendre–Symbol**

$$(\frac{a}{p}) := 1 \text{ falls } \bar{a} \text{ Quadrat in } \mathbb{Z}/p\mathbb{Z} \qquad (\frac{a}{p}) := -1 \text{ sonst}$$

Der Beweis des folgenden Satzes wird zeigen, dass $(\frac{\div}{p})$ einen Gruppenhomomorphismus von $(\mathbb{Z}/p\mathbb{Z})^*$ in die multiplikative Gruppe $\{\pm 1\}$ induziert, dessen Kern gerade aus den Quadraten besteht.

Satz 2.4.10 (Euler) *Sei $p > 2$ Primzahl, $p \nmid a \in \mathbb{Z}$. Dann ist*

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Beweis: Nach Folgerung 1.3.8 ist $(\mathbb{Z}/p\mathbb{Z})^*$ zyklisch; sei g ein Erzeuger. Dann ist $g^{\frac{p-1}{2}} = \overline{-1}$, denn $(g^{\frac{p-1}{2}})^2 = g^{p-1} = \overline{1}$ und $p-1$ ist die Ordnung von g in $(\mathbb{Z}/p\mathbb{Z})^*$. Für $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ gibt es also ein $0 \leqslant j < p-1$ mit $g^j = \bar{a}$.
Ist j gerade, so ist $\bar{a} = (g^{\frac{j}{2}})^2$ ein Quadrat. Ist j ungerade, so ist $\bar{a}$, kein Quadrat, da es nur $\frac{p-1}{2}$ Quadrate gibt, die alle schon durch gerade j abgedeckt sind. Also gilt $\bar{a}^{\frac{p-1}{2}} = (g^j)^{\frac{p-1}{2}} = (g^{\frac{p-1}{2}})^j = (\overline{-1})^j$, und somit: $\bar{a}^{\frac{p-1}{2}} = \overline{1} \iff j$ gerade $\iff \bar{a}$ Quadrat. □

Satz 2.4.11 (Quadratisches Reziprozitätsgesetz (Gauss)) *Seien p, q ungerade Primzahlen. Dann*

$$(\frac{p}{q}) \cdot (\frac{q}{p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

(ohne Beweis)

2.4.12 [Anwendung: Primzahltests II]
Man erweitert das Legendre–Symbol multiplikativ durch $(\frac{kp}{p}) = 0$ für $k \in \mathbb{Z}$ und für ungerades n durch $(\frac{a}{n}) = \prod (\frac{a}{p_i})^{k_i}$, sofern $n = \prod p_i^{k_i}$ die Primfaktorzerlegung ist. Dieses erweiterte Legendre–Symbol lässt sich mit Hilfe des quadratischen Reziprozitätsgesetzes und einiger anderer Regeln schnell berechnen.

Ist gegebenes $n \in \mathbb{N}$ eine Primzahl? Teste dazu, ob für $a < n$ Satz 2.4.10 gilt, d.h. ob $(\frac{a}{n}) \equiv a^{\frac{n-1}{2}} \pmod{n}$. Ist die Antwort „nein“, so ist n keine Primzahl. Ist umgekehrt n keine Primzahl, so gibt es nach einem Ergebnis von Solovay und Strassen weniger als $\frac{1}{2}\varphi(n)$ Testzahlen a, die den Test erfüllen. Durch viele unabhängige Test kann man daher die Wahrscheinlichkeit einer falschen Antwort sehr klein machen.

Definition 2.4.13 *Ein Integritätsbereich R heißt*

(a) ***Hauptidealring**, falls alle Ideale Haupideale sind, also von der Form rR für ein $r \in R$.*

(b) ***euklidischer Ring**, falls es eine Abbildung $\varphi : R \setminus \{0\} \to \mathbb{N}$ gibt mit den Eigenschaften*
- *$\varphi(ab) \geqslant \varphi(a)$ für alle $a, b \in R \setminus \{0\}$,*

– *zu $a, b \in R$, $a \neq 0$, gibt es eine Darstellung $b = qa + r$ mit $r = 0$ oder $\varphi(r) < \varphi(a)$ („Division mit Rest“).*

(c) ***faktorieller Ring**, falls eine der beiden äquivalenten Bedingungen gilt:*
(I) Jedes Element $r \in R$, $r \neq 0$ und $r \notin R^*$, lässt sich als Produkt von Primelementen schreiben, d.h. $r = p_1 \cdot \ldots \cdot p_k$ mit $k \geqslant 1$ und p_i prim.
(II) Jedes Element $r \in R$, $r \neq 0$ und $r \notin R^*$, lässt sich „eindeutig“ als Produkt von irreduziblen Elementen schreiben, d.h. $r = u_1 \cdot \ldots \cdot u_k$ mit $k \geqslant 1$ und u_i irreduzibel, und die Darstellung ist in folgendem Sinne eindeutig: falls auch $r = v_1 \cdot \ldots \cdot v_l$ mit irreduziblen v_j, dann gilt $k = l$ und es gibt ein $\sigma \in \mathrm{Sym}(n)$ mit $u_i R = v_{\sigma(i)} R$.

Die Äquivalenz von (I) und (II) wird in Folgerung 2.4.22 gezeigt.

Beispiel 2.4.14 [**für euklidische Ringe**]

– $\mathbb{Z}$ mit Betragsfunktion als φ.
– Polynomringe $K[X]$ über Körpern K mit der Gradfunktion als φ.
– $\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \in \mathbb{C} \mid, a, b \in \mathbb{Z}\}$ mit $\varphi(a + b\mathrm{i}) = a^2 + b^2$.
– Jeder Körper mit konstantem φ.

Satz 2.4.15 *Euklidische Ringe sind Hauptidealringe.*

Beweis: Sei $I \neq \{0\}$ ein Ideal in einem euklidischen Ring. Wähle $0 \neq a \in I$ mit minimalem Wert unter φ. Für $b \in I$ gibt es nun eine Darstellung $b = qa + r$ wie in der Definition der euklidischen Ringe. Mit a und b ist dann auch $r = b - qa \in I$, also ist $r = 0$ nach der Wahl von a und somit $b \in aR$. Die umgekehrte Inklusion $aR \subseteq I$ ist klar. □

Bemerkung 2.4.16 Seien $r_1, \ldots, r_n$ aus R. Ein **größter gemeinsamer Teiler** (ggT) von $r_1, \ldots, r_n$ ist ein gemeinsamer Teiler von $r_1, \ldots, r_n$, der von allen anderen gemeinsamen Teilern von $r_1, \ldots, r_n$ geteilt wird. Entsprechend ist ein **kleinstes gemeinsames Vielfaches** (kgV) von $r_1, \ldots, r_n$ ein gemeinsames Vielfaches, das alle anderen gemeinsamen Vielfachen teilt. Es gilt nun:

$$\bigcap_{i=1}^{n} r_i R = kR \iff k \text{ ist ein kgV von } r_1, \ldots, r_n$$
$$\sum_{i=1}^{n} r_i R = gR \iff g \text{ ist ein ggT von } r_1, \ldots, r_n$$

Insbesondere existieren kgV und ggT stets in Hauptidealringen. Außerdem ist ein ggT von $r_1, \ldots, r_n$ stets eine R-Linearkombination der r_i (vergleiche Fakt 1.2.7).

Lemma 2.4.17 *Ist $p \in R$ prim, und kein Nullteiler, so ist p irreduzibel. Insbesondere sind in Integritätsbereichen alle Primelemente irreduzibel.*

Beweis: Sei $p = ab$, insbesondere $p \mid ab$, also $p \mid a$ oder $p \mid b$, da p prim. O.E. $p \mid a$, also $px = a$ für ein $x \in R$. Dann gilt $pxb = ab = p$, also $p(xb - 1) = 0$. Da p nicht Nullteiler ist, muss $xb = 1$ gelten, d.h. b ist Einheit. □

Beispiel: In $\mathbb{Z}/6\mathbb{Z}$ ist $3 + 6\mathbb{Z}$ ein Primelement, da $(\mathbb{Z}/6\mathbb{Z})/(3 + 6\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ ein Integritätsbereich ist. Es gilt aber $3 + 6\mathbb{Z} = (3 + 6\mathbb{Z}) \cdot (3 + 6\mathbb{Z})$, also ist es nicht irreduzibel.

Satz 2.4.18 *Sei R Hauptidealring. Dann sind irreduzible Elemente prim und Primideale $\neq \{0\}$ maximale Ideale.*

BEWEIS: Sei p irreduzibel und $a \notin pR$. Dann ist $pR + aR = gR$ für einen ggT g von a und p (da R Hauptidealring), also $p = gr$ für ein $r \in R$. Da p irreduzibel, ist entweder r Einheit – aber dann nach Lemma 2.4.4 $pR = gR \ni a$: Widerspruch – oder g Einheit – also letzteres. Dann ist aber $gR = R$, und somit pR ein maximales Ideal. Maximale Ideale sind aber Primideale, also ist p prim. Überdies ist jedes Primideal $P \neq \{0\}$ von einem Primelement erzeugt, das nach Lemma 2.4.17 irreduzibel ist, also ist P maximal. □

Satz 2.4.19 *Hauptidealringe sind faktoriell.*

BEWEIS: Angenommen $a_0 \in R$, $a_0 \neq 0$ und $a_0 \notin R^*$, lässt sich nicht als Produkt irreduzibler Elemente schreiben. Insbesondere ist a_0 selbst nicht irreduzibel, schreibt sich also als $a_0 = a_1 a_1'$ mit Nicht-Einheiten a_1, a_1'. Insbesondere ist $a_0 R \subsetneq a_1 R$. Mindestens eines, o.E. a_1, lässt sich dann auch nicht als Produkt irreduzibler Elemente schreiben (denn sonst wäre das Produkt eine Schreibweise für a_0). Auf diese Weise erhält man eine Kette

$$a_0 R \subsetneq a_1 R \subsetneq a_2 R \subsetneq \dots$$

Man überlegt sich schnell, dass die Vereinigung $\bigcup_{n\in\mathbb{N}} a_n R$ wieder ein Ideal ist, also von der Form sR, da R Hauptidealring. Dann muss aber bereits $s \in a_m R$ für ein $m \in \mathbb{N}$ gelten, was zu dem Widerspruch $sR \subseteq a_m R$ führt.

Also lässt sich jede Nicht-Einheit $\neq 0$ als Produkt von irreduziblen Elementen, und damit nach Satz 2.4.18 als Produkt von Primelementen schreiben, was die eine mögliche Definition faktorieller Ringe ist. □

Satz 2.4.20 *Eine Zerlegung in Primelemente ist stets eindeutig in Integritätsbereichen.*

BEWEIS: Wir zeigen: Falls $\varepsilon p_1 \cdots p_k = \varepsilon' q_1 \cdots q_l$ für Einheiten $\varepsilon, \varepsilon'$ und Primelemente p_i, q_j, so ist $k = l$ und für ein $\sigma \in \mathrm{Sym}(k)$ gilt $p_i R = q_{\sigma(i)} R$.

Ohne Einschränkung sei $k \leqslant l$. Es gilt $p_1 \mid q_1 \cdots q_l$, also, da p_1 prim ist, $p_1 \mid q_{j_0}$ für ein j_0. Setze dann $\sigma(1) = j_0$. Ohne Einschränkung können wir annehmen, dass $j_0 = 1$. Wir schreiben dann $q_1 = x_1 p_1$, und da Primelemente irreduzibel sind, ist $x_1 \in R^*$, also auch $p_1 R = q_1 R$. Mit der Kürzungsregel folgt dann $\varepsilon p_2 \cdots p_k = \varepsilon' x_1 q_2 \cdots q_l$. O.E. erhält man induktiv $p_i = x_i q_i$ für Einheiten x_i und alle $i = 1, \dots, k$. Also ist zuletzt $\varepsilon = \varepsilon' x_1 \cdots x_n q_{k+1} \cdots q_l$. Da Primelemente keine Einheiten sind, folgt $l = k$. □

Lemma 2.4.21 *In faktoriellen Ringen sind irreduzible Elemente prim.*

BEWEIS: Mit Definition (I) sieht man es folgendermaßen:

Sei u irreduzibel, $u = p_1 \dots p_k$ eine Schreibweise als Produkt von Primelementen. Falls $a \notin R^*$ und $b \in R$, dann ist $ab \in aR \neq R$, also ist auch ab keine Einheit. Also ist kein Teilprodukt der p_i eine Einheit, somit $k = 1$ und $u = p_1$ prim.

Mit Definition (II):

Sei u irreduzibel, $u \mid ab$. Dann gilt $ux = ab$ für ein $x \in R$. Man zerlegt x, a, b in irreduzible Elemente, so dass also $ux_1 \dots x_j = a_1 \dots a_k b_1 \dots b_l$. Wegen der Eindeutigkeit der Zerlegung

muss bis auf Multiplikation mit einer Einheit u auch auf der rechten Seite auftreten, also etwa $uR = a_i R$. Dann gilt aber $u \mid a$. □

Folgerung 2.4.22 *Die beiden Definitionen für faktorelle Ringe in 2.4.13 sind äquivalent.*

Beweis: Aus beiden Definitionen folgt, dass irreduzible Elemente prim sind. Zerlegungen in Primelemente sind stets eindeutig. □

Beispiel 2.4.23

- Es gibt Hauptidealringe, die nicht euklidisch sind (aber der Nachweis ist nicht einfach).
- Satz (ohne Beweis): Ist R faktoriell, so auch $R[X]$.
  Also sind alle Polynomringe $\mathbb{Z}[X_1, \ldots, X_n]$ und $K[X_0, \cdots, X_n]$ für Körper K faktoriell; jedoch sind es für $n \geqslant 1$ keine Hauptidealringe.
- $\mathbb{Z}[\sqrt{-5}]$ ist kein faktorieller Ring, jedoch ist jede Nicht-Einheit $\neq 0$ Produkt von irreduziblen Elementen.

Eine Übersicht:

$$\boxed{pR \text{ maximal}} \quad \begin{array}{c}\text{in Hauptidealringen}\\ \Longleftarrow\\ \Longrightarrow\\ \text{in allen Ringen}\\ \text{(außer Körpern)}\end{array} \quad \boxed{p \text{ prim}} \quad \begin{array}{c}\text{in faktoriellen Ringen}\\ \Longleftarrow\\ \Longrightarrow\\ \text{in Integritätsbereichen}\end{array} \quad \boxed{p \text{ irreduzibel}}$$

2.4.24 [Ein bisschen algebraische Zahlentheorie]

Frage: Welche Primzahlen p von $\mathbb{N}$ bleiben prim im unitären Oberring $\mathbb{Z}[\mathrm{i}]$? (Beide sind Hauptidealringe, somit stimmen Primelement und irreduzible Elemente jeweils überein.)

Zum Beispiel zerfällt $2 = (1+\mathrm{i})(1-\mathrm{i}) = 1^2 - \mathrm{i}^2$ in $\mathbb{Z}[\mathrm{i}]$.

Man sieht schnell: p zerfällt genau dann in $\mathbb{Z}[\mathrm{i}]$, wenn p Summe zweier Quadratzahlen ist. Denn einerseits ist $p = a^2 + b^2 = (a+\mathrm{i}b)(a-\mathrm{i}b)$. Andererseits liefert komplexe Konjugation aus einer Zerlegung $p = q \cdot r$ auch die Zerlegung $p = \overline{p} = \overline{q} \cdot \overline{r}$. Wegen der eindeutigen Primfaktorzerlegung in $\mathbb{Z}[\mathrm{i}]$ muss $r = \overline{q}$ gelten, und die Zerlegung hat die Form $p = q \cdot \overline{q}$.

Wir betrachten nun folgende Homomorphismen: einerseits „modulo (p)“, das jeweils von dem Primelement p erzeugte Ideal, und andererseits „modulo (X^2+1)“. Dabei muss man sich überlegen, dass tatsächlich immer die im Diagramm angegebenen Ringe herauskommen, und dass das „Diagramm kommutiert“, d.h. die Reihenfolge keine Rolle spielt.

$$\begin{array}{ccccc} & & \mathbb{Z}[X] & & \\ & \mod p\cdot\mathbb{Z}[X] \swarrow & & \searrow \mod (X^2+1)\cdot\mathbb{Z}[X] & \\ & \mathbb{F}_p[X] & & \mathbb{Z}[\mathrm{i}] & \\ \mod (X^2+\overline{1})\cdot\mathbb{F}_p[X] \searrow & & & & \swarrow \mod p\cdot\mathbb{Z}[\mathrm{i}] \\ & & \mathbb{F}_p[X]/(X^2+\overline{1}) & & \end{array}$$

Nun gilt: Eine Primzahl $p \in \mathbb{Z}$ ist prim in $\mathbb{Z}$[i]

$\iff p\mathbb{Z}$[i] ist Primideal von $\mathbb{Z}$[i]

$\iff \mathbb{F}_p[X]/(X^2+1)$ ist Integritätsbereich (und dann der Körper $\mathbb{F}_p$[i])

$\iff X^2 + \overline{1}$ ist prim in $\mathbb{F}_p[X]$

$\iff X^2 + \overline{1}$ ist irreduzibel in $\mathbb{F}_p[X]$ (da Hauptidealring)

$\iff X^2 + \overline{1}$ hat keine Nullstelle in $\mathbb{F}_p[X]$

$\iff \overline{-1}$ ist kein Quadrat in $\mathbb{F}_p$

$\iff p \equiv 3 \pmod 4$

Nur die letzte Äquivalenz ist noch zu beweisen: Für $p = 2$ ist $\overline{-1} = \overline{1} = \overline{1}^2$. Sei also $p \neq 2$; dann ist $\overline{-1} \neq \overline{1}$. Zu zeigen ist jetzt also für $p \neq 2$: $\overline{-1}$ ist Quadrat in $\mathbb{F}_p \iff p \equiv 1 \pmod 4$.

„$\Rightarrow$“: Sei $\overline{-1} = a^2$ ein Quadrat in $\mathbb{F}_p$. Dann hat die Gleichung $X^4 = 1$ vier Lösungen $\overline{1}, \overline{-1}, a, -a$ in $\mathbb{F}_p$. Also hat der Homomorphismus $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^4$ einen Kern der Größe 4 und damit $\left|\text{Bild}(x \mapsto x^4)\right| = \frac{p-1}{4} \in \mathbb{N}$. Also gilt $p \equiv 1 \pmod 4$.

„$\Leftarrow$“: Sei $\mathbb{F}_p^\times = \langle g \rangle$ (Folgerung 1.3.8). Dann $a := (g^{\frac{p-1}{4}})^2 = g^{\frac{p-1}{2}} \neq \overline{1}$, aber $a^2 = (g^{\frac{p-1}{4}})^4 = \overline{1}$, somit $a^2 = \overline{-1}$.

Folgerung 2.4.25 *Eine Primzahl $p \in \mathbb{N}$ ist genau dann Summe von zwei Quadraten in $\mathbb{N}$, wenn $p = 2$ oder $p \equiv 1 \pmod 4$.*

2.5 Das Lemma von Gauss[2]

Definition 2.5.1 *Sei R ein faktorieller Ring, K der Quotientenkörper und $f \in R[X]$. Der **Inhalt** von f ist der (nur bis auf Einheit in R bestimmte) ggT der Koeffizienten von f. Das Polynom f heißt **primitiv**, wenn die Koeffizienten teilerfremd sind, d.h. wenn der Inhalt von f eine Einheit ist (kurz: „f hat Inhalt 1“).*

Normierte Polynome sind primitiv.

Bemerkung 2.5.2 Falls $f(X) = \sum_{i=0}^{n} \frac{r_i}{s_i} X^i \in K[X]$ mit $r_i, s_i \in R$ teilerfremd, so kann man mit $C_f := \text{ggT}_R(r_0, \ldots, r_n) \in R$ den „R-Inhalt“ von f definieren: für $f \in R[X]$ ist C_f gerade der Inhalt. Setzt man $\widetilde{r_i} := \frac{r_i}{C_f}$ und $\tilde{f}(X) := \sum_{i=0}^{n} \frac{\widetilde{r_i}}{s_i} X^i$, so gilt $f(X) = C_f \cdot \tilde{f}(X)$.

Sei ferner $N_f := \text{kgV}_R(s_0, \ldots, s_n) \in R$, wiederum nur bis auf Einheit in R bestimmt. Dann sind C_f und N_f teilerfremd, und es gilt $N_f \cdot f = C_f \cdot \underbrace{N_f \cdot \tilde{f}(X)}_{\in R[X] \text{ primitiv}}$.

Lemma 2.5.3 *Der Inhalt ist multiplikativ.*

Beweis: Sei $f = g \cdot h = C_g \cdot C_h \cdot \tilde{g} \cdot \tilde{h}$, alles in $R[X]$. Es reicht zu zeigen, dass $\tilde{g} \cdot \tilde{h}$ primitiv ist, denn dann ist $C_g C_h$ der Inhalt von f. Angenommen nicht, und ein Primelement p teilt $C_{\tilde{g}\cdot\tilde{h}}$. Man prüft ohne Schwierigkeiten nach, dass der natürliche Epimorphismus $R[X] \to (R/pR)[X]$ den Kern $pR[X]$ hat und somit $R[X]/pR[X] \cong (R/pR)[X]$ ein Integritätsbereich ist. Im Widerspruch dazu gilt nun aber nach Annahme einerseits $\tilde{g} \cdot \tilde{h} + pR[X] = 0 \in R[X]/pR[X]$, andererseits $\tilde{g} + pR[X] \neq 0 \neq \tilde{h} + pR[X]$. □

[2] In der Literatur werden verschiedene Ergebnisse dieses Abschnittes als „Lemma von Gauss“ bezeichnet.

Lemma 2.5.4 *Sei $f \in R[X]$ primitiv. Dann ist f genau dann irreduzibel in $R[X]$, wenn f irreduzibel in $K[X]$ ist.*

BEWEIS: „$\Leftarrow$“: Angenommen f ist irreduzibel in $K[X]$, aber $f = g \cdot h$ in $R[X]$. Dann ist ohne Einschränkung g eine Einheit in $K[X]$, also $g \in K[X]^* \cap R[X] = K^* \cap R[X] \subseteq R$. Da g dann den Inhalt von f teilt, ist g eine Einheit in R.

„$\Rightarrow$“: Sei $f = g \cdot h$ in $K[X]$ eine Zerlegung in Nicht-Einheiten. Dann gilt $N_g N_h f = C_g C_h \cdot N_g \tilde{g} N_h \tilde{h}$, wobei f und $N_g \tilde{g} N_h \tilde{h}$ primitiv sind, also $N_g N_h = C_g C_h$ gilt. Da nun N_g, C_g und N_h, C_h jeweils teilerfremd sind, folgt $N_g = C_h$ und $N_h = C_g$, und somit ist $f = (N_g \tilde{g}) \cdot (N_h \tilde{h})$ eine echte Zerlegung in $R[X]$. □

Folgerung 2.5.5 *Sei $f = g \cdot h \in R[X]$ mit $g, h \in K[X]$.*

(a) *Falls g, h normiert sind, so sind $g, h \in R[X]$.*

(b) *Falls $g \in R[X]$ primitiv ist, so ist auch $h \in R[X]$.*

BEWEIS: (a) Da g und h normiert sind, ist einerseits f auch normiert, andererseits sind g und h primitiv, d.h. $C_g = 1$ und $g = \widetilde{g}$, entsprechend für h. Also ist $N_g N_h f = (N_g \widetilde{g})(N_h \widetilde{h})$ primitiv, d.h. $N g N_h = 1$, N_g und N_h sind Einheiten in R und damit $g, h \in R[X]$.

(b) Hier gilt $N_h f = g \cdot C_h N_h \tilde{h}$, wobei g und $N_h \tilde{h}$ primitiv sind. Also ist C_h der Inhalt von $N_h f$, d.h. N_h teilt C_h. Da C_h, N_h aber teilerfremd sind, ist $N_h = 1$. □

Lemma 2.5.6 *Wenn p prim in R ist, dann ist auch p prim in $R[X]$.*
Wenn $p(X)$ primitiv und irreduzibel in $R[X]$ ist, dann ist $p(X)$ prim in $R[X]$.
Es gibt keine anderen Primelemente in $R[X]$.

BEWEIS: Das erste wurde schon im Beweis von Lemma 2.5.3 gezeigt.

Im zweiten Fall ist $p(X)$ auch irreduzibel in $K[X]$ nach Lemma 2.5.4, und damit, da $K[X]$ faktoriell ist, auch prim in $K[X]$. Man betrachte nun den Homomorphismus $\varphi : R[X]/p(X)R[X] \to K[X]/p(X)K[X]$, $f(X) + p(X)R[X] \mapsto f(X) + p(X)K[X]$. Es reicht zu zeigen, dass es injektiv ist, denn dann ist $R[X]/p(X)R[X]$ als Unterring des Integritätsbereiches $K[X]/p(X)K[X]$ auch ein Integritätsbereich.

Sei also $\varphi(f(X) + p(X)R[X]) = 0$, d.h. $p(X)$ teilt $f(X)$ in $K[X]$. Da $p(X)$ primitiv ist, ist nach Folgerung 2.5.5 (b) $p(X)$ auch ein Teiler von $f(X)$ in $R[X]$.

Ist $f(X)$ prim in $R[X]$, so auch irreduzibel. Wenn f nicht konstant ist, hat f also Inhalt 1. Wenn f konstant ist, dann ist f auch irreduzibel in R (da $R^* = R[X]^*$), also prim in R, da R faktoriell. □

Folgerung 2.5.7 *Wenn R faktoriell ist, dann auch $R[X]$.*

BEWEIS: $K[X]$ ist faktoriell, also zerlegt sich $f \in R[X]$ in $K[X]$ in irreduzible Faktoren $g_1, \ldots, g_k$. Dann ist auch $N_i \widetilde{g_i}$, da nur durch eine Einheit von $K[X]$ von g_i unterschieden, irreduzibel, und zwar nach Lemma 2.5.4 auch in $R[X]$. Nun ist

$$N_{g_1} \ldots N_{g_k} f = \underbrace{C_{g_1} \ldots C_{g_k}}_{\in R} \cdot \underbrace{(N_{g_1} \widetilde{g_1}) \ldots (N_{g_k} \widetilde{g_k})}_{\in R[X] \text{ primitiv}}$$

insbesondere ist $C_{g_1} \dots C_{g_k}$ der Inhalt beider Seiten und wird von $N_{g_1} \dots N_{g_k}$ geteilt. Beides sind Elemente von R, lassen sich also dort eindeutig in Primelemente zerlegen. Wegen der Eindeutigkeit tauchen die Faktoren von $N_{g_1} \dots N_{g_k}$ in der Primfaktorzerlegung von $C_{g_1} \dots C_{g_k}$ auf und können auf beiden Seiten weggelassen werden. Was übrig bleibt ist dann nach Lemma 2.5.6 eine Zerlegung von f in Primelemente von $R[X]$. □

3 Körper

3.1 Körpererweiterungen

Definition 3.1.1 **(a)** *Ein* ***Unterkörper*** *eines Körpers ist eine Teilmenge, die unter den eingeschränkten Operationen wieder ein Körper ist, also eine Teilmenge, die* 0 *und* 1 *enthält und unter Addition, Subtraktion, Multiplikation und Division (durch Elemente ungleich null) abgeschlossen ist.*

(b) *Der* ***Primkörper*** *eines Körpers ist der kleinste Unterkörper, also der Schnitt über alle Unterkörper.*

Satz 3.1.2 *Der Primkörper eines Körpers ist entweder $\mathbb{Q}$ oder $\mathbb{F}_p$ für eine Primzahl p. Diese sind paarweise nicht isomorph.*

BEWEIS: Sei K ein beliebiger Körper. Man rechne nach, dass die Abbildung $\mathbb{N} \to K$, $n \mapsto \underbrace{1 + \dots + 1}_{n \text{ mal}}$ sich zu einem Ringhomomorphismus $\mathbb{Z} \to K$ fortsetzt. Falls der Homomorphismus injektiv ist, so enthält K mit $\mathbb{Z}$ auch dessen Quotientenkörper $\mathbb{Q}$. Andernfalls hat der Homomorphismus hat einen Kern $m\mathbb{Z}$ für $m \neq 0$. Dann enthält der Körper einen Unterring $\mathbb{Z}/m\mathbb{Z}$. Dieser muss als Unterring eines Integritätsbereiches selbst ein Integritätsbereich sein, also $m = p$ eine Primzahl.

Da sowohl $\mathbb{Q}$ als auch $\mathbb{F}_p$ von 1 erzeugt sind, haben sie keine echten Unterkörper und sind somit Primkörper. Außerdem haben sie jeweils verschiedene Anzahlen von Elementen, sind also paarweise nicht isomorph. □

Definition 3.1.3 *Die* ***Charakteristik*** *eines Körpers K, $\mathrm{char}(K)$, ist p, falls $\mathbb{F}_p$ der Primkörper ist, und* 0 *sonst.*

Definition 3.1.4 *Eine* ***Körpererweiterung*** *L/K besteht aus einem Körper K,* ***Grundkörper*** *genannt, und einem Oberkörper L, auch* ***Erweiterungskörper*** *genannt.*

Dann ist L ein K-Vektorraum. Umgekehrt ist jeder Körper, der ein K-Vektorraum ist, bis auf Isomorphie ein Erweiterungskörper von K.

Die Dimension von L als K-Vektorraum heißt der ***Grad*** *der Erweiterung, geschrieben $[L : K]$.*
Falls $[L : K] < \infty$, so heißt die Erweiterung ***endlich****.*
Falls $[L : K] = 2$, so heißt die Erweiterung ***quadratisch****.*

Gegeben L/K und $a_1, \dots, a_n \in L$, so gibt es den ***Auswertungshomomorphimus*** *zwischen Ringen* $\mathrm{eval}_{a_1,\dots,a_n} : K[X_1, \dots, X_n] \to L$, $P(X_1, \dots, X_n) \mapsto P(a_1, \dots, a_n)$.

Lemma 3.1.5 *Sei L/K Körpererweiterung und V ein L-Vektorraum. Dann gilt* $\dim_K V = [L : K] \cdot \dim_L V$. *Insbesondere: Ist M/L Körpererweiterung, so ist $[M : K] = [M : L] \cdot [L : K]$.*

BEWEIS: Ist $\{v_i \mid i \in I\}$ eine L-Basis von V und $\{l_j \mid j \in J\}$ eine K-Basis von L, so sieht man leicht, dass $\{v_i l_j \mid i \in I, j \in J\}$ eine K-Basis von V ist. □

Definition 3.1.6 *Sei L/K eine Körpererweiterung und $a_1, \ldots, a_n \in L$.*

- *$K[a_1, \ldots, a_n]$ ist der kleinste Unterring von L, der K und die Elemente $a_1, \ldots, a_n$ enthält. Dies ist genau das Bild des Auswertungshomomorphismus* $\mathrm{eval}_{a_1,\ldots,a_n}$.
- *$K(a_1, \ldots, a_n)$ ist der kleinste Unterkörper von L, der K und die Elemente $a_1, \ldots, a_n$ enthält.*

$$\begin{aligned} K(a_1, \ldots, a_n) &= \mathrm{Quot}(K[a_1, \ldots, a_n]) \\ &= \left\{ \tfrac{P}{Q}(a_1, \ldots, a_n) \;\middle|\; \tfrac{P}{Q} \in K(X_1, \ldots, X_n) \text{ mit } Q(a_1, \ldots, a_n) \neq 0 \right\}. \end{aligned}$$

- *$[K(a) : K]$ heißt der **Grad von** a **über** K. Falls L/K endlich, so teilt der Grad von a über K den Grad von L/K (nach Lemma 3.1.5).*
- *a heißt **primitives Element** der Körpererweiterung L/K, falls $L = K(a)$. Die Körpererweiterung heißt dann **primitive** oder **einfache Erweiterung**.*

Es ist klar per Definition, daß $K(a, b) = K(a)(b)$ ist.

Satz und Definition 3.1.7 *Es sei L/K eine Körpererweiterung und $a \in L$. Wir betrachten den Auswertungshomomorphismus* $\mathrm{eval}_a : K[X] \to L$ *mit Kern* $\{P \in K[X] \mid P(a) = 0\} = K[X] \cap (X - a) \cdot L[X]$. *Es gibt zwei Fälle:*

(I) $\mathrm{Kern}(\mathrm{eval}_a) = \{0\}$. *Dann heißt a **transzendent über** K und es gilt $K[a] \cong_K K[X]$, $K(a) \cong_K K(X)$. Die Erweiterung $K(a)/K$ hat unendlichen Grad, und die Potenzen a^i für $i \in \mathbb{Z}$ sind linear unabhängig über K.*

(II) $\mathrm{Kern}(\mathrm{eval}_a) = P(X) \cdot K[X] = (P) \neq \{0\}$. *Dann heißt a **algebraisch über** K. Wählt man P normiert, so heißt es **Minimalpolynom von** a **über** K,* $\min_{a/K}(X)$. *Es gilt dann:*

(a) $\min_{a/K}$ *ist das eindeutige bestimmte, normierte Polynom minimalen Grades mit Nullstelle a. Es ist irreduzibel.*

(b) $K[a] = K(a) \cong_K K[X]/(\min_{a/K}(X))$

(c) *Der Grad n des Minimalpolynoms ist gleich $[K(a) : K]$.*

(d) $\{1, a, a^2, \ldots, a^{n-1}\}$ *ist eine K-Basis von $K(a)$.*

BEWEIS: Fall (I): Die Isomorphie $K[a] \cong_K K[X]$ folgt sofort aus dem Homomorphiesatz; die Isomorphie $K(a) \cong_K K(X)$ ergibt sich daraus und aus der Eindeutigkeit Quotientenkörper. Wären die Potenzen von a^i linear abhängig, gäbe es eine nicht-triviale Linearkombination. Multiplizierte man diese mit einer hinreichend großen Potenz von a durch, ergäbe sich ein Polynom mit Koeffizienten in K, welches a zur Nullstelle hat. Insbesondere folgt, dass der Grad der Körpererweiterung unendlich ist.

Fall (II): P existiert, da $K[X]$ ein Hauptidealring ist. Es ist bis auf Multiplikation mit einer Einheit eindeutig bestimmt, kann also normiert werden. Da $K[X]$ euklidisch bezüglich der Gradfunktion ist, sind Ideale von den Elementen minimalen Grades erzeugt (Beweis von Satz 2.4.15) Dies beweist (a). Mit dem Homomorphiesatz folgt $K[X]/(\min_{a/K}(X)) \cong_K K[a]$. Als Unterring von L ist $K[a]$ ein Integritätsbereich, also ist $(\min_{a/K})$ Primideal und damit einerseits $\min_{a/K}$ irreduzibel, andererseits nach Satz 2.4.18 $(\min_{a/K})$ maximales Ideal und somit $K[a]$ ein Körper.

(c),(d): Eine nicht-triviale Linearkombination von $1, a, \ldots, a^{n-1}$ ergäbe ein Polynom kleineren Grades als $\min_{a/K}$ mit Nullstelle a. Division mit Rest: jedes Polynom in $K[X]$ ist von der Form $Q \cdot \min_{a/K} + R$, wobei $R = 0$ oder Grad kleiner n hat. Also ist $K(a) = \text{Bild}(\text{eval}_a) = \{R(a) \mid R \in K[X], \text{Grad}(R) < n\}$ und $1, a, \ldots, a^{n-1}$ auch Erzeugendensystem. □

Beispiel 3.1.8 • $\sqrt[3]{2}$ ist algebraisch über $\mathbb{Q}$ mit Minimalpolynom $X^3 - 2$. Die Erweiterung $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$ hat Grad 3 über $\mathbb{Q}$.

- i ist algebraisch über $\mathbb{R}$ und hat Minimalpolynom $X^2 + 1$. Es ist also $\mathbb{C} := \mathbb{R}[\text{i}] = \mathbb{R}(\text{i})$ eine quadratische Erweiterung von $\mathbb{R}$.
- Sei α eine Lösung von $X^5 - 4X + 2 = 0$ in $\mathbb{C}$. Dann ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. Das Element α lässt sich nicht durch Wurzelausdrücke beschreiben.
- π ist transzendent über $\mathbb{Q}$ (Satz von Lindemann von 1882; die Hauptidee kam ihm bei einem Spaziergang über den Lorettoberg).
- Sei $K(X)$ der rationale Funktionenkörper über K. Dann ist $K(\sqrt{X}) = K(X)[\sqrt{X}]$ eine zu $K(X)$ isomorphe quadratische Erweiterung von $K(X)$.

Satz 3.1.9 *Sei $f \in K[X]$ irreduzibel. Dann gibt es bis auf Isomorphie über K einen eindeutig bestimmten Oberkörper von K, der von einer Nullstelle von f erzeugt ist, nämlich $K[X]/(f)$.*

Beweis: Sei $\pi : K[X] \to K[X]/(f)$ der natürliche Epimorphismus. Dann ist $f(\pi(X)) = \pi(f(X)) = 0 \in K[X]/(f)$, also ist $\pi(X) \in K[X]/(f)$ eine Nullstelle von f.

Sei $a \in L \supseteq K$ eine Nullstelle von f. Dann gibt es den Ringhomomorphismus $\text{eval}_a : K[X] \to K(a) \subseteq L$ mit Kern $(\min_{a/K}) = (f)$, da $f(a) = 0$ und f irreduzibel ist. Also folgt $K[X]/(f) \cong_K K(a)$. □

Definition 3.1.10 *Ein Körper heißt **algebraisch abgeschlossen**, wenn jedes Polynom aus $K[X]$ in $K[X]$ in Linearfaktoren zerfällt, d.h. von der Form $a_0 \cdot (X - a_1) \cdot \ldots \cdot (X - a_n)$ für ein $n \in \mathbb{N}$ und $a_i \in K$ ist.*

Folgerung 3.1.11 *Jeder Körper hat einen algebraisch abgeschlossenen Oberkörper.*

Beweis: Es reicht zu zeigen, dass es zu jedem Körper K_i einen Oberkörper K_{i+1} gibt, in dem jedes Polynom aus $K_i[X]$ in Linearfaktoren zerfällt. Zu $K = K_0$ ist dann $\bigcup_{i \in \mathbb{N}} K_i$ ein algebraisch abgeschlossener Oberkörper. Dazu reicht es wiederum, zu jedem Körper L_i einen Oberkörper L_{i+1} zu finden, in dem jedes Polynom aus $L_i[X]$ eine Nullstelle hat. Dann ist erneut $\bigcup_{i \in \mathbb{N}} L_i$ ein Körper mit der Eigenschaft, dass jedes Polynom aus L_0 darin in Linearfaktoren zerfällt.

Um zu einem Körper L einen solchen Oberkörper zu finden, kann man entweder mit etwas Mengenlehrekenntnissen und transfiniter Induktion eine Aufzählung $(f_i)_{i<\kappa}$ der nicht-linearen irreduziblen Polynome aus $L[X]$ nehmen, und bildet induktiv $M_0 := L$, $M_{i+1} := M_i[X]/(f_i)$ und in Limesschritten $M_\lambda := \bigcup_{i<\lambda} M_i$. Dann ist M_κ der gewünschte Körper. (Für abzählbare Körper funktioniert dies auch ohne Mengenlehre).

Die Mengenlehre kann man durch Anwendung des sogenannten Zornschen Lemmas umgehen: Dadurch werden gewissermaßen alle Adjunktionen auf einmal durchgeführt.

Dazu betrachtet man den Polynomring $R := L[X_f \mid f \in L[X], f \text{ irreduzibel}]$ über L in so vielen Variablen, wie es irreduzible Polynome in $L[X]$ gibt. Darin gibt es das von allen $f(X_f)$ erzeugte Ideal I (das später erzwingen wird, dass X_f zu einer Nullstelle von f wird). Dies ist ein echtes

Ideal, denn andernfalls gäbe es eine Linearkombination $g_1 f_1(X_{f_1}) + \cdots + g_k f_k(X_{f_k}) = 1$ mit $g_i \in R$ und irreduziblen $f_i \in L[X]$. Nach Adjunktion von Nullstellen für alle f_i (in endlich vielen Schritten) kann man aber einen Oberkörper von L finden, in dem man den linken Ausdruck durch Einsetzen dieser Nullstellen annulieren kann und bekäme $0 = 1$: Widerspruch.

Nun kann man das Lemma von Zorn anwenden auf die durch Inklusion partiell geordneten echten Ideale von R, die I enthalten: Für jede aufsteigende Kette solcher Ideale ist die Vereinigung wieder ein Ideal, das I enthält und echt ist (denn es enthält nicht die Eins, da kein Ideal in der Kette sie enthält). Also gibt es ein maximales Element dieser partiellen Ordnung. Dies ist ein maximales Ideal $\mathfrak{m}$ des Ringes R. Dann ist $R/\mathfrak{m}$ ein Oberkörper von L, in dem jedes irreduzible Polynom $f \in L[X]$ eine Nullstelle $X_f + \mathfrak{m}$ hat. □

3.2 Algebraische Erweiterungen

Definition 3.2.1 *L/K heißt **algebraische Körpererweiterung**, falls jedes Element $a \in L$ algebraisch über K ist.*

Satz 3.2.2 *Äquivalent sind:*

(a) *L/K ist endlich.*

(b) *L/K ist algebraisch und L ist über K endlich erzeugt, d.h. $L = K(a_1, \ldots, a_n)$.*

(c) *L ist über K von endlich vielen algebraischen Elementen erzeugt.*

Beweis: (a)⇒(b): Wenn L/K endlich ist, so wähle induktiv $a_{i+1} \in L \setminus K(a_0, \ldots, a_i)$. Da dann $[K(a_0, \ldots, a_i) : K] \geqslant 2^i$, muss irgendwann $K(a_0, \ldots, a_i) = L$ gelten. Jedes $a \in L$ ist algebraisch über K, da $[K(a) : K] \leqslant [L : K]$.

(b)⇒(c) ist klar.

(c)⇒(a): Sei $L = K(a_1, \ldots, a_n)$ mit über K algebraischen a_i. Dann ist

$$\begin{aligned} [L : K] &= [K(a_1) : K] \cdot [K(a_1, a_2) : K(a_1)] \cdot \ldots \cdot [L : K(a_1, \ldots, a_{n-1}] \\ &\leqslant [K(a_1) : K] \cdot [K(a_2) : K] \qquad \cdot \ldots \cdot [K(a_n) : K] \leqslant \infty \end{aligned}$$

□

Folgerung 3.2.3 **(a)** *M/L und L/K algebraisch $\iff$ M/K algebraisch.*

(b) *Sind $a_1, \ldots, a_n \in L$ algebraisch über K und $\frac{P}{Q} \in K(X_1, \ldots, X_n)$ mit $Q(a_1, \ldots, a_n) \neq 0$, so ist $\frac{P(a_1, \ldots, a_n)}{Q(a_1, \ldots, a_n)}$ algebraisch über K. Insbesondere sind dies $a_1 \pm a_2$, $a_1 a_2$ und $\frac{a_1}{a_2}$ für $a_2 \neq 0$.*

Beweis: (a) „⇐“ ist klar.
„⇒“: Sei $a \in M$ und $c_0, \ldots, c_k$ die Koeffizienten von $\min_{a/L}$. Dann ist a algebraisch über $K(c_0, \ldots, c_k) \subseteq L$ und $K(c_0, \ldots, c_k)$ ist eine algebraische Erweiterung von K nach Satz 3.2.2. Damit ist auch

$$[K(a, c_0, \ldots, c_k) : K] = [K(a, c_0, \ldots, c_k) : K(c_0, \ldots, c_k)] \cdot [K(c_0, \ldots, c_k) : K]$$

endlich und somit a algebraisch über K.

(b) $\frac{P(a_1, \ldots, a_n)}{Q(a_1, \ldots, a_n)} \in K(a_1, \ldots, a_n)$ ist algebraisch nach Satz 3.2.2. □

Folgerung 3.2.4 *Sei L/K eine Körpererweiterung. Dann ist $\{a \in L \mid a$ algebraisch über $K\}$ ein Körper, der* ***relative algebraische Abschluss von*** *K* ***in*** *L.*

Definition 3.2.5 *L heißt* ***Zerfällungkörper von*** *$f \in K[X]$* ***über*** *K, falls f in $L[X]$ in Linearfaktoren zerfällt und L von den Nullstellen von f über K erzeugt wird, also $L = K(a_1, \ldots, a_n)$ und $f(X) = c \cdot (X - a_1) \cdots (X - a_n)$.*

Bemerkung: Ein Isomorphismus $\varphi : L_1 \to L_2$ setzt sich fort zu einem Isomorphismus zwischen den Polynomringen $L_1[X] \to L_2[X]$ mit $g = \sum_{i=0}^{k} c_i X^i \;\mapsto\; g^\varphi := \sum_{i=0}^{k} \varphi(c_i) X^i$.

Satz 3.2.6 *Zu jedem $f \in K[X]$, $f \neq 0$, existiert ein Zerfällungskörper über K. Er ist bis auf Isomorphie über K eindeutig bestimmt.*

Beweis: Die Existenz folgt durch iterierte Anwendung von Satz 3.1.9. (Es folgt damit auch, dass der Grad des Zerfällungskörpers höchstens $n!$ ist, falls n der Grad von f ist. Tatsächlich ist der Grad der Zerfällungskörpers sogar ein Teiler von $n!$, wie aus der Galois–Theorie leicht folgen wird.)

Eindeutigkeit: Seien $K(a_1, \ldots, a_n)$ und $K(b_1, \ldots, b_n)$ zwei Zerfällungskörper von f über K. Mit Satz 3.1.9 gibt es einen Isomorphismus $\varphi_1 : K(a_1) \to K(b_1)$ über K. Zerfällt $\frac{f(X)}{X-a_1}$ in irreduzible Faktoren $g_1(X), \ldots, g_k(X)$, so zerfällt also $\frac{f(X)}{X-b_1}$ in irreduzible Faktoren $g_1^{\varphi_1}(X), \ldots, g_k^{\varphi_1}(X)$. Ohne Einschränkung ist dann $K(a_1, a_2) \cong K(a_1)[X]/(g_1)$ und $K(b_1, b_2) \cong K(b_1)[X]/(g_1^{\varphi_1})$. Dann setzt sich φ_1 zu einem Isomorphismus $\varphi_2 : K(a_1, a_2) \to K(b_1, b_2)$ fort, indem man φ_1 zunächst irgendwie zu $K(a_1, a_2) \to L \supseteq K(b_1)$ fortsetzt. Es gilt dann $L \cong K(b_1)[X]/(g_1^{\varphi_1})$, und damit $L \cong_{K(b_1)} K(b_1, b_2)$ nach Satz 3.1.9. Induktiv erreicht man dann einen Isomorphismus $\varphi_n : K(a_1, \ldots, a_n) \to K(b_1, \ldots, b_n)$. □

Beispiel 3.2.7 • Sei $K = \mathbb{Q}$ und $f(X) = X^3 - 2$.
In $\mathbb{R}[X]$ gilt $X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$, und der letzte Faktor ist irreduzibel.
In $\mathbb{C}[X]$ gilt $X^3 - 2 = (X - \sqrt[3]{2})(X - \zeta_3\sqrt[3]{2})(X - \zeta_3^2\sqrt[3]{2})$, wobei ζ_3 eine primitive dritte Einheitswurzel ist, also $\zeta_3^3 = 1 \neq \zeta_3$, etwa $\zeta_3 = e^{\frac{2i\pi}{3}}$. Es ist $\zeta_3 \notin \mathbb{R}$. Also ist $\mathbb{Q}(\sqrt[3]{2})$ noch nicht der Zerfällungskörper von f über $\mathbb{Q}$, sondern $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ vom Grad 6 über $\mathbb{Q}$.

• Sei $K = \mathbb{Q}$ und $f(X) = X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$, der letzte Faktor ist irreduzibel in $\mathbb{Q}[X]$. Ist $\zeta_5 = e^{\frac{2i\pi}{5}} \in \mathbb{C}$ eine primitive 5-te Einheitswurzel, so sind $1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4$ die Nullstellen von f; also ist $\mathbb{Q}(\zeta_5)$ der Zerfällungskörper von f über $\mathbb{Q}$ vom Grad 4.

Lemma 3.2.8 *Gleichwertig sind:*

(a) *K ist algebraisch abgeschlossen.*

(b) *K ist relativ algebraisch abgeschlossen in allen Oberkörpern.*

(c) *K hat keine echten algebraischen Erweiterungen.*

Beweis: (a)⇒(b): Sei K algebraisch abgeschlossen, $K \subseteq L$ und $a \in L$ algebraisch über K. Dann zerfällt das Minimalpolynom $\min_{a/K}(X)$ in $K[X]$ in Linearfaktoren $X - a_i$. Da $\min_{a/K}(a) = 0$ ist $X - a$ ein Teiler von $\min_{a/K}(X)$. Aus der eindeutigen Primfaktorzerlegung folgt dann $a = a_i \in K$ für ein i.

(Mit diesem Argument sieht man auch, dass ein Polynom vom Grad n über einem Körper, und damit auch über einem Integritätsbereich, darin höchstens n Nullstellen hat.)

(b)⇒(c): Sei L/K algebraische Erweiterung. Nach Voraussetzung ist K der relative algebraische Abschluss von K in L, also $K = L$.

(c)⇒(a): Sei $f \in K[X]$ und L der Zerfällungskörper von f über K. Dann ist L eine algebraische Erweiterung von K, also gleich K. Also zerfällt f in $K[X]$ in Linearfaktoren. □

Definition 3.2.9 *L heißt **algebraischer Abschluss** von K, falls L algebraisch abgeschlossen und algebraische Erweiterung von K ist.*

Satz 3.2.10 *Jeder Körper K hat einen algebraischen Abschluss $\widetilde{K}$. Er ist bis auf Isomorphie über K eindeutig bestimmt.*

Beweis: Nach Folgerung 3.1.11 existiert ein algebraisch abgeschlossener Oberkörper von K. Sei $\widetilde{K}$ der relative algebraische Abschluss von K in L. Dann ist nach Definition $\widetilde{K}$ algebraisch über K. Ein Polynom $f \in K[X]$ zerfällt über L in Linearfaktoren, die Nullstellen sind aber algebraisch über K und liegen daher in $\widetilde{K}$: Also ist $\widetilde{K}$ auch algebraisch abgeschlossen.

Seien K_1, K_2 zwei algebraische Abschlüsse von K. Man betrachtet die Menge der Isomorphismen von Zwischenkörpern $\{\varphi \mid \varphi : L_1 \to L_2$ Isomorphismus über K, $K \subseteq L_i \subseteq K_i\}$. Diese ist durch „$\varphi \subseteq \varphi'$, falls φ durch φ' fortgesetzt wird“ partiell geordnet. Eine aufsteigende Kette hat, wie man leicht nachrechnet, als obere Schranke die kleinste gemeinsame Fortsetzung. Also gibt es mit dem Zornschen Lemma ein maximales Element $\varphi : L_1 \to L_2$.

Falls $L_1 \neq K_1$, so setze φ fort zu $L_1[X]/(\min_{a/L_1}(X)) \to L_2[X]/(\min^{\varphi}_{a/L_1}(X))$ für beliebiges $a \in L_1 \setminus K_1$: Dies ist ein Widerspruch zur Maximalität von φ. Also ist φ auf K_1 definiert. Mit dem gleichen Argument für φ^{-1} ist φ surjektiv. □

Folgerung 3.2.11 *Jede algebraische Erweiterung L/K lässt sich über K in $\widetilde{K}$ einbetten.*

Beweis: $\widetilde{L}$ ist auch ein algebraischer Abschluss von K, also gibt es einen Isomorphismus $\varphi : \widetilde{L} \to \widetilde{K}$ über K und $\varphi\,|_L$ ist die gesuchte Einbettung. □

Beispiel 3.2.12 • $\mathbb{C}$ ist der algebraische Abschluss von $\mathbb{R}$ (Beweis in Satz 3.5.6).
• $\mathbb{A} := \{x \in \mathbb{C} \mid x$ algebraisch über $\mathbb{Q}\}$, der **Körper der algebraischen Zahlen**, ist der algebraische Abschluss von $\mathbb{Q}$. Dieser Körper ist abzählbar, d.h. es gibt eine Bijektion $\mathbb{N} \to \mathbb{A}$. Dagegen sind $\mathbb{R}$ und $\mathbb{C}$ überabzählbar.

Bemerkung: Ein Element $a \in K$ heißt algebraisch/tranzendent, wenn es algebraisch bzw. transzendent über dem Primkörper von K ist.

3.2.13 [Anwendung: Konstruktionen mit Zirkel und Lineal] Man identifiziert auf die übliche Weise $\mathbb{C}$ mit $\mathbb{R}^2$. Sei $\{0, 1\} \subseteq A \subseteq \mathbb{C}$. Die **über A konstruierbaren Punkte** werden von der kleinsten Teilmenge von $\mathbb{C}$ gebildet, die A enthält und abgeschlossen ist bezüglich Schnittpunkten von Objekten der folgenden Art:
— Geraden durch konstruierbare Punkte,
— Kreise um konstruierbare Punkte, deren Radien Abstände zwischen konstruierbaren Punkten sind.

Die konstruierbaren Punkte sind genau die mit Zirkel und Lineal von den gegebenen Punkten in A aus konstruierbaren.

Satz 3.2.14 *Die über A konstruierbaren Punkte bilden einen Körper $\mathbb{Q}(A)^{\mathsf{qu}}$, den **quadratischen Abschluss** von $\mathbb{Q}(A)$, d.h. den kleinsten Teilkörper von $\mathbb{C}$, der A enthält und unter Quadratwurzeln abgeschlossen ist.*

Beweis: Konstruierbare Zahlen werden durch Lösungen quadratischer Gleichungen beschrieben. Wenn alle Zahlen in einem Körper Quadratwurzeln haben, besitzen alle quadratischen Gleichungen mit der üblichen Lösungsformel Nullstellen in dem Körper. Also gilt „$\subseteq$“.

Umgekehrt muss man sich überlegen, dass man mit Zirkel und Lineal komplexe Zahlen in der Gaussschen Ebene addieren, subtrahieren und multiplizieren sowie Kehrwerte bilden und Quadratwurzeln ziehen kann. (Hinweis: Addieren und Subtrahieren ist einfach. Den Rest macht man mit Polarkoordinaten. Für Multiplikation, Kehrwert und Wurzel muss man Winkel addieren, spiegeln und halbieren (einfach). Für die Multiplikation und Kehrwerte der Beträge nutzt man den Strahlensatz aus. Für die Wurzel eines Betrages $r > 1$ konstruiert man zunächst ein rechtwinkliges Dreieck mit Kathede $\frac{r-1}{2}$ und Hypotenuse $\frac{r+1}{2}$: die zweite Kathede hat dann die Länge $\sqrt{r}$. □

$\mathbb{Q}(A)^{\mathsf{qu}}$ entsteht durch sukzessive Adjunktion von Quadratwurzeln. Falls $c \in \mathbb{Q}(A)^{\mathsf{qu}}$, so gibt es also $b_1, \ldots, b_k$ mit $c \in \mathbb{Q}(A)(\sqrt{b_1})(\sqrt{b_2}) \ldots (\sqrt{b_k})$. Daraus folgt, dass der Grad von c über $\mathbb{Q}(A)$ ein Teiler von 2^k, also selbst eine Zweierpotenz ist.

Mit diesen Überlegungen kann man zeigen, dass einige berühmte altgriechische Probleme nicht lösbar sind:

(a) Würfelverdoppelung: Man konstruiere zu einer gegebenen Seitenlänge a eines Würfels die Seitenlänge eines Würfels mit doppeltem Volumen. Dies übersetzt sich in die Frage, ob $\sqrt[3]{2}$ konstruierbar ist. Das Minimalpolynom $X^3 - 2$ von $\sqrt[3]{2}$ hat Grad 3: also nein.

(b) Winkeldrittelung: Man drittele einen beliebigen gegebenen Winkel. Sei der Scheitel des Winkels im Ursprung und ein Schenkel auf der reellen Achse, und sei a der Schnittpunkt des zweiten Schenkels mit dem Einheitskreis. Dann fragt die Winkeldrittelung nach der Konstruierbarkeit von $\sqrt[3]{a}$. Für transzendentes a ist aber $\sqrt[3]{a} \notin \mathbb{Q}(a)$, hat also Grad 3 über $\mathbb{Q}(a)$, d.h. im allgemeinen kann man Winkel nicht mit Zirkel und Lineal dritteln (spezielle Winkel aber schon).

(c) Quadratur des Kreises: Man konstruiere zu einem gegebenen Kreisradius die Seitenlänge eines zum Kreis flächengleiches Quadrats. Dies geht nicht, da nach dem Satz von Lindemann π transzendent ist.

In diesem Zusammenhang interessant ist auch folgender Satz:

Satz 3.2.15 (Gauss) *Das reguläre n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^k p_1 \ldots p_k$ mit paarweise verschiedenen Fermatschen Primzahlen p_i.*

Fermatsche Primzahlen sind Primzahlen der Form $2^i + 1$. Man kennt $3, 5, 17, 257, 65537$ und weiß nicht, ob es weitere gibt oder gar unendlich viele.

Die Konstruktion des regulären n-Ecks läuft auf die Konstruierbarkeit der primitiven n-ten Einheitswurzel $\zeta_n = e^{\frac{2i\pi}{n}}$ hinaus. Die Körper $\mathbb{Q}(\zeta_n)$ heißen Kreisteilungskörper und werden in Abschnitt 3.6 näher behandelt, der Satz in 3.6.17 bewiesen.

3.3 Endliche Körper

Bemerkung 3.3.1 $\mathbb{F}_p$ ist $\mathbb{Z}/p\mathbb{Z}$ als Körper betrachtet. Die Elemente werden zukünftig einfach als $0, 1, \ldots, p-1$ geschrieben.

Erinnerung: Ist $g \in G$ abelsche Gruppe und $n \in \mathbb{N}$, so $ng := \underbrace{g + \cdots + g}_{n \text{ mal}}$ und $(-n)g = -(ng)$. Dies macht G zu einem $\mathbb{Z}$-Modul.

— Ist K Körper der Charakteristik 0, so ist $\mathbb{Z} \subseteq K$ und die Modul–Multiplikation stimmt mit der Körpermultiplikation überein.

— Ist $\operatorname{char}(K) = p > 0$ und $n = pk$, so $nx = k \cdot \underbrace{(1 + \cdots + 1)}_{p \text{ mal}} \cdot x = k \cdot 0 \cdot x = 0$.

Definition und Lemma 3.3.2 *Sei* $\operatorname{char}(K) = p > 0$. *Dann ist* $x \mapsto x^p$ *ein Körperendomorphismus, der* ***Frobenius(–Endomorphismus)*** Frob.

K heißt ***vollkommen*** *oder* ***perfekt****, falls der Frobenius surjektiv (also ein Automorphismus) ist. Körper der Charakteristik null heißen auch perfekt. Endliche Körper sind perfekt.*

Beweis: $(xy)^p = x^p y^p$ ist klar.

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \ldots \binom{p}{p-1} x y^{p-1} + y^p = x^p + y^p$$

da für $1 \leqslant k \leqslant p-1$ stets p ein Teiler des Binomialkoeffizients $\binom{p}{k}$ ist.

Körperhomomorphismen sind stets injektiv; injektive Abbildungen zwischen gleichmächtigen endlichen Mengen sind surjektiv. □

Definition 3.3.3 *Für ein Polynom* $f(X) = \sum_{i=0}^{n} c_i X^i \in K[X]$ *definiert man die* ***formale Ableitung*** $f'(X) = \sum_{i=1}^{n} i c_i X^{i-1}$. *Es gelten dann die üblichen Regeln:* $f' = 0 \iff f$ *konstant,* $(f+g)' = f' + g'$ *und* $(fg)' = f'g + fg'$.

Lemma 3.3.4 *f hat nur einfache Nullstellen in $\widetilde{K}$*
$\iff$ *keine Nullstelle von f ist Nullstelle von f' (in $\widetilde{K}$)*
$\iff$ *f und f' sind teilerfremd in $\widetilde{K}[X]$.*

Beweis: Falls $f(X) = c(X - a_1) \ldots (X - a_n)$, so $f'(X) = c \cdot \sum_{i=1} \prod_{j \neq i} (X - a_j)$. Man sieht: Ist $a_1 = a_2$ doppelte Nullstelle, so auch Nullstelle von f' und $X - a_1$ ist gemeinsamer Teiler. Haben f und f' einen gemeinsamen Teiler, o.E. ein Linearfaktor $X - a_i$, dann teilt $X - a_i$ auch $\prod_{j \neq i} (X - a_j)$, also folgt $a_i = a_j$ für ein $j \neq i$. □

Lemma 3.3.5 *Sei K ein Körper und $\alpha_i \in \operatorname{Aut}(K)$ für $i \in I$. Dann ist* $\operatorname{Fix}(\{\alpha_i \mid i \in I\}) := \{x \in K \mid \alpha_i(x) = x \text{ für alle } i \in I\}$ *ein Körper.*

Beweis: Ist $\alpha_i(x) = x$ und $\alpha_i(y) = y$, so auch $\alpha_i(x+y) = \alpha_i(x) + \alpha_i(y) = x + y$, ebenso für die anderen Körperoperationen. □

Satz 3.3.6 (Klassifikation der endlichen Körper) *Zu jeder Primzahl p und jedem $m > 0$ gibt es bis auf Isomorphie genau einen Körper $\mathbb{F}_{p^m}$ mit p^m Elementen, nämlich der Zerfällungskörper von $X^{p^m} - X$ über $\mathbb{F}_p$. Es gibt keine anderen endlichen Körper.*

BEWEIS: Ist K endlich, so ist der Primkörper auch endlich, also ein $\mathbb{F}_p$, und da K dann ein $\mathbb{F}_p$-Vektorraum ist, gilt $|K| = p^m$ für ein m. Dann gilt klarerweise $0^{p^m} = 0$, und für $a \in K^\times$ gilt $a^{p^m-1} = a^{|K^\times|} = 1$, also $a^{p^m} = a$. Für $K \subseteq \widetilde{\mathbb{F}_p}$ ist also $K = \{a \in \widetilde{\mathbb{F}_p} \mid a^{p^m} = a\}$, da alle Elemente von K Nullstellen von $X^{p^m} - X$ sind, das höchstens p^m Nullstellen hat.

Umgekehrt ist $\{a \in \widetilde{\mathbb{F}_p} \mid a^{p^m} = a\} = \mathrm{Fix}(\mathrm{Frob}^m)$ nach Lemma 3.3.5 ein Körper, und dann offensichtlich der Zerfällungskörper von $X^{p^m} - X$, der nach Lemma 3.3.4 p^m Elemente hat, da $(X^{p^m} - X)' = p^m X^{p^m-1} - 1 = -1$ keine Nullstellen hat. □

Bemerkung: Es gibt keine endlichen echten Schiefkörper (Satz von Wedderburn 3.6.18).

Lemma 3.3.7 *Innerhalb eines festen $\widetilde{\mathbb{F}_p}$ gilt:* $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n$.

BEWEIS: „⇒“: $\mathbb{F}_{p^n}$ ist ein $\mathbb{F}_{p^m}$-Vektorraum, also $p^n = (p^m)^k = p^{mk}$.

„⇐“: $X^{p^m} - X$ teilt $X^{p^n} - X = (X^{p^m} - X)(X^{p^n-p^m} + X^{p^n-2p^m+1} + \cdots + 1)$. □

Folgerung 3.3.8

(a) *Je zwei endliche Körpern gleicher Charakteristik $\mathbb{F}_{p^m}, \mathbb{F}_{p^n}$ können isomorph in einen gemeinsamen (endlichen) Oberkörper eingebettet werden; der kleinste ist $\mathbb{F}_{p^{\mathrm{kgV}(m,n)}}$.*

(b) *$\bigcup_{m>1} \mathbb{F}_{p^m}$ ist ein Körper und $\cong \widetilde{\mathbb{F}_p}$.*

(c) *$\widetilde{\mathbb{F}_p}$ ist vollkommen und hat keine zu sich selbst isomorphen echten Unterkörper.*

Bemerkung: Algebraisch abgeschlossene Körper sind stets perfekt. $\mathbb{F}_p(X_0, X_1, X_2, \dots)$ hat als echten zu sich selbst isomorphen Unterkörper $\mathbb{F}_p(X_1, X_2, \dots)$; dies gilt dann auch für die algebraischen Abschlüsse.

Bemerkung 3.3.9 **(a)** Sowohl die additive als auch die multiplikative Gruppe endlicher Körper sind wohlbekannt (vgl. Folgerung 1.3.8):

$$\begin{aligned} (\mathbb{F}_{p^m}, +) &\cong \underbrace{\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}}_{m \text{ mal}} \\ (\mathbb{F}_{p^m}^\times, \cdot) &\cong \mathbb{Z}/(p^m - 1)\mathbb{Z} \end{aligned}$$

Schwierig: wie passen beide Gruppenstrukturen als Körper zusammen?
Insbesondere sieht man: Ist g ein Erzeuger der multiplikativen Gruppe, so gilt $\mathbb{F}_p(g) = \mathbb{F}_{p^m}$. Endliche Körper sind also stets einfache Erweiterungen der Primkörper.

(b) Sind K, L Körper, so ist $K \times L$ kein Körper. Im allgemeinen kann man zwei Körper nicht in einen gemeinsamen Oberkörper einbetten (z.B. wenn die Charakteristiken verschieden sind). Sind $K, L \subseteq M$, so existiert der kleinste, beide enthaltende Unterkörper von M, das **Kompositum** $K \cdot L$ von K und L. Es gilt $K \cdot L = K(L) = L(K)$.

Lemma 3.3.10 *Es gilt:* $\mathrm{Aut}(\mathbb{F}_{p^m}) = \langle \mathrm{Frob} \rangle \cong \mathbb{Z}/m\mathbb{Z}$ *und* $\mathrm{Fix}(\langle \mathrm{Frob}^k \rangle) = \mathbb{F}_{p^k}$ *für $k \mid m$.*

BEWEIS: $\mathrm{Fix}(\langle \mathrm{Frob}^k \rangle) = \mathrm{Fix}(\mathrm{Frob}^k) = \{a \mid a^{p^k} = a\}$ besteht aus den Nullstellen von $X^{p^k} - X$, also aus $\mathbb{F}_{p^k}$. Insbesondere ist $\mathrm{Frob}^k \neq \mathrm{id}$ auf $\mathbb{F}_{p^m}$ für einen echten Teiler k von m. Da andererseits $\mathrm{Frob}^m = \mathrm{id}$ auf $\mathbb{F}_{p^m}$ ist, muss die Ordnung des Frobenius in $\mathrm{Aut}(\mathbb{F}_{p^m})$ ein Teiler von m sein. Also ist sie m und alle Automorphismen $\mathrm{id}, \mathrm{Frob}, \mathrm{Frob}^2, \dots, \mathrm{Frob}^{m-1}$ sind verschieden.

Sei nun $\mathbb{F}_{p^m} = \mathbb{F}_p(a)$. Dann ist ein $\alpha \in \mathrm{Aut}(\mathbb{F}_{p^m})$ bereits festgelegt durch $\alpha(a)$, das eine Nullstelle von $\min_{a/\mathbb{F}_p}$ sein muss. Dessen Grad ist aber $m = [\mathbb{F}_{p^m} : \mathbb{F}_p]$, es kann also höchstens m Automorphismen geben; somit errzeugt der Frobenius die Automorphismengruppe als zyklische Gruppe der Ordung m. □

Folgerung 3.3.11 (Spezialfall der Galois–Theorie) *Für $k \mid m$ gilt*

$$\mathrm{Aut}(\mathbb{F}_{p^m}/\mathbb{F}_{p^k}) := \{\alpha \in \mathrm{Aut}(\mathbb{F}_{p^m}) \mid \mathbb{F}_{p^k} \subseteq \mathrm{Fix}(\alpha)\} = \langle \mathrm{Frob}^k \rangle \cong \mathbb{Z}/\frac{m}{k}\mathbb{Z}.$$

Jeder Untergruppe G der Automorphismengruppe entspricht ein Zwischenkörper $\mathrm{Fix}(G)$ *und umgekehrt. Je größer die Gruppe, desto kleiner der Körper.*

$$\begin{array}{lccl} & \mathbb{F}_{p^m} & \{\mathrm{id}\} & = \mathrm{Aut}(\mathbb{F}_{p^m}/\mathbb{F}_{p^m}) \\ \text{Grad } \frac{m}{l} & | & | & \text{Index } \frac{m}{l} \\ & \mathbb{F}_{p^l} & \langle \mathrm{Frob}^l \rangle & = \mathrm{Aut}(\mathbb{F}_{p^m}/\mathbb{F}_{p^l}) \\ \text{Grad } \frac{l}{k} & | & | & \text{Index } \frac{l}{k} \\ & \mathbb{F}_{p^k} & \langle \mathrm{Frob}^k \rangle & = \mathrm{Aut}(\mathbb{F}_{p^m}/\mathbb{F}_{p^k}) \end{array}$$

3.4 Normale und separable Erweiterungen

Von nun an betrachten wir algebraische Erweiterungen L/K in einem festen algebraischen Abschluß $\widetilde{K}$.

Bemerkung 3.4.1 $\mathrm{Aut}(L/K)$, oder auch $\mathrm{Aut}_K(L)$ geschrieben, ist die Untergruppe $\left\{\alpha \in \mathrm{Aut}(L) \;\middle|\; \alpha|_K = \mathrm{id}\right\}$ von $\mathrm{Aut}(L)$.

Sind L_1/K und L_2/K zwei isomorphe Erweiterungen, $\alpha : L_1 \to L_2$ ein Isomorphismus über K, so lässt sich α wegen Satz 3.2.10 zu $\widetilde{\alpha} \in \mathrm{Aut}(\widetilde{K}/K)$ fortsetzen.

Sei $\min_{a/K}(X) = (X - a_1) \cdots (X - a_n)$ mit $a = a_1$. Dann heißen die a_i die **Konjugierten** von a über K. Jeder Isomorphismus $\alpha_i : K(a) \to K(a_i)$ über K setzt sich fort zu $\widetilde{\alpha_i} \in \mathrm{Aut}(\widetilde{K}/K)$. Umgekehrt ist $\beta(a)$ für $\beta \in \mathrm{Aut}(\widetilde{K}/K)$ eine Nullstelle von $\min^{\beta}_{a/K} = \min_{a/K}$, also $\beta(a) = a_i$ für ein i. Es gibt also soviele Bilder von $K(a)$ unter $\mathrm{Aut}(\widetilde{K}/K)$ wie Konjugierte von a über K.

Definition 3.4.2 *L/K heißt **normal**, falls jedes irreduzible $f \in K[X]$, das in L eine Nullstelle hat, alle seine Nullstellen in L hat, d.h. in $L[X]$ in Linearfaktoren zerfällt.*

*L heißt $\mathrm{Aut}(\widetilde{K}/K)$-**invariant**, falls $\alpha(L) = L$ für alle $\alpha \in \mathrm{Aut}(\widetilde{K}/K)$.*

Satz 3.4.3 *Für eine endliche Erweiterung L/K sind gleichwertig:*
(a) L/K ist normal;
(b) L ist $\mathrm{Aut}(\widetilde{K}/K)$-invariant;
(c) L ist Zerfällungskörper über K eines Polynoms $f \in K[X]$.

Beweis: (a)⇒(c):
Sei $L = K(b_1, \ldots, b_n)$, so ist L Zerfällungskörper von $\min_{b_1/K}(X) \cdots \min_{b_n/K}(X)$ über K.

(c)⇒(b): Sei $\alpha \in \mathrm{Aut}(\widetilde{K}/K)$. Dann ist $\alpha(L)$ ebenfalls ein Zerfällungskörper von f über K, also $L = \alpha(L) = K(a_1, \ldots, a_k)$ für $f(X) = c(X - a_1) \ldots (X - a_k)$.

(b)⇒(a): Sei $f \in K[X]$ irreduzibel mit Nullstellen $a \in L, a' \notin L$. Dann existiert nach Satz 3.1.9 ein Isomorphismus $\alpha : K(a) \to K(a')$ über K, der sich nach Bemerkung 3.4.1 zu $\widetilde{\alpha} \in \mathrm{Aut}(\widetilde{K}/K)$ fortsetzen lässt. Da $\widetilde{\alpha}(a) = a' \notin L$, ist L dann nicht $\mathrm{Aut}(\widetilde{K}/K)$-invariant. □

Folgerung 3.4.4 **(a)** *Ist L/K normal und $K \subseteq M \subseteq L$, so ist auch L/M normal.*

(b) *Zu jeder endlichen Erweiterung L/K existiert ein kleinster Oberkörper L' von L so, dass L'/K normal ist, die* ***normale Hülle*** *von L/K.*

Beweis: (a) L ist über M Zerfällungskörper des gleichen Polynoms wie über K.

(b) Falls $L = K(b_1, \ldots, b_n)$, so ist L' der Zerfällungskörper von $\min_{b_1/K}(X) \cdots \min_{b_n/K}(X)$ über K. □

Definition 3.4.5 **(a)** *Ein nicht-konstanten Polynom $f \in K[X]$ heißt* ***separabel****, falls f (in $\widetilde{K}$) nur einfache Nullstellen hat.*

(b) *$a \in \widetilde{K}$ heißt* ***separabel über*** *K, falls $\min_{a/K}$ separabel ist.*

(c) *Eine algebraische Erweiterung L/K heißt* ***separable Erweiterung****, falls alle $a \in L$ separabel über K sind.*

Bemerkung 3.4.6 Sei $K \subseteq L$ und $f, h \in K[X]$. Dann ist $g \in K[X]$ genau dann ein ggT von f und h in $K[X]$, wenn g ein ggT von f und h in $L[X]$ ist.

Beweis: Seien g_k und g_L ggT von f und h in $K[X]$ bzw. $L[X]$, also $g_K K[X] = fK[X] + hK[X]$ und $g_L L[X] = fL[X] + hL[X]$. Dann folgt $g_K \in fK[X] + hK[X] \subseteq fL[X] + hL[X] = g_L L[X]$. Andererseits ist $g_K \mid g_L$ in $L[X]$, da g_K in $L[X]$ ein gemeinsamer Teiler bleibt. Also gilt $g_L \in g_K L[X]$. Somit unterscheiden sich g_K und g_L nur um eine Einheit in L. □

Lemma 3.4.7 *Sei f irreduzibel in $K[X]$. Dann ist f genau dann nicht separabel, wenn K der Charakteristik $p \neq 0$ ist und $f(X) = g(X^p)$ für ein $g \in K[X]$.*

Beweis: „⇐“ Es ist dann $f' = 0$, also sind f und f' nicht teilerfremd.

„⇒“ Wenn f nicht separabel ist, so sind f und f' nach Lemma 3.3.4 nicht teilerfremd, mit ggT in $K[X]$ (Bemerkung 3.4.6). Da aber f irreduzibel ist, muss $\mathrm{ggT}(f, f') = f$ gelten, also $f' = 0$. Da f nicht konstant ist, bleibt nur die Möglichkeit $f(X) = g(X^p)$ mit $p = \mathrm{char}(K) \neq 0$. □

Folgerung 3.4.8 *Algebraische Erweiterungen vollkommener Körper sind separabel.*

Beweis: Nach Lemma 3.4.7 klar, falls die Charakteristik null ist. Im Falle der Charakteristik $p \neq 0$ sei $f(X) = a_0 + a_1 X^p + \cdots + a_n (X^p)^n$ nicht separabel. Da K vollkommen ist, existieren $b_i \in k$ mit $b_i^p = a_i$. Also ist $f(X) = b_0^p + b_1^p X^p + \cdots + b_n^p X^{pn} = (b_0 + b_1 X + \cdots + b_n X^n)^p$ im Widerspruch zur Irreduzibilität! □

Beispiel 3.4.9 Sei K der Charakteristik p und nicht vollkommen, etwa habe $a \in K$ keine p-te Wurzel in K. Dann ist $K[T]/(T^p - a)$ eine inseparable Erweiterung von K.

Definition 3.4.10 *Sei L/K endlich. Der* ***Separabilitätsgrad*** *$[L : K]_s$ ist die Anzahl der isomorphen Einbettungen von L über K in $\widetilde{K}$, also $\{\alpha|_L \mid \alpha \in \mathrm{Aut}(\widetilde{K}/K)\}$.*

Satz 3.4.11 **(a)** *Ist $K \subseteq L \subseteq M$, so $[M : K]_s = [M : L]_s \cdot [L : K]_s$.*

(b) $[L : K]_s \leqslant [L : K]$.

Beweis: (a) Jede Einbettung von M über K setzt sich zusammen aus einer Einbettung von L über K und einer isomorphen Kopie einer Einbettung von M über L.

(b) Mit Bemerkung 3.4.1 gilt: $[K(a) : K]_s$ = Zahl der Nullstellen von $\min_{a/K} \leqslant$ Grad von $\min_{a/K} = [K(a) : K]$. Im allgemeinen Fall zerlegt man eine endliche Erweiterung in einen Turm einfacher Erweiterungen und schließt mit (a) und Lemma 3.1.5. □

Insbesondere ist für eine endliche Erweiterung L/K die Anzahl der Bilder von L unter isomorphen Abbildungen in $\widetilde{K}$, also $\{\alpha(L) \mid \alpha \in \mathrm{Aut}(\widetilde{K}/K)\}$, endlich. Die Anzahl ist $[L : K]_s$ geteilt durch $|\mathrm{Aut}(L/K)|$ — beim Separabilitätsgrad zählen auch die verschiedenen Arten, wie L auf ein Bild abgebildet werden kann! Das Kompositium all dieser Bilder $\alpha(L)$ ist gerade die normale Hülle von L/K.

Satz 3.4.12 *Für eine endliche Erweiterung L/K sind gleichwertig:*
(a) L/K ist separabel;
(b) $L = K(a_1, \ldots, a_m)$, wobei alle a_i separabel über K sind;
(c) $[L : K]_s = [L : K]$.

Beweis: (a)⇒(b) ist klar.

Für $m = 1$ gilt ferner nach Bemerkung 3.4.1: a ist separabel über $K \iff [K(a) : K]_s$, also die Anzahl der Nullstellen von $\min_{a/K}$, ist gleich dem Grad von $\min_{a/K}$, also $[K(a) : K]$.

(b)⇒(c): a_{i+1} ist auch separabel über $K_i := K(a_1, \ldots, a_i)$, denn $\min_{a_{i+1}/K_i}$ teilt $\min_{a_{i+1}/K}$, hat also wie dieses keine doppelten Nullstellen. Dann gilt

$$[L : K]_s = [K_m : K_{m-1}]_s \cdot [K_2 : K_1]_s \cdot [K_1 : K]_s = [K_m : K_{m-1}] \cdot [K_2 : K_1] \cdot [K_1 : K] = [L : K].$$

(c)⇒(a): Sei $a \in L$. Mit Satz 3.4.11 und Lemma 3.1.5 folgt dann $[K(a) : K]_s = [K(a) : K]$, also ist a separabel über K. □

Folgerung 3.4.13 **(a)** *Sei $K \subseteq L \subseteq M$, so ist M/K genau dann separabel, wenn M/L und L/K separabel sind (mit den Sätzen 3.4.11 und 3.4.12 (c)).*

(b) $K^{sep} := \{a \in \widetilde{K} \mid a \text{ separabel über } K\}$ *ist ein Körper, der* ***separable Anschluss von*** K.

(c) *Jede Körpererweiterung L/K zerlegt sich in eine maximal separable Teilerweiterung $(L \cap K^{sep})/K$ und eine „rein inseprable“ Erweiterung $L/(L \cap K^{sep})$, d.h. ohne separable Elemente.*

Satz 3.4.14 (vom primitiven Element) *Endliche separable Erweiterungen sind einfach.*

Beispiel 3.4.15 $\mathbb{F}_p(\sqrt[p]{X}, \sqrt[p]{Y})/\mathbb{F}_p(X, Y)$ ist endlich, nicht separabel und nicht einfach.

Beweis von Satz 3.4.14: Falls K endlich, so ist L/K einfach nach Bemerkung 3.3.9. Sei also K unendlich. Ein Element $a \in L \setminus K$ ist genau dann ein primitives Element, wenn es nicht in einem echten Zwischenkörper M mit $K \subseteq M \subset L$ liegt (denn dann kann nicht $K(a) \neq L$ sein). Es reicht zu zeigen, dass es nur endlich viele Zwischenkörper M gibt, denn (Übung in

linearer Algebra) ein Vektorraum über einem unendlichen Körper ist nie Vereinigung endlich vieler echter Unterräume.

Betrachte zu einem Zwischenkörper M nun $A_M := \{\alpha|_L \mid \alpha \in \mathrm{Aut}(\widetilde{K}/M)\}$. Das nächste Lemma zeigt $M = \mathrm{Fix}(A_M)$, womit M durch A_M bestimmt ist. Da A_M Teilmenge von A_K ist, gibt es höchstens soviele Zwischenkörper wie Teilmengen von A_K, und $|A_K| = [L : K]_s$ ist endlich. □

Lemma 3.4.16 *Sei L'/K normal und separabel, $K \subseteq M \subseteq L'$. Dann $M = \mathrm{Fix}(\mathrm{Aut}(L'/M))$.*

Da L'/K normal ist, ist L' auch normal über M, und also besteht $\mathrm{Aut}(L'/M)$ gerade aus den Einschränkungen von $\mathrm{Aut}(\widetilde{K}/M)$ aus L'. Daher kann man das Lemma im Beweis von Satz 3.4.14 anwenden.

Beweis: Per Definition gilt $M \subseteq \mathrm{Fix}(\mathrm{Aut}(L'/M)) =: F$ und $\mathrm{Aut}(L'/M) = \mathrm{Aut}(L'/F)$. Da L'/K normal ist, so (Folgerung 3.4.4) auch L'/M und L'/F und es gilt daher $[L' : M]_s = |\mathrm{Aut}(L'/M)|$, ebenso für F statt M. Da L'/K separabel ist, so (Folgerung 3.4.13) auch L'/M und L'/F. Also ist $[L' : M] = [L' : M]_s = |\mathrm{Aut}(L'/M)| = |\mathrm{Aut}(L'/F)| = [L' : F]_s = [L' : F]$. Zusammen mit $M \subseteq F$ folgt $M = F$. □

3.5 Galois–Theorie

Definition 3.5.1 *Eine endliche Erweiterung L/K heißt **Galois–Erweiterung**, falls sie normal und separabel ist. Die Gruppe $\mathrm{Aut}(L/K)$ heißt dann **Galois–Gruppe** von L über K (und wird auch $\mathrm{Gal}(L/K)$ geschrieben).*

Bemerkung: Die Gruppe $\mathrm{Aut}(\widetilde{K}/K)$ heißt die **(absolute) Galois–Gruppe** von K.

Bemerkung 3.5.2 Sei $K \subseteq L \subseteq M$. Falls M/K galoissch ist, so auch M/L, aber L/K muss nicht galoissch sein (z.B. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$ und $M = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

Sind L/K und M/L galoissch, so muss M/K nicht galoissch sein (vgl. Übungen).

Satz 3.5.3 (Hauptsatz der Galois–Theorie) *Sei M/K eine Galois–Erweiterung. Dann gibt es eine inklusions–umkehrende Bijektion:*

$$\begin{array}{rcl} \textit{Zwischenkörper } L, \textit{ also } K \subseteq L \subseteq M & \longrightarrow & \textit{Untergruppen } G \leqslant \mathrm{Aut}(M/K) \\ L & \mapsto & \mathrm{Aut}(M/L) \\ \mathrm{Fix}(G) & \hookleftarrow & G \end{array}$$

Dabei gilt $[M : L] = |\mathrm{Aut}(M/L)|$ und $[L : K] = \big(\mathrm{Aut}(M/K) : \mathrm{Aut}(M/L)\big)$.

Beweis: Nach Lemma 3.4.16 gilt $L = \mathrm{Fix}(\mathrm{Aut}(M/L))$ und $[M : L] = |\mathrm{Aut}(M/L)|$. Es bleibt also nur noch zu zeigen, dass jede Untergruppe G von $\mathrm{Aut}(M/K)$ der Form $\mathrm{Aut}(M/L)$ ist für einen Zwischenkörper L. Wir setzen $L := \mathrm{Fix}(G)$, denn dies ist die einzige Möglichkeit, sofern der Satz stimmt. Dann gilt $G \leqslant \mathrm{Aut}(M/L)$.

Sei nun, mit dem Satz vom primitiven Element, $M = L(a)$ und setze $f(X) := \prod_{\alpha \in G} (X - \alpha(a))$. Dann gilt $f^\alpha = f$ für alle $\alpha \in G$, also liegen die Koeffizienten von f im Fixkörper von G, d.h. $f \in L[X]$. Da $f(a) = 0$ ist das Minimalpolynom von a über L ein Teiler von f. Dann gilt $|\mathrm{Aut}(M/L)| = [M : L] =$ der Grad von $\min_{a/L} \leqslant$ der Grad von $f = |G|$. □

Lemma 3.5.4 *Sei M/K galoissch und $K \subseteq L \subseteq M$. Dann ist L/K genau dann eine normale Erweiterung, wenn* $\mathrm{Aut}(M/L)$ *eine normale Untergruppe von* $\mathrm{Aut}(M/K)$ *ist. In diesem Fall ist* $\mathrm{Aut}(M/K)/\mathrm{Aut}(M/L) \cong \mathrm{Aut}(L/K)$ *durch* $\alpha \mapsto \alpha|_L$.

Beweis: Sei $\beta \in \mathrm{Aut}(M/K)$. Dann ist $\alpha \in \mathrm{Aut}(M/L) \iff \beta^{-1} \circ \alpha \circ \beta \in \mathrm{Aut}(M/\beta^{-1}(L))$, also $\mathrm{Aut}(M/L)^\beta = \mathrm{Aut}(M/\beta^{-1}(L))$ und mit Satz 3.5.3: $\mathrm{Aut}(M/L)^\beta = \mathrm{Aut}(M/L) \iff L = \beta^{-1}(L) \iff L = \beta(L)$.

Ist L/K normal, so gibt es den Einschränkungshomomorphismus $\mathrm{Aut}(M/K) \to \mathrm{Aut}(L/K)$, $\alpha \mapsto \alpha|_L$, der nach Bemerkung 3.4.1 surjektiv ist und dessen Kern gerade $\mathrm{Aut}(M/L)$ ist. □

Beispiel 3.5.5 Sei $K = \mathbb{Q}(X, Y)$ der rationale Funktionenkörper über $\mathbb{Q}$ in zwei Variablen, sei $L = \mathbb{Q}(\sqrt{X}, \sqrt{Y})$ der Zerfällungskörper von $(T^2 - X)(T^2 - Y)$. Die Galois–Gruppe ist $Z_2 \times Z_2$, denn es gibt drei echte Zwischenkörper: $\mathbb{Q}(X, \sqrt{Y})$, $\mathbb{Q}(\sqrt{X}, Y)$ und $\mathbb{Q}(X, Y, \sqrt{XY})$, alle normale Erweiterungen von K.

$\sqrt{X} + \sqrt{Y}$ ist ein primitves Element, denn zunächst gilt $\frac{1}{2}\big((\sqrt{X} + \sqrt{Y})^2 - X - Y\big) = \sqrt{XY} \in \mathbb{Q}(\sqrt{X} + \sqrt{Y})$, also auch $\frac{1}{Y-X}\big(\sqrt{XY}(\sqrt{X} + \sqrt{Y}) - X(\sqrt{X} + \sqrt{Y})\big) = \sqrt{X} \in \mathbb{Q}(\sqrt{X} + \sqrt{Y})$, was $\mathbb{Q}(\sqrt{X} + \sqrt{Y}) = \mathbb{Q}(\sqrt{X}, \sqrt{Y})$ impliziert.

Satz 3.5.6 (Fundamentalsatz der Algebra) $\mathbb{C} = \mathbb{R}[i] := \mathbb{R}[T]/(T^2 + 1)$ *ist algebraisch abgeschlossen.*

Beweis: Sei $K/\mathbb{C}$ endlich. Es ist zu zeigen, dass $K = \mathbb{C}$. Ohne Einschränkung (Folgerung 3.4.4) ist $K/\mathbb{C}$ galoissch. Sei $[K : \mathbb{R}] = 2^{n+1}u$ mit ungeradem u.

(1) Sei K' die normale Hülle von $K/\mathbb{R}$. Dann teilt u auch $[K' : \mathbb{R}]$. Sei G eine 2-Sylow–Gruppe von $\mathrm{Aut}(K'/\mathbb{R})$. Dann ist u ein Teiler von dem ungeraden Grad $[\mathrm{Fix}(G) : \mathbb{R}]$. Für jedes $a \in \mathrm{Fix}(G)$ ist $\min_{a/\mathbb{R}}$ ein irreduzibles Polynom ungeraden Grades, also linear, da alle ungeraden Polynome über $\mathbb{R}$ eine Nullstelle haben. Somit ist $\mathrm{Fix}(G) = \mathbb{R}$ und $u = 1$.

(2) Also ist $\mathrm{Aut}(K/\mathbb{C})$ eine 2-Gruppe und damit nach Beispiel 1.6.7 auflösbar. Wir nehmen nun $K \neq \mathbb{C}$ an. Dann ist die Kommutatorgruppe $\mathrm{Aut}(K/\mathbb{C})' \neq \mathrm{Aut}(K/\mathbb{C})$ und $K_0 := \mathrm{Fix}(\mathrm{Aut}(K/\mathbb{C})')$ eine echte normale Erweiterung von $\mathbb{C}$ mit abelscher Galois–Gruppe

$$\mathrm{Aut}(K_0/\mathbb{C}) \cong \mathrm{Aut}(K/\mathbb{C})/\mathrm{Aut}(K/\mathbb{C})'.$$

(3) $\mathrm{Aut}(K_0/\mathbb{C})$ ist nach dem Hauptsatz über endlich erzeugte Gruppen ein Produkt zyklischer 2-Gruppen, also etwa $\cong Z_{2^m} \times C$. Dann gibt es einen Normalteiler $H \cong Z_{2^{m-1}} \times C$ vom Index 2, und $\mathrm{Fix}(H)$ ist eine quadratische Erweiterung von $\mathbb{C}$.

(4) In $\mathbb{R}$ hat jede positive Zahl eine Quadratwurzel. Daraus errechnet man leicht, dass man in $\mathbb{C}$ aus jeder Zahl eine Quadratwurzel ziehen kann. Mit der Lösungsformel für quadratische Gleichungen folgt daraus, dass über $\mathbb{C}$ jede quadratische Gleichung in Linearfaktoren zerfällt und also $\mathbb{C}$ keine quadratischen Erweiterungen hat: Widerspruch! □

Bemerkung 3.5.7 • Der Beweis benutzt nur, dass $(\mathbb{R}, \leqslant)$ ein angeordneter Körper ist, in dem jedes positive Element eine Quadratwurzel und jedes Polynom ungeraden Grades eine Nullstelle hat. Körper R mit dieser Eigenschaft heißen **reell abgeschlossene Körper**. Dann ist $R[i] := R[T]/(T^2 + 1)$ ein algebraisch abgeschlossener Körper.

- Falls L/K endlich ist und L algebraisch abgeschlossen, so ist entweder $L = K$ oder $[L : K] = 2$, K ist reell abgeschlossen und $L = K[i]$ (Artin–Schreier–Theorie).
- Es gibt Unterkörper R von $\mathbb{C}$ mit $[\mathbb{C} : R] = 2$, die aber nicht isomorph zu den reellen Zahlen sind (sogar unendlich viele Isomorphietypen). Falls $R \cong \mathbb{R}$, so gibt es immer noch unendlich viele Möglichkeiten für R.

Bemerkung 3.5.8 **(a)** Sei L/K galoissch, $a \in L$ vom Grad n über K, und sei $\{a_1, \ldots, a_n\} = \{\alpha(a) \mid \alpha \in \mathrm{Aut}(L/K)\}$ die Menge der n Konjugierten von a. Dann ist

$$\min_{a/K}(X) = (X - a_1) \cdots (X - a_n) = X - c_{n-1}X^{n-1} + c_{n-2}X^{n-2} - + \cdots + (-1)^n c_0.$$

Die Koeffizienten c_i sind die **elementar–symmetrischen Funktionen** in den a_i: c_i besteht aus allen Summen von Produkten von $n-i$ der Konjugierten $a_1, \ldots, a_n$. Insbesondere ist

$$\begin{aligned} c_{n-1} = a_1 + \cdots + a_n &= \sum_{\alpha \in \mathrm{Aut}(L/K)} \alpha(a) \\ c_0 \;=\; a_1 \cdot \cdots \cdot a_n &= \prod_{\alpha \in \mathrm{Aut}(L/K)} \alpha(a) \end{aligned}$$

(b) Sei $f \in K[X]$ vom Grad n und L der Zerfällungskörper von f über K. Ist f separabel, so ist die Erweiterung L/K galoissch und die Galois–Gruppe operiert treu auf den Nullstellen von f, d.h. bis auf Isomorphie ist $\mathrm{Aut}(L/K)$ eine Untergruppe von $\mathrm{Sym}(n)$. Ist f irreduzibel, so operiert $\mathrm{Aut}(L/K)$ transitiv auf den Nullstellen.

3.6 Einheitswurzeln und Radikalerweiterungen

Bemerkung 3.6.1 Eine Galois–Erweiterung heißt **zyklisch / abelsch / auflösbar**, falls die zugehörige Galois–Gruppe diese Eigenschaft hat.

Definition und Bemerkung 3.6.2 Sei K ein Körper, $n \geqslant 1$. Ein Element $a \in K$ heißt dann **n-te Einheitswurzel**, falls $a^n = 1$ gilt. Die n-ten Einheitswurzeln sind die Nullstellen des Polynoms $X^n - 1$, also gibt es höchstens n n-te Einheitswurzeln. Sie bilden eine endliche multiplikative Untergruppe $\mu_n(K)$ von $K^\times$, die also zyklisch ist (Folgerung 1.3.8).

1. Fall: Die Charakterisik von K teilt n nicht.

Dann ist das Polynom $X^n - 1$ separabel, es gibt in $\widetilde{K}$ n verschiedene n-te Einheitswurzeln und $\mu_n(\widetilde{K}) \cong Z_n$. Die Erzeuger von $\mu_n(\widetilde{K})$ heißen dann **primitive n-te Einheitswurzeln**, ihre Anzahl ist $\varphi(n)$. Dies sind genau die n-ten Einheitswurzeln in $\widetilde{K}$ der Ordnung n.

In $\mathbb{C}$ bilden die n-ten Einheitswurzeln die Ecken eines regulären n-Ecks auf dem Einheitskreis. Diese Ecken sind die $e^{\frac{2\pi i k}{n}}$ für $k = 0, \ldots, n-1$, und die primitiven Einheitswurzeln darunter sind genau die mit $\mathrm{ggT}(k, n) = 1$.

1. Fall: Die Charakterisik von K ist $p \neq 0$ und $n = p^k m$ mit $p \nmid m$.

Dann hat $X^n - 1 = (X^m - 1)^{p^k}$ m verschiedene Nullstellen (denn $X^m - 1$ ist separabel), jede mit Vielfachheit p^k. Also gilt $\mu_n(\widetilde{K}) \cong Z_m$.

Stets gilt $\mu_l(K) \subseteq \mu_n(K) \iff l \mid n$.

Die **Einheitengruppe von** K ist

$$\mu(K) := \bigcup_{n \geqslant 1} \mu_n(K) = \{a \in K \mid a^n = 1 \text{ für ein } n \geqslant 1\} \leqslant K^\times.$$

Von nun an sei ζ_n stets eine primitive n-te Einheitswurzel in $\widetilde{K}$. Wenn ζ_n auftritt, ist stets $\mathrm{char}(K) \nmid n$ vorausgesetzt!

Lemma 3.6.3 *$K(\zeta_n)/K$ ist eine abelsche Galois–Erweiterung und $\mathrm{Aut}(K(\zeta_n)/K)$ bettet sich in $(\mathbb{Z}/n\mathbb{Z})^*$ ein.*

Beweis: Da ζ_n eine primitive n-te Einheitswurzel ist, enthält $K(\zeta_n)$ alle n-ten Einheitswurzeln, ist also Zerfällungskörper von $X^n - 1$ über K. Nach der impliziten Voraussetzung $\mathrm{char}(K) \nmid n$ ist $X^n - 1$ separabel.

$\alpha \in \mathrm{Aut}(K(\zeta_n)/K)$ ist festgelegt durch $\alpha(\zeta_n) \in \mu_n(\widetilde{K}) = \mu_n(K(\zeta_n))$. Es gibt daher einen injektiven Homomorphismus

$$\begin{aligned} \mathrm{Aut}(K(\zeta_n)/K) \to \mathrm{Aut}(\mu_n(\widetilde{K})) \;\cong\; \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \;\cong\; (\mathbb{Z}/n\mathbb{Z})^* \\ \alpha \mapsto \alpha \restriction_{\mu_n(\widetilde{K})} \end{aligned}$$

und diese Gruppe ist abelsch (siehe Folgerung nach Lemma 1.2.8). □

Lemma 3.6.4 *Sei $a \notin K$, aber $a^n = b \in K$ mit $\mathrm{char}(K) \nmid n$. Dann ist $K(a)$ genau dann der Zerfällungskörper von $X^n - b$ über K, wenn $\zeta_n \in K(a)$. In diesem Fall gilt*

$$X^n - b = (X - a)(X - \zeta_n a)(X - \zeta_n^2 a) \cdots (X - \zeta_n^{n-1} a)$$

und die Erweiterung ist zyklisch. Die Zwischenkörper sind von der Form $K(a^k)$ für die Teiler k von n.

Beweis: „⇐“: $(\zeta_n^i a)^n = (\zeta_n^n)^i a^n = 1^i b = b$, und für $0 \leqslant i < j \leqslant n-1$ ist $\frac{\zeta_n^j a}{\zeta_n^i a} = \zeta_n^{j-i} \neq 1$, also $\zeta_n^j a \neq \zeta_n^i a$. Damit sieht man die Zerlegung des Polynoms, und dass $K(a)$ der Zerfällungskörper ist. Die Erweiterung ist also galoissch. Jeder Automorphismus $\alpha \in \mathrm{Aut}(K(a)/K)$ ist festgelegt durch $a \mapsto \zeta_n^i a$, die Abbildung $\alpha \mapsto i$ ergibt eine Injektion der Galois–Gruppe in Z_n, also ist die Erweiterung zyklisch. Die $K(a^k)$ sind klarerweise Zwischenkörper (nicht notwendig paarweise verschieden, nur wenn n minimal ist mit $a^n \in K$), und da es zu jedem Teiler von n genau eine Untergruppe von Z_n gibt, gibt es keine weiteren.

„⇒“: $X^n - b$ ist separabel. Seien a, a' zwei verschiedene Nullstellen. Dann ist $(\frac{a}{a'})^n = \frac{b}{b} = 1$, also ist $\frac{a}{a'}$ eine n-te Einheitswurzel. Wenn a' die Nullstellen von $X^n - b$ durchläuft, erhält man n verschiedene n-te Einheitswurzeln, also auch eine primitive. □

Insbesondere gilt in dem Spezialfall $b = 1$ und $a = \zeta_n$:

$$X^n - 1 \;=\; (X - 1)(X - \zeta_n)(X - \zeta_n^2) \cdots (X - \zeta_n^{n-1})$$

Satz 3.6.5 *Sei q eine Primzahl $\neq \mathrm{char}(K)$ und $\zeta_q \in K$. Für eine Erweiterung L/K sind dann gleichwertig:*

(a) *L/K ist galois'sch und $\mathrm{Aut}(L/K) \cong Z_q$;*

(b) *L/K ist galois'sch und $[L:K]=q$;*

(c) *es gibt ein $a\in L$ mit $L=K(a)$ und $a^q\in K$, d.h. L entsteht aus K durch Adjunktion eine q-ten Wurzel.*

Bemerkung: (a)$\Leftrightarrow$(c) gilt allgemeiner für $\mathrm{char}(K)\nmid n$ und $\zeta_n\in K$.

Beweis: (c)$\Rightarrow$(b) ist klar und (b)$\Rightarrow$(a) ist leicht: Die Galois–Gruppe $\mathrm{Aut}(L/K)$ hat Ordnung q, ist also isomorph zu Z_q, da q prim.

(a)$\Rightarrow$(c): Sei $\mathrm{Aut}(L/K)=\langle\alpha\rangle$ und $c\in L\setminus K$. Setze $c_i:=\alpha^i(c)$ für $i=0,\dots,q-1$ und $f(X):=c_0+c_1X+\cdots+c_{q-1}X^{q-1}\notin K[X]$.

Wenn an allen q q-ten Einheitswurzeln $\zeta\in K$ auch $f(\zeta)\in K$ gelten würde, so gäbe nach dem Interpolationssatz ein Polynom $g\in K[X]$ vom Grad höchstens $q-1$ mit $g(\zeta)=f(\zeta)$ für alle q Wahlen von ζ. Dann folgt aus Gradgründen aber $g=f$. Also gibt es ζ mit $a:=f(\zeta)\notin K$.

Dann gilt $L=K(a)$, da der Grad der Erweiterung prim ist, und da $\zeta\in K=\mathrm{Fix}(\alpha)$, folgt

$$\begin{aligned}\alpha(a)&=\alpha(c_0+c_1\zeta+\cdots+c_{q-1}\zeta^{q-1})\\&=\alpha(c_0)+\alpha(c_1)\zeta+\cdots+\alpha(c_{q-1})\zeta^{q-1}\\&=c_1+c_2\zeta+\cdots+c_{q-1}\zeta^{q-2}+c_0\zeta^{q-1}\\&=(c_0+c_1\zeta+\cdots+c_{q-1}\zeta^{q-1})\zeta^{-1}\;=\;a\zeta^{-1}\end{aligned}$$

Mithin ist $\alpha(a^q)=\alpha(a)^q=(a\zeta^{-1})^q=a^q$, wodurch $a^q\in K$ gezeigt ist. □

Definition 3.6.6 **(a)** *L/K heißt **Radikalerweiterung**, falls L aus K durch sukzessive Adjunktion von Wurzeln entsteht, d.h. $L=K(a_1,\dots,a_n)$ mit $a_i^{n_i}\in K(a_1,\dots,a_{i-1})$ für alle i und geeignete n_i.*

(b) *Für $f\in K[X]$ heißt **die Gleichung** $f(X)=0$ **auflösbar** (über K), falls der Zerfällungskörper von f über K in einer Radikalerweiterung enthalten ist.*

Ist die Gleichung $f(X)=0$ auflösbar, so sind die Nullstellen von f aus den Koeffizienten von f mit den Körperoperationen und Wurzeln ausdrückbar.

Klar ist aus der Defnition, dass für $K\subseteq L\subseteq M$ gilt: sind M/L und L/K Radikalerweiterungen so auch M/K. Ist M/K Radikalerweiterung, so auch M/L.

Beispiel 3.6.7 • $\mathbb{Q}\Big(\sqrt[3]{2},\sqrt{5+\sqrt[3]{2}},\sqrt[5]{\sqrt[3]{2}-\frac{1}{3}\sqrt{5+\sqrt[3]{2}}}\Big)/\mathbb{Q}$ ist eine Radikalerweiterung, ebenso $K(\zeta_n)/K$.

• $aX^2+bX+c=0$ ist für $\mathrm{char}K\neq 2$ auflösbar, da die Nullstellen in $K(\sqrt{b^2-4ac})$ liegen.

Satz 3.6.8 *Sei $\mathrm{char}(K)=0$, $f\in K[X]$ und L der Zerfällungskörper von f über K. Dann gilt: $f(X)=0$ ist auflösbar $\iff$ $\mathrm{Aut}(L/K)=:\mathrm{Gal}(f/K)$ ist eine auflösbare Gruppe.*

Beweis: „$\Rightarrow$“: Sei $L\subseteq M$ eine Radikalerweiterung von K. Die normale Hülle M' von M/K ist als Kompositum endlich vieler isomorphe Bilder von M/K ein Kompositum endlich vieler Radikalerweiterungen über K, also selbst eine Radikalerweiterungen über K. Sei also $M'=K(a_1,\dots,a_n)$ mit $a_i^{k_i}\in K(a_1,\dots,a_{i-1})$. Ohne Einschränkung sind alle k_i Primzahlen (da $a^{lm}=(a^l)^m$). Sei $k:=\mathrm{kgV}(k_1,\dots,k_n)$. Dann sind alle Erweiterungsschritte in dem Erweiterungsturm

$$K\subseteq K(\zeta_k)\subseteq K(\zeta_k,a_1)\subseteq K(\zeta_k,a_1,a_2)\subseteq\cdots\subseteq K(\zeta_k,a_1,\dots,a_n)=M'(\zeta_k)$$

galoissch mit abelscher Galois–Gruppe (nach Lemma 3.6.3 und Lemma 3.6.4), außerdem ist die Gesamterweiterung $M'(\zeta_k)/K$ galoissch. Mit Lemma 3.5.4 sind also die Gruppen

$$\mathrm{Aut}(M'(\zeta_k)/K(\zeta_k))/\mathrm{Aut}(M'(\zeta_k)/K) \text{ und}$$
$$\mathrm{Aut}(M'(\zeta_k)/K(\zeta_k,a_1,\ldots,a_{i-1}))/\mathrm{Aut}(M'(\zeta_k)/K(\zeta_k,a_1,\ldots,a_i)) \text{ für alle } i=1,\ldots,n$$

abelsch. Somit ist nach Satz 1.6.12 die Gruppe $\mathrm{Aut}(M'(\zeta_k)/K)$ auflösbar und damit auch $\mathrm{Aut}(L/K) = \mathrm{Aut}(M'(\zeta_k)/K)/\mathrm{Aut}(M'(\zeta_k)/L)$.

„$\Leftarrow$“: Sei $\mathrm{Aut}(L/K)$ auflösbar, also gibt es eine Kompositionsreihe

$$\{\mathrm{id}\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_k = \mathrm{Aut}(L/K)$$

mit einfachen abelschen Faktoren, also zyklisch von Primzahlordnung. Sei $L_i := \mathrm{Fix}(H_i)$, dann ist $L = L_0 \supseteq L_1 \supseteq \cdots \supseteq L_k = K$ ein Turm zyklischer Erweiterungen. Setze $n := \mathrm{kgV}([L_0 : L_1],\ldots,[L_{k-1} : L_k])$ und betrachte einerseits die zyklische Radikalerweiterung $L_k(\zeta_n)/L_k$, andererseits die Erweiterungen $L_i(\zeta_n)/L_{i+1}(\zeta_n)$. Es reicht nun zu zeigen, dass auch diese zyklische Radikalerweiterungen sind, denn dann ist L in der Radikalerweiterung $L(\zeta_n)$ von K enthalten.

Zum einen ist $L_i(\zeta_n)$ Zerfällungskörper des gleichen Polynoms über $L_{i+1}(\zeta_n)$ wie L_i über L_{i+1}; die Erweiterungen sind also galoissch. Zum andern definiert

$$\varphi : \mathrm{Aut}(L_i(\zeta_n)/L_{i+1}(\zeta_n)) \to \mathrm{Aut}(L_i/L_{i+1})$$
$$\alpha \mapsto \alpha|_{L_i}$$

einen injektiven Homomorphismus (definiert ist die Abbildung, da L_i/L_{i+1} normal ist, und injektiv, da ζ_n festgelassen wird, ein Automorphismus in $\mathrm{Aut}(L_i(\zeta_n)/L_{i+1}(\zeta_n))$ also durch $\alpha|_{L_i}$ festgelegt ist), somit ist $\mathrm{Aut}(L_i(\zeta_n)/L_{i+1}(\zeta_n))$ als Untergruppe einer zyklischen Gruppe selbst zyklisch. □

Folgerung 3.6.9 *Gleichungen von Grad $\leqslant 4$ sind auflösbar, denn dann ist $\mathrm{Gal}(f/K) \leqslant S_4$ und S_4 ist auflösbar.*

Lemma 3.6.10 *Sei $p \geqslant 3$ Primzahl, $f \in \mathbb{Q}[X]$ irreduzibel vom Grad p mit $p-2$ reellen Nullstellen und 2 nicht reellen (also konjugiert komplexen) Nullstellen. Dann ist $\mathrm{Gal}(f/\mathbb{Q}) = \mathrm{Sym}(p)$.*

Beweis: Es gilt $G := \mathrm{Gal}(f/\mathbb{Q}) \leqslant \mathrm{Sym}(p)$. Da der Zerfällungskörper L von f über Q die Teilerweiterung $\mathbb{Q}[T]/(f)$ vom Grad p enthält, ist p ein Teiler von $[L : \mathbb{Q}]$ und somit enthält G nach dem Satz von Cauchy ein Element g der Ordnung p. Dann ist g ein p-Zykel (weil p eine Primzahl ist). Außerdem operiert die komplexe Konjugation auf den Nullstellen wie eine Transposition τ.

Nun gilt, dass ein p-Zykel und eine Transposition $\mathrm{Sym}(p)$ erzeugen: Die Transposition ist ohne Einschränkung $(1,2)$, und eine gewisse Potenz der p-Zykels ist dann von der Form $(1,2,\ldots)$, also ist g ohne Einschränkung $(1,2,\ldots,p)$. Dann ist aber auch $(1,2,\ldots,p)^k \circ (1,2) \circ (1,2,\ldots,p)^{-k} = (1+k, 2+k) \in G$, und man sieht sofort, dass $(1,2),(2,3),\ldots,(p-1,p)$ die $\mathrm{Sym}(p)$ erzeugen. □

Beispiel 3.6.11 Sei $f(X) = X^5 - 6X + 3$. Dann ist $f(X) = 0$ über $\mathbb{Q}$ nicht auflösbar (denn f ist irreduzibel z.B. mit dem Eisensteinschen Kriterium und erfüllt die Bedingungen von Lemma 3.6.10, wie man mit elementarer Analysis leicht nachrechnet).

3.6.12 [Symmetrische Polynome und die allgemeine Gleichung]

Seien $t_1, \ldots, t_n$ verschiedene Variablen; sei in $K(t_1, \ldots, t_n)[X]$

$$f(X) = (X - t_1)(X - t_2)\ldots(X - t_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - + \cdots + (-1)^n s_n$$

Dabei sind die $s_i = s_i(t_1, \ldots, t_n) \in K[t_1, \ldots, t_n]$ die elementar–symmetrischen Funktionen in $t_1, \ldots, t_n$.

$K(t_1, \ldots, t_n)/K(s_1, \ldots, s_n)$ ist galoissch mit Galois–Gruppe S_n, denn $K(t_1, \ldots, t_n)$ ist per Definition der Zerfällungskörper von f, das separabel ist, und jedes $\sigma \in S_n$ definiert einen Automorphismus $\widetilde{\sigma} \in \mathrm{Aut}(K(t_1, \ldots, t_n)/K(s_1, \ldots, s_n))$ mit $\widetilde{\sigma}|_K = \mathrm{id}$ und $\widetilde{\sigma}(t_i) = t_{\sigma(i)}$.

Folgerung 1: Falls $\mathrm{char}(K) = 0$ und $n \geqslant 5$, so ist die **allgemeiner Gleichung n-ten Grades** $f(X) = 0$ nicht auflösbar.

Folgerung 2: $\mathrm{Fix}(\mathrm{Aut}(K(t_1, \ldots, t_n)/K(s_1, \ldots, s_n))) = K(s_1, \ldots, s_n)$, also ist jede symmetrische rationale Funktion $r(t_1, \ldots, t_n)$ in den t_i (d.h. $r(t_1, \ldots, t_n) = r(t_{\sigma(1)}, \ldots, t_{\sigma(n)})$ für alle $\sigma \in \mathrm{Sym}(n)$) eine rationale Funktion in den elementar-symmetrischen Funktionen der t_i.

Der Hauptsatz über symmetrische Polynome besagt, dass auch jedes symmetrische Polynom in den t_i ein Polynom in den elementar-symmetrischen Funktionen der t_i ist.

Definition 3.6.13 **(a)** *Körper der Form $\mathbb{Q}(\zeta_n)$ heißen **Kreisteilungskörper**.*

(b) $\Phi_n(X) := \prod_{\substack{\zeta \text{ primitive} \\ n\text{-te EW}}} (X - \zeta)$ *ist das n-te **Kreisteilungspolynom**.*

$\Phi_n(X)$ hat Grad $\varphi(n)$. Es gilt offenbar $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

$$\begin{aligned} \Phi_1(X) &= X - 1 & \Phi_4(X) &= X^2 + 1 \\ \Phi_2(X) &= X + 1 & \Phi_5(X) &= X^4 + X^3 + X^2 + X + 1 \\ \Phi_3(X) &= X^2 + X + 1 & \Phi_6(X) &= X^2 - X + 1 \end{aligned}$$

Satz 3.6.14 *Es gilt $\Phi_n(X) \in \mathbb{Z}[X]$ und ist irreduzibel in $\mathbb{Q}[X]$. Somit ist $\Phi_n(X) = \min_{\zeta_n/\mathbb{Q}}(X)$, $[\mathbb{Q}(\zeta_n)/\mathbb{Q}] = \varphi(n)$ und $\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.*

Beweis: (1) $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ist galoissch (Lemma 3.6.3). Ein Automorphismus in der Galois–Gruppe muss primitive n-te Einheitswurzeln wieder auf primitive abbilden, also liegen die Koeffizienten von $\Phi_n(X)$ im Fixkörper $\mathbb{Q}$.

(2) Zeige nun per Induktion nach n, dass $\Phi_n(X) \in \mathbb{Z}[X]$ mit konstantem Term ± 1:

Es gilt $\Phi_n(X) \cdot \prod_{d|n, d \neq n} \Phi_d(X) = X^n - 1$. Per Induktion ist das Produkt in $\mathbb{Z}[X]$ mit konstantem Koeffizient ± 1. Ist $\Phi_n(X) = c_0 + c_1 X + \cdots + c_k X^k$ und das Produkt $= d_0 + d_1 X + \cdots + d_l X^l$, so gilt zum einen $c_0 d_0 = -1$, also ist $c_0 = -d_0$ ebenfalls ± 1. Für die anderen Koeffizienten folgt dann per Induktion nach i, dass $c_i = \frac{1}{d_0}(c_0 d_i + \cdots + c_{i-1} d_1) \in \mathbb{Z}$.

(3) Angenommen $\Phi_n(X) = q_1(X) \cdot q_2(X)$ mit $q_i(X) \in \mathbb{Q}[X]$ normiert und q_1 irreduzibel. Mit dem Lemma von Gauss sind $q_1, q_2 \in \mathbb{Z}[X]$. Sei ζ eine Nullstelle von q_1. Dann ist also $q_1 = \min_{\zeta/\mathbb{Q}}$. Es reicht nun zu zeigen, dass für alle $p \nmid n$ auch $q_1(\zeta^p) = 0$. Denn dann gilt auch $q_1(\zeta^k) = 0$ für jedes zu n teilerfremdes k (Primfaktorzerlegung von k!). Nun sind aber sämtliche primitiven n-ten Einheitswurzeln von der Form ζ^k für festes ζ und zu n teilerfremdem k, somit ist dann

$q_1 = \Phi_n$ irreduzibel vom Grad $\varphi(n)$. Die Injektion $\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ aus Lemma 3.6.3 ist damit auch surjektiv.

(4) Angenommen $q_1(\zeta^p) \neq 0$. Dann $q_2(\zeta^p) = 0$, also ist ζ Nullstelle von $q_2(X^p)$ und folglich $q_1(X) \mid q_2(X^p) = q_1(X) \cdot q_3(X)$ für $q_3(X) \in \mathbb{Z}[X]$ erneut nach dem Lemma von Gauss. Betrachte nun die Abbildung „modulo p“ $\mathbb{Z}[X] \to \mathbb{F}_p[X]$. Es gilt dann $\overline{q_1(X)} \cdot \overline{q_3(X)} = \overline{q_2(X^p)} = \overline{q_2(X)}^p$, denn $\overline{q_2} \in \mathbb{F}_p[X]$ hat seine Koeffizienten im Fixkörper des Frobenius. Also sind $\overline{q_1}, \overline{q_2}$ nicht teilerfremd, und somit ist $\overline{\Phi_n} = \overline{q_1} \cdot \overline{q_2}$ nicht separabel. Aber $\overline{\Phi_n} \mid \overline{X^n - 1} = X^n - \overline{1}$, das separabel ist: Widerspruch. □

Satz 3.6.15 *Sei $p \nmid n$. Dann ist $\mathbb{F}_p[\zeta_n] = \mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^{\varphi(n)}}$, wobei k minimal ist mit der Eigenschaft $p^k \equiv 1 \pmod{n}$.*

Beweis: Suche k minimal so, dass $X^n - 1 \mid X^{p^k} - X = X(X^{p^k - 1} - 1)$, also so, dass $n \mid p^k - 1$. Mit dem Satz von Euler gilt $p^{\varphi(n)} \equiv 1 \pmod{n}$, also $k \mid \varphi(n)$. □

Bemerkung 3.6.16 Sei $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ die Primfaktorzerlegung. Mit dem chinesischen Restsatz gilt

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z} \\ \text{also auch } (\mathbb{Z}/n\mathbb{Z})^* &\cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) * \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^* \\ \text{und somit } \varphi(n) &= \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}) \;=\; (p_1 - 1)p_1^{\alpha_1 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1} \end{aligned}$$

denn es gibt $\frac{p^\alpha}{p}$ viele Zahlen $\leqslant p^\alpha$, die durch p teilbar sind, wewegen $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.

Folgerung: φ ist multiplikativ für teilerfremde Zahlen.
Ist $\mathrm{ggT}(n, m) = 1$, so $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)] = \varphi(m)$.

3.6.17 [Konstruktion des regulären n-Ecks] (Beweis von Satz 3.2.15)

Wenn ζ_n konstruierbar ist, so ist $\varphi(\zeta_n)$ eine 2er Potenz, also (mit der Primfaktorzerlegung von oben) gilt $\alpha_i = 1$ für alle Primfaktoren $p_i \neq 2$, und diese sind von der Form $2^{n_i} + 1$.

Umgekehrt: Ist $\varphi(\zeta_n)$ eine 2er Potenz, so ist $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ abelsch vom Grad 2er Potenz. Die Galois–Gruppe ist als 2-Gruppe also auflösbar mit Kompositionsfaktoren $\mathbb{Z}/2\mathbb{Z}$. Die Fixkörper einer Kompositionereihe bilden einen Turm quadratischer Erweiterungen, welcher die Konstruierbarkeit von ζ_n zeigt.

Satz 3.6.18 (Wedderburn) *Sei D ein endlicher Schiefkörper. Dann ist D kommutativ.*

Beweis: Sei $Z(D) := \{d \in D \mid xd = dx \text{ für alle } x \in D\}$ das Zentrum von D und $C_D(a) := \{d \in D \mid ad = da\}$ der Zentralisator von $a \in D$. Man rechnet leicht nach, dass $C_D(a)$ ein Schiefkörper ist, also $Z(D) = \bigcap_{a \in D} C_D(a)$ sogar ein Körper, und dass D und $C_D(a)$ $Z(D)$-Vektorräume sind (vgl. Übung).

Sei $q := |Z(D)|$, $n := \dim_{Z(D)}(D)$ und $n_i := \dim_{Z(D)}(C_D(a_i))$. Mit der Klassengleichung 1.4.16 für $D^\times$ gilt dann

$$q^n - 1 = (q - 1) \;+\; \sum_{i \in I} \frac{q^n - 1}{q^{n_i} - 1},$$

wobei $(a_i)_{i\in I}$ ein Repräsentantensystem der nicht–zentralen Konjugationsklassen ist. Insbesondere folgt $n_i \mid n$. Nun gilt

$$\frac{q^n-1}{q^{n_i}-1} \;=\; \frac{\prod_{d|n}\Phi_d(q)}{\prod_{d|n_i}\Phi_d(q)} \;=\; \prod_{\substack{d|n\\ d\nmid n_i}}\Phi_d(q) \;=\; \Phi_n(q)\cdot z_i$$

mit einem $z_i \in \mathbb{Z}$. Also folgt

$$\Phi_n(q) \;\Big|\; q^n-1 \;=\; q-1+\Phi_n(q)\cdot\sum_{i\in I} z_i$$

und damit $\Phi_n(q) \mid q-1$ und $|\Phi_n(q)| \leqslant q-1$.

Falls $n>1$, so ist $|q-\zeta| > q-1$ für alle primitiven n-ten Einheitswurzeln ζ (denn $q \geqslant 2$). Dann aber ist $|\Phi_n(q)| \;=\; \prod_{\zeta \text{ prim. } n\text{-te EW}} |q-\zeta| \;>\; (q-1)^{\varphi(n)} \;\geqslant\; q-1$: Widerspruch! □

Sei p eine ungerade Primzahl. Dann hat $\mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$ eine eindeutige Untergruppe vom Index 2. Also gibt es eine eindeutige quadratische Erweiterung Q_p von $\mathbb{Q}$ innerhalb $\mathbb{Q}(\zeta_p)$ (denn quadratische Erweiterungen sind automatisch normal). Man überlegt sich ohne Schwierigkeiten, dass es dann eine eindeutig bestimmte quadratfreie ganze Zahl d_p gibt mit $Q_p = \mathbb{Q}(\sqrt{d_p})$.

Satz 3.6.19 $d_p = (-1)^{\frac{p-1}{2}}\cdot p$.

Beweis: Seien $\zeta_0, \zeta_1, \ldots, \zeta_{p-1}$ die p-ten Einheitswurzeln, $\zeta_0 = 1$. Dann ändert $\Delta = \prod_{i<j}(\zeta_i - \zeta_j)$ unter dem Erzeuger der Galois–Gruppe $\mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ das Vorzeichen, also ist $\Delta^2 \in \mathbb{Q}$ und $Q_p = \mathbb{Q}(\Delta)$. Nun gilt

$$\Delta^2 = (-1)^{\frac{p(p-1)}{2}}\prod_{i\neq j}(\zeta_i-\zeta_j) = (-1)^{\frac{p-1}{2}}\prod_{i=0}^{p-1}(X^p-1)'_{X=\zeta_i} = (-1)^{\frac{p-1}{2}}\prod_{i=0}^{p-1}p\zeta_i^{p-1} = (-1)^{\frac{p-1}{2}}p^p,$$

denn $\prod_{i=0}^{p-1}\zeta_i = 1$. Da p ungerade, ist also $d_p = (-1)^{\frac{p-1}{2}}\cdot p$. □

Es gilt nun die erstaunliche Beziehung

$$\sqrt{(-1)^{\frac{p-1}{2}}\cdot p} \;=\; \pm\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\cdot\zeta_p^a$$

wobei das Vorzeichen von der Wahl von ζ_p abhängt. Wenn man jetzt noch ein wenig weiterrechnet, ist das quadratische Reziprozitätsgesetz nicht mehr fern....

Literatur

Zur Algebra gibt es reichlich Bücher und Skripte; hier einige Empfehlungen:

- Serge Lang „Algebra“ (3. Auflage bei Addison–Wesley, 4. Auflage bei Springer)
- Falko Lorenz „Algebra I und II“ (BI)
- B. van der Waerden „Moderne Algebra“ (Springer),
  verschiedene Ausgaben auch unter dem Titel „Algebra“
- Algebra–Skript von Martin Ziegler
  `http://home.mathematik.uni-freiburg.de/ziegler/Skripte.html`

Weiterführendes zur Gruppentheorie:

- D. R. S. Robinson „A course in the theory of groups“ (Springer)
- H. Kurzweil, B. Stellmacher „Theorie der endlichen Gruppen“ (Springer)
- Mein Gruppentheorie–Skript (leider mit vielen Tippfehlern behaftet)
  `http://home.mathematik.uni-freiburg.de/junker/skripte.html`

Weiterführendes zur Ringtheorie:

- H. Matsumura „Commutative ring theory“ (Cambridge University Press)

Weiterführendes zur Körpertheorie:

- Emil Artin „Galois Theory“
- Antoine Chambert–Loir „A field guide to algebra“ (Springer)