Fakultät für Mathematik
Universität Bielefeld

Prof. Dr. William Crawley-Boevey
WS 2023/24

Algebra I

Vorlesungsskript lose basierend auf einem Skript von Dr. Andrew Hubery

Was ist Algebra? Wir werden studieren:

(1) Gruppen. Gruppen wurden bereits bei der Definition eines Vektorraums verwendet. Wir erfahren mehr über die Struktur von Gruppen.

(2) Gruppenaktionen und Anwendungen. Die wichtigste Verwendung von Gruppen besteht darin, Symmetrie zu verstehen. Dies ergibt sich aus der Idee einer Gruppenaktion.

(3) Ringe. Historisch gesehen ist Algebra die Manipulation von Gleichungen, um sie zu lösen. Besonders wichtig sind Polynomgleichungen. Ringe und Körper sind die mathematischen Objekte, an denen man dies verstehen kann.

(4) Faktorisierung. Jede positive ganze Zahl kann auf im Wesentlichen einzigartige Weise als Produkt von Primzahlen geschrieben werden. Einige Ringe, beispielsweise Polynomringe, haben eine analoge Eigenschaft.

(5) Körpererweiterungen. Anhand der Eigenschaften von Körpern können wir berühmte klassische Unmöglichkeiten demonstrieren, beispielsweise die Unmöglichkeit, Winkel mit Lineal und Zirkel zu dreiteilen.

(6) Galoistheorie. Dies ist die Verwendung von Symmetrie zur Untersuchung von Körpern. Als Anwendung: Es gibt eine bekannte Formel für die Nullstellen eines quadratischen Polynoms. Es gibt kompliziertere Versionen für Polynome vom Grad 3 oder 4. Anhand der Eigenschaften von Gruppen werden wir sehen, dass es für Polynome vom Grad 5 oder höher keine ähnliche Formel gibt.

Inhaltsverzeichnis

1 Gruppen

1.1 Definition und Beispiele

Erinnerung von LA I.

Definition. Eine **Gruppe** besteht aus eine Menge G zusammen mit einer Verknüpfung

$$* : G \times G \to G, \quad (g, h) \mapsto g * h,$$

sodass

(1) die Verknüpfung ist **assoziativ**, d.h. $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$,

(2) es gibt ein Element $e \in G$, genannt **neutrales Element**, für das gilt $e * a = a * e = a$ für alle $a \in G$, und

(3) zu jedem $a \in G$ gibt es ein Element $b \in G$, genannt **inverses Element zu** a, mit $a * b = b * a = e$

Die Gruppe heißt **kommutativ** oder **abelsch** falls $a * b = b * a$ für alle $a, b \in G$.

Wir bezeichnen die Gruppe mit $(G, *)$ oder G.

Die Mächtigkeit $|G|$ heißt auch die **Ordnung** der Gruppe G. Eine natürliche Zahl oder ∞.

Eigenschaften. (i) Es ist leicht zu zeigen, dass das neutrale Element e in einer Gruppe eindeutig ist und dass auch das inverse Element zu jedem Element a eindeutig ist. Sehen Sie LA I.

(ii) Durch assoziativität ist ein Produkt $a * b * \ldots$ ohne Klammern eindeutig bestimmt. z.B. $(a * b) * (c * d) = ((a * b) * c) * d = (a * (b * c)) * d = \ldots$.

(iii) Für abelsche Gruppen können wir die **additive Notation** verwenden. Wir schreiben die Operation als $a + b$. Das neutrale Element wird mit 0 bezeichnet und das Inverse von a wird mit $-a$ bezeichnet.

Ansonsten verwenden wir normalerweise die **multiplikative Notation**. Die Operation wird als ab (oder $a.b$ oder $a \cdot b$) geschrieben, das neutrale Element wird mit e oder 1 bezeichnet und das Inverse von a wird mit a^{-1} bezeichnet.

(iv) In multiplikativer Notation gilt: $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$. (Solche Regeln erlebt man täglich: Morgens erst Socken anziehen, dann Schuhe. Abends erst

Schuhe ausziehen, dann Socken.)

(In additive Notation: $-(-a) = a$, $-(a+b) = (-a) + (-b)$.)

(v) Sei $a, b \in G$. Die Gleichung $ax = b$ hat eine eindeutige Lösung $x = a^{-1}b$. Beweis: $ax = b \Rightarrow a^{-1}b = a^{-1}ax = 1x = x$, und $x = a^{-1}b \Rightarrow ax = aa^{-1}b = 1b = b$.

Ebenso hat die Gleichung $xa = b$ eine eindeutige Lösung $x = ba^{-1}$.

(vi) Die Verknüpfungstafel für G ist ein *lateinische Quadrat*, d.h. jedes Element der Gruppe in jeder Zeile genau einmal und in jeder Spalte genau einmal vorkommt. Folgt von (v).

(vii) (Kürzungsregel). $ax = ay \Rightarrow x = y$ und $xa = ya \Rightarrow x = y$. Folgt von (v).

(viii) Die Potenzen a^n von $a \in G$ sind wie folgt definiert (in multiplikativer Notation). Wir setzen $a^0 = 1$. Für $n > 0$ definieren wir a^n rekursiv durch $a^n = a^{n-1}.a$, und für $n < 0$ definieren wir $a^n = (a^{-1})^{-n}$.

(In additive Notation ist das $0a = 0$, $na = (n-1)a + a$ für $n > 0$ und $na = (-n)(-a)$ für $n < 0$.)

Dann gilt $a^n a^m = a^{n+m}$ und $(a^n)^m = a^{nm}$.

a^n kommutiert immer mit a^m, weil $a^n a^m = a^{n+m} = a^m a^n$.

Wenn a und b kommutieren, dann kommutiert jeder Potenz von a mit jeder Potenz von b. Aufgabe.

Wenn a und b kommutieren, gilt $(ab)^n = a^n b^n$.

Beispiele. (1) Die additive Gruppe $(R, +)$ wobei R ein Ring ist. Also $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

(Andererseits ist $(\mathbb{N}, +)$ keine Gruppe.)

(2) Die additive Gruppe $(V, +)$ wobei V ein Vektorraum über einem Körper ist.

(3) Sei K ein Körper und $K^\times := K \setminus \{0\} = \{a \in K : a \neq 0\}$. Dann ist $(K^\times, .)$ eine Gruppe. Also $(\mathbb{Q}^\times, .)$, $(\mathbb{R}^\times, .)$ oder $(\mathbb{C}^\times, .)$. Die Inverse zu $a \neq 0$ ist $a^{-1} = 1/a$.

(Andereseits ist $(K, .)$ keine Gruppe.)

(4) Sind G, H Gruppen (z.B. mit multiplikativer Notation), dann ist $G \times H$ eine

Gruppe bezüglich die Verknüpfung

$$(g,h)\cdot(g',h') \coloneqq (gg',hh').$$

Falls G, H endlich sind, ist $|G\times H| = |G|\cdot|H|$. Das neutrale Element ist $(1,1)$ und $(g,h)^{-1} = (g^{-1},h^{-1})$.

(5) Sei K ein Körper. Erinnerung: eine $n\times n$ Matrix $A\in M_n(K)$ ist **invertierbar** oder **nichtsingulär**, falls es eine Matrix B gibt, so dass $AB = BA = I_n$. Äquivalent ist, dass $\det(A)\neq 0$.

Die **allgemeine lineare Gruppe** $\mathrm{GL}_n(K)$ ist die Gruppe alle invertierbare $n\times n$ Matrizen $A\in M_n(K)$. Die Verknüpfung ist Multiplikation. Das neutrale Element ist die Einheitsmatrix I_n.

(6) Die **symmetrische Gruppe** S_X auf einer Menge X besteht aus allen Permutationen von X, also allen bijektiven Abbildungen $f: X\to X$. Die Verknupfung ist komposition von Abbildungen. Wenn also $f,g\in S_X$, dann ist $f\circ g$ oder fg die Abbildung mit $(f\circ g)(x) = (fg)(x) = f(g(x))$ für $x\in X$.

Falls $X = \{1,\dots,n\}$ schreiben wir S_n, die **symmetrische Gruppe von Grad** n. Wir bezeichnen eine Permutation $f\in S_n$ in **Zweizeilenform** als

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n)\end{pmatrix}$$

Die Ordnung ist $|S_n| = n!$.

Für $n\geq 3$ ist S_n nicht abelsch, z.B. für

$$f = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, g = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

gilt

$$fg = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, gf = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

z.B. $(fg)(1) = f(g(1)) = f(1) = 2$, $(gf)(1) = g(f(1)) = g(2) = 3$.

In LA I §6.1 hatten wir mehr über Permutationen.

Seien $a_1, a_2, \dots, a_k$ verschiedene Elemente in der Menge $\{1,2,\dots,n\}$. Wir bezeichnen mit $(a_1\ a_2\ \dots\ a_k)$ die Permutation in S_n, so dass

$$a_1\mapsto a_2\mapsto a_3\mapsto\cdots\mapsto a_k\mapsto a_1,$$

und mit $a \mapsto a$ für alle a die nicht in der Liste sind. Der ist ein k**-Zyklus**.

Eine **Vertauschung** oder **Transposition** ist ein 2-Zyklus $(i\ j)$.

Eine Menge von Zyklen ist **disjunkt**, wenn in zwei von ihnen keine Zahl a vorkommt.

Jede Permutation σ kann als Produkt disjunkter Zyklen geschrieben werden. Die Zerlegung ist im Wesentlichen einzigartig, abgesehen von der Reihenfolge der Zyklen und den unterschiedlichen Schreibweisen eines Zyklus. z.B. für

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 1 & 8 & 5 & 2 & 6 & 3 & 7 & 10 & 9 \end{pmatrix} \in S_{10}.$$

gilt

$$\sigma = (1\ 4\ 5\ 2)(3\ 8\ 7)(6)(9\ 10) = (3\ 8\ 7)(10\ 9)(5\ 2\ 1\ 4)$$

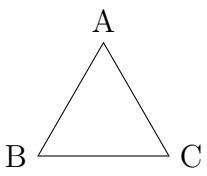
Jede Permutation kann als Produkt von Transpositionen geschrieben werden, z.B. $(2\ 5\ 4\ 6) = (2\ 6)(2\ 4)(2\ 5)$

(7) Die **Kleinsche Vierergruppe** V ist eine Gruppe von Ordnung 4 mit $x^2 = e$ für alle $x \in V$. Die Verknüpfungstabelle wird vollständig durch diese und die lateinische Quadrateigenschaft bestimmt. Sei $V = \{e, a, b, c\}$.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(8) Die **Diedergruppe** D_n ist die Gruppe der Symmetrien eines regulären n-Ecks. Die erlaubten Symmetrien sind Drehungen und Spiegelungen.

Beispielsweise ist D_3 die Symmetriegruppe eines gleichseitigen Dreiecks.



Wir betrachten die Symmetrien als Permutationen der Eckpunkte. Sei σ die Drehung durch $2\pi/3$ Gegenuhrzeigesinn. Also $\sigma(A) = B$, $\sigma(B) = C$, $\sigma(C) = A$.

Sei τ_A die Spiegelung in der Gerade durch A und the centre of the triangle. Also $\tau_A(A) = A$, $\tau_A(B) = C$, $\tau_A(C) = B$.

Also $\tau_A\sigma(A) = \tau_A(B) = C$, $\tau_A\sigma(B) = \tau_A(C) = B$, $\tau_A\sigma(C) = \tau_A(A) = A$, also $\tau_A\sigma = \tau_B$, usw.

Die Verküpfungstabelle für D_3 ist:

	e	σ	σ^2	τ_A	τ_B	τ_C
e	e	σ	σ^2	τ_A	τ_B	τ_C
σ	σ	σ^2	e	τ_C	τ_A	τ_B
σ^2	σ^2	e	σ	τ_B	τ_C	τ_A
τ_A	τ_A	τ_B	τ_C	e	σ	σ^2
τ_B	τ_B	τ_C	τ_A	σ^2	e	σ
τ_C	τ_C	τ_A	τ_B	σ	σ^2	e

Nun betrachten wir D_n, die Gruppe der Symmetrien eines regulären n-Ecks.

Sei σ die Drehung um den Winkel $2\pi/n$ und sei τ eine Spiegelung, die einen Eckpunkt A beibehält. Es gibt n Drehungen $e, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ und n Spiegelungen $\tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{n-1}$. Also $|D_n| = 2n$. Wir haben $\tau^2 = e$, $\sigma^n = e$, $\tau\sigma = \sigma^{-1}\tau$.

1.2 Untergruppen und Nebenklassen

Definition. Sei $(G, *)$ eine Gruppe und $H \subseteq G$ eine Teilmenge. Ist H eine Gruppe mit derselben Verknüpfung $*$ (eingeschränkt auf H), so nennen wir H eine *Untergruppe von* G, und wir schreiben $H \leq G$.

Lemma. *Sei $H \leq G$. Gilt:*

(i) H und G haben dasselbe neutrale Element (insbesondere enthält H das neutrale Element von G), und

(ii) das Inverse jedes Elements von H ist dasselbe, egal ob Sie die Gruppenstruktur von H oder die von G verwenden.

Beweis. LA I □

Satz. *(Untergruppenkriterium). Sei $(G, *)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ ist eine Untergruppe, genau dann wenn es die folgenden Eigenschaften erfüllt*

(i) Das neutrale Element $e \in H$,

(ii) $a * b \in H \ \forall \ a, b \in H$, und

(iii) Das Inverse von a ist in $H \ \forall \ a \in H$.

Beweis. LA I □

Beispiele. (1) Für jede Gruppe G ist $\{e\}$ eine Untergruppe, die **triviale Untergruppe**.

Die Menge G ist eine Untergruppe von G. Eine **echte Untergruppe** ist eine Untergruppe H von G mit $H \neq G$.

(2) Die Untergruppen von D_3 sind: $\{e\}$, $\{e, \tau_A\}$, $\{e, \tau_B\}$, $\{e, \tau_C\}$, $\{e, \sigma, \sigma^2\}$ und D_3.

(3) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ sind Untergruppen.

$\mathbb{Q}^\times \leq \mathbb{R}^\times \leq \mathbb{C}^\times$ sind Untergruppen.

$\mathbb{R}^{>0} := \{a \in \mathbb{R} : a > 0\} \leq \mathbb{R}^\times$.

($\mathbb{Q}^\times \not\leq \mathbb{Q}$ weil die Verknüpfung anders ist!)

(4) Die Menge alle n-te Einheitswurzeln in $\mathbb{C}$, ist

$$\mu_n := \{z \in \mathbb{C} : z^n = 1\} = \{e^{2\pi i k/n} : k \in \mathbb{Z}\} \leq \mathbb{C}^\times.$$

Die Ordnung ist $|\mu_n| = n$. z.B. $\mu_2 = \{1, -1\}$, $\mu_4 = \{1, i, -1, -i\}$.

(5) Die spezielle lineare Gruppe $\mathrm{SL}_n(K) = \{A \in \mathrm{GL}_n(K) : \det(A) = 1\} \leq \mathrm{GL}_n(K)$.

Die orthogonale Gruppe $\mathrm{O}_n = \{A \in \mathrm{GL}_n(\mathbb{R}) : A^{-1} = A^T\} \leq \mathrm{GL}_n(\mathbb{R})$.

Die spezielle othogonale Gruppe $\mathrm{SO}_n = \mathrm{O}_n \cap \mathrm{SL}_n(\mathbb{R})$.

(6) Falls $A \leq G$ und $B \leq H$, ist $A \times B \leq G \times H$.

(7) Seien $H, K \leq G$ Untergruppen. Dann ist der Schnitt $H \cap K$ wieder eine Untergruppe. Allgemeiner, wenn X eine Menge von Untergruppen von G ist, dann ist $\bigcap_{H \in X} H \leq G$.

(8) Ist $H \leq G$ und $g \in G$, dann ist $gHg^{-1} = \{ghg^{-1} : h \in H\} \leq G$.

Proposition (Untergruppen von $\mathbb{Z}$)**.** *Für $n \in \mathbb{Z}$ ist $\mathbb{Z}n \coloneqq \{an : a \in \mathbb{Z}\}$ eine Untergruppe von $\mathbb{Z}$. Jede Untergruppe von $\mathbb{Z}$ hat die Form $\mathbb{Z}n$ mit $n \geq 0$.*

Beweis. Es gilt $0 = 0n \in \mathbb{Z}n$ Für $an, bn \in \mathbb{Z}n$ gilt $an + bn = (a+b)n \in \mathbb{Z}n$ und $-(an) = (-a)n \in \mathbb{Z}n$. Also ist $\mathbb{Z}n$ eine Untergruppe von $\mathbb{Z}$.

Nun sei $H \leq \mathbb{Z}$ eine Untergruppe. Wenn H kein von Null verschiedenes Element a enthält, dann ist $H = \{0\} = \mathbb{Z}0$. Andernfalls enthält H ein positives Element, entweder a oder $-a$.

Sei n das kleinste positives Element von H. Es folgt, dass $\mathbb{Z}n \subseteq H$. Für $0 < h \in H$ gilt $h \geq n$. Wir nehmen a maximal, sodass $h \geq an$. Wir haben $n > h - an \geq 0$ und $h - an \in H$, also $h - an = 0$ und $h = an \in \mathbb{Z}n$. Für $0 > h \in H$ gilt $0 < -h \in H$ und $-h = an$ für ein a. Also ist $h = -an \in \mathbb{Z}n$. Also $H \subseteq \mathbb{Z}n$. Also $H = \mathbb{Z}n$. □

Definition. Sei $H \leq G$ eine Untergruppe. Die **Linksnebenklassen** von H in G sind die Teilmengen von G der Form $gH = \{gh : h \in H\}$ für $g \in G$.

Wir schreiben G/H für die Menge alle Linksnebenklassen.

Die Kardinalität $[G : H] := |G/H|$ nennt man die **Index** von H in G.

Die **Rechtsnebenklassen** Hg sind ähnlich definitiert, und wir schreiben $H\backslash G$ für die Menge alle Rechtsnebenklassen. Die Kardinalität ist auch $[G : H]$ (Übung).

Für eine abelsche Gruppe sind die Links- und Rechtsnebenklassen gleich. Für eine additive Gruppe G sind die Nebenklassen $H + g = \{h + g : h \in H\}$.

Lemma. *Sei H eine Untergruppe von G.*

(i) H selbst ist eine Linksnebenklasse von H in G.

(ii) Die Linksnebenklassen von H in G sind die Äquivalenzklassen für eine Äquivalenzrelation $\sim$ auf G definiert durch

$$a \sim b \Leftrightarrow a^{-1}b \in H.$$

Also bilden die Äquivalenzklassen eine Partition von G, d.h. G ist die disjunkte Vereinigung der Linksnbenklassen, oder äquivalent, jedes Element von G gehört zu genau einer Linksnebenklasse.

(iii) Alle Linksnebenklassen von H haben die gleiche Mächtigkeit wie H.

Beweis. (i) $H = eH$.

(ii) Es ist leicht zu sehen, dass $\sim$ eine Äquivalenzrelation ist. Die Äquivalenzklasse von $a \in G$ ist

$$[a] = \{b : a \sim b\} = \{b : a^{-1}b \in H\} = \{b : a^{-1}b = h, h \in H\} = \{ah : h \in H\} = aH.$$

Die Behauptung folgt nun aus Eigenschaften von Äquivalenzklassen (LA I, §1.3 Satz).

(iii) Für $g \in G$ betrachten wir die Abbildung $H \to gH$, $h \mapsto gh$. Sie ist surjektiv nach der Definition von gH, und injektiv nach dem Kürzungsregel (§1.1 Lemma). Also ist sie eine Bijektion. □

Beispiele. (1) Für $G = D_3$. Die Linksnebenklassen von $H = \{e, \sigma, \sigma^2\}$ sind

$$eH = \{e, \sigma, \sigma^2\}, \quad \tau_A H = \{\tau_A, \tau_B, \tau_C\}.$$

Die Linksnebenklassen von $H = \{e, \tau_A\}$ sind

$$eH = \{e, \tau_A\}, \quad \sigma H = \{\sigma, \tau_C\}, \quad \sigma^2 H = \{\sigma^2, \tau_B\}.$$

(2) Die Nebenklassen von $\mathbb{Z}3$ in $\mathbb{Z}$ sind

$$\mathbb{Z}3 + 0 = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$\mathbb{Z}3 + 1 = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$\mathbb{Z}3 + 2 = \{\dots, -4, -1, 2, 5, 8, \dots\}.$$

Satz (Satz von Lagrange)**.** *Sie H eine Untergruppe einer endlichen Gruppe G. Dann gilt $|G| = |H|.[G : H]$. Insbesondere, die Ordnung von H teilt die Ordnung von G.*

Beweis. Es gibt $[G : H]$ Linksnebenklassen, und jede enthält $|H|$ Elemente. □

1.3 Normalteiler und Faktorgruppen

Sei $H \leq G$ eine Untergruppe. Im Allgemeinen ist eine Linksnebenklasse kein Rechtsnebenklasse, also $gH \neq Hg$. Zum Beispiel für die Untergruppe $H = \{e, \tau_A\}$ in D_3 haben wir

$$\sigma H = \{\sigma, \tau_C\} \quad \text{und} \quad H\sigma = \{\sigma, \tau_B\}.$$

Definition. Eine Untergruppe $H \leq G$ heißt **Normalteiler**, falls $gH = Hg$ für alle $g \in G$. Wir schreiben $H \trianglelefteq G$.

Eine Gruppe heißt **einfach**, falls es keinen Normalteiler hat außer sich selbst und $\{e\}$.

Lemma. *Sei $H \leq G$. Äquivalent sind:*

(i) $H \trianglelefteq G$.

(ii) $gHg^{-1} = H \ \forall \ g \in G$.

(iii) $gHg^{-1} \subseteq H \ \forall \ g \in G$.

(iv) $ghg^{-1} \in H$ für alle $g \in G$ und $h \in H$.

Beweis. (i)⇒(ii)⇒(iii)⇒(iv) sind trivial.

(iv)⇒(i). Seien $g \in G$ und $h \in H$.

Nach (iv) ist $ghg^{-1} \in H$. Also $gh = (ghg^{-1})g \in Hg$. Also $gH \subseteq Hg$.

Nach (iv) ist $(g^{-1})h(g^{-1})^{-1} = g^{-1}hg \in H$. Also $hg = g(g^{-1}hg) \in gH$. Also $Hg \subseteq gH$.

Also $gH = Hg$. □

Beispiel. (i) $\{e\}$ und G sind immer Normalteiler von G.

(ii) Jede Untergruppe einer abelscher Gruppe ist einen Normalteiler.

(iii) Wenn K ein Körper ist, gilt $\mathrm{SL}_n(K) \trianglelefteq \mathrm{GL}_n(K)$.

(iv) Jede Untergruppe mit Index 2, d.h. $[G : H] = 2$, ist ein Normalteiler. Es gibt zwei Linksnebenklassen, also müssen sie H und $G \setminus H$ sein. Es gibt zwei Rechtsnebenklassen, also müssen sie auch H und $G \setminus H$ sein. Somit sind die Links- und Rechtsnebenklassen gleich.

(v) die Untergruppe von Drehungen $\{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ ist ein Normalteiler von D_n.

(vi) Das **Zentrum** einer Gruppe G ist

$$Z(G) \coloneqq \{a : ab = ba \text{ für alle } b \in G\}.$$

Es ist ein Normalteiler von G.

(vii) Es ist möglich, Normalteiler $K \trianglelefteq H \trianglelefteq G$ zu haben, aber K ist keine Normalteiler von G. z.B. $G = D_4$, $K = \{e, \tau\}$ und $H = \{e, \sigma^2, \tau, \tau\sigma^2\}$. Es gilt $K \trianglelefteq H$ und $H \trianglelefteq G$, da sie Untergruppen von Index 2 sind. Aber $\sigma\tau\sigma^{-1} = \tau\sigma^2 \notin K$.

Proposition. *Sei $N \trianglelefteq G$ ein Normalteiler. Dann bilden die Nebenklassen G/N eine Gruppe, die **Faktorgruppe**, bezüglich die Verknüpfung*

$$aN \cdot bN \coloneqq (ab)N.$$

Beweis. Wir müssen zunächst zeigen, dass diese Verknüpfung wohldefiniert ist, das heißt, das Produkt zweier Nebenklassen aN und bN hängt nicht von der Wahl der Vertreter a, b ab. Angenommen, $aN = a'N$ und $bN = b'N$. Dann ist $a' \in aN$ also $a' = an$ mit $n \in N$. Dann ist $nb' \in Nb' = b'N = bN$, also $nb' = bm$ mit $m \in N$. Dann ist $a'b' = anb' = abm \in (ab)N$, also $(a'b')N = (ab)N$.

Nun zeigen wir, das G/N eine Gruppe ist. Assoziativität:

$$aN \cdot (bN \cdot cN) = aN \cdot (bc)N = (a(bc))N = ((ab)c)N = (ab)N \cdot cN = (aN \cdot bN) \cdot cN.$$

Das neutrales Element ist $eK = K$, da

$$aN \cdot eN = (ae)N = aN \quad \text{und} \quad eN \cdot aN = (ea)N = aN.$$

Die Inverse von aN ist $a^{-1}N$, da

$$aN \cdot a^{-1}N = (aa^{-1})N = eN \quad \text{und} \quad a^{-1}N \cdot aN = (a^{-1}a)N = eN.$$

Also ist G/N eine Gruppe. □

Beispiel. Sei $n > 0$. Da $\mathbb{Z}$ abelsch ist, ist die Untergruppe $\mathbb{Z}n$ von $\mathbb{Z}$ ein Normalteiler. Die Faktorgruppe $\mathbb{Z}/\mathbb{Z}n$ besteht aus den Nebenklassen $\mathbb{Z}n + a$ in $\mathbb{Z}$, die wir auch mit $[a]$ bezeichnen.

In LA I §1.3 haben wir ein Ring $\mathbb{Z}_n$ definiert. Als additive Gruppe ist das genau $\mathbb{Z}/\mathbb{Z}n$.

Wir haben $[a] = [b]$ genau dann, wenn $a - b$ ein Vielfaches von n ist. Das heißt, a ist kongruent zu b modulo n, geschrieben als $a \equiv b \pmod{n}$.

Es gilt $\mathbb{Z}/\mathbb{Z}n = \{[0], [1], \ldots, [n-1]\}$, also $|\mathbb{Z}/\mathbb{Z}n| = n$.

1.4 Homomorphismen

Definition. Eine Abbildung $\theta\colon G \to H$ zwischen zwei Gruppen heißt **Homomorphismus** (oder Gruppenhomomorphismus) falls sie strukturerhaltend ist, d.h. $\theta(ab) = \theta(a)\theta(b)$ für alle $a, b \in G$.

Lemma. *(i) Sei $\theta : G \to H$ ein Homomorphismus. Dann gilt $\theta(e_G) = e_H$ und $\theta(g^{-1}) = (\theta(g))^{-1}$ für alle $g \in G$.*

(ii) Seien $\theta\colon G \to H$ und $\phi\colon H \to K$ zwei Homomorphismen. Dann ist $\phi\theta\colon G \to K$ ein Homomorphismus.

(iii) Für jede $g \in G$ gibt es genau einen Homomorphismus $\theta\colon \mathbb{Z} \to G$ mit $\theta(1) = g$.

Beweis. (i) Es gilt $\theta(g) = \theta(ge_G) = \theta(g)\theta(e_G)$. Wir multiplizieren mit $\theta(g)^{-1}$ auf der linken Seite und bekommen $e_H = \theta(e_G)$. Nun ist $e_H = \theta(e_G) = \theta(gg^{-1}) = \theta(g)\theta(g^{-1})$. Wir multiplizieren nochmal mit $\theta(g)^{-1}$ auf der linken Seite und bekommen $\theta(g)^{-1} = \theta(g^{-1})$.

(ii) Wir haben $\phi(\theta(gh)) = \phi(\theta(g)\theta(h)) = \phi(\theta(g))\phi(\theta(h))$.

(iii) Die Abbildung muss $\theta(n) = g^n$ sein. □

Beispiele. (i) Die Identität $\mathrm{id}\colon G \to G$ ist immer einen Homomorphismus.

(ii) Die Exponentialfunktion ergibt einen Homomorphismus $\mathbb{R} \to \mathbb{R}^\times$ oder $\mathbb{C} \to \mathbb{C}^\times$, da $e^{x+y} = e^x e^y$.

(iii) Wenn K ein Körper ist, dann ist $\det : \mathrm{GL}_n(K) \to K^\times$ ein surjektiver Homomorphismus.

(iv) Bei einer Permutation $\sigma \in S_n$ gibt es eine Matrix $Q^\sigma = (q_{ij}^\sigma) \in \mathrm{GL}_n(\mathbb{Q})$, definiert durch $q_{ij}^\sigma = \delta_{\sigma(i),j}$. Sehen Sie LA I §6.1. Für $\sigma, \pi \in S_n$ gilt

$$Q^{\sigma\pi} = Q^\pi Q^\sigma$$

Daraus folgt, dass die Abbildung $\sigma \mapsto (Q^\sigma)^T$ ein Homomorphismus $S_n \to \mathrm{GL}_n(\mathbb{Q})$ ist.

(v) Das Signum oder Vorzeichen einer Permutation ist

$$\epsilon(\sigma) = \det(Q^\sigma) = \det((Q^\sigma)^T) \in \mathbb{Q}^\times$$

Jede Permutation kann als Produkt von Transpositionen geschrieben werden, und wenn σ ein Produkt von n Transpositionen ist, dann ist $\epsilon(\sigma) = (-1)^n$. Somit ergibt das Signum einen Homomorphismus $\epsilon : S_n \to \mu_2$.

(vi) Ist $H \leq G$ eine Untergruppe, dann ist die Inklusion $H \to G$ einen Homomorphismus.

(vii) Ist $N \trianglelefteq G$ einen Normalteiler. Der **kanonische Homomorphismus** ist die Abbildung $G \to G/N$, $g \mapsto gN$. Sie ist ein surjektive Homomorphismus.

Definition. Das **Bild** und der **Kern** eines Homomorphismus $\theta : G \to H$ sind

$$\text{Bild}(\theta) \text{ oder } \text{Im}(\theta) = \{\theta(g) : g \in G\}, \quad \text{Ker}(\theta) = \{g \in G : \theta(g) = e\}.$$

Ein **Isomorphismus** (oder Gruppenisomorphismus) $\theta : G \to H$ ist ein Homomorphismus, der bijektiv ist.

Wir sagen, dass Gruppen G und H **isomorph** sind, geschrieben $G \cong H$, wenn es einen Isomorphismus $G \to H$ gibt.

z.B. $x \mapsto e^x$ gibt einen Isomorphismus $\mathbb{R} \to \mathbb{R}^{>0}$. Also ist $\mathbb{R} \cong \mathbb{R}^{>0}$.

Proposition. *Sei $\theta\colon G \to H$ ein Gruppenhomomorphismus.*

(i) Wenn $U \leq H$, dann $\theta^{-1}(U) = \{g \in G : \theta(g) \in U\} \leq G$. Wenn $U \trianglelefteq H$, dann $\theta^{-1}(U) \trianglelefteq G$.

(ii) $\text{Bild}(\theta) \leq H$ *und* $\text{Ker}(\theta) \trianglelefteq G$.

(iii) $\theta\colon G \to \text{Bild}(\theta)$ ist ein surjektive Homomorphismus.

(iv) θ ist injektiv genau dann, wenn $\text{Ker}(\theta)$ *trivial ist. In diesem Fall gibt θ ein Isomorphismus $G \to \text{Bild}(\theta)$.*

(v) Wenn θ ein Isomorphismus ist, dann ist $\theta^{-1} : H \to G$ ein Isomorphismus.

(vi) $\cong$ hat die Eigenschaften einer Äquivalenzrelation: (a) $G \cong G$, (b) $G \cong H \Rightarrow H \cong G$, (c) $G \cong H$ und $H \cong L \Rightarrow G \cong L$.

Beweis. (i) $\theta(e_G) = e_H \in U$, also $e_G \in \theta^{-1}(U)$. Wenn $a, b \in \theta^{-1}(U)$, gilt $\theta(ab) = \theta(a)\theta(b) \in U$ und $\theta(a^{-1}) = (\theta(a))^{-1} \in U$, also $ab, a^{-1} \in \theta^{-1}(U)$.

Wenn $U \trianglelefteq H$, $a \in \theta^{-1}(U)$ und $g \in G$, gilt $\theta(gag^{-1}) = \theta(g)\theta(a)\theta(g)^{-1} \in U$, also $gag^{-1} \in \theta^{-1}(U)$.

(ii) Für $\text{Bild}(\theta)$ ist es leicht. Für $\text{Ker}(\theta)$ folgt es von (i).

(iii) Klar

(iv) Wir nehmen an, dass $\text{Ker}(\theta) = \{e\}$. Dann $\theta(a) = \theta(b) \Rightarrow \theta(ab^{-1}) = \theta(a)\theta(b)^{-1} = e \Rightarrow ab^{-1} \in \text{Ker}(\theta) \Rightarrow ab^{-1} = e \Rightarrow a = b$.

(v),(vi) Klar. □

Beispiele. (i) Die Determinante $\det\colon \mathrm{GL}_n(K) \to K^\times$ ist einen surjektiven Homomorphismus. Es ist injektiv genau dann, wenn $n = 1$ ist. Der Kern ist der Normalteiler $\mathrm{SL}_n(K)$.

(ii) Der Kern von $\epsilon : S_n \to \mu_2$ ist die **alternierende Gruppe** A_n. LA I §6.3. Sie ist ein Normalteiler von S_n. Wenn $n \geq 2$, gilt $|A_n| = n!/2$.

(iii) Sei X eine Menge mit $|X| = n$. Eine Bijektion $\alpha : X \to \{1, \ldots, n\}$ liefert einen Isomorphismus $S_X \to S_n$, $f \mapsto \alpha f \alpha^{-1}$.

(iv) Die Beschriftung der Eckpunkte eines regulären n-Ecks mit den Zahlen $1, 2, \ldots, n$ ergibt einen Homomorphismus $\theta : D_n \to S_n$. Es gilt $\mathrm{Ker}(\theta) = \{e\}$, da e die einzige Symmetrie ist, die alle Eckpunkte fest lässt, also ist θ injektiv. Für $n = 3$ ist der Homomorphismus $\theta : D_3 \to S_3$ ein Isomorphismus, weil $|D_3| = 6 = |S_3|$.

(v) Sei $G \leq D_n$ die Untergruppe der Rotationen. Wir haben $G \cong \mu_n$, da es einen Homomorphismus gibt, mit $\sigma^j \mapsto e^{2\pi i j/n}$.

1.5 Die Isomorphiesätze von Emmy Noether

Satz (Homomorphiesatz)**.** *Sei $\theta\colon G \to H$ ein Gruppenhomomorphismus.*

(1) Sei $N \trianglelefteq G$ ein Normalteiler mit $N \subseteq \mathrm{Ker}(\theta)$. Dann gibt es genau einen Homomorphismus $\bar\theta\colon G/N \to H$ mit $\bar\theta(gN) = \theta(g)$ für $g \in G$.

(2) Es gibt einen Isomorphismus $\bar\theta\colon G/\mathrm{Ker}(\theta) \to \mathrm{Bild}(\theta)$ mit $\bar\theta(g\,\mathrm{Ker}(\theta)) = \theta(g)$ für $g \in G$.

Beweis. (1) Wohldefiniert: Sei $aN = bN$ mit $a, b \in G$. Dann gilt $a = bn$ mit $n \in N$ und

$$\theta(a) = \theta(bn) = \theta(b)\theta(n) = \theta(b)e_H = \theta(b).$$

Also ist $\bar\theta$ wohldefiniert.

Homomorphismus: $\bar\theta(aN \cdot bN) = \bar\theta(abN) = \theta(ab) = \theta(a)\theta(b) = \bar\theta(aN)\bar\theta(bN)$.

Eindeutigkeit: Da jedes Element in G/N der Form gN mit $g \in G$ hat, ist $\bar\theta$ eindeutig.

(2) Wir nehmen $N = \mathrm{Ker}(\theta)$ in (1). Es gilt

$$\mathrm{Ker}(\bar\theta) = \{gN : \theta(g) = e_H\} = \{gN : g \in \mathrm{Ker}(\theta) = N\} = \{eN\}.$$

Hier ist eN das neutrale Element von G/N. Nach §1.4 Proposition (iv) ist nun $\bar{\theta}\colon G/N \to \mathrm{Bild}(\theta)$ ein Isomorphismus. □

z.B. $\mathbb{C} \to \mathbb{C}^\times$, $z \mapsto e^z$ ist ein surjektive Homomorphismus mit Kern $2\pi i\mathbb{Z}$. Also gibt es einen Isomorphismus $\mathbb{C}/2\pi i\mathbb{Z} \to \mathbb{C}^\times$.

Satz (Erster Isomorphiesatz)**.** *Seien G eine Gruppe, $H \leq G$ und $N \trianglelefteq G$. Wir definieren*

$$HN \coloneqq \{hn \mid h \in H,\ n \in N\}.$$

Dann $HN \leq G$, $N \trianglelefteq HN$, $H \cap N \trianglelefteq H$ und es gibt einen Isomorphismus

$$H/(H \cap N) \to HN/N, \quad h(H \cap N) \mapsto hN.$$

Beweis. Seien $h_i \in H$ und $n_i \in N$. Da N einen Normalteiler ist, gibt es $n', n'' \in N$ mit $n_1h_2 = h_2n'$ und $n_1^{-1}h_1^{-1} = h_1^{-1}n''$. Es folgt:

$$(h_1n_1)(h_2n_2) = h_1(n_1h_2)n_2 = h_1(h_2n')n_2 = (h_1h_2)(n'n_2) \in HN$$

und

$$(h_1n_1)^{-1} = n_1^{-1}h_1^{-1} = h_1^{-1}n'' \in HN,$$

also ist HN eine Untergruppe.

Da $N \trianglelefteq G$ ein Normalteiler und $N \subseteq HN$ ist, ist es klar, dass $N \trianglelefteq HN$ ein Normalteiler ist.

Seien $h \in H$ und $n \in H \cap N$. Dann liegt $n' = hnh^{-1}$ im Normalteiler N und auch in der Untergruppe H. Also $h(H \cap N)h^{-1} \subseteq H \cap N$ und $H \cap N$ ist einen Normalteiler von H.

Die Komposition der Inklusion $H \to HN$ und der kanonischen Abbildung $HN \to HN/N$ ist ein Homomorphismus $\phi : H \to HN/N$, $h \mapsto hN$. Es ist surjektiv, denn wenn $h \in H$ und $n \in N$, dann ist $(hn)N = hN = \phi(h) \in \mathrm{Bild}(\phi)$. Wir haben

$$\mathrm{Ker}(\phi) = \{h \in H : hN = N\} = \{h \in H : h \in N\} = H \cap N.$$

Also nach dem Homomorphiesatz, induziert ϕ einen Isomorphismus $H/(H \cap N) \to HN/N$. □

Korollar. *Seien G eine endliche Gruppe, $H \leq G$ und $N \trianglelefteq G$. Dann gilt*

$$|HN| = \frac{|H| \cdot |N|}{|H \cap N|}.$$

Beweis. Nach dem ersten Isomorphiesatz, gilt $H/(H \cap N) \cong HN/N$. Also $[H : H \cap N] = |H/(H \cap N)| = |HN/N| = [HN : N]$.

Nach dem Satz von Lagrange gilt $[H : H \cap N] = |H|/|H \cap N|$ und $[HN : N] = |HN|/|N|$. □

Proposition. *Seien $N, K \trianglelefteq G$ zwei Normalteiler. Gilt $N \cap K = \{e\}$, dann ist $KN \cong K \times N$.*

Beweis. Wir zeigen: $nk = kn$ für $n \in N$ und $k \in K$. Da $N \trianglelefteq G$ gilt $knk^{-1} \in N$, also

$$nkn^{-1}k^{-1} = n(kn^{-1}k^{-1}) \in N.$$

Da $K \trianglelefteq G$ gilt $nkn^{-1} \in K$, also

$$nkn^{-1}k^{-1} = (nkn^{-1})k^{-1} \in K$$

Also $nkn^{-1}k^{-1} \in N \cap K = \{e\}$. Somit ist $nkn^{-1}k^{-1} = e$, was $nk = kn$ ergibt.

Nun ist die Abbildung $\theta : K \times N \to KN$, $\theta(k, n) = kn$ ein Homomorphismus, da

$$\theta(k, n)\theta(k', n') = knk'n' = kk'nn' = \theta(kk', nn') = \theta((k, n)(k', n')).$$

Auch $\mathrm{Ker}(\theta) = \{(e, e)\}$, denn wenn $\theta(k, n) = e$, dann $kn = e$, dann $k = n^{-1} \in K \cap N = \{e\}$, also $k = e$ also $n = e$. Somit induziert θ einen Isomorphismus $K \times K \to KN$. □

Satz (Zweiter Isomorphiesatz)**.** *Sei $N \trianglelefteq G$.*

(1) Wenn H eine Untergruppe von G mit $N \subseteq H$ ist, dann ist $N \trianglelefteq H$ und H/N eine Untergruppe von G/N.

(2) Jede Untergruppe U von G/N hat die Form H/N mit H wie oben (explizit $H = \{g \in G : gN \in U\}$) .

(3) $H/N \trianglelefteq G/N$ genau dann wenn $H \trianglelefteq G$. In diesem Fall gibt es einen Isomorphismus

$$G/H \to (G/N)/(H/N), \quad gH \mapsto (gN)(H/N).$$

Beweis. (1) $N \leq H$ ist klar. $N \trianglelefteq G \Rightarrow gN = Ng \ \forall \ g \in G \Rightarrow gN = Ng \ \forall \ g \in H \Rightarrow N \trianglelefteq H$.

Die Elemente von H/N sind Linksnebenklassen der Form hN. Dies sind auch Linksnebenklassen von N in G. Also $H/N \subseteq G/N$.

Sei $i : H \to G$ die Inklusion und $\theta : G \to G/N$ die kanonische Abbildung. Dann ist θi der Homomorphismus $H \to G/N$, $h \mapsto hN$, und $H/N = \text{Bild}(\theta i)$, also ist H/N eine Untergruppe von G/N.

(2) Wenn $U \leq G/N$, dann setzen wir $H = \theta^{-1}(U)$. Nach §1.4 Proposition (i) ist H eine Untergruppe von G, und es ist klar, dass $N \subseteq H$. Da θ surjektiv ist, ist $U = \theta(\theta^{-1}(U)) = \theta(H) = H/N$.

(3) Wenn $H/N \trianglelefteq G/N$, dann ist $H = \theta^{-1}(H/N) \trianglelefteq G$ nach §1.4 Proposition (i).

Umgekehrt, wenn $H \trianglelefteq G$ und $hN \in H/N$ und $gN \in G/N$, dann $(gN)(hN)(gN)^{-1} = (ghg^{-1})N \in H/N$, also $H/N \trianglelefteq G/N$.

Sei $\phi : G/N \to (G/N)/(H/N)$ die kanonische Abbildung. Dann ist $\phi\theta : G \to (G/N)/(H/N)$ die Abbildung $g \mapsto (gN)(H/N)$. Da θ und ϕ surjektiv sind, gilt dies auch für $\phi\theta$. Auch $\text{Ker}(\phi\theta) = H$, da $(gN)(H/N)$ genau dann das neutrale Element von $(G/N)/(H/N)$ ist, wenn

$$gN \in H/N \Leftrightarrow g \in H$$

Nun liefert der Homomorphiesatz das Ergebnis. □

Erinnerung §1.2 Proposition: Für $n \in \mathbb{Z}$ ist $\mathbb{Z}n$ eine Untergruppe von $\mathbb{Z}$, und jede Untergruppe hat die Form $\mathbb{Z}n$ mit $n \geq 0$.

Für $d, n \in \mathbb{Z}$ gilt $\mathbb{Z}n \subseteq \mathbb{Z}d$ genau dann, wenn n ein Vielfaches von d ist, oder mit anderen Worten, d ein Teiler von n ist.

Korollar. *Sei $n > 0$. Die Untergruppen von $\mathbb{Z}/\mathbb{Z}n$ sind genau die Gruppen $\mathbb{Z}d/\mathbb{Z}n$ mit d einem positiven Teiler von n. Weiterhin ist $|\mathbb{Z}d/\mathbb{Z}n| = n/d$.*

Beweis. Folgt vom zweiten Isomorphiesatz. Hier $(\mathbb{Z}/\mathbb{Z}n)/(\mathbb{Z}d/\mathbb{Z}n) \cong \mathbb{Z}/\mathbb{Z}d$ gibt $n/|\mathbb{Z}d/\mathbb{Z}n| = d$. □

Wenn H und N Untergruppen einer additiven Gruppe G sind, schreiben wir $H + N = \{h + n : h \in H, n \in N\}$ anstelle von HN.

Seien $a, b \in \mathbb{Z}$. Sei $\text{ggT}(a, b)$ der größte gemeinsame Teiler von a und b (oder 0, wenn $a = b = 0$), und sei $\text{kgV}(a, b)$ das kleinste gemeinsame positive Vielfache von a und b (oder 0, wenn $a = b = 0$).

Satz (Eigenschaften von ggT und kgV)**.** *Für $a, b \in \mathbb{Z}$ gilt*

$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}\,\text{ggT}(a, b), \quad \mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}\,\text{kgV}(a, b).$$

Insbesondere gibt es $x, y \in \mathbb{Z}$, so dass $\operatorname{ggT}(a,b) = xa + yb$. *Wenn* $a, b > 0$, *gilt* $\operatorname{ggT}(a,b)\operatorname{kgV}(a,b) = ab$.

Beweis. $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}g$ und $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}k$ mit $g, k \geq 0$.

Es gilt: d ist ein gemeinsamer Teiler von a und $b \Leftrightarrow a \in \mathbb{Z}d$ und $b \in \mathbb{Z}d \Leftrightarrow \mathbb{Z}g = \mathbb{Z}a + \mathbb{Z}b \subseteq \mathbb{Z}d \Leftrightarrow d$ ist ein Teiler von g. Somit ist $\operatorname{ggT}(a,b) = g$.

Es gilt: c ist ein gemeinsames Vielfaches von a und $b \Leftrightarrow c \in \mathbb{Z}a$ und $c \in \mathbb{Z}b \Leftrightarrow \mathbb{Z}c \subseteq \mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}k \Leftrightarrow c$ ist ein Vielfaches von k. Somit ist $\operatorname{kgV}(a,b) = k$.

Nach dem ersten Isomorphiesatz, gilt

$$(\mathbb{Z}a + \mathbb{Z}b)/\mathbb{Z}a \cong \mathbb{Z}b/(\mathbb{Z}a \cap \mathbb{Z}b).$$

Also $\mathbb{Z}\operatorname{ggT}(a,b)/\mathbb{Z}a \cong \mathbb{Z}b/\mathbb{Z}\operatorname{kgV}(a,b)$. Also $a/\operatorname{ggT}(a,b) = \operatorname{kgV}(a,b)/b$. □

Bemerkung. Mit Hilfe des **euklidischen Algorithmus** kann man $\operatorname{ggT}(a,b)$ und x, y finden.

Bei gegebenen ganzen Zahlen a, b mit $b > 0$ können wir a durch b dividieren, was einen ganzzahligen Quotienten q und den Rest r mit $0 \leq r < b$ ergibt. Also $a = qb + r$.

Klar ist: $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}b + \mathbb{Z}r$, also $\operatorname{ggT}(a,b) = \operatorname{ggT}(b,r)$.

Wir können also weiter machen mit (b,r) statt (a,b), und da $r < b$ kleiner ist, wird diese Verfahren nach endlich viele Wiederholungen stoppen (mit $r = 0$).

Zum Beispiel, lass uns $\operatorname{ggT}(2183, 1517)$ berechnen.

$$\begin{aligned}
2183 &= 1 \cdot 1517 + 666 \\
1517 &= 2 \cdot 666 + 185 \\
666 &= 3 \cdot 185 + 111 \\
185 &= 1 \cdot 111 + 74 \\
111 &= 1 \cdot 74 + 37 \\
74 &= 2 \cdot 37 + 0
\end{aligned}$$

und $\operatorname{ggT}(2183, 1517) = 37$.

Wir können nun $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = xa + yb$ auch finden:

$$\begin{aligned}
37 &= 111 - 1 \cdot 74 \\
&= 111 - 1 \cdot (185 - 1 \cdot 111) = -1 \cdot 185 + 2 \cdot 111 \\
&= -1 \cdot 185 + 2 \cdot (666 - 3 \cdot 185) - 185 = 2 \cdot 666 - 7 \cdot 185 \\
&= 2 \cdot 666 - 7 \cdot (1517 - 2 \cdot 666) = -7 \cdot 1517 + 16 \cdot 666 \\
&= -7 \cdot 1517 + 16 \cdot (2183 - 1 \cdot 1517) = 16 \cdot 2183 - 23 \cdot 1517.
\end{aligned}$$

1.6 Zyklische Gruppen und Ordnungen von Elementen

Definition. Sei G eine Gruppe und $T \subseteq G$ eine Teilmenge. Dann ist

$$\langle T \rangle := \bigcap_{T \subseteq H \leq G} H$$

die von T **erzeugte Untergruppe von** G, d.h. $\langle T \rangle$ ist der Durchschnitt aller Untergruppen von G, welche T enthalten. Also ist $\langle T \rangle$ die kleinste Untergruppe von G, welche T enthält. Fur $T = \{g_1, \ldots, g_n\}$ schreiben wir auch $\langle g_1, \ldots, g_n \rangle$.

Eine Teilmenge $U \subseteq G$ ist ein **Erzeugendensystem** von G, falls $\langle U \rangle = G$. Eine Gruppe G ist **endlich erzeugt**, falls es ein endliches Erzeugendensystem von G gibt, und G ist **zyklisch**, falls ein $g \in G$ existiert mit $\langle g \rangle = G$.

z.B. In D_3 ist $\langle \sigma, \tau_A \rangle = D_3$. Wenn wir nämlich die Liste der Untergruppen von D_3 verwenden, sehen wir, dass keine echte Untergruppe σ und τ_A enthält. Also ist $\{\sigma, \tau_A\}$ ein Erzeugendensystem von D_3.

Lemma. *(i)* $\langle \emptyset \rangle = \{e\}$,

(ii) $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$,

(iii) $\langle T \rangle = \{s_1 s_2 \ldots s_r : r \geq 0, s_1, \ldots, s_r \in S\}$, *wobei* $S := T \cup \{t^{-1} : t \in T\}$ *und mit der Konvention, dass ein Produkt mit* $r = 0$ *Termen das neutrale Element* e *ist.*

Beweis. (i) Klar.

(ii) Die Menge $\{g^n : n \in \mathbb{Z}\}$ ist eine Untergruppe von G ist (z.B. sie ist das Bild des Homomorphismus θ von §1.4 Lemma (iii)). Sie ist offensichtlich die kleinste Untergruppe von G, die g enthält. Also ist $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.

(iii) Übung. □

Beispiele. (i) Die Gruppe $\{e, \sigma, \ldots, \sigma^{n-1}\}$ von Drehungen eines regulären n-Ecks ist zyklisch, mit Erzeuger σ.

(ii) Die Gruppe μ_n ist zyklisch mit Erzeuger $e^{2\pi i/n}$.

(iii) $\mathbb{Z}$ ist zyklisch mit Erzeuger 1. (Sie ist eine additive Gruppe, daher sind die Potenzen g^n von $g = 1$ als $n1 \in \mathbb{Z}$ geschrieben.)

(iv) $\mathbb{Z}/\mathbb{Z}n$ ist zyklisch mit Erzeuger $\mathbb{Z}n + 1$.

(v) Jede Gruppe G der Ordnung p, eine Primzahl, ist einfach und zyklisch.

Wenn H eine Untergruppe von G ist, dann ist $|H|$ nach dem Satz von Lagrange ein Teiler von $|G| = p$, also $H = \{e\}$ oder $H = G$. Wenn $g \neq e$, dann $\langle g \rangle = G$, also ist G zyklisch.

Satz. *Sei G eine zyklische Gruppe.*

(1) (Klassifikation zyklischer Gruppen) Es gilt

$$G \cong \begin{cases} \mathbb{Z} & \text{falls } |G| = \infty \\ \mathbb{Z}/\mathbb{Z}n & \text{falls } |G| = n < \infty. \end{cases}$$

Insbesondere sind zwei beliebige zyklische Gruppen derselben Ordnung isomorph.

(2) Jede Untergruppe oder Faktorgruppe von G ist zyklisch.

Beweis. (1) Wenn g ein Generator von G ist, dann gibt es einen surjektiven Homomorphismus $\theta : \mathbb{Z} \to G$, $n \mapsto g^n$. Also ist G durch den Homomorphiesatz isomorph zu $\mathbb{Z}/\operatorname{Ker}(\theta)$.

Nun ist $\operatorname{Ker}(\theta) = \mathbb{Z}n$ für ein $n \geq 0$ nach §1.2 Proposition. Falls $n = 0$ ist θ ein Isomorphismus und $|G| = \infty$. Falls $n > 0$ gibt die Homomorphiesatz ein Isomorphismus $\mathbb{Z}/\mathbb{Z}n \to G$, und $|G| = n$.

(2) Wenn G/N eine Faktorgruppe von G ist und g ein Generator für G ist, dann ist G/N zyklisch mit dem Generator gN.

Die Untergruppen von $\mathbb{Z}$ haben die Form $\mathbb{Z}n = \langle n \rangle$, sind also zyklisch. Die Untergruppen von $\mathbb{Z}/\mathbb{Z}n$ haben die Form $\mathbb{Z}d/\mathbb{Z}n$, und $\mathbb{Z}d$ ist zyklisch, also sind sie zyklisch. □

Definition. Sei g ein Element einer Gruppe G. Die **Ordnung** von g, geschrieben $\operatorname{ord}(g)$, ist die kleinste ganze positive Zahl n mit $g^n = e$. Gibt es keine solche Zahl, setzen wir $\operatorname{ord}(g) = \infty$.

Proposition (1)**.** *Seien G eine Gruppe, $g \in G$ und $n = \operatorname{ord}(g)$.*

(i) $n = 1 \Leftrightarrow g = e$.

(ii) Für $m \in \mathbb{Z}$ *gilt* $g^m = e \Leftrightarrow \begin{cases} m \in \mathbb{Z}n & (n < \infty) \\ m = 0 & (n = \infty) \end{cases}$.

(iii) $|\langle g \rangle| = n$.

(iv) Wenn $n < \infty$*, gilt* $\operatorname{ord}(g^k) = n/\operatorname{ggT}(k, n)$ *für* $k \in \mathbb{Z}$.

Beweis. (i) Klar.

(ii) Der Homomorphismus $\theta : \mathbb{Z} \to G$, $m \mapsto g^m$ hat Kern der Form $\mathbb{Z}n$ für ein $n \geq 0$. Dann

$$\operatorname{ord}(g) = \begin{cases} n & (n > 0) \\ \infty & (n = 0) \end{cases}$$

also $\operatorname{ord}(g) = |\mathbb{Z}/\mathbb{Z}n| = |\langle g \rangle|$, weil θ einen Isomorphismus $\mathbb{Z}/\mathbb{Z}n \to \langle g \rangle$ induziert.

(iii) θ induziert einen Isomorphismus $\mathbb{Z}/\mathbb{Z}\operatorname{ord}(g) \to \langle g \rangle$.

(iv) $g^{km} = e \Leftrightarrow km$ ist ein Vielfaches von k und von $n \Leftrightarrow km \in \mathbb{Z}k \cap \mathbb{Z}n = \mathbb{Z}\operatorname{kgV}(k, n) \Leftrightarrow m$ ist ein Vielfaches von $\operatorname{kgV}(k, n)/k = n/\operatorname{ggT}(k, n)$. □

Proposition (2)**.** *Seien G eine endliche Gruppe und $g \in G$.*

(i) $\operatorname{ord}(g)$ *ist endlich und ein Teiler von* $|G|$ *(also* $g^{|G|} = e$*).*

(ii) g ist ein Erzeuger von $G \Leftrightarrow \operatorname{ord}(g) = |G|$.

Beweis. (i) Folgt aus Proposition (1)(iii) und dem Satz von Lagrange. (ii) Folgt. □

Proposition (3)**.** *Wenn Elemente $g, h \in G$ kommutieren und endliche Ordnungen a und b haben, dann ist* $\operatorname{ord}(gh)$ *ein Teiler von* $\operatorname{kgV}(a, b)$.

Wir haben Gleichheit, wenn $\langle g \rangle \cap \langle h \rangle = \{e\}$. Dies gilt, wenn a und b teilerfremd sind, d.h. $\operatorname{ggT}(a, b) = 1$.

Beweis. Wenn c ein gemeinsames Vielfaches von a und b ist, dann ist $(gh)^c = g^c h^c = e$ nach Proposition (1)(ii). Also nach Proposition (1)(ii) ist $\operatorname{ord}(gh)$ ein Teiler von c.

Nehmen wir nun an, dass $\langle g\rangle \cap \langle h\rangle = \{e\}$. Wenn $(gh)^c = e$, dann $g^c = (h^c)^{-1} \in \langle g\rangle \cap \langle h\rangle = \{e\}$, also $g^c = h^c = e$, also ist c ein gemeinsames Vielfaches von a und b. Das gibt Gleichheit.

Sind a und b teilerfremd, dann $\langle g\rangle \cap \langle h\rangle = \{e\}$ nach dem Satz von Lagrange. □

Satz (Chinesischer Restsatz für Gruppen)**.** *Wenn $a, b \in \mathbb{Z}$ teilerfremd sind, also* $\mathrm{ggT}(a, b) = 1$*, dann gilt $(\mathbb{Z}/\mathbb{Z}a) \times (\mathbb{Z}/\mathbb{Z}b) \cong \mathbb{Z}/\mathbb{Z}ab$.*

Beweis. Die Ordnungen von $\mathbb{Z}a + 1$ und $\mathbb{Z}b + 1$ sind a und b, die teilerfremd sind, also hat $(\mathbb{Z}a + 1, \mathbb{Z}b + 1) \in (\mathbb{Z}/\mathbb{Z}a) \times (\mathbb{Z}/\mathbb{Z}b)$ die Ordnung ab. □

2 Gruppenaktionen und Anwendungen

2.1 Aktionen

Definition. Sei G eine Gruppe und sei X eine nicht-leere Menge. Eine **Operation** oder **Aktion** von G auf X ist eine Abbildung

$$*\colon G \times X \to X, \quad (g, x) \mapsto g * x,$$

sodass für alle $g, h \in G$ und $x \in X$ gilt

$$e * x = x \quad \text{und} \quad (gh) * x = g * (h * x).$$

Wir sagen auch, dass X eine G**-Menge** ist. Üblicherweise schreiben wir einfach gx statt $g * x$.

Beispiele. (1) Sei G eine Gruppe und X eine Menge. Die **triviale Aktion** ist durch $gx = x$ für alle $g \in G$ und $x \in X$ gegeben.

(2) Die Gruppe S_X operiert auf die Menge X durch $f * x = f(x)$. Insbesondere, die symmetrische Gruppe S_n operiert auf $\{1, \ldots, n\}$.

(3) Sei X die Eckenmenge eines regulären n-Ecks. Dann operiert die Diedergruppe D_n auf X.

(4) $\mathrm{GL}_n(K)$ operiert auf K^n durch $(A, v) \mapsto Av$.

(5) Ist $H \leq G$ eine Untergruppe, dann operiert G auf die Menge aller Linksnebenklassen: $g \cdot g'H \coloneqq (gg')H$.

Lemma. *Sei G eine Gruppe und X eine Menge. Es gibt eine Bijektion zwischen G-Aktionen auf X und Gruppenhomomorphismen $\rho : G \to S_X$ gegeben durch $g * x = \rho(g)(x)$ für $g \in G$ und $x \in X$.*

Beweis. Wenn $*$ eine Aktion ist, dann $\rho(e)(x) = e * x = x$, also $\rho(e) = \mathrm{Id}_X$, und wenn $g, h \in G$, dann $\rho(g)\rho(h)(x) = \rho(g)(h * x) = g * (h * x) = (gh) * x = \rho(gh)(x)$, also $\rho(g)\rho(h) = \rho(gh)$. Daraus folgt, dass $\rho(g)$ eine Bijektion mit Inverse $\rho(g^{-1})$ ist und dass ρ ein Homomorphismus ist.

Wenn umgekehrt ρ ein Homomorphismus ist, ist es leicht zu sehen, dass $*$ eine Aktion ist. □

Satz (Satz von Cayley)**.** *Jede endliche Gruppe von Ordnung n ist isomorph zu einer Untergruppe von S_n.*

Beweis. Jede Gruppe G operiert auf sich selbst durch Multiplikation:

$$G \times G \to G, \quad (g, h) \mapsto gh.$$

Das gibt ein Homomorphismus $\rho : G \to S_G$. Nach dem Kürzungsregel ist ρ injektive, also ist G isomorph zu eine Untergruppe von S_G. Falls $|G| = n$ kann man eine Bijektion $G \to \{1, \ldots, n\}$ wählen. Dann kann man S_G und S_n identifizieren. □

Definition. Sei X eine G-Menge. Die **Bahn** von $x \in X$ ist

$$Gx \coloneqq \{gx : g \in G\},$$

eine Teilmenge von X, und die **Stabilisator** oder Isotropiegruppe ist

$$\mathrm{Stab}_G(x) = G_x \coloneqq \{g \in G : gx = x\},$$

eine Untergruppe von G.

Die Menge der Bahnen von G auf X ist

$$X/G := \{Gx : x \in X\}.$$

Die Menge der Fixpunkte in X ist

$$X^G \coloneqq \{x \in X : gx = x \text{ für alle } g \in G\}.$$

Die Aktion $G \times X \to X$ ist **transitiv**, falls es nur eine G-Bahn in X gibt. Die Aktion ist **treu** falls die ensprechende Abbildung $G \to S_X$ injektiv ist.

Beispiel. Die Gruppe $G = \mathbb{R}^{>0}$ operiert durch Multiplikation auf $\mathbb{R}$.

Wenn $a > 0$, dann ist $Ga = \mathbb{R}^{>0}$ und $\mathrm{Stab}_G(a) = \{1\}$.

$G0 = \{0\}$ und $\mathrm{Stab}_G(0) = G$.

Wenn $a < 0$, dann $Ga = \mathbb{R}^{<0} := \{x \in \mathbb{R} : x < 0\}$ und $\mathrm{Stab}_G(a) = \{1\}$.

$\mathbb{R}/G = \{\mathbb{R}^{>0}, \{0\}, \mathbb{R}^{<0}\}$.

$\mathbb{R}^G = \{0\}$.

Proposition. *Sei X eine G-Menge.*

(1) Die Bahnen sind die Äquivalenzklassen für eine Äquivalenzrelation auf X definiert durch

$$x \sim y \Leftrightarrow y = gx \text{ für ein } g \in G.$$

Somit ist X die disjunkte Vereinigung der Bahnen.

(2) [Bahnformel] Für $x \in X$ ist die Abbildung

$$G/\operatorname{Stab}_G(x) \to Gx, \quad g\operatorname{Stab}_G(x) \mapsto gx,$$

eine Bijektion zwischen der Menge von Linksnebenklassen $G/\operatorname{Stab}_G(x)$ und der Bahn Gx. Insbesondere:

$$|Gx| = [G : \operatorname{Stab}_G(x)].$$

(3) [Klassengleichung] Wenn X endlich ist, gilt

$$|X| = \sum_{B \in X/G} |B|.$$

Wenn $x_i \in X$ Repräsentanten der nicht trivialen Bahnen sind, dann wird das

$$|X| = \left|X^G\right| + \sum_i |Gx_i|\,.$$

Beweis. (1) Übung.

(2) Die Abbildung $G \to Gx$, $g \mapsto gx$, ist surjectiv. Ist $h \in \operatorname{Stab}_G(x)$, dann ist $(gh)x = g(hx) = gx$. Umgekehrt gilt $gx = g'x$ genau dann, wenn $x = g^{-1}g'x$, äquivalent $g^{-1}g' \in \operatorname{Stab}_G(x)$, oder $g^{-1}g'\operatorname{Stab}_G(x) = \operatorname{Stab}_G(x)$, oder $g\operatorname{Stab}_G(x) = g'\operatorname{Stab}_G(x)$.

(3) Für die Klassengleichung müssen wir jetzt nur merken, dass eine Bahn trivial ist, also $Gx = \{x\}$, genau dann, wenn $x \in X^G$ einen Fixpunkt ist. □

Sei X eine G-Menge. Für $g \in G$ gibt es die Menge alle Fixpunkte unter g

$$\operatorname{Fix}(g) \coloneqq \{x \in X : gx = x\}.$$

Satz (Lemma von Burnside)**.** *Sei X eine G-Menge, mit G und X beide endlich. Dann gilt:*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|\,.$$

Beweis. Zweifachen Abzählen gibt

$$\sum_{g \in G} |\operatorname{Fix}(g)| = |\{(g, x) \in G \times X \mid gx = x\}| = \sum_{x \in X} |\operatorname{Stab}_G(x)|\,.$$

Nun ergibt die Bahnformel $|Gx| = [G : \mathrm{Stab}_G(x)] = |G|/|\mathrm{Stab}_G(x)|$, also $|\mathrm{Stab}_G(x)| = |G|/|Gx|$. Es folgt

$$\sum_{x\in X} |\mathrm{Stab}_G(x)| = |G| \sum_{x\in X} \frac{1}{|Gx|} = |G| \cdot |X/G|\,,$$

denn in der Summe $\sum_{x\in X} 1/|Gx|$ gibt es für jede Bahn Gx $|Gx|$-Terme, die jeweils gleich $1/|Gx|$ sind. □

2.2 Konjugation und platonische Körper

Definition. Jede Gruppe G operiert auf sich selbst durch **Konjugation**:

$$* : G \times G \to G, \quad g * a = gag^{-1}.$$

Die Bahnen heißen **Konjugationsklassen**, geschrieben

$$CC(a) := \{gag^{-1} : g \in G\},$$

Die Stabilasitoren heißen **Zentralisatoren**

$$Z_G(a) := \mathrm{Stab}_G(a) = \{g \in G : gag^{-1} = a\} = \{g \in G : ga = ag\}.$$

Bemerkungen. (i) Wir sagen, dass $a, b \in G$ **konjugiert** sind, wenn sie in derselben Konjugationsklasse sind, oder äquivalent, wenn $b = gag^{-1}$ für ein $g \in G$. Dies ist eine Äquivalenzrelation.

(ii) Die Fixpunktmenge G^G für diese Aktion ist das **Zentrum**

$$Z(G) := \{a \in G : ga = ag \text{ für alle } g \in G\}.$$

(iii) Wenn $g_1, \ldots, g_r$ Repräsentanten der Konjugationsklassen sind, dann lautet die Klassengleichung

$$|G| = \sum_{i=1}^{r} |CC(g_i)|.$$

Wir können das auch als

$$|G| = |Z(G)| + \sum_{i=1}^{s} |CC(g_i)|,$$

schreiben, wobei $g_1, \ldots, g_s$ Vertreter der Konjugationsklassen mit mehr als einem Element sind.

(iv) Eine Untergruppe $H \subseteq G$ ist genau dann ein Normalteiler, wenn H eine Vereinigung von Konjugationsklassen ist.

(v) Konjugierte Elemente haben die gleiche Ordnung, denn wenn $b = gag^{-1}$, dann $b^n = e \Leftrightarrow ga^n g^{-1} = e \Leftrightarrow a^n = e$.

Beispiel. Die Konjugationsklassen in D_4 sind $\{e\}$, $\{\sigma, \sigma^3\}$, $\{\sigma^2\}$ und $\{\tau, \tau\sigma^2\}$, $\{\tau\sigma, \tau\sigma^3\}$.

Zum Beispiel $\tau\sigma\tau^{-1} = \sigma^3$, $\sigma\tau\sigma^{-1} = \tau\sigma^2$, usw.

Das Zentrum ist $Z(D_4) = \{e, \sigma^2\}$.

Die Klassengleichung ist $8 = 1 + 1 + 2 + 2 + 2$, oder $8 = 2 + 2 + 2 + 2$.

Die Untergruppe $\{e, \sigma, \sigma^2, \sigma^3\}$ der Drehungen hat den Index 2, ist also ein Normalteiler, also eine Vereinigung von Konjugationsklassen.

Proposition. *Zwei Permutationen in S_n sind genau dann konjugiert, wenn sie denselben **Zyklustyp** haben, d.h. wenn sie als Produkte disjunkter Zyklen geschrieben werden, erscheint die gleiche Anzahl von Zyklen jeder Größe.*

Beweis. Wenn

$$\sigma = (a_1\ a_2\ \dots\ a_r)(b_1\ b_2\ \dots\ b_s)\dots,$$

dann

$$\pi\sigma\pi^{-1} = (\pi(a_1)\ \pi(a_2)\ \dots\ \pi(a_r))(\pi(b_1)\ \pi(b_2)\ \dots\ \pi(b_s))\dots.$$

Es hat also den gleichen Zyklustyp. Wenn andererseits ρ die Form

$$\rho = (x_1\ x_2\ \dots\ x_r)(y_1\ y_2\ \dots\ y_s)\dots,$$

hat, dann ist $\rho = \pi\sigma\pi^{-1}$, wobei π die Permutation ist, mit $a_i \mapsto x_i$, $b_j \mapsto y_j$, usw. □

Beispiel. Die Konjugationsklassen in S_4 sind:

Zyklustype	Permutationen	Anzahl
-	e	1
(..)	(1 2),(1 3),(1 4),(2 3),(2 4),(3 4)	6
(...)	(1 2 3),(1 3 2),(1 2 4),(1 4 2),(1 3 4),(1 4 3),(2 3 4),(2 4 3)	8
(....)	(1 2 3 4),(1 2 4 3),(1 3 2 4),(1 3 4 2),(1 4 2 3),(1 4 3 2)	6
(..)(..)	(1 2)(3 4),(1 3)(2 4),(1 4)(2 3)	3

Klassengleichung: $24 = 1 + 6 + 8 + 6 + 3$.

Sei $\sigma = (1\ 2)(3\ 4)$, $\pi = (1\ 3)(2\ 4)$ und $\rho = (1\ 4)(2\ 3)$. Die Menge $V = \{e, \sigma, \pi, \rho\}$ ist eine Untergruppe von S_4, die eine Kleinsche Vierergruppe ist. z.B. $\sigma^2 = \pi^2 = \rho^2 = e$ und $\sigma\pi = \rho$.

Da V eine Vereinigung von Konjugationsklassen ist, ist $V \trianglelefteq S_4$.

Da $V \subseteq A_4$ ist, folgt daraus, dass $V \trianglelefteq A_4$.

Beispiel. Die **platonischen Körper** sind konvexe Polyeder, so dass:

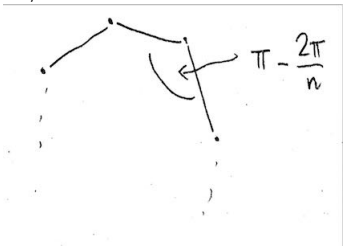
- alle Flächen sind regelmäßige n-Ecke,

- an jeder Ecke treffen k Flächen aufeinander

Für eine beliebige Körperecke ist die Summe der Innenwinkel aller angrenzenden Flächen kleiner als 2π. Der Innenwinkel is $\pi - 2\pi/n$, also brauchen wir

$$k(\pi - 2\pi/n) < 2\pi,$$

oder äquivalent $1/n + 1/k > 1/2$.



Die Möglichkeiten sind:

n	k	Name	Ecken	Flächen	|G|
3	3	Tetraeder	4	4	12
4	3	Würfel	8	6	24
3	4	Oktaeder	6	8	24
5	3	Dodekaeder	20	12	60
3	5	Ikosaeder	12	20	60

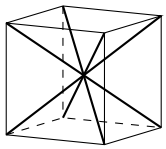
Sei G die Gruppe von Drehungen, die den platonischen Körper erhalten. Durch eine Drehung kann man jede Fläche zu jeder anderen Fläche schicken, mit n möglichen Positionen. Somit ist $|G|$ das Produkt von n und die Anzahl der Flächen.

Die Mittelpunkte der Flächen eines platonischen Körpers sind die Ecken eines anderen Körpers, des Dualen. Das Tetraeder ist selbstdual, der Würfel und das Oktaeder sind dual und das Dodekaeder und das Ikosaeder sind dual.

Duale haben die gleiche Drehgruppe.

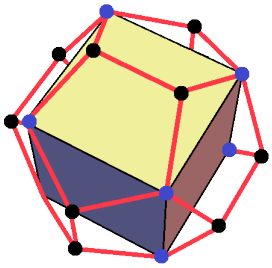
Tetraeder. Die Gruppe operiert auf der Menge aller Ecken. Dies ergibt einen injektiven Homomorphismus $G \to S_4$. Das Bild ist A_4, also $G \cong A_4$.

Würfel. Die Drehgruppe G eines Würfels operiert auf der Menge D aller Diagonalen.



Da $|D| = 4$ bekommen wir einen Homomorphismus $G \to S_4$. Diese Abbildung ist injektiv. Da $|G| = |S_4|$ ist es surjektiv, also $G \cong S_4$.

Dodekaeder. Jede Diagonale einer Fläche des Dodekaeders ist Teil eines einzigartigen einbeschriebenen Würfels. Die Gruppe operiert auf der Menge von 5 einbeschriebenen Würfeln. Dies ergibt einen injektiven Homomorphismus $G \to S_5$. Das Bild ist A_5, also $G \cong A_5$.



(source: Wikipedia)

Beispiel. Sei G die Drehgruppe eines Dodekaeders. Die Konjugationsklassen sind:

Drehachse durch:	Winkel	Anzahl Elemente
-	0	1
Mittelpunkte gegenüberliegender Kanten	π	15
gegenüberliegende Ecken	$\pm 2\pi/3$	20
gegenüberliegende Flächenmittelpunkte	$\pm 2\pi/5$	12
gegenüberliegende Flächenmittelpunkte	$\pm 4\pi/5$	12

Klassengleichung: 1+15+20+12+12=60.

Satz. *Für $n \geq 5$ ist die Gruppe A_n einfach.*

Beweis. Beweis nur für $n = 5$, also für die Gruppe G von Drehungen eines Dodekaeders.

Sei N ein Normalteiler von G.

Dann ist N eine Vereinigung von Konjugationsklassen, einschließlich $\{e\}$.

Somit ist $|N|$ gleich 1 plus eine Summe aus einigen von 15, 20, 12, 12, z.B. $1+15+12 = 28$.

Aber $|N|$ muss 60 teilen.

Die einzige Möglichkeiten sind 1 und 60. Also $N = \{e\}$ oder $N = G$. □

2.3 Die Sylow Sätze

Sei $p \in \mathbb{Z}$ eine Primzahl. Eine Gruppe G heißt **p-Gruppe**, falls $|G| = p^r$ mit $r > 0$.

Satz (Fixpunktsatz für p-Gruppen)**.** *Sei G eine p-Gruppe, und X eine endliche G-Menge. Dann gilt:*

$$|X| \equiv \left|X^G\right| \pmod{p}.$$

Beweis. Die Bahnformel gibt $|Gx| = |G| / |\mathrm{Stab}(x)|$, und diese Zahl ist eine p-Potenz. Die Klassengleichung gibt nun $|X| - \left|X^G\right| = \sum_i |Gx_i|$, wobei jeder Bahn Gx_i nicht trivial ist. Also p teilt jede $|Gx_i|$, und $|X| \equiv \left|X^G\right| \pmod{p}$. □

Korollar (Cauchy)**.** *Sei G eine endliche Gruppe und p einen Primteiler von $|G|$. Dann existiert eine $g \in G$ der Ordnung p.*

Beweis. Wir betrachten die Menge

$$X \coloneqq \{(g_1, \ldots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = e\}.$$

Für $(g_1, \ldots, g_p) \in X$ und $0 \leq r < p$ gilt

$$g_{r+1} \cdots g_p g_1 \cdots g_r = (g_1 \cdots g_r)^{-1}(g_1 \cdots g_p)(g_1 \cdots g_r) = e.$$

Es folgt, dass die Zyklischegruppe $C = \mathbb{Z}/p\mathbb{Z}$ auf X operiert, durch

$$[r] \cdot (g_1, g_2, \ldots, g_p) \coloneqq (g_{r+1}, \ldots, g_p, g_1, \ldots, g_r),$$

und die Fixpunktmenge ist $X^C = \{(g, \ldots, g) \mid g^p = e\}$.

Für jede $(g_2, \ldots, g_p) \in G^{p-1}$ existiert genau eine g_1 mit $(g_1, g_2, \ldots, g_p) \in X$, nämlich $g_1 = (g_2 \cdots g_p)^{-1}$. Also ist $|X| = |G|^{p-1}$ und p teilt $|X|$. Da $(1, 1, \ldots, 1) \in X^C$ und $\left|X^C\right| \equiv |X| \equiv 0 \pmod{p}$, gibt es ein anderes Fixpunkt $(g, g, \ldots, g) \in X^C$, und dieses g hat Ordnung p. □

Korollar. *Jede nicht triviale p-Gruppe hat ein nicht triviales Zentrum.*

Beweis. Eine p-Gruppe G operiert durch Konjugation auf sich selbst, mit Fixpunkte das Zentrum $Z(G)$. Der Fixpunktsatz gibt $|Z(G)| \equiv |G| \equiv 0 \pmod{p}$, und da $e \in Z(G)$ ist $|Z(G)| \geq p$. □

Satz (Sylow 1)**.** *Sei p eine Primzahl und G eine endliche Gruppe. Sei p^r die größte Potenz von p, die $|G|$ teilt, so dass $|G| = p^r m$ mit $\mathrm{ggT}(p, m) = 1$. Wenn $0 \leq s \leq r$, dann existiert eine Untergruppe $P \leq G$ mit $|P| = p^s$.*

Definition. Eine Untergruppe der Ordnung p^r heißt p-**Sylowuntergruppe** von G. Der Fall $s = r$ zeigt, dass p-Sylowuntergruppen immer existieren.

Beweis. Wir können annehmen, dass $s > 0$, sonst ist die Behauptung trivial.

Induktion auf $|G|$. Der Induktionsanfang ist dann $|G| = p$ und in diesem Fall gibt es nichts zu zeigen. Sei nun $|G| > p$. Die Klassengleichung für Konjugation lautet

$$|G| = |Z(G)| + \sum_i |CC(g_i)|$$

wobei die g_i Repräsentanten der Konjugationsklassen der Größe > 1 sind.

Wenn p einen Teiler von $|Z(G)|$ ist, dann existiert eine Untergruppe $K \leq Z(G)$ der Ordnung p (Cauchy). Diese Untergruppe ist einen Normalteiler von G, und die Faktorgruppe G/K hat Ordnung $p^{r-1}m$. Laut Induktion existiert $P' \leq G/K$ der Ordnung p^{s-1}. Nach dem zweiten Isomorphiesatz hat P' die Form P/K mit P von Ordnung $p^s m$.

Wenn p keinen Teiler von $|Z(G)|$ ist, muss es eine i geben, sodass p keinen Teiler von $|CC(g_i)|$ ist. Nun ist $|Z_G(g_i)| = |G| \,/\, |CC(g_i)|$ (Bahnformel), also p^s teilt $|Z_G(g_i)|$. Da $|CC(g_i)| > 1$ ist $|Z_G(g_i)| < |G|$. Laut Induktion existiert eine Untergruppe $P \leq Z_G(g_i) \leq G$ der Ordnung p^s. □

Satz (Sylow 2)**.** *Sei p eine Primzahl, $U \leq G$ eine Untergruppe der Ordnung p^s, und $P \leq G$ eine p-Sylowuntergruppe. Dann existiert $g \in G$ mit $U \subseteq gPg^{-1}$. Insbesondere sind alle p-Sylowuntergruppen von G konjugiert, und damit isomorph.*

Beweis. Dei Gruppe U operiert auf die Linksnebenklassen G/P, $(u, gP) \mapsto ugP$. Da U eine p-Gruppe ist wissen wir, dass $\left|(G/P)^U\right| \equiv |G/P| \pmod{p}$ (Fixpunktsatz). Da P eine p-Sylowuntergruppe ist, gilt $|G/P| \not\equiv 0 \pmod{p}$, also ist $(G/P)^U$ nicht leer.

Sei nun gP ein Fixpunkt. Das heißt, $ugP = gP$ für alle $u \in U$. Umgeschrieben: $g^{-1}ugP = P$, also $g^{-1}ug \in P$ für alle $u \in U$. Äquivalent: $U \subseteq gPg^{-1}$.

Sei U eine p-Sylowuntergruppe. Dann gilt $U = gPg^{-1}$. Also ist die Abbildung $p \mapsto gpg^{-1}$ ein Isomorphismus $P \to U$. □

Satz (Sylow 3)**.** *Sei $|G| = p^r m$ mit $\mathrm{ggT}(p, m) = 1$, und sei n_p die Anzahl aller p-Sylowuntergruppen von G. Dann ist n_p ein Teiler von m und $n_p \equiv 1 \pmod{p}$.*

Beweis. Sei X die Menge alle p-Sylowuntergruppen von G. Die Gruppe G operiert durch Konjugation auf X. Laut Sylow 2 gibt es nur eine Bahn, mit n_p Elemente. Die Stabilisator von P, auch **Normalisator** von P in G genannt, ist

$$N_G(P) = \{g \in G : gPg^{-1} = P\}.$$

Klar ist, dass $P \trianglelefteq N_G(P)$. In der Tat ist $N_G(P)$ die größte Untergruppe von G die P als Normalteiler enthält. Daher der Name „Normalisator“.

Die Bahnformel gibt jetzt $n_p = |G/N_G(P)|$. Da $P \leq N_G(P)$ ist, muss n_p einen Teiler von m sein (Lagrange).

Schließlich betrachten wir die eingeschränkte Aktion von P auf X. Es ist klar, dass P einen Fixpunkt ist. Sei nun Q ein beliebiger Fixpunkt. Dann ist $Q \trianglelefteq N_G(Q)$ ein Normalteiler und eine p-Sylowuntergruppe. Laut Sylow 2 ist Q die einzige p-Sylowuntergruppe von $N_G(Q)$. Da $P \leq N_G(Q)$ auch eine p-Sylowuntergruppe ist, muss $P = Q$ sein. Es folgt, dass es genau einen Fixpunkt gibt, und den Fixpunktsatz gibt

$$n_P = |X| \equiv \left|X^P\right| = 1 \pmod{p}.$$ □

2.4 Anwendungen der Sylow Sätze

Die Sylow Sätze helfen, die strukture endliche Gruppen zu beschreiben.

Proposition (1)**.** *Jede Gruppe der Ordnung 15 ist zyklisch.*

Beweis. Sei G eine Gruppe der Ordnung 15 und n_p die Anzahl aller p-Sylowuntergruppen von G. Laut Sylow 3 ist n_3 ein Teiler von 5 und $n_3 \equiv 1 \pmod{3}$. Es

folgt, dass $n_3 = 1$ ist und die 3-Sylowuntergruppe $N \cong \mathbb{Z}/\mathbb{Z}3$ ist einen Normalteiler. Ähnlich gibt es nur eine 5-Sylowuntergruppe $K \cong \mathbb{Z}/\mathbb{Z}5$. Nun muss $N \cap K = \{e\}$ sein (Lagrange), und $NK \cong N \times K$ ist eine Untergruppe von G nach §1.5 Proposition. Da $|N \times K| = 15$ ist, folgt $G \cong N \times K \cong \mathbb{Z}/\mathbb{Z}15$ (Chinesischer Restsatz für Gruppen). □

Proposition (2)**.** *Es gibt keine einfache Gruppe der Ordnung 30.*

Beweis. Wir nehmen an, dass G eine einfache Gruppe der Ordnung 30 ist. Laut Sylow 3 ist n_5 ein Teiler von 6 und $n_5 \equiv 1 \pmod 5$, also ist $n_5 \in \{1, 6\}$. Wenn $n_5 = 1$ ist, dann ist die 5-Sylowuntergruppe von G einen Normalteiler. Widerspruch. Also ist $n_5 = 6$. Seien jetzt $P \neq Q$ zwei 5-Sylowuntergruppen von G. Wir haben $|P| = 5$, also $P \cong \mathbb{Z}/\mathbb{Z}5$, und $P \cap Q$ ist eine echte Untergruppe von P, also $P \cap Q = \{e\}$. Schließlich erzeugt jedes Element der Ordnung 5 erzeugt eine zyklische Gruppe der Ordnung 5, die in eine 5-Sylowuntergruppe enthalten sein muss (Sylow 2). Es folgt, dass G genau $6 \cdot 4 = 24$ Elemente der Ordnung 5 hat.

Ähnlich Argumente zeigen, dass $n_3 = 10$, $P' \cong \mathbb{Z}/\mathbb{Z}3$ für jede 3-Sylowuntergruppe, und $P' \cap Q' = \{e\}$ für zweu verschiedene 3-Sylowuntergruppen P', Q'. Also enthält G genau $10 \cdot 2 = 20$ Elemente der Ordnung 3. Das heißt, G hat mindestens 45 Elemente. Widerspruch. Es gibt also keine einfache Gruppe der Ordnung 30. □

Die Gruppen der Primzahlordnung p sind zyklisch also abelsch, und einfach $\mathbb{Z}/\mathbb{Z}p$. Jede endliche einfache abelsche Gruppe hat diese Form.

Wir können Sylow-Theoreme verwenden, um zu zeigen, dass die kleinste nichtabelsche einfache Gruppe die Ordnung 60 hat. Tatsächlich ist die Gruppe A_5 die eindeutige einfache Gruppe der Ordnung 60.

Die nächstgrößere nicht-abelsche einfache Gruppe hat Ordnung 168. Sie ist

$$\mathrm{GL}_3(\mathbb{Z}_2) \cong \mathrm{SL}_2(\mathbb{Z}_7)/Z(\mathrm{SL}_2(\mathbb{Z}_7)).$$

Es gibt eine sehr komplizierte Klassifizierung aller endlichen einfachen Gruppen.

Es gibt eine nichtabelsche Gruppe der Ordnung 21. Mithilfe der Sylow-Sätze werden wir zeigen, dass sie eindeutig ist.

Lemma. *(i) Die Menge* $F = \{x^m y^n : 0 \leq m < 7, 0 \leq n < 3\}$ *mit der Verknüpfung*

$$x^m y^n \cdot x^p y^q \coloneqq x^r y^s, \quad r \equiv m + 2^n p \pmod 7 \quad \textit{und} \quad s \equiv n + q \pmod 3$$

ist eine nichtabelsche Gruppe der Ordnung 21.

(ii) F enthält Elemente x, y mit $F = \langle x, y\rangle$ und $x^7 = y^3 = e$ und $yx = x^2y$.

(iii) Wenn G eine Gruppe ist, die Elemente X, Y enthält, mit $G = \langle X, Y\rangle$ und $X^7 = Y^3 = e$ und $YX = X^2Y$, dann gibt es einen surjektiven Homomorphismus $\theta : F \to G$, so dass $\theta(x) = X$ und $\theta(y) = Y$.

Beweis. (i) Man kann überprüfen, dass die Verknüpfung assoziativ ist. Das neutrale Element ist $e = x^0y^0$. Die Inverse von x^my^n ist $x^0y^{3-n} \cdot x^{7-m}y^0$.

(ii) gilt mit $x = x^1y^0$ und $y = x^0y^1$.

(iii) Wir definieren $\theta : F \to G$ durch $\theta(x^my^n) = X^mY^n$. In G gilt $YX^p = X^{2p}Y$, also $Y^nX^p = X^{2^np}Y^n$, also

$$\theta(x^my^n)\theta(x^py^q) = X^mY^nX^pY^q = X^{m+2^np}Y^{n+q} = X^rY^s = \theta(x^ry^s) = \theta((x^my^n)(x^py^q)).$$

Also ist θ ein Homomorphismus. Es ist surjektiv, da $X, Y \in \text{Bild}(\theta)$ und $G = \langle X, Y\rangle$. □

Proposition (3)**.** *Sei G eine Gruppe der Ordnung 21. Dann ist G entweder zyklisch, oder isomorph zu F.*

Beweis. Laut Sylow 3 ist $n_7 = 1$, also hat G genau eine 7-Sylowuntergruppe $N \cong \mathbb{Z}/7\mathbb{Z}$, und die ist einen Normalteiler von G.

Sei $H \cong \mathbb{Z}/3\mathbb{Z}$ eine 3-Sylowuntergruppe. Wie beim ersten Isomorphiesatz ist NH eine Untergruppe von G. Da $N \cap H = \{e\}$ (Lagrange) gilt weiter, dass jedes Element in NH eindeutig als nh mit $n \in N$ und $h \in H$ geschrieben sein kann. Also ist $|NH| = 21$ und $NH = G$. Seien $a \in N$ und $b \in H$ Erzeuger, sodass $G = \{a^mb^n \mid 0 \le m < 7, 0 \le n < 3\}$.

Nun ist $bNb^{-1} = N$, also $bab^{-1} = a^r$ mit $0 < r < 7$. Es folgt:

$$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = a^{r^2}.$$

Weiter gilt

$$b^3ab^{-3} = b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = a^{r^3}.$$

Da $b^3 = e$ ist, muss $a^{r^3} = a$ sein, also $r^3 \equiv 1 \pmod 7$. Die mögliche Lösungen sind dann $r \in \{1, 2, 4\}$.

Ist $r = 1$, dann ist $ba = ab$ und G is abelsch. Es folgt, dass ab Ordnung 21 hat, und G ist zyklisch.

Ist $r = 2$, dann gilt $G = \langle a, b\rangle$, $a^7 = b^3 = e$, $ba = a^2b$. Also gibt es einen surjektive Homomorphismus $\theta\colon F \to G$, $\theta(x) = a$ und $\theta(y) = b$.

Ist $r = 4$, dann gilt $ba = a^4b$. Es gilt $G = \langle a, c\rangle$ mit $c = b^{-1}$. Dann $ac = ca^4$, also $a^2c = ca^8 = ca$. Also gibt es einen surjektive Homomorphismus $\theta\colon F \to G$, $\theta(x) = a$ und $\theta(y) = c$.

Da beide Gruppen Ordnung 21 haben, haben wir in beiden Fällen einen Isomorphismus. □

2.5 Endliche abelsche Gruppen

Satz (Struktursatz für endliche abelsche Gruppen)**.** *Jede endliche abelsche Gruppe G ist isomorph zu einem Produkt zyklischer Gruppen mit Primpotenz Ordnungen, also*

$$G \cong \mathbb{Z}/\mathbb{Z}q_1 \times \cdots \times \mathbb{Z}/\mathbb{Z}q_t \quad \textit{für Primpotenzen } q_i.$$

Weiterhin ist die Liste $(q_1, \ldots, q_t)$ bis auf die Reihenfolge eindeutig bestimmt.

Beispiel. Bis auf Isomorphie gibt es 3 abelsche Gruppen der Ordnung 24:

$$\mathbb{Z}/\mathbb{Z}8 \times \mathbb{Z}/\mathbb{Z}3 \text{ (zyklisch)}, \quad \mathbb{Z}/\mathbb{Z}4 \times \mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}3, \quad (\mathbb{Z}/\mathbb{Z}2)^3 \times \mathbb{Z}/\mathbb{Z}3.$$

Beweis. Schritt (1) Eine p-Gruppe.

Induktion über $|G|$.

Sei $g \in G$ ein Element der maximale Ordnung. Sei $H \leq G$ eine Untergruppe, die maximal bezüglich $H \cap \langle g\rangle = \{e\}$ ist.

Wir zeigen, dass $G = H\langle g\rangle$. Angenommen, nicht. Die Faktorgruppe

$$\bar{G} = G \,/\, H\langle g\rangle$$

ist eine nicht triviale p-Gruppe. Laut Cauchy gibt es $x \in G$, sodass $\bar{x}$ Ordnung p in $\bar{G}$ hat. Das heißt, $x^p = hg^a$ mit $h \in H$ und $a \in \mathbb{Z}$.

Weil $x \in G$, ist $\operatorname{ord}(x)$ ein Potenz von p, also

$$\operatorname{ord}(x) = p \operatorname{ord}(hg^a) = p \operatorname{kgV}(\operatorname{ord}(h), \operatorname{ord}(g^a))$$

nach §1.6 Proposition (3).

Wenn p kein Teiler von a ist, dann nach §1.6 Proposition (1),

$$\operatorname{ord}(g^a) = \operatorname{ord}(g)/\operatorname{ggT}(a, \operatorname{ord}(g)) = \operatorname{ord}(g).$$

Also $\operatorname{ord}(x) \geq p \operatorname{ord}(g^a) = p \operatorname{ord}(g) > \operatorname{ord}(g)$, ein Widerspruch.

Also $a = pb$. Wir setzen $y := xg^{-b}$. Also $y^p = h \in H$ und $\bar{y} = \bar{x}$, also $y \notin H\langle g \rangle$. Sei $H' := H\langle y \rangle$. Dies ist eine größere Untergruppe als H.

Sei $z \in H' \cap \langle g \rangle$, also $z = h_1 y^c = g^d$ mit $h_1 \in H$ und $c, d \in \mathbb{Z}$. Ist p kein Teiler von c, dann existiert $r, s \in \mathbb{Z}$, so dass $cr + \operatorname{ord}(y)s = 1$. Also

$$y = y^{cr+\operatorname{ord}(y)s} = y^{cr} = (g^d h_1^{-1})^r = h_1^{-r} g^{dr} \in H\langle g \rangle,$$

einen Widerspruch. Also ist $c = c_1 p$, $y^c = h^{c_1} \in H$, und $z \in H \cap \langle g \rangle = \{e\}$. Widerspruch, wegen der Maximalität von H.

Es folgt, dass $G = H\langle g \rangle$. Nach §1.5 Proposition ist $G \cong H \times \langle g \rangle$. Nach der Induktion ist H ein Produkt zyklischer Gruppen, daher auch G.

Schritt (2) Eine beliebige endliche abelsche Gruppe.

Seien $N_1, \ldots, N_r$ Sylow p-Untergruppen für die verschiedenen Primteiler von $|G|$.

Wir definieren Untergruppen $H_s \leq G$ für $0 \leq s \leq r$ durch $H_0 = \{e\}$ und

$$H_s = H_{s-1} N_s$$

für $s > 0$. Dies ist eine Untergruppe nach dem ersten Isomorphiesatz. Wir zeigen durch Induktion, dass

$$H_s \cong N_1 \times \cdots \times N_s.$$

Für $s = 0$ stimmt es. Für den induktiven Schritt ist $H_{s-1} \cong N_1 \times \cdots \times N_{s-1}$, also ist die Ordnung teilerfremd zu N_s. Also nach dem Satz von Lagrange

$$H_{s-1} \cap N_s = \{e\}.$$

Also nach §1.5 Proposition,

$$H_s = H_{s-1} N_s \cong H_{s-1} \times N_s \cong N_1 \times \cdots \times N_{s-1} \times N_s.$$

Nun ist H_r eine Untergruppe von G mit

$$H_r \cong N_1 \times N_2 \times \cdots \times N_r.$$

Also $|H_r| = |G|$, also $G = H_r$. Jedes N_i ist ein Produkt zyklischer Gruppen Primzahlpotenz, also so ist G.

Schritt (3) Eindeutikgeit.

Für eine abelsche Gruppe G mit additive Notation und $m \in \mathbb{Z}$ definieren wir

$$mG = \{mg : g \in G\} \leq G.$$

Für $G = G_1 \times \cdots \times G_t$ ist $mG = mG_1 \times \cdots \times mG_t$, und für $G = \mathbb{Z}/\mathbb{Z}q$ ist $m(\mathbb{Z}/\mathbb{Z}q) = (\mathbb{Z}q + \mathbb{Z}m)/\mathbb{Z}q = \mathbb{Z}\,\mathrm{ggT}(q,m)/\mathbb{Z}q$, also $|mG| = q/\,\mathrm{ggT}(q,m)$.

Für $G = \mathbb{Z}/\mathbb{Z}q_1 \times \cdots \times \mathbb{Z}/\mathbb{Z}q_t$ gilt

$$|mG| = \prod_{i=1}^{t} q_i/\,\mathrm{ggT}(q_i, m).$$

Wenn die q_i Primpotenzen sind, gilt

$$\frac{|p^{r+1}G| \cdot |p^{r-1}G|}{|p^r G|^2} = p^k, \quad k = |\{i : q_i = p^r\}|.$$

□

3 Ringe

3.1 Definitionen und Beispiele

Anders als in LA I betrachten wir nur Ringe mit einem Eins-Element.

Definition. Ein **Ring** ist eine Menge R zusammen mit zwei Verknüpfungen Addition und Multiplikation

$$+ : R \times R \to R, (a, b) \mapsto a + b, \quad \cdot : R \times R \to R, (a, b) \mapsto a \cdot b \text{ oder } ab$$

sodass

(1) $(R, +)$ ist eine additive Gruppe (abelsch). Das neutrales Element ist 0.

(2) Die Multiplikation ist assoziativ $(ab)c = a(bc)$ für alle $a, b, c \in R$.

(3) Es gelten die **Distributivgesetze**: für alle $a, b, c \in R$ gelten

$$a(b + c) = (ab) + (ac) \quad \text{und} \quad (a + b)c = (ac) + (bc).$$

(4) Es gibt ein **Eins-Element** 1, d.h. $1a = a = a1$ für alle $a \in R$.

Ein Ring ist **kommutativ**, wenn $ab = ba$ für alle $a, b \in R$.

Ein Element $a \in R$ heißt **invertierbar** oder eine **Einheit**, wenn es $b \in R$ mit $ab = ba = 1$ gibt. In diesem Fall ist b eindeutig und wird mit a^{-1} bezeichnet. Wir setzen

$$R^\times = \{a \in R : a \text{ ist invertierbar}\}.$$

Sie ist eine Gruppe unter Multiplikation.

Ein **Körper** ist ein kommutativer Ring mit $0 \neq 1$ und wobei jedes von Null verschiedene Element invertierbar ist.

Bemerkungen. Die Folgenden sind einfach (sehen Sie LA I §2.2)

(1) Es kann nur ein Eins geben: Wenn beide 1 und $1'$ Eins-Elemente sind, dann gilt $1 = 11' = 1'$.

(2) $0a = a0 = 0$ für alle $a \in R$.

(3) $a(-b) = -(ab) = (-a)b$ und $(-a)(-b) = ab$ für alle $a, b \in R$

(4) $0 = 1$ genau dann, wenn R der Nullring $\{0\}$ ist.

Beispiele. (a) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Körper. $\mathbb{Z}$ ist ein Ring mit $\mathbb{Z}^\times = \{1, -1\}$.

(b) Sei R ein Ring und $n > 0$. Der **Matrixring** $M_n(R)$ ist die Menge alle Matrizen der Größe n mit Einträge aus R. Dann ist $M_n(R)$ ein Ring bezüglich die übliche Addition und Multiplikation von Matrizen. Im allgemein ist es nicht kommutativ.

Wenn K ein Körper ist, gilt $M_n(K)^\times = \mathrm{GL}_n(K)$.

(c) Seien R und S Ringe. Dann ist $R \times S$ ein Ring bezüglich komponentenweise Addition und Multiplikation

$$(a, b) + (c, d) \coloneqq (a + b, c + d) \quad \text{und} \quad (a, b)(c, d) \coloneqq (ac, bd).$$

Die Null ist $(0, 0)$ und das Eins ist $(1, 1)$. Allgemeiner ist ein Produkt $\prod_{i \in I} R_i$ von Ringen R_i ein Ring.

(d) Die Menge $\mathrm{Abb}(X, R) = R^X$ aller Abbildungen von einer Menge X auf einen Ring R ist ein Ring bezüglich punktweise Addition und Multiplikation:

$$(f + g)(x) \coloneqq f(x) + g(x) \quad \text{und} \quad (f \cdot g)(x) \coloneqq f(x)g(x) \quad \forall f, g \in R^X \ \forall x \in X.$$

Die Null ist $0\colon x \mapsto 0$ und das Eins ist $1\colon x \mapsto 1$. Wir können identifizieren $\mathrm{Abb}(X, R) = \prod_{x \in X} R$.

(e) Sei R ein Ring. Der **Polynomring** $R[X]$, mit **Koeffizienten** in R und **Unbekannte** X, hat Elemente

$$p(X) = a_0 + a_1 X + a_2 X^2 + \cdots = \sum_{n \geq 0} a_n X^n$$

mit $a_n \in R$ fast alle Null (d.h. alle bis auf endlich viele Null), punktweise Addition

$$\sum_n a_n X^n + \sum_n b_n X^n \coloneqq \sum_n (a_n + b_n) X^n$$

und Multiplication

$$\sum_n a_n X^n \cdot \sum_n b_n X^n \coloneqq \sum_n c_n X^n \quad \text{wobei } c_n = \sum_{r+s=n} a_r b_s.$$

Das Eins-Element ist $1 = X^0$.

(f) Für n unbestimmte $X_1, X_2, \ldots, X_n$ hat der Polynomring $R[X_1, X_2, \ldots, X_n]$ Elemente der Form

$$p(X_1, X_2, \ldots, X_n) = \sum_{m_1, m_2, \ldots, m_n \geq 0} a_{m_1, m_2, \ldots, m_n} X_1^{m_1} X_2^{m_2} \ldots X_n^{m_n}$$

mit $a_{m_1,m_2,\ldots,m_n} \in R$ fast alles Null.

Allgemeiner: sei X_i für $i \in I$ eine beliebige Familie von Unbestimmten. Sei

$$\mathbb{N}^{(I)} = \{\alpha = (\alpha_i)_{i\in I} \in \mathbb{N}^I : \alpha_i = 0 \text{ für fast alle } i \in I\}.$$

Die Addition $\alpha + \beta \in \mathbb{N}^{(I)}$ für $\alpha, \beta \in \mathbb{N}^{(I)}$ ist komponentenweise definiert. Der Polynomring $R[X_i : i \in I]$ hat Elemente der Form

$$\sum_{\alpha\in\mathbb{N}^{(I)}} a_\alpha X^\alpha, \quad X^\alpha := \prod_i X_i^{\alpha_i}$$

mit $a_\alpha \in R$ fast alle Null. Die Addition ist

$$\sum a_\alpha X^\alpha + \sum b_\alpha X^\alpha = \sum (a_\alpha + b_\alpha) X^\alpha$$

Die Multiplication ist

$$\sum a_\alpha X^\alpha \cdot \sum b_\alpha X^\alpha = \sum c_\alpha X^\alpha, \quad c_\alpha = \sum_{\alpha=\beta+\gamma} a_\beta b_\gamma.$$

3.2 Teilringe, Ideale und Ringhomomorphismen

In der Gruppentheorie betrachten wir Untergruppen und Normalteiler. In der Ringtheorie sind die analogen Konzepte Teilringe und Ideale. Im Gegensatz zu Gruppen ist ein Ideal jedoch normalerweise kein Teilring.

Definition. Sei R ein Ring. Ein **Teilring** oder **Unterring** von R ist eine Teilmenge $T \subseteq R$, die ein Ring unter den (Einschränkungen) derselben Verknüpfungen wie R und mit demselben Eins-Element ist. Äquivalent ist:

(i) $(T, +) \leq (R, +)$ ist eine Untergruppe bezüglich Addition,

(ii) $st \in T$ für alle $s, t \in T$, und

(iii) $1_R \in T$.

Beispiele. (1) $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

(2) Die Menge der oberen Dreiecksmatrizen

$$T_n(R) = \{A = (a_{ij}) \in M_n(R), a_{ij} = 0 \text{ für } i > j\}$$

ist ein Teilring von $M_n(R)$.

(3) Die Menge $C(\mathbb{R},\mathbb{R})$ stetiger Funktionen $\mathbb{R}\to\mathbb{R}$ ist ein Teilring von $\mathrm{Abb}(\mathbb{R},\mathbb{R})$.

(4) Sei $T,U\subseteq R$ Teilringe. Dann ist der Schnitt $T\cap U$ ein Teilring von R. Allgemeiner: Sei R_i $(i\in I)$ eine Familie von Teilringen. Dann ist $\bigcap_{i\in I}R_i$ ein Teilring von R. Somit gibt es für jede Teilmenge $X\subseteq R$ einen eindeutigen kleinsten Teilring von R, der X enthält. Er ist der Schnitt aller Teilringe von R, die X enthalten.

(5) Ist $K\leq R$ ein Teilring, der auch ein Körper ist, dann ist R ein K-Vektorraum bezüglich die übliche Addition und eingeschränkte Multiplikation $K\times R\to R$, $(\lambda,a)\mapsto\lambda a$.

Definition. Sei R ein Ring. Ein **Ideal** $I\trianglelefteq R$ ist eine Teilmenge, sodass

(i) $(I,+)\leq(R,+)$ eine Untergruppe bezüglich Addition ist, und

(ii) $ax\in I$ und $xa\in I$ für alle $a\in R$ und $x\in I$.

Beispiele. (1) $\{0\}$ und R sind Ideale im Ring R.

(2) Wenn $I\trianglelefteq R$ und $1\in I$, dann ist $I=R$. Insbesondere wenn I ein Ideal in R und auch ein Teilring ist, dann ist $I=R$. Allgemeiner: Wenn I ein invertierbares Element enthält, dann ist $I=R$.

(3) Sei R ein kommutative Ring und $a\in R$. Dann ist $Ra=\{ra:r\in R\}$ ein Ideal, gennant **Hauptideal**. Jede additive Untergruppe von $\mathbb{Z}$ hat die Form $\mathbb{Z}m$ mit $m\geq 0$. Somit ist jedes Ideal in $\mathbb{Z}$ ein Hauptideal.

(4) Wenn R ein kommutativer Ring ist, dann ist $Ra=R$ genau dann, wenn a invertierbar ist. Daraus folgt, dass ein kommutativer Ring R genau dann ein Körper ist, wenn er genau zwei Ideale hat, $\{0\}$ und R.

(5) Sei R ein Ring, X eine Menge und $x\in X$. Dann ist $I\coloneqq\{f\in\mathrm{Abb}(X,R):f(x)=0\}$ ein Ideal in $\mathrm{Abb}(X,R)$.

(6) Seien $I\trianglelefteq R$ und $J\trianglelefteq S$. Dann ist $I\times J\trianglelefteq R\times S$.

(7) Seien $I,J\trianglelefteq R$ Ideale. Dann ist $I+J=\{x+y:x\in I,y\in J\}$ ein Ideal in R.

Allgemeiner: Wenn I_i $(i\in I)$ eine Familie von Idealen in R ist, dann ist

$$\sum_{i\in I}I_i:=\{\sum_{i\in I}x_i:x_i\in I_i,\text{ fast alle Null}\}$$

ein Ideal in R.

(8) Seien $I,J\trianglelefteq R$ Ideale. Dann ist $I\cap J$ ein Ideal. In Allgemeinen ist der Schnitt über eine beliebige Familie von Idealen in R wieder ein Ideal in R. Für eine Teilmenge

$X \subseteq R$ definieren wir also das **von X erzeugten Ideal** $(X) \trianglelefteq R$ als das kleinste Ideal von R, das X enthält.

Wenn R ein kommutativer Ring ist, gelten $(a) = Ra$ und $(X) = \sum_{a \in X} Ra$.

(9) Für $I, J \trianglelefteq R$ Ideale, dann ist IJ der Ideal, die von $\{xy : x \in I,\ y \in J\}$ erzeugt ist. Die Elemente sind endliche Summen $\sum_i x_i y_i$ mit $x_i \in I$ und $y_i \in J$.

Definition. Eine Abbildung $\theta\colon R \to S$ zwischen zwei Ringe heißt **Homomorphismus** (oder Ringhomomorphismus) falls

$$\theta(a+b) = \theta(a) + \theta(b), \quad \theta(ab) = \theta(a)\theta(b), \quad \theta(1_R) = 1_S.$$

Da θ eine additive Gruppenhomomorphismus ist, muss $\theta(0_R) = 0_S$.

Ein **Isomorphismus** $\theta : R \to S$ ist ein Homomorphismus, der bijektiv ist.

Proposition. *Sei $\theta\colon R \to S$ ein Ringhomomorphismus.*

(i) $\mathrm{Bild}(\theta) = \{\theta(r) \mid r \in R\}$ *ist ein Teilring von S. Zudem induziert θ einen surjektiven Homomorphismus $R \to \mathrm{Bild}(\theta)$.*

(ii) $\mathrm{Ker}(\theta) = \{r \in R \mid \theta(r) = 0\}$ *ist ein Ideal in R. Zudem ist θ injektive genau dann, wenn* $\mathrm{Ker}(\theta)$ *trivial ist. In diesem Fall gibt θ ein Isomorphismus $G \to \mathrm{Bild}(\theta)$.*

(iii) Sei $\phi\colon S \to T$ ein Ringhomomorphismus. Dann ist $\phi\theta\colon R \to T$ ein Ringhomomorphismus.

(iv) Wenn θ ein Isomorphismus ist, dann ist $\theta^{-1} : S \to R$ ein Isomorphismus.

Beweis. (i) Da θ eine additive Gruppenhomomorphismus ist, muss $\theta(R)$ eine additive Untergruppe von S sein. Seien $s_i \coloneqq \theta(r_i)$. Dann ist $s_1 s_2 = \theta(r_1)\theta(r_2) = \theta(r_1 r_2) \in \mathrm{Im}(\theta)$ und $1_S = \theta(1_R) \in \mathrm{Im}(\theta)$. Also ist $\mathrm{Im}(\theta)$ einen Teilring.

(ii) $\mathrm{Ker}(\theta)$ ist eine additive Untergruppe von R, und für $a \in R$ und $x \in \mathrm{Ker}(\theta)$ gilt $\theta(ax) = \theta(a)\theta(x) = 0$, also ist $ax \in \mathrm{Ker}(\theta)$. Ähnlich für xa.

Der Rest ist leicht. □

Beispiele. (1) Die Identität $\mathrm{id}\colon R \to R$ ist immer einen Ringhomomorphismus. Ist $R \subseteq S$ ein Teilring, dann ist die Inklusion $R \to S$ ein injektive Ringhomomorphismus.

(2) Sei R ein Ring. Es gibt genau einen Ringhomomorphismus $\theta\colon \mathbb{Z} \to R$.

(3) Sei R ein Ring und X eine Menge. Für festes $x \in X$ ist die Abbildung $\mathrm{ev}_x \colon \mathrm{Abb}(X, R) \to R$, $f \mapsto f(x)$, einen Ringhomomorphismus.

(4) Es gibt ein injektive Homomorphismus $R \to R[X_1, \ldots, X_n]$, $a \mapsto a$. Also können wir R als ein Teilring von $R[X_1, \ldots, X_n]$ identifizieren.

(5) Es gibt einen Isomorphismus

$$R[X, Y] \to (R[X])[Y], \quad \sum_{m,n \geq 0} a_{m,n} X^m Y^n \mapsto \sum_{n \geq 0} \left(\sum_{m \geq 0} a_{m,n} X^m \right) Y^n.$$

Ähnlich gibt es einen Isomorphismus

$$R[X_1, \ldots, X_n] \to (R[X_1, \ldots, X_r])[X_{r+1}, \ldots, X_n],$$

$$\sum_{m_1, \ldots, m_n} a_{m_1, \ldots, m_n} X^{m_1} \ldots X^{m_n} \mapsto \sum_{m_{r+1}, \ldots, m_n} \left(\sum_{m_1, \ldots, m_r} a_{m_1, \ldots, m_n} X^{m_1} \ldots X^{m_r} \right) X^{m_{r+1}} \ldots X^{m_n}$$

Definition. Sei R ein kommutative Ring. Die Auswertung (Englisch: evaluation) von

$$p(X_1, X_2, \ldots, X_n) = \sum_{m_1, m_2, \ldots, m_n \geq 0} a_{m_1, m_2, \ldots, m_n} X_1^{m_1} X_2^{m_2} \ldots X_n^{m_n} \in R[X_1, \ldots, X_n],$$

an $r = (r_1, \ldots, r_n) \in R^n$ ist

$$p(r_1, \ldots, r_n) := \sum_{m_1, m_2, \ldots, m_n \geq 0} a_{m_1, m_2, \ldots, m_n} r_1^{m_1} r_2^{m_2} \ldots r_n^{m_n} \in R.$$

Allgemeiner gesagt: Wenn R ein Teilring eines kommutativen Rings S ist und $s = (s_1, \ldots, s_n \in S^n$, können wir $p(s_1, \ldots, s_n) \in S$ betrachten durch Identifizieren von $R[X_1, \ldots, X_n]$ als Teilring von $S[X_1, \ldots, X_n]$.

Lemma (1)**.** *Sei R ein kommutative Ring und sei $r = (r_1, \ldots, r_n) \in R^n$. Die Auswertungsabbildung*

$$\mathrm{ev}_r : R[X_1, \ldots, X_n] \to R, \quad p(X_1, \ldots, X_n) \mapsto p(r_1, \ldots, r_n)$$

ist ein Ringhomomorphismus. Die Abbildung

$$R[X_1, \ldots, X_n] \to \mathrm{Abb}(R^n, R), \quad p(X_1, \ldots, X_n) \mapsto ((r_1, \ldots, r_n) \mapsto p(r_1, \ldots, r_n))$$

ist auch ein Ringhomomorphismus.

z.B. $\mathrm{ev}_0(p(X_1,\ldots,X_n))$ ist der konstante Koeffizient von $p(X_1,\ldots,X_n)$.

Bemerkung. Das Bild des Homomorphismus $R[X_1,\ldots,X_n] \to \mathrm{Abb}(R^n, R)$ ist die Menge der **Polynomabbildungen** $R^n \to R$. Im Allgemeinen ist der Homomorphismus nicht injektiv, sodass verschiedene Polynome dieselbe Polynomabbildung ergeben können.

Wenn K ein unendlicher Körper ist, ist der Homomorphismus $K[X] \to \mathrm{Abb}(K, K)$ injektiv, denn wenn $p(X)$ auf 0 geschickt wird, dann ist $p(r) = 0$ für alle $r \in K$. Da K unendlich ist, bedeutet dies, dass $p(X)$ unendlich viele Nullstellen hat. Ein Polynom ungleich Null kann jedoch nur endlich viele Nullstellen haben. Aus diesem Grund können Polynome über einem unendlichen Körper K mit den entsprechenden Polynomfunktionen $K \to K$ identifiziert werden.

Lemma (2)**.** *Sei S ein kommutative Ring, $R \subseteq S$ ein Teilring and $s_1,\ldots,s_n$ Elemente von S. Der eindeutige kleinste Teilring von S, der $R \cup \{s_1,\ldots,s_n\}$ enthält, ist*

$$R[s_1,\ldots,s_n] := \{p(s_1,\ldots,s_n) : p(X_1,\ldots,X_n) \in R[X_1,\ldots,X_n]\}.$$

Es ist das Bild des Homomorphismus

$$R[X_1,\ldots,X_n] \to S, \quad p(X_1,\ldots,X_n) \mapsto p(s_1,\ldots,s_n).$$

Dies ist die Komposition der Inklusion $R[X_1,\ldots,X_n] \to S[X_1,\ldots,X_n]$ und der Abbildung $ev_s : S[X_1,\ldots,X_n] \to S$.

z.B.

$$\mathbb{Z}[i] = \{a_0 + a_1 i + a_2 i^2 + \cdots + a_n i^n : a_j \in \mathbb{Z}\} = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

und

$$\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Z}\} \subseteq \mathbb{R}$$

Warnung: Die Notation ist hier leider einfach zu verwechseln. $R[X_1,\ldots,X_n]$ ist der Polynomring mit Unbekannten $X_1,\ldots,X_n$, aber $R[s_1,\ldots,s_n]$ ist ein Teilring von S.

Lemma (3)**.** *Sei $\theta : R \to S$ ein Ringhomomorphismus mit S kommutativ und Elemente $s_1,\ldots,s_n \in S$. Es gibt eine eindeutige Erweiterung von θ zu einem Homomorphismus $\tilde{\theta} : R[X_1,\ldots,X_n] \to S$ mit $\tilde{\theta}(X_i) = s_i$.*

Beweis. Für

$$p(X_1, X_2, \ldots, X_n) = \sum_{m_1,m_2,\ldots,m_n \geq 0} a_{m_1,m_2,\ldots,m_n} X_1^{m_1} X_2^{m_2} \ldots X_n^{m_n} \in R[X_1,\ldots,X_n]$$

müssen wir haben

$$\tilde{\theta}(p(X_1,\ldots,X_n)) = \sum_{m_1,m_2,\ldots,m_n\geq 0} \theta(a_{m_1,m_2,\ldots,m_n}) s_1^{m_1} s_2^{m_2} \ldots s_n^{m_n} \in S$$

und dies definiert einen Homomorphismus. □

Bemerkung. Für eine beliebige Familie von Unbekannten X_i $(i \in I)$ können wir die Auswertung von Polynomen in $R[X_i : i \in I]$ an einem Element $r = (r_i) \in R^I$ definieren. Lemma (1)-(3) lassen sich alle leicht auf diese Situation verallgemeinern. Nur die Notation ist schwieriger.

3.3 Faktorringe und die Isomorphiesätze

Proposition. *Sei $I \trianglelefteq R$ ein Ideal und sei R/I die Faktorgruppe von R, die als additive Gruppe betrachtet wird. Somit sind die Elemente von R/I die Nebenklassen $\bar{a} = I + a$ für $a \in R$ und die Addition ist*

$$\bar{a} + \bar{b} = \overline{a+b}.$$

Dann ist R/I ein Ring bezüglich der Multiplikation

$$\bar{a} \cdot \bar{b} = \overline{ab}.$$

Das Null-Element ist $\bar{0}$ und das Eins ist $\bar{1}$. Die kanonische Abbildung $R \to R/I$, $a \mapsto \bar{a}$ ist ein surjektiven Ringhomomorphismus. Wenn R kommutative ist, so ist R/I.

Beweis. Wir müssen zeigen, dass die Multiplikation wohldefiniert ist, das heißt, wenn $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$, dann $\overline{ab} = \overline{a'b'}$. Dies gilt, weil

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b-b') + (a-a')b \in I$$

da I ein Ideal ist. Der Rest ist leicht. z.B. die Multiplikation ist assoziativ, weil

$$(\bar{a}\cdot\bar{b})\bar{c} = \overline{ab}\cdot\bar{c} = \overline{(ab)c} = \overline{a(bc)} = \bar{a}\cdot\overline{bc} = \bar{a}(\bar{b}\cdot\bar{c}).$$

□

Beispiel. Für jede $m \geq 0$ betrachten wir den Faktorring $\mathbb{Z}_m = \mathbb{Z}/\mathbb{Z}m$

Für $m = 0$ ist $\mathbb{Z}0 = \{0\}$, also $\mathbb{Z}_0 \cong \mathbb{Z}$.

Für $m = 1$ ist $\mathbb{Z}1 = \mathbb{Z}$, also $\mathbb{Z}_1 = \{0\}$, der Nullring.

Für $m > 1$ ist $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ wie in LA I.

Proposition. *Sei $m \geq 0$ und $\mathbb{Z}_m = \mathbb{Z}/\mathbb{Z}m$.*

(i) $(\mathbb{Z}_m)^\times = \{\overline{a} : \mathrm{ggT}(a, m) = 1\}$.

(ii) $\mathbb{Z}_m$ ist ein Körper genau dann, wenn m eine Primzahl ist.

Beweis. (i) Wenn $\mathrm{ggT}(m, a) = 1$, gibt es $x, y \in \mathbb{Z}$ mit $ax + my = 1$. Dann ist $\bar{a}\ \bar{x} = \bar{1}$, also hat $\bar{a}$ das Inverse $\bar{x}$.

Wenn $\bar{a}$ hat Inverse $\bar{x}$ ist $ax \equiv 1 \pmod{m}$, also $ax = 1 + km$ für ein $k \in \mathbb{Z}$. Nun ist $\mathrm{ggT}(a, m)$ ein Teiler von ax und km, also von 1, also ist $\mathrm{ggT}(a, m) = 1$.

(ii) Die Ringe $\mathbb{Z}_0$ und $\mathbb{Z}_1$ sind keine Körper. Also ist $\mathbb{Z}_m$ ein Körper genau dann, wenn $m > 1$ und alle $0 < a < m$ teilerfremd zu m sind, also wenn m eine Primzahl ist. □

Bemerkung. Die komplexen Zahlen werden aus den reellen Zahlen konstruiert, indem ein neues Element i hinzugefügt wird, das die Gleichung $i^2 + 1 = 0$ erfüllt. Nehmen wir allgemeiner an, wir möchten ein Element α an einen Ring R hinzufügen, das $g(\alpha) = 0$ für ein Polynom $g(X)$ erfüllt, dann gehen wir wie folgt vor.

Proposition. *Sei R ein kommutativer Ring und sei $g(X) \in R[X]$ ein Polynom der Form*

$$g(X) = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$$

mit $n > 0$ und mit Leitkoeffizient $a_n \in R^\times$ (zum Beispiel ist $g(X)$ normiert).

(i) (Polynomdivision) Wenn $f(X) \in R[X]$, dann gibt es $q(X), r(X) \in R[X]$ mit $f(X) = q(X)g(X) + r(X)$ und $\mathrm{Grad}\, r(X) < \mathrm{Grad}\, g(X)$.

(ii) Sei $I = R[X]g(X)$. Jedes Element des Faktorrings $S = R[X]/I$ lässt sich eindeutig in der Form

$$\overline{b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}}$$

mit $b_0, \ldots, b_{n-1} \in R$ schreiben.

(iii) Wir können R als Teilring von S identifizieren, indem wir $r \in R$ mit $\overline{r} \in R[X]/I$ identifizieren. Das Element $\alpha = \overline{X} \in S$ erfüllt $g(\alpha) = 0$ und $S = R[\alpha]$.

Beweis. (i) (Für R ein Körper war dies in LA I §2.3). Wir beweisen dies durch Induktion nach $m = \mathrm{Grad}\, f(X)$. Wenn $m < n$, können wir $q(X) = 0$ und $r(X) = f(X)$ annehmen. Nehmen wir also an, dass $m \geq n$. Wenn der führende Koeffizient von $f(X)$ k ist, dann

$$\mathrm{Grad}(f(X) - k a_n^{-1} X^{m-n} g(X)) < m$$

Durch Induktion gibt es $q(X), r(X)$ mit

$$f(X) - ka_n^{-1}X^{m-n}g(X) = q(X)g(X) + r(X)$$

und $\operatorname{Grad} r(X) < n$, und dann

$$f(X) = (q(X) + ka_n^{-1}X^{m-n})g(X) + r(X).$$

(ii) Teil (i) gibt Existenz. Wenn $q(X) = c_0 + c_1X + \cdots + c_kX^k$ mit $c_k \neq 0$, dann

$$q(X)g(X) = c_0a_0 + \cdots + c_ka_nX^{k+n}$$

und $c_ka_n \neq 0$ da $c_k \neq 0$ und $a_n \in R^\times$. Somit ist $\operatorname{Grad} q(X)g(X) = k + n \geq n$. Somit enthält I kein von Null verschiedenes Polynom vom Grad $< n$.

(iii) Nach (ii) ist die Komposition $R \to R[X] \to S$ injektiv. Wir haben

$$g(\alpha) = a_0 + a_1\overline{X} + \cdots + a_n\overline{X}^n = \overline{(}g(X)) = 0$$

und jedes Element von S hat die Form

$$\overline{b_0 + b_1X + \cdots + b_{n-1}X^{n-1}} = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

also $S = R[\alpha]$, wie in §3.2 Lemma (2). □

Satz (Homomorphiesatz)**.** *Sei $\theta\colon R \to S$ ein Ringhomomorphismus.*

(1) Sei $I \trianglelefteq R$ ein Ideal mit $I \subseteq \operatorname{Ker}(\theta)$. Dann existiert genau einen Ringhomomorphismus $\bar{\theta}\colon R/I \to S$ mit $\bar{\theta}(\bar{a}) = \theta(a)$ für $a \in R$.

(2) Es gibt ein Isomorphimus $\bar{\theta} : R/\operatorname{Ker}(\theta) \to \operatorname{Bild}(\theta)$ mit $\bar{\theta}(\operatorname{Ker}(\theta) + a) = \theta(a)$ für $a \in R$.

Beweis. (1) Laut der Homomorphiesatz für Gruppen gibt es genau einen additive Gruppenhomomorphismus $\bar{\theta}$ mit $\bar{\theta}(\bar{a}) = \theta(a)$. Nun für $a, b \in R$ gilt:

$$\bar{\theta}(\bar{a}\ \bar{b}) = \bar{\theta}(\overline{ab}) = \theta(ab) = \theta(a)\theta(b) = \bar{\theta}(\bar{a})\bar{\theta}(\bar{b})$$

und $\bar{\theta}(\bar{1}_R) = \theta(1_R) = 1_S$, also ist $\bar{\theta}$ ein Ringhomomorphismus.

(2) Klar. □

Satz (Erster Isomorphiesatz)**.** *Seien R ein Ring, $T \subseteq R$ ein Teilring und $I \trianglelefteq R$ ein Ideal. Wir definieren*

$$T + I := \{a + x : a \in T,\ x \in I\}.$$

Dann $T + I$ ist ein Teilring von R, $I \trianglelefteq T + I$ ist ein Ideal, $T \cap I \trianglelefteq T$ ist ein ideal, und es gibt einen Isomorphismus

$$T/(T \cap I) \to (T + I)/I, \quad (T \cap I) + a \mapsto I + a.$$

Beweis. Wir benutzen den ersten Isomorphiesatz für additive Gruppen.

$T + I$ ist eine additive Untergruppe und $1 = 1 + 0 \in T + I$. Seien nun $a, b \in T$ und $x, y \in I$. Dann gilt

$$(a + x)(b + y) = ab + (ay + xb + xy) \in T + I.$$

Also ist $T + I$ ein Teilring.

Da $I \trianglelefteq R$ ein Ideal ist und $I \subseteq T + I$, ist es klar, dass $I \trianglelefteq T + I$ ein Ideal ist.

$T \cap I$ ist eine additive Untergruppe von T, und für $a \in T$ und $x \in T \cap I$ sind $ax, xa \in T \cap I$. Also ist $T \cap I$ ein Ideal von T.

Sei ϕ die Komposition der zwei Ringhomomorphismen $T \to T+I \to (T+I)/I, a \mapsto \bar{a}$. Sie ist surjektiv, denn wenn $a \in T$ und $x \in I$, dann ist $I+(a+x) = I+a = \phi(a)$. Der kern ist $T \cap I$. Also induziert ϕ einen Isomorphismus $T/(T \cap I) \to (T+I)/I$. □

Satz (Zweite Isomorphiesatz)**.** *Sei $I \trianglelefteq R$.*

(1) Wenn J ein Ideal von R mit $I \subseteq J$ ist, dann ist $J/I := \{I+a : a \in J\}$ ein Ideal von R/I , und jedes ideale X von R/I hat diese Form, mit $J = \{a \in R : I+a \in X\}$.

(2) In diesem Fall, gibt es einen Isomorphismus

$$R/J \to (R/I)/(J/I), \quad J + a \mapsto (J/I) + (I + a).$$

Beweis. Übung. □

Definition. Wir sagen, dass zwei Ideale $I, J \trianglelefteq R$ **koprim** oder **teilerfremd** sind, falls $I + J = R$.

z.B. $\mathbb{Z}m$ und $\mathbb{Z}m$ sind koprim $\Leftrightarrow$ ggT$(m, n) = 1$, d.h. m und n sind teilerfremd.

Satz (Chinesischer Restsatz)**.** *Sei R ein Ring und $I, J \trianglelefteq R$ zwei koprim Ideale. Dann ist die kanonische Abbildung*

$$\theta\colon R \to (R/I) \times (R/J), \quad a \mapsto (I + a, J + a),$$

einen surjektiven Ringhomomorphismus mit Kern $I \cap J$, also gibt es einen Isomorphismus

$$R/(I \cap J) \to (R/I) \times (R/J).$$

Beweis. Es ist klar, dass $\theta(a+b) = \theta(a)+\theta(b)$, $\theta(ab) = \theta(a)\theta(b)$, und $\theta(1) = (1, 1)$, also ist θ ein Ringhomomorphismus. Es gilt $\theta(a) = (0, 0)$ genau dann, wenn $a \in I \cap J$.

Da I und J teilerfremd sind, können wir $1 = x + y$ mit $x \in I$ und $y \in J$ schreiben. Für $a, b \in R$ gilt

$$\theta(ax + by) = (I + ax + b(1 - x), J + a(1 - y) + by) = (I + b, J + a),$$

weil $ax - bx \in I$ und $by - ay \in J$. Also ist θ surjectiv. □

4 Integritätsbereichen und Faktorisierung

4.1 Integritätsbereiche und die Beziehung zu Körpern

Definition. Sei R ein Ring.

(i) Ein Element $a \in R$ heißt **Nullteiler**, falls $a \neq 0$ und $ab = 0$ oder $ba = 0$ für ein $b \neq 0$.

(ii) R ist ein **Integritätsbereich**, wenn es kommutativ ist, $1 \neq 0$ hat und keine Nullteiler hat, d.h. wenn $ab = 0$, dann $a = 0$ oder $b = 0$.

Bemerkung. In einem Integritätsbereich gilt die Kürzungsregel: aus $ab = ac$ und $a \neq 0$ folgt $b = c$.

Beispiele. (i) $\mathbb{Z} \times \mathbb{Z}$ ist kein Integritätsbereich, weil $(1, 0) \cdot (0, 1) = (0, 0)$. $\mathbb{Z}_6$ ist kein Integritätsbereich, weil $\bar{2} \cdot \bar{3} = \bar{6} = 0$.

(ii) Jeder Körper ist ein Integritätsbereich, denn wenn $ab = 0$ und $a \neq 0$, dann gilt

$$b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0.$$

(iii) Jeder Teilring eines Integritätsbereichs (also auch eines Körpers) ist ein Integritätsbereich.

(iv) Jeder endliche Integritätsbereich ist ein Körper: Die Multiplikation mit $a \neq 0$ ist ein injektive Homomorphismus additiver Gruppen $R \to R$. Da R endlich ist, muss sie surjektiv sein, also gibt es $b \in R$ mit $ab = 1$.

(v) Sei K ein Teilring von R, das ein Körper ist, und nehmen wir an, dass R als K-Vektorraum endlichdimensional ist. Wenn R ein Integralbereich ist, dann ist es ein Körper. Die Multiplikation mit $a \neq 0$ ist ein injektive lineare Abbildung $R \to R$, also ein Isomorphismus.

Lemma. *Sei R ein Integritätsbereich. Dann ist $R[X]$ auch einen Integritätsbereich, und für $f(X), g(X) \in R[X]$ nicht Null gilt* $\operatorname{Grad}(f(X)g(X)) = \operatorname{Grad} f(X) + \operatorname{Grad} g(X)$*, und und Leitkoeffizient von $f(X)g(X)$ ist das Produkt der Leitkoeffizienten von $f(X)$ und $g(X)$.*

Beweis. Seien $f(X) = a_0 + a_1X + \cdots + a_nX^n$ und $g(X) = b_0 + \cdots + b_mX^m$ mit $a_n, b_m \neq 0$. Es gilt

$$f(X)g(X) = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + a_nb_mX^{n+m}.$$

Da R ein Integritätsbereich ist, ist $a_n b_m \neq 0$. Also ist $\mathrm{Grad}(fg) = n + m = \mathrm{Grad}\, f + \mathrm{Grad}\, g$, und der Leitkoeffizient von $f(X)g(X)$ ist $a_n b_m$. □

Bemerkungen. (1) Wenn R ein Integritätsbereich ist, gilt $(R[X])^\times = R^\times$. Also ist $R[X]$ kein Körper.

(2) wenn R ein Integritätsbereich ist, dann auch so ist jeder Polynomring $R[X_1, \ldots, X_n]$. (Induktion mit $R[X_1, \ldots, X_n] \cong (R[X_1, \ldots, X_{n-1}])[X_n]$.)

Definition. Sei R ein kommutative Ring. Sei $I \trianglelefteq R$ ein Ideal.

(i) I heißt **maximal**, falls $I \neq R$ und für jedes Ideal $J \trianglelefteq R$ mit $I \subseteq J \subseteq R$ gilt $J = I$ oder $J = R$.

(ii) I heißt **prim**, wenn $I \neq R$ und aus $ab \in I$ folgt $a \in I$ oder $b \in I$.

Proposition. *Sei R ein kommutative Ring.*

(i) Ein Ideal $I \trianglelefteq R$ ist maximal genau dann, wenn R/I ein Körper ist.

(ii) Ein Ideal $I \trianglelefteq R$ ist prim genau dann, wenn R/I ein Integritätsbereich ist.

Insbesondere ist jedes maximal Ideal ein Primideal.

Beweis. (i) Nach dem zweiten Isomorphiesatz ist I genau dann maximal, wenn R/I genau zwei Ideale hat, $\{0\} = I/I$ und R/I. Nach §3.2 Beispiel (4) für Ideale ist es äquivalent, dass R/I ein Körper ist.

(ii) Sei $I \trianglelefteq R$ ein Primideal, und $\bar{a}\bar{b} = 0$ in R/I. Dann gilt $ab \in I$, also $a \in I$ oder $b \in I$. Es folgt, dass entweder $\bar{a} = 0$ oder $\bar{b} = 0$ ist, und R/I ist ein Integritätsbereich.

Sei nun R/I ein Integritätsbereich, und $a, b \in R$ mit $ab \in I$. Dann gilt $\bar{a}\bar{b} = 0$ in R/I, also $\bar{a} = 0$ oder $\bar{b} = 0$. Es folgt, dass entweder $a \in I$ oder $b \in I$, und I ist ein Primideal.

Da jeder Körper einen Integritätsbereich ist, ist jedes maximal Ideal ein Primideal. □

Beispiel. Die maximale Ideale in $\mathbb{Z}$ sind $\mathbb{Z}p$ für eine Primzahl p. Die Primideale in $\mathbb{Z}$ sind $\mathbb{Z}p$ für eine Primzahl p und $\{0\} = \mathbb{Z}0$.

Satz. *Sei R ein Integritätsbereich. Es gibt einen Körper* $\mathrm{Quot}(R)$*, der R als Teilring enthält. Er hat die Eigenschaft, dass für jeden injektiven Homomorphismus $\theta : R \to K$ mit K einem Körper, gibt es eine eindeutige Erweiterung von θ zu einem Homomorphismus $\tilde{\theta} : \mathrm{Quot}(R) \to K$.*

Wir nennen Quot(R) den **Quotientenkörper** von R.

Beweis. Sehen Sie LA II, §8.1. Sei $X = \{(a, b) : a, b \in R, b \neq 0\}$ und sei $\sim$ die Relation auf X, definiert durch

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Es ist leicht zu zeigen, dass $\sim$ eine Äquivalenzrelation ist. Wir definieren Quot(R) als die Menge der Äquivalenzklassen und bezeichnen die Äquivalenzklasse $[(a, b)]_\sim$ mit a/b. Dann hat Quot(R) Verknüpfungen

$$a/b + c/d = (ad + bc)/(bd), \quad (a/b)(c/d) = (ac)/(bd).$$

Es ist leicht zu zeigen, dass diese wohldefiniert sind und dass Quot(R) zu einem Ring mit Null $0/1$ und Eins $1/1$ wird. Wir identifizieren R als Teilring von Quot(R) unter Verwendung des injektiven Homomorphismus $R \to \text{Quot}(R)$, $a \mapsto a/1$.

Nehmen wir nun an, dass $\theta : R \to K$ ein Ringhomomorphismus und K ein Körper ist. Wir definieren $\tilde{\theta}$ durch $\tilde{\theta}(a/b) = \theta(a)\theta(b)^{-1}$. Dies ist ein Ringhomomorphismus, der θ erweitert. Wenn umgekehrt ϕ ein Ringhomomorphismus ist, der θ erweitert, dann ist

$$\phi(a/b) = \phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = \theta(a)\theta(b)^{-1},$$

also $\phi = \tilde{\theta}$. □

Beispiele. (1) Quot($\mathbb{Z}$) = $\{a/b : a, b \in \mathbb{Z}, b \neq 0\} = \mathbb{Q}$. (Sehen Sie LA I, §1.3).

(2) Wenn K ein Körper ist, dann heißt Quot($K[X_1, \ldots, K_n]$) der **Körper rationaler Funktionen in** $X_1, \ldots, X_n$ **mit Koeffizienten in** K. Er wird mit $K(X_1, \ldots, X_n)$ bezeichnet.

4.2 Hauptidealbereiche

Definition. Ein **Hauptidealbereich** ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.

z.B. $\mathbb{Z}$ ist ein Hauptidealbereich.

Definition. Ein Integritätsbereich R heißt **Euklidischen Ring** falls eine Bewertungsfunktion

$$\sigma : R \setminus \{0\} \to \mathbb{N} = \{0, 1, 2, \ldots\}$$

mit folgender Eigenschaft existiert: Für jedes $a, b \in R$ mit $b \neq 0$ gibt es $q, r \in R$, so dass $a = qb + r$ und entweder $r = 0$ oder $\sigma(r) < \sigma(b)$.

Bemerkung. (1) $\mathbb{Z}$ ist ein euklidischer Ring mit $\sigma(d) = |d|$, wobei q und r durch Division mit Rest gegeben sind.

(2) Wenn K ein Körper ist, dann ist $K[X]$ ein euklidischer Ring mit $\sigma(p(X)) = \operatorname{Grad} p(X)$, wobei q und r durch Polynomdivision gegeben sind.

(3) Jeder Körper ist ein euklidischer Ring mit $\sigma(a) = 0$ für alle a.

Proposition. *Jeder euklidische Ring ist ein Hauptidealbereich. Insbesondere wenn K ein Körper ist, dann ist $K[X]$ ein Hauptidealbereich.*

Beweis. Dies ist dasselbe wie der Beweis, dass jede Untergruppe von $\mathbb{Z}$ die Form $\mathbb{Z}m$ hat, wobei $\sigma(a)$ anstelle von $|d|$ verwendet wird.

Das Nullideal ist $R0$, also nehmen wir an, dass R ein Ideal ungleich Null ist. Wählen Sie $0 \neq b \in I$ mit minimalem $\sigma(b)$. Wir behaupten, dass $I = Rb$. Es gilt $Rb \subseteq I$.

Angenommen, $a \in I$. Wir können $q, r \in R$ mit $a = qb + r$ und entweder $r = 0$ oder $\sigma(r) < \sigma(b)$ finden. Jetzt ist $r = a - qb \in I$. Also nach Minimalität $r = 0$. Somit ist $a = qb \in Rb$. Also $I \subseteq Rb$. □

Definition. Sei $d \in \mathbb{Z}$ kein Quadrat. Wir betrachten

$$\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Für $d = -1$ ist dies der Ring der **Gaußschen Zahlen** $\mathbb{Z}[i]$.

Für $a = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ definieren wir die **Norm** von a als

$$N(a) = |x^2 - dy^2|.$$

Das ist durch das nächste Lemma wohldefiniert. Wenn $d < 0$, dann ist $N(a) = |a|^2$ als komplexe Zahl.

Lemma. *Wenn $d \in \mathbb{Z}$ kein Quadrat ist, dann ist $\sqrt{d}$ irrational, also wenn $a = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, dann sind $x, y \in \mathbb{Z}$ eindeutig bestimmt.*

Beweis. (Wenn $d < 0$ ist $\sqrt{d} \notin \mathbb{R}$, also nicht rational.) Wenn $\sqrt{d}$ rational ist, können wir $\sqrt{d} = a/b$ mit $a, b \in \mathbb{Z}$ teilerfremd und $b > 0$ schreiben. Dann ist $a^2 = db^2$ und $ax + by = 1$ mit $x, y \in \mathbb{Z}$. Dann

$$db^2x^2 = a^2x^2 = (1 - by)^2 = 1 - 2by + b^2y^2$$

also ist 1 ein Vielfaches von b, also $b = 1$, also $\sqrt{d} = a$, also $d = a^2$. □

Lemma. *Sei $a \in \mathbb{Z}[\sqrt{d}]$.*

(i) $N(a)$ ist eine nicht negative ganze Zahl.

(ii) $N(a) = 0 \Leftrightarrow a = 0$.

(iii) $N(ab) = N(a)N(b)$.

(iv) a ist eine Einheit $\Leftrightarrow N(a) = 1$.

Beweis. (i) Klar.

(ii) Das letzte Lemma.

(iii) Berechnung.

(iv) Wenn a eine Einheit ist, dann ist $1 = N(1) = N(a^{-1})N(a)$, also $N(a) = 1$ nach (i). Wenn $a = x + y\sqrt{d}$ und $N(a) = 1$, dann ist a invertierbar, $a^{-1} = \pm(x - y\sqrt{d})$. □

Satz. *Für $d = -2, -1, 2, 3$ ist der Ring $\mathbb{Z}[\sqrt{d}]$ ein euklidischer Ring mit $\sigma(a) = N(a)$, also ein Hauptidealbereich.*

Beweis. Wir erweitern die Norm auf

$$\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Q}\}$$

nach der gleichen Formel. Wir haben immer noch $N(ab) = N(a)N(b)$.

Durch eine Einzelfallunterscheidung können wir zeigen: für alle $a \in \mathbb{Q}[\sqrt{d}]$ gibt es $q \in \mathbb{Z}[\sqrt{d}]$ mit $N(a-q) < 1$. z.B. für $d = -2$. Das Worst-Case-Element im Rechteck $0, 1, 1 + \sqrt{d}, \sqrt{d}$ ist $1/2 + 1/2\sqrt{d}$ und seine Norm ist $(1/4) + 2(1/4) = 3/4 < 1$.

Seien nun $a, b \in \mathbb{Z}[\sqrt{d}]$ mit $b \neq 0$. Dann

$$\frac{a}{b} = \frac{s + t\sqrt{d}}{n + m\sqrt{d}} = \frac{(s + t\sqrt{d})(n - m\sqrt{d})}{n^2 - dm^2} \in \mathbb{Q}[\sqrt{d}].$$

Wählen Sie q mit $N(a/b-q) < 1$ und sei $r = a-qb$. Dann $N(r) = N((a/b-q)b) = N(a/b - q)N(b) < N(b)$. □

Definition. Ein kommutativer Ring R heißt **noetherisch**, wenn jede aufsteigende Folge von Idealen

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stationär ist. Das heißt es gibt n, sodass $I_n = I_r$ für alle $r \geq n$.

Das nächste Lemma zeigt, dass jede Hauptidealbereich noethersch ist.

Lemma. *Sei R ein kommutativer Ring. Dann ist R genau dann noethersch, wenn jedes ideale $I \trianglelefteq R$ endlich erzeugt ist, das heißt, es gibt $a_1, \ldots, a_m \in I$ mit*

$$I = (a_1, \ldots, a_m) = Ra_1 + \cdots + Ra_m.$$

Beweis. Sei $I_1 \subseteq I_2 \subseteq \cdots$ eine aufsteigende Folge von Idealen. Dann ist die Vereinigung $I = \bigcup_r I_r$ wieder ein Ideal, da für $x, y \in I$ und $a \in R$ gibt es m mit $x, y \in I_m$, und dadurch sind beide $x + y, ax \in I_m \subseteq I$.

Wenn jedes Ideal endlich erzeugt wird, dann ist $I = (a_1, \ldots, a_m)$. Dann gibt es ein n mit $a_1, \ldots, a_m \in I_n$. Dann ist $I \subseteq I_n \subseteq I$, also $I = I_n = I_{n+1} = \ldots$.

Nehmen wir umgekehrt an, dass I nicht endlich erzeugt ist. Wählen Sie $a_1 \in I$. Dann ist $(a_1) \neq I$, also können wir $a_2 \in I \setminus (a_1)$ wählen. Dann ist $(a_1, a_2) \neq I$, also können wir $a_3 \in I \setminus (a_1, a_2)$ usw. wählen. Dann

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \ldots$$

ist eine aufsteigende Folge, die nicht stationär ist. □

4.3 Factorizierung

Definition. Sei R ein Integritätsbereich.

Ein Element $a \in R$ wird als **Teiler** von $b \in R$ bezeichnet, geschrieben als $a|b$, wenn $b = ra$ für ein $r \in R$.

Sei $\sim$ die Relation auf R, definiert durch $a \sim b \Leftrightarrow a = ub$ mit $u \in R^\times$. Sie ist eine Äquivalenzrelation. Elemente $a, b \in R$ heißen **assoziiert** zueinander, wenn $a \sim b$.

Ein Element $a \in R$ heißt **irreduzibel**, falls $a \neq 0$, $a \notin R^\times$, und aus $a = bc$ folgt $b \in R^\times$ oder $c \in R^\times$.

Ein Element $a \in R$ heißt **prim**, falls $a \neq 0$, $a \notin R^\times$ und aus $a|bc$ folgt $a|b$ oder $a|c$.

Lemma. *Für Elemente in einem Integritätsbereich R gilt:*

(i) $b|a \Leftrightarrow Ra \subseteq Rb$

(ii) a und b sind assoziiert $\Leftrightarrow a|b$ und $b|a \Leftrightarrow Ra = Rb$.

(iii) Wenn $a = bc$ und $c \notin R^\times$, dann ist $Ra \subset Rb$ eine strikte Inklusion.

(iv) Ra ist ein Primideal $\Leftrightarrow$ a ist prim oder $a = 0$.

(v) Jedes Primelement a ist irreduzibel.

Beweis. (i) Klar.

(ii) Nach (i) sind die letzten beiden Bedingungen äquivalent. Wenn $a \sim b$, dann gelten diese Bedingungen eindeutig. Nehmen wir umgekehrt an, dass $a|b$ und $b|a$. Also $a = xb$ und $b = ya$ mit $x, y \in R$. Dann ist $(1 - xy)a = 0$. Also $a = 0$ oder $1 - xy = 0$. Im ersten Fall, ist $b = 0$, also $a \sim b$. Im zweiten Fall ist $x \in R^\times$, also $a \sim b$.

(iii) Wenn $Ra = Rb$, ist $a = bu$ mit $u \in R^\times$. Durch die Kürzungsregel ist $c = u \in R^\times$.

(iv) Folgt aus der Definition.

(v) Sei a prim und $a = bc$. Also $a|bc$. Also $a|b$ oder $a|c$.

Wenn $a|b$ gilt, haben wir ebenfalls $b|a$. Also $Ra = Rb$, also $c \in R^\times$ nach (iii).

Wenn $a|c$ gilt, dann ist $b \in R^\times$. □

Beispiele. (1) Die Einheiten in $\mathbb{Z}$ sind ± 1, also sind a und b genau dann assoziiert, wenn $a = \pm b$. Die irreduziblen Elemente sind $\pm p$, wobei p eine Primzahl ist. Die Primelemente sind gleich.

(2) Die Einheiten in $\mathbb{Z}[i]$ sind $\pm 1, \pm i$.

2 ist nicht irreduzibel, weil $2 = (1 + i)(1 - i)$.

$1 + i$ ist irreduzibel, weil $N(1 + i) = 2$ eine Primzahl ist. Wenn $1 + i = ab$ mit a, b kein Einheiten sind $N(a), N(b) > 1$ und $N(1 + i) = 2 = N(a)N(b)$. Unmöglich.

3 ist irreduzibel, weil wenn $3 = ab$, mit a, b nicht Einheiten, dann ist $N(a) = N(b) = 3$. Aber es gibt keine Löesung zu $x^2 + y^2 = 3$ mit $x, y \in \mathbb{Z}$.

5 ist nicht irreduzibel, weil $5 = 1 + 2^2 = (1 + 2i)(1 - 2i)$.

$1 + 2i$ ist irreduzibel, ...

(3) Die Einheiten in $\mathbb{Z}[\sqrt{-3}]$ sind ± 1, für $N(x + y\sqrt{-3}) = 1$ genau dann, wenn $x^2 + 3y^2 = 1$ gdw. $(x, y) = (\pm 1, 0)$.

2 ist irreduzibel in $\mathbb{Z}[\sqrt{-3}]$, denn wenn $2 = ab$ mit a, b keine Einheiten, dann ist

$N(2) = 4$, also $N(a)N(b) = 4$, also $N(a) = N(b) = 2$. Aber es gibt keine Elemente in $\mathbb{Z}[\sqrt{-3}]$ der Norm 2, da die Gleichung $x^2 + 3y^2 = 2$ keine Lösungen mit $x, y \in \mathbb{Z}$ hat.

Ebenso ist $1 + \sqrt{-3}$ irreduzibel in $\mathbb{Z}[\sqrt{-3}]$.

$(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2 \cdot 2$, also $2|(1+\sqrt{-3})(1-\sqrt{-3})$. Aber 2 ist kein Teiler von $1 \pm \sqrt{-3}$, denn wenn $1 \pm \sqrt{-3} = 2(x + y\sqrt{-3})$, dann ist $1 = 2x$, Widerspruch. Somit ist 2 kein Primelement in $\mathbb{Z}[\sqrt{-3}]$.

Definition. Sei R ein Integritätsbereich. Dann heißt R **faktoriell** (englisch: unique factorisation domain) falls

(1) Jedes $a \in R$ nicht Null lässt sich als ein Produkt von irreduziblen Elemente und einem Einheit darstellen, also $a = up_1 \cdots p_r$ mit $u \in R^\times$ und $p_1, \ldots, p_r$ irreduzibel.

(2) Diese Darstellung ist, bis auf Einheiten und die Reihenfolge der Faktoren, eindeutig: Wenn

$$up_1 \cdots p_r = vq_1 \cdots q_s$$

mit $u, v \in R^\times$ und p_i, q_j irreduzible Elemente, dann ist $r = s$ und, nach Umordnung, sind p_i und q_i assozierte Elemente für alle $1 \leq i \leq r$.

Aufgrund des nächsten Ergebnisses können wir $a = up_1 \cdots p_r$ die **Primfaktorzerlegung** von a nennen.

Lemma. *Wenn R faktoriell ist, dann ist jedes irreduzible Element prim.*

Beweis. Sei a irreduzibel, und $a|bc$. Dann existiert d mit $bc = ad$. Wir zerlegen nun b, c, d als Produkte von irreduziblen Elemente. Dann bekommen wir zwei solche Zerlegungen für $bc = ad$, und die Eindeutigkeit sagt, dass (bis auf Einheit) a als Faktor von b oder c vorkommt. Also $a|b$ oder $a|c$. Also a ist prim. □

Beispiele. (i) $\mathbb{Z}$ ist faktoriell. Jede ganze Zahl $m \neq 0$ kann in Primfaktoren zerlegt werden, also $m = \pm p_1^{n_1} \cdots p_r^{n_r}$ mit $r \geq 0$, p_i verscheidene Primzahlen, und $n_i \geq 1$. Weiterhin ist diese Zerlegung bis auf die Reihenfolge der Primzahlen eindeutig bestimmt. Wir wollen jetzt untersuchen, in welchen Ringe solche Zerlegungen existieren.

(ii) $\mathbb{Z}[\sqrt{-3}]$ ist nicht faktoriell, weil 2 kein Primelement in $\mathbb{Z}[\sqrt{-3}]$ ist.

Bemerkung. Sei R faktoriell. Es seien p_i ($i \in I$) Repräsentanten der Äquivalenzklassen irreduzibler Elemente unter der Äquivalenzrelation $\sim$. Dann kann jedes von

Null verschiedene Element $a \in R$ eindeutig in der Form geschrieben werden

$$a = u \prod_{i \in I} p_i^{n_i}$$

wobei $n_i \geq 0$, fast alles Null und u eine Einheit ist. Darüber hinaus sind die Teiler von a die Elemente der Form

$$b = v \prod_{i \in I} p_i^{m_i}$$

mit $m_i \leq n_i$ für alle i.

Satz. *Jeder Hauptidealbereich R ist faktoriell. Wenn R kein Körper ist, gilt:*

- Die maximalen Ideale sind die Hauptideale Ra mit a irreduzibel.

- Die Primideale sind die maximalen Ideale und $\{0\}$.

Beweis. Ein Körper ist eindeutig faktoriell, ohne irreduzible Elemente, daher können wir annehmen, dass R kein Körper ist.

Angenommen, es gibt ein Element $a \in R$ mit $a \neq 0$, $a \notin R^\times$ und so, dass a nicht als Produkt irreduzibler Elemente geschrieben werden kann. Wir werden eine Folge von Elementen $a_1, a_2, \ldots$ mit denselben Eigenschaften und konstruieren, so dass

$$Ra_1 \subset Ra_2 \subset \ldots$$

ist eine aufsteigende Folge von Idealen, die nicht stationär ist. Dies widerspricht der Tatsache, dass R noethersch ist. Wir beginnen mit $a_1 = a$. Angenommen, wir haben a_n konstruiert. Dann ist a_n nicht irreduzibel, also $a_n = bc$, wobei b und c keine Einheiten sind, und da a_n nicht als Produkt von Irreduziblen geschrieben werden kann, mindestens eines von b und c hat diese Eigenschaft, sagen wir b. Dann ist $Ra_n \subset Rb$, und das ist streng, da sonst $a_n = ub$, mit u eine Einheit, also durch Kurzung $c = u \in R^\times$. Somit können wir $a_{n+1} = b$ nehmen.

R ist kein Körper, daher gibt es ein Ideal, das sich von $\{0\}$ und R unterscheidet. Wenn also Ra maximal ist, dann ist $a \neq 0$. Auch $a \notin R^\times$, und dann ist a nach (iii) des ersten Lemmas irreduzibel.

Wenn umgekehrt a irreduzibel ist, dann ist Ra maximal, denn wenn Rb ein Ideal genau zwischen Ra und R ist, dann ist b keine Einheit und $a = bc$ wobei c keine Einheit ist.

Nun ist jedes maximale Ideal ein Primideal, also ist jedes irreduzible Element prim.

Für die Eindeutigkeit der Zerlegung betrachten wir $up_1 \cdots p_r = vq_1 \cdots q_s$ mit u, v Einheiten und p_i, q_j irreduzible Elemente.

Da p_1 prim ist und p_1 ein Teiler von $vq_1 \cdots q_s$ ist, folgt daraus, dass $p_1 | q_i$ für ein i. Nach der Umordnung können wir davon ausgehen, dass $i = 1$. Da q_1 irreduzibel ist, folgt daraus, dass p_1 und q_1 assoziiert sind, sagen wir $q_1 = wp_1$ mit w einer Einheit. Dann

$$up_2 \dots p_r = (vw)q_2 \dots q_s.$$

Induktion über $r + s$ zeigt, dass $r = s$ und (nach Umordnung) die Elemente p_j und q_j assoziierte Elemente für alle j sind.

Schließlich ist ein Primideal ungleich Null ein Hauptideal, also durch ein Primelement gegeben. Aber jedes Primelement ist irreduzibel, also ist das Ideal maximal. □

Definition. Sei R ein Integritätsbereich und $a, b \in R$.

Wir sagen, dass $\mathrm{ggT}(a, b)$ existiert, falls es $g \in R$ gibt mit $g|a$ und $g|b$ und aus $d|a$ und $d|b$ folgt $d|g$. Wenn g existiert, dann ist es bis auf Einheiten eindeutig bestimmt, und wir setzen $\mathrm{ggT}(a, b) \coloneqq g$.

Wir sagen, dass $\mathrm{kgV}(a, b)$ existiert, falls es $k \in R$ gibt mit $a|k$ und $b|k$ und aus $a|f$ und $b|f$ folgt $k|f$. Wenn k existiert, dann ist es bis auf Einheiten eindeutig bestimmt, und wir setzen $\mathrm{kgV}(a, b) \coloneqq k$.

Bemerkungen. (1) $\mathrm{ggT}(a, 0) = a$, $kgV(a, 0) = 0$.

(2) Wir erweitern diese Definition zu endlich viele Elemente, z.B. $\mathrm{ggT}(a, b, c) = \mathrm{ggT}(a, \mathrm{ggT}(b, c))$.

(3) Für einen Hauptidealbereich R, gilt

$$Ra + Rb = R\,\mathrm{ggT}(a, b), \quad Ra \cap Rb = R\,\mathrm{kgV}(a, b)$$

Der Beweis ist derselbe wie für $\mathbb{Z}$ in §1.6

(4) Für einen euklidischen Ring R können wir $\mathrm{ggT}(a, b)$ mit dem Algorithmus von Euklid berechnen. Daher der Name!

Lemma. *Sei R faktoriell. Für zwei Elemente $a, b \in R$ existieren beide $g = \mathrm{ggT}(a, b)$ und $k = \mathrm{kgV}(a, b)$. Weiterhin gilt $ab \sim gk$.*

Beweis. Wir können annehmen, dass $a, b \neq 0$. Wählen Sie Vertreter p_i $(i \in I)$ der Äquivalenzklassen irreduzibler Elemente. Dann können wir schreiben

$$a = u \prod_{i \in I} p_i^{n_i}, \quad b = v \prod_{i \in I} p_i^{m_i}.$$

Dann sind

$$\mathrm{ggT}(a,b) = w \prod p_i^{\min(n_i,m_i)}, \quad \mathrm{kgV}(a,b) = z \prod p_i^{\max(n_i,m_i)}$$

für beliebige $w, z \in R^\times$. □

4.4 Polynome über faktorielle Ringe

In diesem Abschnitt wollen wir zeigen, dass wenn R faktoriell ist, ist $R[X]$ auch faktoriell. Insbesondere sind $\mathbb{Z}[X_1, \ldots, X_n]$, und $K[X_1, \ldots, X_n]$ für einen Körper K, immer faktoriell.

Definition. Sei R ein faktorieller Ring und $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$. Der **Inhalt** (englisch: content) von $f(X)$ ist

$$\text{Inhalt } f(X) \coloneqq \mathrm{ggT}(a_0, a_1, \ldots, a_n).$$

Denken Sie daran, dass dies bis zur Multiplikation mit einer Einheit in R wohldefiniert ist. Wir sagen: $f(X)$ ist **primitiv**, wenn Inhalt $f(X)$ eine Einheit ist.

Bemerkung. Seien R faktoriell und $p \in R$ ein irreduzibles Element. Es gibt einen Ringhomomorphismus $R \to R/Rp$, $a \mapsto \bar{a}$, also einen Ringhomomorphisms $R[X] \to (R/Rp)[X]$,

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n \mapsto \overline{f(X)} = \bar{a}_0 + \bar{a}_1 X + \cdots + \bar{a}_n X^n.$$

Wir nennen $\overline{f(X)}$ die **Reduktion von** $f(X)$ **modulo** p.

Nach dem zweiten Lemma von §4.3 ist das Element p prim, also nach dem ersten Lemma ist das Hauptideal Rp ein Primideal. Also nach §4.1 Proposition ist der Faktorring R/Rp ein Integritätsbereich. Also ist $(R/Rp)[X]$ ein Interitätsbereich.

Lemma (Gauss)**.** *Sei R faktoriell. Sind die Polynome $f(X), g(X) \in R[X]$ primitiv, so ist auch ihr Produkt $f(X)g(X)$.*

Beweis. Angenommen, dass $f(X)g(X)$ nicht primitiv ist. Also hat Inhalt$(f(X)g(X))$ einen irreduziblen Teiler $p \in R$. Die Reduktion von $f(X)g(X)$ modulo p ist dann $\overline{f(X)g(X)} = 0$. Also ist $\overline{f(X)} \cdot \overline{g(X)} = 0$. Also $\overline{f(X)} = 0$ oder $\overline{g(X)} = 0$. Also und $p|$ Inhalt $f(X)$ oder $p|$ Inhalt $g(X)$. Also ist mindestens eins von $f(X)$ und $g(X)$ nicht primitiv. Widerspruch. □

Lemma. *Sei R faktoriell, mit Quotientenkörper K. Jedes Polynom $0 \neq g(X) \in K[X]$ kann als $g(X) = \lambda h(X)$ geschrieben sein, mit $\lambda \in K^\times$ and $h(X) \in R[X]$ primitiv.*

Beweis. Sei d ein gemeinsamer Nenner für die Koeffizienten in $g(X)$. Dann gilt $g(X) = d^{-1}k(X)$ mit $k(X) \in R[X]$. Jetzt sei $c = \text{Inhalt}\, k(X)$, sodass $k(X) = ch(X)$ mit $h(X) \in R[X]$ primitiv. Nun gilt $g(X) = (c/d)h(X)$ wie gewünscht. □

Satz. *Sei R faktoriell mit Quotientenkörper K.*

(i) Wenn $f(X) \in R[X]$ und $\text{Grad}\, f(X) > 0$*, dann ist $f(X)$ genau dann irreduzibel in $R[X]$, wenn $f(X)$ primitiv und $f(X)$ irreduzibel in $K[X]$ ist.*

(ii) Die irreduzible Elemente in $R[X]$ sind:

- die irreduzible Elemente aus R, und

- die Polynome $f(X) \in R[X]$, so dass $\text{Grad}\, f(X) > 0$*, $f(X)$ primitiv und $f(X)$ irreduzibel in $K[X]$ ist.*

(iii) Der Polynomring $R[X]$ ist faktoriell.

Beweis. Erinnerung: $(R[X])^\times = R^\times$.

(i) Angenommen, $f(X)$ ist irreduzibel in $K[X]$ und primitiv. Wenn es eine Zerlegung $f(X) = g(X)h(X)$ mit $g(X), h(X) \in R[X]$ gibt, dann impliziert die erste Bedingung, dass eine von $g(X), h(X)$, ist ein konstantes Polynom, sagen wir $g(X) = a$. Dann ist a ein Teiler von $\text{Inhalt}\, f(X)$, also impliziert die zweite Bedingung, dass a eine Einheit ist. Somit ist $f(X)$ in $R[X]$ irreduzibel.

Nehmen wir nun an, dass $f(X)$ in $R[X]$ irreduzibel ist. Wir können $f(X) = ah(X)$ mit $a = \text{Inhalt}\, f(X)$ und $h(X)$ primitiv schreiben, also ist a aufgrund der Irreduzibilität eine Einheit, also ist $f(X)$ primitiv.

Angenommen, $f(X) = g_1(X)g_2(X)$ für nicht konstante Polynome $g_1(X), g_2(X) \in K[X]$. Nach dem Lemma ist $g_i(X) = \lambda_i h_i(X)$ für $\lambda_i \in K$ ungleich Null und primitive Polynome $h_i(X) \in R[X]$. Schreiben Sie $\lambda = \lambda_1\lambda_2 = a/b$ mit $a, b \in R$ ungleich Null. Dann ist $bf(X) = ah_1(X)h_2(X)$. Dann ist b ein Teiler von $\text{Inhalt}(ah_1(X)h_2(X))$, aber $h_1(X)h_2(X)$ ist primitiv, also ist b ein Teiler von a. Also $\lambda \in R$. Somit ist $f(X) = \lambda h_1(X)h_2(X)$. Widerspruch.

(ii) Folgt von (i).

(iii) Ein von Null verschiedenes Polynom $f(X) \in R[X]$ kann als $f(X) = ah(X)$ mit $a = \text{Inhalt}\, f(X) \in R$ und $h(X)$ primitiv geschrieben werden. Jetzt kann a als Produkt einer Einheit in R und irreduziblen Elementen von R geschrieben werden. Durch Induktion über den Grad kann $h(X)$ als Produkt primitiver irreduzibler Polynome in $R[X]$ geschrieben werden. Somit kann $f(X)$ als Produkt einer Einheit

und irreduzibler Elemente in $R[X]$ geschrieben werden.

Seien jetzt $ag_1(X)\cdots g_r(X) = bh_1(X)\cdots h_s(X)$ zwei Zerlegungen mit $a, b \in R\backslash\{0\}$, und $g_i(X), h_j(X) \in R[X]$ primitiv und irreduzibel in $K[X]$. Da $K[X]$ faktoriell ist wissen wir, dass $r = s$ und, nach Umordnung, existieren $\mu_i \in K^\times$ mit $h_i(X) = \mu_i g_i(X)$ für alle $1 \leq i \leq r$. Schreiben Sie $\mu_i = c_i/d_i$ mit $c_i, d_i \in R$. Dann gilt $d_i h_i(X) = c_i g_i(X)$ in $R[X]$, und da $g_i(X), h_i(X)$ primitiv sind, gibt es Einheiten $u_i \in R^\times$ mit $c_i = u_i d_i$ für alle i. Insbesondere ist $\mu_i = u_i \in R^\times$. Letztendlich haben wir $ag_1(X)\cdots g_r(X) = bh_1(X)\cdots h_r(X) = ubg_1(X)\cdots g_r(X)$ für $u = u_1\cdots u_r \in R^\times$. Da $R[X]$ ein Integritätsbereich ist, gilt nun $a = ub$, und das Ergebnis folgt aus der Eindeutigkeit der Zerlegung für $a \in R$. □

Bemerkungen. (i) Wie bereits erwähnt, folgt daraus, dass, wenn R ein faktorieller Ring ist, $R[X_1, \ldots, X_n]$ für alle n faktoriell ist.

(ii) Normalerweise sind diese Ringe keine Hauptidealbereiche. Zum Beispiel die Ideale $(2, X) \trianglelefteq \mathbb{Z}[X]$ und $(X, Y) \trianglelefteq K[X, Y]$ sind nicht Hauptideale.

(iii) Die Primzahlen sind Repräsentanten der Äquivalenzklassen irreduzibler Elemente in $\mathbb{Z}$. Ähnlich: Wenn K ein Körper ist, dann sind die normierten irreduziblen Polynome Repräsentanten der irreduziblen Polynome in $K[X]$.

Proposition. *Sei K ein Körper. Dann in $K[X]$ gibt es unendlich viele normierte irreduzible Polynome.*

Beweis. Wenn es nur endlich viele wäre, sagen wir $f_1(X), \ldots, f_n(X)$, dann muss $f_1(X)\cdots f_n(X)-1$ von irgendein $f_i(X)$ teilbar sein. Aber aus $f_1(X)\cdots f_n(X)-1 = f_i(X)g(X)$ folgt $1 = f_1(X)\cdots f_n(X) - f_i(X)g(X) \in R[X]f_i(X)$, aber $f_i(X)$ ist keine Einheit. Widerspruch. □

Zusammenfassung:

$$R \text{ euklidischer Ring} \Rightarrow R \text{ Hauptidealbereich} \Rightarrow R \text{ faktoriell} \Rightarrow R[X] \text{ faktoriell}$$

$$\mathbb{Z}, \mathbb{Z}[i], K[X] \qquad \mathbb{Z}[\tfrac{1+\sqrt{-19}}{2}] \qquad K[X_1, \ldots, X_n], \mathbb{Z}[X_1, \ldots, X_n]$$

Der Ring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ ist Hauptidealbereich, aber kein euklidischen Ring. Ein Beweis findet man hier:
`https://webspace.maths.qmul.ac.uk/r.a.wilson/MTH5100/PIDnotED.pdf`

4.5 Irreduzible Polynome

Sei K ein Körper. Ein Polynom $f(X) \in K[X]$ ist irreduzibel, wenn Grad $f(X) > 0$ und für jede Faktorisierung $f(X) = g(X)h(X)$, Grad $g(X) = 0$ oder Grad $h(X) = 0$.

Lemma. *(i) Die irreduziblen Polynome in $\mathbb{C}[X]$ sind die linearen Polynome $aX+b$.*

(ii) Die irreduziblen Polynome in $\mathbb{R}[X]$ sind die linearen Polynome $aX+b$ und die quadratischen Polynome aX^2+bX+c ohne reelle Nullstellen.

Beweis. (i) Über $\mathbb{C}$ hat jedes nicht konstante Polynom $f(X)$ eine Nullstelle a. Dann ist $f(X) = (X-a)g(X)$, und wenn $f(X)$ irreduzibel ist, dann ist $g(X)$ ein konstantes Polynom.

(ii) Sei $f(X)$ irreduzibel in $\mathbb{R}[X]$ vom Grad > 1. Es muss eine Nullstelle $a = u+vi \in \mathbb{C}$ mit $v \neq 0$ haben. Dann ist $\overline{a} = u - vi$ auch eine Nullstelle, also ist $f(X)$ durch

$$g(X) = (X-a)(X-\overline{a}) = (x-u-vi)(x-u+vi) = (x-u)^2 + v^2 \in \mathbb{R}[X]$$

teilbar. Dann ist $f(X) = g(X)h(X)$ für ein $h(X) \in \mathbb{C}[X]$. Jetzt kann man $h(X)$ durch Polynomdivision berechnen, also $h(X) \in \mathbb{R}[X]$. Somit ist $h(X)$ aufgrund der Irreduzibilität ein konstantes Polynom, also ist $f(X)$ quadratisch. □

Lemma. *Hat $f(X) \in K[X]$ Grad 2 oder 3, dann ist $f(X)$ irreduzibel genau dann, wenn es keine Nullstellen in K hat.*

Beweis. Ist $f(X) = g(X)h(X)$ eine echte Zerlegung, dann muss eins von $g(X), h(X)$ Grad 1 haben. Also hat $f(X)$ einen Teiler der Form $X-a$, und a ist eine Nullstelle von $f(X)$ in K. □

Beispiele. (1) $f(X) = X^3+X^2+\bar{2} \in \mathbb{Z}_3[X]$ hat keine Nullstelle in $\mathbb{Z}_3$, da $f(\bar{0}) = \bar{2}$, $f(\bar{1}) = \bar{1}$ und $f(\bar{2}) = \bar{2}$. Somit ist $f(X)$ irreduzibel.

(2) Sei $f(X) = X^4 + X^3 + 1$ in $\mathbb{Z}_2[X]$. Dann hat $f(X)$ keine Nullstellen: $f(\bar{0}) = f(\bar{1}) = \bar{1}$, also keine Faktorisierung $f(X) = g(X)h(X)$ mit Grad $g(X) = 1$ und Grad $h(X) = 3$. Angenommen

$$f(X) = (X^2+aX+b)(X^2+cX+d) = X^4+(a+c)X^3+(ac+b+d)X^2+(ad+bc)X+bd.$$

Koeffizient von X^0: $bd = 1$, also $b = d = 1$.
Koeffizient von X^1: $ad + bc = a + c = 0$.
Koeffizient von X^3: $a + c = 1$. Widerspruch.

Also ist $f(X)$ irreduzibel.

Satz (rationaler Nullstellentest)**.** *Sei R faktoriell, $K = \mathrm{Quot}(R)$, und $f(X) = a_0 + a_1X + \cdots + a_nX^n$ ein Polynom in $R[X]$. Ist $a \in K$ eine Nullstelle von $f(X)$, dann ist $a = r/s$ mit $r, s \in R$, $r|a_0$ und $s|a_n$.*

Insbesondere, für $f(X)$ normiert, d.h. $a_n = 1$, gilt: ist $a \in K$ eine Nullstelle von f, dann ist $a \in R$ und $a|a_0$.

Beweis. Wir schreiben $a = r/s$ mit $r, s \in R$ und $\mathrm{ggT}(r, s)$ eine Einheit. Dann gilt

$$0 = s^n f(r/s) = a_0 s^n + a_1 r s^{n-1} + \cdots + a_n r^n.$$

Also $a_0 s^n = -r(a_1 s^{n-1} + \cdots + a_n r^{n-1})$. Also $r|a_0 s^n$, also $r|a_0$. Ähnlich $s|a_n$.

Wenn $f(X)$ normiert ist, dann ist $s \in R^\times$ eine Einheit, und $a = rs^{-1}$ liegt in R. □

Beispiel. Jede rationale Nullstelle des Polynoms $2X^3 + X + 9 \in \mathbb{Z}[X]$ muss die Form r/s mit $r|9$ und $s|2$ haben. Also $r = \pm 1, \pm 3, \pm 9$ und $s = \pm 1, \pm 2$. Somit hat jede rationale Nullstelle die Form $\pm 1, \pm 3, \pm 9, \pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{9}{2}$. Durch Versuch und Irrtum ist keiner eine Nullstelle. Somit ist $2X^3 + X + 9$ irreduzibel in $\mathbb{Q}[X]$. Da es primitiv ist, ist es auch in $\mathbb{Z}[X]$ irreduzibel.

Definition. (verschoben) Sei S ein Integritätsbereich und R ein Teilring. Wir sagen, dass $s \in S$ **ganz über** R ist, wenn es ein normiertes Polynom $p(X) \in R[X]$ mit $p(s) = 0$ gibt. Wir sagen, dass R **ganz abgeschlossen in** S ist, wenn $s \in S$ ganz über $R \Rightarrow s \in R$.

Korollar. *(verschoben) Wenn R ein faktorieller Ring ist, ist R ganz abgeschlossen in seinem Quotientenkörper.*

z.B. $\omega = e^{2\pi i/3} = \frac{1}{2}(-1 + \sqrt{-3}) \in \mathbb{C}$ ist ganz über $\mathbb{Z}$, weil $\omega^3 - 1 = 0$, oder $\omega^2 + \omega + 1 = 0$. Also ist $\mathbb{Z}[\sqrt{3}]$ in seinem Quotientenkörper nicht ganz abgeschlossen.

Lemma. *Sei R faktoriell mit Quotientenkörper K und sei $f(X) \in R[X]$ ein nichtkonstantes Polynom. Wenn $f(X)$ nicht als Produkt zweier nicht konstanter Polynome in $R[X]$ faktorisiert werden kann, dann ist $f(X)$ in $K[X]$ irreduzibel. Wenn $f(X)$ auch primitiv ist, ist es auch in $R[X]$ irredizibel.*

Beweis. Der Fall, dass $f(X)$ primitiv ist, ist Teil von §4.4 Satz (i). Der dortige Beweis funktioniert auch für den Fall, dass $f(X)$ nicht primitiv ist. □

Lemma. *Sei R faktoriell mit Quotientenkörper K und sei $f(X) \in R[X]$ ein nichtkonstantes Polynom. Sei p ein irreduzibles Element von R, dass kein Teiler des Leitkoeffizienten von $f(X)$ ist. Wenn die Reduktion $\overline{f(X)}$ von $f(X)$ modulo p irreduzibel in $(R/Rp)[X]$ ist, dann ist $f(X)$ irreduzibel in $K[X]$. Wenn $f(X)$ auch primitiv ist, ist es auch in $R[X]$ irredizibel.*

Beweis. Angenommen $f(X) = g(X)h(X)$ mit $g(X), h(X) \in R[X]$ nicht konstante Polynome. Seien a und b die Leitkoeffizienten von $g(X)$ und $h(X)$. Dann ist ab der Leitkoeffizient von $f(X)$. Nach Annahme $p \nmid ab$, also $p \nmid a$ und $p \nmid b$. Somit ist $\operatorname{Grad} \overline{g(X)} = \operatorname{Grad} g(X) > 0$ und $\operatorname{Grad} \overline{h(X)} = \operatorname{Grad} h(X) > 0$. Aber $\overline{f(X)} = \overline{g(X)} \cdot \overline{h(X)}$. Dies widerspricht der Tatsache, dass $\overline{f(X)}$ irreduzibel ist. Somit ist $f(X)$ irreduzibel in $K[X]$. □

Beispiele. (1) Sei $f(X) = X^4 + 15X^3 + 7 \in \mathbb{Z}[X]$. Wir betrachten die Reduktion modulo $p = 2$. Dann ist

$$\overline{f(X)} = X^4 + X^3 + 1 \in \mathbb{Z}_2[X]$$

was irreduzibel ist. Also ist $f(X)$ irreducibel in $\mathbb{Q}[X]$. Weiterhin ist $f(X)$ primitiv, also ist es irreduzibel in $\mathbb{Z}[X]$.

(2) (verschoben) Sei $f(X) = X^4 + 4X^3 + 5X^2 + 1 \in \mathbb{Z}[X]$. Dann gilt

$$f(X) = X^4 + X^2 + 1 = (X^2 + X + 1)^2 \in \mathbb{Z}_2[X]$$

und

$$f(X) = X^4 + X^3 + 2X^2 + 1 = (X + 1)(X^3 + 2X + 1) \in \mathbb{Z}_3[X].$$

Nun sind beide $X^2 + X + 1 \in \mathbb{Z}_2[X]$ und $X^3 + 2X + 1 \in \mathbb{Z}_3[X]$ irreduzibel (keine Nullstellen). Ist $f(X) = g(X)h(X)$ eine echte Zerlegung in $\mathbb{Z}[X]$, dann muss $\operatorname{Grad} g(X) = \operatorname{Grad} h(X) = 2$ (Reduktion modulo 2) und $\operatorname{Grad} g(X) = 3$, $\operatorname{Grad} h(X) = 1$ (Reduktion modulo 3), einen Widerspruch. Es folgt, dass $f(X) \in \mathbb{Z}[X]$ irreduzibel ist.

Satz (Eisensteinkriterium)**.** *Sei R faktoriell und $K = \operatorname{Quot}(R)$. Sei*

$$f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X].$$

Ist $p \in R$ irreduzibel mit $p|a_i$ für $0 \leq i < n$, aber $p \nmid a_n$ und $p^2 \nmid a_0$, dann ist $f(X)$ irreduzibel in $K[X]$. Wenn $f(X)$ auch primitiv ist, ist $f(X)$ irreducibel in $R[X]$.

Beweis. Sei $f(X) = g(X)h(X)$ eine Zerlegung mit $g(X), h(X)$ nicht konstante Polynome. Sei

$$g(X) = b_0 + b_1X + \cdots, \quad h(X) = c_0 + c_1X + \cdots.$$

Dann ist

$$\overline{g(X)} \cdot \overline{h(X)} = \overline{f(X)} = \bar{a}_nX^n \neq 0.$$

Ist $\bar{b}_0 \neq 0$ in R/Rp, und i minimal mit $\bar{c}_i \neq 0$, dann gilt

$$\bar{a}_nX^n = \overline{g(X)} \cdot \overline{h(X)} = \bar{b}_0\bar{c}_iX^i + \cdots$$

einen Widerspruch da $\bar{b}_0\bar{c}_i \neq 0$ und $i \leq \operatorname{Grad} h(X) < n$. Es folgt, dass $\bar{b}_0 = 0$, also $p \mid b_0$. Das gleiche Argument zeigt auch, dass $p \mid c_0$, und damit muss p^2 ein Teiler von $a_0 = b_0c_0$ sein. □

Beispiele. (1) $2X^5 - 3X^2 + 12$ ist irreduzibel in $\mathbb{Q}[X]$ nach Eisenstein mit $p = 3$.

(2) Wenn p eine Primzahl ist und $n > 1$, dann ist $f(X) = X^n - p$ nach Eisenstein irreduzibel in $\mathbb{Q}[X]$. Somit hat $f(X)$ keine Nullstelle in $\mathbb{Q}$. Somit ist $\sqrt[n]{p}$ irrational.

(3) Sei p eine Primzahl. Dann ist $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$ irreduzibel in $\mathbb{Q}[X]$. Wir haben $\Phi_p(X)(X-1) = X^p - 1$. Sei $f(X) = \Phi_p(X+1)$. Dann

$$f(X)X = (X+1)^p - 1 = -1 + \sum_{n=0}^{p} \binom{p}{n} X^n,$$

also

$$f(X) = \sum_{n=1}^{p} \binom{p}{n} X^{n-1}.$$

Das Leitkoeffizient ist $\binom{p}{p} = 1$. Für $1 \leq n < p$ ist

$$p! = \binom{p}{n} \cdot n!(p-n)!$$

Es gilt $p \,|\, p!$ und $p \nmid n!(p-n)!$, also $p | \binom{p}{n}$. Weiterhin ist $\binom{p}{1} = p$ nicht durch p^2 teilbar.

Somit ist $f(X)$ nach Eisenstein irreduzibel. Daraus folgt, dass $\Phi_p(X)$ irreduzibel ist.

5 Körper

5.1 Teilkörper und Körpererweiterungen

Definition. Sei L ein Körper. Ein **Teilkörper** ist ein Teilring $K \subseteq L$, der selbst einen Körper ist. Äquivalent ist: K ist ein Teilring von L und $a^{-1} \in K$ für alle $a \in K$ ungleich Null.

In diesem Fall sagen wir, dass L/K eine **Körpererweiterung** ist. Verwechseln Sie dies nicht mit einem Faktorring.

Sei L ein Körper, und $E_i \subseteq L$ $(i \in I)$ eine Familie von Teilkörper. Dann ist der Schnitt $\bigcap_{i\in I} E_i$ einen Teilkörper von L.

Daraus folgt, dass es ein eindeutiger kleinster Teilkörper von L gibt (der Schnitt aller Teilkörper). Es wird der **Primkörper** von L genannt.

Die Charakteristik $\operatorname{Char} R$ eines Rings R ist die kleinste positive ganze Zahl n, so dass $n1_R = 0$ oder 0, wenn es kein solches n gibt. Somit ist die Charakteristik die ganze Zahl $n \geq 0$, so dass der eindeutige Ringhomomorphismus $\mathbb{Z} \to R$ den Kern $\mathbb{Z}n$ hat.

Proposition. *Die Charakteristik eines Körpers L ist entweder eine Primzahl p oder 0. Entsprechend, ist die Primkörper von L isomorph zu $\mathbb{Z}_p$ oder $\mathbb{Q}$.*

Beweis. Das Bild des Ringhomomorphismus $\mathbb{Z} \to L$ ist ein Integritätsbereich, daher ist der Kern ein Primideal, also $\mathbb{Z}p$ oder $\mathbb{Z}0$. Im ersten Fall ist $\operatorname{Bild}(\theta) = \mathbb{Z}/\mathbb{Z}p$ ein Körper, also der Primkörper. Im zweiten Fall ist θ ein injektiver Ringhomomorphismus, also induziert es einen Homomorphismus $\mathbb{Q} = \operatorname{Quot}(\mathbb{Z}) \to L$, und das Bild ist der Primkörper. □

Lemma. *Jeder Ringhomomorphismus von einem Körper zu einem Ring ungleich Null ist injektiv.*

Beweis. Sei $\theta : K \to R$. Da $\theta(1_K) = 1_R \neq 0$, ist $\operatorname{Ker}\theta \neq R$. Aber ein Körper hat nur zwei Ideale, also $\operatorname{Ker}\theta = \{0\}$. □

Definition. Für eine Körpererweiterung L/K und Elemente $a_1, \ldots, a_n \in L$ können wir den kleinsten Teilkörper $K(a_1, \ldots, a_n)$ betrachten, das $K \cup \{a_1, \ldots, a_n\}$ enthält. Dieser Teilkörper heißt den **von K und $a_1, \ldots, a_n$ erzeugte Teilkörper**. Mit anderen Worten, er wird aus K durch **Adjunktion** von $a_1, \ldots, a_n$ erhalten.

Beispiele. (1) $\mathbb{Q}(\pi) \subseteq \mathbb{Q}(\alpha)$, wobei $\alpha = \sqrt{\pi + 1}$, weil $\pi = \alpha^2 - 1 \in \mathbb{Q}(\alpha)$.

(2) $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{4})$ weil $\sqrt[3]{4} = (\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$ und $\sqrt[3]{2} = 2/\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{4})$.

(3) $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2}+i)$. Wir haben $\beta = \sqrt{2}+i \in \mathbb{Q}(\sqrt{2}, i)$, also $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\sqrt{2}, i)$. Nun $(\beta - i)^2 = 2$, also $\beta^2 - 2i\beta - 1 = 2$. Also $i = (\beta^2 - 3)/(2\beta) \in \mathbb{Q}(\beta)$. Dann $\sqrt{2} = \beta - i \in \mathbb{Q}(\beta)$. Also $\mathbb{Q}(\sqrt{2}, i) \subseteq \mathbb{Q}(\beta)$.

Erinnerung. Sei L/K eine Körpererweiterung und sei $a_1, \ldots, a_n \in L$. Dann ist $K[a_1, \ldots, a_n] = \text{Bild}(\theta)$, wobei $\theta : K[x_1, \ldots, x_n] \to L$ der Homomorphismus ist, der $p(x_1, \ldots, x_n)$ zu $p(a_1, \ldots, a_n)$ schickt. Somit ist $K[a_1, \ldots, a_n]$ ein Teilring von L, also ein Integritätsbereich.

Lemma. *$K(a_1, \ldots, a_n)$ ist isomorph zu* $\text{Quot}(K[a_1, \ldots, a_n])$.

Beweis. Offensichtlich ist $K[a_1, \ldots, a_n] \subseteq K(a_1, \ldots, a_n)$.

Die Inklusion $\theta : K[a_1, \ldots, a_n] \to K(a_1, \ldots, a_n)$ ist ein injektiver Ringhomomorphismus, und $K(a_1, \ldots, a_n)$ ist ein Körper, also gibt es einen Homomorphismus $\tilde{\theta} : \text{Quot}(K[a_1, \ldots, a_n]) \to K(a_1, \ldots, a_n)$.

Nun ist $\tilde{\theta}$ nach dem letzten Lemma injektiv, also ist $\text{Bild}(\tilde{\theta}) \cong \text{Quot}(K[a_1, \ldots, a_n])$ ein Teilkörper von $K(a_1, \ldots, a_n)$. Aber dann aufgrund der Minimalität bekommen wir $K(a_1, \ldots, a_n) = \text{Bild}(\tilde{\theta})$. □

Definition. Ist L/K eine Körpererweiterung, dann ist L auf natürlicherweise einen K-Vektorraum. Wir schreiben $[L : K] \coloneqq \dim_K L$ für die enstprechende Dimension, und nennen sie auch den **Grad** der Körpererweitung. Wir sagen, dass L/K eine **endliche** Körpererweiterungist ist, falls $[L : K]$ endlich ist.

z.B. $[\mathbb{C} : \mathbb{R}] = 2$, also ist $\mathbb{C}/\mathbb{R}$ endlich.

Satz (Gradsatz - Multiplikativität des Grades - Tower Law)**.** *Seien $M/L/K$ Körpererweiterungen. Dann ist M/K genau dann endlich, wenn beide M/L und L/K endlich sind, und*

$$[M : K] = [M : L][L : K].$$

Beweis. Angenommen, M/L und L/K sind endlich.

Sei $(x_1, \ldots, x_n)$ eine K-Basis für L und $(y_1, \ldots, y_m)$ eine L-Basis für M. Wir behaupten, dass $(x_i y_j : 1 \leq i \leq n, 1 \leq j \leq m)$ eine K-Basis für M ist.

Lineare Unabhängigkeit: Sei $\sum_{i,j} \lambda_{ij} x_i y_j = 0$ in M, wobei $\lambda_{ij} \in K$. Setzen Sie $\mu_j \coloneqq \sum_i \lambda_{ij} x_i$ in L. Dann gilt $\sum_j \mu_j y_j = 0$ in M, also $\mu_j = 0$ für alle j. Es folgt, dass $\lambda_{ij} = 0$ für alle (i, j).

Erzeugendensystem: Sei $z \in M$. Dann gilt $z = \sum_j \mu_j y_j$ mit $\mu_j \in L$. Nun schreiben Sie $\mu_j = \sum_i \lambda_{ij} x_i$ mit $\lambda_{ij} \in K$. Es folgt, dass $z = \sum_{i,j} \lambda_{ij} x_i y_j$.

Also M/K ist endlich und $[M : K] = [M : L][L : K]$.

Nehmen wir umgekehrt an, dass M/K endlich ist. Eine K-Basis von M ist ein Erzeugendensystem für M als Vektorraum über L, also ist M/L endlich. Als Vektorraum über K ist jedes linear unabhängige Tupel in L auch ein linear unabhängige Tupel in M, hat also höchstens $[M : K]$ Elemente. Somit ist L/K endlich. □

5.2 Algebraische und transzendente Elemente

Definition. Sei L/K eine Körpererweiterung, und sei $a \in L$. Wir sagen, dass a **algebraisch über** K ist, falls es $0 \neq f(X) \in K[X]$ gibt mit $f(a) = 0$. Ansonsten heißt a **transzendent über** K.

Beispiele. (1) Jedes Element $a \in K$ ist algebraisch über K, da es eine Nullstelle von $X - a \in K[X]$ ist.

(2) Für $\mathbb{R}/\mathbb{Q}$, $\sqrt[n]{2}$ ist algebraisch über $\mathbb{Q}$, da es eine Nullstelle von $X^n - 2 \in \mathbb{Q}[X]$ ist.

(3) Für $\mathbb{C}/\mathbb{Q}$, i ist algebraisch über $\mathbb{Q}$, weil $i^2 + 1 = 0$.

(4) Für $\mathbb{R}/\mathbb{Q}$, nach dem Satz von Lindemann–Weierstraß, sind π und e transzendent über $\mathbb{Q}$.
`https://de.wikipedia.org/wiki/Satz_von_Lindemann-Weierstrass`

(5) Sei K ein Körper und $K(T)$ der Körper rationaler Funktionen in T mit Koeffizienten in K. Dann ist jedes Element von $a \in K(T) \setminus K$ transzendent über K. Sagen wir $p(X) = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$ und $p(a) = 0$. Wir können annehmen, dass $a_0, a_n \neq 0$. Wir betrachten $p(X)$ als Polynom in $(K[T])[X]$. Durch den rationalen Nullstellentest können wir $a = r/s$ schreiben, wobei $r, s \in K[T]$, $r|a_0$ und $s|a_n$. Aber dann $r, s \in K$, also $a \in K$.

Proposition. *Sei L/K eine Körpererweiterung und nehmen Sie an, dass $a \in L$ transzendental über K ist. Dann*

(1) $K[a]$ ist kein Teilkörper von L, also $K[a] \neq K(a)$.

(2) $K(a)$ ist isomorph zu dem Körper rationaler Funktionen $K(X)$.

(3) $K(a)/K$ ist eine unendliche Körpererweiterung.

Beweis. Der Ringhomomorphismus $\theta : K[X] \to L$, $p(X) \mapsto p(a)$ ist injektiv.

(1) Somit ist $K[a]$ isomorph zu $K[X]$, was kein Körper ist.

(2) Dann gilt $K(a) \cong \mathrm{Quot}(K[a]) \cong \mathrm{Quot}(K[X]) = K(X)$.

(3) Wir haben $[K(a) : K] = \infty$, weil $(1, a, a^2, \ldots, a^n)$ linear unabhängig über K für alle n ist. □

Definition. Sei L/K eine Körpererweiterung und nehmen Sie an, dass $a \in L$ über K algebraisch ist. Somit gibt es ein Polynom ungleich Null $f(X) \in K[X]$ mit $f(a) = 0$. Es gibt also ein normiertes Polynom kleinsten Grades $m(X)$, so dass $m(a) = 0$. Es ist eindeutig bestimmt, denn wenn $m'(X)$ ein anderes normiertes Polynom gleichen Grades mit a als Nullstelle ist, dann ist $f(X) = m(X) - m'(X)$ ein von Null verschiedenes Polynom kleineren Grades mit a als Nullstelle, und daher gibt es ein normiertes Polynom kleineren Grades mit a als Nullstelle. Wir nennen $m(X)$ das **minimale Polynom** von a über K, bezeichnet mit $m_{a/K}(X)$.

Lemma. *Sei L/K eine Körpererweiterung und sei $a \in L$ algebraisch über K. Sei $f(X)$ ein normiertes Polynom in $K[X]$. Die folgenden sind äquivalent:*

(i) $f(X)$ ist das minimale Polynom $m_{a/K}(X)$ von a über K.

(ii) $f(X)$ ist irreduzibel in $K[X]$ und $f(a) = 0$.

(iii) Der Homomorphismus $\theta : K[X] \to L$, $\theta(p(X)) = p(a)$ hat $\operatorname{Ker}\theta = K[X]f(X)$. Das heißt, wenn $p(X) \in K[X]$, dann ist $p(a) = 0$ genau dann, wenn $f(X)|p(X)$.

Beweis. (i)⇒(ii) Wenn $f(X)$ nicht irreduzibel ist, dann ist $f(X) = g(X)h(X)$ mit $g(X)$ und $h(X)$ von kleinerem Grad als $f(X)$. Aber $g(a) = 0$ oder $h(a) = 0$.

(ii)⇒(iii) $K[X]$ ist ein Hauptidealbereich, also ist $\operatorname{Ker}\theta = K[X]g(X)$ für ein Polynom $g(X)$. Da a über K algebraisch ist, ist $g(X) \neq 0$. Also können wir annehmen, dass es normiert ist. Jetzt ist $f(a) = 0$, also $\theta(f(X)) = 0$, also ist $f(X)$ durch $g(X)$ teilbar. Da $f(X)$ irreduzibel ist, folgern wir, dass $f(X) = g(X)$.

(iii)⇒(i) ist klar. □

Satz. *Sei L/K eine Körpererweiterung, sei $a \in L$ algebraisch über K, und sei $n = \operatorname{Grad} m_{a/K}(X)$. Dann gilt:*

(1) $K[a]$ ist ein Teilkörper von L, also $K(a) = K[a]$;

(2) Jedes Element von $K(a)$ kann eindeutig in der Form $b_0 + b_1 a + \cdots + b_{n-1}a^{n-1}$ mit $b_i \in K$ geschrieben werden. Mit anderen Worten, $K(a)$ hat eine K-Basis $(1, a, a^2, \ldots, a^{n-1})$.

(3) $K(a)/K$ ist eine endliche Körpererweiterung, mit $[K(a) : K] = n$.

Beweis. Sei $\theta : K[X] \to L$ der Ringhomomorphisms $p(X) \mapsto p(a)$.

Also $\mathrm{Ker}(\theta) = K[X]m_{a/K}(X)$.

(1) Weil $m_{a/K}(X)$ irredizibel ist, ist $K[X]m_{a/K}(X)$ ein maximale Ideal in $K[X]$. Also ist $K[a] = \mathrm{Bild}(\theta) \cong K[X]/K[X]m_{a/K}(X)$ ein Körper. Also $K(a) = K[a]$.

(2) Nach der dritte Proposition von §3.3 kann die Elemente von $K[X]/K[X]m_{a/K}(X)$ eindeutig in der Form

$$\overline{b_0 + b_1 X + \cdots + b_{n-1}X^{n-1}}$$

mit $b_i \in K$ geschrieben werden. Somit können die Elemente von $K(a) = K[a] \cong K[X]/K[X]m_{a/K}(X)$ eindeutig in der Form

$$b_0 + b_1 a + \cdots + b_{n-1}a^{n-1}.$$

geschrieben werden.

(3) Folgt. □

Beispiele. (1) $m_{\sqrt[n]{2}/\mathbb{Q}}(X) = X^n - 2$, weil $\sqrt[n]{2}$ eine Nullstelle ist, und nach Eisenstein mit $p = 2$ ist das Polynom irreduzibel. Es gilt:

$$\mathbb{Q}(\sqrt[n]{2}) = \{b_0 + b_1 \sqrt[n]{2} + \cdots + b_{n-1}(\sqrt[n]{2})^{n-1} : b_i \in \mathbb{Q}\}.$$

(2) Sei $\alpha = \sqrt{\sqrt{7} - 1}$. Dann ist $(\alpha^2 + 1)^2 = 7$, also $\alpha^4 + 2\alpha^2 - 6 = 0$. Nach Eisenstein mit $p = 2$ ist das Polynom $X^4 + 2X^2 - 6$ irreduzibel in $\mathbb{Q}[X]$. Also ist es das minimale Polynom von α über $\mathbb{Q}$. Also $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

(3) Sei p eine Primzahl. Dann ist $\zeta = \exp(2\pi i/p) \in \mathbb{C}$ eine Nullstelle von $X^p - 1$, also ist ζ algebraisch über $\mathbb{Q}$. Es gilt $X^p - 1 = (X - 1)(X^{p-1} + \cdots + X + 1)$, $\zeta \neq 1$, und wir wissen schon, dass $X^{p-1} + \cdots + X + 1$ in $\mathbb{Q}[X]$ irreduzibel ist. Also ist $m_{\zeta/\mathbb{Q}}(X) = X^{p-1} + \cdots + X + 1$, und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$.

(4) Sei $\beta = \sqrt{2} + i$. Jetzt ist $(\beta - i)^2 = 2$, also $\beta^2 - 2i\beta - 1 = 2$, also $\beta^2 - 3 = 2i\beta$, also $(\beta^2 - 3)^2 = -4\beta^2$, also $\beta^4 - 2\beta^2 + 9 = 0$. Somit ist β eine Nullstelle von $X^4 - 2X^2 + 9$. Ist es das minimale Polynom?

Nach §5.1 Beispiel (3) wissen wir schon, dass $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2}, i)$. Sei $K = \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. Dann ist $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2}, i) = K(i)$. Die Elemente von K sind reelle Zahlen, also hat $X^2 + 1$ keine Nullstelle in K. Daher ist es in $K[X]$ irreduzibel. Also $m_{i/K}(X) = X^2 + 1$. Also

$$[\mathbb{Q}(\beta) : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [K(i) : K] = 2 \cdot 2 = 4.$$

Somit ist $\operatorname{Grad} m_{\beta/\mathbb{Q}}(X) = 4$. Also ist $m_{\beta/\mathbb{Q}}(X) = X^4 - 2X^2 + 9$.

Definition. Eine Körpererweiterung L/K heißt **algebraisch**, wenn jedes $a \in L$ algebraisch über K ist.

Korollar. *Sei L/K eine Körpererweiterung.*

(i) Wenn L/K eine endliche Körpererweiterung ist, dann ist sie algebraisch.

(ii) Wenn $a_1, \ldots, a_n \in L$ algebraisch über K sind, dann ist $K(a_1, \ldots, a_n)/K$ eine endliche Erweiterung.

Beweis. (i) Sei $a \in L$. Also haben wir Körpererweiterungen $L/K(a)/K$. Nach dem Gradsatz ist $K(a)/K$ endlich. Also ist a algebraisch über K.

(ii) Definieren Sie $K_i = K(a_1, \ldots, a_i)$. Also,

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K(a_1, \ldots, a_n).$$

Dann ist $K_i = K_{i-1}(a_i)$. Nun ist a_i algebraisch über K, also auch über K_{i-1}. Somit ist K_i/K_{i-1} endlich. Dann ist

$$[K(a_1, \ldots, a_n) : K] = [K_1 : K_0] \cdot [K_2 : K_1] \cdot \cdots \cdot [K_n : K_{n-1}] < \infty$$

aufgrund der Multiplikativität des Grades. □

5.3 Konstruktionen mit Zirkel und Lineal

Beispiele. (i) Konstruieren Sie die Mittelsenkrechte einer Strecke AB.

Zeichnen Sie den Kreis mit Mittelpunkt A und Radius $|AB|$. Zeichnen Sie den Kreis mit dem Mittelpunkt B und demselben Radius. Zeichnen Sie die Gerade CD durch die Schnittpunkte.

(ii) Konstruieren Sie die Gerade durch einen Punkt P senkrecht zu einer Geraden L.

Zeichnen Sie einen Kreis mit dem Mittelpunkt P und einem ausreichenden Radius, um L bei A und B zu treffen. Konstruieren Sie dann die Mittelsenkrechte von AB.

(iii) Konstruieren Sie die Gerade durch einen Punkt P parallel zu einer Geraden L.

Zeichnen Sie die Gerade L' durch P senkrecht zu L und dann die Gerade durch P senkrecht zu L'.

Definition. Eine Zahl $a \in \mathbb{R}$ ist **konstruierbar**, wenn man mit zwei markierten Punkten in der Ebene im Einheitsabstand beginnt und es mit den folgenden Operationen möglich ist, zwei markierte Punkte zu konstruieren, deren Abstand zwischen ihnen ist $|a|$.

(i) Zeichnen Sie die Gerade durch zwei markierte Punkte,

(ii) Zeichnen Sie einen Kreis mit einem markierten Punkt als Mittelpunkt und einem Radius, der dem Abstand zwischen zwei markierten Punkten entspricht.

(iii) Markieren Sie einen beliebigen Schnittpunkt von Geraden und Kreisen.

Lemma. *Die Menge S der konstruierbaren Zahlen ist ein Teilkörper von $\mathbb{R}$ und wenn $a > 0$ in S ist, dann gilt $\sqrt{a} \in S$.*

Beweis. Wir wissen, dass $0, 1 \in S$ und S unter negativen Werten geschlossen sind. Um zu zeigen, dass S ein Teilkörper ist, reicht es zu beweisen, dass, wenn $a, b \in S$ positiv sind, $a \pm b, a/b \in S$.

Bei gegebenen Längen a, b können wir einen Zirkel verwenden, um die Längen a, b auf derselben Gerade zu ermitteln und somit $a \pm b$ zu konstruieren.

Zeichnen Sie senkrechte Liniensegmente OA und OB mit den Längen a und b. Sei P ein Punkt auf der Geraden OB mit $|OP| = 1$. Die Linie parallel zu AB durch P trifft die Linie OA an einem Punkt T mit $|OT| = a/b$, also $a/b \in S$. Insbesondere $1/a \in S$. Dann ist $ab = a/(1/b) \in S$.

Markieren Sie auf einer Gerade L die Punkte A, B, C mit $|AB| = 1$ und $BC = a$. Zeichnen Sie den Kreis mit dem Durchmesser AC und lassen Sie ihn bei D auf die Senkrechte zu L durch B treffen. Sei $b = |DB|$. Dann ist der Winkel ADC gleich $\pi/2$, also ist Winkel DCB = Winkel ADB, also sind diese Dreiecke ähnlich. Somit ist $a/b = b/1$. Also $b = \sqrt{a}$. □

Satz. *Wenn $\alpha \in \mathbb{R}$, dann ist a genau dann konstruierbar, wenn $\alpha \in K_n$ für eine Folge von Körpern*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R},$$

wobei $K_i = K_{i-1}(\sqrt{\lambda_i})$ mit $\lambda_i \in K_{i-1}$ und $\lambda_i \geq 0$.

(Möglicherweise $\sqrt{\lambda_i} \in K_{i-1}$, zum Beispiel wenn $\lambda_i = 0$, so dass $K_i = K_{i-1}$.)

Beweis. Wenn es eine Folge von Körpern gibt, ist α durch das Lemma konstruierbar.

Nehmen wir nun an, dass α konstruierbar ist. Beginnend mit markierten Punkten $P_{-1} = (0,0), P_0 = (1,0)$ konstruieren wir Punkte $P_i = (x_i, y_i)$ für $i = 1, \ldots, n$ mit $P_n = (\alpha, 0)$. Wir definieren

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$

durch $K_i = K_{i-1}(x_i, y_i)$. Es genügt zu zeigen, dass $K_i = K_{i-1}(\sqrt{\lambda_i})$ mit $\lambda_i \in K_{i-1}$, $\lambda_i \geq 0$.

$P_i = (x_i, y_i)$ ist ein Schnittpunkt von Geraden und Kreisen, der durch markierte Punkte definiert wird, deren Koordinaten in K_{i-1} liegen. Wir betrachten einen Schnittpunkt zweier Kreise (die anderen Fälle sind einfacher). Wenn ein Kreis den Mittelpunkt P_j und den Radius $|P_k P_\ell|$ hat, mit $j, k, \ell < i$, dann hat er die Gleichung

$$(x - x_j)^2 + (y - y_j)^2 = (x_k - x_\ell)^2 + (y_k - y_\ell)^2$$

welches von der Form

$$x^2 + y^2 + ax + by + c = 0 \qquad (1)$$

ist, mit $a, b, c \in K_{i-1}$. Der andere Kreis hat eine Gleichung

$$x^2 + y^2 + a'x + b'y + c' = 0. \qquad (2)$$

Dann ergibt (1)-(2).

$$(a - a')x + (b - b')y + (c - c') = 0. \qquad (3)$$

Ohne Beschränkung der Allgemeinheit können wir annehmen, dass $a \neq a'$. Dann

$$x = -\frac{1}{a - a'}\left((b - b')y + (c - c')\right). \qquad (4)$$

Durch Einsetzen in (1) erhalten wir eine quadratische Gleichung für y

$$Ay^2 + By + C = 0. \qquad (5)$$

Wenn wir nach y und dann nach x auflösen, erhalten wir $x_i, y_i \in K_i(\sqrt{d})$, wobei $d = B^2 - 4AC \in K_{i-1}$ und $d \geq 0$, also $K_i = K_{i-1}(\sqrt{d})$. □

Korollar. *Wenn a konstruierbar ist, dann ist es algebraisch über $\mathbb{Q}$ und* $\operatorname{Grad} m_{a/\mathbb{Q}}(X)$ *ist eine Potenz von 2.*

Beweis. Wir haben $[K_i : K_{i-1}] \in \{1, 2\}$, abhängig davon, ob $\sqrt{\lambda_i} \in K_{i-1}$ oder nicht. Aufgrund der Multiplikativität des Grades ist $[K_n : \mathbb{Q}]$ eine Potenz von 2. Dann ist $[\mathbb{Q}(a) : \mathbb{Q}]$ ein Teiler von $[K_n : \mathbb{Q}]$, also es ist auch eine Potenz von 2. □

Korollar (Wantzel 1837)**.** *(i) (Verdoppelung des Würfels) $\sqrt[3]{2}$ ist nicht konstruierbar. Daher gibt es keine Lineal- und Zirkelkonstruktion, die bei einer gegebenen Strecke der Länge r eine Strecke der Länge $\sqrt[3]{2}r$ konstruiert, die Seite eines Würfels mit dem doppelten Volumen.*

(ii) (Quadratur des Kreises) $\sqrt{\pi}$ ist nicht konstruierbar. Daher gibt es keine Lineal- und Zirkelkonstruktion, die bei einer gegebenen Strecke der Länge r eine Strecke der Länge $\sqrt{\pi}r$ konstruiert, die Seite eines Quadrats mit der gleichen Fläche wie ein Kreis mit dem Radius r.

(iii) (Dreiteilung des Winkels) $\cos(\pi/9)$ *ist nicht konstruierbar. Daher gibt es kein allgemeines Verfahren zur Dreiteilung von Winkeln.*

(iv) Wenn ein reguläres p-Eck konstruiert werden kann und p eine Primzahl ist, dann ist $p - 1$ eine Potenz von 2, das heißt, p ist eine Fermat-Primzahl.

Beweis. (i) $\sqrt[3]{2}$ hat minimales Polynom $x^3 - 2$ vom Grad 3.

(ii) π ist nach einem Satz von Lindemann (1882) transzendent über $\mathbb{Q}$. Daraus folgt, dass $\sqrt{\pi}$ über $\mathbb{Q}$ transzendent ist.

(iii) Es gilt $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ und $\cos(\pi/3) = 1/2$, also ist $a = \cos(\pi/9)$ eine Nullstelle des Polynoms

$$8X^3 - 6X - 1.$$

Dies ist durch den rationaler Nullstellentest irreduzibel in $\mathbb{Q}[X]$. Somit gilt

$$m_{a/\mathbb{Q}}(X) = X^3 - \tfrac{6}{8}X - \tfrac{1}{8}.$$

Also ist a nicht konstruierbar. Es ist einfach, ein gleichseitiges Dreieck zu konstruieren, also den Winkel $\pi/3$. Wenn es dreigeteilt werden könnte, könnten wir a konstruieren.

(iv) Wenn ein reguläres p-Eck konstruiert werden kann, dann ist $a = \cos(2\pi/p) \in S$. Also ist $[\mathbb{Q}(a) : \mathbb{Q}] = 2^n$. Sei $\zeta = e^{2\pi i/p}$. Dann ist $a = \frac{1}{2}(\zeta + \zeta^{-1}) \in \mathbb{Q}(\zeta)$, also $\mathbb{Q}(a) \subseteq \mathbb{Q}(\zeta)$. Jetzt ist $\zeta^2 - 2a\zeta + 1 = 0$ und ζ ist nicht reell, also ist ζ algebraisch

über $\mathbb{Q}(a)$ mit minimalem Polynom $X^2 - 2aX + 1$. Dann ist $p - 1 = [\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}(a)] = 2^n \cdot 2$. □

Bemerkung. Jede Fermat-Primzahl muss die Form

$$F_n = 2^{2^n} + 1$$

haben, und $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ und $F_4 = 65537$ sind Primzahlen. Fermat vermutete, dass alle Zahlen F_n Primzahlen sind, aber Euler faktorisierte F_5, und tatsächlich sind keine anderen Fermat-Primzahlen bekannt.

Gauß (1798) hatte bewiesen: wenn p eine Fermat-Primzahl ist, das reguläre p-Eck konstruiert werden kann. Am besten lässt sich dieser Beweis anhand der Galois-Theorie verstehen. (Die Körpererweiterung $\mathbb{Q}(\zeta)/Q$ ist Galois mit abelscher Galois-Gruppe.)

5.4 Zerfällungskörper

Als nächstes wollen wir einen Körpererweiterung L/K konstruieren, in dem ein gegebenes Polynom $f(X) \in K[X]$ alle seinen Nullstellen hat.

Lemma. *Sei K ein Körper. Sei $f(X) \in K[X]$ ein irreduzibles Polynom vom Grad n. Dann ist $L = K[X]/K[X]f(X)$ ein Körper. Der Ringhomomorphismus $K \to L$ ist injektiv, daher können wir L als Erweiterungskörper von K identifizieren. Sei $a = K[X] + X \in L$. Dann sind $f(a) = 0$ und $(1, a, a^2, \ldots, a^{n-1})$ eine K-Basis von L. Somit ist $L = K(a)$ und L/K ist eine endliche Körpererweiterung vom Grad $[L : K] = n$.*

Beweis. Da $f(X)$ irreduzibel ist, ist $K[X]f(X)$ nach §4.3 Satz ein maximales Ideal in $K[X]$.

Dann ist L ein Körper nach §4.1 Proposition.

Nach §3.3 dritter Proposition ist $(1, a, \ldots, a^{n-1})$ eine K-Basis von L, und $f(a) = 0$. □

Satz (Kronecker)**.** *Sei K ein Körper und $f(X) \in K[X]$ ein nicht konstantes Polynom. Dann gibt es eine Körpererweiterung L/K mit*

$$[L : K] \leq \operatorname{Grad} f(X)$$

in dem $f(X)$ eine Nullstelle hat.

Beweis. Wenden Sie das Lemma auf einem irreduziblen Faktor von $f(X)$ an. $\square$

Definition. Sei $f(X) \in K[X]$ ein Polynom ungleich Null. Ein **Zerfällungskörper** von $f(X)$ über K ist eine Körpererweiterung L/K, so dass:

(i) $f(X)$ zerfällt vollständig in lineare Faktoren in $L[X]$, d.h

$$f(X) = c(X - a_1) \dots (X - a_n)$$

mit $c \in K$ der Leitkoeffizient von $f(X)$ und $a_i \in L$.

(ii) $f(X)$ zerfällt nicht in lineare Faktoren in $E[X]$ für jeden echten **Zwischenkörper** E, d.h. $K \subseteq E \subseteq L$ und $E \neq L$.

Lemma. *Sei $f(X) \in K[X]$ ein Polynom ungleich Null und M/K eine Körpererweiterung, sodass $f(X)$ zerfällt in Linearfaktoren in $M[X]$,*

$$f(X) = c(X - a_1) \dots (X - a_n) \in L[X].$$

Dann ist $K(a_1, \dots, a_n)$ ein Zerfällungskörper von $f(X)$.

Beweis. Sei L ein Körper mit $K \subseteq L \subseteq M$. Wenn $a_1, \dots, a_n \in L$, dann kann $f(X)$ als Produkt linearer Faktoren in $L[X]$ geschrieben werden. Wenn umgekehrt $f(X)$ als Produkt linearer Faktoren $c(X - b_1) \dots (X - b_n)$ in $L[X]$ geschrieben werden kann, dann durch die Eindeutigkeit der Zerlegung in $M[X]$ sind die b_i bis auf die Reihenfolge die gleichen wie die a_i. Somit sind $a_1, \dots, a_n \in L$. $\square$

Satz. *Sei $f(X) \in K[X]$ ein Polynom ungleich Null. Dann existiert ein Zerfällungskörper L/K mit*

$$[L : K] \leq (\operatorname{Grad} f(X))!$$

Beweis. Nach dem Lemma genügt es, eine Körpererweiterung L/K zu finden, so dass $f(X)$ in lineare Faktoren in $L[X]$ zerfällt.

Wir beweisen dies durch Induktion nach $\operatorname{Grad} f(X)$. Wenn $\operatorname{Grad} f(X) = 0$, ist dies klar, also nehmen wir an, $\operatorname{Grad} f(X) = n > 0$. Nach dem Satz von Kronecker gibt es eine Körpererweiterung L/K mit $[L : K] \leq n$, in der $f(X)$ eine Nullstelle a hat. Dann ist $f(X) = (X - a)g(X)$ in $L[X]$. Durch die Induktion gibt es eine Körpererweiterung M/L mit $[M : L] \leq (n-1)!$, sodass $g(X)$ in linearen Faktoren in $M[X]$ zerfällt. Dann zerfällt auch $f(X)$, und $[M : K] = [M : L] \cdot [L : K] \leq (n-1)! \cdot n = n!$. $\square$

Wir werden später sehen, dass Zerfällungskörper bis auf Isomorphie eindeutig sind.

Beispiel. (1) Wenn $d \in \mathbb{Q}$, dann ist $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ ein Zerfällungskörper von $X^2 - d$.

(2) Wenn n eine positive ganze Zahl ist und $\zeta = e^{2\pi i/n}$, dann ist $\mathbb{Q}(\zeta)/\mathbb{Q}$ ein Zerfällungskörper von $X^n - 1$, da es Nullstellen $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ in $\mathbb{C}$ hat.

(3) $\alpha = \sqrt[3]{2}$ ist eine Nullstelle von $X^3 - 2$, und in $\mathbb{Q}(\alpha)[X]$ können wir schreiben

$$X^3 - 2 = (X - \alpha)(X^2 + \alpha X + \alpha^2),$$

aber wir können den quadratischen Faktor nicht als Produkt über $\mathbb{Q}(\alpha)$ schreiben, also ist $\mathbb{Q}(\alpha)$ kein Zerfällungskörper von $X^3 - 2$.

In der Tat, wenn $\omega = e^{2\pi i/3} = \frac{1}{2}(-1 + \sqrt{-3})$, dann sind $\alpha, \omega\alpha, \omega^2\alpha$ die Nullstellen von $X^3 - 2$ in $\mathbb{C}$, also

$$X^3 - 2 = (X\alpha)(X - \omega\alpha)(X - \omega^2\alpha).$$

Somit ist $L = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) = \mathbb{Q}(\alpha, \omega)$ ein Zerfällungskörper von $X^3 - 2$. Es gilt

$$[L : \mathbb{Q}] = [\mathbb{Q}(\alpha, \omega)) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Hier ist $m_{\alpha/\mathbb{Q}}(X) = X^3 - 2$, weil $X^3 - 2$ irreduzible nach Eisenstein ist. Und $m_{\omega/\mathbb{Q}(\alpha)}(X) = X^2 + X + 1$, weil $\omega^2 + \omega + 1$ und $\omega \notin \mathbb{Q}(\alpha) \subseteq \mathbb{R}$.

(4) Seien $f(X) = X^3 - 2X - 2 \in \mathbb{Q}[X]$ und $u = \sqrt[3]{27 - 3\sqrt{57}} \in \mathbb{R}$. Man kann zeigen, dass

$$\alpha = \tfrac{u}{3} + \tfrac{2}{u}, \quad \beta = \tfrac{\omega u}{3} + \tfrac{2}{\omega u}, \quad \gamma = \tfrac{\omega^2 u}{3} + \tfrac{2}{\omega^2 u}$$

sind drei unterschiedliche Nullstellen von $f(X)$ in $\mathbb{C}$ mit $\alpha \in \mathbb{R}$ und $\beta, \gamma \notin \mathbb{R}$. Der Zerfällungskörper für $f(X)$ über $\mathbb{Q}$ ist also $L = \mathbb{Q}(\alpha, \beta, \gamma)$.

Die Formeln für α, β, γ sind durch Radikale gegeben, aber dazu verwenden wir die Elemente u, ω und wir werden zeigen, dass $u \notin L$.

Es gilt $L = \mathbb{Q}(\alpha, \beta)$, denn wenn ein Teilkörper von alle bis auf eine Nullstelle von $f(X)$ enthält, dann enthält es durch Polynomdivision die letzte.

Wir haben $m_{\alpha/\mathbb{Q}}(X) = f(X)$, also $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Durch Polynomdivision in $\mathbb{Q}(\alpha)[X]$ finden wir

$$f(X) = (X - \alpha)g(X), \quad g(X) = X^2 + \alpha X + \alpha^2 - 2.$$

Das Polynom $g(X)$ hat keine Nullstelle in $\mathbb{Q}(\alpha)$, da $\beta, \gamma \notin \mathbb{R}$ sind. Somit ist $m_{\beta/\mathbb{Q}(\alpha)}(X) = X^2 + \alpha X + \alpha^2 - 2$. Also $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$. Daher ist

$$[L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 3 \cdot 2 = 6.$$

Es gilt $[\mathbb{Q}(u) : \mathbb{Q}] \leq 6$, weil $(27 - u^3)^2 = 9 \cdot 57$, also ist u eine Nullstelle von $X^6 - 54X^3 + 27^2 - 9 \cdot 57$. Es gelten $\mathbb{Q}(\alpha), \mathbb{Q}(\sqrt{57}) \subseteq \mathbb{Q}(u)$ und $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, $[\mathbb{Q}(\sqrt{57}) : \mathbb{Q}] = 2$, also ist $[\mathbb{Q}(u) : \mathbb{Q}]$ durch 3 und 2 teilbar, also ist $[\mathbb{Q}(u) : \mathbb{Q}] = 6$.

Nun $u \notin L$, sonst $\mathbb{Q}(u) \subseteq L$, aber beide haben Grad 6 über $\mathbb{Q}$, also $\mathbb{Q}(u) = L$. Aber $\mathbb{Q}(u)$ besteht aus reellen Zahlen und L nicht.

5.5 Endliche Körper

Lemma (1)**.** *Die Characteristik eines endlichen Körpers $\mathbb{F}$ muss eine Primzahl p sein, daher ist der Primkörper von $\mathbb{F}$ gleich $\mathbb{Z}_p$. Darüber hinaus ist $\mathbb{F}/\mathbb{Z}_p$ eine endliche Körpererweiterung und $\mathbb{F}$ hat $q = p^n$ Elemente, wobei $n = [\mathbb{F} : \mathbb{Z}_p]$.*

Beweis. Klar. □

Lemma (2)**.** *(i) Sei R ein kommutativer Ring. Seien $a, b \in R$ und $n \geq 0$. Dann gilt*

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

(ii) Sei R ein kommutativer Ring mit $\operatorname{Char} R = p$ eine Primzahl. Dann gilt

$$(a + b)^p = a^p + b^p$$

*für $a, b \in R$. Also ist die Abbildung $\mathrm{Fr} : R \to R$, $\mathrm{Fr}(a) = a^p$ ein Ringhomomorphismus, genannt der **Frobeniusendomorphismus** von R. Wenn $q = p^m$ eine Potenz von p ist, ist Fr^m auch ein Ringhomomorphismus, mit $\mathrm{Fr}^m(a) = a^q$.*

(iii) Sei I eine Menge und seien $\theta_i : R \to S$ Ringhomomorphismen für $i \in I$. Dann ist

$$T = \{r \in R : \theta_i(r) = \theta_j(r) \ \forall i, j \in I\}$$

ein Teilring von R. Wenn $r \in T$ eine Einheit in R ist, dann ist $r^{-1} \in T$. Wenn insbesondere R ein Körper ist, dann ist T ein Teilkörper von R.

Beweis. (i) Induktion auf n.

(ii) Für $0 < i < n$ ist $\binom{p}{i}$ ein Vielfaches von p, also Null in R. Es ist klar, dass $(ab)^p = a^p b^p$ und $1^p = 1$.

(iii) Übung. □

Lemma (3)**.** *Wenn K ein Körper ist, dann ist jede endliche Untergruppe G von $K^\times$ zyklisch. Insbesondere wenn $\mathbb{F}$ ein endlicher Körper ist, dann ist $\mathbb{F}^\times$ zyklisch.*

Beweis. Die Gruppe G ist abelsch, also nach §2.5 ist $G \cong \mathbb{Z}/\mathbb{Z}q_1 \times \cdots \times \mathbb{Z}/\mathbb{Z}q_t$ für Primpotenzen q_i. Nach dem chinesischen Restsatz reicht es zu zeigen, dass die q_i paarweise teilerfremd sind. Wenn nicht, dann ist $d = \mathrm{kgV}(q_1, \ldots, q_t) < q_1 \ldots q_t = |G|$. Es gilt $dx = 0$ für alle $x \in \mathbb{Z}/\mathbb{Z}q_1 \times \cdots \times \mathbb{Z}/\mathbb{Z}q_t$, also, multiplikativ geschrieben, $g^d = 1$ für alle $g \in G$. Aber das Polynom $X^d - 1$ kann höchstens d Nullstellen in K haben. □

Satz. *Sei p eine Primzahl. Für jede Primpotenz $q = p^n$ mit $n \geq 1$ existiert einen Körper $\mathbb{F}_q$ mit q Elemente. Der ist eindeutig bis auf Isomorphie, und kann als Zerfällungskörper für $X^q - X$ über $\mathbb{Z}_p$ konstruiert werden.*

Beweis. Existenz. Sei $\mathbb{F}/\mathbb{Z}_p$ ein Zerfällungskörper für das Polynom $X^q - X$ über $\mathbb{Z}_p$. Also

$$X^q - X = (X - a_1) \ldots (X - a_q)$$

für $a_i \in \mathbb{F}$. Sie sind Nullstellen von $X^q - X$, also $a_i^q = a_i$.

Beachten Sie, dass die a_i verschieden sind, denn wenn $a = a_i = a_j$ mit $i \neq j$, dann ist $(X - a)^2$ ein Teiler von

$$X^q - X = (X^q - X) - (a^q - a) = (X^q - a^q) - (X - a) = (X - a)^q - (X - a)$$

da nach Lemma (2)(ii) der Frobenius-Endomorphismus von $\mathbb{Z}_p[X]$ ein Ringhomomorphismus ist. Dann ist $(X - a)^2$ ein Teiler von $X - a$, was Unsinn ist.

Nach Lemma (2)(iii) ist

$$L = \{\alpha \in \mathbb{F} : \alpha^q = \alpha\} = \{\alpha \in \mathbb{F} : \mathrm{Fr}^n(\alpha) = \mathrm{Id}_{\mathbb{F}}(\alpha)\}$$

ein Teilkörper von $\mathbb{F}$. Aber $X^q - X$ zerfällt über L, also gilt aufgrund der Minimalität von Zerfällungskörper $L = \mathbb{F}$.

Nun kann ein Polynom vom Grad d höchstens d Nullstellen in einem Körper haben, also $|L| \leq q$. Aber $a_1, \ldots, a_q \in L$, also ist $\mathbb{F} = L$ ein Körper mit q Elementen.

Eindeutigkeit. Angenommen, $\mathbb{F}'$ ist ein weiterer Körper mit q Elementen.

Nach Lemma (1) ist $\mathrm{Char}\,\mathbb{F}' = p$ und $\mathbb{F}'$ hat Primkörper $\mathbb{Z}_p$.

Nach Lemma (3) ist die Gruppe $(\mathbb{F}')^\times$ zyklisch mit Ordnung $q-1$. Sei β ein Erzeuger dieser Gruppe. Offensichtlich $\mathbb{F}' = \mathbb{Z}_p(\beta)$. Außerdem ist $\beta^{q-1} = 1$, also $\beta^q - \beta = 0$.

Somit ist das minimale Polynom $m(X)$ von β über $\mathbb{Z}_p$ ein Faktor von $X^q - X$ in $\mathbb{Z}_p[X]$.

Somit ist eines der a_i eine Nullstelle von $m(X)$ in $\mathbb{F}$. Da $m(X)$ irreduzibel ist, ist es das Minimalpolynom von q_i über $\mathbb{Z}_p$. Der Auswertungshomomorphismus $\mathbb{Z}_p[X] \to \mathbb{F}$, $f(X) \mapsto f(a_i)$. gibt einen Ringhomomorphismus

$$\mathbb{F}' = \mathbb{Z}_p(\beta) \cong \mathbb{Z}_p[X]/\mathbb{Z}_p[X]m(X) \to \mathbb{F}.$$

Diese Abbildung ist injektiv und $\mathbb{F}$ und $\mathbb{F}'$ haben beide q Elemente, also ist dieser Homomorphismus ein Isomorphismus. □

Bemerkung. Für eine Primzahl p gilt $\mathbb{F}_p = \mathbb{Z}_p$, aber $\mathbb{F}_{p^n} \ncong \mathbb{Z}_{p^n}$ für $n > 1$.

z.B. $\mathbb{F}_4 = \mathbb{F}_2[X]/\mathbb{F}_2[X](X^2 + X + 1) = \{0, 1, a, 1 + a\}$, mit $a = \bar{X}$. Also $1 + 1 = 0$, $a + a = 0$, $a^2 = a + 1$.

6 Galoistheorie

Die Galois-Theorie ist die Untersuchung von Polynomen anhand bestimmter Permutationen ihrer Nullstellen oder äquivalenter Symmetriegruppen ihrer Zerfällungskörper.

Es wurde von Galois (1811-1832) erfunden, um diejenigen Polynome zu charakterisieren, die durch Radikale gelöst werden können.

Zum Beispiel, $f(X) = X^3 - 2X - 2$ in $\mathbb{Q}[X]$ hat eine Nullstelle $\alpha \in \mathbb{R}$, wobei

$$\alpha = \frac{u}{3} + \frac{2}{u} \qquad \text{für } u = \sqrt[3]{27 - 3\sqrt{57}}.$$

Anderseits kann man keine Nullstelle von $g(X) = X^5 - 4X + 2 \in \mathbb{Q}[X]$ durch Radikale über $\mathbb{Q}$ darstellen.

In diesem Abschnitt untersuchen wir Symmetriegruppen für Körpererweiterungen. Im nächsten Abschnitt untersuchen wir die Lösung von Polynomen durch Radikale.

6.1 Fortsetzung von Homomorphismen

Definition. Seien L, M Körper. Wir schreiben $\mathrm{Alg}(L, M)$ für die Menge aller Ringhomomorphismen $L \to M$. Sie müssen injektiv sein.

Sei L/K eine Körpererweiterung und $j \in \mathrm{Alg}(K, M)$. Einschränkung definiert eine Abbildung $\mathrm{Alg}(L, M) \to \mathrm{Alg}(K, M)$, $\theta \mapsto \theta|_K$. Ein Homomorphismus $\tilde{\jmath} \in \mathrm{Alg}(L, M)$ ist eine **Fortsetzung** von j, falls $\tilde{\jmath}\,|_K = j$. Wir schreiben $\mathrm{Alg}_K(L, M)$ für die Menge aller Fortsetzungen von j. Dies hängt von j ab, aber j erscheint nicht in der Notation.

Sei R ein Ring. Wir schreiben $\mathrm{Aut}(R)$ für die Gruppe aller Ringautomorphismen von R, d.h. Ringisomorphismen $R \to R$.

Die **Galoisgruppe** von einer Körpererweiterung L/K ist die Gruppe

$$\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) : \sigma(\alpha) = \alpha \text{ für alle } \alpha \in K\}.$$

Lemma. *Ist L/K endlich, dann gilt $\mathrm{Gal}(L/K) = \mathrm{Alg}_K(L, L)$, wobei $j : K \to L$ die Inklusionsabbildung ist.*

Beweis. Es ist klar, dass $\mathrm{Gal}(L/K) \subseteq \mathrm{Alg}_K(L, L)$.

Sei $\sigma \in \mathrm{Alg}_K(L, L)$. Dann ist σ eine injektive lineare Abbildung zwischen K-Vektorräume. Also gilt $\dim_K \mathrm{Bild}(\sigma) = \dim_K L$, und dadurch $\mathrm{Bild}(\sigma) = L$. Es folgt, dass σ ein Ringisomorphismus ist. □

Lemma (Fortsetzungslemma)**.** *Sei $j\colon K \to M$ ein Homomorphismus, und $L = K(\alpha)$ eine endliche Erweiterung von K. Ist*

$$m(X) = a_0 + a_1 X + a_2 X^2 + \cdots \in K[X]$$

das Minimalpolynom von α über K, dann bildet die Abbildung $\mathrm{Alg}_K(L, M) \to M$, $\tilde{\jmath} \mapsto \tilde{\jmath}(\alpha)$, eine Bijektion zwischen die Fortsetzungen von j und die Nullstellen in M von dem Polynom

$$j(m(X)) := j(a_0) + j(a_1)X + j(a_2)X^2 + \cdots \in M[X].$$

Beweis. Wir haben $L \cong K[X]/K[X]m(X)$, also stehen nach dem Homomorphiesatz die Elemente von $\mathrm{Alg}_K(L, M)$ in Bijektion mit den Homomorphismen $\theta : K[X] \to M$, die j erweitern und mit $m(X) \in \mathrm{Ker}(\theta)$.

Nun gibt es für $\beta \in M$ den Homomorphismus $\mathrm{ev}_\beta : K[X] \to M$, $\sum_i a_i X^i \mapsto \sum_i j(a_i)\beta^i$. Darüber hinaus hat nach Lemma (3) von §3.2 jeder Ringhomomorphismus $\theta : K[X] \to M$, der j erweitert, diese Form.

Nun ist $m(X) \in \mathrm{Ker}(\mathrm{ev}_\beta)$ genau dann, wenn β eine Nullstelle von $j(m(X))$ ist. □

Satz. *Sei $j\colon K \to M$ ein Homomorphismus, und L/K eine endliche Erweiterung. Dann gilt*

$$|\mathrm{Alg}_K(L, M)| \leq [L : K].$$

Insbesondere ist $|\mathrm{Gal}(L/K)| \leq [L : K]$.

Beweis. Wir beweisen dies durch Induktion über $n = [L : K]$. Wenn $n = 1$ ist, ist es trivial, also nehmen wir an, dass $n > 1$ ist. Sei $\alpha \in L \setminus K$ und setzen Sie $E = K(\alpha)$.

Ein Element $\tilde{\jmath} \in \mathrm{Alg}_K(L, M)$ ist ein Homomorphismus $L \to M$, der j erweitert. Durch Einschränkung ergibt sich ein Homomorphismus $j' : E \to M$, und dann kann $\tilde{\jmath}$ unter Verwendung von j' als Element von $\mathrm{Alg}_E(L, M)$ betrachtet werden.

Laut dem Forsetzungslemma gibt es höchstens $\mathrm{Grad}\, m_{\alpha/K}(X) = [E : K]$ Fortsetzungen von j zu j'. Nun ist $[L : E] < [L : K]$, also nach der Induktion ist $|\mathrm{Alg}_E(L, M)| \leq [L : E]$.

Also $|\mathrm{Alg}_K(L, M)| \leq [E : K] \cdot [L : E] = [L : K]$. □

Beispiel. (1) Betrachten Sie $\sqrt{2} \in \mathbb{C}$, mit Minimalpolynom $m(X) = X^2 - 2 \in \mathbb{Q}[X]$. Die Nullstellen sind $\pm\sqrt{2}$ und wir haben genau zwei Homomorphismen $\mathbb{Q}(\sqrt{2}) \to \mathbb{C}$, nämlich die Identität und σ mit $\sigma(\sqrt{2}) = -\sqrt{2}$.

Beide Homomorphismen induzieren Automorphismen von $\mathbb{Q}(\sqrt{2})$. Es folgt, dass $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

(2) Sei $\omega = \exp(2\pi i/3) = \frac{1}{2}(-1 + \sqrt{-3}) \in \mathbb{C}$. Das Minimalpolynom über $\mathbb{Q}$ ist $X^2 + X + 1$, mit Nullstellen ω und $\omega^2 = \bar{\omega}$. Es gibt also zwei Homomorphismen $\mathbb{Q}(\omega) \to \mathbb{C}$, nämlich die Identität und die komplexe Konjugation $\omega \mapsto \bar{\omega}$.

Beide Homomorphismen induzieren Automorphismen von $\mathbb{Q}(\omega)$. Es folgt, dass $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

(3) Sei $\alpha = \sqrt[3]{2} \in \mathbb{R}$. Das Minimalpolynom über $\mathbb{Q}$ ist $m(X) = X^3 - 2$. Dann ist α das einzige Nullstelle in $\mathbb{R}$, also $|\mathrm{Alg}(\mathbb{Q}(\alpha), \mathbb{R})| = 1$. Andererseits gibt es die drei Nullstellen $\alpha, \omega\alpha, \omega^2\alpha$ in $\mathbb{C}$, und wir bekommen drei Homomorphismen $\theta_r \colon \mathbb{Q}(\alpha) \to \mathbb{C}$, $\theta_r(\alpha) = \omega^r\alpha$, für $r = 0, 1, 2$.

Hier haben wir also, dass $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{\mathrm{id}\}$ und $\mathrm{Alg}(\mathbb{Q}(\alpha), \mathbb{C}) = \{\theta_0, \theta_1, \theta_2\}$.

(4) Sei $\beta = \sqrt[4]{2} \in \mathbb{R}$, sodass $\beta^2 = \sqrt{2}$, und betrachten Sie die Körpererweiterung $L/K/\mathbb{Q}$ mit $L = \mathbb{Q}(\beta)$ und $K = \mathbb{Q}(\beta^2)$. Es gibt also zwei Homomorphismen $K \to L$, $i \colon \sqrt{2} \mapsto \sqrt{2}$ und $j \colon \sqrt{2} \mapsto -\sqrt{2}$.

Das Minimalpolynom von β über K ist $m(X) = X^2 - \sqrt{2} \in K[X]$. Es gibt nun zwei Fortsetzungen von i zu einem Homomorphismus $L \to L$, nämlich $\beta \mapsto \pm\beta$, aber keine Fortsetzungen von j da $j(X^2 - \sqrt{2}) = X^2 + \sqrt{2}$ keine reellen Nullstellen hat.

Es folgt, dass $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(L/K) = \mathbb{Z}/2\mathbb{Z}$.

(5) Sei p eine Primzahl, $q = p^n$, und $\mathbb{F} = \mathbb{F}_q$. Der Primkörper von $\mathbb{F}$ ist $\mathbb{F}_p$.

Ich hätte in §5.5 klar sagen sollen, dass $a^q = a$ für alle $a \in \mathbb{F}$. Dies wurde im dortigen Beweis des Satzes gezeigt. Aber der Beweis ist leicht: die Gruppe $\mathbb{F}^\times$ hat die Ordnung $q - 1$, also $a^{q-1} = 1$ für alle $a \in \mathbb{F}^\times$, und daher ist $a^q = a$.

Der Frobeniusendomorphismus $\mathrm{Fr} : \mathbb{F} \to \mathbb{F}$, $a \mapsto a^p$ ist injektiv, also ein Automorphismus. Für alle $a \in \mathbb{F}_p$ gilt $a = a^p = \mathrm{Fr}(a)$. Daher ist $\mathrm{Fr} \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$.

Sei r die Ordnung des Frobeniusendomorphismus. Da $\alpha^q = \alpha$ für alle $\alpha \in \mathbb{F}$ folgt es, dass $\mathrm{Fr}^n = \mathrm{id}$, und daher is r ein Teiler von n. Umgekehrt gilt $\alpha = \mathrm{Fr}^r(\alpha) = \alpha^{p^r}$, also ist jedes $\alpha \in \mathbb{F}$ eine Nullstelle von $X^{p^r} - X$. Es folgt, dass $p^r \geq |\mathbb{F}|$ ist, also

$r \geq n$. Also $r = n$.

Wir haben also gezeigt, dass der Frobeniusendomorphismus $\mathrm{Fr} \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ die Ordnung n hat. Da auch $|\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)| \leq [\mathbb{F} : \mathbb{F}_p] = n$ ist, folgt es, dass $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ zyklisch ist, mit Fr als Erzeuger.

(6) Seien $\alpha = \sqrt[3]{2}$ und $\omega = e^{2\pi i/3}$. Dann ist $L = \mathbb{Q}(\alpha, \omega)$ ein Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$.

Sei $K = \mathbb{Q}(\alpha)$. Also $\mathbb{Q} \subseteq K \subseteq L$. Wir wissen, dass $[K : \mathbb{Q}] = 3$ und $[L : K] = 2$. Also $[L : \mathbb{Q}] = 6$.

Es gilt $m_{\alpha/\mathbb{Q}}(X) = X^3 - 2$. Die Nullstelle in $\mathbb{C}$ since α, $\omega\alpha$, $\omega^2\alpha$. Alle sind in L, gibt es also drei homomorphismen $j_k : K \to L$, $j_k(\alpha) = \omega^k\alpha$ $(k = 0, 1, 2)$.

Es gilt $m_{\omega/K}(X) = X^2 + X + 1$ und $j_k(m_{\omega/K}(X)) = X^2 + X + 1$. Die Nullstelle in $\mathbb{C}$ sind ω und ω^2. Beide sind in L, also gibt es zwei Fortsetzungen von j_k zu einem Homomorphismus $L = K(\omega) \to L$. Insgesamt gibt es 6 Elemente in $\mathrm{Gal}(L/\mathbb{Q})$:

$$\begin{array}{ccc}
\alpha \mapsto \alpha, & \omega \mapsto \omega, & \mathrm{Id} \\
\alpha \mapsto \alpha, & \omega \mapsto \omega^2, & \tau \\
\alpha \mapsto \omega\alpha, & \omega \mapsto \omega, & \sigma \\
\alpha \mapsto \omega\alpha, & \omega \mapsto \omega^2, & \tau\sigma^2 \\
\alpha \mapsto \omega^2\alpha, & \omega \mapsto \omega, & \sigma^2 \\
\alpha \mapsto \omega^2\alpha, & \omega \mapsto \omega^2, & \tau\sigma.
\end{array}$$

Das erste ist die Identität. Seien τ und σ die nächsten zwei Homomorphismen. Der Rest sind dann Kompositionen von τ und σ, z.B.

$$\tau\sigma^2(\alpha) = \tau\sigma(\omega\alpha) = \tau(\omega \cdot \omega\alpha) = \omega\alpha, \quad \tau\sigma^2(\omega) = \tau(\omega) = \omega^2.$$

Es gilt $\tau^2 = \sigma^2 = \mathrm{Id}$ und $\tau\sigma = \sigma^2\tau$, also

$$\mathrm{Gal}(L/\mathbb{Q}) \cong D_3 \cong S_3.$$

6.2 Galoiserweiterungen

Sei L ein Körper und $G \leq \mathrm{Aut}(L)$ eine Untergruppe. Wir definieren

$$L^G \coloneqq \{\alpha \in L : \sigma(\alpha) = \alpha \text{ für alle } \sigma \in G\}.$$

Nach §5.5 Lemma (2)(iii) ist L^G einen Teilkörper von L, der **Fixkörper** von G.

Definition. Eine **Galoiserweiterung** ist eine endliche Körpererweiterung L/K, für die $K = L^{\mathrm{Gal}(L/K)}$ gilt.

Satz (Lemma von Artin)**.** *Sei L ein Körper, $G \leq \mathrm{Aut}(L)$ eine endliche Gruppe, und $K \coloneqq L^G$ ihren Fixkörper. Dann gilt: L/K ist endlich, $[L : K] = |G|$, und $G = \mathrm{Gal}(L/K)$. Insbesondere ist L/K eine Galoiserweiterung.*

Beweis. Sei $G = \{\sigma_1, \ldots, \sigma_m\}$ und seien $x_1, \ldots, x_n \in L$ linear Unabhängig über K. Wir definieren die Matrix $M = (\sigma_i(x_j)) \in M_{m\times n}(L)$, und betrachten sie als eine L-lineare Abbildung $L^n \to L^m$. Falls $m < n$ ist, dann ist der Kern nicht trivial. Es gibt also ein Element $0 \neq \lambda = (\lambda_1, \ldots, \lambda_n) \in L^n$ mit

$$\sum_{j=1}^{n} \sigma_i(x_j)\lambda_j = 0 \quad \text{für alle } i.$$

Wir nehmen ein solches λ mit maximale Anzahl von Nulleinträge. Nach Umordnung der x_j und neu Skalierung, können wir annehmen, dass $\lambda_n = 1$. Sind jetzt alle $\lambda_j \in K$, dann gilt $\sigma_i(\sum_j \lambda_j x_j) = 0$, also $\sum_j \lambda_j x_j = 0$, einen Widerspruch. Nach Umordnung der x_j können wir also weiter annehmen, dass $\lambda_1 \notin K$. Da $L^G = K$ ist, gibt es nun $\sigma \in G$ mit $\sigma(\lambda_1) \neq \lambda_1$. Wir wenden σ auf die Gleichungen oben an, und bekommen

$$\sum_{j} (\sigma\sigma_i)(x_j)\sigma(\lambda_j) = 0 \quad \text{für alle } i.$$

Da $G = \{\sigma\sigma_1, \ldots, \sigma\sigma_m\}$ gilt nun, dass

$$\sum_{j} \sigma_i(x_j)\sigma(\lambda_j) = 0 \quad \text{für alle } i.$$

Durch Subtraktion der originalen Gleichungen bekommen wir

$$\sum_{j} \sigma_i(x_j)(\sigma(\lambda_j) - \lambda_j) = 0 \quad \text{für alle i.}$$

Für $j = 1$ gilt $\sigma(\lambda_1) - \lambda_1 \neq 0$, also ist $\mu \coloneqq \sigma(\lambda) - \lambda \in L^n$ ungleich Null und liegt im Kern. Ist $\lambda_j = 0$, dann ist $\mu_j = \sigma(\lambda_j) - \lambda_j = 0$, also μ hat mindestens genau so viele Nulleinträge. Schließlich für $j = n$ gilt $\lambda_1 = \sigma(\lambda_1) = 1$, also $\mu_n = 0$ und μ hat tatsäschlich mehrere Nulleinträge, einen Widerspruch.

Es folgt, dass $m \geq n$, also L/K ist endlich mit $[L : K] \leq |G|$. Nun ist es klar, dass $G \leq \mathrm{Gal}(L/K)$ eine Untergruppe ist, und laut dem Satz in §6.1 ist $|\mathrm{Gal}(L : K)| \leq [L : K]$. Wir sehen also, dass $[L : K] = |G|$ und $G = \mathrm{Gal}(L/K)$ sind. □

Das nächste Korollar sagt, dass eine Galoiserweiterung ist eine mit der maximal möglichen Anzahl von Symmetrien, oder äquivalent den kleinstmöglichen Fixkörper.

Korollar. *Sei L/K eine endliche Körpererweiterung. Dann:*

$$L/K \text{ ist eine Galoiserweiterung} \Leftrightarrow |\operatorname{Gal}(L/K)| = [L : K].$$

Beweis. Sei $G = \operatorname{Gal}(L/K)$. Nach §6.1 Satz ist $|G| \leq [L : K]$.

Angenommen, L/K ist eine Galoiserweiterung. Dann ist $K = L^G$. Dann gilt nach dem Satz $[L : K] = |G|$.

Umgekehrt sei $|G| = [L : K]$. Für $\alpha \in L \setminus K$ ist $\operatorname{Gal}(L/K(\alpha))$ eine Untergruppe von $\operatorname{Gal}(L/K)$, und laut dem Satz in §6.1 hat sie Ordnung höchstens $[L : K(\alpha)] < [L : K]$. Es folgt, dass es $\sigma \in \operatorname{Gal}(L/K)$ gibt mit $\sigma \notin \operatorname{Gal}(L/K(\alpha))$. Es muss gelten, dass $\sigma(\alpha) \neq \alpha$, also ist $\alpha \notin L^G$. Also $K = L^G$. Also ist L/K eine Galoiserweiterung. □

Beispiel. (1) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist Galois, mit Galoisgruppe $\mathbb{Z}/2\mathbb{Z}$.

(2) $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ ist Galois, mit Galoisgruppe S_3.

(3) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht Galois.

(4) Ist $q = p^n$ ein Primpotenz, dann ist $\mathbb{F}_q/\mathbb{F}_p$ eine Galoiserweiterung, mit Galoisgruppe $\mathbb{Z}/\mathbb{Z}n$.

Satz (Hauptsatz der Galoistheorie)**.** *Sei L/K eine Galoiserweiterung mit Galoisgruppe G. Die Abbildungen $H \mapsto L^H$ und $E \mapsto \operatorname{Gal}(L/E)$ ergeben inverse Bijektionen zwischen den Mengen der Untergruppen H von G und den Zwischenkörpern E mit $K \subseteq E \subseteq L$.*

Beweis. Sei $H \leq G$ eine Untergruppe, und $E = L^H$ ihre Fixkörper. Da G endlich ist, ist auch H endlich, und nach dem Lemma von Artin ist L/E Galois und $\operatorname{Gal}(L/E) = H$.

Umgekehrt sei E ein Zwischenkörper. Dann ist $\operatorname{Alg}_K(E, L)$ eine G-Menge durch Komposition, also $\sigma * \tau \coloneqq \sigma\tau$ für $\sigma \in G$ und $\tau \colon E \to L$. Sei $j \in \operatorname{Alg}_K(E, L)$ die Inklusionsabbildung. Die Stabilisator von j ist $\operatorname{Stab}_G(j) = \operatorname{Gal}(L/E)$. Nach der Bahnformel in §2.1 gibt es eine Bijektion

$$G/\operatorname{Stab}_G(j) \to Gj, \quad \sigma \operatorname{Stab}_G(j) \mapsto \sigma j$$

zwischen der Menge von Linksnebenklassen und der Bahn von j. Also

$$[G : \operatorname{Gal}(L/E)] = [G : \operatorname{Stab}_G(j)] = |Gj| \leq |\operatorname{Alg}_K(E, L)|.$$

Also

$$[L:K] = |G| = |\mathrm{Gal}(L/E)| \cdot [G : \mathrm{Gal}(L/E)] \leq |\mathrm{Gal}(L/E)| \cdot |\mathrm{Alg}_K(E,L)|$$

$$\leq [L:E] \cdot [E:K] = [L:K].$$

Es folgt, dass $|\mathrm{Gal}(L/E)| = [L:E]$. Also ist L/E Galois. Also $E = L^{\mathrm{Gal}(L/E)}$.

Bemerken Sie: Wir haben auch $Gj = \mathrm{Alg}_K(E,L)$, und daher eine Bijektion

$$G/\operatorname{Gal}(L/E) = G/\operatorname{Stab}_G(j) \to \mathrm{Alg}_K(E,L), \quad \sigma H \mapsto \sigma j = \sigma|_E.$$

□

Definition. Erinnerung (LA I, §1.3): Wenn S eine Menge ist, dann ist eine Relation $\leq$ auf S eine **Halbordnung** (englisch: partial order), wenn sie Folgendes erfüllt:

- $\leq$ ist reflexiv, das heißt $x \leq x$ für alle $x \in S$,

- $\leq$ ist transitiv, das heißt, $x \leq y$ und $y \leq z$ implizieren $x \leq z$

- $\leq$ ist antisymmetrisch, das heißt, $x \leq y$ und $y \leq x$ implizieren $x = y$.

Eine **halbgeordnete Menge** ist eine Menge zusammen mit einer Halbordnung.

Eine halbgeordnete Menge ist ein **Verband** (Englisch: lattice), wenn:

- Bei zwei beliebigen Elementen a, b gibt es ein Element $c = a \wedge b$, der **Durchschnitt** (englisch: meet), so dass $c \leq a, b$ und $x \leq a, b \Rightarrow x \leq c$. Also ist c das eindeutige größtes Element mit $c \leq a, b$.

- Bei zwei beliebigen Elementen a, b gibt es ein Element $d = a \vee b$, die **Vereinigung** (englisch: join), so $a, b \leq d$ und $a, b \leq x \Rightarrow d \leq x$. Also ist d das eindeutiges kleinstes Element mit $a, b \leq d$.

Beispiele. (i) Die Potenzmenge $\mathcal{P}(X)$ aller Teilmengen T einer Menge X ist ein Verband unter $\subseteq$. Der Durchschnitt ist $T \cap T'$. Die Vereinigung ist $T \cup T'$.

(ii) $\mathbb{R}$ ist ein Verband unter $\leq$. Der Durchschnitt ist $\min\{a, b\}$. Die Vereinigung ist $\max\{a, b\}$.

$\mathbb{Z} \times \mathbb{Z}$ ist ein Verband unter $(x, y) \leq (x', y') \Leftrightarrow x \leq x'$ und $y \leq y'$. Der Durchschnitt ist $(x, y) \wedge (x'y') = (\min\{x, x'\}, \min\{y, y'\})$. Die Vereinigung ist $(x, y) \vee (x'y') = (\max\{x, x'\}, \max\{y, y'\})$.

(iii) Die Menge der Untergruppe H von eine Gruppe G ist ein Verband unter $\leq$. Der Durchschnitt ist $H \cap H'$. Die Vereinigung ist $\langle H \cup H' \rangle$.

(iv) Sei L/K eine Körpererweiterung. Die Menge der Zwischenkörper E, d.h. $K \subseteq E \subseteq L$, ist ein Verband unter $\subseteq$. Der Durchschnitt ist $E \cap E'$. Die Vereinigung ist das **Körperkompositum** EE', der kleinste Teilkörper von L, der $E \cup E'$ enthält. z.B. $K(a_1, \ldots, a_n)K(b_1, \ldots, b_m) = K(a_1, \ldots, a_n, b_1, \ldots, b_m)$.

Satz (Galoiskorrespondenz)**.** *Sei L/K eine Galoiserweiterung mit Galoisgruppe G. Dann gilt:*

(1) Wenn H eine Untergruppe von G und E der entsprechende Zwischenkörper sind, dann ist L/E eine Galoiserweiterung mit der Galoisgruppe H, also $|H| = [L : E]$ und daher $[G : H] = [E : K]$. Es gibt eine Bijektion

$$G/H \to \mathrm{Alg}_K(E, L), \quad \sigma H \mapsto \sigma|_E.$$

(2) Wenn Untergruppen H, H' Zwischenkörper E, E' entsprechen, dann

$$H \leq H' \quad \Leftrightarrow \quad E \supseteq E'.$$

Das heißt, die Galois-Korrespondenz ist eine inklusions-umkehrende Bijektion zwischen halbgeorneten Mengen.

(3) Wenn Untergruppen H, H' Zwischenkörper E, E' entsprechen, dann entspricht die Untergruppe $H \cap H'$ dem Körperkompositum EE', und die Untergruppe $\langle H \cup H' \rangle$ entspricht dem Schnitt $E \cap E'$.

(4) Wenn H und E entsprechen, und $\sigma \in G$, dann entspricht die Untergruppe $\sigma H \sigma^{-1}$ dem Zwischenkörper $\sigma(E)$.

(5) Wenn H und E entsprechen, dann ist die Erweiterung E/K Galois genau dann, wenn $H \trianglelefteq G$ ein Normalteiler ist. In diesem Fall gilt $\mathrm{Gal}(E/K) = G/H$.

Beweis. (1) Die Aussagen werden im Beweis vom Hauptsatz der Galoistheorie gezeigt.

(2) Ist $H \leq H'$ und $\alpha \in E'$, dann gilt $\sigma(\alpha) = \alpha$ für alle $\sigma \in H$, also ist $\alpha \in E$. Umgekehrt ist $E' \subseteq E$ und $\sigma \in H$, dann gilt $\sigma(\alpha') = \alpha'$ für alle $\alpha' \in E'$, also ist $\sigma \in \mathrm{Gal}(L/E') = H'$.

(3) Wegen (2) muss der Durchschnitt und die Vereinigung entsprechen.

(4) Der zu $\sigma H \sigma^{-1}$ entsprechende Zwischenkörper ist

$$L^{\sigma H \sigma^{-1}} = \{a \in L : \sigma h \sigma^{-1}(a) = a \ \forall \ h \in H\}$$

$$= \{a \in L : \sigma^{-1}(a) \in L^H\} = \{a \in L : \sigma^{-1}(a) \in E\} = \sigma(E).$$

(5) Angenommen, $H \trianglelefteq G$. Nach (4) gilt: Wenn $\sigma \in G$, dann ist $\sigma(E) = E$. Somit ist $\sigma|_E \in \mathrm{Alg}_K(E, E) = \mathrm{Gal}(E/K)$. Die Abbildung

$$G \to \mathrm{Gal}(E/K), \quad \sigma \mapsto \sigma|_E$$

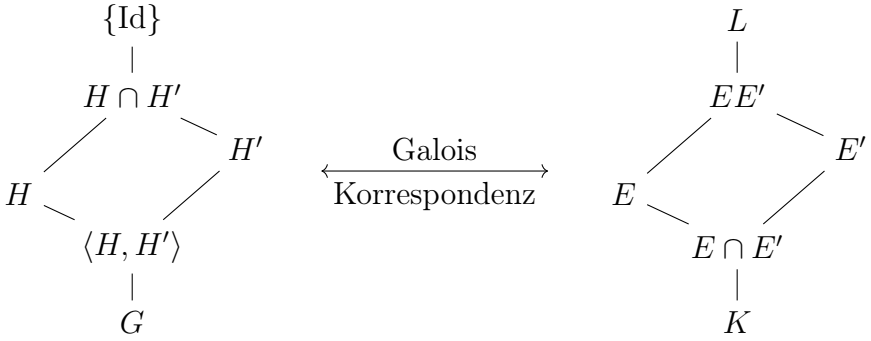
ist ein Gruppenhomomorphismus und der Kern ist $\mathrm{Gal}(L/E) = H$. Somit induziert sie einen injektiven Homomorphismus $\theta : G/H \to \mathrm{Gal}(E/K)$. Nach §6.1 Satz, gilt

$$|\mathrm{Gal}(E/K)| \leq [E : K] = [L : K]/[L : E] = |G|/|H| = |G/H|.$$

Wir müssen also Gleichheit haben, also ist E/K Galois gemäß der Korollar zu Artins Lemma, und θ ist ein Isomorphismus.

Umgekehrt sei E/K Galois. Wir haben eine injektive Abbildung $\mathrm{Gal}(E/K) \to \mathrm{Alg}_K(E, L)$, $\tau \mapsto j\tau$, wobei $j : E \to L$ die Inklusion ist. Beide Mengen haben die Mächtigkeit $[E : K]$, also ist sie bijektiv, und jeder $\theta : E \to L$ hat das Bild E. Das gilt insbesondere für jede $\sigma|_E$, wobei $\sigma \in G$ ist. Also $\sigma(E) = E$ für alle $\sigma \in G$. Nach (4) ist $\sigma H \sigma^{-1} = H$, und dadurch ist $H \trianglelefteq G$ einen Normalteiler. □

Das folgende Bild stellt Teil (3) diese Korrespondenz dar. Wir zeichnen das Diagramm der Untergruppen von G auf den Kopf.



Beispiel (Der Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$)**.** Sei $\alpha = \sqrt[3]{2}$ und $\omega = \exp(2\pi i/3)$. Die Nullstelle in $\mathbb{C}$ sind α, $\alpha\omega$, $\alpha\omega^2$. Wir haben gesehen, dass der Zerfällungskörper $L = \mathbb{Q}(\alpha, \omega)$ ist, und $[L : \mathbb{Q}] = 6$. Es gilt

$$\mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau : \sigma^3 = \tau^2 = \mathrm{Id}, \tau\sigma = \sigma^2\tau \rangle = D_3 \cong S_3,$$

wobei

$$\sigma(\alpha) = \omega\alpha, \quad \sigma(\omega) = \omega \qquad \text{und} \qquad \tau(\alpha) = \alpha, \quad \tau(\omega) = \omega^2.$$

Also ist $L/\mathbb{Q}$ Galois.

Die Untergruppen von D_3 sind D_3, $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\tau\sigma\rangle$, $\langle\tau\sigma^2\rangle$, und $\{\mathrm{id}\}$.

Die entsprechende Fixkörper sind $\mathbb{Q}$, $\mathbb{Q}(\omega)$, $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\omega^2\alpha)$, $\mathbb{Q}(\omega\alpha)$, und L.

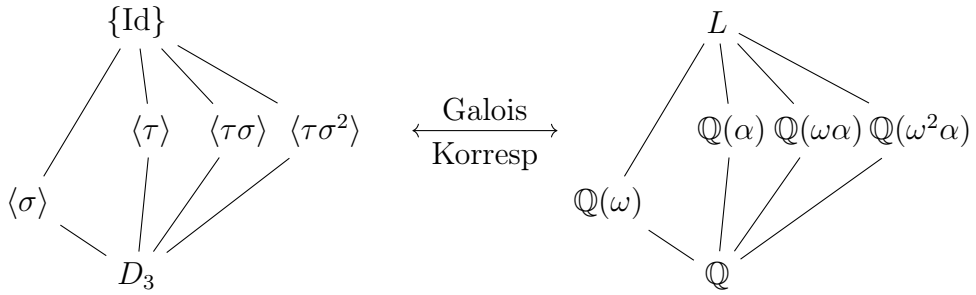
$L^{\langle\sigma\rangle}$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad $[S_3 : \langle\sigma\rangle] = 2$ und enthält ω, also ist es $\mathbb{Q}(\omega)$.

$L^{\langle\tau\rangle}$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad $[S_3 : \langle\tau\rangle] = 3$ und enthält α, also ist es $\mathbb{Q}(\alpha)$.

$L^{\langle\tau\sigma\rangle}$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad 3 und enthält $\omega\alpha$, also ist es $\mathbb{Q}(\omega\alpha)$.

$L^{\langle\tau\sigma^2\rangle}$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad 3 und enthält $\omega^2\alpha$, also ist es $\mathbb{Q}(\omega^2\alpha)$.

Die Galoiskorrespondenz ist also



Wir merken, dass $\langle\sigma\rangle$ einen Normalteiler von D_3 ist, und $\mathbb{Q}(\omega)/\mathbb{Q}$ ist Galois.

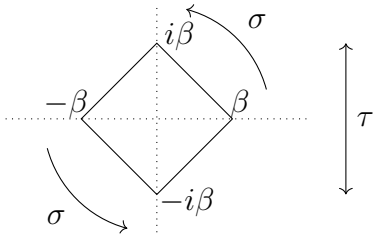
Beispiel (Der Zerfällungskörper von $X^4 - 2$ über $\mathbb{Q}$)**.** Sei $\beta = \sqrt[4]{2}$. Die Nullstellen von $X^2 - 2$ in $\mathbb{C}$ sind $\pm\beta, \pm i\beta$. Also ist der Zerfällungskörper $L = \mathbb{Q}(\beta, i)$ und $[L : \mathbb{Q}] = 8$.

Da $[\mathbb{Q}(i, \beta) : \mathbb{Q}(i)] = 4$ ist, ist das Minimalpolynom von β über $\mathbb{Q}(i)$ immer noch $X^4 - 2$.

Sei $j : \mathbb{Q}(i) \to L$ die Inklusion und $c \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ komplexe Konjugation. Es gilt $j(X^4-2) = jc(X^4-2) = X^4-2$ und dieses Polynom hat Nullstellen $\pm\beta, \pm i\beta$ in L. Das Fortsetzungslemma gibt also, dass Beide j und jc haben vier Erweiterungen in $\mathrm{Alg}_{\mathbb{Q}(i)}(L, L)$. Das gibt 8 Elemente von $\mathrm{Gal}(L/\mathbb{Q})$,

$$i \mapsto \pm i, \quad \beta \mapsto \pm\beta, \pm i\beta.$$

Nach §6.1 Satz gilt $|\operatorname{Gal}(L/\mathbb{Q})| \leq [L:\mathbb{Q}] = 8$. Daher besteht $\operatorname{Gal}(L/\mathbb{Q})$ aus diesen 8 Elementen und $L/\mathbb{Q}$ ist eine Galoiserweiterung. Jedes Element von $\operatorname{Gal}(L/\mathbb{Q})$ ergibt eine Symmetrie des Quadrats



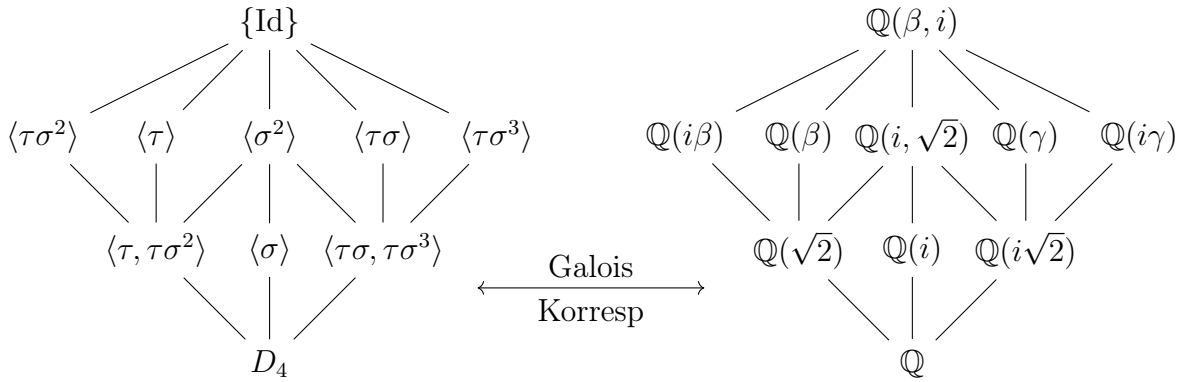
Also $\operatorname{Gal}(L/\mathbb{Q}) = D_4 = \langle \sigma, \tau \rangle$, wobei

$$\sigma(i) = i, \sigma(\beta) = i\beta, \quad \tau(i) = -i, \tau(\beta) = \beta,$$

also $\sigma^4 = \tau^2 = \mathrm{Id}$ und $\tau\sigma = \sigma^{-1}\tau$.

Die Untergruppen von D_4 sind D_4 selbst, die Drehgruppe $\langle \sigma \rangle$, die Untergruppen $\langle \tau, \tau\sigma^2 \rangle$, $\langle \tau\sigma, \tau\sigma^3 \rangle$, die von zwei Spiegelungen mit senkrechte Achsen erzeugt sind, die Untergruppen $\langle \tau \rangle$, $\langle \sigma^2 \rangle$, $\langle \tau\sigma \rangle$, $\langle \tau\sigma^3 \rangle$, die von einer Spiegelung erzeugt sind, die Untergruppe $\langle \sigma^2 \rangle$, die von eine Drehung durch π erzeugt ist, und $\{\mathrm{Id}\}$.

Die Korrespondenz ist:



Hier $\gamma = (1+i)/\beta$.

$L^{\langle \sigma \rangle}$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad 2 und enthält i, also ist es $\mathbb{Q}(i)$.

$L^{\langle \tau, \tau\sigma^2 \rangle}$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad 2 und enthält $\sqrt{2} = \beta^2$, also ist es $\mathbb{Q}(\sqrt{2})$.

$L^{\langle \tau\sigma, \tau\sigma^3 \rangle}$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad 2 und enthält $i\sqrt{2}$. Das Minimalpolynom ist $X^2 + 2$, also ist is $\mathbb{Q}(i\sqrt{2})$.

$L^{\langle \tau\sigma^2 \rangle}$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad 4 und enthält $i\beta$. Das minimale Polynom von $i\beta$ ist $X^4 - 2$, also ist es $\mathbb{Q}(i\beta) = \mathbb{Q}(\beta\zeta^2)$.

$L^{\langle \tau \rangle}$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad 4 und enthält β, also ist es $\mathbb{Q}(\beta)$.

$L^{\langle \sigma^2 \rangle}$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad 4 und enthält i und $\sqrt{2}$, also ist es $\mathbb{Q}(i, \sqrt{2})$.

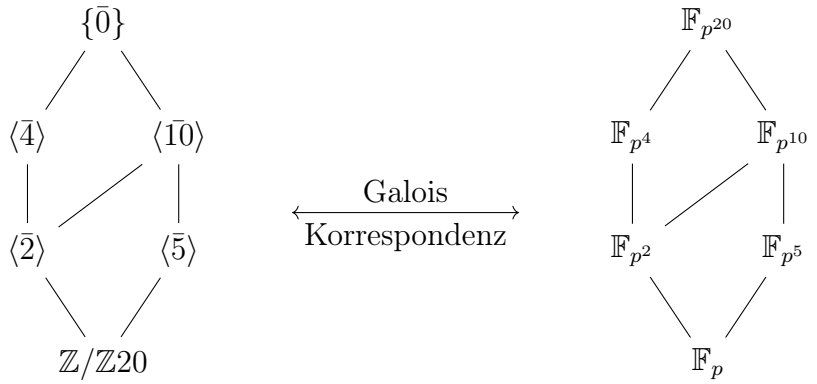
$L^{\langle \tau\sigma^3 \rangle}$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad 4 und enthält γ, das Minimalpolynom über $\mathbb{Q}$ ist $X^4 + 2$, also ist es $\mathbb{Q}(\gamma)$.

$L^{\langle \tau\sigma \rangle}$ ist eine Erweiterung von $\mathbb{Q}$ vom Grad 4 und enthält $i\gamma$, das Minimalpolynom ist $X^4 + 2$, also ist es $\mathbb{Q}(i\gamma)$.

Beispiel. Die Körpererweiterung $\mathbb{F}_{p^n}/\mathbb{F}_p$ ist Galois mit Galoisgruppe $\mathbb{Z}/\mathbb{Z}n$. Die Untergruppen von $\mathbb{Z}/\mathbb{Z}n$ sind $\langle \bar{m} \rangle$, so dass m ein Teiler von n ist, und

$$(\mathbb{F}_{p^n})^{\langle \bar{m} \rangle} = \{a \in \mathbb{F}_{p^n} : \mathrm{Fr}^m(a) = a\} = \{a \in \mathbb{F}_{p^n} : a^{p^m} = a\} \cong \mathbb{F}_{p^m}.$$

z.B.



6.3 Minimalpolynome für Elemente in Galoiserweiterungen

Lemma. *Sei L/K eine Galoiserweiterung mit Galoisgruppe G. Das Minimalpolynom von $\alpha \in L$ ist*

$$m_{\alpha/K}(X) = \prod_{\beta \in G\alpha} (X - \beta),$$

wobei $G\alpha = \{\sigma(\alpha) : \sigma \in G\}$ die Bahn von α ist.

Beweis. Sei $m(X) = \prod_{\beta \in G\alpha}(X - \beta) \in L[X]$. Für $\sigma \in G$ gilt $\{\sigma(\beta) \mid \beta \in G\alpha\} = G\alpha$, und dadurch auch

$$\sigma(m(X)) = \prod_{\beta}(X - \sigma(\beta)) = \prod_{\beta}(X - \beta) = m(X).$$

Es folgt, dass jede Koeffizient von $m(X)$ in $L^G = K$ liegt, also $m(X) \in K[X]$. Da α eine Nullstelle von $m(X)$ ist, muss nun $m(X)$ von das Minimalpolynom $m_{\alpha/K}(X)$ teilbar sein. Umgekehrt, ist $\beta \in G\alpha$, sagen wir $\beta = \sigma(\alpha)$ für ein $\sigma \in G$, dann gilt

$$m_{\alpha/K}(\beta) = m_{\alpha/K}(\sigma(\alpha)) = \sigma(m_{\alpha/K}(\alpha)) = 0,$$

also ist β eine Nullstelle von $m_{\alpha/K}(X)$, und $\operatorname{Grad} m_{\alpha/K}(X) \geq \operatorname{Grad} m(X)$. Da beide $m(X)$ und $m_{\alpha/K}(X)$ normiert sind, mussen sie jetzt gleich sind. □

Wir sehen, dass für eine Galoiserweiterung L/K und $\alpha \in L$, das Minimalpolynom von α zerfällt in L mit keine mehrfachen Nullstellen.

Definition. Eine endliche Körpererweiterung L/K ist **normal**, falls für jedes $\alpha \in L$, das Minimalpolynom $m_{\alpha/K}(X)$ zerfällt in L.

Äquivalent: Jedes irreduzible Polynom in $K[X]$, das eine Nullstelle in L hat, zerfällt in L.

Eine endliche Körpererweiterung L/K ist **separabel**, falls für jedes $\alpha \in L$, das Minimalpolynom $m_{\alpha/K}(X)$ hat keine mehrfachen Nullstellen in einem Zerfällungskörper.

Wir haben nun eine „interne Charakterisierung“ von Galoiserweiterungen.

Satz. *Eine Körpererweiterung L/K ist galois genau dann, wenn sie endlich, separabel und normal ist.*

Beweis. Ist L/K galois, dann ist sie endlich, und laut des vorherrigen Lemmas auch normal und separabel.

Umgekehrt sei L/K endlich, separabel und normal, mit Galoisgruppe G. Für jedes $\alpha \in L \setminus K$ finden wir $\sigma \in G$ mit $\sigma(\alpha) \neq \alpha$. Das zeigt, dass $L^G = K$ ist, also ist L/K galois.

Da L/K normal ist, zerfällt das Minimalpolynom $m_{\alpha/K}(X)$. Da $\operatorname{Grad} m_{\alpha/K}(X) \geq 2$ ist und $m_{\alpha/K}(X)$ keine mehrfachen Nullstellen hat, muss es eine Nullstelle $\alpha' \neq \alpha$ in L geben.

Nach dem Fortsetzungslemma, bekommen wir also einen Ringhomomorphismus $j : K(\alpha) \to L$ mit $j(\alpha) = \alpha'$ und $j|_K = \mathrm{id}$.

Sei E ein Zwischenkörper, der $K(\alpha)$ enthält, wobei $[E : K]$ so groß wie möglich ist, so dass es einen Homomorphismus $\sigma : E \to L$ gibt, der j erweitert.

Angenommen, $E \neq L$. Sei $\beta \in L \setminus E$. Nun ist $m_{\beta/E}(X)$ ein Teiler von $m_{\beta/K}(X)$ in $E[X]$, also ist $\sigma(m_{\beta/E}(X))$ ein Teiler von $\sigma(m_{\beta/K}(X)) = m_{\beta/K}(X)$. Da L/K normal ist, zerfällt $m_{\beta/K}(X)$, sodass $\sigma(m_{\beta/E}(X))$ eine Nullstelle $\beta' \in L$ hat.

Nach dem Fortsetzungslemma bekommen wir einen Ringhomomorphismus $\tilde{\sigma} : E(\beta) \to L$ mit $\tilde{\sigma}(\beta) = \beta'$ und $\tilde{\sigma}|_E = \sigma$. Somit ist $\tilde{\sigma}|_{K(\alpha)} = j$. Aber $[E(\beta) : K] > [E : K]$, ein Widerspruch.

Also $E = L$. Also $\sigma \in \mathrm{Gal}(L/K)$ und $\sigma(\alpha) = \alpha' \neq \alpha$. □

Wir untersuchen als nächstes die Eigenschaften normal und separabel genauer.

6.4 Normale Erweiterungen

In §5.4 sahen wir, dass ein Zerfällungskörper L für $f(X) \in K[X]$ über K existiert. Wir zeigen jetzt, dass zwei solche Zerfällungskörper isomorph sein muss.

Proposition. *Sei $j\colon K \to K'$ ein Isomorphismus und $f(X) \in K[X]$. Ist L ein Zerfällungskörper für $f(X)$ über K, und L' ein Zerfällungskörper für $j(f(X))$ über K', dann gibt es einen Isomorphismus $\tilde{j} : L \to L'$ mit $\tilde{j}|_K = j$.*

Beweis. Induktion über $n = [L : K]$. Wenn $n = 1$, dann zerfällt $f(X)$ in $K[X]$, also zerfällt $j(f(X))$ in K', also $L' = K'$, also j ist ein Isomorphismus $L \to L'$.

Nehmen wir also $n > 1$ an. Somit hat $f(X)$ eine Nullstelle $\alpha \in L \setminus K$. Dann ist $m_{\alpha/K}(X)$ ein Teiler von $f(X)$, also ist $j(m_{\alpha/K}(X))$ ein Teiler von $j(f(X))$. Somit gibt es eine Nullstelle α' von $j(m_{\alpha/K}(X))$ in L'. Nach dem Fortsetzungslemma gibt es also einen Homomorphismus $j' : K(\alpha) \to K'(\alpha')$ mit $j'(\alpha) = \alpha'$ und $j'|_K = j$. Offensichtlich ist j' ein Isomorphismus.

Nun ist L einen Zerfällungskörper von $f(X)$ über $K(\alpha)$, und L' einen Zerfällungskörper von $j'(f(X)) = j(f(X))$ über $K'(\alpha')$. Da $[L : K(\alpha)] < [L : K]$ ist, gibt es durch Induktion einen Isomorphismus $\tilde{j}$: $L \to L'$ mit $\tilde{j}|_{K(\alpha)} = j'$, also $\tilde{j}|_K = j$. □

Wir haben nun den überraschenden Satz, dass jeder Zerfällungskörper normal ist.

Satz. *Sei L/K eine endliche Erweiterung. Dann ist L/K normal genau dann, wenn L ein Zerfällungskörper eines Polynoms über K ist.*

Beweis. Sei L/K endlich und normal und sei $L = K(\alpha_1, \ldots, \alpha_n)$ (zum Beispiel sei $\alpha_1, \ldots, \alpha_n$ eine K-Basis von L). Dann ist L auch ein Zerfällungskörper von $f(X) = \prod_{i=1}^{n} m_{\alpha_i/K}(X)$ über K.

Umgekehrt sei L ein Zerfällungskörper von $f(X)$ über K und sei $\alpha \in L \setminus K$.

Sei β eine Nullstelle von $m_{\alpha/K}(X)$ in einem Zerfällungskörper M von $m_{\alpha/K}(X)$ über L. Nach dem Fortsetzungslemma gibt es einen Homomorphismus $j : K(\alpha) \to K(\beta)$ mit $j(\alpha) = \beta$ und $j|_K$ die Inklusion von K in $K(\beta)$. Also j ein Isomorphismus.

L ist ein Zerfällungskörper von $f(X)$ über $K(\alpha)$, weil L ein Zerfällungskörper von $f(X)$ über K und $\alpha \in L$ sind.

$L(\beta)$ ist ein Zerfällungskörper von $f(X) = j(f(X))$ über $K(\beta)$, weil $f(X)$ über $L(\beta)$ zerfällt, und falls $f(X)$ über L' zerfällt, wobei $K(\beta) \subseteq L' \subseteq L(\beta)$, dann muss $L \subseteq L'$, also $L' = L(\beta)$.

Nach der Proposition, gibt es einen Isomorphismus $\tilde{j} : L \to L(\beta)$ mit $\tilde{j}|_{K(\alpha)} = j$. Es folgt, dass $[L : K] = [L(\beta) : K]$, also $L(\beta) = L$, also $\beta \in L$. Also zerfällt das Minimalpolynom $m_{\alpha/K}(X)$ in L. □

Definition. Sei L/K endlich. Eine **normale Hülle** von L/K ist eine Erweiterung M/L, sodass M/K normal ist, und minimal bezüglich diese Eigenschaften: $L \subseteq M' \subseteq M$ und M'/K normal impliziert $M' = M$.

Proposition. *Jede endliche Erweiterung L/K hat eine normale Hülle. Insbesondere, wenn $L = K(\alpha_1, \ldots, \alpha_n)$, dann ist der Zerfällungskörper M von $f(X) = \prod_{i=1}^{n} m_{\alpha_i/K}(X)$ über L eine normale Hülle von L/K.*

Beweis. $f(X)$ zerfällt über M, und wenn es über E zerfällt, mit $K \subseteq E \subseteq M$, dann ist jedes $\alpha_i \in E$, also $L \subseteq E$, also $E = M$ nach der Minimalität von M. Somit ist M ein Zerfällungskörper von $f(X)$ über K. Somit ist M/K nach dem Satz normal.

Angenommen, $L \subseteq M' \subseteq M$ und M'/K ist normal. Da jedes $\alpha_i \in M'$ liegt, zerfällt $f(X)$ über M'. Nach der Minimalität von M ist $M' = M$. □

6.5 Separable Erweiterungen

Sei R ein kommutativer Ring. Die (formale) **Ableitung** eines Polynoms $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in R[X]$ ist

$$f'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

Sie erfüllt die üblichen Regeln

$$(\lambda f + \mu g)'(X) = \lambda f'(X) + \mu g'(X), \quad (fg)'(X) = f'(X)g(X) + f(X)g'(X)$$

für alle $\lambda, \mu \in R$ und $f(X), g(X) \in R[X]$.

Sei nun K ein Körper. Ein Polynom $f(X) \in K[X]$ heißt **separabel**, falls es keine mehfachen Nullstellen in einem Zerfällungskörper hat.

Proposition. *Sei K ein Körper und $f(X) \in K[X]$ irreduzibel. Die Folgenden sind äquivalent:*

(1) $f(X)$ ist nicht separabel.

(2) $f(X)$ und $f'(X)$ sind nicht teilerfremd.

(3) $f'(X) = 0$.

(4) $\operatorname{Char} K = p > 0$ und $f(X) = g(X^p)$ für ein Polynom $g(X) \in K[X]$.

Insbesondere wenn $\operatorname{Char} K = 0$, dann ist jedes irreduzible Polynom separabel.

Beweis. (1)⇒(2). Falls $f(X)$ und $f'(X)$ teilerfremd sind, gibt es $p(X), q(X) \in K[X]$, so dass $p(X)f(X) + q(X)f'(X) = 1$. Sei L/K ein Zerfällungskörper von $f(X)$ und $\alpha \in L$ eine mehrfache Nullstelle von $f(X)$. Also $f(X) = (X - \alpha)^2 g(X)$ in $L[X]$. Dann ist α auch eine Nullstelle von $f'(X) = 2(X-\alpha)g(X)+(X-\alpha)^2g'(X)$, also eine Nullstelle von 1. Widerspruch.

(2)⇒(3). Das Polynom $g(X) = \mathrm{ggT}(f(X), f'(X))$ ist nicht konstant und teilt $f(X)$. Da $f(X)$ irreduzibel ist, ist $f(X) = ag(X)$ mit $a \in R^\times$. Dann ist $f(X)$ ein Teiler von $f'(X)$. Aber $\mathrm{Grad}(f'(X)) < \mathrm{Grad}\, f(X)$, also muss $f'(X) = 0$ sein.

(3)⇒(4). Schreiben Sie $f(X) = a_0 + a_1X + \cdots + a_nX^n$. Dann ist $0 = f'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}$, also $ia_i = 0$ für alle i. Ist $\mathrm{Char}\, K = 0$, dann ist $a_i = 0$ für alle $i > 0$, also ist $f(X) = a_0$ konstant, ein Widerspruch. Also muss $\mathrm{Char}\, K = p > 0$ sein, und $f(X) = a_0 + a_pX^p + a_{2p}X^{2p} + \cdots = g(X^p)$, wobei $g(X) = a_0 + a_pX + a_{2p}X^2 + \ldots$.

(4)⇒(1). Sei L/K ein Zerfällungskörper von $f(X)$, und $\alpha \in L$ eine Nullstelle von $f(X)$. Dann gilt $g(\alpha^p) = f(\alpha) = 0$, also ist α^p eine Nullstelle von $g(X)$. Schreiben Sie $g(X) = (X - \alpha^p)h(X)$ in $L[X]$. Dann gilt

$$f(X) = g(X^p) = (X^p - \alpha^p)h(X^p) = (X - \alpha)^p h(X^p)$$

in $L[X]$. Also ist α eine mehrfache Nullstelle von $f(X)$. □

Per Definition ist eine endliche Körpererweiterung L/K genau dann separierbar, wenn $m_{\alpha/K}(X)$ für alle $\alpha \in L$ separabel ist. Nach der Proposition ist jede endliche Körpererweiterung L/K separierbar, wenn $\mathrm{Char}\, K = 0$.

Satz. *Sei L/K eine endliche Körpererweiterung. Die Folgenden sind äquivalent.*

(1) L/K ist separabel.

(2) $L = K(\alpha_1, \ldots, \alpha_n)$, wobei jedes $m_{\alpha_i/K}(X)$ separabel ist.

(3) $|\mathrm{Alg}_K(L, M)| = [L : K]$ für jede Erweiterung M/L, so dass M/K normal ist.

Beweis. (1)⇒(2). Klar, z.B. $\alpha_1, \ldots, \alpha_n$ eine K-Basis von L.

(2)⇒(3). Angenommen, $|\mathrm{Alg}_K(E, M)| = [E : K]$, wobei $E = K(\alpha_1, \ldots, \alpha_{i-1})$. Sei $j \in \mathrm{Alg}_K(E, M)$. Nun ist $m_{\alpha_i/E}(X)$ ein Teiler von $m_{\alpha_i/K}(X)$, also ist $j(m_{\alpha_i/E}(X))$ ein Teiler von $j(m_{\alpha_i/K}(X)) = m_{\alpha/K}(X)$. Somit zerfällt $j(m_{\alpha_i/E}(X))$ in M ohne mehrfachen Nullstellen. Nach dem Fortsetzungslemma gibt es $\mathrm{Grad}\, m_{\alpha_i/E}(X)$ Fortsetzungen von j in $\mathrm{Alg}_K(E(\alpha_i), M)$. Daher gilt

$$|\mathrm{Alg}_K(K(\alpha_1, \ldots, \alpha_i), M)| = |\mathrm{Alg}_K(E(\alpha_i), M)| = |\mathrm{Alg}_K(E, M)| \cdot \mathrm{Grad}\, m_{\alpha_i/E}(X)$$

$$= [E : K] \cdot [E(\alpha) : E] = [E(\alpha) : K] = [K(\alpha_1, \ldots, \alpha_i) : K].$$

Durch Induktion gilt dies für $i = n$.

(3)⇒(1). Sei M/L eine normale Hülle von L/K und $\alpha \in L$. Ist $m_{\alpha/K}(X)$ nicht separabel, dann hat es weniger als $[K(\alpha) : K]$ verschiedene Nullstellen in M, also gilt $|\mathrm{Alg}_K(K(\alpha), M)| < [K(\alpha), K]$. Für jeden Homomorphismus $j : K(\alpha) \to M$ gibt es höchstens $[L : K(\alpha)]$ Fortsetzungen zu einem Homomorphismus $L \to M$, also gilt

$$|\mathrm{Alg}_K(L, M)| < [L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K],$$

□

Korollar. *Eine Körpererweiterung L/K ist genau dann galois, wenn sie der Zerfällungskörper eines Produkts separabler irreduzibler Polynome über K ist.*

Beweis. Nach §6.4 Satz können wir annehmen, dass L der Zerfällungskörper eines Polynoms $f(X)$ ist. Also ist $L = K(\alpha_1, \ldots, \alpha_n)$, wobei die α_i die Nullstellen von $f(X)$ sind. Die irreduziblen Faktoren von $f(X)$ sind die Minimalpolynome von den α_i, also sind sie nach dem Satz genau dann separabel, wenn L/K separabel ist. □

Lemma (1)**.** *Sei L/K der Zerfällungskörper eines Polynoms $f(X) \in K[X]$.*

(i) $\mathrm{Gal}(L/K)$ *operiert auf der Menge $\{\alpha_1, \ldots, \alpha_n\}$ von Nullstellen von $f(X)$ mit entsprechendem Gruppenhomomorphismus $\rho : G \to S_n$, $\sigma(\alpha_i) = \alpha_{\rho(\sigma)(i)}$.*

(ii) die Aktion ist treu, d.h. ρ ist injektive, und

(iii) Falls $f(X)$ irreduzibel und separabel ist, ist die Aktion transitiv, d.h. für jede i, j gibt es $\sigma \in G$ mit $\sigma(\alpha_i) = \alpha_j$, also $\rho(\sigma)(i) = j$.

Beweis. (i) Wenn $\sigma \in \mathrm{Gal}(L/K)$, gilt

$$f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = \sigma(0) = 0$$

also $\sigma(\alpha_i) = \alpha_j$ für ein j.

(ii) Ist $\rho(\sigma) = \mathrm{Id}$, dann gilt $\sigma(\alpha_i) = \alpha_i$ für alle i. Nach §5.5 Lemma (2)(iii) ist $\{a \in L : \sigma(a) = a\}$ ein Teilkörper von L und enthält $K \cup \{\alpha_1, \ldots, \alpha_n\}$ also ist alles von L, also $\sigma = \mathrm{Id}$.

(iii) Bis auf einen Skalar ist $f(X)$ das Minimalpolynom von α_i, und nach §6.3 Lemma ist die Menge der Nullstellen von $f(X)$ genau die Bahn $G\alpha_i$. □

Proposition. *Sei p eine Primzahl und $f(X) \in \mathbb{Q}[X]$ irreduzibel der Grad p. Seien $L/\mathbb{Q}$ der Zerfällungskörper von $f(X)$ und G die Galoisgruppe. Hat $f(X)$ genau zwei nicht reele Nullstellen, dann ist $\rho : G \to S_p$ ein Isomorphismus.*

z.B. $p = 5$ und $f(X) = X^5 - 6X + 3$.

Beweis. Weil $\operatorname{Char} \mathbb{Q} = 0$, ist $f(X)$ separabel, also hat es p Nullstellen in L. Also $\rho : G \to S_p$. Die Aktion von G auf der Menge von Nullstellen ist transitiv, also gibt die Bahnformel

$$p = |G\alpha_1| = [G : \operatorname{Stab}_G(\alpha_1)],$$

also ist p ein Teiler von $|G|$. Nach dem Satz von Cauchy enthält G also ein Element der Ordnung p, also muss $\rho(\sigma)$ ein p-Zyklus sein.

Komplexe Konjugation liefert ein Element $\tau \in G$, sodass $\rho(\tau)$ eine Transposition ist.

Wenn wir die Nullstellen umbenennen und eine Potenz des p-Zyklus berücksichtigen, können wir annehmen, dass $(1\ 2\ \ldots\ p), (1\ 2) \in \text{Bild}(\rho)$. Dann ist ρ nach dem nächsten Lemma ein Isomorphismus. □

Lemma (2)**.** $S_n = \langle (1\ 2\ \ldots\ n), (1\ 2) \rangle$.

Beweis. Seien $c = (1\ 2\ \ldots\ n)$, $t = (1\ 2)$ und $H = \langle c, t \rangle$. Für $1 \leq i < n$ gilt

$$(i\ i+1) = c^{i-1} t c^{-(i-1)} \in H,$$

und für $1 \leq i < j \leq n$ gilt

$$(i\ j) = (i\ i+1) \ldots (j-2\ j-1)(j-1\ j)(j-2\ j-1) \ldots (i\ i+1) \in H.$$

Dann gilt $H = S_n$, weil jede Permutation ein Produkt von Transpositionen ist. □

6.6 Auflösbarkeit von Gleichungen durch Radikale

In diesem Abschnitt ist $\operatorname{Char} K = 0$, also endliche Erweiterungen sind separabel und endliche normale Erweiterungen sind galois.

Definition. Eine Körpererweiterung L/K ist **radikal**, wenn $L = K(\alpha_1, \ldots, \alpha_n)$, $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ für alle i, und $n_i > 0$.

Lemma. *Wenn L/K radikal ist, dann gibt es eine normale Hülle M/L mit M/K radikal.*

Beweis. Der Zerfällungskörper M von $\prod_i m_{\alpha_i/K}(X)$ über L ist eine normale Hülle von L/K. Seien β_{ij} die Nullstellen von $m_{\alpha_i/K}(X)$. Dann ist $E_i = K(\beta_{ij} : j)$ ein Zerfällungskörper von $m_{\alpha_i/K}(X)$ über K, also ist E_i/K galois. Nach §6.5 Lemma(1)(iii) gibt es $\tau_{ij} \in \mathrm{Gal}(E_i/K)$ mit $\tau_{ij}(\alpha_i) = \beta_{ij}$. Nach der Galois-Korrespondenz erweitern sich die τ_{ij} auf Elemente $\sigma_{ij} \in \mathrm{Gal}(M/K)$. Es gilt

$$M = K(\beta_{ij} : i, j) = K(\sigma_{ij}(\alpha_i) : i, j) = K(\sigma_{ij}(\alpha_k) : i, j, k)$$

und

$$\sigma_{ij}(\alpha_k)^{n_k} = \sigma_{ij}(\alpha_k^{n_k}) \in \sigma_{ij}(K(\alpha_1, \ldots, \alpha_{k-1})) = K(\sigma_{ij}(\alpha_1), \ldots, \sigma_{ij}(\alpha_{k-1})),$$

also ist M/K radikal. □

Satz. *Wenn L/K normal und radikal ist, dann ist* $\mathrm{Gal}(L/K)$ *auflösbar (Sehen Sie Aufgabe 5.4.)*

Beweis. Bei der Definition einer radikale Erweiterung können wir davon ausgehen, dass die n_i Primzahlen sind und $\alpha_i \notin E_i := K(\alpha_i^{n_i})$. Da L/K galois ist, ist L/E_i galois. Weil $\alpha_i \notin E_i$, hat das Polynom $m_{\alpha_i/E_i}(X)$ den Grad > 1, also hat es eine andere Nullstelle α_i' in L. Dann ist $(\alpha_i')^{n_i} = \alpha_i^{n_i}$, da $m_{\alpha_i/E_i}(X)$ ein Teiler von $X^{n_i} - \alpha_i^{n_i}$ ist. Also ist $\epsilon_i = \alpha_i'/\alpha_i$ eine primitive n_i Einheitswurzel.

Sei $K_i = K($die ersten i der Elemente $\epsilon_1, \alpha_1, \epsilon_2, \alpha_2, \ldots, \epsilon_n, \alpha_n)$. Dann

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{2n} = L,$$

also

$$\mathrm{Gal}(L/K) = \mathrm{Gal}(L/K_0) \geq \mathrm{Gal}(L/K_1) \geq \cdots \geq \mathrm{Gal}(L/K_{2n}) = \{\mathrm{Id}\}.$$

Wir behaupten, dass K_i/K_{i-1} Galois ist, also $\mathrm{Gal}(L/K_i) \trianglelefteq \mathrm{Gal}(L/K_{i-1})$, und

$$\mathrm{Gal}(L/K_{i-1})/\mathrm{Gal}(L/K_i) \cong \mathrm{Gal}(K_i/K_{i-1}),$$

und wir behaupten, dass diese Gruppe abelsch ist. Somit ist $\mathrm{Gal}(L/K)$ auflösbar.

Wenn i ungerade ist, sagen wir $i = 2j - 1$, dann ist $K_i = K_{i-1}(\epsilon_j)$. Es ist ein Zerfällungskörper von $X^{n_j} - 1 = \prod_{k=0}^{n_j-1}(X - \epsilon_j^k)$ über K_{i-1}, also ist K_i/K_{i-1} galois. Jedes Element von $\mathrm{Gal}(K_i/K_{i-1})$ hat die Form $\sigma_k(\epsilon_j) = \epsilon_j^k$ für ein k, und $\sigma_k\sigma_{k'}(\epsilon_j) = \epsilon_j^{kk'}$, also ist $\mathrm{Gal}(K_i/K_{i-1})$ abelsch.

Wenn i gerade ist, sagen wir $i = 2j$, dann ist $\epsilon_j \in K_{i-1}$ und $K_i = K_{i-1}(\alpha_j)$. Es ist ein Zerfällungskörper von $X^{n_j} - \alpha_j^{n_j} = \prod_{k=0}^{n_j-1}(X - \epsilon_j^k\alpha_j)$ über K_{i-1}. Jedes Element von $\mathrm{Gal}(K_i/K_{i-1})$ hat die Form $\sigma_k(\alpha_j) = \epsilon_j^k\alpha_j$ für ein k, und $\sigma_k\sigma_{k'}(\alpha_j) = \epsilon_j^{k+k'}\alpha_j$, also ist $\mathrm{Gal}(K_i/K_{i-1})$ abelsch. □

Korollar. *Das Polynom $f(X) = X^5 - 6X + 3$ ist durch Radikale nicht lösbar. Das heißt, es gibt keine radikale Erweiterung $L/\mathbb{Q}$, die eine Nullstelle von $f(X)$ enthält.*

Beweis. Wir können annehmen, dass $L/\mathbb{Q}$ normal ist, und da es dann eine Nullstelle von $f(X)$ enthält, enthält es einen Zerfällugskörper E von $f(X)$. Dann ist $\mathrm{Gal}(E/\mathbb{Q})$ ein Quotient von $\mathrm{Gal}(L/\mathbb{Q})$, also auflösbar. Die Gruppe A_5 ist einfach und nichtabelsch, also nicht auflösbar, und A_5 ist eine Untergruppe von S_5, also ist S_5 nicht auflösbar. Aber $\mathrm{Gal}(E/\mathbb{Q}) \cong S_5$. Widerspruch. □

Daraus folgt, dass es keine Formel für die Nullstellen eines allgemeinen Polynoms vom Grad 5 in Form von Radikalen gibt, ähnlich der Formel für ein quadratisches Polynom.

Mit mehr Arbeit kann man auch zeigen, dass, wenn die Galoisgruppe des Zerfällungskörpers eines Polynoms auflösbar ist, die Nullstellen in Form von Radikalen geschrieben werden können. Insbesondere ist der Zerfällungskörper des Polynoms $ax^4 + bx^3 + cx^2 + dx + e$ über $\mathbb{Q}(a, b, c, d, e)$ isomorph zu einer Untergruppe von S_4, also auflösbar (weil $\{\mathrm{Id}\} \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4$), also gibt es eine Formel für die Nullstellen eines allgemeinen Polynoms vom Grad 4. Sehen Sie, z.B.

`https://de.wikipedia.org/wiki/Quartische_Gleichung`