Algebra

Hamburg
Vorlesung im Wintersemester 24/25
Tobias Dyckerhoff

Letztes Update: 13. März 2025, 01:54Uhr

Inhaltsverzeichnis

Kapitel 1

Gruppen und Symmetrie

1.1 Die Definition einer Gruppe

Definition 1.1.1. Eine *Gruppe* ist ein Paar $(G, \circ)$ bestehend aus einer Menge G und einer Abbildung

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

mit den folgenden Eigenschaften:

(G1) Für alle $g_1, g_2, g_3 \in G$ gilt: $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$

(G2) Es gibt ein Element $e \in G$, so dass gelten:

- (G2.1) Für jedes $g \in G$ gilt $e \circ g = g$.
- (G2.2) Für jedes $g \in G$ existiert $g' \in G$, so dass $g' \circ g = e$.

Dabei verwenden wir folgende Terminologie: Die Abbildung $\circ$ heißt *Verknüpfung*, ein Element e mit den aufgeführten Eigenschaften heißt *neutrales Element*, und ein Element g' zu gegebenem $g \in G$ heißt *Inverses von* g.

Aufgabe 1.1.2. Sei $(G, \circ)$ eine Gruppe. Beweise die folgenden Aussagen:

(1) Das neutrale Element e ist eindeutig bestimmt und hat zudem die Eigenschaft: Für jedes $g \in G$ gilt $e \circ g = g$.

(2) Zu gegebenem $g \in G$ ist das Inverse $g' \in G$ eindeutig bestimmt und erfüllt zudem $g \circ g' = e$.

(3) Für $n \geq 3$, hängt das Produkt von Gruppenelementen $g_1, g_2, ..., g_n \in G$ nicht von der gewählten Klammerung ab.

Beispiele 1.1.3. (1) Die Gruppe $(\mathbb{Z}, +)$ der ganzen Zahlen mit Addition bildet eine Gruppe.

(2) Für jeden Körper K existiert die additive Gruppe $(K, +)$ und die multiplikative Gruppe $(K^*, \cdot)$, wobei $K^* := K \setminus \{0\}$.

(3) Für jede Menge M definiert man die symmetrische Gruppe $(S_M, \circ)$, wobei S_M die Menge der bijektiven Selbstabbildungen ist und $\circ$ die Kompositionsabbildung. Zudem legen wir auch die Notation

$$S_n := S_{\{1,2,...,n\}}$$

fest.

(4) Für $n \geq 1$ und jeden Körper K definieren wir die allgemeine lineare Gruppe $(\mathrm{GL}(n, K), \circ)$, wobei

$$\mathrm{GL}(n, K) := \{A \in K^{n \times n} \mid \det(A) \neq 0\}$$

die Menge der invertierbaren $n \times n$ Matrizen mit Einträgen in K und $\circ$ die Matrixmultiplikation bezeichnet.

Um uns die alltägliche Arbeit mit Gruppen zu erleichtern, verwenden wir üblicherweise folgende Konventionen:

(1) Wir bezeichnen eine Gruppe $(G, \circ)$ oft einfach mit G und lassen die Verknüpfung implizit.

(2) Für $g, h \in G$ schreiben wir gh statt $g \circ h$, schreiben 1 für das neutrale Element e, und schliesslich g^{-1} für das Inverse.

(3) Falls für alle $g, h \in G$ gilt: $gh = hg$, dann heißt die Gruppe *abelsch*. Um diese Eigenschaft implizit hervorzuheben, verwenden wir für abelsche Gruppen oft das Additionssymbol $+$ für die Verknüpfung, 0 für das neutrale Element, sowie $-g$ für das Inverse eines Elements $g \in G$.

(4) Nach Aufgabe 1.1.2 hängt das Produkt von Elementen $g_1, g_2, ..., g_n \in G$ nicht von der Klammerung ab, daher lassen wir die Klammern oft weg.

(5) Für eine Gruppe G, bezeichnen wir die Kardinalität

$$|G| \in \mathbb{N} \cup \{\infty\}$$

als die *Ordnung von* G.

Beispiel 1.1.4. Wir definieren die *Quaternionengruppe*

$$Q_8 := \{\pm 1, \pm i, \pm j, \pm k\}$$

mit komplexen Einheiten i, j und k, wobei die zusätzliche Relation $i^2 = j^2 = k^2 = ijk = -1$ die Verknüpfungstafel eindeutig bestimmt. Daraus lässt sich leicht ableiten, dass z.B. $ij = -ji$ gilt, Q_8 ist also ein Beispiel für eine nicht-abelsche Gruppe.

1.2 Untergruppen

Definition 1.2.1. Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt *Untergruppe von* $(G, \circ)$, falls gelten

(U1) $H \neq \emptyset$,

(U2) für alle $a, b \in H$ gilt: $ab^{-1} \in H$.

Wir verwenden die Notation $H \leq G$, um Untergruppen zu kennzeichnen.

Proposition 1.2.2. *Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ ist genau dann eine Untergruppe von $(G, \circ)$, wenn die folgenden Bedingungen gelten:*

(U1') $1 \in H$,

(U2') *für alle* $a, b \in H$ *gilt* $ab \in H$,

(U3') *für alle* $a \in H$ *gilt* $a^{-1} \in H$.

Beweis. Falls (U1'),(U2'), und (U3') erfüllt sind, dann ist klar, dass (U1) und (U2) gelten, so dass $H \leq G$ eine Untergruppe ist. Nehmen wir umgekehrt an, dass (U1) und (U2) gelten. Dann existiert wegen (U1) ein Element $a \in H$. Wegen (U2) ist damit

$$1 = aa^{-1} \in H$$

also gilt (U1'). Für gegebenes $a \in H$ gilt, wiederum wegen (U2), für das Inverse

$$a^{-1} = 1a^{-1} \in H,$$

so dass also (U2') gilt. Schliesslich gilt damit auch (U3'), denn für $a, b \in H$ gilt zunächst $b^{-1} \in H$ und dann auch

$$ab = a(b^{-1})^{-1} \in H.$$

□

Korollar 1.2.3. *Sei $(G, \circ)$ eine Gruppe und $H \leq G$ eine Untergruppe von $(G, \circ)$. Dann definiert die eingeschränkte Verknüpfung*

$$\circ_{|H\times H} : H \times H \to H$$

eine Gruppe $(H, \circ_{|H\times H})$

Beweis. Dies ist eine direkte Konsequenz der Charakterisierung der Untergruppeneigenschaft durch die Bedingungen (U1'),(U2'), und (U3') in Proposition 1.2.2. □

Beispiele 1.2.4. (1) Die Teilmenge $\mathbb{Z} \subseteq \mathbb{R}$ ist eine Untergruppe von $(\mathbb{R}, +)$.

(2) Für $n \geq 1$ und einen Körper K definieren die folgenden Teilmengen Untergruppen von $(\mathrm{GL}(n, K), \circ)$:

(a) $\mathrm{SL}(n, K) := \{A \in \mathrm{GL}(n, K) \mid \det(A) = 1\} \leq \mathrm{GL}(n, K)$, genannt *spezielle lineare Gruppe*,

(b) $\mathrm{O}(n, K) := \{A \in \mathrm{GL}(n, K) \mid A^T A = I_n\} \leq \mathrm{GL}(n, K)$, genannt *orthogonale Gruppe*.

(3) Sei G eine Gruppe und $\{H_i\}_{i\in I}$ eine Familie von Untergruppen $H_i \leq G$, indiziert durch die (möglicherweise unendliche) Indexmenge I. Dann ist

$$\bigcap_{i\in I} H_i \leq G$$

eine Untergruppe.

(4) Für $n \geq 1$ und K Körper, ist

$$\mathrm{SO}(n, K) = \mathrm{SL}(n, K) \cap \mathrm{O}(n, K) \leq \mathrm{GL}(n, K)$$

eine Untergruppe, genannt die *spezielle orthogonale Gruppe*.

Definition 1.2.5. Sei G eine Gruppe und $M \subseteq G$ eine Teilmenge. Dann heißt die Untergruppe

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

die *von M erzeugte Untergruppe von G*. Der Schnitt wird hier gebildet über alle Untergruppen von G, die M enthalten. Für $M = \{g\}$ schreiben wir auch $\langle g\rangle$ für die von $\{g\}$ erzeugte Gruppe.

Definition 1.2.6. Sei G eine Gruppe und $g \in G$. Die Kardinalität

$$\mathrm{ord}(g) := |\langle g\rangle|$$

der von $\{g\}$ erzeugten Untergruppe von G heißt die *Ordnung von g*.

Proposition 1.2.7. *Sei G eine Gruppe und $g \in G$.*

(1) Falls $\mathrm{ord}(g) < \infty$, dann gilt

$$\mathrm{ord}(g) = \min\{k \geq 1 \mid g^k = 1\}$$

und

$$\langle g\rangle = \{1, g, g^2, ..., g^{n-1}\}$$

mit $n = \mathrm{ord}(g)$.

(2) Falls $\mathrm{ord}(g) = \infty$, dann gilt

$$\langle g\rangle = \{..., g^{-2}, g^{-1}, 1, g, g^2, ...\}$$

wobei die Potenzen g^i, $i \in \mathbb{Z}$, paarweise verschieden sind.

Beweis. Zunächst einmal ist klar, dass für beliebiges $g \in G$ gilt

$$\langle g \rangle = \{..., g^{-2}, g^{-1}, 1, g, g^2, ...\}$$

wobei die Potenzen nicht notwendigerweise paarweise verschieden sein müssen.

Um (1) zu zeigen, sei nun $\mathrm{ord}(g) < \infty$. Dann gibt es insbesondere $i \neq j$, so dass $g^i = g^j$. Sei ohne Einschränkung $i > j$, dann ist also $k = i - j \geq 1$ eine natürliche Zahl mit $g^k = 1$. Nach dem Wohlordnungssatz existiert eine kleinste natürliche Zahl n, für die $n \geq 1$ und $g^n = 1$ gilt. Sei nun $m \in \mathbb{Z}$. Dann gibt es eindeutig bestimmte Zahlen $a \in \mathbb{Z}$ und $0 \leq r < n$ so dass gilt

$$m = an + r.$$

Dann folgt

$$g^m = g^r$$

also gilt

$$\langle g \rangle = \{1, g, g^2, ..., g^{n-1}\}$$

Wir müssen noch zeigen, dass die Elemente $1, g, g^2, ..., g^{n-1}$ paarweise verschieden sind, aber dies folgt sofort aus der Minimalität von n.

Dieses Argument zeigt durch Kontraposition nun auch sofort (2), denn wenn die Potenzen g^i, $i \in \mathbb{Z}$ *nicht* paarweise verschieden sind, dann folgt aus dem obigen Argument, dass die Ordnung von g endlich sein muss. □

1.3 Homomorphismen

Definition 1.3.1. Seien G, G' Gruppen. Eine Abbildung

$$\varphi : G \to G'$$

heißt *Homomorphismus*, falls:

(H1) Für alle $g, h \in G$ gilt: $\varphi(gh) = \varphi(g)\varphi(h)$.

Wir schreiben $\mathrm{Hom}(G, G')$ für die Menge aller Gruppenhomomorphismen von G nach G'.

Aufgabe 1.3.2. Für jeden Homomorphismus $\varphi : G \to G'$ von Gruppen gelten zusätzlich:

(H2) Es gilt $\varphi(1_G) = 1_{G'}$, wobei 1_G und $1_{G'}$ die neutralen Elemente von G respektive G' bezeichnen.

(H3) Für alle $g \in G$ gilt $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Beispiele 1.3.3. (1) Sei G eine Gruppe. Die Einbettung $H \hookrightarrow G$ einer Untergruppe $H \leq G$ ist ein Homomorphismus.

(2) Für $n \geq 1$ und K Körper, definiert die Determinante

$$\det : \mathrm{GL}(n, K) \to K^*, \ A \mapsto \det(A)$$

einen Homomorphismus bezüglich der multiplikativen Gruppenstruktur auf $K^* = K \setminus \{0\}$.

(3) Sei

$$P : S_n \to \mathrm{GL}(n, K), \sigma \mapsto P_\sigma$$

wobei P_σ die zu σ gehörige *Permutationsmatrix* mit Einträgen

$$(P_\sigma)_{ij} := \begin{cases} 1 & \text{falls } i = \sigma(j), \\ 0 & \text{sonst} \end{cases}$$

ist. Dann ist P ein injektiver Homomorphismus.

(4) Sei G Gruppe und $g \in G$. Dann definiert die Abbildung

$$\gamma_g : G \to G,\ h \mapsto ghg^{-1}$$

einen Homomorphismus, genannt *Konjugation mit g* .

(5) Sei G eine Gruppe und $g \in G$. Dann ist die Abbildung

$$\mathbb{Z} \to G,\ i \mapsto g^i$$

ein Homomorphismus bezüglich der Addition auf $\mathbb{Z}$. Das Bild dieses Homomorphismus ist die von $\{g\}$ erzeugte Untergruppe von G.

Terminologie 1.3.4. Einen bijektiven Homomorphismus von Gruppen nennen wir *Isomorphismus*. Wir sagen, Gruppen G und G' sind *isomorph*, falls es einen Isomorphismus $\varphi : G \to G'$ gibt, und schreiben $G \cong G'$.

Aufgabe 1.3.5. Sei $\varphi : G \to G'$ ein Isomorphismus von Gruppen und sei $\psi : G' \to G$ die inverse Abbildung zu φ. Dann ist ψ ein Isomorphismus.

Beispiele 1.3.6. (1) Die Abbildung P aus Beispiel 1.3.3(3) induziert einen Isomorphismus

$$P : S_n \to P(n, K)$$

wobei $P(n, K) \leq \mathrm{GL}(n, K)$ die Untergruppe der Permutationsmatrizen ist, nämlich die Teilmenge der Matrizen, für die in jeder Zeile und Spalte genau ein Eintrag 1 ist und alle anderen Einträge 0.

(2) Die Exponentialfunktion

$$\exp : \mathbb{R} \to \mathbb{R}_{>0}, x \mapsto \exp(x)$$

definiert einen Isomorphismus der additiven Gruppe $(\mathbb{R}, +)$ mit der Gruppe $(\mathbb{R}_{>0}, \cdot)$ der positiven reellen Zahlen mit Multiplikation. Das Inverse von exp ist der natürliche Logarithmus

$$\ln : \mathbb{R}_{>0} \to \mathbb{R}, x \mapsto \ln(x),$$

der nach Aufgabe 1.3.5 auch ein Isomorphismus ist.

Proposition 1.3.7. *Sei $\varphi : G \to G'$ ein Homomorphismus.*

(1) Die Teilmenge

$$\mathrm{Bild}(\varphi) := \{g' \in G' \mid \exists g \in G\ :\ \varphi(g) = g'\} \subseteq G'$$

ist eine Untergruppe von G'.

(2) Die Teilmenge

$$\mathrm{Kern}(\varphi) := \{g \in G \mid \varphi(g) = 1\} \subseteq G$$

ist eine Untergruppe von G.

Beweis. Dies folgt recht direkt aus den Homomorphismus Axiomen (H1),(H2) und (H3). □

Proposition 1.3.8. *Sei $\varphi : G \to G'$ ein Homomorphismus von Gruppen. Dann sind äquivalent:*

(i) φ ist injektiv.

(ii) $\mathrm{Kern}(\varphi) = \{1\}$.

Beweis. Die Implikation (i) ⇒ (ii) ist klar. Sei also $\mathrm{Kern}(\varphi) = \{1\}$ und $g, h \in G$ mit $\varphi(g) = \varphi(h)$. Damit folgt

$$\varphi(gh^{-1}) = \varphi(g)\varphi(h^{-1}) = \varphi(g)\varphi(h)^{-1} = 1,$$

also $gh^{-1} \in \mathrm{Kern}(\varphi) = \{1\}$. Daher gilt $gh^{-1} = 1$, also $g = h$, so dass wir die Injektivität von φ gezeigt haben. □

Definition 1.3.9. Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Für $g \in G$ definieren wir die *Linksnebenklasse* von H bezüglich g

$$gH := \{gh \mid h \in H\} \subseteq G$$

sowie die *Rechtsnebenklasse* von H bezüglich g

$$Hg := \{hg \mid h \in H\} \subseteq G.$$

Aufgabe 1.3.10. Sei G eine Gruppe und $H \leq G$ eine Untergruppe.

(1) Die Linksnebenklassen sind die Äquivalenzklassen bezüglich der folgenden Äquivalenzrelation auf G:

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

(2) Die Rechtsnebenklassen sind die Äquivalenzklassen bezüglich der folgenden Äquivalenzrelation auf G:

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

Terminologie 1.3.11. Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Wir bezeichnen die Menge der Linksnebenklassen von H mit G/H und die Menge der Rechtsnebenklassen von H mit $H\backslash G$. Die Kardinalität

$$(G : H) := |G/H| \in \mathbb{N} \cup \infty$$

heißt der *Index von H in G*. Beachte, dass gilt: $|G/H| = |H\backslash G|$, denn die Abbildung $G \to G, g \mapsto g^{-1}$ identifiziert Linksnebenklassen mit Rechtsnebenklassen.

Korollar 1.3.12 (Satz von Lagrange)**.** *Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Dann gilt*

$$|G| = |H|(G : H).$$

Insbesondere gilt für jedes Element $g \in G$ einer endlichen Gruppe:

$$\mathrm{ord}(g)||G|.$$

Beweis. Dies folgt aus Aufgabe 1.3.10: Als Äquivalenzklassen einer Äquivalenzrelation bilden die Linksnebenklassen eine Partition von G. Zudem sind alle Nebenklassen gleichmächtig mit Kardinalität $|H|$, denn für gegebenes $g \in G$, schränkt sich die Abbildung

$$G \to G, x \mapsto gx$$

auf eine Bijektion $H \cong gH$ ein. □

Definition 1.3.13. Eine Untergruppe $N \leq G$ heißt *normal* oder auch *Normalteiler*, falls für alle $g \in G$ gilt:

$$gN = Ng.$$

Falls $N \subseteq G$ eine normale Untergruppe ist, dann schreiben wir auch $N \trianglelefteq G$.

Bemerkung 1.3.14. Eine Untergruppe $N \leq G$ ist genau dann normal, wenn

(N1) für alle $g \in G$ und $h \in N$ gilt: $ghg^{-1} \in N$,

wenn also N *abgeschlossen unter Konjugation* mit Elementen aus G ist.

Proposition 1.3.15. *Sei $\varphi : G \to G'$ ein Homomorphismus von Gruppen. Dann ist*

$$\mathrm{Kern}(\varphi) \trianglelefteq G$$

eine normale Untergruppe.

Beweis. Wir verifizieren (N1). Sei also $h \in \mathrm{Kern}(\varphi)$ und $g \in G$. Wir rechnen

$$\begin{aligned}\varphi(ghg^{-1}) &= \varphi(g)\varphi(h)\varphi(g^{-1}) \\ &= \varphi(g)1\varphi(g)^{-1} = 1,\end{aligned}$$

also $ghg^{-1} \in \mathrm{Kern}(\varphi)$. □

Beispiele 1.3.16. (1) Sei $n \geq 1$ und K ein Körper. Für den Homomorphismus

$$\det : \mathrm{GL}(n, K) \longrightarrow K^*$$

gilt

$$\mathrm{Kern}(\det) = \mathrm{SL}(n, K) \trianglelefteq \mathrm{GL}(n, K).$$

(2) Betrachte für $n \geq 1$ die Komposition der Homomorphismen

$$S_n \xrightarrow{P} \mathrm{GL}(n, \mathbb{Q}) \xrightarrow{\det} \mathbb{Q}^*$$

Da die Determinante einer Permutationsmatrix entweder $+1$ oder -1 ist, nimmt diese Komposition Werte in der multiplikativen Untergruppe $\{1, -1\} \leq \mathbb{Q}^*$ an. Wir erhalten also einen Homomorphismus

$$\mathrm{sign} : S_n \to \{\pm 1\}, \sigma \mapsto \det(P_\sigma),$$

genannt *Signum*. Wir bezeichnen seinen Kern mit

$$A_n := \mathrm{Kern}(\mathrm{sign}) \trianglelefteq S_n,$$

genannt die *alternierende Gruppe*.

Proposition 1.3.17. *Sei G eine Gruppe und $N \trianglelefteq G$ eine normale Untergruppe.*

(1) Auf der Menge G/N von Nebenklassen von N existiert eine Gruppenstruktur mit Verknüpfung

$$G/N \times G/N \to G/N,\ (aN, bN) \mapsto (ab)N. \tag{1.3.18}$$

(2) Die Quotientenabbildung

$$\pi : G \to G/N,\ a \mapsto aN$$

ist ein Gruppenhomomorphismus mit $\mathrm{Kern}(\pi) = N$.

Beweis. Um (1) zu zeigen, müssen wir zunächst nachweisen, dass die Verknüpfungsabbildung wohldefiniert ist. Seien also $\tilde{a} \in aN$ and $\tilde{b} \in bN$ beliebige Vertreter der Nebenklasse aN respektive bN. Dann gibt es also $m, n \in N$ mit $\tilde{a} = am$ und $\tilde{b} = bn$. Wir rechnen:

$$\begin{aligned}\tilde{a}\tilde{b} &= ambn \\ &= ab(b^{-1}mb)n,\end{aligned}$$

also ein Element von abN, denn da N normal ist, gilt $b^{-1}mb \in N$.
Im vorigen Satz scheint etwas zu fehlen. Ist $\tilde{a}\tilde{b} \in abN$ gemeint?
Damit ist also $\tilde{a}\tilde{b}$ ein Vertreter der Nebenklasse abN, so dass also

$$\tilde{a}\tilde{b}N = abN,$$

womit gezeigt ist, dass die Abbildungsvorschrift (1.3.18) also unabhängig von der Vertreterwahl ist. Alle Gruppenaxiome für G/N vererben sich nun von den entsprechenden Gruppenaxiomen für G, mit neutralem Element

$$1_{G/N} = N,$$

denn die Verknüpfung ist auf Vertretern definiert.

Wir zeigen noch (2). Per Definition gilt

$$\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b),$$

so dass π also ein Homomorphismus ist. Desweiteren gilt für $a \in G$

$$\pi(a) = N \Leftrightarrow aN = N \Leftrightarrow a \in N,$$

also $\operatorname{Kern}(\pi) = N$. □

Satz 1.3.19 (Homomorphiesatz)**.** *Sei $\varphi : G \to G'$ ein Homomorphismus von Gruppen. Dann induziert φ einen Isomorphismus*

$$\overline{\varphi} : G/\operatorname{Kern}(\varphi) \to \operatorname{Bild}(\varphi),\ a\operatorname{Kern}(\varphi) \mapsto \varphi(a).$$

Beweis. Zunächst ist $\overline{\varphi}$ wohldefiniert, denn für $n \in \operatorname{Kern}(\varphi)$ und $a \in G$ gilt $\varphi(an) = \varphi(a)\varphi(n) = \varphi(a)$. Per Konstruktion ist $\overline{\varphi}$ surjektiv und injektiv, da $\operatorname{Kern}(\overline{\varphi}) = \{\operatorname{Kern}(\varphi)\} = 1_{G/\operatorname{Kern}(\varphi)}$. □

Korollar 1.3.20. *Sei $\varphi : G \to G'$ ein Homomorphismus von Gruppen. Dann lässt sich φ schreiben als Komposition*

$$\varphi = \iota \circ \overline{\varphi} \circ \pi$$

wobei

1. *$\pi : G \twoheadrightarrow G/\operatorname{Kern}(\varphi)$ der (surjektive) Quotientenhomomorphismus ist,*
2. *$\overline{\varphi} : G/\operatorname{Kern}(\varphi) \to \operatorname{Bild}(\varphi)$ der Isomorphismus aus Satz 1.3.19 ist,*
3. *und $\iota : \operatorname{Bild}(\varphi) \hookrightarrow G'$ die (injektive) Einbettung des Bildes von φ ist.*

In anderen Worten kommutiert das Quadrat

$$\begin{array}{ccc} G & \xrightarrow{\ \varphi\ } & G' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ G/\operatorname{Kern}(\varphi) & \xrightarrow{\ \overline{\varphi}\ } & \operatorname{Bild}(\varphi). \end{array}$$

Beispiele 1.3.21. (1) Für $n \geq 1$ und einen Körper K induziert der Homomorphismus

$$\det : \mathrm{GL}(n, K) \to K^*$$

einen Isomorphismus

$$\mathrm{GL}(n, K)/\mathrm{SL}(n, K) \xrightarrow{\cong} K^*.$$

(2) Für $n \geq 2$, induziert der Homomorphismus

$$\operatorname{sign} : S_n \to \{\pm 1\}$$

einen Isomorphismus

$$S_n/A_n \xrightarrow{\cong} \{\pm 1\}.$$

(3) Sei G eine Gruppe und $g \in G$. Betrachte den Homomorphismus

$$\varphi : \mathbb{Z} \to G,\ i \mapsto g^i$$

aus Beispiel 1.3.3.

(a) Falls $\operatorname{ord}(g) = \infty$, dann gilt $\operatorname{Kern}(\varphi) = \{0\}$ und φ induziert einen Isomorphismus

$$\mathbb{Z} \xrightarrow{\cong} \langle g \rangle,$$

denn in diesem Fall ist der Quotientenhomomorphismus $\pi : \mathbb{Z} \to \mathbb{Z}/\{0\}$ ein Isomorphismus.

(b) Falls $\mathrm{ord}(g) = N < \infty$, dann gilt $\mathrm{Kern}(\varphi) = N\mathbb{Z}$ und φ induziert einen Isomorphismus

$$\mathbb{Z}/N\mathbb{Z} \xrightarrow{\cong} \langle g \rangle.$$

Abschließend führen wir noch ein in der gesamten Algebra sehr wichtiges Werkzeug im gruppentheoretischen Rahmen ein und untersuchen dieses in den Übungen näher:

Definition 1.3.22. Eine *kurze exakte Sequenz*

$$\{0\} \to N \xrightarrow{\varphi} G \xrightarrow{\psi} H \to \{0\}$$

von Gruppen besteht aus Gruppenhomomorphismen $\varphi : N \to G$ und $\psi : G \to H$, so dass gilt:

(1) φ ist injektiv.

(2) $\mathrm{Bild}(\varphi) = \mathrm{Kern}(\psi)$.

(3) ψ ist surjektiv.

Wir sagen, dass eine kurze exakte Sequenz *zerfällt*, falls ein Homomorphismus $\sigma : H \to G$ mit $\psi \circ \sigma = \mathrm{id}_H$ existiert. Dann heißt σ *Schnitt*.

1.4 Operationen

Definition 1.4.1. Eine *Operation* (oder *Wirkung*) einer Gruppe G auf einer Menge M ist eine Abbildung

$$G \times M \to M,\ (g, x) \mapsto g.x$$

so dass gelten:

(1) für alle $g, h \in G$ und $x \in M$ gilt: $(gh).x = g.(h.x)$.

(2) für alle $x \in M$ gilt: $1.x = x$.

Wir sagen, G operiert auf M und schreiben $G \circlearrowright M$.

Beispiele 1.4.2. (1) Jede Gruppe G operiert auf sich selbst via

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

(2) Jede Gruppe G operiert auf sich selbst via Konjugation:

$$G \times G \to G,\ (g, h) \mapsto ghg^{-1}.$$

(3) Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Dann operiert G auf der Menge G/H von Linksnebenklassen via

$$G \times G/H \to G/H,\ (g', gH) \mapsto g'gH.$$

(4) Für jede Menge M operiert die symmetrische Gruppe S_M auf M via

$$S_M \times M \to M,\ (\sigma, x) \mapsto \sigma(x).$$

(5) Für $n \geq 1$ und einen Körper K operiert die Gruppe $\mathrm{GL}(n, K)$ auf K^n via

$$\mathrm{GL}(n, K) \times K^n \to K^n,\ (A, v) \mapsto Av.$$

Definition 1.4.3. Für Operationen $G \circlearrowright M$ und $G \circlearrowright N$ heißt eine Abbildung

$$\varphi : M \to N$$

von Mengen *G-äquivariant*, falls für alle $g \in G$ und $x \in M$ gilt: $\varphi(g.x) = g.\varphi(x)$.

Terminologie 1.4.4. Gegeben sei eine Operation $G \curvearrowright M$ einer Gruppe G auf einer Menge M.

(1) Die Relation
$$x \underset{G}{\sim} y \ :\Leftrightarrow\ \exists g \in G : x = g.y$$
definiert eine Äquivalenzrelation auf M. Die Äquivalenzklassen sind die Mengen der Form
$$G.x = \{g.x \mid g \in G\} \subseteq M,$$
genannt *Bahn von x unter G*. Die Quotientenmenge
$$G\backslash\!\backslash M := M/\underset{G}{\sim}$$
heißt der *Bahnenraum von $G \curvearrowright M$*.

(2) Für $x \in M$ heißt die Untergruppe (!)
$$G_x := \{g \in G \mid g.x = x\} \leq G$$
der *Stabilisator von x*.

(3) Ein Punk $x \in M$ heißt *Fixpunkt*, falls $G_x = G$, und wir bezeichnen die Menge aller Fixpunkte mit
$$M^G \subseteq M.$$

(4) Die Operation $G \curvearrowright M$ heißt *transitiv*, falls für jedes $x \in M$ gilt: $G.x = M$.

Proposition 1.4.5. *Sei $G \curvearrowright M$ und $x \in M$. Dann definiert*
$$G/G_x \to G.x,\ gG_x \mapsto g.x$$
eine bijektive G-äquivariante Abbildung. Die Gruppenwirkungen sind hierbei die G-Wirkung auf G/G_x von Beispiel 1.4.2 (3) sowie die Einschränkung der Wirkung $G \curvearrowright M$ auf die Bahn $G.x$.

Insbesondere gilt die Bahnformel
$$|G.x| = (G : G_x).$$

Beweis. Wir zeigen zunächst, dass die Abbildungsvorschrift wohldefiniert ist: Für $g \in G$ und $h \in G_x$ gilt $(gh).x = g.(h.x) = g.x$. Die Abbildung ist desweiteren injektiv, denn falls $g_1.x = g_2.x$, dann gilt $g_1^{-1}g_2 \in G_x$, also auch $g_1G_x = g_2G_x$. Die Surjektivität ist klar, per Definition von $G.x$. □

Korollar 1.4.6. *Sei $G \curvearrowright M$ mit $|M| < \infty$. Dann gilt*
$$|M| = \sum_{G.x \in G\backslash\!\backslash M} (G : G_x), \tag{1.4.7}$$
wobei die Summe durch ein Repräsentantensystem von $G\backslash\!\backslash M$ indiziert ist.

Beweis. Es gilt
$$M = \bigcup_{G.x \in G\backslash\!\backslash M} G.x.$$
□

Bemerkung 1.4.8. Die Formel (1.4.7) lässt sich weiter umschreiben als
$$|M| = |X^G| + \sum_{\substack{G.x \in G\backslash\!\backslash M \\ G_x \neq G}} (G : G_x) \tag{1.4.9}$$

Terminologie 1.4.10. Sei $G \curvearrowright G$ die Wirkung

$$G \times G \to G,\ (g,x) \mapsto gxg^{-1}$$

durch Konjugation. Da das Beispiel dieser Gruppenwirkung besonders wichtig ist, führen wir spezielle Terminologie ein:

(1) Für $x \in G$ heißt die Bahn

$$G.x = \{gxg^{-1} | g \in G\} \subseteq G$$

die *Konjugationsklasse von* x.

(2) Die Menge der Fixpunkte

$$\mathrm{Z}(G) := G^G = \{x \in G | \forall g \in G : gx = xg\} \leq G$$

bildet eine Untergruppe von G, genannt das *Zentrum von* G.

(3) Für $x \in G$ heißt der Stabilisator

$$\mathrm{C}_G(x) := G_x = \{g \in G | gx = xg\} \leq G$$

der *Zentralisator von* x.

(4) Die Gleichung (1.4.7) lautet

$$|G| = |\,\mathrm{Z}(G)| + \sum_{\substack{G.x \in G\backslash M \\ G_x \neq G}} (G : \mathrm{C}_G(x)). \tag{1.4.11}$$

und heißt die *Klassengleichung von* G.

(5) *Beobachtung:* Da $\mathrm{Z}(G)$ eine Untergruppe von G bildet, teilen alle Summanden der Klassengleichung (1.4.11) die Ordnung von G.

Beispiel 1.4.12. Wir bestimmen die Klassengleichung der alternierenden Gruppe $A_4 \trianglelefteq S_4$. Es gilt $(S_4 : A_4) = 2$, also

$$|A_4| = \frac{|S_4|}{(S_4 : A_4)} = 12.$$

Wir listen und benennen alle Elemente. Neben dem neutralen Element (1) gibt es die Elemente

$$(12)(34),\ (13)(24),\ (14)(23)$$

der Ordnung 2 und schließlich die Elemente

$$\begin{array}{cccc} (123) & (124) & (134) & (234) \\ (132) & (142) & (143) & (243) \end{array}$$

der Ordnung 3. Wir beschreiben nun alle Untergruppen von A_4. Nach dem Satz von Lagrange müssen deren Ordnungen Teiler von 12 sein, also $1, 2, 3, 4, 6, 12$. Wir erhalten zunächst die zyklischen Untergruppen

$$\langle (12)(34) \rangle,\ \langle (13)(24) \rangle,\ \langle (14)(23) \rangle$$

der Ordnung 2 sowie

$$\langle (123) \rangle,\ \langle (124) \rangle,\ \langle (134) \rangle,\ \langle (234) \rangle$$

der Ordnung 3. Die Untergruppe

$$\langle \{(12)(34), (13)(24)\} \rangle$$

hat Ordnung 4, wobei gilt $(12)(34) \circ (13)(24) = (14)(23)$, so dass diese Gruppe also alle Elemente der Ordnung 2 enthält. Daher muss dies die einzige Untergruppe der Ordnung 4 sein. Wir werden später mittels der

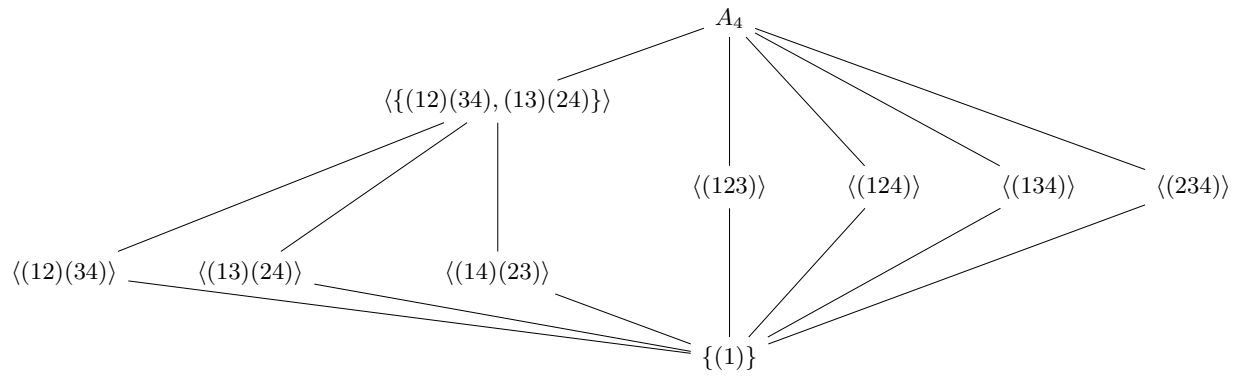


Abbildung 1.1: Untergruppenverband von A_4

Klassengleichung zeigen, dass es keine Untergruppen der Ordnung 6 gibt, so dass dies also alle Untergruppen sind (vgl. Abbildung 1.1).

Ganz allgemein gilt für eine Permutation $\sigma \in S_n$ und einen Zykel $(a_1 a_2 \cdots a_k) \in S_n$ die Formel

$$\sigma \circ (a_1 a_2 ... a_k) \circ \sigma^{-1} = (\sigma(a_1)\sigma(a_2)...\sigma(a_k)).$$

Dies hilft bei der Berechnung der Konjugationsklassen, welche neben dem Zentrum $\mathrm{Z}(G) = \{1\}$ gegeben sind durch

$$\{(12)(34),(13)(24),(14)(23)\}$$

sowie

$$\{(123),(243),(142),(134)\}$$

und

$$\{(132),(234),(124),(143)\}.$$

Daher lautet die Klassengleichung von A_4 also

$$12 = 1 + 3 + 4 + 4.$$

Wir können nun folgern, dass es keine Untergruppen der Ordnung 6 in A_4 geben kann: Als Untergruppen der Ordnung 2 wären diese nämlich normal, also Vereinigungen von Konjugationsklassen. Doch dann müsste sich 6 als eine Summe von Summanden der Klassengleichung schreiben lassen, was nicht der Fall ist.

1.5 Euklidische Bewegungen

Sei $n \geq 1$. Für Vektoren

$$v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}, w = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} \in \mathbb{R}^n$$

definieren wir das *Skalarprodukt*

$$\langle v, w \rangle := \sum_{i=1}^{n} v_i w_i \in \mathbb{R},$$

die *Euklidische Norm*

$$||v|| := \sqrt{\langle v, v \rangle}$$

sowie den *Euklidischen Abstand*

$$d(v, w) := ||v - w||.$$

Definition 1.5.1. Eine Abbildung $T : \mathbb{R}^n \to \mathbb{R}^n$ heißt *(Euklidische) Bewegung* (oder *Isometrie*) falls für alle $v, w \in \mathbb{R}^n$ gilt:

$$d(T(v), T(w)) = d(v, w),$$

falls T also den Euklidischen Abstand erhält. Wir schreiben $E(n)$ für die Menge der Euklidischen Bewegungen.

Beispiele 1.5.2. (1) Für jedes $b \in \mathbb{R}^n$ definiert die Translation

$$\tau_b : \mathbb{R}^n \to \mathbb{R}^n,\ v \mapsto v + b$$

eine Isometrie.

(2) Für jede orthonormale Matrix $A \in \mathrm{O}(n, \mathbb{R})$, ist die Abbildung

$$\mu_A : \mathbb{R}^n \to \mathbb{R}^n,\ v \mapsto Av$$

eine Isometrie. Denn mit

$$\langle v, w \rangle = v^T w$$

rechnen wir

$$\begin{aligned} \langle Av, Aw \rangle &= (Av)^T Aw \\ &= v^T A^T Aw \\ &= v^T w = \langle v, w \rangle, \end{aligned}$$

so dass μ_A also das Skalarprodukt erhält. Damit gilt dann auch weiterhin

$$\begin{aligned} d(Av, Aw) &= ||Av - Aw|| \\ &= ||A(v - w)|| \\ &= \sqrt{\langle A(v - w), A(v - w) \rangle} \\ &= \sqrt{\langle v - w, v - w \rangle} = d(v, w). \end{aligned}$$

Satz 1.5.3. *Sei $T \in E(n)$ mit $T(0) = 0$. Dann existiert $A \in \mathrm{O}(n, \mathbb{R})$, so dass*

$$T = \mu_A.$$

Beweis. Schritt 1. T erhält das Skalarprodukt.

Da $T \in E(n)$ gilt für $v, w \in \mathbb{R}^n$,

$$\langle T(v) - T(w), T(v) - T(w) \rangle = \langle v - w, v - w \rangle \tag{1.5.4}$$

Wir setzen $w = 0$ in (1.5.4) und erhalten (wegen $T(0) = 0$)

$$\langle T(v), T(v) \rangle = \langle v, v \rangle \tag{1.5.5}$$

Unter Verwendung der Bilinearität und Symmetrie des Skalarprodukts erhalten wir aus (1.5.4) die Gleichung

$$\langle T(v), T(v) \rangle - 2\langle T(v), T(w) \rangle + \langle T(w), T(w) \rangle = \langle v, v \rangle - 2\langle v, w \rangle \langle w, w \rangle,$$

woraus mit (1.5.5) folgt:

$$\langle T(v), T(w) \rangle = \langle v, w \rangle. \tag{1.5.6}$$

Schritt 2. Falls zusätzlich gilt: $\forall 1 \leq i \leq n$: $T(e_i) = e_i$, dann folgt $T = \mathrm{id}$.

Für $v \in \mathbb{R}^n$ gilt dann nämlich für $1 \leq i \leq n$:

$$(T(v))_i = \langle T(v), e_i \rangle = \langle T(v), T(e_i) \rangle = \langle v, e_i \rangle = v_i,$$

also $T(v) = v$.
Schritt 3. Sei nun wieder T allgemein mit $T(0) = 0$. Wir setzen

$$A := (T(e_1), T(e_2), \ldots, T(e_n)) \in \mathbb{R}^{n\times n},$$

T ist also die Matrix mit den Spalten $T(e_i)$, $1 \leq i \leq n$. Wegen

$$\langle T(e_i), T(e_j)\rangle = \langle e_i, e_j\rangle$$

gilt $A \in \mathrm{O}(n, \mathbb{R})$. Zudem ist

$$\widetilde{T} := \mu_{A^T} \circ T \in E(n)$$

eine Isometrie mit $\widetilde{T}(0) = 0$ und, für alle $1 \leq i \leq n$, $\widetilde{T}(e_i) = e_i$, so dass also nach Schritt 2 gilt: $\widetilde{T} = \mathrm{id}$ und daher auch

$$T = \mu_A.$$

□

Korollar 1.5.7. *Jede Euklidische Bewegung $T \in E(n)$ ist von der Form*

$$T : \mathbb{R}^n \to \mathbb{R}^n,\ v \mapsto Av + b$$

für eindeutig bestimmte $A \in \mathrm{O}(n, \mathbb{R})$ und $b \in \mathbb{R}$.

Beweis. Setze $b = T(0)$. Dann gilt $\tau_{-b} \circ T(0) = 0$, also nach Satz 1.5.3

$$\tau_{-b} \circ T = \mu_A$$

für $A \in \mathrm{O}(n, \mathbb{R})$, also

$$T = \tau_b \circ \mu_A.$$

□

Korollar 1.5.8. *Die Menge $E(n)$ der Euklidischen Bewegungen mit der Komposition bildet eine Gruppe.*

Beweis. Die einzige Aussage, die nicht a priori klar ist, ist, dass eine Bewegung $T \in E(n)$ ein Inverses hat. Die Injektivität von T folgt sofort aus der Definition. Die Surjektivität folgt aus unserem Klassifikationsresultat Korollar 1.5.7: Das Inverse von $\tau_b \circ \mu_A$ ist $\mu_{A^T} \circ \tau_{-b}$. □

Bemerkung 1.5.9. Im allgemeinen lässt sich aus gegebenen Gruppen G und G' eine neue Gruppe, das *direkte Produkt* von G und G' wie folgt definieren: Auf der Menge $G \times G'$ definieren wir die "komponentenweise" Verknüpfung:

$$(g_1, g_1') \circ (g_2, g_2') = (g_1 \circ g_2, g_1' \circ g_2').$$

Wegen Korollar 1.5.7 erhalten wir eine Bijektion von *Mengen*

$$E(n) \cong \mathrm{O}(n, \mathbb{R}) \times \mathbb{R}^n.$$

Allerdings ist die Komposition von Bewegungen durch die Formel

$$(A, b) \circ (A', b') = (AA', Ab' + b)$$

beschrieben, also *nicht* die komponentenweise Verknüpfung. Wir definieren nun diese Art von Gruppenstruktur in einem etwas allgemeineren Rahmen.

Proposition 1.5.10. *Seien H, N Gruppen und H operiere auf N via Gruppenhomomorphismen. Für jedes $h \in H$ ist also die Abbildung*

$$N \to N,\ x \mapsto h.x$$

ein Gruppenhomomorphismus. Dann definiert die Verknüpfung

$$(H \times N) \times (H \times N) \to (H \times N), ((h, x), (h', x')) \mapsto (hh', x(h.x'))$$

eine Gruppenstruktur auf der Menge $H \times N$.

Beweis. Direktes Nachrechnen. □

Definition 1.5.11. Die Gruppe $(H \times N, \circ)$ aus Proposition 1.5.10 heißt das *semidirekte Produkt* von $(H, N, H \curvearrowright N)$, geschrieben $H \ltimes N$.

Beispiele 1.5.12. (1) Falls H trivial auf N operiert, dann definiert die Identitätsabbildung

$$H \ltimes N \cong H \times N$$

einen Isomorphismus mit dem *direkten* Produkt von H und N.

(2) Sei $\mathrm{O}(n, \mathbb{R}) \curvearrowright \mathbb{R}^n$ die Operation durch Matrix-Vektor-Multiplikation. Dann besagt die Formel aus Bemerkung 1.5.9, dass die Abbildung

$$\mathrm{O}(n, \mathbb{R}) \ltimes \mathbb{R}^n \to E(n),\ (A, b) \mapsto \tau_b \circ \mu_A$$

ein Isomorphismus von Gruppen ist.

(3) Sei $\mathrm{GL}(n, \mathbb{R}) \curvearrowright \mathbb{R}^n$ die Operation durch Matrix-Vektor-Multiplikation. Dann erhalten wir die *allgemeine affine Gruppe*

$$\mathrm{GA}(n, \mathbb{R}) := \mathrm{GL}(n, \mathbb{R}) \ltimes \mathbb{R}^n.$$

Diese ist isomorph zur Gruppe der *Affinitäten* (= bijektive affine Selbstabbildungen) von $\mathbb{R}^n$

Beispiel 1.5.13. Aus elementargeometrischen Überlegungen erhalten wir, dass sich jede Matrix $A \in \mathrm{O}(2)$ schreiben lässt als

$$\begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$

wobei $\epsilon = \det(A) \in \{\pm 1\}$ und $\theta \in \mathbb{R}/2\pi\mathbb{Z}$. Daraus resultiert, dass sich jede Bewegung $T \in E(2)$ als Komposition von Translationen, Spiegelungen und Drehungen schreiben lässt. Eine etwas präzisere Klassifikation wird auf Übungsblatt 4 bewiesen: Jede euklidische Bewegung von $\mathbb{R}^2$ ist eine der folgenden Abbildungen

(1) Translation τ_b mit $b \in \mathbb{R}^2$,

(2) Drehung $\delta_{x,\theta}$ um einen Punkt $x \in \mathbb{R}^2$ mit Winkel θ,

(3) Spiegelung σ_l an einer Geraden l,

(4) Gleitspiegelung $\tau_b \sigma_l$ wobei $0 \neq b \in \mathbb{R}^2$ parallel zur Geraden l ist.

Satz 1.5.14. *Sei $A \in \mathrm{SO}(3, \mathbb{R})$. Dann existiert eine Orthonormalbasis $B = (v, p, q)$ von $\mathbb{R}^3$, so dass die Darstellungsmatrix von μ_A bezüglich der Basis B die Gestalt*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}$$

für $\theta \in \mathbb{R}/2\pi\mathbb{Z}$ hat. In anderen Worten: μ_A ist eine Drehung um die von v aufgespannte Achse mit Winkel θ.

Beweis. Wir rechnen

$$\begin{aligned} \det(A - I) &= \det(A(I - A^T)) && (1.5.15)\\ &= \det(A)\det((I - A)^T) && (1.5.16)\\ &= \det(I - A) && (1.5.17)\\ &= \det(-(A - I)) && (1.5.18)\\ &= -\det(A - I). && (1.5.19) \end{aligned}$$

Daher folgt $\det(A - I) = 0$. Also ist 1 eine Nullstelle des charakteristischen Polynoms von A, so dass es also einen Eigenvektor $v \neq 0$ zum Eigenwert 1 gibt, also

$$Av = v.$$

Wir ergänzen v zu einer Orthonormalbasis $B = (v, p, q)$. Dann ist die Darstellungsmatrix

$$D_B(\mu_A) = \begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix}$$

von μ_A bezüglich B eine Blockdiagonalmatrix mit $A' \in \mathrm{SO}(2, \mathbb{R})$. Dies folgt direkt aus $\mu_A(v) = v$ zusammen mit der Tatsache, dass das Bild von B unter μ_A wieder eine Orthonormalbasis ist. Nach Beispiel 1.5.13 hat damit $D_B(\mu_A)$ also die behauptete Gestalt. □

Bemerkung 1.5.20. Nach Satz 1.5.14 korrespondieren die Matrizen $A \in \mathrm{SO}(3, \mathbb{R})$ genau zu den Drehungen von $\mathbb{R}^3$ um beliebige Achsen durch den Ursprung. Insbesondere bilden also letztere eine Untergruppe der Gruppe $E(3)$ der Euklidischen Bewegungen.

1.6 Symmetrie im Raum

Sei $n \geq 1$ und $F \subseteq \mathbb{R}^n$ eine Teilmenge. Wir definieren die *orthogonale Symmetriegruppe* von F als

$$\mathrm{O}(F) := \{A \in \mathrm{O}(n, \mathbb{R}) \mid \mu_A(F) = F\} \leq \mathrm{O}(n, \mathbb{R})$$

sowie die *spezielle orthogonale Symmetriegruppe* (oder *Drehsymmetriegruppe*) von F als

$$\mathrm{SO}(F) := \{A \in \mathrm{SO}(n, \mathbb{R}) \mid \mu_A(F) = F\} \leq \mathrm{SO}(n, \mathbb{R}).$$

In diesem Abschnitt untersuchen wir Drehsymmetrien in $\mathbb{R}^3$ und führen dazu zunächst einige fundamentale Figuren ein.

Beispiele 1.6.1. Eine Teilmenge K von $\mathbb{R}^n$ heißt *konvex*, falls folgende Bedingung erfüllt ist: Für $x, y \in K$ und $t \in [0, 1]$ gilt $tx + (1 - t)y \in K$. Also: K enthält mit jedem Paar von Punkten $x, y \in K$ auch das Geradensegment zwischen x und y. Es folgt sofort aus der Definition, dass beliebige Schnitte von konvexen Teilmengen von $\mathbb{R}^n$ konvex sind. Wir definieren für eine beliebige Teilmenge $M \subseteq \mathbb{R}^n$ die *konvexe Hülle*

$$\mathrm{Konv}(M) := \bigcap_{\substack{M \subseteq K \\ K \text{ konvex}}} K.$$

von M.

(1) Für $n \geq 2$, definieren wir das *reguläre n-gon*

$$R_n = \mathrm{Konv}(\{(\cos(\frac{2\pi k}{n}), \sin(\frac{2\pi k}{n})) \mid 0 \leq k < n\}) \subseteq \mathbb{R}^2,$$

die *reguläre Pyramide*

$$P_n := \mathrm{Konv}(\{\begin{pmatrix} p \\ 0 \end{pmatrix} \mid p \in R_n\} \cup \{(0, 0, 1)\}),$$

sowie den *Zylinder über R_n*

$$Z_n = \{\{\begin{pmatrix} p \\ t \end{pmatrix} \mid p \in R_n,\ -1 \leq t \leq 1\}.$$

Auf die Gefahr hin, die Diskussion aus der Vorlesung hervorzubringen: Ist das in der allgemeinen Vorstellung nicht eher ein reguläres Prisma?

(2) Desweiteren definieren wir den *Tetraeder*

$$T = \mathrm{Konv}(\{(1,1,1),(1,-1,-1),(-1,1,-1),(-1,-1,1)\}),$$

den *Würfel*

$$W = \mathrm{Konv}(\{(\pm 1,\pm 1,\pm 1)\}),$$

den *Oktaeder*

$$O = \mathrm{Konv}(\{(\pm 1,0,0),(0,\pm 1,0),(0,0,\pm 1)\}),$$

den *Ikosaeder*

$$I = \mathrm{Konv}(\{(0,\pm 1,\pm\Phi),(\pm\Phi,0,\pm 1),(\pm 1,\pm\Phi,0)\})$$

und den *Dodekaeder*

$$D = \mathrm{Konv}(\{(\pm 1,\pm 1,\pm 1),(0,\pm\Phi^{-1},\pm\Phi),(\pm\Phi^{-1},0,\pm\Phi),(\pm\Phi^{-1},\pm\Phi,0)\}),$$

wobei $\Phi = \frac{\sqrt{5}+1}{2}$ der goldene Schnitt ist.

Beispiel 1.6.2. Wir werden sehen, dass die Isometriegruppe des regelmäßigen n-gons die *Diedergruppe* D_n ist. Die Gruppe besteht aus den n Drehungen und n Spiegelungen entlang der Symmetrieachsen des n-gons, in Matrixschreibweise gilt also:

$$D_n = \left\{ \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) & \cos\left(\frac{2\pi k}{n}\right) \end{pmatrix}, \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & \sin\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) & -\cos\left(\frac{2\pi k}{n}\right) \end{pmatrix} \mid 0 \le k \le n-1 \right\}.$$

Aufgabe 1.6.3. Die Figuren aus Beispiel 1.6.1 (2) sind tatsächlich Modelle der fünf platonischen Körper.

Proposition 1.6.4. *Für die Figuren F aus Beispiel 1.6.1 gibt es die folgenden Isomorphismen von Gruppen.*

(1) $\mathrm{SO}(P_n) \cong C_n$ *die zyklische Gruppe der Ordnung* n.

(2) $\mathrm{SO}(Z_n) \cong D_n$ *die Diedergruppe der Ordnung* $2n$.

(3) $\mathrm{SO}(T) \cong A_4$ *die alternierende Gruppe der Ordnung* 12.

(4) $\mathrm{SO}(W) \cong \mathrm{SO}(O) \cong S_4$ *die symmetrische Gruppe der Ordnung* 24.

(5) $\mathrm{SO}(I) \cong \mathrm{SO}(D) \cong A_5$ *die alternierende Gruppe der Ordnung* 60.

Beweis. Wir berechnen für jede der Figuren F zunächst die Kardinalität von $\mathrm{SO}(F)$, indem wir die transitive Operation auf der Menge der Randflächen (für P_n ohne die Grundfläche) betrachten. Da der Stabilisator einer Fläche f jeweils die zyklische Gruppe von Drehsymmetrien einer fest gewählten Randfläche ist, ergeben sich mit der Bahnformel

$$|G| = |G.f||G_f|$$

jeweils:

(1) $|\mathrm{SO}(P_n)| = n * 1 = n$.

(2) $|\mathrm{SO}(Z_n)| = 2n * 1 = 2n$. Das macht zwar am Ende keinen Unterschied mehr, aber hier müsste, der obigen Erklärung folgend, $n * 2$ stehen, oder? Wir haben n rechteckige Randflächen, die eine 180°-Drehsymmetrie besitzen, also sind zwei Elemente im Stabilisator.

(3) $|\mathrm{SO}(T)| = 4 * 3 = 12$.

(4) $|\mathrm{SO}(W)| = 6 * 4 = 24 = 8 * 3 = |\mathrm{SO}(O)|$.

(5) $|\mathrm{SO}(I)| = 20 * 3 = 60 = 12 * 5 = |\mathrm{SO}(D)|$.

Die Kenntnis dieser Kardinalitäten vereinfacht nun auch die Konstruktion der behaupteten Isomorphismen:

Die Drehgruppe von P_n enthält die Matrizen

$$\left\{ \begin{pmatrix} \cos(\frac{2\pi k}{n}) & -\sin(\frac{2\pi k}{n}) & 0 \\ \sin(\frac{2\pi k}{n}) & \cos(\frac{2\pi k}{n}) & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid 0 \leq k < n \right\}$$

welche diese also aus Kardinalitätsgründen schon ausschöpfen müssen. Die Projektion auf den Drehblock dieser Matrix induziert den gewünschten Isomorphismus mit C_n, realisiert als 2-dimensionale Drehsymmetriegruppe des regulären n-gons $R_n \subseteq \mathbb{R}^2$ aus Beispiel 1.6.1.

Die Drehgruppe von Z_n enthält die Matrizen

$$\left\{ \begin{pmatrix} \cos(\frac{2\pi k}{n}) & -\sin(\frac{2\pi k}{n}) & 0 \\ \epsilon\sin(\frac{2\pi k}{n}) & \epsilon\cos(\frac{2\pi k}{n}) & 0 \\ 0 & 0 & \epsilon \end{pmatrix} \mid 0 \leq k < n, \epsilon \in \{\pm 1\} \right\},$$

welche, wieder aus Kardinalitätsgründen, schon die volle Gruppe ausschöpfen. Die Projektion auf den oberen Block dieser Matrix induziert den gewünschten Isomorphismus mit D_n, realisiert als 2-dimensionale *orthogonale* (!) Symmetriegruppe des regulären n-gons $R_n \subseteq \mathbb{R}^2$.

Zur Untersuchung der verbleibenden Symmetriegruppen verwenden wir das folgende allgemeine Prinzip: Aus der Wirkung einer Gruppe G auf einer Menge M erhalten wir einen Gruppenhomomorphismus

$$\varphi : G \to S_M.$$

Die Abbildung φ ist desweiteren genau dann injektiv (also insbesondere ein Isomorphismus auf ihr Bild), wenn die Wirkung der Gruppe *treu* ist, wenn also für alle $g \in G$ die Implikation

$$\forall x \in M : g.x = x \quad \Rightarrow g = 1$$

gilt.

Die angegebenen Isomorphismen ergeben sich nun (!) aus

- der Wirkung von $\mathrm{SO}(T)$ auf den Eckpunkten des Tetraeders T,
- der Wirkung von $\mathrm{SO}(W)$ auf der Menge der 4 Raumdiagonalen durch diagonal gegenüberliegende Eckpunkte,
- der Wirkung von $\mathrm{SO}(D)$ auf der Menge der 5 im Dodekaeder D "eingeschriebenen" Würfel. In unserer Koordinatisierung des Dodekaeders lässt sich einer dieser Würfel sofort erkennen: da nämlich

  $$\{(\pm 1, \pm 1, \pm 1)\} \subseteq D$$

  in D konvex ist, ist auch $W \subseteq D$. Die weiteren Würfel in D ergeben sich als Elemente der Bahn von W unter der Wirkung von $\mathrm{SO}(D)$ auf der Menge der Teilmengen von D. 12 der 24 Drehsymmetrien dieses Würfels sind auch Symmetrien des umgebenden Dodekaeders und bilden genau den Stabilisator von W. Daher gibt es nach der Bahnformel also 5 eingeschriebene Würfel in der Bahn von W.

Desweiteren gilt $\mathrm{SO}(W) \cong \mathrm{SO}(O)$ und $\mathrm{SO}(D) \cong \mathrm{SO}(I)$, denn diese Polytope sind *dual* zueinander: Der Oktaeder lässt sich als konvexe Hüller der Menge der Schwerpunkte der Randflächen des Würfels beschreiben und umgekehrt bildet die konvexe Hülle der Schwerpunkte der Randflächen eines Oktaeders einen Würfel. Da jede Drehsymmetrie des Würfels die Randflächen permutiert (und Abstände erhält), werden auch die Schwerpunkte ineinander überführt. Damit erhält die Drehsymmetrie also auch die konvexe Hülle der Schwerpunkte, so dass wir einen injektiven Homomorphismus

$$\mathrm{SO}(W) \to \mathrm{SO}(O)$$

erhalten, der aus Kardinalitätsgründen ein Isomorphismus sein muss. Alternativ kann man auch argumentieren, dass umgekehrt die konvexe Hülle der Flächenschwerpunkte des Oktaeders O einen Würfel W' bildet, welcher eine Skalarstreckung von W ist, und damit die selbe Symmetriegruppe hat.

Ein analoges Argument zeigt $\mathrm{SO}(D) \cong \mathrm{SO}(I)$, da Oktaeder und Ikosaeder dual zueinander sind. □

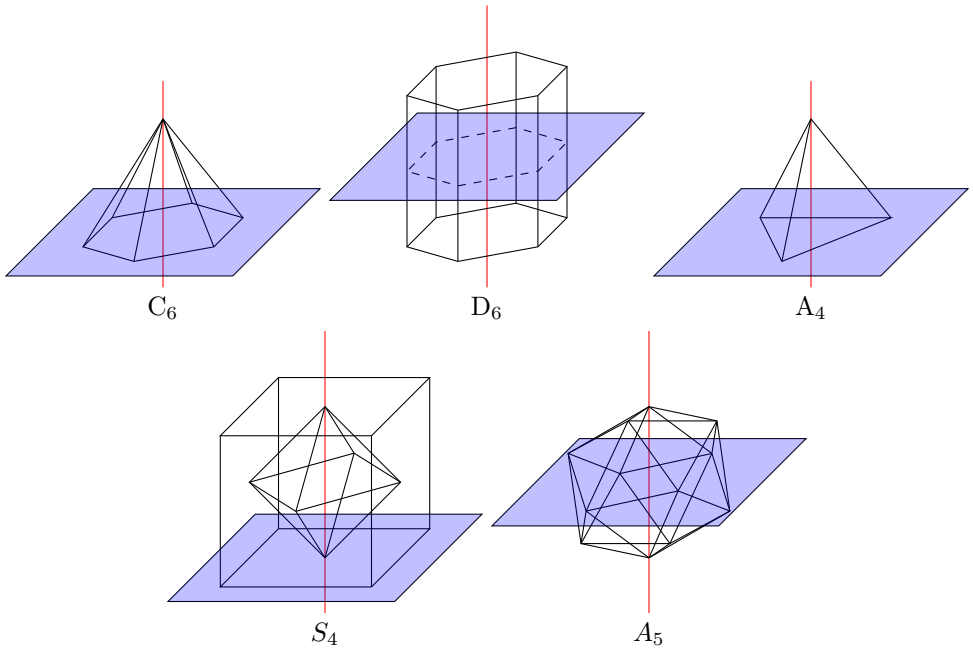


Abbildung 1.2: Klassifikation der Drehgruppe $\mathrm{SO}(3,\mathbb{R})$.

Satz 1.6.5. *Sei $G \leq \mathrm{SO}(3,\mathbb{R})$ eine endliche Untergruppe. Dann ist G konjugiert zu einer der folgenden Gruppen*

(a) der trivialen Gruppe $\{I\}$,

(b) der Drehgruppe der Pyramide P_n,

(c) der Drehgruppe des Zylinders Z_n,

(d) der Drehgruppe des Tetraeders T,

(e) der Drehgruppe des Würfels W (oder äquivalent des Oktaeders O),

(f) der Drehgruppe des Ikosaeders I (oder äquivalent des Dodekaeders D).

Bevor wir den Satz beweisen, halten wir ein Lemma für den Beweis fest.

Lemma 1.6.6. *Sei $0 \neq v \in \mathbb{R}^3$ und sei $\{I\} \neq H \leq \mathrm{SO}(3,\mathbb{R})$ eine endliche Untergruppe von Drehungen um die von v aufgespannte Achse. Dann ist H zyklisch, erzeugt von der Drehung um den Winkel $2\pi/k$ mit $k = |H|$.*

Beweis. Für $0 < \theta < 2\pi$ bezeichnen wir mit δ_θ die Drehung gegen den Uhrzeigersinn um die Achse v mit Winkel θ. Sei δ_θ die Drehung um den kleinsten Winkel $0 < \theta < 2\pi$ gegen den Uhrzeigersinn um v, welche in H enthalten ist. Wir zeigen zunächst $H = \langle \delta_\theta \rangle$. Denn wenn dies nicht so wäre, dann gäbe es $n \in \mathbb{N}$ und $0 < \alpha < 2\pi$, so dass $n\theta < \alpha < (n+1)\theta$ und $\delta_\alpha \in H$. Doch dann folgt

$$0 < \alpha - n\theta < \theta$$

und

$$\delta_{\alpha - n\theta} = \delta_\alpha \circ (\delta_\theta^n)^{-1} \in H$$

doch dies steht im Widerspruch zur Minimalität von θ. Nun folgt auch direkt $\theta = \frac{2\pi}{r}$ mit $r = |H|$, aus der Tatsache, dass θ minimal mit $\delta_\theta^r = 1$, $r > 0$ ist. □

Bemerkung 1.6.7. Indem wir die Gruppe der Drehmatrizen um die Achse

$$\begin{pmatrix}0\\0\\1\end{pmatrix}$$

mit der Gruppe $\mathrm{SO}(2,\mathbb{R})$ identifizieren, beinhaltet Lemma 1.6.6 insbesondere eine Klassifikation der endlichen Untergruppen von $\mathrm{SO}(2,\mathbb{R})$ in Analogie zur Aussage von Satz 1.6.5 für $\mathrm{SO}(3,\mathbb{R})$.

Beweis von Satz 1.6.5. Falls $G = \{I\}$, dann terminiert die Klassifikation mit Fall (a), so dass wir also von nun an annehmen, dass $N := |G| > 1$.

Wir führen zunachst etwas Terminologie für den Beweis ein: Nach Satz 1.5.14 korrespondiert jede Matrix $I \neq A \in \mathrm{SO}(3,\mathbb{R})$ zu einer Drehung um eine Achse, die wir als 1-dimensionalen Unterraum $L \subseteq \mathbb{R}^3$ beschreiben können. Die Elemente der 2-elementigen Menge

$$L \cap \{x \in \mathbb{R}^3 \mid ||x|| = 1\}$$

nennen wir die *Pole von A*. Wir bezeichnen weiterhin die Menge aller Pole aller Matrizen $I \neq A \in G$ mit P.

Schritt 1. Die Wirkung $G \curvearrowright \mathbb{R}^3$ durch Matrixmultiplikation schränkt sich ein auf eine Wirkung $G \curvearrowright P$.

Sei also $p \in P$ ein Pol zur Matrix $A \in G$ und $B \in G$ beliebig. Dann gilt

$$(BAB^{-1})Bp = Bp$$

so dass Bp also ein Pol von $BAB^{-1} \in G$ ist.

Schritt 2. Sei $p \in P$ und setze $n_p = |G.p|$ sowie $r_p = |G_p|$. Dann ergibt die Bahnformel

$$N = r_p n_p. \tag{1.6.8}$$

Schritt 3. Wir betrachten nun die Menge

$$X = \{(p, A) \mid p \in P,\ A \in G \text{ mit Pol } p\} \subseteq P \times G.$$

Einerseits gibt es zu jedem $I \neq A \in G$ genau zwei Pole, so dass also gilt

$$|X| = 2(N-1). \tag{1.6.9}$$

Andererseits ist die Menge der Matrizen in G mit vorgegebenem Pol $p \in P$ genau $G_p \setminus \{I\}$, so dass also auch gilt

$$|X| = \sum_{p \in P} (r_p - 1).$$

Wir stellen weiterhin fest, dass für $p' \in G.p$ gilt: $|G.p| = |G.p'|$, so dass sich die Summation weiter zusammenfassen lässt zu

$$|X| = \sum_{G.p \in G\backslash P} n_p(r_p - 1). \tag{1.6.10}$$

Aus (1.6.9) und (1.6.10) ergibt sich demnach die Identität

$$\sum_{G.p \in P} n_p(r_p - 1) = 2(N-1),$$

welche wir noch auf beiden Seiten durch N teilen, womit wir, unter Verwendung von (1.6.8), erhalten:

$$\sum_{G.p \in G\backslash P} \left(1 - \frac{1}{r_p}\right) = 2 - \frac{2}{N} \tag{1.6.11}$$

Schritt 4. Überraschenderweise führt die Formel (1.6.11) zu starken Restriktionen für die möglichen Konstellationen der Zahlen $|G\backslash P|$, $\{r_p\}$, $\{n_p\}$ und N. Es können nämlich nur die folgenden Möglichkeiten auftreten:

(I) Die Wirkung $G \curvearrowright P$ hat 2 Bahnen. In diesem Fall sind die Kardinalitäten der Stabilisatoren gegeben durch $r_1 = N$ und $r_2 = N$, sowie die Kardinalitäten der Bahnen durch $n_1 = 1$ und $n_2 = 1$, und N beliebig.

(II) Die Wirkung $G \curvearrowright P$ hat 3 Bahnen. Dann ergeben sich folgende Möglichkeiten für N, die Kardinalitäten n_1, n_2, n_3 der Bahnen, sowie die Kardinalitäten r_1, r_2, r_3 der zugehörigen Stabilisatoren:

Fall	(r_1, r_2, r_3)	(n_1, n_2, n_3)	N
(II.1)	$(2, 2, r)$	$(r, r, 2)$	$2r$
(II.2)	$(2, 3, 3)$	$(6, 4, 4)$	12
(II.3)	$(2, 3, 4)$	$(12, 8, 6)$	24
(II.4)	$(2, 3, 5)$	$(30, 20, 12)$	60

Zum Beweis stellen wir zunächst fest, dass alle Summanden auf der linken Seite von (1.6.11) echt größer als $\frac{1}{2}$ sind, denn $r_p \geq 2$. Doch damit kann es höchstens 3 Bahnen geben, denn die rechte Seite der Gleichung ist echt kleiner als 2.

(1) Nehmen wir an, es gibt genau eine Bahn. Dann ergibt (1.6.11) also

$$1 - \frac{1}{r} = 2 - \frac{2}{N},$$

wobei also die linke Seite kleiner als 1 und die rechte Seite größer oder gleich 1 ist. Widerspruch. Es muss also mindestens 2 Bahnen geben.

(2) Nehmen wir an, es gibt genau 2 Bahnen. Dann liest sich (1.6.11) als

$$1 - \frac{1}{r_1} + 1 - \frac{1}{r_2} = 2 - \frac{2}{N}$$

oder äquivalent

$$\frac{1}{r_1} + \frac{1}{r_2} = \frac{2}{N}.$$

Da $r_i \leq N$ folgt dann aber $r_1 = r_2 = N$. Daraus folgen nun natürlich $n_1 = n_2 = 1$, womit wir in Fall (I) sind.

(3) Nun bleibt also noch der Fall $|G\backslash P| = 3$. Hier erhalten wir aus (1.6.11)

$$1 - \frac{1}{r_1} + 1 - \frac{1}{r_2} + 1 - \frac{1}{r_3} = 2 - \frac{2}{N},$$

oder äquivalent

$$\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} - 1 = \frac{2}{N}.$$

Falls alle $r_i \geq 3$, dann ist die linke Seite kleiner oder gleich 0, ein Widerspruch, also gibt es $1 \leq i \leq 3$ mit $r_i = 2$. Wir nehmen o.E. an: $r_1 \leq r_2 \leq r_3$, so dass dann also $r_1 = 2$. Es folgt nun durch elementare Abschätzungen, dass die in (II) aufgelisteten Fälle tatsächlich die einzigen verbleibenden Möglichkeiten für (r_1, r_2, r_3) und N sind, so dass (1.6.11) erfüllt ist.

Es ist natürlich an dieser Stelle des Beweises nicht klar, dass alle diese möglichen Lösungen der Gleichung (1.6.11) auch tatsächlich von endlichen Untergruppen kommen – dies wird sich jedoch im weiteren Verlauf des Beweises bewahrheiten.

Schritt 5. Wir untersuchen nun die verschiedenen Fälle aus Schritt 4 genauer.

(I) Es gibt es also zwei Bahnen, die jeweils aus einem Pol bestehen. Also gilt $P = \{p, -p\}$ und $G = G_p$. Demnach ist G also eine endliche Untergruppe von Drehungen um die von p erzeugten Achse, nach Lemma 1.6.6 also eine zyklische Gruppe erzeugt von der Drehung in G um den kleinsten Winkel. Sei nun $C \in \mathrm{SO}(3, \mathbb{R})$

eine Drehung, welche den Standardbasisvektor e_3 von $\mathbb{R}^3$ auf p abbildet. Dann ist $C^{-1}GC$ die Drehgruppe der Pyraminde P_N.

(II.1) Es gilt $n_3 = 2$, die zugehörige Bahn hat also zwei Pole $\{p, p'\}$. Da p ein Pol ist, gibt es $I \neq A \in G$ mit $Ap = p$. Doch dann gilt auch $Ap' = p'$, denn $A.-$ induziert eine bijektive Selbstabbildung der Bahn $\{p, p'\}$. Also gilt $p' = -p$. Nach Lemma 1.6.6 ist G_p eine zyklische Gruppe der Ordnung $|r|$, erzeugt von der Drehung δ um die von p erzeugte Achse mit Winkel $\frac{2\pi}{r}$. Sei $\tau \in G \setminus G_p$. Dann vertauscht τ die Pole p und $-p$, ist also eine Drehung um eine zu p orthogonale Achse mit Winkel π. Es gilt $G = \langle \delta, \tau \rangle$ mit $\tau\delta\tau^{-1} = \delta^{-1}$, konjugiert zur Symmetriegruppe von Z_N via der Matrix $C \in \mathrm{SO}(3, \mathbb{R})$ aus (I).

(II.2) Es gilt $n_3 = 4$ und $r_3 = 3$. Sei

$$B = \{p_1, p_2, p_3, p_4\}$$

die zugehörige Bahn. Dann gilt $|G_{p_1}| = 3$ und der Stabilisator G_{p_1} besteht aus Drehungen um die Achse p_1. Daher (!) muss G_{p_1} nichttrivial auf $\{p_2, p_3, p_4\}$ wirken und demnach wegen der Bahnformel transitiv. Da G durch Bewegungen wirkt, müssen also die Skalarprodukte

$$\langle p_1, p_2 \rangle = \langle p_1, p_3 \rangle = \langle p_1, p_4 \rangle$$

erfüllen. Nun können wir dieses Argument aber für jeden der Indizes $1 \leq i \leq 4$ statt $i = 1$ wiederholen, und erhalten somit, dass alle Skalarprodukte zwischen beliebigen Polen p_i und p_j übereinstimmen. Damit müssen (Bilinearität des Skalarprodukts) auch alle Abstände

$$||p_i - p_j||$$

zwischen paarweise unterschiedlichen Polen gleich sein. Daher bilden also jeweils 3 der Pole ein gleichseitiges Dreieck, so dass B die Menge der Eckpunkte eines Tetraeders bildet. Die Gruppe G permutiert B und erhält daher auch die konvexe Hülle $\mathrm{Konv}(B)$, so dass $G \leq \mathrm{SO}(\mathrm{Konv}(B))$. Wie in Proposition 1.6.4, gilt $|\mathrm{SO}(\mathrm{Konv}(B))| = 12$ und daher $G = \mathrm{SO}(\mathrm{Konv}(B))$. Durch eine geeignete Drehung C können wir schließlich $\mathrm{Konv}(B)$ noch auf eine Streckung des Standardtetraeders T bewegen, so dass G via C konjugiert zu $\mathrm{Sym}(T)$ ist.

(II.3) Es gilt $n_3 = 6$ und $r_3 = 4$, sei also

$$B = \{p_1, p_2, ..., p_6\}$$

die zugehörige Bahn. Es gilt $|G_{p_1}| = 4$, wobei G_{p_1} aus Drehungen um p_1 besteht. Wegen der Bahnformel muss die Wirkung von G_{p_1} auf $B \setminus \{p_1\}$ einen Fixpunkt haben, o.E. sei dies p_2. Dann muss aber $p_2 = -p_1$ gelten und die Wirkung von G_{p_1} auf $\{p_3, p_4, p_5, p_6\}$ ist transitiv: G_{p_1} ist erzeugt von einer Drehung um $\pi/2$, daher hat jede Bahn, die nicht einelementig ist, Kardinalität 4. Nach obigem Argument muss mit p_3 auch $-p_3 \in B$ sein, daher gilt also o.E. $p_5 = -p_3$ und $p_6 = -p_4$. Es folgt nun, dass die Pole p_3, p_4, p_5 und p_6 die Eckpunkte eines Quadrats in der Ebene senkrecht zur Achse durch p_1 und $-p_1$ bilden. Anders formuliert bildet B die Menge der Schwerpunkte der Flächen eines Würfels. Mit dem analogen Argument zu (II.2) ist G damit konjugiert zu $\mathrm{Sym}(W)$.

(II.4) Es gilt $n_3 = 12$ und $r_3 = 5$, wir betrachten die zugehörige Bahn

$$B = \{p, -p, x_1, x_2, ..., x_5, y_1, y_2, ..., y_5\}$$

wobei $-p \in B$ wie in (II.3). G_p fixiert neben p und $-p$ keine weiteren Pole mehr, so dass die Wirkung von G_p in die beiden Bahnen $\{x_1, x_2, ..., x_5\}$ und $\{y_1, y_2, ..., y_5\}$ zerfällt. Indem wir das selbe Argument für x_1 statt p wiederholen, muss also $-x_1 \in B$ gelten, es kann aber nicht sein, dass $-x_1 = x_i$, also $-x_1 = y_i$, o.E. $-x_1 = y_1$. Indem wir dieses Argument wiederholen, gilt o.E. $y_i = -x_i$. Es kann nicht sein, dass alle x_i senkrecht auf p stehen, denn dann wären die beiden Pole p und $-p$ dadurch ausgezeichnet, dass sie auf allen anderen Polen senkrecht stehen. Dies kann aber nicht sein, denn statt p und $-p$ hätten wir genauso x_1 und $-x_1$ wählen können. Daher gilt also

$$\langle p, x_1 \rangle \neq 0$$

und

$$\langle p, -x_1 \rangle = -\langle p, x_1 \rangle.$$

Durch vertauschen von x_i und y_i können wir o.E. annehmen, dass

$$\langle p, x_1 \rangle > 0$$

so dass p und x_1 also einen spitzen Winkel bilden. Es gilt weiter, für alle $1 \leq i \leq 5$, da G_p via Bewegungen operiert

$$\langle p, x_i \rangle = \langle p, x_1 \rangle,$$

woraus folgt, dass alle Abstände $||p - x_i||$ gleich sind. Indem wir die obige Argumentation auf einen beliebigen anderen Pol $q \in B$ statt p anwenden, folgt also, dass die Abstände von q zu den 5 weiteren Polen in B welche mit q einen spitzen Winkel bilden, gleich sind. Es folgt, dass q, gemeinsam mit diesen 5 benachbarten Polen, die Eckpunkte von 5 gleichseitigen Dreiecken bildet, die sich in q treffen. Es gibt 12 Punkte in B, so dass diese Punkte zusammen also die Eckpunkte von

$$\frac{12 \cdot 5}{3} = 20$$

gleichseitigen Dreiecken bilden. Die konvexe Hülle von B ist also ein Ikosaeder (vgl. Bastelanleitung des Ikosaeders). Der Rest des Arguments ist analog wie oben, wobei wir die elementargeometrische Aussage verwenden, dass sich jedes Ikosaeder auf eine Streckung des Standardikosaeders I drehen lässt.

□

Kapitel 2

Ringe

2.1 Ringe, Ideale, Homomorphismen

Definition 2.1.1. Ein *Ring* ist ein Tupel $(R, +, \cdot)$ bestehend aus einer Menge R und Abbildungen

$$+ : R \times R \to R \quad \cdot : R \times R \to R,$$

so dass die folgenden Bedingungen gelten:

(1) Das Paar $(R, +)$ ist eine abelsche Gruppe.

(2) Für $a, b, c \in R$ gelten

$$\begin{aligned} a \cdot (b \cdot c) &= (a \cdot b) \cdot c, \\ (a + b) \cdot c &= a \cdot c + b \cdot c, \\ a \cdot (b + c) &= a \cdot b + a \cdot c. \end{aligned}$$

(3) Es gibt $1 \in R$, so dass für alle $a \in R$ gilt

$$a \cdot 1 = 1 \cdot a = a.$$

Falls zusätzlich, für alle $a, b \in R$, gilt: $a \cdot b = b \cdot a$, heißt der Ring *kommutativ*.

Beispiele 2.1.2. (1) Der *Nullring* $\{0\}$ ist ein Ring. Insbesondere fordern wir in Definition 2.1.1 nicht $1 \neq 0$, der Nullring ist jedoch der einzige Ring mit dieser Eigenschaft.

(2) Die ganzen Zahlen $\mathbb{Z}$ mit Addition und Multiplikation bilden einen kommutativen Ring.

(3) Jeder Körper bildet einen kommutativen Ring.

(4) Für $\alpha \in \mathbb{C}$ ist die Menge

$$\mathbb{Z}[\alpha] := \left\{ \sum_{k=0}^{n} \lambda_k \alpha^k \mid n \geq 0, \lambda_k \in \mathbb{Z} \right\} \subseteq \mathbb{C}$$

abgeschlossen unter Addition und Multiplikation in $\mathbb{C}$ und bildet, durch Vererbung aller Axiome von $\mathbb{C}$, einen kommutativen Ring. Besonders interessant für die Zahlentheorie ist der Fall, wenn α eine *ganze algebraische Zahl* ist, wenn α also Nullstelle eines monischen Polynoms

$$X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + ... + a_0$$

mit ganzzahligen Koeffizienten $a_i \in \mathbb{Z}$ ist. Zum Beispiel ist die imaginäre Zahl i als Nullstelle des Polynoms $X^2 + 1$ eine ganze algebraische Zahl und erzeugt den Ring

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

der sogenannten *Gaußschen Zahlen*.

(5) Für einen Ring R bildet die Menge $R[X]$ der Polynome in der Variablen X mit Koeffizienten in R einen Ring.

(6) Die Quaternionen $\mathbb{H}$ bilden einen nichtkommutativen Ring. Jedes $q \in \mathbb{H} \setminus \{0\}$ besitzt ein multiplikatives Inverses, daher sagt man auch, die Quaternionen bilden einen *Schiefkörper*.

(7) Für jeden Körper K bildet die Menge $M(n, K)$ der $n \times n$-Matrizen einen Ring mit komponentenweiser Addition und Matrixmultiplikation.

(8) Für Ringe R, S bildet das kartesische Produkt $R \times S$ einen Ring mit komponentenweiser Addition und Multiplikation.

Ein paar historische Kommentare sind hilfreich für die Einordnung der in diesem Kapitel entwickelten Theorie. Der Begriff eines Rings, sowie Begriffe wie Ideale und Moduln (siehe unten), wurden von Dedekind im 19. Jhd. eingeführt, um Verallgemeinerungen des Primzahlbegriffs und zugehörige Primfaktorzerlegungen für ganze algebraischen Zahlen zu untersuchen.

Wir beschreiben hier exemplarisch einige Phänomene, die bei hierbei zum Vorschein kommen, die Beweise und präzisen Begriffe werden später nachgeliefert. Zum Beispiel zerfällt die Primzahl 2 im Ring $\mathbb{Z}[i]$ in ein Produkt

$$(1+i)(1-i) = 2,$$

welches dort eine Zerlegung in "Primfaktoren" bildet. Die Tatsache, dass es im Ring $\mathbb{Z}[i]$ immer noch eindeutige Primfaktorzerlegungen gibt, hat direkte zahlentheoretische Konsequenzen. Dies liefert z.B. einen sehr eleganten Beweis des folgenden klassischen Resultats:

Satz 2.1.3. *Eine ganze Zahl n ist genau dann die Summe $a^2 + b^2$ zweier Quadrate mit $a, b \in \mathbb{Z}$, wenn jeder Primfaktor $p|n$ mit $p \equiv 3 \pmod 4$ mit gerader Vielfachheit in der Primfaktorzerlegung vorkommt.*

Umgekehrt gibt es algebraische Zahlringe, in denen die Eindeutigkeit der Primzahlzerlegung fehlschlägt. Zum Beispiel werden wir sehen, dass die Zahl 6 im Ring $\mathbb{Z}[\sqrt{-5}]$ die unterschiedlichen Primfaktorzerlegungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

besitzt. Im Jahre 1847 stellte Gabriel Lamé einen vermeintlichen Beweis von Fermats letztem Satz vor, der auf der (im allgemeinen falschen!) Annahme basierte, dass es im Ring der *Kreisteilungszahlen*, nämlich $\mathbb{Z}[\zeta_n]$ mit $\zeta_n = e^{\frac{2\pi i}{n}}$, eine eindeutige Primfaktorzerlegung gibt.

Es ist eine der bahnbrechenden Erkenntnisse der algebraischen Zahlentheorie des 19. Jahrhunderts, dass sich diese Problematik auflöst, wenn wir von Zahlen zu Idealen übergehen. Die Idee hierfür geht auf Kummer zurück, der den informellen Begriff einer "idealen Zahl" einführte. Der eigentliche Begriff des Ideals wurde schließlich von Dedekind definiert.

Konvention 2.1.4. Wir wollen uns nun auf das Studium von kommutativen Ringen konzentrieren. Unter einem Ring verstehen wir von nun an implizit immer einen kommutativen Ring. Nichtkommutative Ringe werden wir explizit als solche benennen.

Definition 2.1.5. Eine Teilmenge

$$\emptyset \neq I \subseteq R$$

eines Rings R heißt *Ideal*, falls gelten:

(1) für alle $x, y \in I$ gilt $x + y \in I$,

(2) für $r \in R$ und $x \in I$ gilt $rx \in I$.

Beispiel 2.1.6. Sei R ein Ring und $x \in R$. Dann bildet

$$(x) := Rx = \{rx \mid r \in R\} \subseteq R$$

ein Ideal, genannt das von x erzeugte *Hauptideal*. Allgemeiner ist für eine Teilmenge $M \subseteq R$

$$(M) := \bigcap_{\substack{M \subseteq I \subseteq R \\ I \text{ Ideal}}} I$$

ein Ideal, genannt das von M erzeugte Ideal.

Jeder vom Nullring verschiedene Ring R besitzt mindestens zwei verschiedene Ideale, nämlich $\{0\}$ und R selbst.

Proposition 2.1.7. *Ein Ring R ist genau dann ein Körper, wenn R genau zwei verschiedene Ideale besitzt (nämlich $\{0\}$ und R).*

Beweis. Sei R ein Körper und $\{0\} \neq I \subseteq R$ ein Ideal. Wähle $0 \neq x \in I$. Dann gilt $x^{-1}x = 1 \in I$ und damit auch für jedes $r \in R$: $r \cdot 1 = r \in I$. Also $I = R$ wie behauptet. Sei umgekehrt R ein Ring mit einzigen Idealen $\{0\}$ und R. Für $0 \neq x \in R$ gilt für das Hauptideal $(x) \subseteq R$ demnach $(x) = R$. Doch damit muss es $r \in R$ geben mit $rx = 1$, so dass R also ein Körper ist. □

Definition 2.1.8. Eine Abbildung $\varphi : R \to S$ von Ringen heißt (Ring-)Homomorphismus, falls:

(1) für alle $r_1, r_2 \in R$ gelten:

   (a) $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$,

   (b) $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$,

(2) $\varphi(1) = 1$.

Beispiel 2.1.9. Sei R ein Ring, $R[X]$ der Polynomring über R, und $\alpha \in R$. Dann ist die Abbildung

$$\mathrm{ev}_\alpha : R[X] \to R, f \mapsto f(\alpha)$$

ein Ringhomomorphismus, genannt *Evaluationshomomorphismus*.

Proposition 2.1.10. *Sei $\varphi : R \to S$ ein Homomorphismus von Ringen. Dann gelten:*

(1) $\mathrm{Bild}(\varphi) \subseteq S$ *ist ein Unterring.*

(2) $\mathrm{Kern}(\varphi) \subseteq R$ *ist ein Ideal.*

Beweis. (1) ist klar. Um (2) zu zeigen, rechnen wir: Für $x, y \in \mathrm{Kern}(\varphi)$ gilt $\varphi(x+y) = \varphi(x)+\varphi(y) = 0+0 = 0$ und, für $r \in R$, $\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r)0 = 0$. □

Korollar 2.1.11. *Sei K ein Körper, S ein Ring, und $\varphi : K \to S$ ein Ringhomomorphismus. Dann ist φ entweder injektiv, oder $S = \{0\}$.*

Beweis. Die einzigen Ideale von K sind $\{0\}$ und K. Zudem gilt $\varphi(1) = 1$ und in jedem Ring $S \neq \{0\}$ gilt $1 \neq 0$. □

Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann definiert (!)

$$r_1 \sim r_2 \ :\Leftrightarrow\ r_1 - r_2 \in I$$

eine Äquivalenzrelation auf R. Die Äquivalenzklasse eines Elements $r \in R$ hat die Gestalt

$$[r] = \{r + x \mid x \in I\}.$$

Wir bezeichnen die Menge der Äquivalenzklassen mit R/I.

Proposition 2.1.12. *Sei R ein Ring und $I \subseteq R$ ein Ideal.*

(1) Die Verknüpfungen

$$+ :\ R/I \times R/I \to R/I, ([r_1], [r_2]) \mapsto [r_1 + r_2]$$

und

$$\cdot :\ R/I \times R/I \to R/I, ([r_1], [r_2]) \mapsto [r_1 \cdot r_2]$$

definieren eine Ringstruktur auf R/I, genannt der Quotientenring von R modulo I.

(2) Die Abbildung

$$\pi : R \to R/I, r \mapsto [r]$$

ist ein surjektiver Ringhomomorphismus mit $\mathrm{Kern}(\pi) = I$.

Beweis. Dies sollte nun Routine sein. □

Beispiele 2.1.13. (1) Sei $n \geq 2$ eine natürliche Zahl. Dann heißt der Ring $\mathbb{Z}/(n)$ der *Restklassenring modulo n*.

(2) Sei R ein vom Nullring verschiedener Ring. Wir erklären auf $R \times (R \setminus \{0\})$ die Äquivalenzrelation $(a, b) \sim (c, d) : \iff ad = cb$ und schreiben $\frac{a}{b}$ für eine Äquivalenzklasse $[(a, b)]$. Auf Äquivalenzklassen definieren wir wie gewohnt Addition durch

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$$

und Multiplikation durch

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

Die Quotientenmenge $(R \setminus \{0\})^{-1}R := R \times (R \setminus \{0\})/_\sim$ heißt *Quotientenkörper* oder *Körper der Brüche* von R. Dies ist ein Spezialfall der in den Übungen untersuchten *Lokalisierung* von Ringen. Man überzeuge sich davon, dass tatsächlich ein Körper vorliegt (!).

Satz 2.1.14. *Sei $\varphi : R \to S$ ein Homomorphismus von Ringen. Dann ist*

$$\overline{\varphi} : R/\mathrm{Kern}(\varphi) \to \mathrm{Bild}(\varphi), [r] \mapsto \varphi(r)$$

ein wohldefinierter Ringisomorphismus.

Beweis. Ähnlich wie für Gruppen (!). □

2.2 Primelemente und Primideale

Für Elemente $a, b \in R$ eines Rings R schreiben wir $a|b$ und sagen a *teilt* b, falls es ein $r \in R$ gibt, so dass $b = ar$. Teilbarkeit lässt sich in Termen von Idealen ausdrücken, denn es gilt

$$a|b \quad \Leftrightarrow \quad b \in (a) \quad \Leftrightarrow \quad (b) \subseteq (a).$$

Ganz allgemein können wir also einen Teilbarkeitsbegriff für Ideale definieren als:

$$I|J \quad :\Leftrightarrow \quad J \subseteq I.$$

Wir untersuchen weitere derartige Beziehungen zwischen element- und idealtheoretischen Begriffen.

Terminologie 2.2.1. Sei R ein Ring.

(1) Ein Element $u \in R$ heißt *Einheit*, falls es $v \in R$ gibt mit $uv = 1$. Die Einheiten von R bilden eine Gruppe unter Multiplikation, bezeichnet mit $R^\times$.

(2) Ein Element $0 \neq p \in R$ mit $p \notin R^\times$ heißt *Primelement*, falls für alle $a, b \in R$ gilt:

$$p|ab \quad \Rightarrow p|a \text{ oder } p|b.$$

Beispiel 2.2.2. Die Gruppe der Einheiten in $\mathbb{Z}$ ist $\mathbb{Z}^\times = \{1, -1\}$ und die Primelemente sind genau die Zahlen der Form $\pm p$ für p Primzahl.

Proposition 2.2.3. *Die Einheiten im Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen bilden die Gruppe*

$$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$$

der vierten Einheitswurzeln in $\mathbb{C}$.

Beweis. Wir bestimmen die Gruppe der Einheiten in $\mathbb{Z}[i]$. Dazu definieren wir, für $\alpha = a + ib \in \mathbb{Z}[i]$, die *Norm*

$$N(\alpha) := (a + ib)(a - ib) = a^2 + b^2 \in \mathbb{N}.$$

Die Norm ist multiplikativ, für $u, v \in \mathbb{Z}[i]$ mit $uv = 1$ gilt also $N(u)N(v) = N(uv) = 1$. Die einzige Gaußsche Zahl mit Norm kleiner als 1 ist 0. Daher muss also jede Einheit die Norm 1 haben. Umgekehrt ist aber jede Gaußsche Zahl der Norm 1 eine Einheit, denn ihr komplex Konjugiertes ist ein Inverses. Die Gaußschen Zahlen der Norm 1 sind genau die vierten Einheitswurzeln. □

Definition 2.2.4. Sei R ein Ring. Ein Ideal $P \subsetneq R$ heißt *Primideal*, falls für alle $x, y \in R$ gilt:

$$x \cdot y \in P \quad \Rightarrow \quad x \in P \text{ oder } y \in P.$$

Proposition 2.2.5. *Sei R ein Ring.*

(1) Ein Element $a \in R$ ist genau dann eine Einheit, wenn $(a) = R$.

(2) Ein Element $0 \neq a \in R$ ist ein Primelement genau dann, wenn $(a) \subseteq R$ ein Primideal ist.

Beweis. Folgt direkt aus den Definitionen (!). □

Aufgabe 2.2.6. Sei R ein Ring. Für Ideale I, J definieren wir das Ideal

$$I \cdot J = (\{xy \mid x \in I, y \in J\}).$$

Dann ist $P \subseteq R$ genau dann ein Primideal, wenn für alle Ideale $I, J \subseteq R$ gilt:

$$P | I \cdot J \quad \Leftrightarrow \quad P | I \text{ oder } P | J.$$

Definition 2.2.7. Ein Ring R heißt *nullteilerfrei* oder *Integritätsbereich*, falls $R \neq \{0\}$ und für alle $r, s \in R$ gilt:

$$r \cdot s = 0 \quad \Rightarrow \quad r = 0 \text{ oder } s = 0.$$

Proposition 2.2.8. *Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann sind äquivalent:*

(i) R/I nullteilerfrei.

(ii) I ist ein Primideal.

Beweis. Folgt direkt aus den Definitionen (!). □

Terminologie 2.2.9. Ein Element $0 \neq r \in R$ mit $r \notin R^\times$ heißt *unzerlegbar*, oder *irreduzibel*, falls für alle $a, b \in R$ mit $r = ab$ gilt: $a \in R^\times$ oder $b \in R^\times$.

Beispiel 2.2.10. Jedes Primelement $r \in R$ eines nullteilerfreien Rings R ist unzerlegbar. Denn aus $r = ab$ folgt $r|a$ oder $r|b$. Sei ohne Einschränkung $r|a$, dann gibt es also ein $t \in R$ mit $a = rt$, so dass gilt: $r = rtb$. Daraus folgt wegen der Nullteilerfreiheit aber $tb = 1$, so dass b also eine Einheit ist.

Proposition 2.2.11. *Sei R ein nullteilerfreier Ring. Dann sind für ein Element $0 \neq r \in R$ äquivalent:*

(i) r ist unzerlegbar.

(ii) (r) ist maximal unter den echten Hauptidealen von R.

Beweis. Sei r unzerlegbar und sei $(r) \subseteq (b) \subseteq R$. Dann gibt es also $a \in R$ mit $r = ab$. Doch daraus folgt $a \in R^\times$ oder $b \in R^\times$. Im ersten Fall gilt $(b) = (r)$, im zweiten Fall ist $(b) = R$ kein *echtes* Hauptideal.

Gelte umgekehrt (ii) und sei $r = ab$ eine Zerlegung. Dann gilt

$$(r) \subseteq (b) \subseteq R$$

so dass also entweder gilt $(b) = R$ oder $(b) = (r)$. Im ersten Fall ist $b \in R^\times$. Im zweiten Fall gibt es also $u \in R$ mit $b = ur$. Dann gilt aber $r = aur$ und es folgt, da R nullteilerfrei ist, $1 = au$. In diesem Fall ist also a eine Einheit, so dass r unzerlegbar ist. □

Definition 2.2.12. Sei R ein Ring. Ein Ideal $I \subsetneq R$ heißt *maximal*, falls I maximal unter den echten Idealen von R ist, falls also für jedes Ideal $J \subsetneq R$ mit $I \subseteq J$ gilt: $I = J$.

Proposition 2.2.13. *Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann sind äquivalent:*

(i) R/I Körper.

(ii) $I \subsetneq R$ maximal.

Beweis. Sei zunächst R/I ein Körper und sei $J \subseteq R$ ein Ideal mit $I \subsetneq J$. Wir zeigen nun, dass $J = R$ gilt. Sei nämlich $x \in J \setminus I$. Dann ist die Restklasse $[x] \neq 0$ und besitzt damit also ein multiplikatives Inverses $[r]$. Wegen $[rx] = [1]$ gilt also $rx - 1 \in I$ und demnach auch $1 \in I$.

Sei umgekehrt $I \subsetneq R$ ein maximales Ideal und sei $0 \neq [x] \in R/I$. Dann gilt also $x \notin I$ und damit ist $(I \cup \{x\}) \subseteq R$ ein Ideal, welches echt größer als I ist. Daher also $(I \cup \{x\}) = R$. Also gibt es $y \in I$ und $r \in R$ so dass $1 = y + rx$ und demnach $[r][x] = 1$. □

Korollar 2.2.14. *Jedes maximale Ideal ist ein Primideal.*

Beispiel 2.2.15. Sei K ein Körper und $K[X,Y] := (K[X])[Y]$ der Polynomring in den Variablen X und Y. Die Gruppe der Einheiten ist $K[X,Y]^\times = K^\times$, die multiplikative Gruppe des Körpers K. Das Ideal $(Y) \subseteq K[X,Y]$ ist der Kern des Evaluationshomomorphimus

$$K[X,Y] \to K[X], f(X,Y) \mapsto f(X,0),$$

so dass der Homomorphiesatz einen Isomorphismus $K[X,Y]/(Y) \cong K[X]$ liefert. Dieser Ring ist ein Integritätsbereich, so dass also (Y) ein Primideal ist. Daher ist Y ein Primelement und damit auch unzerlegbar.

Nach Proposition 2.2.11 ist damit das Ideal (Y) maximal unter den echten *Hauptidealen* in $K[X,Y]$. Aber (Y) kann nicht maximal unter den *Idealen* sein, denn nach Proposition 2.2.13 müsste sonst der Quotientenring $K[X,Y]/(Y)$ ein Körper sein. In der Tat sieht man dies sofort ein, denn

$$(Y) \subseteq (X,Y) \subseteq K[X,Y].$$

Der Evaluationshomomorphismus

$$K[X,Y] \to K, f(X,Y) \mapsto f(0,0)$$

induziert einen Isomorphismus $K[X,Y]/(X,Y) \cong K$, so dass das Ideal (X,Y) nun tatsächlich ein maximales Ideal ist. Als Randnotiz sei hier vermerkt, dass, für einen algebraisch abgeschlossenen Körper K, die Ideale der Form $(X-a, Y-b)$, $a \in K$, $b \in K$, genau die maximalen Ideale von $K[X,Y]$ sind. Dies ist der berühmte *Hilbertsche Nullstellensatz*, ein fundamentales Resultat der algebraischen Geometrie, welches wir in dieser Vorlesung (leider) nicht beweisen werden.

Wir untersuchen nun eine Klasse von Ringen, in denen der in Beispiel 2.2.15 erklärte Unterschied zwischen maximalen Hauptidealen und maximalen Idealen per Definition verschwindet:

Definition 2.2.16. Ein nullteilerfreier Ring R heißt *Hauptidealring*, falls jedes Ideal ein Hauptideal ist.

Proposition 2.2.17. *Sie R ein Hauptidealring. Dann sind für $r \in R$ äquivalent:*

(i) r ist unzerlegbar.

(ii) r ist ein Primelement.

Beweis. Dass jedes Primelement auch unzerlegbar ist, gilt nach Proposition 2.2.8 schon in nullteilerfreien Ringen. Sei also nun $r \in R$ unzerlegbar. Dann ist nach Proposition 2.2.11 das Ideal (r) maximal unter den Hauptidealen, was aber in einem Hauptidealring natürlich auch heißt, dass (r) ein maximales Ideal ist. Daher ist (r) also nach Korollar 2.2.14 ein Primideal und daher auch r selbst wegen Proposition 2.2.5 ein Primelement. □

Eine wichtige Klasse von Beispielen für Hauptidealringe erschließt sich aus Ringen, in denen es eine sinnvolle "Division mit Rest" gibt:

Definition 2.2.18. Ein Integritätsbereich R heißt *Euklidisch*, falls es eine Abbildung

$$\lambda : R \setminus \{0\} \to \mathbb{N}$$

mit der folgenden Eigenschaft gibt: Für alle $a, b \in R$ mit $b \neq 0$ gibt es Elemente $q, r \in R$, so dass

$$a = qb + r,$$

wobei entweder $r = 0$ oder $\lambda(r) < \lambda(b)$.

Satz 2.2.19. *Jeder Euklidische Ring ist ein Hauptidealring.*

Beweis. Sei $\{0\} \neq I \subseteq R$ ein Ideal. Sei $0 \neq x \in I$ mit $\lambda(x)$ minimal (Wohlordnung von $\mathbb{N}$). Für $y \in I$ beliebig gibt es nun ein $q \in R$ und $r \in R$, so dass

$$y = qx + r$$

wobei entweder $r = 0$ oder $\lambda(r) < \lambda(x)$. Doch da $r \in I$ ist, kommt wegen der Minimalität von x nur $r = 0$ in Frage. Damit gilt $y = qx$, also $I = (x)$. □

Proposition 2.2.20. *(1) Der Ring $\mathbb{Z}$ ist ein Euklidischer Ring mit $\lambda(n) = |n|$.*

(2) Der Polynomring $K[X]$ über einem Körper (!) K ist ein Euklidischer Ring, wobei $\lambda(f)$ der Grad von f ist.

(3) Der Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen ist ein Euklidischer Ring mit

$$\lambda(a + bi) := N(a + bi) = a^2 + b^2.$$

Beweis. Die Beispiele (1) und (2) sind aus der Schulmathematik bekannt unter "Division mit Rest" und "Polynomdivision". Wir beschränken uns hier daher auf den Beweis von (3). Zu gegebenen Gaußschen Zahlen α und $\beta \neq 0$ müssen wir also $q, r \in \mathbb{Z}[i]$ finden mit

$$\alpha = q\beta + r,$$

wobei entweder $r = 0$ oder $N(r) < N(\beta)$. Wir betrachten die komplexe Zahl $z := \frac{\alpha}{\beta} \in \mathbb{C}$. Falls $z \in \mathbb{Z}[i]$, dann setzen wir $q = z$ und $r = 0$. Andernfalls liegt die Zahl z in einer der quadratischen Maschen, in die das *Gitter* $\mathbb{Z}[i] \subseteq \mathbb{C}$ die komplexe Zahlenebende unterteilt. Es genügt nun (!) ein $q \in \mathbb{Z}[i]$ zu finden, so dass gilt

$$\left| \frac{\alpha}{\beta} - q \right| < 1. \tag{2.2.21}$$

Doch dies ist immer möglich, denn der größtmögliche Abstand eines Punktes im Quadrat zum nächsten Eckpunkt ist $\sqrt{2}/2 < 1$, realisiert vom Mittelpunkt. □

Beispiel 2.2.22. Wir sind nun in der Lage alle Primideale des Rings $\mathbb{Z}$ zu bestimmen. Diese bestehen nämlich aus dem Nullideal (0) zusammen mit den Idealen (p), p Primzahl.

Wir werden nun den von den ganzen Zahlen wohlbekannten Begriff der Primfaktorzerlegung verallgemeinern. Dabei nennen wir Elemente a, b eines Integritätsbereichs R *assoziiert*, wenn sie sich um einen Einheitenfaktor unterscheiden, es also eine Einheit $u \in R^\times$ gibt, so dass $a = ub$. Wir schreiben dann $a \sim b$.

Bemerkung 2.2.23. Elemente a, b eines Integritätsbereichs sind genau dann assoziiert, wenn $(a) = (b)$.

Definition 2.2.24. Ein Integritätsbereich R heißt faktoriell, falls für jede Nichteinheit $a \in R$ mit $a \neq 0$ gilt:

(1) Es gibt eine Faktorzerlegung

$$a = p_1 p_2 \cdots p_m \tag{2.2.25}$$

in unzerlegbare Faktoren.

(2) Falls $a = p_1 p_2 \cdots p_m$ und $a = q_1 q_2 \cdots q_n$ Faktorzerlegungen mit unzerlegbaren Faktoren sind, dann gelten

1. $m = n$, und
2. nach geeigneter Umnumerierung der Faktoren gilt, für alle $1 \leq i \leq m$: $p_i \sim q_i$.

Proposition 2.2.26. *Sei R ein Integritätsbereich in dem jede Nichteinheit $a \neq 0$ eine Faktorzerlegung in irreduzible Faktoren wie in Definition 2.2.24(1) besitzt. Dann sind äquivalent:*

(i) R ist faktoriell.

(ii) Jedes unzerlegbare Element ist ein Primelement.

Beweis. Sei zunächst R faktoriell. Sei $r \in R$ unzerlegbar und $a, b \in R$ mit $r|ab$. Dann gibt es also $t \in R$ mit $ab = tr$. Nach Zerlegung aller Faktoren in unzerlegbare Faktoren erhalten wir

$$a_1 \cdots a_m b_1 \cdots b_n = t_1 \cdots t_k r$$

und damit weiter, dass gelten muss $r \sim a_i$, für ein $1 \leq i \leq m$, oder $a \sim b_j$, für ein $1 \leq j \leq n$. Im ersten Fall gilt also $r|a$, im zweiten Fall $r|b$.

Sei nun umgekehrt jedes unzerlegbare Element ein Primelement und seien

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

Zerlegungen in unzerlegbare Faktoren mit $m \leq n$. Da p_1 ein Primelement ist, teilt p_1 also (!) einen der Faktoren q_i, $1 \leq i \leq n$, ohne Einschränkung sei dies q_1. Doch q_1 ist unzerlegbar, also muss gelten $p_1 \sim q_1$. Wir kürzen p_1 und erhalten

$$p_2 \cdots p_m = q_2' \cdots q_n$$

wobei $q_2' \sim q_2$. Durch Induktion über m reduzieren wir also auf den Fall $m = 1$. In diesem Falle gilt

$$p_1 = q_1 \cdots q_n,$$

doch da p_1 unzerlegbar ist und alle q_i Nichteinheiten sind, muss also $n = 1$ und $p_1 = q_1$ gelten. □

Satz 2.2.27. *Jeder Hauptidealring ist faktoriell.*

Beweis. Wir müssen wegen Proposition 2.2.17 und Proposition 2.2.26 lediglich die Existenz einer Zerlegung in unzerlegbare Faktoren nachweisen. Angenommen es gibt eine Nichteinheit $a \in R$, die keine solche Zerlegung besitzt. Dann ist insbesondere a zerlegbar, lässt sich also schreiben als $a = x_1 y_1$ wobei x_1, y_1 Nichteinheiten in R sind. Nun muss wiederum x_1 oder y_1 keine Zerlegung in unzerlegbare Faktoren haben, ohne Einschränkung x_1. Es gibt also wiederum eine Zerlegung $x_1 = x_2 y_2$. Wir erhalten so eine Folge

$$(x_1) \subsetneq (x_2) \subsetneq \cdots \subsetneq R \tag{2.2.28}$$

von Idealen $(x_i) \subsetneq (x_{i+1})$, $i \geq 0$, von echten Idealinklusionen. Die Vereinigung

$$\bigcup_{i \geq 0} (x_i) \subseteq R$$

ist ein Ideal (!) and damit ein Hauptideal, also von der Form (b) für $b \in R$. Dann muss es aber ein $j \geq 1$ geben, so dass $b \in (x_j)$, also $(b) = (x_j)$. Dies impliziert dann auch für alle $i > j$ die Gleichheit $(b) = (x_i)$. Doch die Idealinklusionen in (2.2.28) sind echt, also ein Widerspruch. □

Bemerkung 2.2.29. Das Argument aus dem Beweis von Satz 2.2.27 zeigt, dass jeder Hauptidealring R die folgende Eigenschaft hat: Für jede aufsteigende Kette

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_k \subseteq R$$

von Idealen in R gibt es ein $k_0 \geq 1$, so dass für alle $k \geq k_0$ gilt: $I_k = I_{k_0}$. Wir sagen auch: Jede aufsteigende Kette von Idealen wird *stationär*. Ringe mit dieser Eigenschaft heißen *Noethersch*, zu Ehren der Mathematikerin Emmy Noether. Wie unser Beweis zeigt, gilt die Existenz einer Zerlegung in ein Produkt von unzerlegbaren Elementen allgemeiner in Noetherschen Ringen (nicht notwendigerweise aber die Eindeutigkeit bis auf Assoziierte).

Wir wollen nun zum Abschluss eine vollständige Klassifikation der Primelemente und damit, nach Proposition 2.2.20, auch der Primideale, in $\mathbb{Z}[i]$ durchführen. Zentral ist dafür folgender Begriff:

Definition 2.2.30. Sei R ein Ring. Die Menge

$$\mathrm{Spec}(R) := \{P \subseteq R \mid P \text{ Primideal}\}$$

heißt *Spektrum von R.*

Lemma 2.2.31. *Sei p eine ungerade Primzahl. Dann sind äquivalent:*

(i) Es gibt Zahlen $a, b \in \mathbb{Z}$ so dass $p = a^2 + b^2$.

(ii) Es gilt $p \equiv 1 \pmod 4$.

Beweis. Sei zunächst $p = a^2 + b^2$ eine ungerade Primzahl. Die Quadrate in $\mathbb{Z}/(4)$ sind 0 und 1. Also muss p kongruent zu 1 modulo 4 sein.

Sie umgekehrt $p = 1 + 4n$, $n \in \mathbb{N}$, eine Primzahl. Wir zeigen zunächst, dass die Kongruenzgleichung

$$x^2 \equiv -1 \pmod p \tag{2.2.32}$$

eine Lösung hat. Wir rechnen zunächst in $\mathbb{Z}/(p)$:

$$[(p-1)!] = [1][2]\cdots[p-1] = [1][p-1] = [-1]$$

wobei die zweite Gleichheit gilt, da der Restklassenring $\mathbb{Z}/(p)$ ein Körper ist, wobei $[1]$ und $[p-1] = [-1]$ die beiden einzigen selbstinversen Elemente sind, so dass die restlichen Faktoren in Paaren von zueinander inversen Elementen auftreten. Wir rechnen nun weiter:

$$[-1] = [(p-1)!] = [1][2]\cdots[2n][p-2n][p-(2n-1)]\cdots[p-2][p-1] = [(2n)!]^2.$$

Also ist $x = (2n)!$ eine Lösung von (2.2.32), so dass also p ein Teiler von

$$x^2 + 1 = (x+i)(x-i)$$

in $\mathbb{Z}[i]$ ist. Aber p teilt weder $x + i$ noch $x - i$ (dazu müsste p sowohl Realteil als auch Imaginärteil dieser Zahlen teilen). Daher ist p also kein Primelement in $\mathbb{Z}[i]$.

Es gibt nun also eine Zerlegung

$$p = \alpha\beta$$

in Nichteinheiten $\alpha, \beta \in \mathbb{Z}[i]$, woraus durch Übergang zu Normen folgt:

$$p^2 = N(\alpha)N(\beta).$$

Da α und β Nichteinheiten sind, ist ihre Norm echt größer als 1 (die Einheiten in $\mathbb{Z}[i]$ sind genau die Elemente der Norm 1). Doch da p eine Primzahl ist, muss dann gelten: $N(\alpha) = N(\beta) = p$, also z.B. für $\alpha = a + ib$, wie behauptet $p = a^2 + b^2$. □

Satz 2.2.33. *Das Spektrum von $\mathbb{Z}[i]$ besteht neben dem Nullideal aus: (Die Primideale in $\mathbb{Z}[i]$ sind neben dem Nullideal genau:)*

(1) Dem Ideal $(1 + i)$.

(2) Den Idealen der Form $(a + bi)$, wobei $a^2 + b^2 = p$ Primzahl mit $p \equiv 1 \pmod 4$ und $a > |b|$ ist.

(3) Den Idealen der Form (p), wobei p eine Primzahl mit $p \equiv 3 \pmod 4$ ist.

Beweis. Die Erzeuger x der Hauptideale aus (1) und (2) sind Primelemente aus folgendem Grund: Für eine Zerlegung $x = \alpha\beta$ ist

$$N(\alpha)N(\beta) = p$$

eine Primzahl, so dass $N(\alpha) = 1$ oder $N(\beta) = 1$ folgt. Also ist α oder β eine Einheit. Eine Primzahl p aus (3) muss unzerlegbar sein, denn eine Zerlegung $p = \alpha\beta$ hätte, mit dem gleichen Argument wie im Beweis von Lemma 2.2.31, die Konsequenz, dass p eine Summe von Quadraten $a^2 + b^2$ ist, was wir dort schon ausgeschlossen haben, denn dies ist äquivalent zu $p \equiv 1 \pmod 4$.

Wir zeigen nun, dass jedes Primelement π assoziiert zu einem der genannten Erzeuger ist. Zunächst folgt aus der Primfaktorzerlegung

$$N(\pi) = \pi\overline{\pi} = p_1 p_2 \cdots p_r$$

in $\mathbb{N}$, dass es $1 \leq i \leq r$ gibt mit $\pi | p_i$. Wir setzen $p := p_i$, dann teilt auch $N(\pi)$ die Zahl $N(p) = p^2$, so dass also gilt: $N(\pi) = p$ oder $N(\pi) = p^2$. Falls $N(\pi) = p$, dann ist $p = a^2 + b^2$ für $\pi = a + ib$, also Fall (2) oder, für $p = 2$, Fall (1). Falls $N(p) = p^2$, dann ist $N(\frac{p}{\pi}) = 1$, also ist π zu p assoziiert. In diesem Fall muss $p \equiv 3 \pmod 4$ gelten, denn andernfalls wäre $p = a^2 + b^2 = (a + ib)(a - ib)$ für $a, b \in \mathbb{Z}$, so dass p nicht unzerlegbar wäre. □

Beispiel 2.2.34. Aus dem Satz erschließt sich nun auch ein präzises Verständnis des Zerlegungssverhaltens der Primideale beim Übergang von $\mathbb{Z}$ nach $\mathbb{Z}[i]$, es gilt nämlich:

(1) Das Primideal (2) zerfällt in ein Quadrat $(2) = (1 + i)^2$,

(2) Die Primideale (p) für $p \equiv 1 \pmod 4$ zerfallen in Produkte $(p) = (a + ib)(a - ib)$ von komplex konjugierten Idealen.

(3) Die Primideale (p) für $p \equiv 3 \pmod 4$ bleiben prim in $\mathbb{Z}[i]$.

Zum Abschluss geben wir eine Definition des für die algebraische Zahlentheorie zentralen Begriffs eines Dedekindrings, dessen genauere Untersuchung jedoch leider den Rahmen dieser Vorlesung sprengen würde.

Definition 2.2.35. Ein Integritätsbereich R heißt *Dedekindring*, falls R kein Körper ist und für jedes Paar von Idealen I, J in R die folgenden Bedingungen äquivalent sind:

(i) $I|J$, also nach unserer Definition $J \subseteq I$.

(ii) Es gibt ein Ideal $K \subseteq R$ mit $J = I \cdot K$.

Bemerkung 2.2.36. Dedekindringe sind also genau diejenigen Ringe, in denen die beiden potenziellen Definitionen ((i)) und ((ii)) für Teilbarkeit von Idealen übereinstimmen. Diese Definition ist aus konzeptioneller Sicht verständlich, aus praktischer Sicht ist es nützlich, Dedekindringe durch etwas technischere Bedingungen zu charakterisieren, z.B. ist ein Integritätsbereich R ein Dedekindring genau dann, wenn gilt:

(1) R ist Noethersch,

(2) R ist ganz abgeschlossen in seinem Körper der Brüche $(R \setminus \{0\})^{-1}R$,

(3) und jedes Primideal $P \subseteq R$ mit $P \neq (0)$ ist ein maximales Ideal.

Der fundamentale Satz über Dedekindringe, den wir hier ohne Beweis zitieren, ist der folgende:

Satz 2.2.37. *Sei R ein Dedekindring und sei $(0) \neq I \subsetneq R$ ein Ideal. Dann gibt es eine bis auf Permutation der Faktoren eine eindeutige "Primfaktorzerlegung"*

$$I = P_1 \cdot P_2 \cdots P_n$$

in Primideale $P_i \subseteq R$.

Aufgabe 2.2.38. Zeige, dass sich die Nichteindeutigkeit der Zerlegungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

in $\mathbb{Z}[\sqrt{-5}]$ nach Übergang zu Idealen auflöst, denn für die Primideale

$$\begin{aligned} P_1 &= (2, 1 + \sqrt{-5}) \\ P_2 &= (2, 1 - \sqrt{-5}) \\ P_3 &= (3, 1 + \sqrt{-5}) \\ P_4 &= (3, 1 - \sqrt{-5}) \end{aligned}$$

gilt

$$\begin{aligned} (2) &= P_1 P_2 \\ (3) &= P_1 P_2 \\ (1 + \sqrt{-5}) &= P_1 P_3 \\ (1 - \sqrt{-5}) &= P_2 P_4 \end{aligned}$$

also auch

$$(6) = P_1 P_2 P_3 P_4.$$

2.3 Faktorisierung in Polynomringen

Sei K ein Körper und $K[X]$ der Polynomring über K. Dann ist $K[X]$ nach Proposition 2.2.20 und Satz 2.2.19 ein Hauptidealring, also insbesondere faktoriell. Die Einheitengruppe $K[X]^\times$ ist die multiplikative Gruppe $K^\times$ des Grundkörpers und, zum Studium der Primfaktorzerlegung, verbleibt die Frage nach den irreduziblen Polynomen.

Beispiele 2.3.1. (1) $K = \mathbb{C}$. Nach dem Fundamentalsatz der Algebra zerfällt jedes Polynom $f \in \mathbb{C}[X]$ in ein Produkt

$$f = c(X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_n), \tag{2.3.2}$$

wobei $\lambda_i \in \mathbb{C}$ die Nullstellen von f sind und $c \in \mathbb{C}$. Aus Gradgründen folgt sofort, dass jedes Polynom der Form $X - \lambda$, $\lambda \in \mathbb{C}$ irreduzibel ist. Es folgt demnach, dass diese Polynome, bis auf Assoziiertheit, genau die irreduziblen Polynome in $\mathbb{C}[X]$ sind. Weiterhin ist (2.3.2) die eindeutige Primfaktorzerlegung von f, wobei der Skalar c beliebig auf die Linearfaktoren verteilt werden kann.

(2) $K = \mathbb{R}$. Wie für jeden Körper sind die Polynome der Form $X - \lambda$, $\lambda \in \mathbb{R}$ irreduzibel. Es folgt weiter, aus der Lösungsformel für die komplexen Nullstellen der quadratischen Gleichung, dass ein Polynom

$$X^2 + aX + b$$

mit $a, b \in \mathbb{R}$ genau dann irreduzibel ist, wenn $a^2 - 4b < 0$. Polynome vom Grad ≥ 3 sind nicht irreduzibel. Denn ein solches Polynom $f \in \mathbb{R}[X]$ können wir zunächst in $\mathbb{C}[X]$ zerlegen:

$$f = r(X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_n),$$

wobei $r \in \mathbb{R}$ und $\lambda_i \in \mathbb{C}$. Wir erweitern die komplexe Konjugation koeffizientenweise auf $\mathbb{C}[X]$ und erhalten

$$f = \overline{f} = r(X - \overline{\lambda_1})(X - \overline{\lambda_2}) \cdots (X - \overline{\lambda_n}).$$

Wegen der Eindeutigkeit dieser Primfaktorzerlegung muss es ein $1 \leq j \leq n$ geben mit $\overline{\lambda_1} = \lambda_j$. Falls $j = 1$, dann ist der Faktor $(X - \lambda_1)$ reell und f lässt sich faktorisieren als

$$f = (X - \lambda_1)g$$

für $g \in \mathbb{R}[X]$ (!) vom Grad ≥ 2. Falls $j \neq 1$, dann lässt sich wiederum f faktorisieren als

$$f = (X - \lambda_1)(X - \overline{\lambda_1})h$$

mit $h \in \mathbb{R}[X]$ vom Grad ≥ 1 und

$$(X - \lambda_1)(X - \overline{\lambda_1}) = X^2 - (\lambda_1 + \overline{\lambda_1})X + \lambda_1\overline{\lambda_1}.$$

In beiden Fällen ist f also nicht irreduzibel. Die Eingangs beschriebenen irreduziblen Polynome vom Grad 1 und 2 sind also genau die irreduziblen Polynome in $\mathbb{R}[X]$ (bis auf Assoziiertheit).

(3) $K = \mathbb{F}_2$. Das Polynom X^2+X+1 ist irreduzibel, denn es hat keine Nullstellen in $\mathbb{F}_2$. Daraus folgt auch, dass $X^2 + X + 1$, aufgefasst als Polynom in $\mathbb{Z}[X]$, irreduzibel ist (Betrachte den Ringhomomorphismus $\mathbb{Z}[X] \to \mathbb{F}_2[X]$ gegeben durch Reduktion der Koeffizienten modulo 2.).

Wie in Beispiel 2.3.1(3) andiskutiert, kann die Irreduzibilität von Polynomen in $\mathbb{Z}[X]$ via Reduktion modulo Primzahlen p nachgewiesen werden. Es ist nun interessant zu verstehen, wie Irreduzibilität in $\mathbb{Z}[X]$ und Irreduzibilität in $\mathbb{Q}[X]$ zusammenhängen. Dies ist der Ausgangspunkt für die Untersuchungen in diesem Abschnitt.

Definition 2.3.3. Ein Polynom

$$f = a_nX^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathbb{Z}[X]$$

heißt *primitiv*, falls

1 . Der Leitkoeffizient a_n ist positiv,

2 . Die Koeffizienten von f sind teilerfremd, also $(a_n, ..., a_0) = (1)$.

Lemma 2.3.4. *(1) Jedes $0 \neq f \in \mathbb{Q}[X]$ lässt sich eindeutig schreiben als*

$$f = cf_0 \tag{2.3.5}$$

mit $c \in \mathbb{Q}$ und $f_0 \in \mathbb{Z}[X]$ primitiv.

(2) Dabei gilt

$$f \in \mathbb{Z}[X] \Leftrightarrow c \in \mathbb{Z}.$$

In diesem Falle ist c der größte gemeinsame Teiler der Koeffizienten von f mit Vorzeichen des Leitkoeffizienten von f.

Beweis. Für die Existenz wählen wir $m \in \mathbb{Z}$, so dass $f_1 = mf \in \mathbb{Z}[X]$. Sei $t \in \mathbb{Z}$ der größte gemeinsame Teiler der Koeffizienten von f_1 mit Vorzeichen des Leitkoeffizienten von f_1. Dann ist $f_0 = t^{-1}f_1$ primitiv und es gilt $f = cf_0$ mit $c = t/m$. Für die Eindeutigkeit: Seien $f = cf_0 = dg_0$ zwei Darstellungen wie in (1). Durch Multiplizieren mit dem Nennerprodukt von c und d können wir o.E. annehmen, dass $c, d \in \mathbb{Z}$. Seien a_i (bzw. b_i), $0 \leq i \leq n$, die Koeffizienten von f_0 (bzw. g_0). Dann gilt also für alle i: $ca_i = db_i$. Da f_0 und g_0 primitiv sind, gilt weiter:

$$(c) = (ca_0, ca_1, ..., ca_n) = (db_0, db_1, ..., db_n) = (d),$$

also $c = \pm d$. Doch da f_0 und g_0 beide einen positiven Leitkoeffizienten haben, muss $c = d$ gelten und damit auch für alle $0 \leq i \leq n$: $a_i = b_i$. □

Terminologie 2.3.6. Für $f \in \mathbb{Q}[X]$ heißt die eindeutig bestimmte rationale Zahl $c \in \mathbb{Q}$ aus (2.3.5) der *Inhalt von f*, bezeichnet mit $c(f)$.

Lemma 2.3.7. *Das Produkt primitiver Polynome ist primitiv.*

Beweis. Seien $f, g \in \mathbb{Z}[X]$ primitiv. Dann ist der Leitkoeffizient von $h = fg$ positiv. Um zu zeigen, dass h primitiv ist, genügt es zu zeigen, dass keine Primzahl p alle Koeffizienten teilt, dass also das Bild $\overline{h}$ von h unter dem Homomorphismus

$$\mathbb{Z}[X] \to \mathbb{F}_p[X],\ \sum_{k=0}^{n} a_k X^k \mapsto \sum_{k=0}^{n} [a_k] X^k$$

nicht null ist. Doch es gilt $\overline{h} = \overline{f}\,\overline{g}$ mit $\overline{f} \neq 0$ und $\overline{g} \neq 0$, da f und g primitiv sind. Wegen der Nullteilerfreiheit von $\mathbb{F}_p[X]$ gilt also $\overline{h} \neq 0$, also h primitiv. □

Korollar 2.3.8. *Für Polynome $f, g \in \mathbb{Q}[X]$ gilt $c(fg) = c(f)c(g)$.*

Satz 2.3.9. *Sei $f \in \mathbb{Z}[X]$ mit positivem Leitkoeffizienten. Dann sind äquivalent:*

(i) f ist irreduzibel in $\mathbb{Z}[X]$.

(ii) (a) f ist eine Primzahl, oder

(b) f ist ein primitives Polynom und irreduzibel in $\mathbb{Q}[X]$.

Beweis. (ii) ⇒ (i) ist klar. Sei also $f \in \mathbb{Z}[X]$ irreduzibel mit positivem Leitkoeffizienten. Wir schreiben $f = c(f)f_0$ mit f_0 primitiv. Dann ist, wegen der Irreduzibilität von f, $c(f)$ oder f_0 eine Einheit in $\mathbb{Z}[X]$.

(1) Falls $f_0 \in \mathbb{Z}[X]^\times$, dann gilt $f_0 = 1$. Dann ist $f = c(f) \in \mathbb{Z}$ irreduzibel und positiv, also eine Primzahl.

(2) Falls $c(f)$ eine Einheit ist, gilt $c(f) = 1$, also ist f primitiv. Wir zeigen noch, dass f dann auch irreduzibel in $\mathbb{Q}[X]$ ist. Sei nämlich $f = gh$ mit $g, h \in \mathbb{Q}[X]$. Dann gilt $1 = c(f) = c(g)c(h)$, also

$$f = c(g)g_0c(h)h_0 = g_0h_0$$

mit $g_0, h_0 \in \mathbb{Z}[X]$. Doch weil f irreduzibel in $\mathbb{Z}[X]$, folgt $g_0 = 1$ oder $h_0 = 1$, so dass also f oder g eine Einheit $\mathbb{Q}[X]$ ist. □

Wir geben noch ein nützliches Kriterium zur Bestimmung der Irreduzibilität von Polynomen an:

Aufgabe 2.3.10 (Eisenstein-Kriterium)**.** Ein *primitives* Polynom

$$f(X) = \sum_{i=0}^{n} a_i X^i$$

ist irreduzibel über $\mathbb{Z}$ und $\mathbb{Q}$, falls gilt: Es existiert eine Primzahl p, so dass:

(i) $\forall i < n :\ p \mid a_i$,

(ii) $p^2 \nmid a_0$ und

(iii) $p \nmid a_n$.

Satz 2.3.11. *Der Ring $\mathbb{Z}[X]$ ist faktoriell.*

Beweis. Zur Existenz einer Primfaktorisierung: Wir betrachten für $f \in \mathbb{Z}[X]$ die Primfaktorzerlegung

$$f = g_1 g_2 \cdots g_k$$

in $\mathbb{Q}[X]$ und weiter

$$f = c(g_1 g_2 \cdots g_k)(g_1)_0(g_2)_0 \cdots (g_k)_0.$$

Dann sind die primitiven Polynome $(g_i)_0$ irreduzibel in $\mathbb{Q}[X]$, denn die Polynome $g_i = c(g_i)(g_i)_0$ sind irreduzibel. Also sind die Polynome $(g_i)_0$ nach Satz 2.3.9 auch irreduzibel in $\mathbb{Z}[X]$. Sei nun $p_1 \cdots p_l$ eine Primfaktorzerlegung von $c(g_1 g_2 \cdots g_k) \in \mathbb{Z}$. Dann ist also

$$f = p_1 \cdots p_l (g_1)_0(g_2)_0 \cdots (g_k)_0.$$

die gewünschte Zerlegung. Um die Eindeutigkeit der Primfaktorzerlegung zu zeigen, genügt es nach Proposition 2.2.26 zu zeigen, dass jedes irreduzible Polynom in $\mathbb{Z}[X]$ ein Primelement ist. Sei also $f \in \mathbb{Z}[X]$ irreduzibel und $g, h \in \mathbb{Z}[X]$ mit $f|gh$. O.E. nehmen wir an, dass f einen positiven Leitkoeffizienten hat. Nach Satz 2.3.9 ist f entweder eine Primzahl oder primitiv und irreduzibel in $\mathbb{Q}[X]$.

(1) Sei $f = p \in \mathbb{Z}$ eine Primzahl. Wir schreiben $g = c(g)g_0$ und $h = c(h)h_0$. Dann ist g_0h_0 primitiv, so dass dieses Produkt also einen Koeffizienten a besitzt, der nicht durch p teilbar ist. Doch da $p|fg$, muss gelten:

$$p|ac(g)c(h)$$

so dass also $p|c(g)$ oder $p|c(h)$ gilt, und damit auch $p|g$ oder $p|h$.
(2) Sei f primitiv und irreduzibel in $\mathbb{Q}[X]$. Dann ist f also ein Primelement in $\mathbb{Q}[X]$, so dass also in $\mathbb{Q}[X]$ gilt: $f|g$ oder $f|h$, o.E. $f|g$. Wir schreiben $g = c(g)g_0$, dann teilt f auch g_0 in $\mathbb{Q}[X]$. Also gibt es $r \in \mathbb{Q}[X]$ mit

$$g_0 = rf = c(r)r_0f,$$

doch da r_0f primitiv ist, gilt $c(r) = 1$, so dass schließlich auch

$$g = c(g)g_0 = c(g)r_0f$$

und demnach $f|g$ in $\mathbb{Z}[X]$. □

Die Aussagen dieses Abschnitts gelten allgemeiner für einen beliebigen faktoriellen Ring R statt $\mathbb{Z}$ und dem Körper der Brüche $(R \setminus \{0\})^{-1}R$ statt $\mathbb{Q}$. Alle Beweise lassen sich mutatis mutandis verallgemeinern. Es ist eine gute Übung sich davon zu überzeugen, und insbesondere zu beweisen:

Satz 2.3.12. *Sei R ein faktorieller Ring. Dann ist der Polynomring $R[X]$ faktoriell.*

Beispiele 2.3.13. (1) Für jeden Körper ist der Polynomring $K[X_1, X_2, ..., X_n]$ faktoriell.

(2) Der Ring $\mathbb{Z}[X_1, X_2, ..., X_n]$ ist faktoriell.

2.4 Moduln

In diesem Abschnitt bezeichnet R stets einen kommutativen Ring.

Definition 2.4.1. Ein *R-Modul* ist ein Tripel $(M, +, .)$, bestehend aus einer abelschen Gruppe $(M, +)$ und einer Abbildung

$$. : R \times M \to M,\ (r, m) \mapsto r.m,$$

genannt *Skalarmultiplikation*, so dass für alle $m, m_1, m_2 \in M$ und $r, s \in R$ gelten:

(M1) $r.(s.m) = (rs).m$,

(M2) $(r + s).m) = r.m + s.m$,

(M3) $r.(m_1 + m_2) = r.m_1 + r.m_2$,

(M4) $1.m = m$.

Beispiele 2.4.2. (1) Sei K ein Körper. Ein K-Modul ist genau ein K-Vektorraum.

(2) Ein $\mathbb{Z}$-Modul ist eine abelsche Gruppe (!).

(3) Sei R ein Ring. Dann ist für jede natürliche Zahl $n \geq 1$ das kartesische Produkt

$$R^n = \underbrace{R \times R \times \cdots \times R}_{n}$$

ein R-Modul mit Skalarmultiplikation:

$$r.(r_1, r_2, ..., r_n) := (rr_1, rr_2, ..., rr_n),$$

genannt der *freie Standard R-Modul vom Rang n.*

(4) Für R-Moduln M, N ist das kartesische Produkt $M \times N$ ein R-Modul mit

$$r.(m,n) = (r.m, r.n).$$

Da sich jedes Element $(m,n) \in M \times N$ auf eindeutige Weise als Summe $(m,n) = (m,0) + (0,n)$ von Elementen in $M \hookrightarrow M \times N$ und $N \hookrightarrow M \times N$ schreiben lässt, verwendet man auch häufig die Notation

$$M \oplus N := M \times N,$$

genannt die *direkte Summe* von M und N.

Die grundlegenden Begriffe und Resultate aus der Theorie der Vektorräume lassen sich direkt auf R-Moduln erweitern, wir lassen daher die Beweise als Übungsaufgaben.

Definition 2.4.3. Eine Abbildung $\varphi : M \to N$ von R-Moduln heißt *R-linear*, falls für alle $r \in R$ und $m_1, m_2 \in M$ gilt:

$$\varphi(rm_1 + m_2) = r\varphi(m_1) + \varphi(m_2).$$

Eine bijektive R-lineare Abbildung heißt *Isomorphismus* von R-Moduln.

Definition 2.4.4. Sei M ein R-Modul.

(1) Ein *Untermodul* ist eine abelsche Untergruppe $N \subseteq M$, die zudem abgeschlossen unter Skalarmultiplikation ist, also für alle $r \in R$ und $n \in N$ gilt $r.n \in N$ Inbesondere vererbt N damit von M eine R-Modulstruktur. Um auszudrücken, dass $N \subseteq M$ ein Untermodul ist, schreiben wir auch $N \leq M$.

(2) Für eine Teilmenge $S \subseteq M$ heißt der Untermodul (!)

$$\langle S \rangle := \bigcap_{S \subseteq N \leq M} N$$

der von S erzeugte Untermodul.

Beispiel 2.4.5. Sei R ein Ring. Dann sind die Untermoduln von R genau die Ideale in R.

Proposition 2.4.6. *Sei $\varphi : M \to N$ eine R-lineare Abbildung von R-Moduln.*

(1) Das Bild von φ ist ein Untermodul von N.

(2) Der $\mathrm{Kern}(\varphi) = \{m \in M | \varphi(m) = 0\}$ *von φ ist ein Untermodul von M.*

(3) Die Abbildung φ ist genau dann injektiv, wenn $\mathrm{Kern}(\varphi) = \{0\}$.

Definition 2.4.7. Sei M ein R-Modul und $N \subseteq M$ ein Untermodul. Dann definiert die Skalarmultiplikation

$$R \times M/N \to M/N,\ (r, [m]) \mapsto [rm]$$

zusammen mit der additiven Quotientengruppe $(M/N, +)$ eine R-Modulstruktur auf M/N, genannt *Quotientenmodul*.

Proposition 2.4.8. *Sei $\varphi : M \to N$ ein Homomorphismus. Dann ist die induzierte Abbildung*

$$\overline{\varphi} : M/\mathrm{Kern}(\varphi) \to \mathrm{Bild}(\varphi), [m] \mapsto \varphi(m)$$

ein R-linearer Isomorphismus.

Definition 2.4.9. Für eine natürliche Zahl $n \geq 0$, heißt ein R-Modul F *frei vom Rang n*, falls es einen Isomorphismus $R^n \cong F$ gibt (für $n = 0$ setze $R^n = \{0\}$).

Beispiele 2.4.10. (1) In diesem Fall besitzt F eine R-Basis $(x_1, x_2, ..., x_n)$, so dass sich jedes $m \in F$ als eindeutige R-Linearkombination

$$m = \lambda_1 x_1 + \lambda_2 x_2 + ... + \lambda_n x_n$$

schreiben lässt. Die Elemente x_i sind nämlich die Bilder der Standardvektoren e_i von R^n unter dem Isomorphismus $R^n \cong F$.

(2) In jedem nullteilerfreien Ring R ist für $0 \neq a \in R$ das Ideal $(a) \subseteq R$ ein freier R-Modul vom Rang 1, denn die Abbildung

$$R \to (a), r \mapsto ra$$

ist ein R-linearer Isomorphismus. Falls a zusätzlich keine Einheit ist, dann ist der Quotientenmodul $R/(a)$ *kein* freier R-Modul, denn es gibt Elemente $0 \neq r \in R$ und $0 \neq x \in M$ mit $rx = 0$ – unmöglich in einem freien R-Modul.

Definition 2.4.11. Ein R-Modul M heißt *endlich erzeugt*, falls es $n \geq 0$ und eine surjektive R-lineare Abbildung $\varphi : R^n \to M$ gibt.

Bemerkung 2.4.12. Ein R-Modul M ist genau dann endlich erzeugt, wenn es eine endliche Teilmenge $S \subseteq M$ mit $\langle S \rangle = M$ gibt.

Definition 2.4.13. Eine *kurze exakte Sequenz*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

von R-Moduln besteht aus R-linearen Abbildungen $f : M' \to M$ und $g : M \to M''$, so dass gilt:

(1) f ist injektiv.

(2) $\text{Bild}(f) = \text{Kern}(g)$.

(3) g ist surjektiv.

Beispiel 2.4.14. Für jedes $0 \neq a \in \mathbb{Z}$ bildet

$$0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/(a) \to 0$$

eine kurze exakte Sequenz, wobei $f : \mathbb{Z} \to \mathbb{Z}, n \mapsto an$ und $g : \mathbb{Z} \to \mathbb{Z}/(a), n \mapsto n + (a)$ die kanonische Quotientenabbildung ist.

Proposition 2.4.15. *Sei*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

eine kurze exakte Sequenz von R-Moduln und sei $s : M'' \to M$ eine R-lineare Abbildung mit $g \circ s = \text{id}_{M''}$. Dann definiert die Abbildung

$$\varphi : M' \oplus M'' \to M, (x, y) \mapsto f(x) + s(y) \tag{2.4.16}$$

einen R-linearen Isomorphismus.

Beweis. Zunächst gilt $\text{Kern}(\varphi) = 0$, denn aus $f(x) + s(y) = 0$ folgt nach Anwendung von g auch $y = 0$, dann aber, da f injektiv ist, auch $x = 0$. Sei nun $m \in M$ beliebig. Dann liegt $m - s(g(m))$ im Kern von g, und demnach im Bild von f. Es gibt also ein $x \in M'$ mit $m - s(g(m)) = f(x)$, doch dann gilt mit $y = g(m)$: $m = \varphi(x, y)$. □

Bemerkung 2.4.17. In der Situation von Proposition 2.4.15 heißt die Abbildung s ein *Schnitt von g* und wir sagen, die exakte Sequenz *spaltet* oder *zerfällt*.

Proposition 2.4.18. *Sei*

$$0 \to N \xrightarrow{f} M \xrightarrow{g} F \to 0$$

eine kurze exakte Sequenz von R-Moduln, wobei F ein freier R-Modul ist. Dann spaltet die Sequenz.

Beweis. Für die Elemente einer R-Basis $e_1, e_2, ..., e_n$ von F wählen wir $x_1, x_2, ..., x_n \in M$ mit $g(x_i) = e_i$. Dann erfüllt die R-lineare Abbildung

$$s : F \to M, \sum \lambda_i e_i \mapsto \sum \lambda_i x_i$$

die gewünschte Bedingung $g \circ s = \mathrm{id}_F$. □

2.5 Endlich erzeugte Moduln über Hauptidealringen

In diesem Abschnitt bezeichnet R einen *Hauptidealring*, also einen Integritätsbereich, in dem jedes Ideal ein Hauptideal ist. Unser Ziel ist die Klassifikation von endlich erzeugten R-Moduln bis auf Isomorphie.

Lemma 2.5.1. *Sei F ein freier R-Modul vom Rang n und $M \subseteq F$ ein Untermodul. Dann ist M frei vom Rang $m \leq n$.*

Beweis. Sei zunächst $n = 1$, also $R \cong F$, o.E. $F = R$. Ein Untermodul von R ist ein Ideal $I \subseteq R$ und damit ein Hauptideal $I = (a)$. Für $a \neq 0$ ist die Abbildung

$$R \longrightarrow (a), r \mapsto ra$$

ein Isomorphismus, denn R ist nullteilerfrei und für $a = 0$ ist $I = 0$ frei vom Rang 0. Sei nun $F = R^n$ und betrachte die Projektionsabbildung

$$p : R^n \to R$$

auf die erste Koordinate, wobei $R^{n-1} \cong \mathrm{Kern}(p)$ der Untermodul der Tupeln mit erster Koordinate 0 ist. Wir schränken p auf M ein und erhalten eine surjektive R-lineare Abbildung

$$p|M : M \to p(M).$$

Der Kern $\mathrm{Kern}(p|M) = M \cap \mathrm{Kern}(p) \subseteq \mathrm{Kern}(p) \cong R^{n-1}$ ist per Induktion ein freier R-Modul vom Rang $\leq n - 1$. Genauso ist $p(M) \subseteq R$ ein freier Modul vom Rang ≤ 1. Wir erhalten eine kurze exakte Sequenz

$$0 \to \mathrm{Kern}(p|M) \to M \to p(M) \to 0$$

und nach Proposition 2.4.18 einen Isomorphismus

$$p(M) \oplus \mathrm{Kern}(p|M) \cong M,$$

womit also M frei vom Rang $\leq n$ ist. □

Definition 2.5.2. Sei M ein R-Modul.

(1) Wir definieren den *Torsionsuntermodul*

$$T(M) = \{x \in M \mid \text{es gibt } 0 \neq r \in R \text{ mit } rx = 0\} \leq M,$$

welcher tatsächlich (!) einen Untermodul von M bildet.

(2) Für ein Primelement $p \in R$ definieren wir den p-Torsionsuntermodul

$$T_p(M) = \{x \in M \mid \text{es gibt } n \geq 0 \text{ mit } p^n x = 0\} \leq T(M).$$

(3) Der Modul M heißt *Torsionsmodul* (bzw. p-Torsionsmodul), falls $T(M) = M$ (bzw. $T_p(M) = M$).

(4) Der Modul M heißt *torsionsfrei*, falls $T(M) = 0$.

Lemma 2.5.3. *Sei M ein torsionsfreier endlich erzeugter R-Modul. Dann ist M ein freier R-modul.*

Beweis. Nach Lemma 2.5.1 reicht es zu zeigen, dass M ein Untermodul eines endlich erzeugten freien R-Moduls ist. Sei M erzeugt von der endlichen Menge $S \subseteq M$. Wir wählen eine maximale R-linear unabhängige Teilmenge $B = \{x_1, x_2, ..., x_d\} \subseteq S$, es gilt also für alle $\lambda_1, ..., \lambda_n \in R$:

$$\sum \lambda_i x_i = 0 \quad \Rightarrow \quad \forall 1 \leq i \leq n : \lambda_i = 0,$$

und die Teilmenge ist maximal mit dieser Eigenschaft. Wir setzen $N := \langle B \rangle \subseteq M$. Dann ist die Abbildung

$$R^d \to N, (\lambda_1, ..., \lambda_d) \mapsto \sum \lambda_i x_i$$

ein Isomorphismus. Wegen der Maximalität von B existiert für jedes $s \in S \setminus B$ ein $0 \neq a_s \in R$ mit $a_s s \in N$. Setze

$$a := \prod_{s \in S \setminus B} a_s.$$

Da M torsionsfrei ist, ist die Abbildung

$$\mu_a : M \to M, m \mapsto am$$

injektiv und daher

$$M \cong \text{Bild}(\mu_a) \subseteq N.$$

□

Lemma 2.5.4. *Sei M ein endlich erzeugter R-Modul mit Torsionsuntermodul $T \subseteq M$. Dann ist T ein endlich erzeugter R-Modul, M/T ein freier R-Modul und es gibt einen Isomorphismus*

$$M \cong T \oplus M/T. \tag{2.5.5}$$

Beweis. Wir zeigen zunächst, dass M/T torsionsfrei ist. Sei also $[x] \in M/T$ und sei $0 \neq r \in R$ mit $[rx] = 0$. Dann gilt $rx \in T$, es gibt also $0 \neq s \in R$ mit $s(rx) = 0$. Dann folgt aber aus $(sr)x = 0$, dass $x \in T$ also $[x] = 0$. Es folgt also nach Lemma 2.5.3, dass M/T ein freier R-Modul ist. Der gewünschte Isomorphismus folgt nun sofort aus Proposition 2.4.18 in Anbetracht der kurzen exakten Sequenz

$$0 \to T \to M \to M/T \to 0$$

von R-Moduln. Aus dem Isomorphismus (2.5.5) folgt nun auch, dass T ein Quotient von M ist, und damit endlich erzeugt, da M endlich erzeugt ist. □

Definition 2.5.6. Sei M ein R-Modul. Dann heißt das Ideal

$$\text{Ann}_R(S) := \{r \in R \mid \text{für alle } x \in S \text{ gilt } r.x = 0\} \subseteq R$$

das *Annihilatorideal* von S.

Proposition 2.5.7. *Sei $0 \neq M$ ein endlich erzeugter Torsionsmodul über R.*

(1) Es gilt $\text{Ann}_R(M) = (d)$ für eine Nichteinheit $d \neq 0$.

(2) Sei $d = \epsilon p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ die Primfaktorzerlegung mit paarweise nichtassoziierten Primelementen $p_i \not\sim p_j$ für $i \neq j$. Dann gilt

$$M \cong \bigoplus_{i=1}^{k} T_{p_i}(M).$$

Beweis. (1) Sei $S = \{x_1, x_2, ..., x_n\} \subseteq M \setminus \{0\}$ eine erzeugende Teilmenge von M. Da M ein Torsionsmodul ist, gibt es für jedes $1 \leq i \leq n$ ein $0 \neq r_i \in R$ mit $r_i x_i = 0$. Dann ist $0 \neq r_1 r_2 \cdots r_n \in \text{Ann}_R(M)$. Da R ein Hauptidealring ist, gilt also $\text{Ann}_R(M) = (d)$ mit $d \neq 0$. Zudem ist d keine Einheit, denn sonst wäre $M = 0$.

(2) Wir setzen $I = \{1, 2, ..., k\}$ und betrachten die Abbildung

$$\varphi : \bigoplus_{i\in I} T_{p_i}(M) \to M,\ (x_i)_{i\in I} \mapsto \sum_{i\in I} x_i.$$

Mit $d_i := d/p_i^{n_i}$ gilt

$$(d_1, d_2, \cdots, d_n) = (1),$$

so dass es also Elemente r_i, $1 \le i \le n$, mit $\sum_i r_i d_i = 1$ gibt. Für beliebiges $x \in M$ gilt für alle $1 \le i \le n$: $x_i = r_i d_i x \in T_{p_i}(M)$ und weiter

$$x = \sum_{i\in I} x_i.$$

Damit ist also φ surjektiv. Wir zeigen nun, dass φ auch injektiv ist. Sei dazu $(x_i)_{i\in I} \in \mathrm{Kern}(\varphi)$ und $1 \le j \le n$ beliebig. Dann gilt

$$-x_j = \sum_{i\in I\setminus\{j\}} x_i,$$

also $p_j x_j = 0$ und $d_j x_j = 0$, doch $(d_j, p_j) = (1)$ und daher auch $1.x_j = x_j = 0$. □

Beispiel 2.5.8. Für $d = \epsilon p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \in R$ gilt nach dem chinesischen Restsatz (Aufgabe 8.4)

$$R/(d) \cong R/(p_1^{n_1}) \oplus R/(p_2^{n_2}) \oplus \cdots \oplus R/(p_k^{n_k})$$

mit

$$T_{p_i}(R/(d)) = R/(p_i^{n_i}).$$

Dies ist also ein Spezialfall von Proposition 2.5.7.

Satz 2.5.9. *Sei $p \in R$ ein Primelement und sei T ein endlich erzeugter p-Torsionsmodul über R. Dann gibt es eindeutig bestimmte Zahlen $m \ge 0$ und $0 < e_1 \le e_2 \le \cdots \le e_m$ mit*

$$T \cong R/(p^{e_1}) \oplus R/(p^{e_2}) \oplus \cdots \oplus R/(p^{e_m}). \tag{2.5.10}$$

Beweis. Sei $T = \langle x_1, x_2, ..., x_m\rangle$ mit m minimal. Wir beweisen zunächst die Existenz des Isomorphismus (2.5.10) per Induktion nach m. Für $m = 1$ fogt die Aussage aus dem chinesischen Restsatz (Beispiel 2.5.8), sei also $m > 1$. Für jedes $1 \le i \le n$ gilt $\mathrm{Ann}_R(x_i) = (p^{n_i})$ für $n_i > 0$ (wieder wegen des chinesischen Restsatzes). Sei o.E. $\mathrm{Ann}_R(x_m) = (p^e)$, wobei e maximal unter den Zahlen n_i ist. Dann gilt auch $\mathrm{Ann}_R(T) = (p^e)$ und $\langle x_m\rangle \cong R/(p^e)$. Wir betrachten nun die kurze exakte Sequenz

$$0 \to \langle x_m\rangle \to T \xrightarrow{\pi} T/\langle x_m\rangle \to 0. \tag{2.5.11}$$

Die minimale Anzahl von Erzeugern von $\overline{T} = T/\langle x_m\rangle$ ist $m - 1$ (denn m ist minimal), daher gibt es per Induktionsannahme einen Isomorphismus

$$\varphi : \overline{T} \xrightarrow{\cong} R/(p^{e_1}) \oplus R/(p^{e_2}) \oplus \cdots \oplus R/(p^{e_{m-1}})$$

mit $0 < e_1 \le e_2 \le \cdots \le e_{m-1}$.

Wir behaupten nun, dass es zu jedem $y \in \overline{T}$ mit $\mathrm{Ann}_R(y) = (p^f)$ ein Element $\tilde{y} \in T$ mit $\pi(\tilde{y}) = y$ und $\mathrm{Ann}_R(\tilde{y}) = (p^f)$ gibt. Zunächst ist klar, dass $f \le e$ gilt. Sei $z \in T$ beliebig mit $\pi(z) = y$, dann gilt $p^f z = r x_m$. Weiter gilt

$$0 = p^e z = p^{e-f} r x_m.$$

Da $\mathrm{Ann}_R(x_m) = (p^e)$, muss $r = s p^f$ für $s \in R$ gelten. Wir setzen nun $\tilde{y} = z - s x_m$, dann gilt $\pi(\tilde{y}) = y$, so dass also $p^j \tilde{y} \ne 0$ für $j < f$. Zudem gilt

$$p^f \tilde{y} = p^f z - p^f s x_m = r x_m - r x_m = 0,$$

also $\mathrm{Ann}_R(\tilde{y}) = (p^f)$. Es folgt (!), dass die kurze exakte Sequenz (2.5.11) spaltet und damit die Existenz des Isomorphismus (2.5.10).

Zur Eindeutigkeit der Parameter m sowie $e_1 \leq e_2 \leq ... \leq e_m$: Die Zahl m ist als die minimale Anzahl von Erzeugern von T eindeutig bestimmt. Alternativ ist m die Dimension des $R/(p)$-Vektorraums T/pT. Analog (!) können wir die Anzahl der Exponenten e_i die größer als 1 sind identifizieren mit der Dimension des $R/(p)$-Vektorraums pT/p^2T und allgemeiner(!), die Anzahl der Exponenten e_i grösser als j mit der Dimension des $R/(p)$-Vektorraums $p^jT/p^{j+1}T$. Diese Dimensionen sind intrinsische Invarianten des R-Moduls T und bestimmen die Exponenten $\{e_i\}$ eindeutig. □

Korollar 2.5.12. *Sei M ein endlich erzeugter R-Modul. Dann gibt es eindeutig bestimmte $r, m \in \mathbb{N}$ und Primelementpotenzen $p_1^{e_1}, ..., p_m^{e_m}$ (wobei die Primelemente p_i nicht paarweise verschieden sein müssen), so dass gilt*

$$M \cong R^r \oplus R/(p_1^{e_1}) \oplus R/(p_2^{e_2}) \oplus \cdots \oplus R/(p_m^{e_m}).$$

Beispiel 2.5.13 (Klassifikation endlich erzeugter abelscher Gruppen)**.** Für jede endlich erzeugte abelsche Gruppe A gibt es eine direkte Summenzerlegung

$$A \cong \mathbb{Z}^r \oplus \mathbb{Z}/(p_1^{e_1}) \oplus \mathbb{Z}/(p_2^{e_2}) \oplus \cdots \oplus \mathbb{Z}/(p_m^{e_m})$$

mit eindeutig bestimmten Summanden.

Beispiel 2.5.14 (Jordansche Normalform)**.** Sei K ein algebraisch abgeschlossener Körper und $K[X]$ der Polynomring über K. Sei weiter V ein endlich–dimensionaler K-Vektorraum und $\varphi : V \to V$ ein K-linearer Endomorphismus. Wir betrachten V als $K[X]$-Modul, wobei wir für $f(X) \in K[X]$ und $v \in V$ die Skalarmultiplikation definieren als

$$f(X).v := f(\varphi)(v),$$

wobei also für

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_0$$

das Symbol $f(\varphi)$ den Endomorphismus

$$a_n \varphi^n + a_{n-1} \varphi^{n-1} + ... + a_0 \,\mathrm{id}$$

von V bezeichnet. Die Primelemente von $K[X]$ sind bis auf Assoziierte genau die Polynome $X - a$, $a \in K$. Da V endlich–dimensional ist, muss V ein Torsionsmodul über $K[X]$ sein. Es folgt also, dass V als $K[X]$-Modul isomorph zu einer direkten Summe von Moduln der Form

$$K[X]/(X - a)^e$$

ist. Wir betrachten die K-Basis $B = ((X-a)^{e-1}, (X-a)^{e-2}, ..., 1)$ dieses Moduls. Anwendung des Endomorphismus φ entspricht der Skalarmultiplikation mit X. Daher hat die Darstellungsmatrix des Endomorphismus φ also bezüglich der Basis B die Gestalt

$$\begin{pmatrix} a & 1 & 0 & \cdots & 0 \\ 0 & a & 1 & \cdots & 0 \\ & & \ddots & & \\ 0 & \cdots & 0 & a & 1 \\ 0 & \cdots & 0 & 0 & a \end{pmatrix}. \tag{2.5.15}$$

Die direkte Summenzerlegung von V in Moduln der Form $K[X]/(X-a)^e$ mit $a \in K$ und $e \in \mathbb{N}$ impliziert, dass die Darstellungsmatrix von φ bezüglich der zusammengesetzten Basen der Gestalt B also Blockdiagonalform mit Blöcken (2.5.15) hat. Dies ist die aus der linearen Algebra bekannte *Jordansche Normalform von φ*.

Korollar 2.5.12 gilt natürlich auch für Moduln über dem Hauptidealring $K[X]$ mit K *nicht* algebraisch abgeschlossen. In diesem Fall erhalten wir also auch eine Jordansche Normalform – allerdings ist diese etwas komplizierter: zu jedem irreduziblen Polynom $f \in K[X]$ gibt es Jordanblöcke, die zu den zyklischen $K[X]$-Moduln

$$K[X]/(f^e)$$

korrespondieren (siehe Übungsaufgaben).

Kapitel 3

Galoistheorie

3.1 Einleitung

Lösungsformeln für polynomiale Gleichungen in einer Variablen bis hin zum Grad vier waren schon im 16. Jhd. bekannt, wenn auch in etwas anderer Form, als wir diese heute dokumentieren würden, siehe Folien unter

https://www.math.uni-hamburg.de/home/dyckerhoff/algebra2425/quintic.pdf .

Die vergeblichen Versuche, eine Lösungsformel für die allgemeine Gleichung fünften Grades zu finden, führten zu der Vermutung (Gauß, 1799), dass eine solche Formel vielleicht gar nicht existiert. Die grundlegende Idee, welche dem Beweis dieser Vermutung durch Abel und Galois zugrunde liegt, ist das Studium der sogenannten *Galoisgruppe*.

Definition 3.1.1. Sei $f(X) \in \mathbb{Q}[X]$ ein Polynom vom Grad $n \geq 1$ mit rationalen Koeffizienten und seien $\lambda_1, \lambda_2, ..., \lambda_n \in \mathbb{C}$ die komplexen Nullstellen (möglicherweise mit Vielfachheiten) von $f(X)$. Die *Galoisgruppe*

$$G(f) \leq S_n$$

von f über $\mathbb{Q}$ ist eine Untergruppe der symmetrischen Gruppe, bestehend aus denjenigen Permutationen σ, welche die folgende Bedingung erfüllen:

- Für jedes
$$r(X_1, X_2, ..., X_n) \in \mathbb{Q}[X_1, X_2, ..., X_n]$$
mit $r(\lambda_1, \lambda_2, ..., \lambda_n) = 0$ gilt auch $r(\lambda_{\sigma(1)}, \lambda_{\sigma(2)}, ..., \lambda_{\sigma(n)}) = 0$.

In anderen Worten, $G(f)$ ist die Untergruppe derjenigen Permutationen, die alle *algebraischen Relationen über* $\mathbb{Q}$ der Nullstellen von $f(X)$ erhalten.

Beispiel 3.1.2. Wir betrachten das Polynom $X^4 - 2 \in \mathbb{Q}[X]$. Die Nullstellen des Polynoms sind gegeben durch

$$a = \lambda_1 = \sqrt[4]{2}, \quad b = \lambda_2 = i\sqrt[4]{2}, \quad c = \lambda_3 = -\sqrt[4]{2}, \quad d = \lambda_4 = -i\sqrt[4]{2}.$$

Wegen $X^4 - 2 = (X-a)(X-b)(X-c)(X-d)$ gelten die Relationen

$$\begin{aligned} abcd &= -2 \\ abc + abd + acd + bcd &= 0 \\ ab + ac + ad + bc + bd + cd &= 0 \\ a + b + c + d &= 0. \end{aligned}$$

Zusätzlich gelten

$$a^2b^2 = -2 \tag{3.1.3}$$
$$b^2c^2 = -2 \tag{3.1.4}$$
$$c^2d^2 = -2 \tag{3.1.5}$$
$$d^2a^2 = -2, \tag{3.1.6}$$

welche wir als Kanten eines Quadrats veranschaulichen können, sowie die Relationen

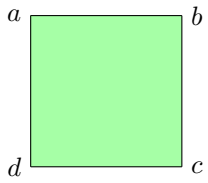


Abbildung 3.1: Veranschaulichung der Wirkung von G

$$a^2c^2 = 2 \tag{3.1.7}$$
$$b^2d^2 = 2, \tag{3.1.8}$$

korrespondierend zu den Diagonalen im Quadrat. Durch diese geometrische Veranschaulichung ist klar, dass nur die Permutationen in der Diedergruppe

$$D_4 = \langle (1234), (12)(34) \rangle \leq S_4$$

die speziellen Relationen erhalten, also $G(f) \leq D_4$. Tatsächlich wird sich später zeigen, dass dies auch die Galoisgruppe des Polynoms $X^4 - 2$ ist. Mit der jetzigen Definition ist dies nicht direkt einzusehen, denn es ist unklar, ob es noch weitere algebraische Relationen gibt. Um dies effizient beantworten zu können, werden wir nun eine abstraktere Definition der Galoisgruppe geben.

3.2 Körpererweiterungen

Sei L ein Körper. Ein *Unterkörper* $K \subseteq L$ ist eine Teilmenge, die 0 und 1 enthält und mit der von L eingeschränkten Addition und Multiplikation einen Körper bildet. Wir sagen für einen gegebenen Teilkörper $K \subseteq L$ auch, dass L/K eine *Körpererweiterung* ist. Insbesondere ist dann L ein K-Vektorraum und wir nennen

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

den Grad von L/K. Eine Körpererweiterung L/K heißt *endlich*, falls der Grad $[L : K]$ endlich ist.

Lemma 3.2.1. *Seien M/L und L/K Körpererweiterungen. Dann ist M/K genau dann endlich, wenn M/L und L/K endlich sind, und in diesem Falle gilt*

$$[M : K] = [M : L][L : K].$$

Ist die Formulierung nicht etwas zu stark? Die Formel gilt doch auch, wenn einer der Terme unendlich ist, und wird in der gängigen Literatur auch so angegeben.

Beweis. Seien Teilmengen $P = \{m_1, ..., m_r\} \subseteq M$ und $Q = \{l_1, ..., l_s\} \subseteq L$ gegeben und betrachte die Teilmenge

$$QP = \{l_i m_j \mid 1 \leq i \leq s, 1 \leq j \leq r\}.$$

Die Behauptungen folgen nun direkt aus den folgenden Aussagen:

(1) Sei P linear unabhängig über L und Q linear unabhängig über K, dann ist QP linear unabhängig über K.

(2) Sei P erzeugend über L und Q erzeugend über K, dann ist QP erzeugend über K.

Diese folgen wiederum direkt aus der Umformung

$$\sum_{i,j} \lambda_{i,j} l_i m_j = \sum_j (\sum_i \lambda_{i,j} l_i) m_j.$$

□

Beispiele 3.2.2. (1) $\mathbb{C}/\mathbb{R}$ ist eine Körpererweiterung vom Grad 2.

(2) $\mathbb{R}/\mathbb{Q}$ ist eine Körpererweiterung von unendlichem Grad, z.B. ist $\{1, \pi, \pi^2, ...\} \subseteq \mathbb{R}$ linear unabhängig über $\mathbb{Q}$ (von Lindemann, 1882).

(3) Sei K ein Körper und $K(X) = (K[X] \setminus \{0\})^{-1} K[X]$ der Körper der Brüche, genannt *Körper der rationalen Funktionen*. Dann ist $K(X)/K$ Körpererweiterung mit $[K(X) : K] = \infty$. Z.B. ist die Menge $\{1, X, X^2, ...\}$ linear unabhängig über K.

(4) Sei $f(X) \in \mathbb{Q}[X]$ ein Polynom vom Grad $n \geq 1$ mit Nullstellen $\lambda_1, ..., \lambda_n \in \mathbb{C}$. Sei $\mathbb{Q}(f)$ das Bild des Ringhomomorphismus

$$\varphi : \mathbb{Q}[X_1, ..., X_n] \to \mathbb{C},\ f(X_1, ..., X_n) \mapsto f(\lambda_1, ..., \lambda_n).$$

Dann ist $\mathbb{Q}(f)/\mathbb{Q}$ eine endliche Körper(!)erweiterung (vom Grad $\leq n^n$) (!).

3.3 Körperautomorphismen

Sei L ein Körper. Einen bijektiven Ringhomomorphismus $\sigma : L \to L$ nennen wir auch *Körperautomorphismus von* L und bezeichnen die Menge der Körperautomorphismen von L mit $\mathrm{Aut}(L)$. Für eine Körpererweiterung L/K bezeichnen wir die Körperautomorphismen, die K invariant lassen, mit

$$G(L/K) := \{\sigma \in \mathrm{Aut}(L) \mid \forall x \in K : \sigma(x) = x\} \leq \mathrm{Aut}(L).$$

Beispiel 3.3.1. Sei $f \in \mathbb{Q}[X]$ ein Polynom und $\mathbb{Q}(f)/\mathbb{Q}$ die Körpererweiterung aus Beispiel 3.2.2. Dann gilt (!)

$$G(\mathbb{Q}(f)/\mathbb{Q}) \cong G(f).$$

Satz 3.3.2. *[Lemma von Artin] Sei L/K eine Körpererweiterung. Dann gilt*

$$|G(L/K)| \leq [L : K].$$

Für den Beweis des Satzes benötigen wir etwas Vorarbeit.

Lemma 3.3.3 (Dedekind-Lemma)**.** *Seien L und E Körper,*

$$\sigma_i : L \to E,\ 1 \leq i \leq n$$

paarweise verschiedene Ringhomomorphismen und $\lambda_i \in E$, $1 \leq i \leq n$, mit

$$\sum_{i=1}^{n} \lambda_i \sigma_i = 0 \in \mathrm{Abb}(L, E). \tag{3.3.4}$$

Dann gilt für alle $1 \leq i \leq n$: $\lambda_i = 0$. Hierbei ist die Formel (3.3.4) im E-Vektorraum $\mathrm{Abb}(L, E)$ aller Abbildungen von L nach E zu interpretieren.

Beweis. Wir beweisen die Aussage durch Induktion nach n. Für $n = 1$ folgt aus (3.3.4) direkt $0 = \lambda_1\sigma_1(1) = \lambda_1$. Sei also $n > 1$. Wir nehmen an, es gäbe eine nichttriviale Linearkombination wie in (3.3.4) und führen die Aussage zum Widerspruch. Sei also

$$\sum_{i=1}^{n} \lambda_i\sigma_i = 0$$

mit o.E. $\lambda_1 \neq 0$. Wir wählen $a \in L$ mit $\sigma_1(a) \neq \sigma_n(a)$. Dann gilt für alle $x \in L$:

$$0 = \sum_{i=1}^{n} \lambda_i\sigma_i(ax) - \sigma_n(a)\sum_{i=1}^{n} \lambda_i\sigma_i(x) = \sum_{i=1}^{n-1} \lambda_i(\sigma_i(a) - \sigma_n(a))\sigma_i(x).$$

Wir erhalten also eine kürzere Linearkombination der $\sigma_1, ..., \sigma_{n-1}$ zu 0, welche nichttrivial ist, denn $\lambda_1(\sigma_1(a) - \sigma_n(a)) \neq 0$ per Konstruktion. Ein Widerspruch. □

Satz 3.3.5. *Seien L/K und E/K Körpererweiterungen und $\sigma_1, ..., \sigma_n$ paarweise verschiedene Ringhomomorphismen $\sigma_i : L \to E$ mit $\sigma_i|K = \mathrm{id}$. Dann gilt:*

$$n \leq [L : K]$$

Beweis. Für $[L : K] = \infty$ ist die Aussage inhaltslos, sei also $[L : K] = m$ endlich und sei $l_1, ..., l_m \in L$ eine K-Basis von L. Falls $n > m$, dann existiert

$$0 \neq (\lambda_1, \lambda_2, ..., \lambda_n) \in E^n,$$

so dass

$$\begin{pmatrix} \sigma_1(l_1) & \cdots & \sigma_n(l_1) \\ \vdots & & \vdots \\ \sigma_1(l_m) & \cdots & \sigma_n(l_m) \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = 0$$

Doch da $\{l_i\}$ eine Basis bildet, folgt daraus $\sum_{i=1}^{n} \lambda_i\sigma_i = 0$. Dies steht jedoch im Widerspruch zum Dedekind-Lemma 3.3.3. □

Der Satz 3.3.2 folgt natürlich sofort aus Satz 3.3.5 mit $L = E$.

3.4 Galoiserweiterungen

Definition 3.4.1. Eine endliche Körpererweiterung L/K heißt *Galoiserweiterung*, oder auch *galoissch*, falls gilt:

$$|G(L/K)| = [L : K].$$

Sei L ein Körper und $G \leq \mathrm{Aut}(L)$ eine Gruppe von Körperautomorphismen von L. Wir nennen den Unterkörper (!)

$$L^G := \{l \in L \mid \text{für alle } \sigma \in G\text{: } \sigma(l) = l\} \subseteq L$$

den *Fixkörper von G*.

Satz 3.4.2. *Sei L/K eine Galoiserweiterung mit Galoisgruppe $G = G(L/K)$. Dann gilt:*

$$L^G = K.$$

Beweis. Es folgt aus den Definitionen, dass $G(L/K) = G(L/L^G)$ gilt. Weiterhin gilt

$$K \subseteq L^G \subseteq L.$$

Daher gilt einerseits, da L/K galoissch ist, $|G| = [L : K]$, und andererseits, wegen Satz 3.3.2, $|G| \leq [L : L^G]$, also letztlich wegen Lemma 3.2.1 auch $[L^G : K] = 1$. Daraus folgt (!) nun aber sofort $L^G = K$. □

Satz 3.4.3 (Artin). *Sei L ein Körper und $G \leq \mathrm{Aut}(L)$. Dann gilt*

$$[L : L^G] = |G|.$$

Insbesondere ist also, für G endlich, die Körpererweiterung L/L^G galoissch mit Galoisgruppe G.

Beweis. Wir setzen $K = L^G$. Wegen $G \leq G(L/L^G)$ gilt

$$|G| \leq |G(L/L^G)| \leq [L : L^G],$$

wobei die letzte Ungleichung aus Satz 3.3.2 folgt. Es genügt also, $[L : L^G] \leq |G|$ zu zeigen. Sei o.E. $|G| = n < \infty$, denn sonst ist die Aussage inhaltslos. Wir zeigen nun, dass je $n+1$ Elemente $x_1, ..., x_{n+1} \in L$ linear abhängig über K sind. Betrachte dazu, für $G = \{\sigma_1, ..., \sigma_n\}$, das L-lineare Gleichungssystem

$$\sum_{j=1}^{n+1} Y_j \sigma_i(x_j) = 0, \quad 1 \leq i \leq n \tag{3.4.4}$$

in den Variablen $Y_1, ..., Y_{n+1}$. Dieses hat n Gleichungen und $n+1$ Unbekannte, also gibt es eine nichttriviale Lösung

$$0 \neq (\lambda_1, ..., \lambda_{n+1}) \in L^{n+1},$$

wobei wir o.E. annehmen: $\lambda_1 \neq 0$. Für $1 \leq i \leq n$ wenden wir σ_i^{-1} auf die i-te Gleichung von (3.4.4) an und erhalten

$$\sum_{j=1}^{n+1} \sigma_i^{-1}(\lambda_j) x_j = 0.$$

Eine Summation über alle so erhaltenen Gleichungen ergibt:

$$\sum_{j=1}^{n+1} \alpha_j x_j = 0 \tag{3.4.5}$$

mit

$$\alpha_j = \sum_{i=1}^{n} \sigma_i^{-1}(\lambda_j) = \sum_{\sigma \in G} \sigma(\lambda_j) \in L^G = K.$$

Wegen des Dedekind-Lemmas gilt $\sum_{\sigma \in G} \sigma \neq 0$, so dass es also ein $0 \neq l \in L$ gibt mit $\sum_{\sigma \in G} \sigma(l) \neq 0$. Indem wir nun die Lösung $(\lambda_1, ..., \lambda_n)$ durch die Skalierung

$$(l\lambda_1^{-1}\lambda_1, ..., l\lambda_1^{-1}\lambda_{n+1})$$

mit dem Skalarfaktor $l\lambda_1^{-1}$ ersetzen, erreichen wir $\alpha_1 \neq 0$, so dass also (3.4.5) eine nichttriviale K-Linearkombination der Elemente $\{x_j\}$ ist. □

Korollar 3.4.6. *Sei L/K eine endliche Körpererweiterung. Dann gilt*

$$|G(L/K)| | [L : K].$$

Beweis. Es gilt

$$[L : K] = [L : L^G][L^G : K],$$

wobei nach dem Satz von Artin gilt: $[L : L^G] = |G|$. □

3.5 Die Galoiskorrespondenz

Für eine Körpererweiterung L/K bezeichnen wir mit

$$\mathcal{U}(G) := \{H \mid H \leq G \text{ Untergruppe}\}$$

die Menge der Untergruppen von G sowie mit

$$\mathcal{Z}(L/K) := \{M \mid K \subseteq M \subseteq L \text{ Zwischenkörper}\}$$

die Menge der *Zwischenkörper von* L/K, also Unterkörper $M \subseteq L$ mit $K \subseteq M$.

Satz 3.5.1 (Galoiskorrespondenz)**.** *Sei L/K eine Galoiserweiterung mit Galoisgruppe $G = G(L/K)$. Dann sind die Abbildungen*

$$\varphi : \mathcal{U}(G) \to \mathcal{Z}(L/K),\ H \mapsto L^H$$

und

$$\psi : \mathcal{Z}(L/K) \to \mathcal{U}(G),\ M \mapsto G(L/M)$$

zueinander inverse Bijektionen.

Beweis. Nach dem Satz von Artin (Satz 3.4.3) gilt $G(L/L^H) = H$, also $\psi \circ \varphi = \mathrm{id}$, so dass insbesondere φ injektiv ist. Es verbleibt also zu zeigen, dass φ surjektiv ist. Dazu nehmen wir an, es gäbe einen Zwischenkörper $K \subseteq M \subseteq L$, der nicht im Bild von φ liegt, und führen dies zum Widerspruch.

Schritt 1. Zunächst wählen wir einen Zwischenkörper $K \subseteq M \subseteq L$ mit $M \notin \mathrm{Bild}(\varphi)$ und $\dim_K(M)$ minimal. Insbesondere gilt also für jeden echten Teilkörper $K \subseteq M' \subsetneq M$, dass $M' \in \mathrm{Bild}(\varphi)$.

Schritt 2. Wir wählen nun $H \leq G$ minimal mit der Eigenschaft $L^H \subseteq M$, es gilt also für alle echten Untergruppen $H' \lneq H$: $L^{H'} \not\subseteq M$. Ein solches H existiert, denn $L^G = K \subseteq M$. Indem wir nun G durch H und K durch L^H ersetzen, können wir ohne Einschränkung annehmen, dass M/K keine echten Zwischenkörper enthält.

Schritt 3. Wir wählen weiter $\alpha \in M \setminus K$ und betrachten das Bild $K[\alpha]$ des Evaluationshomomorphismus

$$K[X] \to M,\ f(X) \mapsto f(\alpha).$$

Dann ist $K[\alpha]$ ein endlich–dimensionaler K-Vektorraum und für jedes $0 \neq x \in K[\alpha]$ ist die Multiplikationsabbildung auf $K[\alpha]$ eine injektive K-lineare Abbildung (denn M ist ein Körper), und daher aus Dimensionsgründen auch surjektiv. Demnach ist also $K[\alpha] \subseteq M$ ein Unterkörper, so dass wegen unserer Annahme aus Schritt 2 gilt: $K[\alpha] = M$.

Schritt 4. Wir betrachten den Stabilisator

$$G_\alpha = \{\sigma \in G \mid \sigma(\alpha) = \alpha\} \leq G.$$

Es gilt

$$K \subseteq K[\alpha] \subseteq L^{G_\alpha}$$

und weiter

$$[L^{G_\alpha} : K] = \frac{[L : K]}{[L : L^{G_\alpha}]} = \frac{|G|}{|G_\alpha|} = |G.\alpha| \tag{3.5.2}$$

wobei wir hier den Satz von Artin und die Bahnformel anwenden.

Schritt 5. Unter den Einschränkungen

$$\sigma|M : M \to L$$

von Automorphismen $\sigma \in G(L/K)$ gibt es mindestens $|G.\alpha|$ verschiedene Homomorphismen, denn diese bilden jeweils α auf $\sigma(\alpha)$ ab. Aus Satz 3.3.5 folgt also

$$|G.\alpha| \leq [M : K]. \tag{3.5.3}$$

Schritt 6. Aus (3.5.2) und (3.5.3) folgt nun aber $[L^{G_\alpha} : K] = [M : K]$ (denn $M \subseteq L^{G_\alpha}$) und daher $L^{G_\alpha} = M$, also $M \in \text{Bild}(\varphi)$. Ein Widerspruch. □

Bemerkung 3.5.4. Die Mengen $\mathfrak{U}(G)$ und $\mathfrak{Z}(L/K)$ aus Satz 3.5.1 sind partiell geordnet (gegeben durch $\subseteq$). Diese partielle Ordnung wird durch die Galoiskorrespondenz umgekehrt, es gilt also für Untergruppen $H_1, H_2 \leq G$:

$$H_1 \leq H_2 \quad \Longleftrightarrow \quad L^{H_2} \subseteq L^{H_1}.$$

Wir untersuchen nun weitere Eigenschaften der Galoiskorrespondenz.

Satz 3.5.5. *Sei L/K eine Galoiserweiterung mit Galoisgruppe $G = G(L/K)$ und sei $H \leq G$ eine Untergruppe. Dann gelten:*

(1) Es gibt genau $(G : H)$ verschiedene Ringhomomorphismen (Körpereinbettungen)

$$\tau : L^H \to L$$

mit der Eigenschaft $\tau|K = \text{id}_K$. Für jede dieser Einbettungen gibt es einen Automorphismus $\sigma \in G$, so dass $\tau = \sigma|L^H$.

(2) Für $\sigma \in G$ gilt

$$\sigma(L^H) = L^{\sigma H \sigma^{-1}},$$

der Bildkörper $\sigma(L^H)$ ist also der Fixkörper der zu H konjugierten Untergruppe $\sigma H \sigma^{-1}$.

(3) Die Körpererweiterung L^H/K ist genau dann galoissch, wenn $H \trianglelefteq G$ eine normale Untergruppe ist. In diesem Falle definiert die Einschränkungsabbildung

$$\rho : G \to G(L^H/K), \sigma \mapsto \sigma|L^H$$

einen surjektiven Gruppenhomomorphismus mit Kern H, es gilt also insbesondere

$$G(L^H/K) \cong G/H.$$

Beweis. (1) Wir bezeichnen mit $\mathcal{E}$ die Menge der Ringhomomorphismen $\tau : L^H \to L$ mit $\tau|K = \text{id}$. Die Galoisgruppe G operiert auf $\mathcal{E}$ via

$$\sigma.\tau = \sigma \circ \tau.$$

Der Stabilisator der Inklusionseinbettung $\iota : L^H \subseteq L$ ist, nach dem Satz von Artin, genau H. Daher gilt:

$$(G : H) = |G.\iota| = |\{\tau \in \mathcal{E} \mid \tau = \sigma|L^H \text{ für ein } \sigma \in G\}| \leq |\mathcal{E}|$$

Andererseits gilt nach Satz 3.3.5

$$|\mathcal{E}| \leq [L^H : K] = \frac{[L : K]}{[L : L^H]} = \frac{|G|}{|H|} = (G : H).$$

(2) Für $\sigma \in G$, $\gamma \in H$ und $x \in L$ gilt

$$\gamma(x) = x \quad \Longleftrightarrow \quad \sigma\gamma\sigma^{-1}(\sigma(x)) = \sigma(x).$$

(3) Nach (1) gilt

$$|\mathcal{E}| = [L^H : K].$$

Die Abbildung

$$\epsilon : G(L^H/K) \to \mathcal{E}, \alpha \mapsto \iota \circ \alpha$$

definiert eine Injektion, so dass also gilt: $|G(L^H/K)| \leq |\mathcal{E}| = [L^H : K]$. Demnach ist die Erweiterung L^H/K galoissch genau dann, wenn die Abbildung ϵ eine Bijektion ist, wenn also für jede der Einbettungen aus $\tau \in \mathcal{E}$ gilt: $\tau(L^H) = L^H$. Da nach (1) die Einschränkungsabbildung eine Surjektion $G \to \mathcal{E}$ definiert, ist dies wegen (2) und Satz 3.5.1 äquivalent zur Bedingung

$$\forall \sigma \in G : \sigma H \sigma^{-1} = H$$

also $H \trianglelefteq G$ normal. In diesem Falle definiert also, für jedes $\sigma \in G$, die Einschränkung $\sigma|L^H$ einen Automorphismus von L^H, so dass wir einen wohldefinierten surjektiven Homomorphismus

$$G \to G(L^H/K),\ \sigma \mapsto \sigma|L^H$$

mit Kern $G(L/L^H) = H$ erhalten. □

Bemerkung 3.5.6. Die verfeinerten Eigenschaften der Galoiskorrespondenz aus Satz 3.5.5 lassen sich sehr einprägsam wie folgt interpretieren:

Die Galoiskorrespondenz definiert eine kanonische Bijektion zwischen der Menge $\mathcal{U}(G)$ der Untergruppen von G und der Menge $\mathcal{Z}(L/K)$ von Zwischenkörpern von L/K. Beide Mengen sind mit natürlichen Wirkungen der Gruppe G ausgestattet: G operiert auf $\mathcal{U}(G)$ via Konjugation, also $\sigma.H = \sigma H \sigma^{-1}$, und auf $\mathcal{Z}(L/M)$ via $\sigma.M = \sigma(M)$. Satz 3.5.5 impliziert nun, dass die Galoiskorrespondenz eine *G-äquivariante* Bijektion ist, die also die beiden G-Wirkungen ineinander überführt:

$$G \circlearrowright \mathcal{U}(G) \quad \overset{\cong}{\longleftrightarrow} \quad \mathcal{Z}(L/K) \circlearrowleft G$$

Die Fixpunkte dieser G-Wirkungen entsprechen einerseits den normalen Untergruppen von G und andererseits den Galoiserweiterungen von K. Allgemeiner entsprechen die Bahnen der G-Wirkung auf $\mathcal{U}(G)$ Konjugationsklassen von Untergruppen, welche über die Galoiskorrespondenz mit G-Bahnen in $\mathcal{Z}(L/K)$ identifiziert werden. Diese entsprechen (!) Isomorphieklassen von Zwischenkörpern über K.

Aufgabe 3.5.7. Sei L/K eine Galoiserweiterung mit Galoisgruppe $G(L/K)$ und $H \leq G$ eine Untergruppe mit zugehörigem Zwischenkörper $M = L^H$. Wir definieren die Normalisatoruntergruppe

$$\mathrm{N}_G(H) = \{\sigma \in G \mid \sigma H \sigma^{-1} = H\} \leq G$$

von H in G. Dann gelten:

(1) Die Inklusionsabbildung $G(M/K) \subseteq G(M/L^{\mathrm{N}_G(H)})$ ist ein Isomorphismus.

(2) Die Untergruppe $H \leq \mathrm{N}_G(H)$ ist normal und die Körpererweiterung $M/L^{\mathrm{N}_G(H)}$ ist galoissch mit Galoisgruppe $\mathrm{N}_G(H)/H$.

(3) Sei $\mathcal{Z}_M$ die Menge der zu M/K isomorphen Zwischenkörper von L/K. Dann gilt:

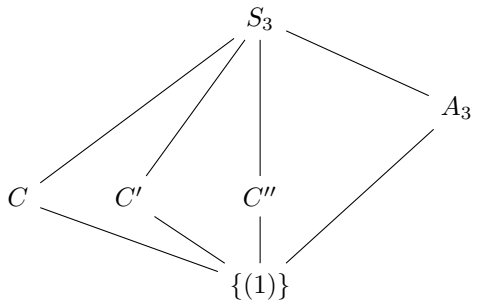
$$|\mathcal{Z}_M| = (G : \mathrm{N}_G(H)).$$

(4) Insbesondere gilt

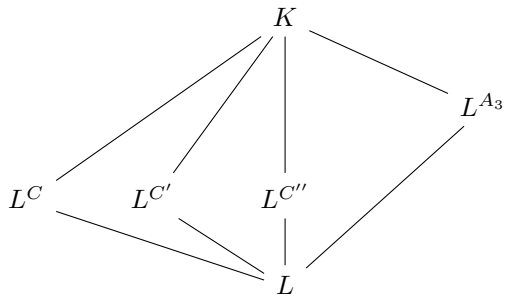
$$(G : H) = |\mathcal{Z}_M||G(M/K)|.$$

Beispiel 3.5.8. Sei L/K eine Galoiserweiterung mit Galoisgruppe $G(L/K) \cong S_3$. In §3.6 werden wir sehen, dass die Erweiterung $\mathbb{Q}(f)/\mathbb{Q}$ für $f(X) = X^3 - 2$ ein Beispiel für eine solche Erweiterung ist. Nach der

Galoiskorrespondenz entspricht der partiell geordneten Menge von Untergruppen



von S_3, mit $C = \langle(12)\rangle$, $C' = \langle(23)\rangle$, $C'' = \langle(13)\rangle$, die Menge von Zwischenkörpern



von L/K. Dabei ist die Erweiterung L^{A_3}/K galoissch mit Galoisgruppe $S_3/A_3 \cong C_2$. Die restlichen Zwischenkörper L^C, $L^{C'}$ und $L^{C''}$ sind nicht galoissch: Die zugehörigen Gruppen C, C' und C'' sind kongugiert, so dass die Zwischenkörper L^C, $L^{C'}$ und $L^{C''}$ also isomorph über K sind. Vom Standpunkt der G-Wirkungen aus Bemerkung 3.5.6 wirkt die Gruppe S_3 mit Fixpunkt A_3 (bzw. L^{A_3}) und durch zyklische Permutation der Untergruppen Gruppen C, C' und C'' (bzw. L^C, $L^{C'}$ und $L^{C''}$).

3.6 Zerfällungskörper

Definition 3.6.1. Sei K ein Körper und $f \in K[X]$ ein Polynom. Ein Körper E mit $K \subseteq E$ heißt *Zerfällungskörper* von f falls

(1) $f = c(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n) \in E[X]$,

(2) $E = K(\alpha_1, ..., \alpha_n)$,

wobei

$$K(\alpha_1, ..., \alpha_n) := \bigcap_{\substack{L \in \mathfrak{L}(E/K) \\ \{\alpha_1,...,\alpha_n\} \subseteq L}} L.$$

Satz 3.6.2. *Sei K ein Körper und $f \in K[X]$ ein Polynom. Dann existiert ein Zerfällungskörper von f und ist bis auf Körperisomorphie über K eindeutig bestimmt.*

Beweis. Wir zeigen zunächst die Existenz. Für eine Körpererweiterung L/K, die eine Nullstelle $\alpha \in L$ von f enthält, gilt

$$f(X) = (X - \alpha)g(X) \in L[X]$$

für $g(X) \in L[X]$ mit $\operatorname{grad}(g(X)) < \operatorname{grad}(f(X))$. Es genügt also, für allgemeines K und f einen Körper L/K zu konstruieren, der eine Nullstelle von f enthält (denn dann kann diese Konstruktion iteriert werden, bis f vollständig in Linearfaktoren zerfällt). Ohne Einschränkung können wir hierbei annehmen, dass f irreduzibel ist (indem wir die Konstruktion auf einen Primfaktor von f anwenden). In diesem Fall erhalten wir mit

$$L := K[T]/(f(T)) \tag{3.6.3}$$

einen Körper, der die Nullstelle $\alpha = [T]$ von f enthält. Körpererweiterungen der Form L/K wie in (3.6.3) nennen wir auch *primitive* Erweiterungen. Durch die oben angedeutete sukzessive Anwendung dieser Konstruktion ergibt sich also ein Turm

$$K \hookrightarrow L_1 \hookrightarrow L_2 \hookrightarrow ... \hookrightarrow L_m$$

von primitiven Körpererweiterungen, wobei L_m ein Zerfällungskörper ist (!). Zum Beweis der Eindeutigkeit benötigen wir noch ein vorbereitendes Lemma. □

Für eine Körpereinbettung $\varphi : L \hookrightarrow E$ und

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_0 \in L[X]$$

definieren wir

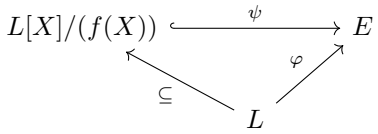
$$f^\varphi(X) := \varphi(a_n) X^n + \varphi(a_{n-1}) X^{n-1} + ... + \varphi(a_n) \in E[X]. \tag{3.6.4}$$

Durch direktes Nachrechnen folgt, dass die Abbildung

$$L[X] \to E[X], f(X) \mapsto f^\varphi(X) \tag{3.6.5}$$

ein Ringhomomorphismus ist.

Lemma 3.6.6. *Sei $\varphi : L \hookrightarrow E$ eine Körpereinbettung, $f(X) \in L[X]$ irreduzibel, und $\alpha \in E$ eine Nullstelle von $f^\varphi(X)$. Dann gibt es eine eindeutig bestimmte Körpereinbettung*



so dass $\varphi(X) = \alpha$. Hier hatten wir schon darüber gesprochen: φ sollte wahrscheinlich ψ sein, korrekt? Selbiges im Beweis unten.

Beweis. Betrachte zunächst den Ringhomomorphismus

$$\xi : L[X] \to E, g \mapsto g^\varphi(\alpha)$$

definiert als die Komposition von (3.6.5) mit dem Evaluationshomomorphismus. Dann gilt

$$(f(X)) \subseteq \mathrm{Kern}(\xi) \subsetneq L[X].$$

Da aber $\widetilde{f(X)}$ irreduzibel ist, ist $(f(X))$ maximal, so dass also gilt: $(f(X)) = \mathrm{Kern}(\widetilde{\psi})$. Daher erhalten wir den gewünschten Homomorphismus als

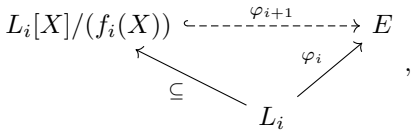
$$\psi := \bar{\xi} : L[X]/(f(X)) \to E.$$

□

Beweis der Eindeutigkeit des Zerfällungskörpers. Sei

$$K \hookrightarrow L_1 \hookrightarrow L_2 \hookrightarrow \cdots \hookrightarrow L_m$$

der im Existenzbeweis konstruierte Zerfällungskörper von $f(X)$ und E/K ein beliebiger Zerfällungskörper mit $L_{i+1} = L_i[X]/(f_i(X))$ für $f_i(X) \in L_i[X]$ irreduzibel. Wir behaupten, dass sich die Inklusionsabbildung $\varphi_0 : K \to E$ zu einer Folge $\varphi_i : L_i \hookrightarrow E$ von Einbettungen fortsetzen lässt, so dass gilt: $\varphi_{i+1}|L_i = \varphi_i$. Wir beweisen dies induktiv, mit folgendem Induktionsschritt:



,

wobei es für die Existenz von φ_{i+1} nach Lemma 3.6.6 ausreicht zu zeigen, dass das Polynom $f_i^{\varphi_i}(X) \in E[X]$ eine Nullstelle besitzt. Es gilt

$$f(X) = f_i(X)g(X) \in L_i[X]$$

mit $f_i(X)$ irreduzibel und demnach auch

$$f(X) = f^{\varphi_i}(X) = f_i^{\varphi_i}(X)g^{\varphi_i}(X) \in E[X].$$

Da E ein Zerfällungskörper ist, zerfällt $f(X)$ in Linearfaktoren (Primfaktoren) und daher auch $f_i^{\varphi_i}(X)$ (und auch $g^{\varphi_i}(X)$), also

$$f_i^{\varphi_i}(X) = b(X-\beta_1)\cdots(X-\beta_k),$$

so dass die Elemente $\beta_1, ..., \beta_k \in E$ Nullstellen von $f_i^{\varphi_i}(X)$ sind. Schließlich gilt zudem, dass die Inklusion $\varphi_n : L_n \hookrightarrow E$ surjektiv ist, denn in $L_m[X]$ gilt

$$f(X) = c(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_m) \in L_n[X]$$

und somit

$$f(X) = f^{\varphi_m}(X) = \varphi_m(c)(X-\varphi_m(\alpha_1))(X-\varphi_m(\alpha_2))\cdots(X-\varphi_m(\alpha_n)) \in E[X].$$

Daher enthält das Bild von φ_m alle Nullstellen $\varphi_m(\alpha_1), ..., \varphi_m(\alpha_n) \in E$ von $f(X)$ in E, und daher

$$E = K(\varphi_m(\alpha_1), ..., \varphi_m(\alpha_n)) \subseteq \text{Bild}(\varphi_n).$$

Ich bin hier etwas verwirrt hinsichtlich der Indizes: Erst zerlegen wir in m Nullstellen über L_n, dann wenden wir φ_m auf einmal auf n Nullstellen über E an. Ist hier eventuell einmal n und m durcheinandergeraten? □

Beispiel 3.6.7. Sei $f(X) = X^4 - 2 \in \mathbb{Q}[X]$. Ein Zerfällungskörper von f lässt sich durch einen Turm von zwei primitiven Erweiterungen konstruieren: Zunächst ist

$$L = \mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}[T]/(f_1(T))$$

eine primitive Erweiterung für das irreduzible Polynom f (Eisenstein-Kriterium), wobei $\sqrt[4]{2} \in \mathbb{C}$ die eindeutige reelle positive 4te Wurzel in $\mathbb{R}$ bezeichnet. Über L zerlegt sich f in

$$f(X) = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X^2 + \sqrt{2}).$$

Das Polynom

$$f_1(X) = X^2 + \sqrt{2} \in L[X] \subseteq \mathbb{R}[X]$$

ist irreduzibel, denn es hat keine reellen Nullstellen. Es definiert daher die primitive Erweiterung

$$E = L[T]/(f_1(T)) \cong \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$$

Alternativ können wir

$$\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$$

als primitive Erweiterung

$$L[S]/(S^2+1)$$

bezüglich des irreduziblen Polynoms $S^2 + 1 \in L[S]$ mit Nullstellen $\pm i \in \mathbb{C}$ beschreiben. Es gilt in $E[X]$:

$$f(X) = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2}),$$

so dass E also ein Zerfällungskörper von f ist.

Wir erhalten

$$[E : \mathbb{Q}] = [E : L][L : \mathbb{Q}] = 2 \cdot 4 = 8.$$

Durch jeweils zweimaliges Anwenden von Lemma 3.6.6 konstruieren wir die folgenden Automorphismen $\sigma, \tau \in G := G(E, \mathbb{Q})$:

$$\tau : E \to E, \begin{cases} \sqrt[4]{2} & \mapsto \sqrt[4]{2} \\ i & \mapsto -i \end{cases}$$

$$\sigma : E \to E, \begin{cases} \sqrt[4]{2} & \mapsto i\sqrt[4]{2} \\ i & \mapsto i. \end{cases}$$

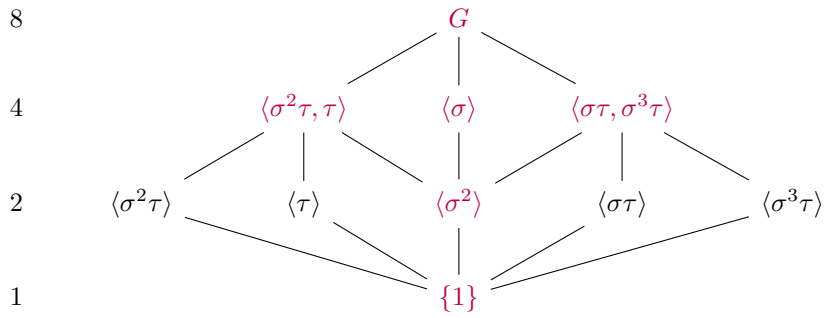
Zum Beispiel unter Zuhilfenahme der Veranschaulichung in Figur 3.1 sieht man ein, dass

$$D_4 \cong \langle \sigma, \tau \rangle \leq G$$

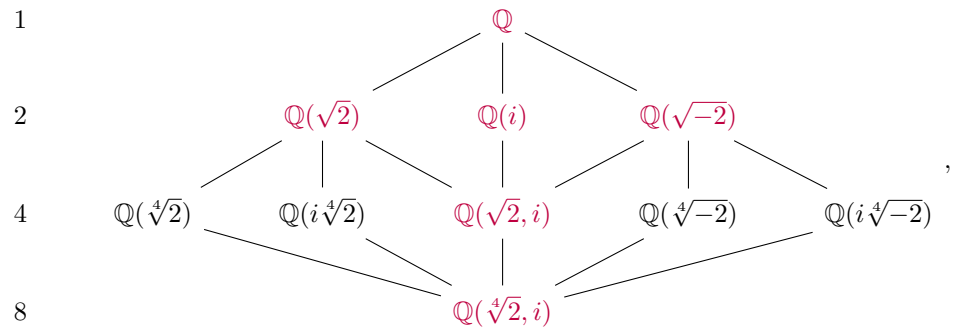
gilt. Wegen Satz 3.3.2 gilt $|G| \leq [E : \mathbb{Q}] = 8$, so dass also gelten muss :

$$\langle \sigma, \tau \rangle = G.$$

Die Menge der Untergruppen $\mathfrak{U}(G)$ sieht wie folgt (!) aus



wobei in der linken Spalte die Ordnungen angegeben sind und die farbigen Gruppen die normalen Untergruppen kennzeichnen. Die korrespondierende Menge der Zwischenkörper von E/K lässt sich wie folgt (!) beschreiben



,

wobei in der linken Spalte der Grad der Körpererweiterungen über $\mathbb{Q}$ angegeben ist und die farbig gekennzeichneten Körper die Galoiserweiterungen von $\mathbb{Q}$ sind. Um zu überprüfen, dass ein angegebener Zwischenkörper M tatsächlich der Fixkörper der korrespondierenden Untergruppe H ist, zeigt man jeweils

1. $M \subseteq E^H$, und
2. $[K : M] = (G : H)$.

Diese Bedingungen implizieren $M = E^H$. Hierbei bedeuten genauer:

$$\sqrt{-2} := i\sqrt{2}$$
$$\sqrt[4]{-2} := \frac{1+i}{\sqrt{2}}\sqrt[4]{2},$$

wobei wir bemerken, dass $\zeta := \frac{1+i}{\sqrt{2}}$ eine primitive achte Einheitswurzel ist (deren Potenzen also alle achten Einheitswurzeln durchläuft), insbesondere gilt $\zeta^4 = -1$. Es gilt weiter

$$\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta),$$

so dass dieser Körper also der Zerfällungskörper des Polynoms $X^8 - 1$ ist. Unter der Galoiskorrespondenz korrespondiert $\mathbb{Q}(\zeta)$ zum Zentrum $\langle \sigma^2 \rangle$ von G. Die Galoisgruppe $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ ist demnach isomorph zu

$$G/\langle \sigma^2 \rangle \cong C_2 \times C_2.$$

Die Galoisgruppen der Zerfällungskörper der Polynome $X^n - 1$, der sogenannten *Kreisteilungskörper*, werden wir im nachfolgenden Abschnitt systematischer untersuchen.

Definition 3.6.8. Sei K ein Körper. Ein irreduzibles Polynom $f \in K[X]$ heißt *separabel*, falls in seinem Zerfällungskörper E/K gilt:

$$f = c(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_k) \in E[X]$$

mit paarweise verschiedenen $\alpha_i \in E$, falls also f in E nur *einfache Nullstellen* hat. Im Allgemeinen heißt ein Polynom in $K[X]$ *separabel*, falls jeder seiner Primfaktoren separabel ist.

Satz 3.6.9. *Sei K ein Körper, $f \in K[X]$ ein separables Polynom, und E ein Zerfällungskörper von f. Dann ist E/K eine Galoiserweiterung.*

Beweis. Der Beweis von Satz 3.6.2 zeigt, dass es eine Kette von primitiven Körpererweiterungen der Form

$$K \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n = E$$

gibt. Es gilt also $L_{i+1} \cong L_i[X]/(f_i)$ für $f_i \in L_i[X]$ irreduzibel. Zu einer gegebenen Einbettung $\varphi_i : L_i \hookrightarrow E$ betrachten wir

$$\begin{array}{ccc} L_{i+1} & \overset{\varphi_{i+1}}{\dashrightarrow} & E \\ \subseteq\uparrow & \nearrow_{\varphi_i} & \\ L_i & & \end{array} .$$

Nach Lemma 3.6.6 gibt es für jede Nullstelle α von $f_i^{\varphi_i}$ in E eine Einbettung φ_{i+1} mit $\varphi_{i+1}(X) = \alpha$. Doch f_i ist Primfaktor des Polynoms $f \in L_i[X]$ und teilt daher (!) einen Primfaktor von $f \in K[X]$. Das Polynom f_i (und damit auch $f_i^{\varphi_i}$) besitzt also genau $\operatorname{grad}(f_i)$ verschiedene Nullstellen in E, so dass es daher auch genau $\operatorname{grad}(f_i) = [L_{i+1} : L_i]$ verschiedene Fortsetzungen φ_{i+1} der vorgegebenen Einbettung φ_i gibt.

Sukzessive erhalten wir durch diese Konstruktion also

$$[E : L_{n-1}][L_{n-1} : L_{n-2}] \cdots [L_1 : K] = [E : K]$$

verschiedene Einbettungen $L_n \hookrightarrow L_n = E$ Hier müsste $L_{n-1} \hookrightarrow L_n = E$ stehen, oder?, die, mit dem Argument im Eindeutigkeitsbeweis von Satz 3.6.2, auch surjektiv sind. Also gilt wegen Satz 3.3.2

$$[E : K] = |G(E/K)|,$$

so dass E/K galoissch ist. □

Es gilt auch umgekehrt:

Aufgabe 3.6.10. Jede Galoiserweiterung E/K ist Zerfällungskörper eines separablen Polynoms in $K[X]$.

Wir stellen nun noch ein einfaches Kriterium zum Testen der Separabilität eines Polynoms bereit. Dazu definieren wir für

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \in K[X]$$

die *algebraische Ableitung*

$$\partial f = \frac{\mathrm{d}f}{\mathrm{d}X} = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \ldots + a_1 \in K[X].$$

Man verifiziert durch direkte Rechnung: Für $\lambda \in K$ und $f, g \in K[X]$ gelten

$$\partial(\lambda f + g) = \lambda\partial(f) + \partial(g) \qquad K\text{-Linearität} \tag{3.6.11}$$

$$\partial(fg) = f\partial(g) + \partial(f)g \qquad \text{Leibnizregel} \tag{3.6.12}$$

Lemma 3.6.13. *Sei $f \in K[X]$ ein Polynom, L/K Körpererweiterung und $\alpha \in L$ Nullstelle von f. Dann sind äquivalent:*

(i) α *einfach,*

(ii) $\partial f(\alpha) \neq 0$.

Beweis. Die Nullstelle α ist genau dann einfach, wenn gilt

$$f(X) = (X - \alpha)g(X)$$

mit $(X - \alpha) \nmid g(X)$, so dass die Behauptung sofort aus (3.6.12)

$$\partial f = g(X) + (X - \alpha)\partial g \tag{3.6.14}$$

folgt. □

Proposition 3.6.15. *Sei K ein Körper und sei $f \in K[X]$ ein irreduzibles Polynom. Dann sind äquivalent:*

(i) f *ist separabel.*

(ii) $\mathrm{ggT}(f, \partial f) = 1$.

(iii) $\partial f \neq 0$.

Beweis. Wir zeigen zunächst die Äquivalenz von (i) und (ii): Sei E/K ein Zerfällungskörper von f. Falls f separabel ist, dann folgt aus (3.6.14), dass keiner der Primfaktoren $(X - \alpha)$ von f in $E[X]$ ein Teiler von ∂f ist, also sind f und ∂f koprim. Sei umgekehrt $\mathrm{ggT}(f, \partial f) = 1$, dann gibt es also $r, s \in K[X]$ mit

$$rf + s\partial f = 1. \tag{3.6.16}$$

Für eine Nullstelle $\alpha \in E$ von f muss dann aber $\partial f(\alpha) \neq 0$ gelten, denn sonst impliziert Evaluation von (3.6.16) bei α die Gleichung $0 = 1$.

Nun zur Äquivalenz von (ii) und (iii): Falls (ii) gilt, dann folgt aus (3.6.16) sofort (iii) denn sonst wäre f eine Einheit in $K[X]$. Falls umgekehrt $\partial f \neq 0$, dann folgt, wegen $\mathrm{grad}(\partial f) < \mathrm{grad}(f)$ und f irreduzibel, dass die einzigen gemeinsamen Teiler von f und ∂f Einheiten sind. □

Korollar 3.6.17. *Sei K ein Körper.*

(1) Falls $\mathrm{char}(K) = 0$*, so ist jedes Polynom $f \in K[X]$ separabel.*

(2) Falls $\mathrm{char}(K) = p$*, so sind für ein irreduzibles Polynom $f \in K[X]$ äquivalent:*

(i) f inseparabel.

(ii) Es gibt $g \in K[X]$ mit $f(X) = g(X^p)$.

Beispiel 3.6.18. Sei K ein Körper der Charakteristik $p > 0$ und sei $f = X^p - a \in K[X]$. Im Zerfällungskörper E/K besitzt f eine Nullstelle $\alpha \in E$, es gilt also $\alpha^p = a$. Dann gilt in $E[X]$:

$$(X - \alpha)^p = X^p + \sum_{k=1}^{p-1} \binom{p}{k} X^{p-k}(-\alpha)^k + (-\alpha)^p = X^p - a,$$

wobei $(-\alpha)^p = -\alpha^p = -a$, da p entweder ungerade ist, oder $1 = -1$ in K. Insbesondere ist also α eine Nullstelle mit Vielfachheit p, so dass f, in Übereinstimmung mit der Aussage von Korollar 3.6.17, inseparabel ist.

3.7 Permutationsdarstellung der Galoisgruppe

In diesem Abschnitt studieren wir die Galoisgruppe eines Polynoms über ihre Wirkung auf den Nullstellen in einem Zerfällungskörper.

Satz 3.7.1. *Sei K Körper, $f \in K[X]$ irreduzibel und separabel mit Leitkoeffizient 1 und $\mathrm{grad}(f) = n$. Über dem Zerfällungskörper E von f gilt also*

$$f = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

wobei $A = \{\alpha_1, ..., \alpha_n\}$ die Menge der (paarweise verschiedenen) Nullstellen von f in E bezeichnet. Sei weiter $G = G(E/K)$ die Galoisgruppe. Dann gelten:

(1) Die Operation $G \curvearrowright E$ schränkt sich ein auf eine Operation $G \curvearrowright A$.

(2) Die Operation $G \curvearrowright A$ ist treu, *d.h. falls für ein $\sigma \in G$ und für alle $\alpha_i \in A$ gilt: $\sigma(\alpha_i) = \alpha_i$, dann folgt schon $\sigma = \mathrm{id}$.*

(3) Die Operation $G \curvearrowright A$ ist transitiv, *d.h. für $\alpha_i \neq \alpha_j$ gibt es $\sigma \in G$ mit $\sigma(\alpha_i) = \alpha_j$.*

Beweis. (1) Die Galoisgruppe G operiert via Ringhomomorphismen auf $E[X]$ via

$$\sigma.g(X) = g^\sigma(X), \quad \sigma \in G, g \in E[X],$$

wobei wir die Notation 3.6.4 verwenden. Es gilt in $E[X]$:

$$\prod_{i=1}^{n}(X - \alpha_i) = f(X) = \sigma.f(X) = \prod_{i=1}^{n}(X - \sigma(\alpha_i)),$$

so dass σ die Nullstellen $\alpha_1, \alpha_2, ..., \alpha_n$ wegen der Eindeutigkeit der Primfaktorzerlegung in $E[X]$ permutieren muss.

(2) Jedes Element in E lässt sich als ein K-polynomialer Ausdruck in den Nullstellen $\alpha_1, \alpha_2, ..., \alpha_n$ schreiben. Wenn $\sigma \in G$ also alle α_i festhält, dann gilt $\sigma = \mathrm{id}_E$.

(3) Es gilt $E[X]^G = K[X]$. Falls $G \curvearrowright A$ nicht transitiv ist, dann zerlegt sich A in Bahnen

$$A = A_1 \dot\cup A_2 \dot\cup \cdots \dot\cup A_k$$

und es gilt entsprechend

$$f = f_1 f_2 \cdots f_k \in E[X] \tag{3.7.2}$$

mit

$$f_i(X) = \prod_{\alpha \in A_i}(X - \alpha).$$

Da die Wirkung von G für jedes $1 \leq i \leq k$ die Teilmenge A_i erhält, gilt $f_i \in E[X]^G = K[X]$. Damit gilt die Zerlegung (3.7.2) schon in $K[X]$, ein Widerspruch zur Irreduzibilität von f. □

Bemerkung 3.7.3. Für ein allgemeines separables Polynom $f \in K[X]$ betrachten wir die Primfaktorzerlegung

$$f(X) = \lambda f_1(X) f_2(X) \cdots f_k(X)$$

mit $f_i(X)$ irreduzbel und Leitkoeffizient 1. Sei E ein Zerfällungskörper von f. Das Argument im Beweis von Satz 3.7.1 (1) zeigt, dass sich die Wirkung $G \curvearrowright E$ auf eine Wirkung auf jeder der Nullstellenmengen A_i der irreduziblen Polynome $f_i(X)$ einschränkt. Für $n = \mathrm{grad}(f)$ und $n_i = \mathrm{grad}(f_i)$ (also $\sum n_i = n$) erhalten wir so einen Homomorphismus

$$G(E/K) \hookrightarrow S_{A_1} \times S_{A_2} \times \cdots S_{A_k} \cong S_{n_1} \times S_{n_2} \times \cdots \times S_{n_k} \hookrightarrow S_n$$

der nach dem Argument im Beweis von Satz 3.7.1 (2) injektiv ist. Wir können also $G(E/K)$ mit einer Untergruppe von S_n identifizieren und es gilt (Argument von Satz 3.7.1 (3)), dass f genau dann irreduzibel in $K[X]$ ist, wenn die Operation $G(E/K) \curvearrowright \{1, ..., n\}$ transitiv ist.

Für die Bestimmung der Galoisgruppe G eines irreduziblen, separablen Polynoms f ergibt sich folgende Strategie:

(1) Bestimme alle transitiven Untergruppen von S_n.

(2) Finde für jede transitive Untergruppe $H \leq S_n$ ein Kriterium, um zu entscheiden, ob $G \leq H$.

Wir illustrieren dies am Beispiel der transitiven Untergruppe

$$A_n \leq S_n.$$

Definition 3.7.4. Sei K ein Körper und $f \in K[X]$ ein irreduzibles separables Polynom vom Grad n. Sei E der Zerfällungskörper von f, so dass also

$$f(X) = \lambda \prod_{i=1}^{n} (X - \alpha_i)$$

für $\alpha_1, ..., \alpha_n \in E$ paarweise verschieden. Das Element

$$D := \prod_{i<j} (\alpha_i - \alpha_j)^2 \in E$$

wird von $G(E/K)$ festgehalten. Es liegt demnach in $K = E^{G(E/K)}$ und heißt die *Diskriminante* von f.

Bemerkung 3.7.5. Im Zerfällungskörper E besitzt die Diskriminante eine Quadratwurzel, nämlich

$$\delta = \prod_{i<j} (\alpha_i - \alpha_j) \in E.$$

Satz 3.7.6. *Sei K ein Körper mit $\mathrm{char}(K) \neq 2$, $f \in K[X]$ ein irreduzibles separables Polynom vom Grad n, E der Zerfällungskörper von f mit Galoisgruppe $G = G(E/K)$. Über die Einbettung $G \hookrightarrow S_n$ aus Bemerkung 3.7.3 identifizieren wir G mit seiner Bilduntergruppe in S_n, schreiben also einfach $G \leq S_n$. Dann sind äquivalent:*

(i) G ist eine Untergruppe der alternierenden Gruppe $A_n \leq S_n$.

(ii) Die Diskriminante D hat eine Quadratwurzel in K.

Beweis. Für $\sigma \in S_n$ gilt

$$\mathrm{sign}(\sigma) = (-1)^{f_\sigma},$$

wobei f_σ die Anzahl der Fehlstände von σ bezeichnet, also der Paare (i, j) mit $1 \leq i < j \leq n$ mit $\sigma(i) > \sigma(j)$. Daher gilt also für $\sigma \in G \subseteq S_n$:

$$\sigma(\delta) = \prod_{i<j} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) = \mathrm{sign}(\sigma)\delta. \tag{3.7.7}$$

Sei nun $G \subseteq A_n$. Dann folgt $\delta \in E^G = K$ mit $\delta^2 = D$. Sei umgekehrt $\alpha \in K$ mit $\alpha^2 = D$, dann gilt in E: $\alpha = \pm\delta$, also $\delta \in K$. Aus (3.7.7) folgt nun $G \subseteq A_n$ (hier verwenden wir die Annahme $\mathrm{char}(K) \neq 2$ sowie $\delta \neq 0$, da f irreduzibel und separabel ist). □

Beispiel 3.7.8. Sei K ein Körper mit $\mathrm{char}(K) \notin \{2, 3\}$ und $f(X) = X^3 + aX^2 + bX + c \in K[X]$ irreduzibel. Durch die Substitution $X \mapsto X - \frac{a}{3}$ reduzieren wir auf die Form $f(X) = X^3 + pX + q$. Sei E der Zerfällungskörper von f, so dass also

$$f(X) = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3) \in E[X]$$

und daher

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 0 \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= p \\ \alpha_1\alpha_2\alpha_3 &= -q. \end{aligned}$$

Eine explizite Rechnung unter Verwendung dieser Relationen zeigt

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = -4p^3 - 27q^2.$$

Später werden wir sehen, dass sich die Diskriminante D immer (auch für Polynome von höherem Grad) als polynomialer Ausdruck in den Koeffizienten des Polynoms schreiben lässt. Die transitiven Untergruppen von S_3 sind S_3 und A_3. Es gilt also

$$G(E/K) \cong \begin{cases} A_3 & \text{falls } D \text{ Quadrat in } K, \\ S_3 & \text{sonst.} \end{cases}$$

3.8 Die allgemeine Gleichung $n$ten Grades

Sei K Körper und S_n die symmetrische Gruppe. Wir betrachten die Operation (!) von S_n via Ringhomomorphismen auf dem Polynomring $K[X_1, ..., X_n]$, gegeben durch

$$(\sigma.f)(X_1, ..., X_n) = f(X_{\sigma^{-1}(1)}, ..., X_{\sigma^{-1}(n)}), \quad , \sigma \in S_n,\ f \in K[X_1, ..., X_n]. \tag{3.8.1}$$

Die Fixpunkte dieser Wirkung heißen *symmetrische Polynome*.

Beispiel 3.8.2. Die Diskriminante $D = \prod_{i<j}(X_i - X_j)^2$ aus (3.7.4) ist ein symmetrisches Polynom. Ebenso sind zum Beispiel die Polynome

$$X_1 + X_2 + \cdots + X_n$$

sowie

$$X_1 X_2 \cdots X_n$$

symmetrisch.

Wir betrachten nun das Polynom

$$g(X) = \prod_{i=1}^{n}(X - X_i) =: \sum_{j=0}^{n}(-1)^j e_j(X_1, ..., X_n)X^{n-j} \tag{3.8.3}$$

mit Koeffizienten in $K[X_1, ..., X_n]$. Da g ein Fixpunkt der induzierten (koeffizientenweisen) Operation von S_n auf $(K[X_1, ..., X_n])[X]$ ist, gilt für $1 \le j \le n$:

$$e_j(X_1, ..., X_n) \in K[X_1, ..., X_n]^{S_n}.$$

Definition 3.8.4. Die Polynome $e_j(X_1, ..., X_n)$, $j = 1, ..., n$, heißen die *elementar symmetrischen Polynome*. Es gilt explizit:

$$\begin{aligned} e_1 &= X_1 + X_2 + \ldots + X_n \\ e_2 &= \sum_{i<j} X_i X_j \\ &\vdots \\ e_n &= X_1 X_2 \cdots X_n \end{aligned}$$

Satz 3.8.5 (Hauptsatz über symmetrische Polynome)**.** *Der Einsetzungshomomorphismus*

$$\varphi : K[Y_1, ..., Y_n] \to K[X_1, ..., X_n],\ p(Y_1, ..., Y_n) \mapsto p(e_1, ..., e_n)$$

ist injektiv und induziert einen Isomorphismus

$$K[Y_1, ..., Y_n] \xrightarrow{\cong} \text{Bild}(\varphi) = K[X_1, ..., X_n]^{S_n}.$$

In Worten: Jedes symmetrische Polynom in den Variablen $X_1, ..., X_n$ lässt sich auf eindeutige Weise als polynomialer Ausdruck in den elementar symmetrischen Polynomen schreiben.

Beweis. Wir zeigen zunächst $\text{Bild}(\varphi) = K[X_1, ..., X_n]^{S_n}$. Die Inklusion $\subseteq$ ist klar, wir müssen also $\supseteq$ zeigen. Für $f \in K[X_1, ..., X_n]$ definieren wir den *(totalen) Grad* von f als Grad des Polynoms $f(X, X, ..., X) \in K[X]$.

Wir definieren weiter die *grad-lexikographische Ordnung* auf der Menge

$$M = \{X_1^{m_1} X_2^{m_2} \cdots X_n^{m_n} | m_i \in \mathbb{N}\}$$

der Monome, indem wir setzen: $X_1^{m_1} X_2^{m_2} \cdots X_n^{m_n} < X_1^{l_1} X_2^{l_2} \cdots X_n^{l_n}$ genau dann, wenn

(a) $\sum_i m_i < \sum_i l_i$, oder

(b) $\sum_i m_i = \sum_i l_i$ und es gibt $1 \leq j \leq n$, so dass

  (a) Für $1 \leq i < j$ gilt: $m_i = l_i$.

  (b) Es gilt $m_j < l_j$.

Diese Ordnung definiert eine Totalordnung auf der Menge M, so dass sich also jedes $f \in K[X_1, ..., X_n]$ eindeutig schreiben lässt als

$$f(X_1, ..., X_n) = \lambda X_1^{m_1} X_2^{m_2} \cdots X_n^{m_n} + r(X_1, ..., X_n)$$

mit *Leitmonom* $\text{LM}(f) = X_1^{m_1} X_2^{m_2} \cdots X_n^{m_n}$, das heißt, r ist eine K-Linearkombination von Monomen, die, bezüglich der grad-lexikographischen Ordnung, kleiner als das Leitmonom sind. Zudem gibt es eine (eindeutige) ordnungserhaltende Bijektion $M \cong \mathbb{N}$ (Es gibt endlich viele Monome mit einem vorgegebenen totalen Grad n, wir können M also Grad für Grad abzählen). Dies ermöglicht es uns die gewünschte Aussage per Induktion nach der grad-lexikographischen Ordnung von $\text{LM}(f)$ zu zeigen. Wir betrachten also genauer $f \in K[X_1, ..., X_n]^{S_n}$ und nehmen an (IA), dass für alle Polynome in $g \in K[X_1, ..., X_n]^{S_n}$ mit $\text{LM}(g) < \text{LM}(f)$ gilt: $g \in \text{Bild}(\varphi)$.

Wie schreiben $f \in K[X_1, ..., X_n]^{S_n}$ als

$$f = \lambda X_1^{m_1} X_2^{m_2} \cdots X_n^{m_n} + \text{Terme niederer Ordnung},$$

wobei $\lambda \neq 0$ und $X_1^{m_1} X_2^{m_2} \cdots X_n^{m_n}$ das Monom mit der maximalen Ordnung in f ist. Es gilt (!) dann $m_1 \geq m_2 \geq ... \geq m_n$. Dann gilt weiter

$$\begin{aligned} g &:= \lambda e_n^{m_n} e_{n-1}^{m_{n-1} - m_n} \cdots e_1^{m_1 - m_2} \\ &= \lambda X_1^{m_1} X_2^{m_2} \cdots X_n^{m_n} + \text{Terme niederer Ordnung}, \end{aligned}$$

also $\text{LM}(g) = \text{LM}(f)$ (Verwende um dies zu zeigen, dass LM multiplikativ ist, da die grad-lexikographische Ordnung multiplikativ ist). Das Polynom $f - g$ ist symmetrisch und hat ein grad-lexikographisch kleineres Leitmonom als f, so dass es per Induktionsannahme im Bild von φ liegt. Doch damit liegt, per Konstruktion von g, auch f im Bild von φ.

Es bleibt zu zeigen, dass φ injektiv ist. Dazu betrachten wir den Einsetzungshomomorphismus

$$\psi : K[X_1, ..., X_n] \to K[X_1, ..., X_{n-1}],\ p(X_1, ..., X_n) \mapsto p(X_1, ..., X_{n-1}, 0).$$

Es gilt dann $\psi(e_n) = 0$ und, für $j = 1, ..., n-1$, $\psi(e_j) = e'_j$ wobei e'_j das $j$te elementar symmetrische Polynom in den Variablen $X_1, ..., X_{n-1}$ bezeichnet. Nun zeigen wir die Implikation

$$p(e_1, e_2, ..., e_n) = 0 \Rightarrow p(X_1, X_2, ..., X_n) = 0$$

per Induktion nach $n + \text{grad}(p)$ wobei $\text{grad}(p)$ den totalen Grad bezeichnet. Falls $p(e_1, ..., e_n) = 0$, dann gilt auch

$$0 = \psi(p(e_1, ..., e_n)) = p(e'_1, ..., e'_{n-1}, 0).$$

Daher gilt per Induktion $p(X_1, ..., X_{n-1}, 0) = 0$, so dass es ein Polynom $h \in K[X_1, ..., X_n]$ gibt mit $p = X_n h$. Also gilt

$$\begin{aligned} p(e_1, ..., e_n) &= e_n h(e_1, ..., e_n) \\ &= X_1 \cdots X_n h(e_1, ..., e_n) = 0. \end{aligned}$$

Da $K[X_1, ..., X_n]$ nullteilerfrei ist, folgt also $h(e_1, ..., e_n) = 0$, so dass per Induktion $h(X_1, ..., X_n) = 0$ folgt. $\square$

Korollar 3.8.6. *Sei K ein Körper und $K(X_1, ..., X_n)$ der Körper der Brüche des Polynomrings $K[X_1, ..., X_n]$. Wir betrachten die S_n-Wirkung*

$$\sigma.\frac{f}{g} := \frac{\sigma.f}{\sigma.g}$$

auf $K(X_1, ..., X_n)$, induziert durch die S_n-Wirkung (3.8.1). Dann gilt

$$K(X_1, ..., X_n)^{S_n} = K(e_1, .., e_n).$$

Insbesondere ist die Körpererweiterung $K(X_1, ..., X_n)/K(e_1, ..., e_n)$ galoissch mit Galoisgruppe S_n.

Beweis. Es ist klar, dass $K(e_1, ..., e_n) \subseteq K(X_1, ..., X_n)^{S_n}$ gilt. Für die umgekehrte Inklusion sei $\frac{f}{g} \in K(X_1, ..., X_n^{S_n})$. Dann gilt

$$\frac{f}{g} = \frac{f \prod_{\sigma \neq \mathrm{id}} \sigma.g}{\prod_{\sigma \in S_n} \sigma.g}.$$

Weiter gilt für den Nenner $v := \prod_{\sigma \in S_n} \sigma.g$, dass $v \in K[X_1, ..., X_n]^{S_n}$ und damit für $u := f \prod_{\sigma \neq \mathrm{id}} \sigma.g$

$$\sigma.uv = uv,$$

also $\sigma.u = u$. Die restlichen Aussagen folgen sofort. □

Korollar 3.8.7. *Jede endliche Gruppe tritt als Galoisgruppe einer Körpererweiterung auf.*

Beweis. Dies folgt direkt aus Korollar 3.8.6 und der Galoiskorrespondenz. □

Bemerkung 3.8.8. Die Frage, ob jede endliche Gruppe als Galoisgruppe *über* $\mathbb{Q}$ auftritt, ist nicht geklärt.

Bemerkung 3.8.9. Die Galoiserweiterung aus Korollar 3.8.6 lässt sich wegen des Hauptsatzes über symmetrische Polynome beschreiben als

$$K(Y_1, ..., Y_n) \hookrightarrow K(X_1, ..., X_n), f(Y_1, ..., Y_n) \mapsto f(e_1, ..., e_n)$$

und ist damit der Zerfällungskörper der Polynoms

$$X^n - Y_1 X^{n-1} + Y_2 X^{n-2} + ... + (-1)^n Y_n$$

mit Koeffizienten im Körper $K(Y_1, ..., Y_n)$. Dieses Polynom nennen wir auch das *allgemeine Polynom n-ten Grades*, dessen Koeffizienten also durch algebraisch unabhängige Variablen gegeben sind. Die Variablen X_i sind damit die Lösungen der Gleichung

$$X^n - Y_1 X^{n-1} + Y_2 X^{n-2} + ... + (-1)^n Y_n = 0,$$

genannt *allgemeine Gleichung n-ten Grades*.

3.8.1 Kreisteilungskörper

Sei K ein Körper und $n \geq 1$. Wir bezeichnen mit

$$\mu_n(K) := \{\xi \in K | \xi^n = 1\}$$

die Menge der *n-ten Einheitswurzeln* in K. Es ist

$$\mu_n(K) \leq K^*$$

eine endliche Untergruppe der multiplikativen Gruppe des Körpers K.

Beispiel 3.8.10. (1) Es gilt

$$\mu_n(\mathbb{Q}) = \begin{cases} \{1\} & \text{für } n \text{ ungerade,} \\ \{\pm 1\} & \text{für } n \text{ gerade.} \end{cases}$$

(2) Es ist

$$\mu_n(\mathbb{C}) = \left\{ \exp(2\pi i \frac{k}{n}) | 0 \leq k \neq n \right\}.$$

Proposition 3.8.11. *Sei K ein Körper. Dann ist die Gruppe $\mu_n(K)$ zyklisch.*

Beweis. Schritt 1. Sei zunächst $n = p^k$ eine Primpotenz. Da $\mu_n(K)$ eine endliche abelsche Gruppe ist, die von p^k annihiliert wird, muss nach Beispiel 2.5.13 gelten:

$$\mu_n(K) \cong \mathbb{Z}/(p^{e_1}) \times \mathbb{Z}/(p^{e_2}) \times ... \times \mathbb{Z}/(p^{e_k}), \tag{3.8.12}$$

wobei ohne Einschränkung $e_1 \geq e_2 \geq ... \geq e_k$ gelte. Damit gibt es also ein $\zeta \in \mu_n(K)$ der Ordnung $m := p^{e_1}$, und es gilt

$$\{1, \zeta, \zeta^2, ..., \zeta^{m-1}\} \leq \mu_n(K),$$

so dass $|\mu_n(K)| \geq m$. Andererseits gilt wegen (3.8.12) für jedes $\xi \in \mu_n(K)$: $\xi^m = 1$. Umformuliert heißt dies, dass alle Elemente in $\mu_n(K)$ Nullstellen des Polynoms $X^m - 1$ sind. Doch dieses hat höchstens m verschiedene Nullstellen in K, so dass also $|\mu_n(K)| = n$ und damit

$$\mu_n(K) = \langle \zeta \rangle.$$

Schritt 2. Sei nun $n = ab$ mit a, b teilerfremd. Dann gibt es $u, v \in \mathbb{Z}$ mit $ua + vb = 1$ und die Abbildung

$$\mu_n(K) \longrightarrow \mu_a(K) \times \mu_b(K), \xi \mapsto (\xi^b, \xi^a)$$

ist ein Isomorphismus (mit Inversem $(\xi_1, \xi_2) \mapsto \xi_1^v \xi_2^u$).

Schritt 3. Induktiv folgt nun für allgemeines $n = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$:

$$\mu_n(K) \cong \mathbb{Z}/(p_1^{e_1}) \times \mathbb{Z}/(p_2^{e_2}) \times ... \mathbb{Z}/(p_k^{e_k}) \cong \mathbb{Z}/(p_1^{n_1} p_2^{n_2} ... p_k^{n_k}).$$

□

Terminologie 3.8.13. Ein Erzeuger ζ der Gruppe $\mu_n(K)$ heißt *primitive n-te Einheitswurzel in K*, falls ζ Ordnung n hat.

Proposition 3.8.14. *Sei $n \geq 1$ und K ein Körper mit $\mathrm{char}(K) \nmid n$. Sei L/K ein Zerfällungskörper von $X^n - 1 \in K[X]$. Dann gelten:*

(1) Es gibt eine primitive n-te Einheitswurzel $\zeta \in L$ mit $L = K(\zeta)$.

(2) Die Erweiterung L/K ist galoissch und es gibt einen injektiven Homomorphismus

$$\rho : G(L/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

in die Gruppe der Einheiten des Restklassenrings modulo n. Die Abbildung ρ ist eindeutig bestimmt durch die Formel $\sigma(\zeta) = \zeta^{\rho(\sigma)}$.

Beweis. Die Menge der Nullstellen von $X^n - 1$ in L ist genau $\mu_n(L)$. Da $\partial(X^n - 1) = nX^{n-1}$, hat das Polynom $X^n - 1$ keine mehrfachen Nullstellen, also $|\mu_n(L)| = n$. Der Erzeuger von $\mu_n(L)$ ist also eine primitive n-te Einheitswurzel und $L = K(\zeta)$. Die restlichen Aussagen folgen sofort aus der Einsicht (!), dass ζ^k für $k \in \mathbb{Z}/n\mathbb{Z}$ eine *primitive* n-te Einheitswurzel ist, genau dann, wenn k eine Einheit in $\mathbb{Z}/n\mathbb{Z}$ ist. □

Sei $n \geq 1$ und sei $L/\mathbb{Q}$ der Zerfällungskörper des Polynoms $X^n - 1$. Da $G(L/\mathbb{Q})$ die primitiven n-ten Einheitswurzeln permutiert, gilt

$$\Phi_n(X) = \prod_{\substack{\zeta \in \mu_n(L) \\ \zeta \text{ primitiv}}} (X - \zeta) \in \mathbb{Q}[X].$$

Das Polynom $\Phi_n(X)$ heißt das *n-te Kreisteilungspolynom*.

Bemerkung 3.8.15. Da das Polynom $X^n - 1$ primitiv ist, $\Phi_n(X)|(X^n - 1)$, und $\Phi_n(X)$ Leitkoeffizient 1 hat, folgt mit dem Gauß-Lemma, dass $\Phi_n(X)$ sogar Koeffizienten in $\mathbb{Z}$ hat und primitiv ist.

Für eine Primzahl p gilt: Jede p-te Einheitswurzel $\zeta \neq 1$ ist primitiv, so dass also gilt

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1.$$

Wir haben in den Übungen gesehen, dass dieses Polynom irreduzibel ist (Eisenstein-Kriterium). Wir zeigen nun die folgende allgemeinere Aussage:

Satz 3.8.16. *Für jedes $n \geq 1$, ist das Kreisteilungspolynom $\Phi_n(X) \in \mathbb{Q}[X]$ irreduzibel.*

Beweis. Nach dem Gauß-Lemma genügt es zu zeigen, dass $\Phi_n(X)$ irreduzibel in $\mathbb{Z}[X]$ ist. Sei also $\Phi_n(X) = f(X)g(X)$, wobei wir ohne Einschränkung annehmen, dass $f(X)$ irreduzibel und primitiv ist, sowie $g(X)$ primitiv (Gauß-Lemma). Wir zeigen nun die folgende Aussage:

(*) Für jede Primzahl p mit $\mathrm{ggT}(p, n) = 1$ und jede primitive n-te Einheitswurzel $\zeta \in L$ gilt die Implikation $f(\zeta) = 0 \Rightarrow f(\zeta^p) = 0$.

Angenommen, (*) gelte nicht. Dann gibt es also eine primitive n-te Einheitswurzel ζ, so dass $f(\zeta) = 0$, aber $f(\zeta^p) \neq 0$. Da ζ^p selbst eine primitive Einheitswurzel und damit eine Nullstelle von $\Phi_n(X)$ ist, folgt $g(\zeta^p) = 0$. Demnach ist ζ eine Nullstelle von $g(X^p)$. Da $f(X)$ irreduzibel ist mit $f(\zeta) = 0$, gilt $g(X^p) = f(X)h(X)$. Wir betrachten nun den Restklassenhomomorphismus

$$\mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X],\ r(X) \mapsto \overline{r}(X)$$

und rechnen

$$\overline{g}(X)^p = \overline{g}(X^p) = \overline{f}(X)\overline{h}(X).$$

Damit gilt auch

$$\overline{\Phi_n}(X)^p = \overline{f}(X)^p\overline{g}(X)^p = \overline{f}(X)^{p+1}\overline{h}(X). \tag{3.8.17}$$

Sei nun $M/\mathbb{F}_p$ ein Zerfällungskörper des Polynoms $\overline{\Phi_n}(X) \in \mathbb{F}_p[X]$. Wegen der Annahme $\mathrm{ggT}(p, n) = 1$ gilt $\frac{d}{dX}\overline{\Phi_n}(X) \neq 0$, so dass also $\overline{\Phi_n}(X)$ in M nur einfache Nullstellen hat. Da $\overline{f}(X)$ ein Teiler von $\overline{\Phi_n}(X)$ ist, zerfällt auch $\overline{f}(X)$ in $M[X]$ in Linearfaktoren, hat also insbesondere eine Nullstelle. Sei ξ eine solche Nullstelle. Dann impliziert (3.8.17) nach dem Schubladenprinzip jedoch, dass ξ eine mehrfache Nullstelle von $\overline{\Phi_n}(X)$ sein muss. Ein Widerspruch, mit dem also (*) gezeigt ist.

Wir schließen nun den Beweis wie folgt: Die primitiven n-ten Einheitswurzeln in L sind genau die Zahlen ζ^m mit $m \in (\mathbb{Z}/n\mathbb{Z})^*$, also $\mathrm{ggT}(m, n) = 1$. In der Primzerlegung eines Vertreters eines solchen m in $\mathbb{N}$ kommen also nur Primzahlen p vor mit $\mathrm{ggT}(p, n) = 1$. Da $f(X)$ irreduzibel ist, besitzt $f(X)$ in L eine Nullstelle ζ. Durch iterative Anwendung von (*) auf alle Primfaktoren $p_1, p_2, \ldots, p_r$ des Vertreters von m schliessen wir nun, dass auch

$$\zeta^{p_1}, (\zeta^{p_1})^{p_2}, \ldots, \zeta^m$$

Nullstellen von f sein müssen. Also sind alle primitiven n-ten Einheitswurzeln in L Nullstellen von f. Dann muss aber $f = \Phi_n(X)$ gelten, so dass $\Phi_n(X)$ insbesondere irreduzibel ist. □

Korollar 3.8.18. *Die Primzerlegung von $X^n - 1 \in \mathbb{Q}[X]$ in irreduzible Faktoren ist gegeben durch*

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{3.8.19}$$

Beweis. Dies ist nun klar, denn die Nullstellen von $X^n - 1$ in einem Zerfällungskörper sind genau die n-ten Einheitswurzeln. Doch jede n-te Einheitswurzel ξ ist eine primitive d-te Einheitswurzel für $d = \mathrm{ord}(\xi)$ und es gilt $d|n$. □

Beispiel 3.8.20. Mit Formel (3.8.19) aus Korollar 3.8.18 können wir die Kreisteilungspolynome rekursiv durch Polynomdivision berechnen. Die ersten Polynome sind:

$$\begin{aligned}
\Phi_1(X) &= X - 1\\
\Phi_2(X) &= X + 1\\
\Phi_3(X) &= X^2 + X + 1\\
\Phi_4(X) &= X^2 + 1\\
\Phi_5(X) &= X^4 + X^3 + x^2 + 1\\
\Phi_6(X) &= X^2 - X + 1\\
\Phi_7(X) &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1\\
\Phi_8(X) &= X^4 + 1\\
&\vdots
\end{aligned}$$

Wir erhalten also zum Beispiel

$$X^8 - 1 = \Phi_1(X)\Phi_2(X)\Phi_4(X)\Phi_8(X) = (X-1)(X+1)(X^2+1)(X^4+1).$$

Es gibt aber auch effizientere Methoden, die Kreisteilungspolynome zu bestimmen, zum Beispiel durch die sogenannte Möbius-Inversion.

Korollar 3.8.21. *Sei L der Zerfällungskörper von $X^n - 1 \in \mathbb{Q}[X]$. Dann ist L auch der Zerfällungskörper von $\Phi_n(X)$ und es gilt*

$$G(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Beweis. Es ist klar, dass $L = \mathbb{Q}(\zeta)$ mit $\zeta \in \mu_n(K)$ primitiv und $\Phi_n(\zeta) = 0$. Da $\Phi_n(X) \in \mathbb{Q}[X]$ irreduzibel ist, gilt

$$[L : \mathbb{Q}] = |\{\text{primitive } n\text{te Einheitswurzeln in } L\}| = |(\mathbb{Z}/n\mathbb{Z})^*|.$$

Da $L/\mathbb{Q}$ galoissch ist, folgt nun aus Kardinalitätsgründen, dass die Injektion ρ aus Proposition 3.8.14 eine Bijektion sein muss. □

Bemerkung 3.8.22. Sei $n = p_1^{n_1} p_2^{n_2} .. p_k^{n_k}$ eine Primfaktorzerlegung. Der chinesische Restsatz liefert einen Isomorphismus

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_2^{n_2}\mathbb{Z} \times ... \times \mathbb{Z}/p_k^{n_k}\mathbb{Z},$$

und nach Übergang zu Einheiten auch

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{n_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{n_2}\mathbb{Z})^\times \times ... \times (\mathbb{Z}/p_k^{n_k}\mathbb{Z})^\times.$$

Man kann weiterhin für p prim zeigen:

$$(\mathbb{Z}/p^l\mathbb{Z})^\times \cong \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{l-1}\mathbb{Z} & \text{für } p \neq 2,\\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{l-2}\mathbb{Z} & \text{für } p = 2 \text{ und } l \geq 2. \end{cases}$$

Wir führen den Beweis hier nicht.

Beispiel 3.8.23. Sei $L = \mathbb{Q}(\zeta)/\mathbb{Q}$ der Zerfällungskörper von $X^9 - 1 \in \mathbb{Q}[X]$. Dann gilt

$$G(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}.$$

Nach der Galoiskorrespondenz gibt es also einen Körper $M \subseteq L$, so dass $M/\mathbb{Q}$ eine Galoiserweiterung mit Galoisgruppe A_3 ist.

3.9 Radikalerweiterungen

Sei K ein Körper und $n \geq 1$ mit $\mathrm{char}(K) \nmid n$. Wir betrachten zu $0 \neq a \in K$ das Polynom

$$f(X) = X^n - a \in K[X]$$

und seinen Zerfällungskörper L.

Proposition 3.9.1. *Unter den obigen Voraussetzungen gelten:*

(1) Es gilt $L = K(\zeta, \alpha)$ wobei $\alpha \in L$ eine Nullstelle von $f(X)$ und $\zeta \in L$ eine primitive n-te Einheitswurzel ist.

(2) Für den Turm

$$\begin{array}{c} L \\ | \\ K(\zeta) \\ | \\ K \end{array}$$

von Körpererweiterungen gibt es injektive Gruppenhomomorphismen

$$\gamma : G(L/K(\zeta)) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$$

und

$$\rho : G(K(\zeta)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times,$$

welche eindeutig bestimmt sind durch die Formeln

$$\tau(\alpha) = \zeta^{\gamma(\tau)}\alpha$$

und

$$\sigma(\zeta) = \zeta^{\rho(\sigma)}.$$

Beweis. (1) Das Polynom f besitzt in L paarweise verschiedene Nullstellen $\alpha_1, ..., \alpha_n$ (f hat einfache Nullstellen, wegen $\partial(f) = nX^{n-1}$). Wir setzen $\alpha = \alpha_1$, dann sind die Elemente $\alpha^{-1}\alpha_1, ..., \alpha^{-1}\alpha_n$ paarweise verschiedene n-te Einheitswurzeln, und demnach *alle* n-ten Einheitswurzeln in L. Wir können also für eine primitive n-te Einheitswurzel $\zeta \in \mu_n(L)$ schreiben:

$$f(X) = \prod_{i=0}^{n-1}(X - \zeta^i\alpha).$$

Insbesondere gilt $L = K(\zeta, \alpha)$.

(2) Der injektive Homomorphismus ρ wurde schon in Proposition 3.8.14 konstruiert. Die Formel für τ ergibt sich sofort aus der Tatsache, dass $G(L/K(\zeta))$ die Nullstellen des Polynoms $X^n - a$ permutiert. □

Korollar 3.9.2. *Die Galoisgruppe $G(L/K(\zeta))$ ist zyklisch.*

Beweis. Die Galoisgruppe ist eine Untergruppe einer endlichen zyklischen Gruppe, also selbst zyklisch Die Anmerkung ist von Dir: (todo: include proof!) □

Satz 3.9.3. *Sei $n \geq 1$, M ein Körper mit $\mathrm{char}(M) \nmid n$, der eine primitive n-te Einheitswurzel enthalte. Sei L/M eine Galoiserweiterung mit $G(L/M) \cong \mathbb{Z}/n\mathbb{Z}$. Dann gibt es $b \in M$, so dass L der Zerfällungskörper von $X^n - b$ ist.*

Beweis. Sei $\zeta \in \mu_n(M)$ primitiv und sei $G(L/M) \cong \langle\tau\rangle$. Wir setzen

$$\alpha := \sum_{i=0}^{n-1} \zeta^{-i}\tau^i(y)$$

wobei $y \in L$ so gewählt ist, dass $\alpha \neq 0$. Ein solches y existiert nach dem Dedekind-Lemma 3.3.3. Wir rechnen:

$$\begin{aligned}\tau(\alpha) &= \sum_{i=0}^{n-1} \zeta^{-i}\tau^{i+1}(y)\\ &= \zeta \sum_{i=0}^{n-1} \zeta^{-i-1}\tau^{i+1}(y)\\ &= \zeta\alpha\end{aligned}$$

Daher gilt also $\tau(b) = b$, und die paarweise verschiedenen Elemente $\zeta^i\alpha$, $0 \leq i \leq n-1$ sind die Nullstellen von $X^n - b$. Da $G(L/M)$ transitiv auf diesen Nullstellen operiert, ist das Polynom $X^n - b$ irreduzibel in $M[X]$. Daher gilt

$$[M(\alpha) : M] = n = |G(L/M)| = [L : M],$$

also $L = M(\alpha)$, so dass L also der Zerfällungskörper von $X^n - b$ ist. □

Definition 3.9.4. Sei K ein Körper.

(1) Eine Körpererweiterung L/K heißt *einfache Radikalerweiterung*, falls es $\alpha \in L$ und $n \geq 1$ gibt, so dass $\alpha^n \in K$.

(2) Eine Körpererweiterung L/K heißt *Radikalerweiterung*, falls es einen Turm

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = L$$

von Körpererweiterungen gibt, so dass für $1 \leq i \leq m$ die Erweiterung K_i/K_{i-1} eine einfache Radikalerweiterung ist.

Lemma 3.9.5. *Sei K ein Körper der Charakteristik 0 und sei L/K eine Radikalerweiterung. Dann existiert eine Körpererweiterung E/L, so dass E/K eine galoissche Radikalerweiterung ist.*

Beweis. Da L/K Radikalerweiterung ist, gibt es $\alpha_1, ..., \alpha_m \in L$, so dass $L = K(\alpha_1, ..., \alpha_m)$, und mit $K_i = K(\alpha_1, ..., \alpha_i)$ gilt: $\alpha_i^{n_i} \in K_{i-1}$, $1 \leq i \leq n$. Seien $f_1, ..., f_m$ die Minimalpolynome von $\alpha_1, ..., \alpha_m$ über K und sei E/L der Zerfällungskörper von $f = f_1 f_2 \cdots f_m$ über L. Dann ist E auch der Zerfällungskörper von f über K, denn $\alpha_1, ..., \alpha_m$ sind Nullstellen von f. Also ist E/K galoissch. Sei $G = G(E/K)$ die Galoisgruppe. Dann gilt

$$E = K(\{\sigma(\alpha_1)\}_{\sigma\in G}, \{\sigma(\alpha_2)\}_{\sigma\in G}, ..., \{\sigma(\alpha_m)\}_{\sigma\in G})$$

denn der Zerfällungskörper E_i eines jeden irreduziblen Faktors f_i ist galoissch über K, so dass G per Einschränkung auf E_i operiert und die Nullstellen von f_i transitiv permutiert. Aus

$$\alpha_i^{n_i} \in K_{i-1}$$

folgt für jedes $\sigma \in G$:

$$\sigma(\alpha_i)^{n_i} \in K(\{\sigma(\alpha_1)\}_{\sigma\in G}, \{\sigma(\alpha_2)\}_{\sigma\in G}, ..., \{\sigma(\alpha_{i-1})\}_{\sigma\in G})$$

so dass also E/K eine Radikalerweiterung ist (wobei es für fixiertes $1 \leq i \leq n$ irrelevant ist, in welcher Reihenfolge die Elemente $\{\sigma(\alpha_i)\}_{\sigma\in G}$ hinzu adjungiert werden). □

3.10 Auflösbarkeit

Definition 3.10.1. Eine endliche Gruppe G heißt auflösbar, falls es eine Kette

$$\{1\} = U_0 \leq U_1 \leq U_2 \leq \cdots \leq U_n = G \tag{3.10.2}$$

von Untergruppen $U_i \leq G$ gibt, so dass für $1 \leq i \leq n$ gelten:

(1) $U_{i-1} \trianglelefteq U_i$ ist eine normale Untergruppe,

(2) U_i/U_{i-1} ist zyklisch.

Beispiele 3.10.3. (1) Jede endliche abelsche Gruppe ist auflösbar. Dies ist eine direkte Konsequenz aus unserem Klassifikationssatz für endlich erzeugte abelsche Gruppen (Satz 2.5.13). Insbesondere ist also, für jedes $n \geq 1$, Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ von Einheiten des Restklassenrings modulo n auflösbar.

(2) Die Gruppe S_3 ist auflösbar mit
$$\{1\} \leq A_3 \leq S_3.$$

(3) Die Gruppe S_4 ist auflösbar mit
$$\{1\} \leq C_2 \leq V_4 \leq A_4 \leq S_4.$$

Für eine Gruppe G definieren wir die *Kommutatoruntergruppe*

$$[G, G] := \{aba^{-1}b^{-1} | a, b \in G\} \leq G.$$

Lemma 3.10.4. *Sei G eine endliche auflösbare Gruppe. Dann ist $[G, G] \lneq G$ eine echte Untergruppe.*

Beweis. Es existiert eine Kette der Form (3.10.2), wobei alle Inklusionen o.E. echte Inklusionen sind. Wir betrachten die Quotientenabbildung

$$\pi : G \to G/U_{n-1}.$$

Da G/U_{n-1} als zyklische Gruppe insbesondere abelsch ist, gilt $\pi([G, G]) = \{1\}$. Doch daraus folgt $[G, G] \subseteq \text{Kern}(\pi) = U_{n-1} \lneq G$. □

Satz 3.10.5. *Die alternierende Gruppe A_n ist für $n \geq 5$ nicht auflösbar.*

Beweis. Wir zeigen, dass gilt: $[A_n, A_n] = A_n$. Da sich jedes Element von A_n als ein Produkt einer geraden Anzahl von Transpositionen schreiben lässt, genügt es, für $a \neq b$ und $c \neq d$ zu zeigen:

$$(ab)(cd) \in [A_n, A_n].$$

Wir unterscheiden die Fälle

1. $b = c$: Dann gilt $(ab)(bd) = (abd)$.
2. a, b, c, d paarweise verschieden: Dann gilt $(ab)(bd) = (abc)(bcd)$.

Um alle Fälle abzudecken, genügt es also, für paarweise verschiedene a, b, c zu zeigen: $(abc) \in [A_n, A_n]$. Es gilt für $1 \leq d < e \leq n$ so dass a, b, c, d, e paarweise verschieden sind:

$$(abc) = [(ac)(de), (cb)(de)].$$

□

Lemma 3.10.6. *Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe.*

(1) Falls G auflösbar ist, dann ist auch H auflösbar.

(2) Falls zusätzlich $H \trianglelefteq G$ eine normale Untergruppe ist, dann sind äquivalent

(i) G ist auflösbar.

(ii) H und G/H sind auflösbar.

Beweis. Sei G auflösbar mit Kette

$$\{1\} = U_0 \leq U_1 \leq U_2 \leq \cdots \leq U_n = G$$

und sei H eine Untergruppe von G. Dann setzen wir für $0 \leq i \leq n$:

$$V_i := H \cap U_i.$$

Dann folgt $V_{i-1} \trianglelefteq V_i$ und nach dem Homomorphiesatz

$$V_i/V_{i-1} \hookrightarrow U_i/U_{i-1},$$

so dass sich V_i/V_{i-1} mit einer Untergruppe der zyklischen Gruppe U_i/U_{i-1} identifiziert, also selbst zyklisch ist. Somit ist H auflösbar. Sei nun $H \trianglelefteq G$ zusätzliche normal. Dann setzen wir

$$W_i = \pi(U_i)$$

wobei $\pi : G \to G/H$ die Quotientenabbildung ist. Dann gilt $W_{i-1} \trianglelefteq W_i$ und der Homomorphiesatz liefert einen surjektiven Homomorphismus

$$U_i/U_{i-1} \to W_i/W_{i-1}.$$

Damit ist W_i/W_{i-1} als Quotient einer zyklischen Gruppe zyklisch.

Sei nun umgekehrt $H \trianglelefteq G$ normale Untergruppe und H sowie G/H auflösbar mit Ketten

$$\{1\} = V_0 \leq V_1 \leq V_2 \leq \cdots \leq V_r = H$$

und

$$\{1\} = W_0 \leq W_1 \leq W_2 \leq \cdots \leq W_s = G/H.$$

Dann setzen wir

$$U_i := \begin{cases} V_i & \text{für } 0 \leq i \leq r, \\ \pi^{-1}(W_{i-r}) & \text{für } r < i \leq r+s. \end{cases}$$

Dies definiert eine Kette mit den gewünschten Eigenschaften (!), so dass G auflösbar ist. □

Definition 3.10.7. Sei $f \in K[X]$ ein Polynom. Wir sagen, f ist *durch Radikale auflösbar*, wenn es eine Radikalerweiterung L/K gibt, so dass $f \in L[X]$ in Linearfaktoren zerfällt (L enthält also einen Zerfällungskörper von f).

Satz 3.10.8. *Sei K ein Körper der Charakteristik 0 und sei $f \in K[X]$ ein Polynom mit Zerfällungskörper L/K. Dann sind äquivalent:*

(i) f ist durch Radikale auflösbar.

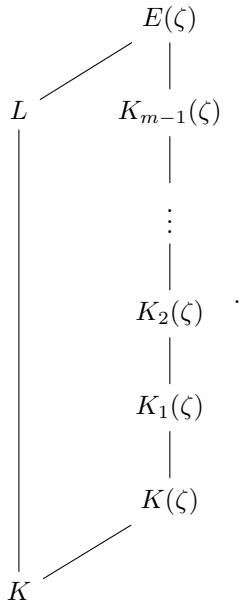
(ii) Die Galoisgruppe $G(L/K)$ ist auflösbar.

Beweis. Sei f durch Radikale auflösbar. Dann gibt es also eine Radikalerweiterung E/K, nach Lemma 3.9.5 ohne Einschränkung galoissch, so dass E einen Zerfällungskörper L von f über K enthält. Es gilt also

$$K = K_0 \subseteq K_1 \subseteq ... \subseteq K_m = E$$

und $K_i = K_{i-1}(\alpha_i)$ mit $\alpha_i^{n_i} \in K_{i-1}$. Sei n das kleinste gemeinsame Vielfache der Zahlen $n_1, ..., n_m$ und sei E'/E der Zerfällungskörper des Polynoms $X^n - 1$. Dann ist auch E'/K galoissch: Sei E Zerfällungskörper

von $g \in K[X]$, dann ist E' Zerfällungskörper von $g(X^n - 1)$. Per Konstruktion enthält E' nun eine primitive n-te Einheitswurzel ζ und es gilt $E' = E(\zeta)$. Wir betrachten nun das Diagramm von Körpereinbettungen

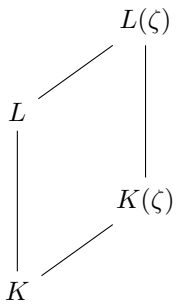


Für jedes $1 \leq i \leq n$ teilt n_i die Zahl n, mit $n = n_i k_i$ ist also ζ^{k_i} eine primitive n_i-te Einheitswurzel. Nach Satz 3.9.1 und Korollar 3.9.2 sind die einfachen Radikalerweiterungen also galoissch mit zyklischer Galoisgruppe. Desweiteren ist die Kreisteilungserweiterung $K(\zeta)/K$ galoissch mit zyklischer Galoisgruppe. Per Galoiskorrespondenz ist die Galoisgruppe $G(E(\zeta)/K)$ also auflösbar mit Kette:

$$\{1\} \trianglelefteq G(E(\zeta)/K_{m-1}(\zeta)) \trianglelefteq G(E(\zeta)/K_{m-2}(\zeta)) \trianglelefteq ... \trianglelefteq G(E(\zeta)/K(\zeta)) \trianglelefteq G(E(\zeta)/K)$$

Doch damit ist, nach Lemma 3.10.6, auch die Galoisgruppe $G(L/K) \cong G(E(\zeta)/K)/G(E(\zeta)/L)$ auflösbar.

Sei nun umgekehrt die Galoisgruppe $G(L/K)$ auflösbar und sei $n = [L : K]$. Sei F der Zerfällungskörper von $X^n - 1$ über L (der auch galoissch über K ist, siehe Argument oben). Es gilt $F = L(\zeta)$ und wir betrachten das Diagram von Körpererweiterungen



Die Galoisgruppen $G(L(\zeta)/L)$ und $G(L/K)$ sind auflösbar, so dass nach Lemma 3.10.6 auch $G(L(\zeta)/K)$ auflösbar ist. Durch nochmalige Anwendung von Lemma 3.10.6 ist die Untergruppe $G(L(\zeta)/K(\zeta)) \leq G(L(\zeta)/K)$ auflösbar.

Per Galoiskorrespondenz erhalten wir einen Turm

$$K(\zeta) \subseteq K_1 \subseteq K_2 \subseteq ... \subseteq K_m = L(\zeta)$$

wobei K_i/K_{i-1} für $1 \leq i \leq n$ eine Galoiserweiterung mit zyklischer Galoisgruppe ist. Wir setzen $n_i = |G(K_i/K_{i-1})|$.

Desweiteren definiert die Einschränkungsabbildung $G(L(\zeta)/K(\zeta)) \to G(L/K), \sigma \mapsto \sigma|L$ einen injektiven (!) Gruppenhomomorphismus. Es gilt also

$$|G(L(\zeta)/K(\zeta))| \mid |G(L/K)| = [L : K] = n.$$

Daher gilt für alle $1 \leq i \leq n$: $n_i | n$, so dass mit $n = n_i k_i$ also ζ^{k_i} eine primitive n_i-te Einheitswurzel ist.

Nach Satz 3.9.3 sind damit alle Erweiterungen K_i/K_{i-1} einfache Radikalerweiterungen. Auch die Kreisteilungserweiterung $K(\zeta)$ ist eine einfache Radikalerweiterung, so dass also $E(\zeta)/K$ eine Radikalerweiterung und somit f durch Radikale auflösbar ist. □

Korollar 3.10.9. *Für $n \geq 5$ ist das allgemeine Polynom n-ten Grades aus Bemerkung 3.8.9 nicht durch Radikale auflösbar.*

Beweis. Das allgemeine Polynom n-ten Grades hat die Galoisgruppe S_n welche, für $n \geq 5$, nach Lemma 3.10.6 nicht auflösbar ist, denn S_n enthält die nicht auflösbare Gruppe A_n (Satz 3.10.5). □

Kapitel 4

Addendum

4.1 Das Auswahlaxiom und seine Folgen

Neben den klassischen Axiomen der Zermelo-Fraenkel-Mengenlehre nehmen wir auch an, dass das Auswahlaxiom wahr ist. Dieses besagt, dass für ein gegebenes Mengensystem $\mathcal{A}$ von nicht-leeren Mengen $A \subseteq \mathcal{A}$ eine Funktion $f : \mathcal{A} \to \cup_{A \subseteq \mathcal{A}} A$ existiert, die jedem $A \subseteq \mathcal{A}$ ein Element von A zuordnet, also vereinfacht gesagt ein Element aus jeder Menge des Systems auswählt. Wir werden vor allem zwei dazu äquivalente Sätze benötigen. Dazu brauchen wir Möglichkeiten, Mengen zu ordnen:

Definition 4.1.1. Eine *total geordnete Menge* ist ein Paar $(M, \preceq)$, bestehend aus einer Menge M und einer Relation $\preceq$, die für alle $x, y, z \in M$ den folgenden Bedingungen genügt:

(1) Reflexivität: $x \preceq x$

(2) Antisymmetrie: $x \preceq y \wedge y \preceq x \implies x = y$

(3) Transitivität: $x \preceq y \wedge y \preceq z \implies x \preceq z$

(4) Totalität: $x \preceq y \vee y \preceq x$.

Gilt nur (1) - (3), so heißt die Menge stattdessen *partiell geordnet*. Eine total geordnete Teilmenge einer partiell geordneten Menge heißt *Kette*.

Definition 4.1.2. Sei $(M, \preceq)$ eine total geordnete Menge. Diese heißt darüber hinaus *wohlgeordnet*, wenn jede nicht-leere Teilmenge von M ein kleinstes Element bezüglich $\preceq$ besitzt.

Beispiele 4.1.3. Einige Beispiele für geordnete Mengen sind:

(1) Die Menge $\mathbb{N}$ wird durch $\leq$ total geordnet, ebenso wie $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$. Die natürlichen Zahlen werden durch $\leq$ sogar wohlgeordnet. Für $\mathbb{Z}$ lässt sich eine Wohlordnung ausgehend von $\leq$ leicht konstruieren.

(2) Die Ordnung $\subseteq$ auf der Potenzmenge $\mathcal{P}(M)$ einer Menge M ist eine partielle Ordnung, aber keine totale Ordnung (!).

(3) Auf $\mathbb{Z}^*$ lässt sich eine Ordnung durch Teilbarkeit $|$ definieren. Da beispielsweise $2 \nmid 3$ und $3 \nmid 2$ gilt, ist dies aber keine Totalordnung.

Mit dem Auswahlaxiom existiert eine solche Wohlordnung immer:

Proposition 4.1.4 (Wohlordnungssatz)**.** *Jede Menge kann wohlgeordnet werden. Insbesondere enthält jede nicht-leere Teilmenge der natürlichen Zahlen eine kleinste Zahl.*

Allgemein ist der Wohlordnungssatz hochgradig nicht-konstruktiv: Es lässt sich zeigen, dass das Auswahlaxiom die Existenz einer Wohlordnung von $\mathbb{R}$ impliziert, aber es unmöglich ist, eine konstruktive Formel für diese anzugeben.
Der nächste Satz garantiert die Existenz maximaler Elemente:

Proposition 4.1.5 (Lemma von Zorn)**.** *Sei $(M, \preceq)$ eine partiell geordnete Menge. Gilt für jede Kette $T \subseteq M$, dass eine obere Schranke $s \in T$ mit $t \preceq s$ für alle $t \in T$ existiert, so besitzt M ein maximales Element $\mathfrak{m} \in M$. Für alle $x \in M$ mit $\mathfrak{m} \preceq x$ gilt also $\mathfrak{m} = x$.*

Wichtige Folgen des Satzes von Zorn sind zum Beispiel die Existenz von Basen für beliebige Vektorräume, der Satz von Tychonoff aus der Topologie oder auch der Satz von Steinitz, der die Existenz algebraischer Abschlüsse garantiert.

Index