Vorlesungsskript Algebra I (LAG)

Wintersemester 2024
CAU Kiel

Daniel Bissinger

Version: 26. Februar 2025

Inhaltsverzeichnis

1 Grundlagen der Gruppentheorie **1**
- 1.1 Elementare Rechenoperationen . . . 1
- 1.2 Gruppen, Untergruppen und der Satz von Lagrange . . . 4
- 1.3 Zyklische Gruppen . . . 8
- 1.4 Homomorphismen und Normalteiler . . . 11
- 1.5 Faktorgruppen und Isomorphiesätze . . . 14
- 1.6 Produkte von Gruppen . . . 17
- 1.7 Operationen von Gruppen und die Klassengleichung . . . 20

2 Strukturtheorie endlicher Gruppen **28**
- 2.1 p-Gruppen . . . 28
- 2.2 Die Sätze von Sylow . . . 29
- 2.3 Endliche abelsche Gruppen . . . 31

3 Grundlagen der Ringtheorie **36**
- 3.1 Grundlegende Definitionen . . . 36
- 3.2 Kommutative Ringe . . . 39
- 3.3 Der Quotientenkörper . . . 47
- 3.4 Teilbarkeit in Integritätsbereichen . . . 49

4 Polynomringe **55**
- 4.1 Grundlegende Definitionen . . . 55
- 4.2 Nullstellen . . . 56
- 4.3 Irreduzible Polynome . . . 59

5 Elementare Theorie der Körpererweiterungen **64**
- 5.1 Körpererweiterungen . . . 64
- 5.2 Endliche Körpererweiterungen . . . 65
- 5.3 Algebraische Körpererweiterungen . . . 68
- 5.4 Zerfällungskörper . . . 71
- 5.5 Normale Erweiterungen . . . 72
- 5.6 Lineare Unabhängigkeit von Körperhomomorphismen . . . 73

6 Galoistheorie **75**
- 6.1 Galoiserweiterungen . . . 75
- 6.2 Charakterisierung von Galoiserweiterungen in Charakteristik 0 . . . 79

7 Anwendungen **81**
- 7.1 Der Fundamentalsatz der Algebra . . . 81
- 7.2 Endliche Körper . . . 81
- 7.3 Einheitswurzeln . . . 83
- 7.4 Konstruktion mit Zirkel und Lineal . . . 86

Einleitung

In der linearen Algebra haben wir uns unter anderem mit den Grundlagen der Gruppen- und Ringtheorie beschäftigt. In dieser Vorlesung werden diese Kenntnisse vertieft und um die Theorie der Körpererweiterungen erweitert. Außerdem werden Verbindungen zwischen diesen auf den ersten Blick unabhängigen Themenbereichen hergestellt.

Mithilfe der vermittelten Theorien lassen sich klassische Probleme der Geometrie präzise formulieren und lösen. Eines dieser Probleme, das einen direkten Bezug zur Schulmathematik hat, ist die Unterteilung von Winkeln: Es seien drei verschiedene Punkte $A, B, C \in \mathbb{R}^2$ gegeben. In der Schule lernen wir, wie man nur mit Zirkel und Lineal den Winkel, der von $\overline{AB}$ und $\overline{AC}$ eingeschlossen wird, halbieren kann. Abbildung 1 zeigt die Konstruktion.

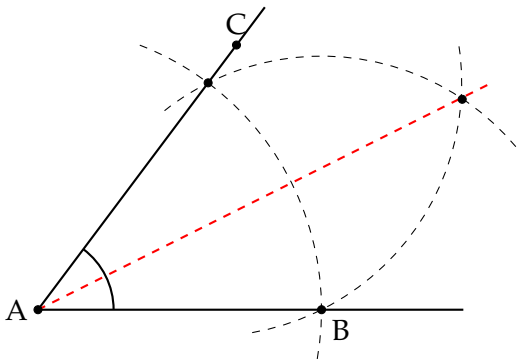


Abbildung 1: Konstruktion der Winkelhalbierenden ausgehend von in der Ebene $\mathbb{R}^2$ gegebenen Punkten A, B und C.

Es stellt sich die Frage, ob es auch eine Methode gibt, jeden gegebenen Winkel zu dritteln. Diese Problemstellung reicht bis in die Antike zurück. Erst 1837 konnte Pierre Wantzel beweisen, dass bestimmte Winkel nicht mit Zirkel und Lineal gedrittelt werden können. Am Ende der Vorlesung werden wir verstehen, warum der Winkel 60° nicht gedrittelt werden kann, der Winkel 180° hingegen schon. Außerdem werden wir sehen, wie man beweisen kann, dass eine Konstruktionsaufgabe nicht lösbar ist.

Anmerkungen zu Vorlesungsinhalten und dem Skript.

- Kommentare sind herzlich willkommen.
- Die Vorlesung ist im größten Teil inhaltlich in sich geschlossen und orientiert sich an [1], [3], und [4]. An geeigneten Stellen verweisen wir auf die Vorlesung „Lineare Algebra I,II“ von Richard Weidmann, die 2023/24 gehalten wurde und online als Skript zur Verfügung steht.
- Beweise die farblich gekennzeichnet sind, wurden in der Vorlesung nicht geführt. Dies hat zweierlei Gründe. Entweder ist der Beweis sehr umfangreich und wurde deshalb aus Zeitgründen weggelassen oder der Beweis ist kurz und eignet sich deshalb gut für das Selbststudium.

1 Grundlagen der Gruppentheorie

1.1 Elementare Rechenoperationen

Im Folgenden bezeichnen wir mit $\mathbb{N} := \{1, 2, 3, \ldots\}$ die natürlichen Zahlen und definieren $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Sind $x, y \in \mathbb{Z}$, so schreiben wir $x \mid y$, falls ein $z \in \mathbb{Z}$ mit $x \cdot z = y$ existiert. In diesem Fall heißt x **Teiler** von y.

Definition. Es seien $a, b \in \mathbb{Z}$ mit $a \neq 0$ oder $b \neq 0$. Wir definieren

$$\mathrm{ggT}(a, b) := \max\{c \in \mathbb{N} \mid \text{Es gilt } c \mid a \text{ und } c \mid b\}$$

und nennen $\mathrm{ggT}(a, b)$ **größten gemeinsamen Teiler** von a und b. Wir sagen, dass a und b **teilerfremd** sind, falls $\mathrm{ggT}(a, b) = 1$ gilt. Weiter definieren wir $\mathrm{ggT}(0, 0) := 0$.

Lemma 1.1.1 (Division mit Rest). *Es seien $a, b \in \mathbb{Z}$ mit $a \neq 0$. Dann existieren eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit folgenden Eigenschaften:*

(1) $b = q \cdot a + r$, *und*

(2) $0 \leq r < |a|$.

Beweis. Wir gehen schrittweise vor.

(i) Existenz von (q, r):

Gilt $b \geq 0$, so gilt $|a| \cdot 0 \leq b$ und wir finden $q \in \mathbb{N}_0$ mit $|a| \cdot q \leq b < |a| \cdot (q + 1)$. Es gilt $b = q \cdot |a| + r$ mit $r := b - q \cdot |a| \geq 0$ und $r = b - q \cdot |a| < |a| \cdot (q + 1) - q \cdot |a| = |a|$.

Gilt $b < 0$, so finden wir $q' \in \mathbb{Z}$ und $0 \leq r' < |a|$ mit $-b = q' \cdot a + r'$. Es folgt $b = (-q') \cdot a + (-r')$ und $-|a| < -r' \leq 0$. Für $-r' = 0$ setzen wir $q := -q'$ und $r := 0$. Für $-r' < 0$ erfüllt $r := -r' + |a|$ die Ungleichung $0 < -r' + |a| < |a|$. Es sei $\ell \in \{-1, 1\}$ das Vorzeichen von a und $q := -q' - \ell$. Dann gilt

$$qa + r = (-q' - \ell)a - r' + |a| = b - \ell a + |a| = b.$$

(ii) Eindeutigkeit: Es seien (q, r) und (q', r') mit den Eigenschaften (1) und (2) und o.b.d.A. sei $r \geq r'$. Wir erhalten $0 \leq r - r' < |a|$ und $r - r' = a(q' - q)$ liefert uns $0 \leq a(q' - q) < |a|$. Das heißt $0 \leq |a| \cdot |q' - q| < |a|$, also $0 \leq |q - q'| < 1$ da $|a| \neq 0$ und damit $q' = q$. Es folgt $r = r'$.

□

Lemma 1.1.2. *Es seien $a, b \in \mathbb{Z}$ nicht beide 0.*

(1) Es existieren $s, t \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = s \cdot a + t \cdot b$.[a]

(2) Für $g \in \mathbb{N}$ sind äquivalent:

(a) $g = \mathrm{ggT}(a,b)$.

(b) Es gelten

(i) $g \mid a$ und $g \mid b$, und

(ii) für alle $g' \in \mathbb{N}$ mit $g' \mid a$ und $g' \mid b$ folgt bereits $g' \mid g$.

(3) Gilt $a \neq 0$ und ist $b = q \cdot a + r$ mit $0 \leq r < |a|$, so gilt $\mathrm{ggT}(a,b) = \mathrm{ggT}(a,r)$.

[a] Diese Aussage ist als Lemma von Bézout bekannt.

Beweis.

(1) Es gilt $g' := a \cdot a + b \cdot b \in \mathbb{N}$. Also finden wir eine Darstellung $g := s \cdot a + t \cdot b \in \mathbb{N}$ mit $s, t \in \mathbb{Z}$ und $g \in \mathbb{N}$ minimal. Es gilt $\mathrm{ggT}(a,b) \mid a$ und $\mathrm{ggT}(a,b) \mid b$ und damit auch $\mathrm{ggT}(a,b) \mid s \cdot a + t \cdot b = g$. Mit $\mathrm{ggT}(a,b), g \in \mathbb{N}$ folgt $\mathrm{ggT}(a,b) \leq g$. Wir schreiben $a = q \cdot g + r$ mit $0 \leq r < |g| = g$ und erhalten

$$r = a - q \cdot g = a - q \cdot (s \cdot a + t \cdot b) = (1 - q \cdot s) \cdot a + (-q \cdot t) \cdot b.$$

Mit $r \in \{0, \ldots, g-1\}$ und Minimalität von g folgt $r = 0$, das heißt $g \mid a$. Analog folgt $g \mid b$. Wir erhalten $g \in \{c \in \mathbb{N} \mid \text{Es gilt } c \mid a \text{ und } c \mid b\}$ und damit $g \leq \mathrm{ggT}(a,b)$. Insgesamt gilt $g = \mathrm{ggT}(a,b)$.

(2) (a) $\Rightarrow$ (b). Klar ist $\mathrm{ggT}(a,b) \mid a$ und $\mathrm{ggT}(a,b) \mid b$. Es sei g' ein gemeinsamer Teiler von a und b. Eine Darstellung $\mathrm{ggT}(a,b) = s \cdot a + t \cdot b$ aus (1) liefert uns $g' \mid \mathrm{ggT}(a,b)$.

(b) $\Rightarrow$ (a). Es erfülle g die Eigenschaften (i),(ii). Nach (i) gilt $g \in \{c \in \mathbb{N} \mid \text{Es gilt } c \mid a \text{ und } c \mid b\}$ und damit $g \leq \mathrm{ggT}(a,b)$. Mit (ii) folgt aber auch $\mathrm{ggT}(a,b) \mid g$, also $\mathrm{ggT}(a,b) \leq g$, da $g \in \mathbb{N}$. Also $g = \mathrm{ggT}(a,b)$.

(3) Ein gemeinsamer von Teiler a, b ist auch ein Teiler von a und $r = b - q \cdot a$. Mit (2) folgt $\mathrm{ggT}(a,b) \mid \mathrm{ggT}(a,r)$. Analog ist ein gemeinsamer Teiler von r und a ein Teiler von a und $b = q \cdot a + r$. Also $\mathrm{ggT}(a,r) \mid \mathrm{ggT}(a,b)$.

□

Beispiel. Es seien $a, b \in \mathbb{Z}$ nicht beide 0. Wir wollen $\mathrm{ggT}(a,b)$ und eine Darstellung der Form $\mathrm{ggT}(a,b) = s \cdot a + t \cdot b$ bestimmen. Der Fall $a \cdot b = 0$ ist trivial. Als Beispiel berechnen wir $\mathrm{ggT}(-462, 1071)$. Es gilt $\mathrm{ggT}(-462, 1071) = \mathrm{ggT}(462, 1071)$. Wiederholte Division mit Rest liefert

$$\begin{aligned} 1071 &= 2 \cdot 462 + 147 \\ 462 &= 3 \cdot 147 + 21 \\ 147 &= 7 \cdot 21 + 0 \end{aligned}$$

Damit gilt

$$\mathrm{ggT}(-462, 1071) = \mathrm{ggT}(462, 1071) = \mathrm{ggT}(462, 147) = \mathrm{ggT}(21, 147) = \mathrm{ggT}(21, 0) = 21.$$

Um eine Darstellung wie im Lemma von Bézout zu erhalten, setzen wir rückwärts ein:

$$21 = 462 - 3 \cdot 147 = 462 - 3 \cdot (1071 - 2 \cdot 462) = 7 \cdot 462 + (-3) \cdot 1071.$$

Da wir ursprünglich an einer Darstellung durch -462 und 1071 interessiert waren, erhalten wir

$$\mathrm{ggT}(-462, 1071) = 21 = (-7) \cdot (-462) + (-3) \cdot 1071.$$

Definition. Eine Zahl $1 \neq n \in \mathbb{N}$ heißt **Primzahl**, falls für $m \in \mathbb{N}$ mit $m \mid n$ schon $m \in \{1, n\}$ gilt. Die Menge der Primzahlen bezeichnen wir mit $\mathbb{P}$.

Der folgende Satz ist uns wohlbekannt und wir werden uns im Laufe des Semester mit speziellen Ringen beschäftigen, die eine ähnliche Eigenschaft besitzen. Der Vollständigkeit halber gegeben wir schon hier einen Beweis.

Satz 1.1.3 (Fundamentalsatz der Arithmetik)**.** *Es sei $1 \neq n \in \mathbb{N}$. Dann existiert eine bis auf Reihenfolge eindeutig bestimmte Zerlegung $n = p_1 p_2 \cdots p_\ell$ von n in Primzahlen $p_1, \ldots, p_\ell$.*

Beweis. Wir gehen schrittweise vor.

(1) Existenz der Zerlegung: Besitzt $n \in \mathbb{N}$ keine Zerlegung dieser Art, so finden wir eine kleinste Zahl $1 \neq n_0 \in \mathbb{N}$ mit dieser Eigenschaft. Insbesondere ist n_0 keine Primzahl und wir finden natürliche Zahlen $1 < a, b < n$ mit $n_0 = ab$. Minimalität liefert eine Zerlegung für a und b und damit auch für das Produkt, ein Widerspruch.

(2) Eindeutigkeit der Zerlegung: Es seien $s, t \in \mathbb{N}$ und $p_1 p_2 \cdots p_s = n = q_1 q_2 \cdots q_t$ zwei Zerlegungen in Primzahlen. Wir zeigen über Induktion nach s, dass sich die Zerlegungen nur um Reihenfolge unterscheiden. Gilt $s = 1$, so ist n eine Primzahl und die Behauptung ist klar. Es sei also $s > 1$. Es gilt $p_1 \mid n = q_1 q_2 \cdots q_t$. In den Übungen wird gezeigt, dass damit ein $i \in \{1, \ldots, t\}$ mit $p_1 \mid q_i$ existiert. O.B.d.A. sei $i = 1$. Mit $p_1 \neq 1$ und q_1 Primzahl, folgt $p_1 = q_1$. Damit ist $p_2 \cdots p_s = q_2 \cdots q_t$ und die Induktionsvoraussetzung zeigt, dass $s = t$ gilt und $q_2 \cdots q_s$ durch Änderung der Reihenfolge aus $p_2 \cdots p_s$ hervorgeht.

□

Definition (Primfaktorzerlegung)**.** Es sei $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Für $p \in \mathbb{P}$ bezeichnen wir $m_p(n) \in \mathbb{N}_0$ die eindeutig bestimmte natürliche Zahl, sodass

$$n = (-1)^\varepsilon \prod_{p \in \mathbb{P}} p^{m_p(n)}$$

gilt, wobei $\varepsilon = 1$ für $n < 1$ und $\varepsilon = 0$ für $n > 1$. [1]

Beispiel. Es gilt $n = 588 = 2^2 \cdot 3 \cdot 7^2$, das heißt $m_2(588) = 2, m_3(588) = 1, m_5(588) = 0, m_7(588) = 2$ und $m_p(588) = 0$ für alle $p \in \mathbb{P}_{>7}$.

[1] Es handelt sich um ein endliches Produkt, da $m_p(n) = 0$ für alle Primzahlen $p > n$ gilt.

1.2 Gruppen, Untergruppen und der Satz von Lagrange

Definition. Sei $G \neq \varnothing$ eine Menge sowie

$$\mu\colon G \times G \longrightarrow G; (x, y) \mapsto \mu(x, y) = x \cdot y = xy$$

eine Abbildung[2]. Das Paar (G, μ) heißt **Gruppe**, falls gilt

(1) $x(yz) = (xy)z$ für alle $x, y, z \in G$ (**Assoziativgesetz**),

(2) es existiert $e \in G$ mit

(i) $ex = x$ für alle $x \in G$,

(ii) zu jedem $x \in G$ gibt es ein $y \in G$ mit $yx = e$.

Gilt lediglich (1), so heißt G **Halbgruppe**.

Lemma 1.2.1. *Sei G eine Gruppe.*

(1) Es existiert genau ein Element $e \in G$ mit $ex = x$ für alle $x \in G$ und dieses Element erfüllt $xe = x$ für alle $x \in G$.

(2) Für jedes $x \in G$ existiert genau ein $y \in G$ mit $yx = e$ und dieses Element erfüllt $xy = e$.

Beweis. Es sei e mit Eigenschaft (2) aus der Definition der Gruppe und $x \in G$. Es sei $y \in G$ mit $yx = e$ und $z \in G$ mit $zy = e$, dann gilt

$$xy = e(xy) = (zy)(xy) = z(yx)y = z(ey) = zy = e.$$

Weiter folgt daraus

$$(*) \quad xe = x(yx) = (xy)x = ex = x.$$

Ist e' ein weiteres Element mit der Eigenschaft (2), so folgt

$$e' \overset{(*)}{=} e'e = e.$$

Damit ist e eindeutig bestimmt. Ist $y' \in G$ ein weiteres Element mit $y'x = e$, so folgt

$$y' \overset{(*)}{=} y'e = y'(xy) = (y'x)y = ey = y.$$

□

Definition. Es sei G eine Gruppe.

(1) Das eindeutig bestimmte Element $e \in G$ heißt **neutrales Element** von G und für $x \in G$ heißt das eindeutig bestimmte Elemente x^{-1} mit $x^{-1}x = e = xx^{-1}$ das zu x **inverse Element**.

[2] Wie in der Linearen Algebra unterdrücken wir μ und schreiben $x \cdot y$ oder xy anstatt $\mu(x, y)$.

(2) Die Gruppe G heißt **abelsch**, falls $xy = yx$ für alle $x, y \in G$ gilt[3].

Beispiele. (1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$ sind (abelsche) Gruppen.

(2) $(\mathbb{N}_0, +), (\mathbb{Z} \setminus \{0\}, \cdot)$ sind keine Gruppen.

(3) Ist $X \neq \varnothing$ Menge, so bildet die Menge

$$\mathcal{S}_X := \{\sigma \colon X \longrightarrow X \mid \sigma \text{ ist bijektive Abbildung}\}$$

eine Gruppe mit der Komposition von Abbildungen als Verknüpfung. Die Gruppe heißt **symmetrische Gruppe auf** X und ein Element in $\mathcal{S}_X$ heißt **Permutation**. Für $X = \{1, \ldots, n\}$ mit $n \in \mathbb{N}$ schreiben wir $\mathcal{S}_n := \mathcal{S}_X$ und erinnern uns, dass $\mathcal{S}_n$ genau $n!$ Elemente enthält. Für $n \geq 3$ ist $\mathcal{S}_n$ nicht abelsch: Es sei σ die Permutation die nur 1 und 2 vertauscht und τ die Permutation die nur 2 und 3 vertauscht. Es gilt

$$(\sigma \circ \tau)(1) = \sigma(1) = 2 \neq 3 = \tau(2) = (\tau \circ \sigma)(1),$$

das heißt $\sigma \circ \tau \neq \tau \circ \sigma$.

Definition. Eine Teilmenge $H \subseteq G$ einer Gruppe G heißt **Untergruppe** von G, wenn $\mu(h_1, h_2) \in H$ für alle $h_1, h_2 \in H$ gilt und $(H, \mu|_{H \times H})$ eine Gruppe ist.[4]

Lemma 1.2.2 (Untergruppenkriterium)**.** *Sei G eine Gruppe, $H \subseteq G$ eine Teilmenge. Dann ist H eine Untergruppe von G genau dann, wenn*

(a) $H \neq \varnothing$,

(b) $xy \in H$ *für alle* $x, y \in H$, *und*

(c) $x^{-1} \in H$ *für alle* $x \in H$.

Beweis. Eine Untergruppe erfüllt die Eigenschaften (a),(b) und (c) aufgrund der Gruppenaxiome. Gelten (a),(b) und (c), so ist $H \neq \varnothing$ und mit $h \in H$ ist damit auch $e = h^{-1}h \in H$. Da sich das Assoziativgesetz stets auf Unterstrukturen vererbt, ist H damit eine Untergruppe. □

Beispiele. (1) Für $n \in \mathbb{N}$ und $i \in \{1, \ldots, n\}$ ist

$$\mathrm{Stab}_{\mathcal{S}_n}(i) := \{\sigma \in \mathcal{S}_n \mid \sigma(i) = i\}.$$

eine Untergruppe von $\mathcal{S}_n$.

[3] Ist G eine abelsche Gruppe, so bezeichnen wir die Verknüpfung auch gelegentlich mit $(G, +)$. In diesem Fall bezeichnen wir das neutrale Element mit 0 und das inverse Elemente von $x \in G$ mit $-x$.

[4] Da $\mu(h_1, h_2) \in H$ gilt, ist $\mu|_{H \times H} \colon H \times H \longrightarrow H$ eine wohldefinierte Abbildung.

(2) Sei $n \in \mathbb{N}$. Die Menge der n-ten Einheitswurzeln $\mathcal{C}_n := \{e^{2\pi i \frac{m}{n}} \mid 0 \leq m \leq n-1\}$ ist eine Untergruppe von $(\mathbb{C} \setminus \{0\}, \cdot)$ mit genau n Elementen: Es gilt $1 = e^0 \in \mathcal{C}_n$. Für $0 \leq m_1, m_2 < n$ schreiben wir $m_1 + m_2 = qn + r$ mit $0 \leq r < n$. Es gilt

$$e^{2\pi i \frac{m_1}{n}} \cdot e^{2\pi i \frac{m_2}{n}} = e^{2\pi i \frac{qn+r}{n}} = e^{2\pi i \frac{qn}{n}} \cdot e^{2\pi i \frac{r}{n}} = (e^{2\pi i})^q \cdot e^{2\pi i \frac{r}{n}} = e^{2\pi i \frac{r}{n}} \in \mathcal{C}_n.$$

Analog zeigt man, dass für $e^{2\pi i \frac{m}{n}} \in \mathcal{C}_n$ auch $(e^{2\pi i \frac{m}{n}})^{-1} \in \mathcal{C}_n$ gilt.

Lemma 1.2.3. *Sei G eine Gruppe, $\mathcal{U}$ eine Menge von Untergruppen von G sowie $S \subseteq G$ eine Teilmenge. Dann gilt:*

(1) $\bigcap_{H \in \mathcal{U}} H$ is eine Untergruppe von G.

(2) Sei $\mathcal{U}_S$ die Menge aller Untergruppen von G, die S enthalten. Dann ist

$$\langle S \rangle := \bigcap_{H \in \mathcal{U}_S} H$$

die kleinste Untergruppe von G, die S enthält. Wir nennen $\langle S \rangle$ die von S in G erzeugte Untergruppe.

(3) $\langle S \rangle = \{s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} \mid n \in \mathbb{N}_0, s_i \in S, \varepsilon_i \in \{1, -1\}\}$[a].

[a] Für G in additiver Schreibweise $(G, +)$ ist $\langle S \rangle = \{(\varepsilon_1)s_1 + \cdots + (\varepsilon_n)s_n \mid n \in \mathbb{N}_0, s_i \in S, \varepsilon_i \in \{1, -1\}\}$.

Beweis.

(1) Dies folgt durch Nachprüfen des Untergruppenkriteriums.

(2) Nach (1) ist $\langle S \rangle$ eine Untergruppe. Sei $U \subseteq G$ eine Untergruppe von U die S enthält, so folgt $U \in \mathcal{U}_S$ und damit $\langle S \rangle \subseteq U$.

(3) Mit dem Untergruppenkriterium lässt sich zeigen, dass

$$V := \{s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} \mid n \in \mathbb{N}_0, s_i \in S, \varepsilon_i \in \{1, -1\}\}$$

eine Untergruppe von G ist, die S enthält. Das heißt $V \in \mathcal{U}_S$. Sei nun $U \in \mathcal{U}_S$. Dann gilt $S \subseteq U$ und damit $s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} \in U$ für alle $n \in \mathbb{N}_0$, $s_i \in S$ und $\varepsilon_i \in \{-1, 1\}$. Insgesamt folgt also $\langle S \rangle \overset{(2)}{\subseteq} V \subseteq \bigcap_{U \in \mathcal{U}_S} U = \langle S \rangle$.

□

Beispiele. (1) Für $n \in \mathbb{Z}$ gilt $\langle \{n\} \rangle = \{nz \mid n \in \mathbb{Z}\} =: n\mathbb{Z}$.

(2) Es gilt $\langle \{1\} \rangle = \mathbb{Z}$.

(3) Es sei $S := \{2, 3\}$. Dann gilt $1 = 3 - 2 \in \langle S \rangle$. Es folgt $\mathbb{Z} = \langle \{1\} \rangle \subseteq \langle S \rangle \subseteq \mathbb{Z}$, also $\langle S \rangle = \mathbb{Z}$.

(4) Es gilt $\langle \{6, 15\} \rangle = \langle \{3\} \rangle$.

Ist S eine endliche Menge, so bezeichnen wir mit $|S|$ die Anzahl der Elemente von S. Ist G eine endliche Gruppe, das heißt die zugrundeliegende Menge ist endlich, so heißt $|G|$ die **Ordnung** von G.

Definition. Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe. Für $x \in G$ heißt

$$xH := \{xh \mid h \in H\}$$

die **Linksnebenklasse** von x in H. Wir schreiben

$$G/H := \{xH \mid x \in G\}.$$

Ist G/H endlich, so heißt $[G : H] := |G/H|$ der **Index** von H in G.

Satz 1.2.4 (Satz von Lagrange). *Sei G eine endliche Gruppe, $H \subseteq G$ eine Untergruppe. Dann gilt*

$$|G| = [G : H]|H|.$$

Beweis. Seien $x, y \in G$. Dann definiert

$$x \sim y :\Leftrightarrow x^{-1}y \in H$$

eine Äquivalenzrelation auf G. Es sei $G/\sim$ die Menge der Äquivalenzklassen. Nach Definition gilt $[x] = xH$ für jedes $x \in G$. Damit ist

$$G = \bigsqcup_{[x] \in G/\sim} [x]$$

die disjunkte Vereinigung der Äquivalenzklassen und $G/H = G/\sim$. Außerdem ist für jedes $x \in G$ die Abbildung

$$f_x : H \longrightarrow xH = [x] \;\; ; \;\; h \mapsto xh$$

bijektiv. Damit folgt

$$|G| = |\bigsqcup_{[x] \in G/H} [x]| = \sum_{G/H} |[x]| = \sum_{G/H} |H| = [G : H] \cdot |H|.$$

□

Beispiel. Nach dem Satz von Lagrange ist für eine endliche Gruppe G die Mächtigkeit jeder Untergruppe ein Teiler von $|G|$. Zum Beispiel folgt für $|G| = 6$, dass für eine Untergruppe U nicht $|U| = 4$ oder $|U| = 5$ gelten kann.

1.3 Zyklische Gruppen

Es sei $(G, \cdot)$ eine Gruppe, $x \in G$ und $z \in \mathbb{Z}$. Wir definieren

$$x^z := \begin{cases} e & z = 0 \\ \underbrace{x \cdot x \cdots x}_{z-\text{mal}} & z > 0 \\ \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{|z|-\text{mal}} & z < 0. \end{cases}$$

Ist G abelsch und in additiver Schreibweise $G = (\mathbb{Z}, +)$ gegeben, so schreiben wir zx anstatt x^z.

Definition. Eine Gruppe G heißt **zyklisch**, falls ein $x \in G$ mit $G = \langle \{x\} \rangle$ existiert. In diesem Fall gilt $G = \{x^z \mid z \in \mathbb{Z}\}$. Wir schreiben dann $G = \langle x \rangle$.

Beispiele. (1) Es sei $n \in \mathbb{N}$. Dann ist die Gruppe der n-ten Einheitswurzeln $\mathcal{C}_n = \{e^{2\pi i \frac{m}{n}} \mid 0 \leq m \leq n-1\}$ zyklisch, da $(e^{\frac{2\pi i}{n}})^m = e^{2\pi i \frac{m}{n}}$ für alle $m \in \{0, \ldots, n-1\}$ gilt.

(2) Division mit Rest zeigt, dass jede Untergruppe $H \subseteq \mathbb{Z}$ zyklisch ist: Ist $H \neq \{0\}$, so finden wir $n \in H \cap \mathbb{N}$ minimal. Damit ist $\langle n \rangle \subseteq H$. Für $m \in H$ liefert Division mit Rest eine Darstellung $m = qn + r$ mit $0 \leq r < n$. Das heißt $r = m - qn \in H \cap \mathbb{N}_0$. Minimalität von n liefert $r = 0$. Das heißt $m = qn$ und $m \in \langle n \rangle$.[5]

(3) Es sei G eine Gruppe mit $|G| = p \in \mathbb{P}$ Primzahl und $x \in G \setminus \{e\}$. Dann ist $\{e, x\} \subseteq \langle x \rangle \subseteq G$ eine Untergruppe mit mindestens zwei Elementen. Nach dem Satz von Lagrange folgt $|\langle x \rangle| = p = |G|$ und damit $\langle x \rangle = G$. Also ist G zyklisch.

(4) $(\mathbb{Q}, +)$ ist nicht zyklisch: Angenommen $(\mathbb{Q}, +)$ ist zyklisch, so finden wir $n, m \in \mathbb{N}$ mit $\langle \frac{n}{m} \rangle = \mathbb{Q}$. Sei $p \in \mathbb{P}$ eine Primzahl mit $p \nmid m$. Dann gilt $z\frac{n}{m} \neq \frac{1}{p}$ für alle $z \in \mathbb{Z}$.

(5) Jede zyklische Gruppe $G = \langle x \rangle$ ist abelsch, da $x^{z_1} x^{z_2} = x^{z_1 + z_2} = x^{z_2 + z_1} = x^{z_2} x^{z_1}$ für alle $z_1, z_2 \in \mathbb{Z}$ gilt. Die Umkehrung gilt nicht nach (4).

Definition. Sei G eine Gruppe, $x \in G$. Ist $\langle x \rangle$ endlich, so heißt $\operatorname{ord}(x) := |\langle x \rangle|$ die **Ordnung** von x. Andernfalls hat x **unendliche Ordnung**.

Satz 1.3.1. *Sei G eine Gruppe sowie $x \in G$. Dann gilt:*

(1) Hat x endliche Ordnung, so gilt

$$\operatorname{ord}(x) = \min\{n \in \mathbb{N} \mid x^n = e\} \text{ und } \langle x \rangle = \{x^0 = e, x^2, \ldots, x^{\operatorname{ord}(x)-1}\}.$$

(2) Ist $m \in \mathbb{N}$ ein Element mit $x^m = e$, so hat x endliche Ordnung und $\operatorname{ord}(x)$ teilt m.

[5] Hier verwenden wir die additive Schreibweise.

(3) Hat $x \in G$ endliche Ordnung, so hat x^s für jedes $s \in \mathbb{Z}$ endliche Ordnung und es gilt

$$\operatorname{ord}(x^s) = \frac{\operatorname{ord}(x)}{\operatorname{ggT}(\operatorname{ord}(x), s)}.$$

(4) Ein Element $x \in G$ hat unendliche Ordnung genau dann, wenn alle Potenzen von x paarweise verschieden sind.

Beweis.

(1) Wir betrachten $H := \{n \in \mathbb{Z} \mid x^n = e\}$. Dann ist $H \subseteq \mathbb{Z}$ eine Untergruppe und es gibt $m_0 \in \mathbb{N}_0$ mit $H = \langle m_0 \rangle = \{zm_0 \mid z \in \mathbb{Z}\}$.

Die Annahme $m_0 = 0$ liefert $H = \{0\}$ und aus $x^n = x^m$ mit $n \geq m \geq 1$ folgt $x^{n-m} = e$. Das heißt $n - m \in H = \{0\}$ und $n = m$. Damit ist die Abbildung

$$f : \mathbb{Z} \longrightarrow \langle x \rangle \ ; \ n \mapsto x^n$$

ist injektiv und hat x unendliche Ordnung, ein Widerspruch.

Es gilt also $m_0 > 0$ und wir behaupten, dass $\langle x \rangle = \{x^n \mid 0 \leq n \leq m_0 - 1\}$. Die Inklusion $\supseteq$ folgt aus Lemma 1.2.3(3). Sei $h \in \langle x \rangle$. Dann existiert nach Lemma 1.2.3(3) ein $s \in \mathbb{Z}$ mit $h = x^s$. Division mit Rest liefert $q, r \in \mathbb{Z}$ mit $s = qm_0 + r$, wobei $r \in \{0, \ldots, m_0 - 1\}$. Es folgt dann

$$h = x^s = (x^{m_0})^q x^r = x^r.$$

Dies beweist die Behauptung und wir erhalten $\operatorname{ord}(x) \leq m_0$.

Seien $0 \leq s \leq t \leq m_0 - 1$ mit $x^s = x^t$ gegeben. Dann gilt $0 \leq t - s \leq m_0 - 1$ sowie

$$x^{t-s} = e.$$

Es folgt $t - s \in H$ und somit $s = t$. Also haben wir $\operatorname{ord}(x) = m_0 = \min H \cap \mathbb{N}$.

(2) Sei $s \in \mathbb{Z}$, dann existieren $q \in \mathbb{Z}$ und $0 \leq r < m$ mit $s = qm + r$. Wir erhalten $x^s = (x^m)^q x^r = x^r$. Es folgt $\operatorname{ord}(x) \leq m$. Wir schreiben nun $m = q \operatorname{ord}(x) + r$ mit $0 \leq r < \operatorname{ord}(x)$ und erhalten $e = x^m = x^r$. Da $r < \operatorname{ord}(x)$ gilt, liefert (1) $r = 0$. Damit ist $\operatorname{ord}(x)$ ein Teiler von m.

(3) Es sei ohne Beschränkung der Allgemeinheit $s \in \mathbb{N}$. Dann gilt

$$(x^s)^{\operatorname{ord}(x)} = (x^{\operatorname{ord}(x)})^s = e$$

Damit hat x^s nach (2) endliche Ordnung. Es sei nun

$$d := \operatorname{ggT}(\operatorname{ord}(x), s).$$

Das Lemma von Bézout liefert $a, b \in \mathbb{Z}$ mit $d = a \operatorname{ord}(x) + bs$. Damit erhalten wir

$$x^{\operatorname{ord}(x^s)d} = ((x^{\operatorname{ord}(x)})^{\operatorname{ord}(x^s)})^a \cdot x^{\operatorname{ord}(x^s)bs} = ((x^s)^{\operatorname{ord}(x^s)})^b = e.$$

Wegen (2) gilt $\operatorname{ord}(x^s)d = \operatorname{ord}(x)n$ für ein $n \in \mathbb{N}$. Wegen $\frac{s}{d} \in \mathbb{N}$ folgt außerdem

$$(x^s)^{\frac{\operatorname{ord}(x)}{d}} = (x^{\operatorname{ord}(x)})^{\frac{s}{d}} = e,$$

also gibt es $m \in \mathbb{N}$ mit $\frac{\operatorname{ord}(x)}{d} = m \operatorname{ord}(x^s)$. Insgesamt erhalten wir somit

$$\operatorname{ord}(x) = \operatorname{ord}(x^s)dm = \operatorname{ord}(x)mn$$

und daher $m = n = 1$. Damit folgt $\operatorname{ord}(x^s)d = \operatorname{ord}(x)n = \operatorname{ord}(x)$.

(4) Sind alle Potenzen paarweise verschieden, so ist die Abbildung

$$f : \mathbb{Z} \longrightarrow \langle x \rangle \ ; \ n \mapsto x^n$$

injektiv und x hat unendliche Ordnung. Gibt es $n < m$ mit $x^n = x^m$, so folgt $x^{m-n} = e$ und x hat nach (2) endliche Ordnung.

□

Beispiel.

(1) Wir verwenden für Permutationen die aus der Linearen Algebra bekannte Schreibweise. Es sei $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \in \mathcal{S}_5$. Nachrechnen zeigt $\sigma^i \neq \mathrm{id}$ für $i \in \{1, 2, 3, 4\}$ und $\sigma^5 = \mathrm{id}$. Das heißt $\mathrm{ord}(\sigma) = 5$. Weiter gilt $\mathrm{ord}(\sigma^2) = \frac{\mathrm{ord}(\sigma)}{\mathrm{ggT}(\mathrm{ord}(\sigma),2)} = 5$. Mit $\langle \sigma^2 \rangle \subseteq \langle \sigma \rangle$ folgt $\langle \sigma \rangle = \langle \sigma^2 \rangle$.

(2) Es sei G eine endliche Gruppe und $x \in G$. Dann ist $\mathrm{ord}(x) = |\langle x \rangle|$ nach dem Satz von Lagrange ein Teiler von $|G|$. Wir schreiben $\mathrm{ord}(x)\ell = |G|$ mit $\ell = [G : \langle x \rangle] \in \mathbb{N}$. Es folgt $x^{|G|} = (x^{\mathrm{ord}(x)})^\ell = e^\ell = e$.

Satz 1.3.2. *Sei $G = \langle x \rangle$ eine zyklische Gruppe.*

(1) Jede Untergruppe $H \subseteq G$ is zyklisch.

(2) Gilt $|G| = n$, so ist für einen Teiler d von n

$$G_d := \langle x^{\frac{n}{d}} \rangle$$

die einzige Untergruppe von G der Ordnung d.

(3) Gilt $|G| = n$ und ist $H \subseteq G$ eine Untergruppe, so existiert ein Teiler d von n mit $H = G_d$.

Beweis.

(1) Ist $H \neq \{e\}$, so existiert

$$n_0 := \min\{n \in \mathbb{N} \mid x^n \in H\}.$$

Wir behaupten: $H = \langle x^{n_0} \rangle$, wobei die Inklusion $\supseteq$ aus Lemma 1.2.3(2) folgt. Sei $h = x^n \in H$. Dann existieren $q, r \in \mathbb{Z}$ mit $n = qn_0 + r$ und $r \in \{0, \ldots, n_0 - 1\}$. Es folgt $x^r = h(x^{n_0})^{-q} \in H$. Nach Definition von n_0 impliziert dies $r = 0$, und damit $h = (x^{n_0})^q \in \langle x^{n_0} \rangle$. Insbesondere ist H damit zyklisch.

(2) Wegen $d \mid n$ gilt $\frac{n}{d} = \mathrm{ggT}(n, \frac{n}{d})$ und Satz 1.3.1 liefert $\mathrm{ord}(x^{\frac{n}{d}}) = d$. Also hat G_d die Ordnung d.

Sei nun $H \subseteq G$ eine Untergruppe der Ordnung d. Für $d = 1$ gilt $H = \{e\} = G_1$. Andernfalls liefert (1) ein $m \in \mathbb{N}$ mit $H = \langle x^m \rangle$ und nach dem Beweis von (1) können wir $m = \min\{t \in \mathbb{N} \mid x^t \in H\}$ wählen. Dann gilt nach Satz 1.3.1(3)

$$d = \mathrm{ord}(x^m) = \frac{n}{\mathrm{ggT}(m, n)}.$$

Wie schreiben $n = qm + r$ mit $r \in \{0, \ldots, m-1\}$. Dann gilt mit Bespiel (2) der vorherigen Seite

$$x^{-r} = ex^{-r} = x^n \cdot x^{-r} = x^{n-r} = (x^m)^q \in H.$$

Also ist $x^r = (x^{-r})^{-1}$ ein Element von H, was nach Wahl von m die Gleichung $r = 0$ impliziert. Wir erhalten $n = qm$ und $\mathrm{ggT}(m, n) = m$. Dies liefert $d = \frac{n}{m}$ und $m = \frac{n}{d}$, also $H = G_d$.

(3) Sei H eine Untergruppe der Ordnung d. Nach dem Satz von Lagrange ist d ein Teiler von n und (2) impliziert $H = G_d$.

□

Beispiel. Wir betrachten die Permutationen

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ und } \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Es sind $\langle\sigma\rangle \neq \langle\tau\rangle$ Untergruppen von $\mathcal{S}_3$ der Ordnung 2. Damit ist $\mathcal{S}_3$ nach Satz 1.3.2 nicht zyklisch.

1.4 Homomorphismen und Normalteiler

Definition. Es seien G, G' Gruppen.

(1) Eine Abbildung $\varphi : G \longrightarrow G'$ zwischen zwei Gruppen heißt **Homomorphismus**, falls

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

für alle $x, y \in G$ gilt.

(2) Ein bijektiver Homomorphismus $\varphi\colon G \longrightarrow G'$ heißt **Isomorphismus**. In diesem Fall ist die Umkehrabbildung $\varphi^{-1}\colon G' \longrightarrow G$ ebenfalls ein Homomorphismus.

(3) Wir sagen G ist **isomorph** zu G', falls ein Isomorphismus $\varphi\colon G \longrightarrow G'$ existiert. In diesem Fall schreiben wir $G \cong G'$.

Lemma 1.4.1. *Sei $\varphi : G \longrightarrow G'$ ein Homomorphismus. Es gelten die folgenden Aussagen.*

(1) $\varphi(e_G) = e_{G'}$.

(2) $\varphi(x^{-1}) = \varphi(x)^{-1}$ *für alle* $x \in G$.

(3) Das ***Bild*** $\operatorname{im}\varphi := \{\varphi(x) \mid x \in G\}$ *von φ ist eine Untergruppe von G'.*

(4) Der ***Kern*** $\ker\varphi := \varphi^{-1}(e_{G'}) = \{x \in G \mid \varphi(x) = e_{G'}\}$ *von φ ist eine Untergruppe von G.*

(5) $\varphi^{-1}(\varphi(x)) = x \ker\varphi = \{xz \mid z \in \ker\varphi\}$ *für alle* $x \in G$.

Beweis. Siehe [5, (3.2.30), (3.2.39)] für die Beweise von (1) - (4). Wir zeigen (5). Sei $x \in G$ und $y \in \varphi^{-1}(\varphi(x))$, dann ist $y = xx^{-1}y \in x \ker \varphi$, da $\varphi(x^{-1}y) \overset{(2)}{=} \varphi(x)^{-1}\varphi(y) = \varphi(x)^{-1}\varphi(x) = e_{G'}$. Anderseits ist $\varphi(xz) = \varphi(x)\varphi(z) = \varphi(x)$ für alle $z \in \ker \varphi$. Das heißt $xz \in \varphi^{-1}(\varphi(x))$. □

Bemerkung 1.4.2. Nach Lemma 1.4.1 ist ein Homomorphismus $\varphi\colon G \longrightarrow G'$ injektiv, genau dann, wenn $\ker \varphi = \{e_G\}$ gilt, da

$$\varphi \text{ ist injektiv } \Leftrightarrow \varphi^{-1}(\varphi(x)) = \{x\} \text{ für alle } x \in G \Leftrightarrow \ x \ker \varphi = \{x\} \text{ für alle } x \in G \Leftrightarrow \ker \varphi = \{e\}.$$

Definition. Es sei G eine Gruppe. Ein Isomorphismus $\varphi\colon G \longrightarrow G$ heißt **Automorphismus**. Dann ist

$$\mathrm{Aut}(G) := \{\varphi \in \mathcal{S}_G \mid \varphi \text{ ist Automorphismus}\}$$

eine Untergruppe von $\mathcal{S}_G$.

Beispiele. (1) $\exp\colon (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \cdot)\ ;\ z \mapsto e^z$ ist ein Isomorphismus.

(2) $\varphi\colon (\mathbb{C} \setminus \{0\}, \cdot) \longrightarrow (\mathbb{R} \setminus \{0\}, \cdot)\ ;\ z \mapsto |z|$ ist ein Homomorphismus, der weder injektiv noch surjektiv ist. Sei $S \subseteq \mathbb{C}$ der Einheitskreis und $z \in \mathbb{C} \setminus \{0\}$, so gilt

$$\varphi^{-1}(\varphi(z)) = z \ker \varphi = zS^1 = |z|e^{i \arg(z)}S = |z|S,$$

da $e^{i \arg(z)} = \cos(\arg(z)) + i \sin(\arg(z)) \in S$ und S eine Untergruppe von $(\mathbb{C} \setminus \{0\}, \cdot)$ ist. Abbildung 1.1 zeigt die Urbilder $\varphi^{-1}(2)$ und $\varphi^{-1}(\frac{7}{2})$ in der Gaußschen Zahlenebene.

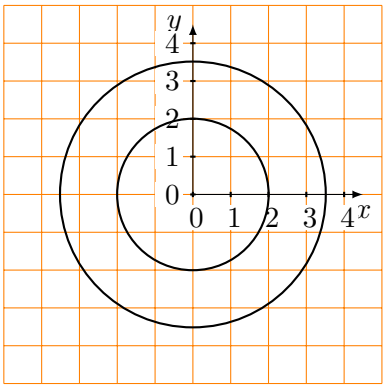


Abbildung 1.1: Urbilder von 2 und $\frac{7}{2}$ unter dem Homomorphismus φ aus Beispiel (2).

(3) Es sei $n \in \mathbb{N}$ und $\mathrm{GL}_n(\mathbb{R})$ die Menge der invertierbaren $n \times n$-Matrizen. Nach dem Determinantenproduktsatz ist die Determinantenabbildung

$$\det\colon (\mathrm{GL}_n(\mathbb{R}), \cdot) \longrightarrow (\mathbb{R} \setminus \{0\}, \cdot)\ ;\ A \mapsto \det(A)$$

ein Gruppenhomomorphismus mit $\ker \det = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\} =: \mathrm{SL}_n(\mathbb{R})$.

(4) Es sei $n \in \mathbb{N}$, $\sigma \in \mathcal{S}_n$ und $A(\sigma) \in \mathrm{GL}_n(\mathbb{R})$ die zugehörige **Permutationsmatrix**. Per Definition gilt $A(\sigma) = (a_{ij})$ mit $a_{ij} = \delta_{i\sigma(j)}$ für alle $i, j \in \{1, \ldots, n\}$. Die Leibnizformel liefert

$$\det(A(\sigma)) = \sum_{\tau \in \mathcal{S}_n} \operatorname{sgn}(\tau) \prod_{i=1}^{n} a_{\tau(i)i} = \sum_{\tau \in \mathcal{S}_n} \operatorname{sgn}(\tau) \prod_{i=1}^{n} \delta_{\tau(i)\sigma(i)} = \operatorname{sgn}(\sigma),$$

wobei $\operatorname{sgn}(\tau)$ das **Signum/Vorzeichen** von τ bezeichnet (siehe [5, (3.3.5)]). Nachrechnen zeigt, dass $A(\sigma)A(\tau) = A(\sigma \circ \tau)$ für alle $\sigma, \tau \in \mathcal{S}_n$ gilt. Nach (3) ist damit auch $\operatorname{sgn}\colon \mathcal{S}_n \longrightarrow (\{\pm 1\}, \cdot), \sigma \mapsto \operatorname{sgn}(\sigma)$ ein Gruppenhomomorphismus (vergleiche [5, (3.3.9)]).

(5) Ist G eine Gruppe und $g \in G$, so ist $\iota_g\colon G \longrightarrow G; x \mapsto gxg^{-1}$ ein Automorphismus mit Umkehrabbildung $\iota_g^{-1} = \iota_{g^{-1}}$ (Übung).

Der folgende Satz besagt, dass eine Gruppe G als Untergruppe der symmetrischen Gruppe $\mathcal{S}_G$ aufgefasst werden kann.

Proposition 1.4.3 (Satz von Cayley). *Sei G eine Gruppe. Dann ist $\varphi : G \longrightarrow \mathcal{S}_G$, mit*

$$\varphi(x)(y) := xy \quad \textit{für alle } x, y \in G$$

ein injektiver Gruppenhomomorphismus.

Beweis. Sei $x \in G$. Wegen $\varphi(x)(x^{-1}y) = y$ für alle $y \in G$ ist die Abbildung $\varphi(x) : G \longrightarrow G$ surjektiv. Gilt für $y, z \in G$ die Gleichung $\varphi(x)(y) = \varphi(x)(z)$, so erhalten wir $xy = xz$ und somit $y = z$. Mithin ist $\varphi(x) \in \mathcal{S}_G$ und die Abbildung φ ist wohldefiniert. Wegen $\varphi(xy)(z) = (xy)z = x(yz) = \varphi(x)(\varphi(y)(z)) = [\varphi(x) \circ \varphi(y)](z)$ für alle $x, y, z \in G$ folgt

$$\varphi(xy) = \varphi(x) \circ \varphi(y).$$

Damit ist φ ein Gruppenhomomorphismus.
Ist $x \in \ker \varphi$, so gilt $\varphi(x) = \mathrm{id}_G$ und somit $e = \mathrm{id}_G(e) = \varphi(x)(e) = xe = x$. Also ist φ injektiv. □

Definition. Sei G eine Gruppe. Eine Untergruppe $N \subseteq G$ heißt **Normalteiler von** G oder **normal in** G, falls

$$xNx^{-1} = N$$

für alle $x \in G$ gilt. In diesem Fall schreiben wir $N \trianglelefteq G$.

Lemma 1.4.4. *Sei G eine Gruppe und $N \subseteq G$ eine Untergruppe. Folgende Bedingungen sind äquivalent:*

(1) N ist ein Normalteiler von G.

(2) Es gilt $xN = Nx$ für alle $x \in G$.

(3) Es gilt $xnx^{-1} \in N$ für alle $x \in G$.

Beweis. (1) $\Rightarrow$ (2) und (2) $\Rightarrow$ (3) folgen unmittelbar. Gelte also $xnx^{-1} \in N$ für alle $x \in G$. Sei $y \in G$ fixiert, dann erhalten wir direkt $yNy^{-1} \subseteq N$. Sei nun $n \in N$, dann ist

$$n = y(y^{-1}ny)y^{-1} = y(\underbrace{y^{-1}n(y^{-1})^{-1}}_{\in N})y^{-1} \in yNy^{-1}.$$

□

Beispiele. (1) $H := \mathrm{Stab}_{\mathcal{S}_3}(3)$ ist nicht normal in $\mathcal{S}_3$: Es sei $\tau := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in H$. Für $\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in \mathcal{S}_3$ gilt $(\sigma \circ \tau \circ \sigma^{-1})(3) = (\sigma \circ \tau)(2) = \sigma(1) = 1$, und somit $\sigma \circ \tau \circ \sigma^{-1} \notin H$.

(2) Ist G eine abelsche Gruppe und $N \subseteq G$ eine Untergruppe. Für $x \in G$ und $n \in N$ gilt $xnx^{-1} = xx^{-1}n = n \in N$. Damit ist N ein Normalteiler.

(3) Ist $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus, so sind Urbilder von Normalteilern wieder Normalteiler. Insbesondere ist $\ker\varphi = \varphi^{-1}(\{e_{G'}\})$ ein Normalteiler von G. Bilder von Normalteilern sind in der Regel keine Normalteiler (siehe Beispiel (1)).

(4) Sei $n \in \mathbb{N}$, dann ist $\mathcal{A}_n := \ker\mathrm{sgn} \trianglelefteq \mathcal{S}_n$ ein Normalteiler von $\mathcal{S}_n$. Die Gruppe $\mathcal{A}_n$ heißt die **alternierende Gruppe auf n Elementen**.

1.5 Faktorgruppen und Isomorphiesätze

Sei G eine Gruppe, $N \trianglelefteq G$ eine normale Untergruppe. Die spezielle Beschaffenheit von Normalteilern erlaubt uns auf der Menge der Linksnebenklassen G/N in natürlicher Weise eine Gruppenstruktur zu definieren: Die Menge

$$G/N = \{xN \mid x \in G\}$$

erhält durch

$$(xN) \cdot (yN) := xyN$$

die Struktur einer Gruppe mit neutralem Element $e_{G/N} = N = eN$. Diese Gruppe heißt **Faktorgruppe** von G nach N. Die Abbildung

$$\pi : G \longrightarrow G/N \; ; \; x \mapsto xN$$

ist ein surjektiver Homomorphismus mit $\ker\pi = N$. Wir nennen π die **kanonische Projektion**.

Bemerkungen 1.5.1.

(1) Obige Zuordnung ist wohldefiniert, da N ein Normalteiler von G ist: Sind $x_1, x_2, y_1, y_2 \in G$ mit $x_1N = x_2N$ und $y_1N = y_2N$, so gilt $x_1^{-1}x_2, y_1^{-1}y_2 \in N$ und damit

$$(x_1y_1)^{-1}(x_2y_2)N = y_1^{-1}x_1^{-1}x_2y_2N = (y_1^{-1}y_2)\underbrace{(y_2^{-1}(x_1^{-1}x_2)y_2)}_{\in N}N = N,$$

da N ein Normalteiler ist. Das heißt $x_1y_1N = x_2y_2N$

(2) Es gilt $(xN)^{-1} = x^{-1}N$ für jedes $x \in G$.

(3) $U := \mathrm{Stab}_{\mathcal{S}_3}(3)$ ist kein Normalteiler von $\mathcal{S}_3$ und die Zuordnung

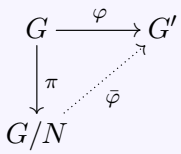
$$\mathcal{S}_3/U \times \mathcal{S}_3/U \longrightarrow \mathcal{S}_3/U, (\sigma U, \tau U) \mapsto \sigma \circ \tau U^{6}$$

nicht wohldefiniert:
Es seien $\sigma = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ und $\tau = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \in \mathcal{S}_3$. Es gilt $\sigma^{-1} \circ \tau = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \in U$, also $\sigma U = \tau U$. Es gilt aber $\sigma \circ \sigma = \mathrm{id} \in U$ und $\tau \circ \tau = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \notin U$. Das heißt

$$(\sigma \circ \sigma)U = U \neq (\tau \circ \tau)U.$$

(4) Wir haben bereits gesehen, dass für einen Homomorphismus $\varphi\colon G \longrightarrow G'$ der Kern $\ker\varphi$ ein Normalteiler von G ist. Es sei nun $N \trianglelefteq G$ ein Normalteiler, so ist $\pi\colon G \longrightarrow G/N$ ein Homomorphismus und $\ker\varphi = N$. Damit sind Normalteiler genau die Untergruppen, die als Kern eines Homomorphismus auftreten.

Satz 1.5.2 (Homomorphiesatz). *Seien $\varphi : G \longrightarrow G'$ ein Homomorphismus von Gruppen und $N \trianglelefteq G$ ein Normalteiler mit $N \subseteq \ker\varphi$. Dann existiert genau ein Homomorphismus $\bar{\varphi} : G/N \longrightarrow G'$ derart, dass $\bar{\varphi} \circ \pi = \varphi$ gilt. Das heißt wir erhalten das kommutative Diagram*



Beweis. Sind $\bar{\varphi}_1, \bar{\varphi}_2\colon G/N \longrightarrow G'$ mit $\bar{\varphi}_1 \circ \pi = \varphi = \bar{\varphi}_2 \circ \pi$, dann stimmen $\bar{\varphi}_1$ und $\bar{\varphi}_2$ auf $\mathrm{im}\,\pi = G/N$ überein und es folgt $\bar{\varphi}_1 = \bar{\varphi}_2$. Damit ist die Abbildung $\bar{\varphi}$ eindeutig bestimmt. Notwendigerweise setzen wir

$$\bar{\varphi}(xN) := \varphi(x)$$

für alle $x \in G$. Gilt $xN = yN$, so folgt nach Voraussetzung $x^{-1}y \in N \subseteq \ker\varphi$. Damit erhalten wir

$$\varphi(x) = \varphi(x)e_{G'} = \varphi(x)\varphi(x^{-1}y) = \varphi(xx^{-1}y) = \varphi(y).$$

Also ist $\bar{\varphi}$ wohldefiniert. Die restlichen Behauptungen ergeben sich durch direktes Nachrechnen. □

Der folgende Satz ist nun eine einfache Folgerung, die Konsequenzen dieser Aussage sind jedoch weitreichend.

[6] Streng genommen müssten wir hier $\sigma \circ \tau \circ U$ schreiben.

Korollar 1.5.3. *Sei $\varphi : G \longrightarrow G'$ ein Homomorphismus. Dann ist*

$$\bar{\varphi}\colon G/\ker\varphi \longrightarrow G' \ ;\ x\ker\varphi \mapsto \varphi(x)$$

ein injektiver Homomorphismus mit $\operatorname{im}\bar{\varphi} = \operatorname{im}\varphi$. Insbesondere gilt daher $G/\ker\varphi \cong \operatorname{im}\varphi$.

Beweis. Nach Satz 1.5.2 ist $\bar{\varphi}$ wohldefiniert. Da $\pi\colon G \longrightarrow G/\ker\varphi$ surjektiv ist, folgt $\operatorname{im}\varphi = \operatorname{im}(\bar{\varphi}\circ\pi) = \operatorname{im}\bar{\varphi}$. Ist $x\ker\varphi \in \ker\bar{\varphi}$, so gilt $e_{G'} = \bar{\varphi}(x\ker\varphi) = \varphi(x)$ und damit $x \in \ker\varphi$. Das heißt $x\ker\varphi = \ker\varphi = e_{G/\ker\varphi}$ □

Bemerkung 1.5.4. Da der Satz erfahrungsgemäß einschüchternd wirkt, geben wir hier eine mögliche Interpretation: Wir starten mit einem Homomorphismus $\varphi\colon G \longrightarrow G'$ und nehmen an, dass wir die Gruppe G' gut kennen (und damit auch insbesondere alle Untergruppen).

Ist φ injektiv, so können wir $G \cong \operatorname{im}\varphi$ als Untergruppe von G' auffassen. In diesem Fall verstehen wir also auch G.

Ist φ nicht injektiv, so gilt $\ker\varphi \neq \{e\}$. Um wieder einen injektiven Homomorphismus zu erhalten, fassen wir alle Elemente in $\ker\varphi$ als ein Element auf. Dies geschieht durch den Übergang zu $G/\ker\varphi$. In dieser Gruppe ist $\ker\varphi \in G/\ker\varphi$ das neutrale Element und $\ker\bar{\varphi} = \ker\varphi$. Damit ist $\bar{\varphi}\colon G/\ker\varphi \longrightarrow G$ injektiv. Der Preis den wir zahlen müssen, ist der Übergang zu einer „kleineren" Gruppe $G/\ker\varphi$, die G mithilfe von $\ker\varphi$ approximiert: Für $x, y \in G$ stimmen die Nebenklassen $x\ker\varphi$, $y\ker\varphi$ genau dann überein, wenn sich x und y nur durch Multiplikation mit einem Element aus $\ker\varphi$ unterscheiden.

Beispiele. (1) Übungsaufgabe: Mithilfe von Korollar 1.5.3 lässt sich zeigen, dass für jede zyklische Gruppe G genau ein $n \in \mathbb{N}_0$ mit $G \cong \mathbb{Z}/\langle n\rangle$ existiert. Insbesondere gilt $\mathcal{C}_n \cong \mathbb{Z}/\langle n\rangle$ für $n \in \mathbb{N}$.

(2) Ist $\varphi\colon G \longrightarrow G'$ ein surjektiver Homomorphismus zwischen endlichen Gruppen, so ist nach dem Satz von Lagrange und Korollar 1.5.3 die Ordnung von G' ein Teiler der Ordnung von G, da $|G'| = |\operatorname{im}\varphi| = |G/\ker\varphi| = \frac{|G|}{|\ker\varphi|}$.

(3) Ist $\varphi\colon \mathbb{Z}/\langle 12\rangle \longrightarrow \mathbb{Z}/\langle 7\rangle$ ein Homomorphismus, so gilt $\varphi(x) = 0_{\mathbb{Z}/\langle 7\rangle}$ für alle $x \in \mathbb{Z}/\langle 7\rangle$: Wäre $\varphi(x) \neq 0_{\mathbb{Z}/\langle z\rangle}$ für ein $x \in \mathbb{Z}/\langle 12\rangle$, so wäre $\operatorname{im}\varphi$ eine Untergruppe von $\mathbb{Z}/\langle 7\rangle$ mit mindestens 2 Elementen. Der Satz von Lagrange liefert $\operatorname{im}\varphi = \mathbb{Z}/\langle 7\rangle$. Nach dem Homomorphiesatz folgt

$$(\mathbb{Z}/\langle 12\rangle)/\ker\varphi \cong \operatorname{im}\varphi = \mathbb{Z}/\langle 7\rangle.$$

Erneute Anwendung von dem Satz von Lagrange liefert

$$12 = |\mathbb{Z}/\langle 12\rangle| = |\ker\varphi| \cdot |\operatorname{im}\varphi| = 7|\ker\varphi|.$$

Das ist nicht möglich.

Seien $\varnothing \neq S_1, S_2 \subseteq G$ Teilmengen einer Gruppe G. Dann definieren wir

$$S_1S_2 := \{s_1s_2 \mid s_i \in S_i, i \in \{1,2\}\}.$$

Satz 1.5.5 (Erster Isomorphiesatz[a]). *Es seien G eine Gruppe, $H \subseteq G$ eine Untergruppe und $N \subseteq G$ ein Normalteiler. Dann gilt:*

(1) NH ist eine Untergruppe von G.

(2) $N \cap H$ ist ein Normalteiler von H.

(3) Die Abbildung

$$\varphi\colon H/(N \cap H) \longrightarrow NH/N \; ; \; x(N \cap H) \mapsto xN.$$

ist ein Isomorphismus.

[a] Es gibt auch einen zweiten Isomorphiesatz, dieser ist jedoch für unsere Vorlesung nicht relevant.

Beweis.

(1) Es ist $e \in NH$. Sind $n, n' \in N$ und $h, h' \in H$. Da N ein Normalteiler ist, gilt

$$(nh)(n'h') = (n\underbrace{hn'h^{-1}}_{\in N})hh' \in NH,$$

sowie

$$(nh)^{-1} = h^{-1}n^{-1} = (\underbrace{h^{-1}n^{-1}h}_{\in N})h^{-1} \in NH.$$

(2)+(3) Es ist $N \subseteq NH$ ein Normalteiler der Gruppe NH. Sei $\sigma : H \longrightarrow NH/N$ die Restriktion der kanonischen Projektion $\pi : NH \longrightarrow NH/N$. Wegen

$$nhN = h(\underbrace{h^{-1}nh}_{\in N})N = hN = \sigma(h)$$

für $h \in H$ und $n \in N$ ist σ surjektiv. Ferner gilt $\ker \sigma = \ker \pi \cap H = N \cap H$. Damit liefert Korollar 1.5.3 das Gewünschte. Weiter ist damit $N \cap H = \ker \sigma$ ein Normalteiler von H.

□

Bemerkung 1.5.6. Da N ein Normalteiler von G ist, gilt $Nh = hN$ für alle $h \in H$ und damit $NH = HN$. Ist zusätzlich H ein Normalteiler von G, so ist auch $NH = HN$ ein Normalteiler von G.

1.6 Produkte von Gruppen

Es sei G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler von G und $H \subseteq G$ eine Untergruppe. Wir haben gesehen, dass dann $NH = HN$ eine Untergruppe von G. In diesem Abschnitt beschäftigen wir uns mit der Untersuchung dieser Gruppe und allgemeiner dem endlichen Produkt von Normalteilern. Dazu halten wir zunächst einige Beobachtungen fest.

(1) Es gilt zwar $NH = HN$, das heißt aber nicht, dass $nh = hn$ für alle $n \in N$ und $h \in H$ gilt, selbst wenn N und H abelsch sind (siehe Übung).

(2) Wir haben im Beweis von Satz 1.5.5 gesehen, dass $(n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1})(h_1h_2)$ mit $n_1(h_1n_2h_1^{-1}) \in N$ und $h_1h_2 \in H$ gilt. Im Allgemeinen ist diese Darstellung nicht eindeutig. Mit der Zusatzannahme $N \cap H = \{e\}$ folgt aus $nh = n'h'$ die Gleichung $(n')^{-1}n' = h'h^{-1} \in N \cap H = \{e\}$. Das heißt $n = n'$ und $h = h'$ und die Darstellung ist eindeutig.

(3) Sind N und H endlich, so ist NH endlich und nach Satz 1.5.5 gilt

$$H/(N \cap H) \cong NH/N.$$

Mit dem Satz von Lagrange folgt $|NH| = \frac{|N||H|}{|N \cap H|}$. Die Gruppe NH ist also genau dann von Ordnung $|N||H|$, wenn $N \cap H = \{e\}$ gilt.

Definition. Es sei G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler und $H \subseteq G$ eine Untergruppe. Wir sagen, dass G das **semidirekte Produkt** von N und H ist, falls

(1) $NH = G$, und

(2) $N \cap U = \{e\}$ gilt.

In diesem Fall schreiben wir $G = N \rtimes H$[7].

Beispiele. (1) Sei $n \geq 3$. Wir betrachten den surjektiven Homomorphismus $\operatorname{sgn}\colon \mathcal{S}_n \longrightarrow (\{\pm 1\}, \cdot)$. Der Satz von Lagrange zusammen mit Korollar 1.5.3 liefert $|\mathcal{A}_n| = |\ker \operatorname{sgn}| = \frac{|\mathcal{S}_n|}{|\{\pm 1\}|} = \frac{n!}{2}$. Es sei $\tau \in \mathcal{S}_n$ die Abbildung die nur 1 und 2 vertauscht, dann gilt $\langle \tau \rangle \cap \mathcal{A}_n = \{\mathrm{id}\}$ und Beobachtung (3) zeigt $|\mathcal{A}_n\langle \tau \rangle| = |\mathcal{A}_n| \cdot |\langle \tau \rangle| = n! = |\mathcal{S}_n|$, also $\mathcal{A}_n \rtimes \langle \tau \rangle$.

(2) Es sei $n \in \mathbb{N}$. Wir betrachten den Vektorraum $\mathbb{R}^n$ zusammen mit dem Standardskalarprodukt $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$. In der linearen Algebra betrachtet man die Gruppe der Isometrien

$$\mathrm{Iso}(\mathbb{R}^n) = \{f\colon \mathbb{R}^n \longrightarrow \mathbb{R}^n \mid \forall\, x, y \in \mathbb{R}^n\colon ||\varphi(x) - \varphi(y)|| = ||x - y||\}.$$

Diese enthält die Untergruppe der orthogonalen Abbildungen

$$O(\mathbb{R}^n) = \mathrm{Iso}(\mathbb{R}^n) \cap \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R}^n)$$

und die Gruppe der Translationen

$$T(\mathbb{R}^n) = \{\tau_a \mid a \in \mathbb{R}^n\},$$

wobei $\tau_a\colon \mathbb{R}^n \longrightarrow \mathbb{R}^n; x \mapsto a + x$. Es gilt $\mathrm{Iso}(\mathbb{R}^n) = T(\mathbb{R}^n) \rtimes O(\mathbb{R}^n)$ (vergleiche [5, (9.7.9)]).

Eine besonders einfache Beschreibung der Untergruppe $NH \subseteq G$ ergibt sich, wenn $N \cap H = \{e\}$ gilt und sowohl N als auch H Normalteiler sind. Wir diskutieren im Folgenden direkt den verallgemeinerten Fall.

[7] Das Zeichen $\rtimes$ deutet an, dass N in G normal ist. Da $HN = NH = G$ gilt, wird das semidirekte Produkt auch manchmal als $H \ltimes N = G$ notiert.

Definition. Es seien $G_1, \dots, G_n$ Gruppen (nicht zwangsweise Untergruppen einer gemeinsamen Gruppe), dann erhält das kartesische Produkt $\prod_{i=1}^n G_i = G_1 \times G_2 \times \cdots \times G_n$ die Struktur einer Gruppe durch

$$(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) := (x_1 y_1, \dots, x_n y_n).$$

Diese Gruppe nennt man das **(äußere) Produkt** der Gruppen $G_1, \dots, G_n$.[8]

Lemma 1.6.1. *Es sei G eine Gruppe mit Normalteilern $G_1, \dots, G_n \trianglelefteq G$.*

(1) Gilt $G_i \cap G_j = \{e\}$ für alle $i \neq j$, so ist die (surjektive) Abbildung

$$\varphi\colon \prod_{i=1}^n G_i \longrightarrow G_1 G_2 \cdots G_n; (g_1, \dots, g_n) \mapsto g_1 g_2 \cdots g_n$$

ein Homomorphismus.

(2) Gilt

$$G_j \cap (G_1 \cdots G_{j-1} G_{j+1} \cdots G_n) = \{e\} \text{ für alle } j \in \{1, \dots, n\},$$

so ist φ ein Isomorphismus.

Beweis. Als Produkt von Normalteilern ist $G_1 G_2$ ein Normalteiler von G (Übung). Induktiv, folgt dass $G_1 G_2 \cdots G_n$ ein Normalteiler von G ist.

(1) Es seien $i \neq j \in \{1, \dots, n\}$ und $x \in G_i$, $y \in G_j$. Dann gilt aufgrund der Normalität beider Gruppen $xyx^{-1} \in G_j$ und $yx^{-1}y^{-1} \in G_i$. Wir erhalten

$$xyx^{-1}y^{-1} = x(\underbrace{yx^{-1}y^{-1}}_{\in G_i}) = (\underbrace{xyx^{-1}}_{\in G_j})y^{-1} \in G_i \cap G_j = \{e\},$$

das heißt

$$(*) \quad xy = yx.$$

Nach Definition von φ und $G_1 G_2 \cdots G_n$ ist φ surjektiv. Es gilt für alle $(g_1, \dots, g_n), (h_1, \dots, h_n) \in \prod_{i=1}^n G_i$:

$$\begin{aligned}\varphi((g_1, \dots, g_n)(h_1, \dots, h_n)) &= \varphi(g_1 h_1, \dots, g_n h_n) = (g_1 h_1)(g_2 h_2) \cdots (g_n h_n) \\ &\overset{(*)}{=} (g_1 g_2 \cdots g_n)(h_1 h_2 \cdots h_n) = \varphi(g_1, \dots, g_n)\varphi(h_1, \dots, h_n).\end{aligned}$$

Also ist φ ein Gruppenhomomorphismus.

(2) Es seien $i \neq j \in \{1, \dots, n\}$. Nach Voraussetzung gilt $G_j \cap G_i \subseteq G_j \cap (G_1 \cdots G_{j-1} G_{j+1} \cdots G_n) = \{e\}$. Damit ist (1) anwendbar. Es sei $x = (g_1, \dots, g_n) \in \ker \varphi$. Dann gilt für $j \in \{1, \dots, n\}$

$$\begin{aligned}g_j^{-1} = g_j^{-1}\varphi(x) = g_j^{-1}(g_1 g_2 \cdots g_n) &\overset{(*)}{=} g_j^{-1}(g_j \cdot g_1 \cdots g_{j-1} g_{j+1} \cdots g_n) \\ &= g_1 \cdots g_{j-1} g_{j+1} \cdots g_n \in G_j \cap (G_1 \cdots G_{j-1} G_{j+1} \cdots G_n) = \{e\}.\end{aligned}$$

Es folgt $x = e_{\prod_{i=1}^n G_i}$ und damit $\ker \varphi = \{e_{\prod_{i=1}^n G_i}\}$. Also ist φ ein Gruppenisomorphismus.

[8] Bemerke, dass für $j \in \{1, \dots, n\}$ die Menge

$$N_j := \{e_{G_1}\} \times \cdots \times \{e_{G_{j-1}}\} \times G_j \times \{e_{G_{j+1}}\} \times \cdots \times \{e_{G_n}\}$$

ein Normalteiler von $G := \prod_{i=1}^n G_i$ ist und $G = N_1 N_2 \cdots N_n$ sowie $N_j \cap (N_1 \cdots N_{j-1} N_{j+1} \cdots N_n) = \{e_G\}$ gilt.

□

Korollar 1.6.2. *Es sei G eine Gruppe, $n \in \mathbb{N}_{\geq 2}$ und $N_1, N_2, \ldots, N_n \trianglelefteq G$ endliche Normalteiler mit $\mathrm{ggT}(|N_i|, |N_j|) = 1$ für $i \neq j$. Dann gilt $N_1 N_2 \cdots N_n \cong \prod_{i=1}^{n} N_i$.*

Beweis. Es seien $i \neq j \in \{1, \ldots, n\}$. Dann ist $N_i \cap N_j$ eine Untergruppe von N_i und N_j. Der Satz von Lagrange zusammen mit der Voraussetzung liefert $N_i \cap N_j = \{e\}$. Nach Lemma 1.6.1 ist die Abbildung

$$\varphi\colon \prod_{i=1}^{n} N_i \longrightarrow N_1 N_2 \cdots N_n; (x_1, \ldots, x_n) \mapsto x_1 x_2 \cdots x_n$$

ein surjektiver Gruppenhomomorphismus. Es sei $j \in \{1, \ldots, n\}$ und $U := N_1 \times N_2 \times \cdots \times N_{j-1} \times \{e\} \times N_{j+1} \times \cdots \times N_n$. Dann gilt $\varphi(U) = N_1 \cdots N_{j-1} N_{j+1} \cdots N_n$. Nach dem Homomorpiesatz gilt damit

$$|N_1 \cdots N_{j-1} N_{j+1} \cdots N_n| = |\operatorname{im} \varphi|_U| = \frac{|U|}{|\ker \varphi|_U|},$$

also ist $|N_1 \cdots N_{j-1} N_{j+1} \cdots N_n|$ ein Teiler von $|U| = \prod_{i \neq j}^{n} |N_i|$. Damit sind

$$|N_j| \text{ und } |N_1 \cdots N_{j-1} N_{j+1} \cdots N_n|$$

teilerfremd nach Voraussetzung und der Satz von Lagrange liefert $N_j \cap (N_1 \cdots N_{j-1} N_{j+1} \cdots N_n) = \{e\}$. Nun wenden wir Lemma 1.6.1 an. □

1.7 Operationen von Gruppen und die Klassengleichung

Definition. Sei G eine Gruppe, $X \neq \varnothing$ eine Menge. Eine Abbildung

$$G \times X \longrightarrow X \;;\; (g, x) \mapsto g.x$$

heißt **Operation von G auf X**, falls gilt:

(1) $g.(h.x) = (gh).x$ für alle $g, h \in G, x \in X$,

(2) $e.x = x$ für alle $x \in X$.

In diesem Fall nennen wir X eine **G-Menge**.

Beispiele. (1) Die Gruppe $\mathcal{S}_n$ operiert auf der Menge $X := \{1, \ldots, n\}$ durch Anwendung, das heißt

$$\sigma.i := \sigma(i) \quad \text{für alle } \sigma \in \mathcal{S}_n, i \in X.$$

(2) Sei G eine Gruppe. Dann wird durch

$$g.x := gx \quad \text{für alle } g, x \in G$$

eine Operation von G auf G definiert (**Operation durch Linksmultiplikation**).

(3) Sei G eine Gruppe. Dann wird durch

$$g.x := gxg^{-1} \text{ für alle } g, x \in G$$

eine Operation von G auf G definiert. (**Operation durch Konjugation**)

Lemma 1.7.1. *Sei G eine Gruppe, $X \neq \varnothing$ eine Menge.*

(1) Ist $G \times X \longrightarrow X\ ;\ (g,x) \mapsto g.x$ eine Operation von G auf X, so ist $\varphi : G \longrightarrow \mathcal{S}_X\ ;\ \varphi(g)(x) := g.x$ ein Homomorphismus.

(2) Ist $\varphi : G \longrightarrow \mathcal{S}_X$ ein Homomorphismus, so definiert

$$G \times X \longrightarrow X\ \ ;\ \ (g,x) \mapsto g.x := \varphi(g)(x)$$

eine Gruppenoperation.

Beweis.

(1) Für jedes $g \in G$ ist

$$\varphi(g) : X \longrightarrow X; x \mapsto g.x$$

eine Abbildung. Es ist $\varphi(e) = \mathrm{id}_X$. Weiter gilt für alle $g, h \in G, x \in X$:

$$(*) \quad \varphi(gh)(x) = (gh).x = g.(h.x) = [\varphi(g) \circ \varphi(h)](x).$$

Insbesondere folgt $\varphi(g) \circ \varphi(g^{-1}) = \varphi(e) = \mathrm{id}_X = \varphi(e) = \varphi(g^{-1}) \circ \varphi(g)$. Damit erhalten wir $\varphi(g) \in \mathcal{S}_X$ für jedes $g \in G$. Zudem zeigt $(*)$, dass φ ein Homomorphismus ist.

(2) Analog.

□

Bemerkung 1.7.2. Der vorherige Satz ist eine Verallgemeinerung des Satzes von Cayley: Betrachten wir die Operation von G auf G durch Linksmultiplikation, so erhalten wir den Homomorphismus $\varphi\colon G \longrightarrow \mathcal{S}_G$ aus Proposition 1.4.3. Im Allgemeinen muss der Homomorphismus $\varphi\colon G \longrightarrow \mathcal{S}_X$ nicht injektiv sein, wie die Operation einer abelschen Gruppe durch Konjugation auf sich selbst zeigt. In diesem Fall ist $\varphi(g) = \mathrm{id}_G$ für alle $g \in G$, also $\ker \varphi = G$.

Definition. Sei X eine G-Menge, $x \in X$. Dann heißt

$$G.x := \{g.x \mid g \in G\} \subseteq X$$

die **Bahn** von x. Weiter ist

$$G_x := \mathrm{Stab}_G(x) := \{g \in G \mid g.x = x\} \subseteq G$$

eine Untergruppe von G, der **Stabilisator** von x. Man schreibt

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

für die Menge der Bahnen.

Bemerkung 1.7.3. Es sei X eine G-Menge. Wir definieren eine Äquivalenzrelation auf $X \times X$ durch

$$x \sim y :\Leftrightarrow G.x = G.y.$$

Die Äquivalenzklassen sind genau die Mengen $G.x$ mit $x \in X$. Insbesondere gilt für $x, y \in X$ entweder $G.x = G.y$ oder $G.x \cap G.y = \varnothing$. Wir nennen eine Teilmenge $R \subseteq X$ ein **Repräsentantensystem der Bahnen**, falls

$$X = \bigcup_{x \in R} G.x$$

und $G.x \neq G.y$ für alle $x \neq y \in R$ gilt. Wir schreiben dann auch kurz $X = \bigsqcup_{x \in R} G.x$. Nach obiger Überlegung lässt sich stets ein Repräsentantensystem der Bahnen finden.

Als erste Anwendung von Gruppenoperationen geben wir nun einen formalen Beweis für ein Resultat, das bereits in der Linearen Algebra behandelt, aber nicht bewiesen wurde (siehe [5, (3.3.4)]). Sei $n \in \mathbb{N}$ eine Menge, $\sigma \in \mathcal{S}_n$ eine Permutation. Dann heißt

$$\operatorname{supp}(\sigma) := \{i \in \{1, \dots, n\} \mid \sigma(i) \neq i\}$$

der **Träger** von σ. Ist $|\operatorname{supp}(\sigma)| = m \geq 2$ endlich und existiert $a \in \operatorname{supp}(\sigma)$ mit $\operatorname{supp}(\sigma) = \{\sigma^i(a) \mid 0 \leq i \leq m-1\}$, so nennt man σ einen m**-Zykel** und m die **Länge** von σ. Die 2-Zyklen von $\mathcal{S}_n$ werden auch **Transpositionen** genannt. Sind $a_1, \dots, a_m \in \{1, \dots, n\}$ $(m \geq 2)$ paarweise verschiedene Elemente, so bezeichnet $(a_1, \dots, a_m)$ den durch

$$(a_1, \dots, a_m)(a) := \begin{cases} a & \text{, falls } a \notin \{a_1, \dots, a_m\} \\ a_{i+1} & \text{, falls } a = a_i \text{ für ein } 1 \leq i \leq m-1 \\ a_1 & \text{, falls } a = a_m \end{cases}$$

definierten m-Zykel.

Bemerkung 1.7.4. Wir nennen Permutationen $\sigma, \tau \in \mathcal{S}_n$ **disjunkt**, falls $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \varnothing$ gilt. Sind σ und τ disjunkt, so gilt $\sigma \circ \tau = \tau \circ \sigma$ und $\operatorname{supp}(\sigma \circ \tau) = \operatorname{supp}(\sigma) \cup \operatorname{supp}(\tau)$.

Satz 1.7.5. *Sei $n \in \mathbb{N}$.*

(1) Ist $\sigma \neq \mathrm{id} \in \mathcal{S}_n$, so gibt es Zyklen $\sigma_1, \dots, \sigma_\ell$ mit

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_\ell \text{ und } \operatorname{supp}(\sigma) = \bigsqcup_{i=1}^{\ell} \operatorname{supp}(\sigma_i).$$

Diese Darstellung ist bis auf Reihenfolge eindeutig.

(2) Sind $a_1, \dots, a_t \in \{1, \dots, n\}$ paarweise verschieden, so gilt

$$\sigma \circ (a_1, \dots, a_t) \circ \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_t)) \quad \text{für alle } \sigma \in \mathcal{S}_n.$$

(3) Die Gruppe $\mathcal{S}_n$ wird von der Menge $\{(1,2), (1,3), \dots, (1,n)\}$ erzeugt.

Beweis.

(1) Sei $\sigma \neq \mathrm{id} \in \mathcal{S}_n$. Wir definieren die Untergruppe $\{\mathrm{id}, \sigma, \ldots, \sigma^{\mathrm{ord}(\sigma)-1}\} = \langle\sigma\rangle =: U \subseteq \mathcal{S}_n$ und betrachten die Operation (es handelt sich um die Einschränkung der Operation von $\mathcal{S}_n$ auf $\{1, \ldots, n\}$)

$$U \times \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}; (\sigma^j, i) \mapsto \sigma^j(i).$$

Es sei $a \in \{1, \ldots, n\}$. Dann existiert $1 \leq r_a \leq \mathrm{ord}(\sigma)$ minimal mit $\sigma^{r_a}(a) = a$. Damit gilt für die Bahn $U.a$, dass $|U.a| = r_a$ und

$$U.a = \{a, \sigma(a), \ldots, \sigma^{r_a-1}(a)\}.$$

Wir wählen ein Repräsentantensystem $a_1, \ldots, a_m \in \{1, \ldots, n\}$ der Bahnen, d.h. $\{1, \ldots, n\} = \bigsqcup_{i=1}^{m} U.a_i$. Es sei $J := \{j \in \{1, \ldots, m\} \mid |U.a_j| > 1\}$. Es gilt $J \neq \varnothing$, da $\sigma \neq \mathrm{id}$. Nach Umnummerierung können wir $J = \{1, \ldots, \ell\}$ mit $1 \leq \ell \leq m$ annehmen. Es sei $a \in \{1, \ldots, n\}$. Wir finden ein eindeutiges Element $j \in \{1, \ldots, m\}$ mit $a \in U.a_j$ und erhalten $U.a = U.a_j$, also

$$a \notin \mathrm{supp}(\sigma) \Leftrightarrow \sigma(a) = a \Leftrightarrow U.a = \{a\} \Leftrightarrow U.a_j = \{a\} \Leftrightarrow U.a_j = \{a_j\} \Leftrightarrow |U.a_j| = 1 \Leftrightarrow j \notin J.$$

Das heißt $\mathrm{supp}(\sigma) = \bigcup_{j=1}^{\ell} \mathrm{supp}(\sigma_j) = \bigcup_{j=1}^{\ell} U.a_j$. Für $j \in J$ definieren wir

$$\sigma_j := (a_j, \sigma(a_j), \sigma^2(a_j), \ldots, \sigma^{r_{a_j}-1}(a_j)) \in \mathcal{S}_n.$$

Nach Konstruktion gilt $\mathrm{supp}(\sigma_j) = U.a_j$. Es sei $\tau = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_\ell$. Nach Bemerkung 1.7.4 spielt die Reihenfolge keine Rolle und es gilt

$$\mathrm{supp}(\tau) = \bigcup_{j=1}^{\ell} \mathrm{supp}(\sigma_j) = \bigcup_{j=1}^{\ell} U.a_j = \mathrm{supp}(\sigma).$$

Ist $a \in \mathrm{supp}(\sigma)$, so gibt es also genau ein $j \in J$ mit $a \in \mathrm{supp}(\sigma_j) = U.a_j$. Nach Definition von σ_j gilt $\sigma_j(a) = \sigma(a)$. Weiter gilt $\sigma_i(a) = a$ für $i \in J \setminus \{j\}$ und wir erhalten

$$\tau(a) = [\sigma_j \circ \prod_{i \in J \setminus \{j\}} \sigma_i](a) = \sigma_j(a) = \sigma(a).$$

Wegen $\mathrm{supp}(\tau) = \mathrm{supp}(\sigma)$ impliziert dies $\sigma = \tau$.

Ist nun $\sigma = \tau_1 \circ \cdots \circ \tau_k$ eine weitere derartige Zerlegung, so ist $\{\mathrm{supp}(\tau_i) \mid i \in \{1, \ldots, k\}\}$ die Menge der Bahnen in $\{1, \ldots, n\}/U$ mit mindestens 2 Elementen. Insbesondere gilt $k = \ell$ und es existiert eine Bijektion $f\colon \{1, \ldots, \ell\} \longrightarrow \{1, \ldots, k\}$ mit $\mathrm{supp}(\sigma_i) = \mathrm{supp}(\tau_{f(i)})$ für alle $i \in \{1, \ldots, \ell\}$. Sei $i \in \{1, \ldots, \ell\}$ und $a \in \mathrm{supp}(\sigma_i) = \mathrm{supp}(\tau_{f(i)})$. Dann gilt

$$\sigma_i \circ (\sigma_1 \circ \cdots \circ \sigma_{i-1} \circ \sigma_{i+1} \circ \cdots \circ \sigma_\ell) = \sigma = \tau_{f(i)} \circ (\tau_1 \circ \cdots \circ \tau_{f(i)-1} \circ \tau_{f(i)+1} \circ \cdots \circ \tau_\ell)$$

und damit

$$\sigma_i(a) = \sigma_i((\sigma_1 \circ \cdots \circ \sigma_{i-1} \circ \sigma_{i+1} \circ \cdots \circ \sigma_\ell)(a)) = \tau_{f(i)}((\tau_1 \circ \cdots \circ \tau_{f(i)-1} \circ \tau_{f(i)+1} \circ \cdots \circ \tau_\ell)(a)) = \tau_{f(i)}(a).$$

Trivialerweise gilt $\sigma_i(b) = \tau_{f(i)}(b)$ für alle $b \notin \mathrm{supp}(\sigma_i) = \mathrm{supp}(\tau_{f(i)})$ und damit $\sigma_i = \tau_{f(i)}$. Dies liefert die Eindeutigkeit der Zerlegung.

(2) Sei $x \in \operatorname{supp}(\sigma \circ (a_1, \ldots, a_t) \circ \sigma^{-1})$. Dann gilt $[\sigma \circ (a_1, \ldots, a_t) \circ \sigma^{-1}](x) \neq x$ und somit

$$[(a_1, \ldots, a_t) \circ \sigma^{-1}](x) \neq \sigma^{-1}(x).$$

Dies bedeutet $\sigma^{-1}(x) \in \{a_1, \ldots, a_t\}$ und $x \in \sigma(\{a_1, \ldots, a_t\})$. Wir erhalten damit $\operatorname{supp}(\sigma \circ (a_1, \ldots, a_t) \circ \sigma^{-1}) = \{\sigma(a_1), \ldots, \sigma(a_t)\}$ sowie

$$[\sigma \circ (a_1, \ldots, a_t) \circ \sigma^{-1}](\sigma(a_j)) = \begin{cases} \sigma(a_{j+1}) & \text{, falls } j < t \\ \sigma(a_1) & \text{, falls } j = t. \end{cases}$$

Dies bedeutet $\sigma \circ (a_1, \ldots, a_t) \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_t))$.

(3) Die Behauptung ist klar für $n = 2$. Sei daher $n \geq 3$. Es sei $T \subseteq \mathcal{S}_n$ die Menge der Transpositionen. Ist $(a_1, \ldots, a_t)$ ein t-Zykel, so gilt für $t \geq 3$

$$(a_1, \ldots, a_t) = (a_1, \ldots a_{t-1}) \circ (a_{t-1}, a_t).$$

Induktion nach t liefert $(a_1, \ldots, a_t) \in \langle T \rangle$ und (1) impliziert damit $\mathcal{S}_n = \langle T \rangle$.

Seien nun $1 < i < j \in \{1, \ldots, n\}$. Aus (2) folgt

$$(1, i) \circ (1, j) \circ (1, i) = (i, j),$$

und somit $T \subseteq \langle \{(1, i) \mid i \in \{2, \ldots, n\}\} \rangle$. Mithin haben wir $\mathcal{S}_n = \langle \{(1, i) \mid i \in \{2, \ldots, n\}\} \rangle$.

□

Beispiele.

(1) Es gilt $\mathcal{S}_9 \ni (1, 2, 3, 4)(4, 5, 1, 3)(7, 5, 8)(1, 2) = (1, 3)(2, 4, 5, 8, 7)(6)(9) = (1, 3)(2, 4, 5, 8, 7)$[9].

(2) Es gilt für $i \neq j$ ungleich 1 die Gleichung $(1, i)(1, j)(1, i) = (i, j)$ und damit

$$\begin{aligned}(1, 2, 4, 5, 8, 7) &= (1, 2)(2, 4)(4, 5)(5, 8)(8, 7) \\ &= (1, 2)[(1, 2)(1, 4)(1, 2)][(1, 4)(1, 5)(1, 4)][(1, 5)(1, 8)(1, 5)][(1, 8)(1, 7)(1, 8)].\end{aligned}$$

(3) Nach Satz 1.7.5(2) sind je zwei Zyklen gleicher Länge zueinander konjugiert.

Lemma 1.7.6 (Bahnformel). *Sei X eine G-Menge und $x \in X$.*

(1) Die Abbildung

$$\varphi : \begin{cases} G/G_x & \longrightarrow & G.x \\ gG_x & \mapsto & g.x \end{cases}$$

ist bijektiv.

(2) Ist G endlich, so ist $|G.x|$ ein Teiler der Gruppenordnung und es gilt $|G| = |G.x| \cdot |G_x|$.

Beweis.

[9] Wir verzichten ab jetzt auf das Symbol $\circ$ für die Komposition.

(1) Wir zeigen zunächst, dass φ wohldefiniert ist. Seien $g, h \in G$ mit $gG_x = hG_x$. Dann gilt $g^{-1}h \in G_x$ und somit $(g^{-1}h).x = x$. Also folgt

$$g.x = g.[(g^{-1}h).x] = (g(g^{-1}h)).x = h.x.$$

Seien nun $g, h \in G$ mit $\varphi(gG_x) = \varphi(hG_x)$ gegeben. Dann gilt $g.x = h.x$ und daher

$$(g^{-1}h).x = g^{-1}.(h.x) = g^{-1}.(g.x) = (g^{-1}g).x = e.x = x.$$

Damit haben wir $g^{-1}h \in G_x$ und somit $gG_x = hG_x$. Die Abbildung φ ist also injektiv.

Die Surjektivität von φ folgt unmittelbar aus der Definition.

(2) Dies folgt unmittelbar aus (1) und dem Satz von Lagrange.

□

Beispiele. (1) Die wichtige Erkenntnis aus der Bahnformel ist, dass für eine endliche Gruppe G die Mächtigkeit der Bahn $G.x \subseteq X$ ein Teiler der Gruppenordnung ist. Operiert also eine Gruppe der Ordnung 49 auf einer Menge der Ordnung 40, so gilt entweder $|G.x| = 1$ (das heißt $g.x = x$ für alle $g \in G$) oder $|G.x| = 7$, da auch $|G.x| \leq |X| = 40$ gilt.

(2) Die Gruppe $\mathcal{S}_n$ operiert auf $\{1, \ldots, n\}$ durch Anwendung. Wir berechnen die Bahn $\mathcal{S}_n.n$ von n. Mit $(1, n), (2, n), \ldots, (n-1, n), \mathrm{id} \in \mathcal{S}_n$ gilt $\{1, \ldots, n\} \subseteq \mathcal{S}_n.n \subseteq \{1, \ldots, n\}$. Damit gilt $\mathcal{S}_n.n = \{1, \ldots, n\}$ und die Bahnformel liefert

$$|\operatorname{Stab}_{\mathcal{S}_n}(n)| = |(\mathcal{S}_n)_n| = \frac{|\mathcal{S}_n|}{|\mathcal{S}_n.n|} = \frac{|\mathcal{S}_n|}{|\{1, \ldots, n\}|} = \frac{n!}{n} = (n-1)!.$$

Es sei $\sigma \in \operatorname{Stab}_{\mathcal{S}_n}(n)$. Dann ist $\sigma(n) = n$ und damit $\sigma(i) \in \{1, \ldots, n-1\}$ für alle $i \neq n$. Das heißt die Restriktion der Operation liefert eine Operation

$$\operatorname{Stab}_{\mathcal{S}_n}(n) \times \{1, \ldots, n-1\} \longrightarrow \{1, \ldots, n-1\}; (\sigma, i) \mapsto \varphi(\sigma)(i) = \sigma(i).$$

Nach Lemma 1.7.1 erhalten wir einen Gruppenhomomorphismus

$$\varphi\colon \operatorname{Stab}_{\mathcal{S}_n}(n) \longrightarrow \mathcal{S}_{n-1}; \sigma \mapsto \sigma.i = \sigma(i).$$

Ist $\sigma \in \ker \varphi$, so gilt $\sigma(i) = i$ für alle $i \in \{1, \ldots, n-1\}$ und $\sigma(n) = n$ zeigt $\sigma = \mathrm{id}_{\{1,\ldots,n\}}$. Damit ist φ injektiv. Da $|\operatorname{Stab}_{\mathcal{S}_n}(n)| = (n-1)! = |\mathcal{S}_{n-1}|$ gilt, ist φ ein Isomorphismus, also $\operatorname{Stab}_{\mathcal{S}_n}(n) \cong \mathcal{S}_{n-1}$.

(3) Wir verallgemeinern das vorherige Beispiel. Es sei $k \in \mathbb{N}$ mit $1 \leq k \leq n$. Die Gruppe $\mathcal{S}_n$ operiert in natürlicher Weise auf der Menge

$$X := \{T \subseteq \{1, \ldots, n\} \mid |T| = k\}$$

der k-elementigen Mengen von $\{1, \ldots, n\}$ durch $\sigma.T := \sigma(T) = \{\sigma(t) \mid t \in T\}$. Wir betrachten die Teilmenge $S := \{1, \ldots, k\} \in X$. Ist $T = \{t_1, \ldots, t_k\} \in X$ ein weiteres Element, so finden wir $\sigma \in \mathcal{S}_n$ mit $\sigma.S = T$. Das heißt $X = \mathcal{S}_n.S$. Es ist $\operatorname{Stab}_{\mathcal{S}_n}(S) = \{\sigma \in \mathcal{S}_n \mid \sigma(S) = S\}$ und die Abbildung

$$\varphi\colon \mathcal{S}_k \times \mathcal{S}_{\{k+1,\ldots,n\}} \longrightarrow \operatorname{Stab}_{\mathcal{S}_n}(S); (\sigma, \tau) \mapsto \varphi(\sigma, \tau)(i) = \begin{cases} \sigma(i) & \text{, falls } 1 \leq i \leq k \\ \tau(i) & \text{, falls } k+1 \leq i \leq n \end{cases}$$

ist eine Bijektion. Wir schließen mit der Bahnformel und dem Satz von Lagrange

$$|X| = |\mathfrak{S}_n.S| = |\mathfrak{S}_n/\operatorname{Stab}_{\mathfrak{S}_n}(S)| = \frac{|\mathfrak{S}_n|}{|\operatorname{Stab}_{\mathfrak{S}_n}(S)|} = \frac{|\mathfrak{S}_n|}{|\mathfrak{S}_k \times \mathfrak{S}_{\{k+1,\dots,n\}}|} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Definition. Sei X eine G-Menge. Dann heißt

$$X^G := \{x \in X \mid \forall\, g \in G\colon g.x = x\}$$

die Menge der **Fixpunkte** von X.

Satz 1.7.7. *Sei X eine endliche G-Menge. Dann gilt*

$$|X| = |X^G| + \sum_{G.x \in X/G, |G.x| \neq 1} [G : G_x].$$

Beweis. Wegen $x \in G.x$ gilt

$$x \in X^G \Leftrightarrow G.x = \{x\} \Leftrightarrow |G.x| = 1.$$

Mit $X = \bigsqcup_{G.x \in X/G} G.x$ folgt also

$$X^G = \bigsqcup_{G.x \in X/G, |G.x| = 1} G.x$$

und Lemma 1.7.6 impliziert

$$|X| = |X^G| + \sum_{G.x \in X/G, |G.x| \neq 1} |G.x| = |X^G| + \sum_{G.x \in X/G, |G.x| \neq 1} [G : G_x],$$

wie behauptet. □

Definition. Operiert G auf G durch Konjugation so heißt $Z_G(x) := G_x = \{g \in G \mid gx = xg\}$ der **Zentralistor** von x in G. Ferner nennt man $Z(G) := G^G = \{x \in G \mid \forall\, g \in G\colon gx = xg\}$ das **Zentrum** von G.

Eine unmittelbare Folgerung aus Satz 1.7.7 ist die sogenannte Klassengleichung:

Korollar 1.7.8 (Klassengleichung)**.** *Sei G eine endliche Gruppe. Dann gilt*

$$|G| = |Z(G)| + \sum_{|G.x| \neq 1} [G : Z_G(x)].$$

Beispiel (A Necklace Problem)**.** Es seien $n, m \in \mathbb{N}$. Wir färben die Zellen eines farblosen Glücksrads R mit m Zellen ein (siehe Figur 1.2). Dazu stehen uns n verschiedene Farben zur Verfügung.

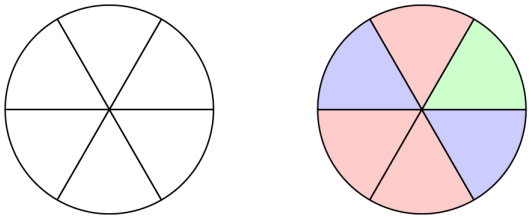


Abbildung 1.2: Farbloses Glücksrad R mit $m = 6$ Zellen und eine mögliche Färbung.

Im Folgenden untersuchen wir die Frage, wie viele bunte Glücksräder wir auf diese Weise erhalten.
Zwei Einfärbungen von R ergeben dasselbe farbige Glücksrad, genau dann, wenn sich eine Färbung durch Drehung aus der anderen Färbung um ein Vielfaches von $\frac{360}{m}^\circ$ ergibt (siehe Figur 1.3).

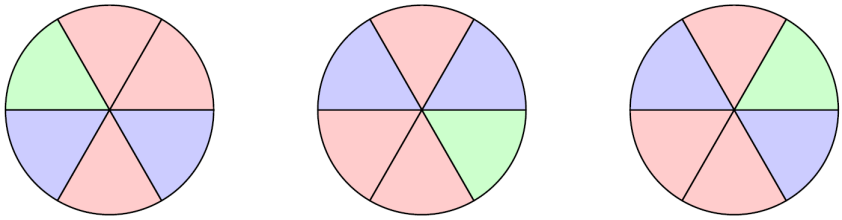


Abbildung 1.3: Drei verschiedene Einfärbungen von R. Nur die ersten beiden Einfärbungen beschreiben dasselbe bunte Glücksrad.

Wir formulieren diese Fragestellung algebraisch. Dazu nehmen wir an, dass R in $\mathbb{R}^2$ um den Nullpunkt zentriert ist. Es sei G die n-elementige Drehgruppe die von der Drehung σ im $\mathbb{R}^2$ um $\frac{360}{m}^\circ$ erzeugt ist. Wir bezeichnen mit X die Menge der möglichen Färbungen von R. Die Gruppe G wirkt in natürlicher Weise auf X und die Anzahl der Bahnen ist genau die Anzahl der verschiedenen bunten Glücksräder, die wir erhalten können. Wir sind also an der Mächtigkeit von X/G interessiert. Wir wollen die Zahl im Spezialfall $m = p \in \mathbb{P}$ Primzahl.

Zunächst gilt $|X| = n^p$, da wir bei jeder Zelle die Wahl zwischen n Farben haben. Sei $x \in X^G$ ein Fixpunkt. Dann gilt insbesondere $\sigma.x = x$. Damit haben je zwei benachbarte Zellen von x dieselbe Farbe. Damit sind die Fixpunkte genau die einfarbig gefärbten Glücksräder und somit gilt $|X^G| = n$. Sei nun $G.x \in X/G$ mit $|G.x| \neq 1$. Dann ist $1 \neq |G.x| = |G/G_x| = [G : G_x]$ ein Teiler der Gruppenordnung $|G| = p$ und somit $[G : G_x] = p$. Wir schließen mit Satz 1.7.7

$$n^p = |X| = |X^G| + \sum_{G.x \in X/G; |G.x| \neq 1} [G : G_x] = |X^G| + (|X/G| - |X^G|)p = n + (|X/G| - n)p$$

und somit

$$|X/G| = \frac{n^p + np - n}{p}.$$

Dieses Beispiel zeigt, dass sich bei Gruppenoperationen einige Untersuchungen vereinfachen können, wenn G eine Gruppe von Primzahlordnung ist. Im nächsten Abschnitt widmen wir uns dem systematischen Studium von Gruppen deren Ordnung eine Primzahlpotenz ist.

2 Strukturtheorie endlicher Gruppen

2.1 p-Gruppen

Definition. Sei p eine Primzahl. Eine endliche Gruppe G heißt **p-Gruppe**, falls es ein $n \in \mathbb{N}_0$ mit $|G| = p^n$ existiert.

Korollar 2.1.1. *Sei p eine Primzahl und $G \neq \{e\}$ eine p-Gruppe.*

(1) Dann gilt $Z(G) \neq \{e\}$.

(2) Gilt $|G| = p^2$, so ist G abelsch.

Beweis.

(1) Wir betrachten die Operation von G auf G durch Konjugation. Es sei $x \in G$ mit $|G.x| \neq 1$. Da $[G : Z_G(x)] = |G.x| \neq 1$ ein Teiler der Gruppenordnung p^n ist, gilt $[G : Z_G(x)] \equiv 0 \bmod(p)$[1]. Wir schließen mit der Klassengleichung

$$|Z(G)| \equiv |Z(G)| + \sum_{|G.x| \neq 1} [G : Z_G(x)] = |G| = p^n \equiv 0 \bmod(p).$$

Mit $e \in Z(G)$ und $p \mid |Z(G)|$ folgt $Z(G) \neq \{e\}$.

(2) Nach (1) und dem Satz von Lagrange ist $|Z(G)| \in \{p, p^2\}$. In den Übungsserien (Aufgabe 14) wurde gezeigt, dass $G/Z(G)$ nicht zyklisch ist. Da Gruppen von Primzahlordnung zyklisch sind, folgt $|G/Z(G)| \neq p$ und damit $|Z(G)| = p^2$, d.h. $Z(G) = G$.

□

Auf analogem Weg, lässt sich das folgende Resultat beweisen.[2]

Lemma 2.1.2. *Es sei G eine p-Gruppe. Ist X eine endliche G-Menge, so gilt*

$$|X| \equiv |X^G| \mod(p).$$

Beweis. Nach 1.7.7 gilt

$$(*) \quad |X| = |X^G| + \sum_{|G.x| \neq 1} [G : G_x].$$

Wegen 1.7.1 erhalten wir $|G.x| = [G : G_x]$ und nach Voraussetzung damit $p|[G : G_x]$ für $|G.x| \neq 1$. Nun liefert $(*)$ die Behauptung. □

[1] Wir schreiben $m \equiv n \bmod(\ell)$ für $m, n, \ell \in \mathbb{Z}$, $\ell \neq 0$, falls $\ell \mid (m - n)$, das heißt bei Division mit Rest durch ℓ besitzen m und n denselben Rest.

[2] Korollar 2.1.1 lässt sich auch aus Lemma 2.1.2 herleiten, da G auf $G \setminus \{e\}$ durch Konjugation operiert.

2.2 Die Sätze von Sylow

Ist G eine endliche Gruppe, so wissen wir nach dem Satz von Lagrange, dass für jede Untergruppe U von G die Ordnung $|U|$ ein Teiler von $|G|$ ist. Es ist daher natürlich folgende Fragestellungen zu untersuchen:

- Existiert für einen Teiler ℓ von $|G|$ stets eine Untergruppe der Ordnung ℓ?
- Sind gegebene Untergruppen derselben Ordnung isomorph (also strukturgleich)?

Beispiele. (1) Wir definieren $V_4 := \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \subseteq \mathcal{S}_4$. Direktes Nachrechnen zeigt, dass V_4 eine Untergruppe von $\mathcal{S}_4$ ist. Weiter besitzt jedes Element $\sigma \in V_4 \setminus \{\mathrm{id}\}$ Ordnung 2. Damit ist V_4 nicht zyklisch. Die Gruppe $\langle (1,2,3,4) \rangle \subseteq \mathcal{S}_4$ hingegen ist zyklisch und von Ordnung 4. Damit enthält die $\mathcal{S}_4$ mindestens zwei Untergruppen der Ordnung 4, die nicht isomorph sind.

(2) Angenommen die alternierende Gruppe $\mathcal{A}_4 \trianglelefteq \mathcal{S}_4$ von Ordnung 12 enthält eine Untergruppe $U \subseteq \mathcal{A}_4$ von Ordnung 6. Da $\mathcal{A}_4$ alle acht 3-Zyklen der $\mathcal{S}_4$ enthält, gibt es mindestens einen 3-Zykel in $\sigma \in \mathcal{A}_4 \setminus U$. Es gilt $|\langle \sigma \rangle| = 3$ und $U \cap \langle \sigma \rangle = \{\mathrm{id}\}$ nach dem Satz von Lagrange. Wir betrachten die Abbildung

$$\varphi \colon U \times \langle \sigma \rangle \longrightarrow \mathcal{A}_4; (x, y) \mapsto xy.$$

Gilt $\varphi(x_1, y_1) = \varphi(x_2, y_2)$, so folgt $x_1 y_1 = x_2 y_2$, also $x_2^{-1} x_1 = y_2 y_1^{-1} \in U \cap \langle \sigma \rangle = \{\mathrm{id}\}$. Das heißt $x_1 = x_2$ und $y_1 = y_2$. Damit ist φ injektiv. Dies ist ein Widerspruch, da $|U \times \langle \sigma \rangle| = 6 \cdot 3 > 12 = |\mathcal{A}_4|$.

(3) Ist G zyklisch und $d \mid |G|$ ein Teiler der Gruppenordnung, so existiert nach Satz 1.3.2 eine Untergruppe der Ordnung d.

Definition. Sei G eine endliche Gruppe.

(1) Sei $p \in \mathbb{N}$ eine Primzahl mit $|G| = p^m q$ und $p \nmid q$. Eine p-Untergruppe $S \subseteq G$ heißt **Sylow p-Untergruppe**, falls $|S| = p^m$ gilt.

(2) Es sei mit $\mathrm{Syl}_p(G)$ die Menge der Sylow p-Untergruppen von G bezeichnet.

Beispiel. Es sei G eine Gruppe der Ordnung $360 = 2^3 \cdot 3^2 \cdot 5$. Eine Untergruppe U von G ist eine Sylow 2-Untergruppe falls $|U| = 2^3 = 8$ gilt.

Satz 2.2.1 (Die Sylowschen Sätze[a]). *Sei G eine endliche Gruppe, $p \in \mathbb{N}$ eine Primzahl mit $|G| = p^m q$ und $p \nmid q$. Dann gilt:*

(1) Für jedes $n \in \{1, \ldots, m\}$ gibt es eine Untergruppe $H \subseteq G$ mit $|H| = p^n$.

(2) Ist $H \subseteq G$ eine p-Untergruppe und $S \subseteq G$ eine Sylow p-Untergruppe, so gibt es $g \in G$ mit $gHg^{-1} \subseteq S$ ($\Leftrightarrow H \subseteq g^{-1}Sg$). Insbesondere ist H in einer Sylow p-Untergruppe enthalten.

[a] Es gibt einen weiteren Satz von Sylow der Aussagen über $|\mathrm{Syl}_p(G)|$ macht.

Beweis.

(1) Für $m = 0$ ist nichts zu zeigen; wir nehmen daher $m \in \mathbb{N}$ an. Sei $1 \leq n \leq m$ und $\ell := m - n \in \mathbb{N}_0$. Wir betrachten die Menge

$$X := \{S \subseteq G \mid |S| = p^n\}^3$$

der p^n elementigen Teilmengen von G. Es operiert G auf X durch

$$G \times X \longrightarrow X, (g, S) \mapsto g.S := \{gs \mid s \in S\}.$$

Es sei $\alpha := p^\ell q$. Dann gilt (siehe Aufgabe 5 (die Aussage gilt trivialerweise für $\alpha = 1$.))

$$m_p(|X|) = m_p\left[\binom{|G|}{p^n}\right] = m_p\left[\binom{p^n\alpha}{p^n}\right] \leq m_p(\alpha) = \ell.$$

Insbesondere gilt $p^{\ell+1} \nmid |X|$. Da X die disjunkte Vereinigung seiner Bahnen ist, existiert daher ein $S \in X$ mit $p^{\ell+1} \nmid |G.S|$, d.h. $m_p(|G.S|) \leq \ell$. Wir setzen $U := \mathrm{Stab}_G(S) \subseteq G$ und erhalten eine Operation

$$U \times S \longrightarrow S, (u, s) \mapsto u.s = us.$$

Sei $s \in S$, dann ist die Abbildung $U \longrightarrow U.s, u \mapsto u.s$ eine Bijektion, da $\{s\}, U \subseteq G$. Da S disjunkte Vereinigung der Bahnen ist, existiert $k \in \mathbb{N}$ mit $p^n = |S| = k|U|$. Insbesondere ist $|U|$ ein Teiler von p^n. Andererseits liefert die Bahnformel

$$|G| = |\mathrm{Stab}_G(S)| \cdot |G.S| = |U| \cdot |G.S|$$

und damit $m_p(|U|) = m_p(|G|) - m_p(|G.S|) \geq m - \ell = n$. Insgesamt gilt also $|U| = p^n$.

(2) Sei $H \subseteq G$ eine p-Untergruppe. Nach (1) gibt es eine Sylow p-Untergruppe $S \subseteq G$. Wir betrachten $X := G/S$ sowie die Operation $H \times X \longrightarrow X\ ;\ (h, gS) \mapsto hgS$ (dies ist wohldefiniert). Nun liefert Lemma 2.1.2:

$$|X^H| \equiv |X| = |G/S| = \frac{|G|}{|S|} = q \not\equiv 0 \bmod(p).$$

Das heißt $X^H \neq \varnothing$ und es existiert $g \in G$ mit $hg^{-1}S = g^{-1}S$ für alle $h \in H$ und damit $ghg^{-1} \in S$, das heißt $gHg^{-1} \subseteq S$.

□

Die folgenden Sätze zeigen exemplarisch, wie man mit Hilfe der Sylowschen Sätze Einblicke in die Struktur endlicher Gruppen gewinnen kann.

Korollar 2.2.2. *Sei G eine endliche Gruppe, $p \in \mathbb{N}$ eine Primzahl. Sind $S, T \in \mathrm{Syl}_p(G)$, so gibt es $g \in G$ mit $T = gSg^{-1}$. Insbesondere sind alle Sylow p-Gruppen isomorph und eine Sylowgruppe $S \in \mathrm{Syl}_p(G)$ ist ein Normalteiler von G genau dann, $\mathrm{Syl}_p(G) = \{S\}$ gilt.*

[3] Gemeint sind hier Teilmengen (nicht Untergruppen) von G mit p^n Elementen.

Beweis. Es sei $g \in G$. Da Konjugation $\iota_g \colon G \longrightarrow G; x \mapsto gxg^{-1}$ ein Automorphismus (also insbesondere bijektiv) ist, ist $gSg^{-1} = \iota_g(S)$ eine Untergruppe der Ordnung $|S|$. Damit gilt $gSg^{-1} \in \mathrm{Syl}_p(G)$.

Nach dem Satz von Sylow existiert ein $x \in G$ mit $xSx^{-1} \subseteq T$. Mit $|S| = |T|$ folgt $xSx^{-1} = T$. Weiter gilt damit die Äquivalenzkette

$$\mathrm{Syl}_p(G) = \{S\} \Leftrightarrow gSg^{-1} = S \text{ für alle } g \in G \Leftrightarrow S \trianglelefteq G.$$

□

Korollar 2.2.3. *Sei $n \in \mathbb{N}_{\geq 4}$ und $S \in \mathrm{Syl}_2(\mathcal{S}_n)$. Dann ist S nicht zyklisch.*

Beweis. Wir betrachten erneut die nicht zyklische Untergruppe

$$V_4 := \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \subseteq \mathcal{S}_n.$$

der Ordnung 2^2. Nach Satz 2.2.1(2) existiert eine Sylow 2-Untergruppe T von $\mathcal{S}_n$, die V_4 enthält. Damit ist T nach Satz 1.3.2 nicht zyklisch. Weiter liefert Korollar 2.2.2 uns $T \cong S$. Damit ist auch S nicht zyklisch. □

2.3 Endliche abelsche Gruppen

Wir haben gesehen, dass jede Gruppe der $4 = 2^2$ abelsch ist und, dass $\mathcal{C}_4$ und $\mathcal{C}_2 \times \mathcal{C}_2$ nicht isomorphe Gruppe der Ordnung 4 sind. Es stellt sich die Frage, ob noch weitere Isomorphietypen existieren, die wir übersehen haben. Am Ende des Abschnittes werden wir verstehen warum $\mathcal{C}_4$ und $\mathcal{C}_2 \times \mathcal{C}_2$ die einzigen Isomorphietypen für Gruppen der Ordnung 4 sind. Allgemeiner werden wir in der Lage sein für jede vorgegebene Ordnung n die Anzahl der Isomorphieklassen abelscher Gruppen mit Ordnung n zu bestimmen.

Definition. Es sei G eine endliche abelsche Gruppe und $\ell \in \mathbb{N}$. Dann ist $G(\ell) := \{g^\ell \mid g \in G\}$ eine Untergruppe von G.

Beispiel. Es sei $n \in \mathbb{N}$ und $\mathcal{C}_n$, dann ist $\zeta := e^{\frac{2\pi i}{n}}$ ein zyklischer Erzeuger von $\mathcal{C}_n$. Es sei $\ell \in \mathbb{N}$. Dann gilt

$$\mathcal{C}_n(\ell) = \{(\zeta^z)^\ell \mid z \in \mathbb{Z}\} = \{(\zeta^\ell)^z \mid z \in \mathbb{Z}\} = \langle \zeta^\ell \rangle.$$

Insbesondere gilt für $1 \leq \ell \leq n$ mit $\ell \mid n$, dass $\frac{n}{\ell} \in \mathbb{N}$ und $\mathcal{C}_n(\ell) = \langle \zeta^\ell \rangle = \langle e^{\frac{2\pi i}{\frac{n}{\ell}}} \rangle$, das heißt

$$\mathcal{C}_n(\ell) = \mathcal{C}_{\frac{n}{\ell}}.$$

Bemerkung 2.3.1. Aus Notationsgründen führen wir die restlichen Beweise in diesem Abschnitt mit den Gruppen $(\mathcal{C}_n, \cdot)$ für $n \in \mathbb{N}$. Da $(\mathcal{C}_n, \cdot) \cong (\mathbb{Z}/\langle n \rangle, +)$ gilt, können die Resultate auch mit den additiv geschriebenen Gruppen $(\mathbb{Z}/\langle n \rangle, +)$ formuliert und genutzt werden.

Satz 2.3.2. *Es sei $G \neq \{e\}$ eine abelsche p-Gruppe der Ordnung p^n. Dann existieren eindeutig bestimmte Elemente $k_1 \geq k_2 \geq \cdots \geq k_\ell \geq 1$ mit $G \cong \prod_{i=1}^{\ell} \mathcal{C}_{p^{k_i}}$.*

Beweis.

(1) Existenz der Zerlegung: Wir schreiben $|G| = p^n$ und führen Induktion nach n. Der Fall $n = 1$ ist klar. Sei nun $n > 1$. Wir können stets annehmen, dass G nicht zyklisch ist. Wir wählen in G ein Element maximaler Ordnung g, etwa $\operatorname{ord}(g) = p^m$ mit $1 \leq m < n$. Dann existiert eine Untergruppe U maximaler Ordnung mit $U \cap \langle g \rangle = \{e\}$. Wir nehmen $U \cdot \langle g \rangle \neq G$ an und führen diese Annahme zum Widerspruch.

Die Annahme liefert $h \in G \setminus U \cdot \langle g \rangle$. Wir wählen h mit minimaler Ordnung unter all diesen Elementen. Dann ist $\operatorname{ord}(h) = p^r$ mit $1 \leq r \leq m$ (da $h \neq e$). Es gilt

$$\operatorname{ord}(h^p) \overset{1.3.1}{=} \frac{\operatorname{ord}(h)}{\operatorname{ggT}(\operatorname{ord}(h), p)} = \frac{\operatorname{ord}(h)}{p} < \operatorname{ord}(h)$$

und damit $h^p \in U \cdot \langle g \rangle$ aufgrund der Minimalität der Ordnung von h. Wir finden $u \in U$ und $\ell \in \mathbb{N}_0$ mit $h^p = u \cdot g^\ell$. Es gilt

$$e = h^{p^r} = (h^p)^{p^{r-1}} \overset{G \text{ abelsch}}{=} u^{p^{r-1}} \cdot g^{\ell p^{r-1}}$$

und damit $g^{\ell p^{r-1}} = (u^{-1})^{p^{r-1}} \in U \cap \langle g \rangle = \{e\}$. Nach Satz 1.3.1 gilt also $\operatorname{ord}(g) = p^m \mid \ell p^{r-1}$ und damit $p \mid \ell$, da $r - 1 < m$. Wir schreiben $\ell = k \cdot p$ und erhalten $(h \cdot g^{-k})^p = h^p \cdot g^{-\ell} = u \in U$. Weiter gilt $h \cdot g^{-k} \notin U$, da $h \notin U \cdot \langle g \rangle$ (ansonsten wäre $h = (h \cdot g^{-k}) \cdot g^k \in U \cdot \langle g \rangle$). Maximalität von $U \subsetneq \langle h \cdot g^{-k} \rangle \cdot U$ liefert $\langle h \cdot g^{-k} \rangle \cdot U \cap \langle g \rangle \neq \{e\}$[4]. Wir finden $a, b \in \mathbb{Z}$ und $u \in U$ mit

$$e \neq g^a = (h \cdot g^{-k})^b \cdot u.$$

Es folgt $h^b = u^{-1} \cdot g^{kb+a} \in U \cdot \langle g \rangle$. Die Annahme $p \mid b$ liefert uns $(h \cdot g^{-k})^b = ((h \cdot g^{-k})^p)^{\frac{b}{p}} \in U$ und damit $g^a = (h \cdot g^{-k})^b \cdot u \in U \cap \langle g \rangle = \{e\}$, ein Widerspruch. Also gilt $\operatorname{ggT}(b, p) = 1$ und wir finden $s, t \in \mathbb{Z}$ mit $1 = sb + tp$. Es folgt

$$h = h^{sb+tp} = (h^b)^s \cdot (h^p)^t \in U \cdot \langle g \rangle.$$

Dies ist ein Widerspruch. Also gilt $U \cdot \langle g \rangle = G$. Da $U \cap \langle g \rangle = \{e\}$ gilt, können wir Lemma 1.6.1 anwenden und erhalten

$$G \cong U \times \langle g \rangle \cong U \times \mathcal{C}_{\operatorname{ord}(g)}$$

mit einer p-Gruppe U von echt kleinerer Ordnung. Nun wenden wir Induktion an.

(2) Eindeutigkeit: Wir führen Induktion über $|G| = p^n$. Der Fall $n = 1$ ist trivial. Es sei nun $n \geq 2$. Wir betrachten zwei Zerlegungen von G wie in der Behauptung

$$\prod_{i=1}^{\ell} \mathcal{C}_{p^{k_i}} \cong G \cong \prod_{i=1}^{\ell'} \mathcal{C}_{p^{m_i}}.$$

[4] Da G abelsch ist, ist jede Untergruppe ein Normalteiler und das Produkt von Untergruppen stets eine Untergruppe.

Es sei $0 \leq s \leq \ell$ und $0 \leq t \leq \ell'$ mit $k_i = 1 \Leftrightarrow i > s$ und $m_i = 1 \Leftrightarrow i > t$. Es folgt

$$G(p) \cong \prod_{i=1}^{\ell} \mathcal{C}_{p^{k_i}}(p) = \prod_{i=1}^{s} \mathcal{C}_{p^{k_i-1}} \text{ und } G(p) \cong \prod_{i=1}^{\ell'} \mathcal{C}_{p^{m_i}}(p) \cong \prod_{i=1}^{t} \mathcal{C}_{p^{m_i-1}}.$$

Es gilt $|G(p)| < |G|$ und damit nach Induktionsvoraussetzung $t = s$ und $k_i - 1 = m_i - 1$ für $1 \leq i \leq s = t$. Es folgt

$$\prod_{i=1}^{s} \mathcal{C}_{p^{k_i}} \times \prod_{i=s+1}^{\ell} \mathcal{C}_p \cong G \cong \prod_{i=1}^{s} \mathcal{C}_{p^{k_i}} \times \prod_{i=s+1}^{\ell'} \mathcal{C}_p$$

und damit $\ell = \ell'$ aufgrund der Mächtigkeit beider Gruppen.

□

Definition. Es sei $n \in \mathbb{N}$. Eine **Partition von** n ist eine Folge $\kappa = (k_1, \ldots, k_\ell)$ von natürlichen Zahlen mit $k_1 \geq k_2 \geq \cdots \geq k_\ell \geq 1$, sodass

$$n = k_1 + k_2 + \cdots + k_\ell$$

gilt. Für eine Primzahl $p \in \mathbb{P}$ und eine Partition $\kappa = (k_1, \ldots, k_\ell)$ definieren wir die abelsche Gruppe

$$\mathcal{C}_{p^\kappa} := \mathcal{C}_{p^{k_1}} \times \mathcal{C}_{p^{k_2}} \times \cdots \times \mathcal{C}_{p^{k_\ell}} \cong \mathbb{Z}/\langle p^{k_1} \rangle \times \mathbb{Z}/\langle p^{k_2} \rangle \times \cdots \times \mathbb{Z}/\langle p^{k_\ell} \rangle.$$

Beispiel. Es gilt $14641 = 11^4$. Nach dem vorherigen Satz korrespondieren die abelschen Gruppen dieser Ordnung (bis auf Isomorphie) zu den Gruppen $\mathcal{C}_{11^\kappa}$, wobei κ eine Partition von 4 ist. Die Partitionen von 4 sind $(4), (3,1), (2,2), (2,1,1), (1,1,1,1)$. Bis auf Isomorphie existieren also genau fünf abelsche Gruppen der Ordnung 14641. Diese sind

$$\mathcal{C}_{11^{(4)}} = \mathcal{C}_{11^4}, \mathcal{C}_{11^{(3,1)}} = \mathcal{C}_{11^3} \times \mathcal{C}_{11}, \mathcal{C}_{11^{(2,2)}} = \mathcal{C}_{11^2} \times \mathcal{C}_{11^2},$$

$$\mathcal{C}_{11^{(2,1,1)}} = \mathcal{C}_{11^2} \times \mathcal{C}_{11} \times \mathcal{C}_{11}, \mathcal{C}_{11^{(1,1,1,1)}} = \mathcal{C}_{11} \times \mathcal{C}_{11} \times \mathcal{C}_{11} \times \mathcal{C}_{11}.$$

Satz 2.3.3. *Es sei $G \neq \{e\}$ eine abelsche endliche Gruppe und $p_1, \ldots, p_t$ die paarweise verschiedenen Primteiler von $|G|$ und $S_i \in \mathrm{Syl}_{p_i}(G)$ für $1 \leq i \leq t$.*

(1) Es gilt $\mathrm{Syl}_{p_i}(G) = \{S_i\}$ für alle $1 \leq i \leq t$.

(2) Es gilt $G \cong S_1 \times S_2 \times \cdots \times S_t$.

(3) Ist $g \in G$ ein Element maximaler Ordnung in G, so gilt $\mathrm{ord}(h) \mid \mathrm{ord}(g)$ für alle $h \in G$.

Beweis.

(1) Da G abelsch ist, gilt $gSg^{-1} = S$ für jede Sylowgruppe. Wir wenden Korollar 2.2.2 an.

(2) Da G abelsch ist, ist jede Sylowgruppe ein Normalteiler. Wir wenden Korollar 1.6.2 an und erhalten $S_1 S_2 \cdots S_t \cong S_1 \times S_2 \times \cdots \times S_t$. Mit $|S_1 \times S_2 \times \cdots \times S_t| = |G|$ folgt $G = S_1 S_2 \cdots S_t \cong S_1 \times S_2 \times \cdots \times S_t$.

(3) Nach (2) und Satz 2.3.2, finden wir $m \in \mathbb{N}$ und $\ell_1, \dots, \ell_m \in \mathbb{N}_{\geq 2}$ mit $G \cong \prod_{i=1}^{m} \mathcal{C}_{\ell_i}$. O.B.d.A. nehmen wir Gleichheit an und wählen Erzeuger $\mathcal{C}_{\ell_i} = \langle g_i \rangle$. Es gilt $k := \operatorname{ord}((g_1, \dots, g_m)) \leq \operatorname{ord}(g)$ und

$$(e_{\mathcal{C}_{\ell_1}}, \dots, e_{\mathcal{C}_{\ell_m}}) = e_G = (g_1, \dots, g_m)^k = (g_1^k, \dots, g_m^k).^{5}$$

Das heißt $g_i^k = e_{\mathcal{C}_{\ell_i}}$ für $1 \leq i \leq m$. Es sei $x \in G$. Wir schreiben $x = (g_1^{a_1}, \dots, g_m^{a_m})$. Es folgt

$$x^k = ((g_1^k)^{a_1}, \dots, (g_m^k)^{a_m}) = e_G.$$

Nach Satz 1.3.1 folgt $\operatorname{ord}(x) \mid k$. Anwendung auf $x = g$ liefert $\operatorname{ord}(g) \mid k$ und damit $\operatorname{ord}(g) = k$. Für $x = h$ folgt $\operatorname{ord}(h) \mid k = \operatorname{ord}(g)$.

□

Korollar 2.3.4. *Es sei $G \neq \{e\}$ eine endliche abelsche Gruppe, $p_1, \dots, p_t$ paarweise verschiedene Primzahlen und $n_1, \dots, n_t \in \mathbb{N}$ mit $|G| = \prod_{i=1}^{t} p_i^{n_i}$. Dann existieren eindeutige bestimmte Partitionen $\kappa_1, \dots, \kappa_t$ von $n_1, \dots, n_t$ mit*

$$G \cong \mathcal{C}_{p_1^{\kappa_1}} \times \mathcal{C}_{p_2^{\kappa_2}} \times \cdots \times \mathcal{C}_{p_t^{\kappa_t}}.$$

Beweis.

(1) Existenz der Zerlegung: Nach Satz 2.3.3 existiert für jedes $i \in \{1, \dots, t\}$ genau eine Sylow p_i-Gruppe S_i und $G \cong S_1 \times S_2 \times \cdots \times S_t$. Jedes S_i ist eine abelsche p_i-Gruppe. Das heißt wir finden nach Satz 2.3.2 eine Zerlegung

$$S_i \cong \prod_{j=1}^{\ell_i} \mathcal{C}_{p_i^{k_j}}$$

mit $k_1 \geq k_2 \geq \cdots \geq k_{\ell_i} \geq 1$. Mit $p_i^{\ell_i} = |S_i| = p_i^{k_1} \cdot p_i^{k_2} \cdots p_i^{k_{\ell_i}} = p_i^{k_1 + k_2 + \dots + k_{\ell_i}}$ folgt, dass $\kappa_i := (k_1, k_2, \dots, k_{\ell_i})$ eine Partition von n_i ist.

(2) Es seien κ_i, κ_i' Partitionen von n_i für $1 \leq i \leq t$ mit

$$\mathcal{C}_{p_1^{\kappa_1}} \times \mathcal{C}_{p_2^{\kappa_2}} \times \cdots \times \mathcal{C}_{p_t^{\kappa_t}} \cong \mathcal{C}_{p_1^{\kappa_1'}} \times \mathcal{C}_{p_2^{\kappa_2'}} \times \cdots \times \mathcal{C}_{p_t^{\kappa_t'}}$$

und φ ein entsprechender Isomorphismus. Es sei $i \in \{1, \dots, t\}$. Für $j \in \{1, \dots, t\}$ sei e_j das neutrale Element von $\mathcal{C}_{p_j^{\kappa_j}}$ und e_j' das neutrale Element von $\mathcal{C}_{p_j^{\kappa_j'}}$. Da beide Gruppen abelsch sind, sind

$$T_i := \{e_1\} \times \cdots \times \{e_{i-1}\} \times \mathcal{C}_{p_i^{\kappa_i}} \times \{e_{i+1}\} \times \cdots \times \{e_t\}, \text{ und}$$

$$T_i' := \{e_1\} \times \cdots \times \{e_{i-1}\} \times \mathcal{C}_{p_i^{\kappa_i'}} \times \{e_{i+1}\} \times \cdots \times \{e_t\}^{6}$$

[5] Es gilt $e_{\mathcal{C}_n} = 1_{\mathbb{R}}$ für alle $n \in \mathbb{N}$. Wir benennen die neutrale Elemente verschieden damit klar ist, in welcher Gruppe wir uns befinden.

[6] Siehe vorherige Fußnote.

die eindeutig bestimmten Sylow p_i-Untergruppen der beiden Gruppen (siehe Satz 2.3.3). Da ein Isomorphismus Sylowgruppen erhält, folgt

$$\mathcal{C}_{p_i^{\kappa_i}} \cong T_i \cong \varphi(T_i) = T_i' \cong \mathcal{C}_{p_i^{\kappa_i'}}.$$

Anwendung von Satz 2.3.2 liefert nun $\kappa_i = \kappa_i'$.

□

Beispiel. Wir wollen (bis auf Isomorphie) alle abelschen Gruppen der Ordnung

$$263538 = 2^1 \cdot 3^2 \cdot 11^4$$

bestimmen. Nach den vorherigen Ergebnissen müssen wir nur alle möglichen Partitionen von 1,2 und 4 bestimmen.

(1) 1 besitzt genau 1 Partition, nämlich (1).

(2) 2 besitzt genau 2 Partitionen, nämlich $(2), (1,1)$.

(3) 4 besitzt 5 Partitionen, nämlich $(4), (3,1), (2,2), (2,1,1), (1,1,1,1)$.

Nach Korollar 2.3.4 gibt es damit genau $1 \cdot 2 \cdot 5 = 10$ Isomorphietypen. Wir listen diese der Vollständigkeit halber:

$\mathcal{C}_{2^{(1)}} \times \mathcal{C}_{3^{(2)}} \times \mathcal{C}_{11^{(4)}}$, $\mathcal{C}_{2^{(1)}} \times \mathcal{C}_{3^{(2)}} \times \mathcal{C}_{11^{(3,1)}}$, $\mathcal{C}_{2^{(1)}} \times \mathcal{C}_{3^{(2)}} \times \mathcal{C}_{11^{(2,2)}}$, $\mathcal{C}_{2^{(1)}} \times \mathcal{C}_{3^{(2)}} \times \mathcal{C}_{11^{(2,1,1)}}$, $\mathcal{C}_{2^{(1)}} \times \mathcal{C}_{3^{(2)}} \times \mathcal{C}_{11^{(1,1,1,1)}}$,

$\mathcal{C}_{2^{(1)}} \times \mathcal{C}_{3^{(1,1)}} \times \mathcal{C}_{11^{(4)}}$, $\mathcal{C}_{2^{(1)}} \times \mathcal{C}_{3^{(1,1)}} \times \mathcal{C}_{11^{(3,1)}}$, $\mathcal{C}_{2^{(1)}} \times \mathcal{C}_{3^{(1,1)}} \times \mathcal{C}_{11^{(2,2)}}$, $\mathcal{C}_{2^{(1)}} \times \mathcal{C}_{3^{(1,1)}} \times \mathcal{C}_{11^{(2,1,1)}}$, $\mathcal{C}_{2^{(1)}} \times \mathcal{C}_{3^{(1,1)}} \times \mathcal{C}_{11^{(1,1,1,1)}}$.

3 Grundlagen der Ringtheorie

3.1 Grundlegende Definitionen

Definition. Ein **Ring** R ist ein Tripel $(R, +, \cdot)$, wobei $R \neq \varnothing$ eine Menge ist und $+, \cdot : R \times R \longrightarrow R$ Abbildungen sind, sodass folgende Axiome gelten:

(1) $(R, +)$ ist eine abelsche Gruppe (mit neutralem Element 0 und inversen Elementen $-x$).

(2) $(R, \cdot)$ ist eine Halbgruppe (wir schreiben $ab = a \cdot b$).

(3) $a(b + c) = ab + ac$; $(a + b)c = ac + bc$ für alle $a, b, c \in R$ (**Distributivgesetze**).

(4) Es existiert $1 \in R$ mit $1 \cdot a = a = a \cdot 1$ für alle $a \in R$.

Gilt zudem $ab = ba$ für alle $a, b \in R$, so nennt man R einen **kommutativen Ring**.

Beispiele. (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind kommutative Ringe.

(2) Sind $R_1, \ldots, R_n$ Ringe, so ist $\prod_{i=1}^{n} R_i$ ein Ring mit Operationen

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$$

und

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) := (x_1 y_1, \ldots, x_n y_n).$$

(3) Es sei $n \in \mathbb{N}$. Die Menge der $n \times n$-Matrizen $\mathrm{Mat}_n(\mathbb{R})$ erhält mit der Matrizenaddition und Matrizenmultiplikation die Struktur eines Rings. Der Ring ist genau dann kommutativ, wenn $n = 1$ gilt.

(4) Es sei V ein $\mathbb{R}$-Vektorraum, dann erhält die Menge der $\mathbb{R}$-linearen Abbildungen $\mathrm{End}_{\mathbb{R}}(V)$ die Struktur eines Rings durch

$$(f + g)(x) := f(x) + g(x) \text{ und } (f \cdot g)(x) := (f \circ g)(x) \text{ für alle } f, g \in \mathrm{End}_{\mathbb{R}}(V), x \in V.$$

Definition. Sei R ein Ring.

(1) Eine Teilmenge $S \subseteq R$ heißt **Unterring** von R, falls gilt

(i) S ist eine Untergruppe von R bezüglich $+$,

(ii) $ab \in S$ für alle $a, b \in S$,

(iii) $1 \in S$.

(2) Eine Teilmenge $I \subseteq R$ heißt **Ideal**, falls gilt

(i) I ist Untergruppe von R bezüglich $+$,

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

Lemma 3.1.1. *Sei R ein Ring, $I, J \subseteq R$ Ideale von R sowie $(I_\ell)_{\ell\in\Lambda}$ eine Familie von Idealen von R.*

(1) $\sum_{\ell\in\Lambda} I_\ell := \{\sum_{\ell\in\Lambda'} x_\ell \mid \Lambda' \subseteq \Lambda$ *endlich*, $x_\ell \in I_\ell$ *für alle* $\ell \in \Lambda'\}$ *ist ein Ideal von R.*

(2) $\bigcap_{\ell\in\Lambda} I_\ell$ *ist ein Ideal von R.*

(3) $I \cdot J := IJ := \{\sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}_0, a_i \in I, b_i \in J\}$ *ist ein Ideal von R.*

Beweis. Die Aussagen folgen durch direktes Nachrechnen. □

Definition. Ist $I \subseteq R$ ein Ideal und $n \in \mathbb{N}_{\geq 2}$, so definiert man induktiv I^n durch $I^n := I \cdot I^{n-1}$.

Beispiele. (1) Sei $n \in \mathbb{Z}$, dann ist die abelsche Untergruppe $\langle z\rangle \subseteq (\mathbb{Z}, +)$ auch ein Ideal des Rings $(\mathbb{Z}, +, \cdot)$.

(2) Für ein Ideal $I \subseteq R$ gilt $I = R$ genau dann, wenn $1 \in I$ gilt, denn $1 \in I$ liefert $r = r \cdot 1 \in R$ für alle $r \in R$.

Definition. Sei R ein Ring, $I \subseteq R$ ein Ideal. Dann heißt $R/I = \{x + I \mid x \in R\}$ zusammen mit den Verknüpfungen

(i) $(x + I) + (y + I) := (x + y) + I$, und

(ii) $(x + I) \cdot (y + I) := (xy) + I$

der **Faktorring** oder **Restklassenring** von R nach I.

Bemerkung 3.1.2. Da $(R, +)$ eine abelsche Gruppe ist, ist die Addition auf R/I wohldefiniert. Erst für die Wohldefiniertheit der Multiplikation wird die Idealeigenschaft benötigt.

Definition. Eine Abbildung $\varphi : R \longrightarrow R'$ zwischen zwei Ringen heißt **Homomorphismus**, falls gilt

(a) $\varphi(x + y) = \varphi(x) + \varphi(y)$ für alle $x, y \in R$,

(b) $\varphi(xy) = \varphi(x)\varphi(y)$ für alle $x, y \in R$ und

(c) $\varphi(1_R) = 1_{R'}$.

Bemerkungen 3.1.3. Sei $\varphi\colon R \longrightarrow R'$ ein Homomorphimus von Ringen.

- Ist $S \subseteq R$ ein Unterring, so ist $\varphi(S)$ Unterring von R'.
- Ist $S' \subseteq R'$ ein Unterring, so ist $\varphi^{-1}(S')$ ein Unterring von R.
- Ist $I' \subseteq R'$ ein Ideal, so ist $\varphi^{-1}(I')$ ein Ideal von R. Bilder von Idealen sind hingegen im Allgemeinen keine Ideale: Es ist $\mathbb{Z} \subseteq \mathbb{Q}$ kein Ideal.
- Ist $\varphi : R \longrightarrow R'$ ein bijektiver Homomorphismus, so ist $\varphi^{-1} : R' \longrightarrow R$ ein Homomorphismus.
- Ist $I \subseteq R$ ein Ideal. Dann ist die kanonische Projektion

  $$\pi : R \longrightarrow R/I; r \mapsto r + I$$

  ein surjektiver Ringhomomorphismus mit $\ker \pi = I$.
- Die Abbildung $\varphi\colon \mathbb{Z} \longrightarrow \mathbb{Z}, x \mapsto 0$ ist kein Ringhomomorphismus. Es gilt jedoch

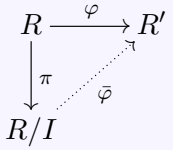
  $$\varphi(xy) = \varphi(x)\varphi(y)$$

  und

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

  für alle $x, y \in \mathbb{Z}$.

Satz 3.1.4. *Es sei $\varphi : R \longrightarrow R'$ ein Homomorphismus von Ringen und $I \subseteq \ker \varphi$ ein Ideal von R. Dann gibt es genau einen Homomorphismus von Ringen $\bar{\varphi} : R/I \longrightarrow R'$ derart, dass $\bar{\varphi} \circ \pi = \varphi$ gilt. Wir erhalten also das kommutative Diagramm:*



Beweis. Der Beweis kann analog wie im Fall von Gruppen geführt werden. □

Definition. Es sei R ein Ring. Ein Element $x \in R$ heißt **invertierbar** oder **Einheit** falls $y, z \in R$ mit $x \cdot y = 1 = z \cdot x$ existieren.

Bemerkung 3.1.5. Sei $x \in R$ invertierbar und $a, b \in R$ mit $ax = 1 = xb$. Es folgt $a = a(xb) = (ax)b = b$. Wir bezeichnen mit $x^{-1} \in R$ das damit eindeutig bestimmte Element mit $x \cdot x^{-1} = 1 = x^{-1} \cdot x$.

Beispiele.

(1) Es sei $A \in \mathrm{Mat}_n(\mathbb{R})$. Angenommen es existiert $B \in \mathrm{Mat}_n(\mathbb{R})$ mit $BA = I_n$, dann gilt $\det(B)\det(A) = \det(BA) = \det(I_n) = 1$. Insbesondere gilt $B \in \mathrm{GL}_n(\mathbb{R})$ und $AB = (B^{-1}B)AB = B^{-1}(BA)B = I_n$ und A ist eine Einheit.

(2) Es sei $V := \{(x_n)_{n\geq 1} \mid x_n \in \mathbb{R}\}$ der $\mathbb{R}$-Vektorraum aller Folgen in $\mathbb{R}$, sowie $R := \mathrm{End}_{\mathbb{R}}(V)$. Es ist

$$\varphi : V \longrightarrow V \ ; \ \varphi((x_n)_{n\in\mathbb{N}}) := (0, x_1, x_2, \ldots)$$

$\mathbb{R}$-linear. Wir betrachten

$$\psi : V \longrightarrow V \ ; \ \psi((x_n)_{n\in\mathbb{N}}) := (x_2, x_3, \ldots).$$

Dann gilt $\psi \in R$ und $\psi \circ \varphi = \mathrm{id}_V$. Angenommen, es existiert $\gamma \in \mathrm{End}_{\mathbb{R}}(V)$ mit $\varphi \circ \gamma = \mathrm{id}_V$. Dann ist φ ist surjektiv. Aus $(1, 0, 0, \ldots) \notin \mathrm{im}\,\varphi$ erhalten wir einen Widerspruch.

Definition. Sei R ein Ring.

(1) Die Menge

$$R^\times = \{x \in R \mid x \text{ ist invertierbar}\} \subseteq R$$

ist eine Gruppe bezüglich der Multiplikation und heißt **Einheitengruppe** von R.

(2) Ist R kommutativ, $R \neq \{0\}$ und $R^\times = R \setminus \{0\}$, so heißt R **Körper**.

Beispiele.

(1) Es gilt $\mathbb{Z}^\times = \{1, -1\}$.

(2) Es gilt $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

(3) Es gilt $(R \times S)^\times = R^\times \times S^\times$ für Ringe R, S.

3.2 Kommutative Ringe

Im Folgenden sei R stets ein kommutativer Ring.

Definition. Es sei R ein kommutativer Ring und $X \subseteq R$ eine Teilmenge. Dann ist

$$(X) := \{\sum_{i=1}^{n} r_i x_i \mid n \in \mathbb{N}_0, x_1, \ldots, x_n \in X, r_1, \ldots, r_n \in R\} = \bigcap_{X\subseteq I\subseteq R, I \text{ Ideal}} I$$

ein Ideal von R. Man nennt (X) das **von** X **erzeugte Ideal** von R. Gilt $X = \{x_1, \ldots, x_n\}$, so schreiben wir $(X) = (x_1, \ldots, x_n)$. Für $x \in R$ gilt $(x) = Rx = \{rx \mid r \in R\}$. Solche Ideale heißen **Hauptideale**.

Beispiele. (1) Es sei $I \subseteq \mathbb{Z}$ ein Ideal. Dann ist $(I, +)$ eine Untergruppe und es gilt $I = \langle n\rangle$ für ein $n \in \mathbb{N}_0$. Da $\langle n\rangle$ auch ein Ideal ist, folgt $I = \langle n\rangle = (n)$. Also sind alle Ideale von $\mathbb{Z}$ Hauptideale.

(2) In $(\mathbb{Q}, +, \cdot)$ gilt $\langle 2\rangle = \mathbb{Z}$ und $(2) = \mathbb{Q}$.

Satz 3.2.1. *Sei $R \neq \{0\}$ ein kommutativer Ring. Dann sind folgende Aussagen äquivalent.*

(1) R ist ein Körper.

(2) $\{0\}$ und R sind die einzigen Ideale von R.

(3) Ist $\varphi : R \longrightarrow R'$ ein Homomorphismus von Ringen mit $R' \neq \{0\}$, so ist φ injektiv.

Beweis. (1) $\Rightarrow$ (2). Es sei $I \neq \{0\}$ ein Ideal von R. Wir finden $0 \neq x \in I$. Da R ein Körper ist, gilt $x \in R \setminus \{0\} = R^\times$. Die Idealeigenschaft liefert $1 = x^{-1}x \in I$. Für $r \in R$ folgt $r = r \cdot 1 \in I$ und damit $I = R$.

(2) $\Rightarrow$ (3). Wegen $\varphi(1_R) = 1_{R'} \neq 0_{R'}$ gilt $\ker\varphi \neq R$. Damit liefert (2) $\ker\varphi = \{0\}$ und φ ist injektiv.

(3) $\Rightarrow$ (1). Es sei $x \in R \setminus \{0\}$. Es ist $\{0\} \neq Rx$ ein Ideal von R. Wir betrachten den Homomorphismus von Ringen

$$\pi \colon R \longrightarrow R/Rx \quad r \mapsto r + Rx.$$

Es gilt $\ker\pi = Rx$. Die Voraussetzung liefert uns nun $R/Rx = \{0\}$. Das heißt $R = Rx$. Insbesondere existiert $y \in R$ mit $1 = y \cdot x$ und x ist eine Einheit. □

Definition. Sei $R \neq \{0\}$ ein kommutativer Ring.

(1) Ein Element $x \in R$ heißt **Nullteiler**, falls es ein $r \in R \setminus \{0\}$ mit $xr = 0$ ($rx = 0$) existiert.

(2) Ist 0 der einzige Nullteiler von R, so nennt man R einen **Integritätsbereich**.

Beispiele.

(1) $\mathbb{Z}$ ist ein Integritätsbereich. Weiter sind Körper stets Integritätsbereiche.

(2) $\mathbb{R} \times \mathbb{R}$ ist kein Integritätsbereich.

(3) Ist V ein endlich dimensionaler $\mathbb{R}$-Vektorraum, so ist $\mathrm{End}_{\mathbb{R}}(V)$ genau dann ein Integritätsbereich, wenn $\dim_{\mathbb{R}} V = 1$ gilt: Ist $\dim_{\mathbb{R}} V \geq 2$ so finden wir echte Untervektorräume $U, W \subseteq V$ mit $U \oplus W = V$. Die Projektionen $\pi_U \colon V \longrightarrow V, u + w \mapsto u$, $\pi_W \colon V \longrightarrow V, u + w \mapsto w$ erfüllen $0 = \pi_U \circ \pi_W$, aber $\pi_U \neq 0 \neq \pi_W$.

Lemma 3.2.2. *Sei R ein endlicher Integritätsbereich. Dann ist R ein Körper.*

Beweis. Sei $x \in R \setminus \{0\}$. Da R ein Integritätsbereich ist, ist die Abbildung

$$\ell_x : \begin{cases} R & \longrightarrow & R \\ r & \mapsto & xr \end{cases}$$

injektiv. Da R endlich ist, ist ℓ_x auch surjektiv und es existiert $r \in R$ mit $1 = \ell_x(r) = xr$. Damit ist x invertierbar und R ist ein Körper. □

Satz 3.2.3. *Sei $n \geq 2$. Folgende Aussagen sind äquivalent:*

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

(2) $\mathbb{Z}/(n)$ ist ein Körper.

(3) n ist eine Primzahl.

Beweis. (1) $\Rightarrow$ (2). Dies folgt aus Lemma 3.2.2.

(2) $\Rightarrow$ (3). Es gilt $n \neq 1$. Es sei $n \neq a$ ein Teiler von n und $b \in \mathbb{N}$ mit $ab = n$ wir erhalten $(a+(n))(b+(n)) = ab+(n) = 0_{\mathbb{Z}/(n)}$. Da $\mathbb{Z}/(n)$ ein Körper ist, folgt $a+(n) = 0$ oder $b+(n) = 0$. Da $n \neq a$ gilt, folgt $n \nmid a$, also $b+(n) = 0$. Das heißt $n \mid b$ und damit $n = b$, da $b \leq n$. Wir schließen $a = 1$. Damit ist n eine Primzahl.

(3) $\Rightarrow$ (1). Es seien $a+(n), b+(n)$ mit $(a+(n))(b+(n)) = 0_{\mathbb{Z}/(n)}$. Wir erhalten $ab \in (n)$. Da n eine Primzahl ist, folgt $n|a$ oder $n|b$ und daher $a+(n) = 0_{\mathbb{Z}/(n)}$ oder $b+(n) = 0_{\mathbb{Z}/(n)}$. Damit ist $\mathbb{Z}/(n)$ ein Integritätsbereich. □

Sei $R \neq \{0\}$ ein kommutativer Ring. Für $n \in \mathbb{N}_0$ und $x \in R$ schreiben wir

$$nx := \underbrace{x + x + \cdots + x}_{n - \text{mal}}$$

sowie $(-n)x := -(nx)$. Damit haben wir also nx für $n \in \mathbb{Z}$ definiert.

Definition. Die Abbildung

$$\varphi : \mathbb{Z} \longrightarrow R \,;\, n \mapsto n1_R$$

ist ein Homomorphismus von Ringen. Damit ist $\ker\varphi \subseteq \mathbb{Z}$ ein Ideal und insbesondere eine Untergruppe. Es existiert also ein eindeutig bestimmtes $n \in \mathbb{N}_0$ mit $\ker\varphi = \langle n \rangle = (n)$. Die Zahl $\operatorname{char}(R) := n$ heißt die **Charakteristik** von R.

Beispiele. (1) Es gilt $\operatorname{char}(\mathbb{Z}) = \operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{C}) = 0$.

(2) Es gilt $\operatorname{char}(\mathbb{Z}/(n)) = n$ für alle $n \in \mathbb{N}_0$.

(3) Ist R ein endlicher Ring, so gilt $\operatorname{char}(R) \neq 0$. Die Umkehrung gilt aber nicht, wie zum Beispiel $R := \prod_{\mathbb{N}} \mathbb{Z}/(2)$[1] zeigt.

Lemma 3.2.4. *Sei R ein Integritätsbereich. Dann ist $\operatorname{char}(R) = 0$ oder $\operatorname{char}(R)$ ist eine Primzahl.*

Beweis. Die Abbildung $\varphi : \mathbb{Z} \longrightarrow R \,;\, n \mapsto n1_R$ induziert einen injektiven Homomorphismus $\bar{\varphi} : \mathbb{Z}/(\operatorname{char}(R)) \longrightarrow R$. Damit ist $\mathbb{Z}/(\operatorname{char}(R)) \cong \operatorname{im}\varphi$ ein Integritätsbereich. Wegen $R \neq \{0\}$ folgt $\operatorname{char}(R) \neq 1$ und Satz 3.2.3 liefert die Behauptung. □

[1] Hier ist unendliche kartesische Produkt von Ringen gemeint.

Definition. Sei R ein kommutativer Ring.

(a) Ein Ideal $\mathfrak{m} \subsetneq R$ heißt **maximal**, falls es kein Ideal $I \subseteq R$ mit $\mathfrak{m} \subsetneq I \subsetneq R$ gibt.

(b) Ein Ideal $\mathfrak{p} \subsetneq R$ heißt **Primideal**, falls für $x, y \in R$ mit $xy \in \mathfrak{p}$ stets $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$ gilt.

Lemma 3.2.5. *Sei R ein kommutativer Ring, $I \subseteq R$ ein Ideal.*

(1) I ist genau dann ein maximales Ideal, wenn R/I ein Körper ist.

(2) I ist genau dann ein Primideal, wenn R/I ein Integritätsbereich ist.

Beweis.

(1) Es sei I ein maximales Ideal. Dann gilt $I \neq R$ und $R/I \neq \{0\}$. Für $a + I \in R/I \setminus \{0\}$ gilt $a \notin I$. Damit gilt $I \subsetneq (a) + I$ und Maximalität liefert $(a) + I = R$. Insbesondere existieren $b \in R$ und $r \in I$ mit $ba + r = 1$. Das heißt $(b+I)(a+I) = 1 - r + I = 1 + R = 1_{R/I}$ und $a + I$ ist eine Einheit.

Sei umgekehrt R/I ein Körper. Dann gilt $I \neq R$. Es sei $I \subsetneq J$ ein Ideal von R und $a \in J \setminus I$. Dann ist $a + I \in R/I \setminus \{0\} = (R/I)^\times$ eine Einheit. Also existiert $b + I \in R/I$ mit $ab + I = (a + I)(b + I) = 1 + I$. Das heißt $1 - ab \in I$. Also $1 \in ab + I \subseteq J$ und $J = R$.

(2) Sei $I \subseteq R$ ein Primideal. Wegen $I \neq R$ folgt $R/I \neq \{0\}$. Seien nun $\bar{x}, \bar{y} \in R/I$ mit $\bar{x}\bar{y} = 0$.Wir schreiben $\bar{x} = x + I$ und $\bar{y} = y + I$ und erhalten $xy + I = 0$. Also gilt $xy \in I$ und da I ein Primideal ist, dürfen wir $x \in I$ annehmen. Es folgt $\bar{x} = 0$. Damit ist R/I ein Integritätsbereich.

Sei R/I ein Integritätsbereich. Dann gilt $I \neq R$. Sind $x, y \in R$ mit $xy \in I$, so folgt $(x + I)(y + I) = 0_{R/I} = I$. Da R/I Integritätsbereich ist, erhalten wir $x + I = 0$ oder $(y + I) = 0$, also gilt $x \in I$ oder $y \in I$. Damit ist I ein Primideal.

□

Bemerkung 3.2.6. Da jeder Körper ein Integritätsbereich ist, liefert Lemma 3.2.5: Jedes maximale Ideal $\mathfrak{m} \subseteq R$ ist ein Primideal.

Beispiel. Sei $I = (n)$ mit $n \in \mathbb{N}_0$ ein maximales Ideal von $\mathbb{Z}$. Da weder $\langle 0 \rangle = \{0\}$ noch $\langle 1 \rangle = \mathbb{Z}$ maximale Ideale sind, folgt $n \geq 2$ und Satz 3.2.3 liefert $n \in \mathbb{P}$. Das heißt I ist maximal genau dann, wenn eine Primzahl $p \in \mathbb{P}$ mit $I = (p)$ existiert. Analog zeigt man, dass die Primideale in $\mathbb{Z}$ genau von der Form $\langle p \rangle$ oder $\langle 0 \rangle = \{0\}$ sind.

Definition. Es sei $X = (X, \leq)$ eine partiell geordnete Menge. Eine Teilmenge $Y \subseteq X$ heißt **total geordnet** oder **Kette**, falls für $x, y \in Y$ stets $x \leq y$ oder $y \leq x$ gilt. Ein Element $x \in X$ heißt **obere Schranke von** Y falls $y \leq x$ für alle $y \in Y$ gilt. Ein Element $x_0 \in X$ heißt **maximal**, falls $x \geq x_0$ stets $x = x_0$ impliziert.

Eine entscheidende Rolle im Studium kommutativer Ringe spielt das folgende Resultat, das unter dem Namen Zornsches Lemma bekannt ist.[2]

Lemma 3.2.7 (Zornsches Lemma)**.** *Es sei $(X, \leq)$ eine nichtleere partiell geordnete Menge, in der jede total geordnete Teilmenge $Y \subseteq X$ in X eine obere Schranke besitzt. Dann existiert ein maximales Element $x_0 \in X$.*

Satz 3.2.8. *Sei $R \neq \{0\}$ ein kommutativer Ring.*

(1) Der Ring R besitzt ein maximales Ideal.

(2) Ist $I \subsetneq R$ ein Ideal. Dann gibt es ein maximales Ideal $\mathfrak{m} \subseteq R$ mit $I \subseteq \mathfrak{m}$.

Beweis.

(1) Übungsaufgabe.

(2) Wir betrachten die kanonische Projektion $\pi\colon R \longrightarrow R/I$. Es gilt $R/I \neq \{0\}$ und wir finden nach (1) ein maximales Ideal $\mathfrak{n} \trianglelefteq R/I$. Es ist $\mathfrak{m} := \pi^{-1}(\mathfrak{n})$ ein Ideal von R mit $I = \ker \pi = \pi^{-1}(\{0_{R/I}\}) \subseteq \pi^{-1}(\mathfrak{n}) = \mathfrak{m}$. Es sei $\mathfrak{m} \subsetneq \mathfrak{u} \trianglelefteq R$ ein Ideal. Da π surjektiv ist, ist $\pi(\mathfrak{u})$ ein Ideal von R/I mit $\mathfrak{n} = \pi(\pi^{-1}(\mathfrak{n})) = \pi(\mathfrak{m}) \subseteq \pi(\mathfrak{u})$. Weiter liefert die Annahme $\pi(\mathfrak{m}) = \pi(\mathfrak{u})$ mit $I \subseteq \mathfrak{m}, \mathfrak{u}$ die Gleichung

$$\mathfrak{m} = \pi^{-1}(\pi(\mathfrak{m})) = \pi^{-1}(\pi(\mathfrak{u})) = \mathfrak{u},$$

ein Widerspruch. Damit gilt $\mathfrak{n} \subsetneq \pi(\mathfrak{u})$ und Maximalität von $\mathfrak{n}$ liefert $\pi(\mathfrak{u}) = R/I$. Das heißt $\mathfrak{u} = \pi^{-1}(\pi(\mathfrak{u})) = \pi^{-1}(R/I) = R$ und $\mathfrak{m}$ ist maximal.

□

Definition. Zwei Ideale I, J eines kommutativen Rings R heißen **teilerfremd**, falls $I + J = R$ gilt.

Bemerkungen 3.2.9. (1) Sind $\mathfrak{m}, J$ Ideale von R mit $\mathfrak{m}$ maximal, so gilt entweder $J \subseteq \mathfrak{m}$ oder $\mathfrak{m}$ und J sind teilerfremd.

(2) Der Satz von Bézout zeigt, dass zwei Ideale $(n), (m)$ von $\mathbb{Z}$ genau dann teilerfremd sind, wenn $\mathrm{ggT}(m, n) = 1$ gilt.

[2] Äquivalent zum Zornschen Lemma ist die Aussage des Auswahlaxioms: Ist A eine Menge von nichtleeren Mengen, so existiert stets eine **Auswahlfunktion**, d.h. eine Funktion $F\colon A \longrightarrow \bigcup_{X \in A} X$ mit $F(X) \in X$ für alle $X \in A$. Weitere Informationen und der Zusammenhang zum Axiomensystem **ZFC** finden sich zum Beispiel in [2, Kapitel VIII]. Das Zornsche Lemma wird auch verwendet um zu zeigen, dass jeder (auch unendlich dimensionale) k-Vektorraum eine Basis besitzt (vgl. [5, 4.2.15]).

Satz 3.2.10 (Satz von Sun/Qin[a]). *Es sei R ein kommutativer Ring, $I_1, \ldots, I_n \subseteq R$ paarweise teilerfremde Ideale von R. Dann gilt:*

(1) Für jedes $j \in \{1, \ldots, n\}$ sind die Ideale I_j und $I_1 I_2 \cdots I_{j-1} I_{j+1} \cdots I_n$ teilerfremd.

(2) Es gilt $\bigcap_{i=1}^n I_j = I_1 I_2 \cdots I_n$.

(3) Der Homomorphismus $\varphi : R \longrightarrow \prod_{j=1}^n R/I_j \; ; \; x \mapsto (x + I_1, \ldots, x + I_n)$ ist surjektiv mit $\ker \varphi = \bigcap_{j=1}^n I_j$.

(4) Es gilt $R/(\bigcap_{j=1}^n I_j) \cong \prod_{j=1}^n R/I_j$.

[a] Benannt nach den chinesischen Mathematikern Sun, Zi und Qin, Jiushao (1202-1261). Bekannter ist der Satz als chinesischer Restsatz.

Beweis.

(1) Sei $j \in \{1, \ldots, n\}$. Nach Voraussetzung gibt es für jedes $i \neq j$ Elemente $x_i \in I_j$ und $y_i \in I_i$ mit $x_i + y_i = 1$. Damit folgt $1 = \prod_{i \neq j}(x_i + y_i)$. Es sei $\pi : R \longrightarrow R/I_j$ die kanonische Projektion. Dann erhalten wir

$$\pi(1) = \prod_{i \neq j} \pi(x_i + y_i) = \prod_{i \neq j} \pi(y_i) = \pi(\prod_{i \neq j} y_i)$$

und damit $1 - \prod_{i \neq j} y_i \in \ker \pi = I_j$. Also existiert $z \in I_j$ derart, dass

$$1 = z + \prod_{i \neq j} y_i \in I_j + \prod_{i \neq j} I_i.$$

(2) Aus den Definitionen folgt $\prod_{j=1}^n I_j \subseteq \bigcap_{j=1}^n I_j$ (auch wenn die I_j nicht paarweise teilerfremd sind). Für die Inklusion $\bigcap_{j=1}^n I_j \subseteq \prod_{j=1}^n I_j$ verwenden wir Induktion nach n. Sei $n = 2$ sowie $x \in I_1 \cap I_2$. Nach Voraussetzung gilt $1 = x_1 + x_2$ für geeignete $x_i \in I_i$. Also folgt $x = x x_1 + x x_2 \in I_1 I_2$.

Für $n > 2$ betrachten wir $J := I_2 \cdots I_n$. Nach (1) sind die Ideale I_1 und J teilerfremd und der Fall $n = 2$ liefert somit $I_1 \cap J \subseteq I_1 J = \prod_{j=1}^n I_j$. Aufgrund der Induktionsannahme gilt zudem $\bigcap_{j=2}^n I_j \subseteq J$. Damit folgt $\bigcap_{j=1}^n I_j = I_1 \cap J \subseteq \prod_{j=1}^n I_j$.

(3) Nach Definition von φ folgt $\ker \varphi = \bigcap_{j=1}^n I_j$. Für $n = 1$ ist φ surjektiv. Sei nun $n \geq 2$. Für $j \in \{1, \ldots, n\}$ betrachten wir $\mathfrak{I}_j := \bigcap_{i \neq j} I_i$. Nach (1) und (2) sind die Ideale I_j und $\mathfrak{I}_j$ teilerfremd und es gibt $u_j \in I_j$ und $v_j \in \mathfrak{I}_j$ mit $u_j + v_j = 1$. Für $l \neq j$ gilt insbesondere $v_j + I_l = I_l$, da $v_j \in \mathfrak{I}_j \subseteq I_l$.

Seien nun $x_1, \ldots, x_n \in R$. Wir setzen $x := \sum_{j=1}^n x_j v_j$. Für $\ell \in \{1, \ldots, n\}$ erhalten wir

$$x + I_\ell = \sum_{j=1}^n x_j v_j + I_\ell = x_\ell v_\ell + I_\ell = x_\ell - x_\ell u_\ell + I_\ell = x_\ell + I_\ell.$$

Damit folgt $\varphi(x) = (x_1 + I_1, \ldots, x_n + I_n)$. Also ist φ surjektiv.

(4) Da φ surjektiv ist mit $\ker \varphi = \bigcap_{j=1}^{n} I_j$, induziert φ einen Isomorphismus

$$\bar{\varphi} : R/(\bigcap_{j=1}^{n} I_j) \xrightarrow{\sim} \prod_{j=1}^{n} R/I_j.$$

□

Beispiel. Wir stellen uns folgende Frage: Existiert ein $x \in \mathbb{Z}$ das die Kongruenzgleichungen

$$x \equiv 3 \bmod(5), x \equiv 2 \bmod(6), x \equiv 4 \bmod(7)$$

erfüllt? Die Ideale $(5), (6), (7)$ von $\mathbb{Z}$ sind paarweise teilerfremd. Nach Satz 3.2.10 ist

$$\bar{\varphi}\colon \mathbb{Z}/(210) \longrightarrow \mathbb{Z}/(5) \times \mathbb{Z}/(6) \times \mathbb{Z}/(7)$$

$$z + (210) \mapsto (z + (5), z + (6), z + (7))$$

ein Isomorphismus. Insbesondere existiert ein $x \in \mathbb{Z}$ mit

$$(x + (5), x + (6), x + (7)) = (3 + (5), 2 + (6), 4 + (7)).$$

Gemäß dem Beweis von 3.2.10(3) lässt sich eine Lösung wie folgt bestimmen. Wir verwenden den erweiterten euklidischen Algorithmus und erhalten die Gleichungen

$$\begin{aligned} 1 &= 17 \cdot 5 + (-2) \cdot (6 \cdot 7) \\ 1 &= 6 \cdot 6 + (-1) \cdot (5 \cdot 7) \\ 1 &= 13 \cdot 7 + (-3) \cdot (5 \cdot 6). \end{aligned}$$

Damit ist

$$x := 3 \cdot (-2) \cdot (6 \cdot 7) + 2 \cdot (-1) \cdot (5 \cdot 7) + 4 \cdot (-3) \cdot (5 \cdot 6) = -682$$

eine Lösung der drei Kongruenzgleichungen. Die Lösungsmenge wird daher durch

$$\{-682 + 210m \mid m \in \mathbb{Z}\}$$

beschrieben.

Definition. Für $n \in \mathbb{N}$ sei

$$\varphi(n) := |\{s \in \{1, \ldots, n\} \mid \mathrm{ggT}(s, n) = 1\}|.$$

Die Funktion $\varphi\colon \mathbb{N} \longrightarrow \mathbb{N}; n \mapsto \varphi(n)$ heißt **Eulersche φ-Funktion**.

Mithilfe des chinesischen Restsatzes lässt sich folgende Konsequenz ziehen.

Korollar 3.2.11.

(1) Es $p \in \mathbb{P}$ eine Primzahl und $a \in \mathbb{N}$ kein Vielfaches von p. Dann gilt $a^{p-1} \equiv 1 \mod (p)$.

(2) Es sei $n \in \mathbb{N}_{\geq 2}$ und $a \in \mathbb{N}$. Es ist $a+(n)$ genau dann eine Einheit in $\mathbb{Z}/(n)$, wenn $\mathrm{ggT}(a,n) = 1$ gilt.

(3) Für alle $n, m \in \mathbb{N}$ teilerfremd gilt $\varphi(nm) = \varphi(n)\varphi(m)$.

Beweis. Übung. □

Beispiel. Nach Korollar 3.2.11 ist $6 + (23)$ eine Einheit in $\mathbb{Z}/(23)$. Division mit Rest liefert eine Darstellung

$$4 \cdot 6 + (-1) \cdot 23 = 1$$

Wir erhalten $(4 + (23)) \cdot (6 + (23)) = 1 + 23 + (23) = 1 + (23) = 1_{\mathbb{Z}/(23)}$. Damit ist $4 + (23)$ das Inverse zu $6 + (23)$.

Beispiel (RSA-Verfahren)**.** Alice erwartet von Bob (übliche Namen in Texten zur Verschlüsselung) eine Nachricht, möchte aber vermeiden, dass jemand der die Nachricht abfängt, diese verstehen kann. Beide haben keine Möglichkeit auf einem abhörsicheren Weg miteinander zu kommunizieren. Alice hat in der Algebra I LAG Vorlesung aufgepasst und geht deshalb wie folgt vor:

(1) Alice wählt zwei sehr große Primzahlen und $p < q$ und bildet $n := pq$. Nach Korollar 3.2.11 gilt $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$. Alice wählt zusätzlich eine Zahl $1 < e < \varphi(n)$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$ (existiert da $\mathrm{ggT}(\varphi(n), \varphi(n) - 1) = 1$) und berechnet wie im vorherigen Beispiel die eindeutige Zahl $1 \leq d < n$ mit $(d + (\varphi(n)))(e + (\varphi(n))) = 1_{\mathbb{Z}/(\varphi(n))}$

Das Element d heißt **private key** und wird, genauso wie p, q, nicht öffentlich gemacht.

(2) Nun schickt Alice ihrem Freund Bob folgende Nachricht: "Mein **public key** ist (e, n). Wenn Du mir eine Nachricht schicken willst, gehe wie folgt vor:

(i) Codiere Deine Nachricht mit den Zahlen $01, \ldots, 26, 27$, wobei $01 = a, 02 = b, \ldots, 26 = z$, 27 = „Leerzeichen" in eine Zahlenfolge der Form $c_1, \ldots, c_\ell$, etwa:

$$\text{ja bob} = 10, 01, 27, 02, 15, 02.$$

(ii) Berechne die eindeutigen Elemente $0 \leq x_i < n$ mit $c_i^e \equiv x_i \bmod(n)$.

(iii) Sende mir die Folge $x_1, \ldots, x_\ell$ zu."

(3) Alice erhält von Bob eine Folge $x_1, \ldots, x_\ell$ und bestimmt die eindeutigen Elemente $0 \leq y_i < n$ mit

$$x_i^d \equiv y_i \bmod(n).$$

und übersetzt die Zahlenfolge $y_1, \ldots, y_\ell$ wie in (2) beschrieben wieder in eine Nachricht.

Behauptung: Es gilt $y_i = c_i$ für alle $i \in \{1, \dots, \ell\}$.

Begründung: Nach Wahl von d, gilt $ed - 1 \in (\varphi(n))$, das heißt es $(p-1)(q-1) = \varphi(n)$ teilt $ed-1$ und es existieren $a_p, a_q \in \mathbb{N}$ mit $a_p(p-1) = ed - 1 = a_q(q-1)$. Es gilt

$$(c_i^e)^d = c_i^{ed-1+1} = c_i^{a_p(p-1)} c_i = (c_i^{p-1})^{a_p} c_i \overset{3.2.11}{\equiv} 1^{a_p} c_i = c_i \bmod(p)^3.$$

Analog gilt $(c_i^e)^d \equiv c_i \bmod(q)$. Es folgt $p, q \mid (c_i^e)^d - c_i$ und da p, q teilerfremd sind, folgt $(c_i^e)^d \equiv c_i \bmod(n)$. Es folgt

$$y_i \equiv x_i^d \equiv (c_i^e)^d \equiv c_i \bmod(n)$$

und $0 \leq y_i, c_i < n$ liefert $y_i = c_i$.

Das RSA-Verfahren wird zur Zeit als sicher eingestuft. Der Grund ist, dass zum jetzigen Zeitpunkt keine effiziente Methode existiert eine große Zahl n in Primfaktoren zu zerlegen (selbst wenn bekannt ist, dass n Produkt von nur zwei Primfaktoren ist) oder $\varphi(n)$ zu berechnen. Ebenso existiert aktuell keine Methode effizient die e-te Wurzel modulo n zu berechnen.

Wenn eine dritte Person die Nachricht von Alice und Bob und abfängt, hat diese folgende Informationen: $e, n, x_1, \dots, x_\ell$. Selbst wenn die Person zusätzlich weiß, dass Alice das RSA-Verfahren verwendet, ist d unbekannt und müsste aus e und n errechnet werden. Dafür wird die Primfaktorzerlegung von n bzw. $\varphi(n)$ benötigt. Ebenso ist das Rückrechnen $c_i \equiv x_i^e \bmod(n)$ nicht effizient möglich.

3.3 Der Quotientenkörper

In diesem Abschnitt wird die Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ auf Integritätsbereiche verallgemeinert.

Lemma 3.3.1. *Es sei R ein Integritätsbereich. Dann definiert*

$$(r_1, d_1) \sim (r_2, d_2) \quad :\Leftrightarrow \quad r_1 d_2 = r_2 d_1$$

auf $R \times (R \setminus \{0\})$ eine Äquivalenzrelation.

Beweis. Übungsaufgabe. □

Für $(r, d) \in R \times (R \setminus \{0\})$ setzen wir

$$\frac{r}{d} := [(r, d)]$$

für die Äquivalenzklasse von (r, d). Die Menge der Äquivalenzklassen wird mit $Q(R)$ bezeichnet.

Satz 3.3.2. *Es sei R ein Integritätsbereich. Dann erhält $Q(R)$ durch*

$$\frac{r_1}{d_1} + \frac{r_2}{d_2} := \frac{r_1 d_2 + r_2 d_1}{d_1 d_2} \quad \textit{sowie} \quad \frac{r_1}{d_1} \cdot \frac{r_2}{d_2} = \frac{r_1 r_2}{d_1 d_2}$$

[3] Da p sehr groß gewählt wurde, gilt insbesondere $p \nmid c_i \neq 0$.

für $r_1, r_2 \in R$ und $d_1, d_2 \in R \setminus \{0\}$ die Struktur eines Körpers mit $0_{Q(R)} = \frac{0}{1}$ und $1_{Q(R)} = \frac{1}{1}$.

Beweis. Wir müssen uns zunächst darüber Gedanken machen, ob die Addition und Multiplikation unabhängig von der Wahl des Repräsentanten sind. Wir zeigen exemplarisch die Wohldefiniertheit der Addition. Seien $r_i \in R, d_i \in R \setminus \{0\}$ für $1 \leq i \leq 4$ mit $(r_1, d_1) \sim (r_3, d_3)$ und $(r_2, d_2) \sim (r_4, d_4)$. Es gilt $r_1 d_3 - r_3 d_1 = 0 = r_2 d_4 - r_4 d_2$. Es folgt

$$\begin{aligned}[(d_1 d_2)(r_3 d_4 + r_4 d_3) - (d_3 d_4)(r_1 d_2 + r_2 d_1)] &= (d_2 d_4)(r_3 d_1 - r_1 d_3) + (d_1 d_3)(r_2 d_4 - r_4 d_2) \\ &= 0 + 0 = 0.\end{aligned}$$

Dies zeigt $(r_1 d_2 + r_2 d_1, d_1 d_2) \sim (r_3 d_4 + r_4 d_3, d_3 d_4)$. Analog zeigt man, dass die Addition unabhängig von Repräsentanten ist.

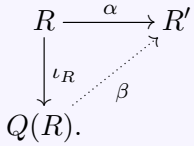
Direkte Rechnung zeigt nun, dass $Q(R)$ ein kommutativer Ring ist. Es gilt $\frac{0}{1} \neq \frac{1}{1}$, da $0 \cdot 1 \neq 1 \cdot 1$ und damit $Q(R) \neq \{0\}$. Es sei $\frac{r}{d} \in Q(R) \setminus \{0\}$. Dann gilt $r \neq 0$, also $\frac{d}{r} \in Q(R)$ mit $\frac{d}{r} \cdot \frac{r}{d} = \frac{rd}{rd} = 1_{Q(R)}$.

□

Definition. Sei R ein Integritätsbereich, so bezeichnen wir mit ι_R den injektiven Ringhomomorphismus

$$\iota_R \colon R \longrightarrow Q(R) \;\; ; \;\; r \mapsto \frac{r}{1}.$$

Satz 3.3.3 (Die universelle Eigenschaft des Quotientenkörpers)**.** *Es sei R ein Integritätsbereich sowie $\alpha : R \longrightarrow R'$ ein Homomorphismus kommutativer Ringe derart, dass $\alpha(R \setminus \{0\}) \subseteq (R')^\times$. Dann existiert genau ein Homomorphismus $\beta : Q(R) \longrightarrow R'$ mit $\beta \circ \iota_R = \alpha$. Wir erhalten also das kommutative Diagram*



Beweis. Da $\alpha(R \setminus \{0\}) \subseteq (R')^\times$ gilt, ist folgende Zuordnung eine wohldefinierte Abbildung

$$\bar{\alpha} : R \times (R \setminus \{0\}) \longrightarrow R' \;\; ; \;\; (r, d) \mapsto \alpha(r)\alpha(d)^{-1}.$$

Wir gehen schrittweise vor.

- $\bar{\alpha}$ ist konstant auf Äquivalenzklassen: Angenommen $(r_1, d_1) \sim (r_2, d_2)$. Dann gilt $r_1 d_2 = r_2 d_1 = 0$, also $\alpha(r_1)\alpha(d_2) = \alpha(r_2)\alpha(d_1)$. Wegen $\alpha(d_i) \in (R')^\times$ erhalten wir

$$\bar{\alpha}(r_1, d_1) = \alpha(r_1)\alpha(d_1)^{-1} = \alpha(r_2)\alpha(d_2)^{-1} = \bar{\alpha}(r_2, d_2).$$

- Definition von β: Da $\bar{\alpha}$ konstant auf Äquivalenzklassen ist, ist

$$\beta : Q(R) \longrightarrow R' \;\; ; \;\; \frac{r}{d} \mapsto \alpha(r)\alpha(d)^{-1}$$

eine wohldefinierte Abbildung. Insbesondere gilt $[\beta \circ \iota_R](r) = \beta(\frac{r}{1}) = \alpha(r)$ für alle $r \in R$. Direktes Nachrechnen zeigt, dass β ein Homomorphismus ist.

- Eindeutigkeit der Abbildung: Sei nun $\gamma : Q(R) \longrightarrow R'$ ein weiterer Homomorphismus mit $\gamma \circ \iota_R = \alpha$. Dann gilt für $(r, d) \in R \times (R \setminus \{0\})$

$$\alpha(d)\gamma(\frac{r}{d}) = \gamma(\iota_R(d))\gamma(\frac{r}{d}) = \gamma(\frac{d}{1}\frac{r}{d}) = \gamma(\frac{r}{1}) = \gamma(\iota_R(r)) = \alpha(r)$$

und somit $\gamma(\frac{r}{d}) = \alpha(r)\alpha(d)^{-1} = \beta(\frac{r}{d})$.

□

Korollar 3.3.4. *Es gelten die folgenden Aussagen.*

(1) Es gilt $Q(\mathbb{Z}) \cong \mathbb{Q}$.

(2) Sei K ein Körper mit $\mathrm{char}(K) = 0$. Dann existiert ein injektiver Homomorphismus $\iota : \mathbb{Q} \hookrightarrow K$.

(3) Sei K ein Körper, dann gilt $K \cong Q(K)$.

Beweis.

(1) Die Abbildung $\alpha\colon \mathbb{Z} \longrightarrow \mathbb{Q}, z \mapsto z$ erfüllt die Voraussetzungen von Satz 3.3.3. Damit existiert ein Ringhomomorphismus $\beta\colon Q(\mathbb{Z}) \longrightarrow \mathbb{Q}, \frac{r}{d} \mapsto \frac{r}{d}$. Dieser ist offensichtlich bijektiv.

(2) Wir betrachten $\alpha : \mathbb{Z} \longrightarrow K ; n \mapsto n1$. Wegen $\mathrm{char}(K) = 0$ ist α injektiv und es folgt $\alpha(\mathbb{Z} \setminus \{0\}) \subseteq K \setminus \{0\} = K^\times$. Damit gibt es nach Satz 3.3.3 einen Homomorphismus $\beta : Q(\mathbb{Z}) \longrightarrow K$ mit $\beta \circ \iota_{\mathbb{Z}} = \alpha$. Da $Q(\mathbb{Z})$ ein Körper ist, ist β nach Satz 3.2.1 injektiv. Nun wenden wir (1) an.

(3) Die Abbildung $\alpha\colon K \longrightarrow K, a \mapsto a$ erfüllt die Voraussetzung von Satz 3.3.3 und wir erhalten einen eindeutig bestimmten Ringhomomorphismus $\beta\colon Q(K) \longrightarrow K$ mit $\beta \circ \iota_K = \alpha$. Da α surjektiv ist, gilt dies auch für β. Weiter ist $Q(K)$ ein Körper und damit β injektiv nach Satz 3.2.1.

□

3.4 Teilbarkeit in Integritätsbereichen

Definition. Es sei R ein Integritätsbereich.

(1) Seien $a, b \in R$. Man sagt a **teilt** b (wir schreiben in diesem Fall wie bereits in $\mathbb{Z}$ nur $a|b$), falls es ein $t \in R$ mit $b = ta$ gibt.

(2) Seien $a, b \in R$. Dann heißen a und b **assoziiert**, falls $a|b$ und $b|a$ gilt. Man schreibt dann $a \sim b$.

Bemerkungen 3.4.1. Es sei R ein Integritätsbereich.

(1) Es gilt $a|b \Leftrightarrow (b) \subseteq (a)$.

(2) Zwei Elemente $a, b \in R$ sind genau dann assoziiert, wenn es ein $u \in R^\times$ mit $b = ua$ gibt: Angenommen $a|b$ und $b|a$ dann gibt es $s, t \in R$ mit $b = sa$ und $a = tb$. Gilt $b = 0$, so folgt $a = 0$ und somit $b = 1 \cdot a$ mit $1 \in R^\times$. Andernfalls erhalten wir aus $b = sa = stb$ die Gleichung

$$b(1 - st) = 0,$$

und damit folgt $1 = st$, da R ein Integritätsbereich ist. Das heißt $s, t \in R^\times$ und $u := s$ liefert das Gewünschte.

Definition. Sei R ein Integritätsbereich und $p \in R \setminus (\{0\} \cup R^\times)$.

(1) Das Element p heißt **irreduzibel** (oder **unzerlegbar**), falls für alle $a, b \in R$ mit $p = ab$ schon $a \in R^\times$ oder $b \in R^\times$ gilt.

(2) Das Element p heißt **prim** oder **Primelement**, falls für alle $a, b \in R$ mit $p|ab$ schon $p|a$ oder $p|b$ folgt.

Beispiele. (1) Sei $p \in R$ ein Primelement. Gilt $p = ab$, so folgt ohne Einschränkung $p|a$. Wegen $a|p$ sind a und p zueinander assoziiert und es gibt $u \in R^\times$ mit $p = ua$. Damit folgt $a(u-b) = 0$ und wegen $a \neq 0$ gilt $b = u \in R^\times$. Also ist p unzerlegbar.

(2) In den Übungen haben wir gesehen, dass in $\mathbb{Z}$ die Begriffe prim und irreduzibel übereinstimmen. Die irreduziblen Elemente sind genau die Elemente in $\pm\mathbb{P}$.

(3) Wir betrachten den Unterring

$$\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Dann ist $\mathbb{Z}[\sqrt{-5}]$ ein Integritätsbereich. Wir betrachten die (multiplikative) Abbildung

$$\mathcal{N}\colon \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}, a + b\sqrt{5}i \mapsto |a + b\sqrt{5}i|^2 = a^2 + 5b^2 \in \mathbb{Z}.$$

Es gelte $2 = (x_1 + y_1\sqrt{5}i)(x_2 + y_2\sqrt{5}i)$. Dann folgt

$$\begin{aligned} 4 &= \mathcal{N}(2) = \mathcal{N}(x_1 + y_1\sqrt{5}i)\mathcal{N}(x_2 + y_2\sqrt{5}i) = (x_1^2 + 5y_1^2)(x_2^2 + 5y_2^2) \\ &\geq 25y_1^2y_2^2 + 5x_1^2y_2^2 + 5x_2^2y_1^2. \end{aligned}$$

Also erhalten wir $y_1 = 0 = y_2$, $4 = (x_1x_2)^2$ und ohne Beschränkung $x_1 \in \{\pm 1\}$, das heißt $x_1 + y_1\sqrt{5}i = x_1 \in \mathbb{Z}[\sqrt{-5}]^\times$. Weiter ist $2 \in \mathbb{Z}[\sqrt{-5}]$ keine Einheit, da $\mathcal{N}(2) \neq 1$. Somit ist 2 irreduzibel in $\mathbb{Z}[\sqrt{-5}]$. Jedoch ist 2 kein Primelement: Es gilt $2|6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$, aber $2 \nmid (1 \pm \sqrt{5}i)$, da $\mathcal{N}(2) = 4$ und $\mathcal{N}(1 \pm \sqrt{5}) = 6$.

Definition. Sei R ein Integritätsbereich.

(1) R heißt **euklidisch**, falls eine Abbildung $\rho : R \setminus \{0\} \longrightarrow \mathbb{N}_0$ existiert, sodass für alle $a, b \in R$, $b \neq 0$ Elemente $q, r \in R$ mit $a = qb + r$ und $r = 0$ oder $\rho(r) < \rho(b)$ existieren.

(2) R heißt **Hauptidealring**, falls für jedes Ideal $I \subseteq R$ ein $x \in R$ mit $I = (x)$ existiert.

(3) R heißt **faktoriell**, falls gilt

(i) Für jedes $a \in R \setminus (\{0\} \cup R^\times)$ gibt es irreduzible Elemente $p_1, \ldots, p_n$ mit $a = p_1 p_2 \cdots p_n$.

(ii) Gilt $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ mit $p_i, q_j \in R$ irreduzibel, so gilt $m = n$ und es gibt eine Permutation $\sigma \in \mathcal{S}_n$ mit $q_i \sim p_{\sigma(i)}$ für jedes $i \in \{1, \ldots, n\}$.

Im verbleibenden Abschnitt beweisen wir den folgenden Satz.

Satz 3.4.2. *Es sei R ein Ring. Es gilt*

$$R \text{ euklidischer Ring} \Longrightarrow R \text{ Hauptidealring} \Longrightarrow R \text{ faktorieller Ring} \Longrightarrow R \text{ Integritätsbereich.}$$

Satz 3.4.3. *Sei R ein euklidischer Ring. Dann ist R ein Hauptidealring.*

Beweis. Da R ein Integritätsbereich ist, müssen wir lediglich zeigen, dass jedes Ideal $I \subseteq R$ ein Hauptideal ist. Sei $I \neq \{0\}$. Dann gibt es $r_0 \in I \setminus \{0\}$ derart, dass

$$\rho(r_0) = \min\{\rho(r) \mid r \in I \setminus \{0\}\}.$$

Sei nun $x \in I$. Dann gibt es $q, r \in R$ mit $x = qr_0 + r$ und $r = 0$ oder $\rho(r) < \rho(r_0)$. Wegen $r = x - qr_0 \in I$ folgt nach Wahl von r_0, dass $r = 0$ gilt. Also gilt $x \in (r_0)$ und damit $I = (x_0)$. □

Bemerkung 3.4.4. Nicht jeder Hauptidealring ist ein euklidischer Ring. Ein Beispiel dafür ist der Ring

$$R := \{a + \frac{1 + i\sqrt{19}}{2} b \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Der Beweis ist nicht trivial. Wir verweisen daher nur auf [6].

Satz 3.4.5. *Es sei R ein Ring.*

(1) Ist R faktoriell, so ist jedes irreduzible Element prim (d.h. irreduzibel = prim).

(2) Ist R ein Integritätsbereich, so sind folgende Aussagen äquivalent.[a]

(i) R ist ein faktorieller Ring.

(ii) Für jede Nichteinheit $0 \neq r \in R$ existieren $n \in \mathbb{N}$ und $p_1, \ldots, p_n$ Primelemente mit $r = p_1 p_2 \cdots p_n$.

(3) Ist R ein Hauptidealring, so ist jedes Primideal $\mathfrak{p} \neq \{0\}$ maximal und jedes irreduzible Element bereits prim.

[a] Der Beweis verläuft analog zum Beweis von Satz 1.1.3

Beweis.

(1) Sei $p \in R$ irreduzibel und $a, b \in R$ mit $p \mid ab$. Wir wollen $p \mid a$ oder $p \mid b$ zeigen und können ohne Beschränkung $a, b \notin \{0\} \cup R^\times$ annehmen und schreiben $ab = pc$ für ein $c \in R \setminus \{0\}$. Da R faktoriell ist, existieren $m, n \in \mathbb{N}$ sowie irreduzible Elemente $p_1, \ldots, p_n, q_1, \ldots, q_m$ mit $a = p_1 \cdot \cdots \cdot p_n$ und $b = q_1 \cdot \cdots \cdot q_m$. Da R faktoriell und p irreduzibel ist, folgt aus $m+n \geq 2$, dass c keine Einheit ist und wir finden $l \in \mathbb{N}$ und irreduzible Elemente $s_1, \ldots, s_l$ mit $c = s_1 \cdot \cdots \cdot s_l$. Da R faktoriell ist, folgt ohne Beschränkung der Allgemeinheit $p \sim p_1$, d.h. $p \mid a$.

(2) (i) $\Rightarrow$ (ii). Dies folgt direkt aus (i).

(ii) $\Rightarrow$ (i). Es sei $0 \neq r \in R$ keine Einheit. Nach Annahme finden wir eine Zerlegung $r = p_1 \cdots p_n$ mit $p_1, \ldots, p_n$ Primelementen. Insbesondere existiert also eine Zerlegung in irreduzible Elemente. Es seien $q_1, \ldots, q_m$ irreduzible Elemente mit $p_1 \cdots p_n = r = q_1 \cdots q_m$. Wir zeigen die Eindeutigkeit der Zerlegung (bis auf Einheiten und Umnummerierung) durch Induktion nach n.

Gilt $n = 1$, so folgt $p_1 = q_1(q_2 \cdots q_m)$. Da p_1 irreduzibel und q_1 keine Einheit ist, ist der zweite Faktor eine Einheit, was $m = 1$ impliziert. Sei $n > 1$. Da p_n ein Primelement ist, gibt es ein $j_n \in \{1, \ldots, m\}$ $p_n | q_{j_n}$. Da q_{j_n} irreduzibel und p_n keine Einheit ist, existiert eine Einheit u mit $q_{j_n} = up_n$ und es folgt $p_n \sim q_{j_n}$. Da R ein Integritätsbereich ist, erhalten wir zudem

$$p_1 \cdots p_{n-1} = uq_1 \cdots q_{j_n-1} q_{j_n+1} \cdots q_m.$$

Da uq_1 irreduzibel ist, folgt nach Induktionsannahme $n - 1 = m - 1$. Ebenso erhalten wir eine Bijektion $\tau : \{1, \ldots, n-1\} \longrightarrow \{1, \ldots, n\} \setminus \{j_n\}$ mit $p_i \sim q_{\tau(i)}$ für $1 \leq i \leq n-1$. Wir definieren nun $\sigma \in \mathcal{S}_n$ durch

$$\sigma(i) := \begin{cases} \tau(i) & i \neq n \\ j_n & i = n. \end{cases}$$

Dann gilt $p_i \sim q_{\sigma(i)}$ für $1 \leq i \leq n$.

(3) Sei $\mathfrak{p} \neq \{0\}$ ein Primideal. Da R ein Hauptidealring ist, gilt $\mathfrak{p} = (p)$, wobei $p \in R$ ein Primelement ist. Satz 3.2.8 liefert ein maximales Ideal $\mathfrak{m} \supseteq (p)$. Da R ein Hauptidealring ist, gibt es $q \in R$ mit $\mathfrak{m} = (q)$. Wegen $p \in \mathfrak{m}$ gibt es $r \in R$ mit $p = rq$. Da q aufgrund von $\mathfrak{m} \neq R$ keine Einheit ist, impliziert die Unzerlegbarkeit von p dass r eine Einheit ist. Damit ist $(p) = (rq) = (q) = \mathfrak{m}$ ein maximales Ideal. Sei nun $p_0 \in R$ irreduzibel. Dann ist $(p_0) \neq R$ und wir finden mit analogen Elementen ein Primelement q_0 mit $q_0 | p_0$. Die Irreduzibilität von p_0 liefert $p_0 \sim q_0$. Also ist q_0 ein Primelement.

□

Satz 3.4.6. *Sei R ein Hauptidealring. Dann ist R faktoriell.*

Beweis. Sei $a \in R \setminus (\{0\} \cup R^\times)$. Wir zeigen, dass a ein Produkt von Primelementen ist. Angenommen es existiert keine solche Zerlegung. Wegen $a \in R \setminus (\{0\} \cup R^\times)$ gilt $\{0\} \subsetneq (a) \subsetneq R$ und nach Satz 3.2.8

gibt es ein maximales Ideal $\mathfrak{m}_1 \subseteq R$ mit $(a) \subseteq \mathfrak{m}_1$[4]. Da R ein Hauptidealring ist, gilt $\mathfrak{m}_1 = (p_1)$ für ein Primelement $p_1 \in R$. Wegen $a \in \mathfrak{m}_1$ gibt es $a_1 \in R$ mit $a = a_1 p_1$.

Gilt $a_1 \in R^\times$, so ist $a_1 p_1$ ein Primelement und $a = a_1 p_1$, im Widerspruch zu unserer Annahme. Damit gibt es wie oben ein Primelement p_2 und $a_2 \in R$ mit $a_1 = a_2 p_2$. Wegen $a = a_2 p_1 p_2$ ist wie zuvor a_2 keine Einheit. Dies impliziert $(a_1) \subsetneq (a_2) \subsetneq R$. Induktiv erhalten wir eine Folge $(a_i)_{i\in\mathbb{N}}$ von Idealen mit $(a_i) \subsetneq (a_{i+1}) \subsetneq R$ für alle $i \in \mathbb{N}$. Als Kette von echten Idealen ist $\bigcup_{i\in\mathbb{N}}(a_i)$ ein echtes Ideal. Da R ein Hauptideal ist, existiert $b \in R$ mit $(b) = \bigcup_{i\in\mathbb{N}}(a_i)$ und wir finden $n \in \mathbb{N}$ mit $b \in (a_n)$. Dann gilt aber

$$(a_{n+1}) \subseteq \bigcup_{i\in\mathbb{N}}(a_i) = (b) \subseteq (a_n) \subsetneq (a_{n+1}),$$

ein Widerspruch. Nun wenden wir 3.4.5(2) an. □

Bemerkung 3.4.7. Wir werden im Verlauf der Vorlesung zeigen, dass $\mathbb{Z}[X]$ ein faktorieller Ring ist, der kein Hauptidealring ist. Wir haben bereits gesehen, dass $\mathbb{Z}[\sqrt{-5}]$ ein Integritätsbereich ist, der nicht faktoriell ist. Damit sind alle Implikationen in Satz 3.4.2 nicht umkehrbar.

Definition. Es sei R ein Integritätsbereich und $r_1, \dots, r_n \in R$ mit $n \in \mathbb{N}$. Ein Element $a \in R$ heißt ggT (**größter gemeinsamer Teiler**) von $r_1, \dots, r_n$, falls folgende Bedingungen erfüllt sind.

(1) Es gilt $a \mid r_i$ für alle $i \in \{1, \dots, n\}$.

(2) Ist $b \in R$ mit $b \mid r_i$ für alle $i \in \{1, \dots, n\}$, so gilt bereits $b \mid a$.

Wir bezeichnen die Menge der größten gemeinsamen Teiler von $r_1, \dots, r_n$ mit $\mathrm{ggT}(r_1, \dots, r_n)$.

Bemerkung 3.4.8. Sind $a, b \in \mathrm{ggT}(r_1, \dots, r_n)$, so gilt $a|b$ und $b|a$. Das heißt $a \sim b$. Weiter sieht man ein, dass für jeden größten gemeinsamen Teiler $c \in \mathrm{ggT}(r_1, \dots, r_n)$ die Gleichung

$$\mathrm{ggT}(r_1, \dots, r_n) = cR^\times$$

gilt.

Beispiele. (1) In $\mathbb{Z}$ gilt $\mathrm{ggT}(60, 105) = \{\pm 15\} = 15\mathbb{Z}^\times$.

(2) In $\mathbb{Z}[\sqrt{-5}]$ gilt $\mathrm{ggT}(6, 2(1+\sqrt{5}i)) = \varnothing$: Angenommen t ist ein größter gemeinsamer Teiler. Dann gilt $\mathcal{N}(t) \mid 36$ und $\mathcal{N}(t) \mid 24$, das heißt $\mathcal{N}(t) \mid \mathrm{ggT}(36, 24) = 12$. Da 2 und $1+\sqrt{5}i$ Teiler von 6 und $2(1+\sqrt{5}i)$ sind, liefert die ggT-Eigenschaft $2 \mid t$ und $1+\sqrt{5}i \mid t$. Das heißt $4 \mid \mathcal{N}(t)$ und $6 \mid \mathcal{N}(t)$, also $12|\mathcal{N}(t)$. Damit gilt $\mathcal{N}(t) = 12$. Wir schreiben $t = a + b\sqrt{5}i$. Dann gilt $12 = \mathcal{N}(t) = a^2 + 5b^2$. Diese Gleichung besitzt in $\mathbb{Z}^2$ keine Lösung, ein Widerspruch.

(3) Es gilt $r_1 = r_2 = \cdots = r_n = 0 \Leftrightarrow \mathrm{ggT}(r_1, \dots, r_n) = \{0\}$.

[4]Die Existenz eines solchen maximalen Ideals kann in Hauptidealbereichen auch ohne Verwendung des Zornschen Lemma bewiesen werden, da in Hauptidealbereichen aufsteigende Ketten von Idealen stets stationär werden.

Lemma 3.4.9. *Es sei R ein faktorieller Ring und $r_1, \ldots, r_n \in R$. Dann gilt $\varnothing \neq \mathrm{ggT}(r_1, \ldots, r_n)$.*

Beweis. Wir können annehmen, dass ein $1 \leq \ell \leq n$ mit $r_i \neq 0 \Leftrightarrow 1 \leq i \leq \ell$ existiert. Wir fixieren ein Repräsentantensystem $\mathcal{P}$ aller irreduziblen Elemente in R. Da R ein faktorieller Ring ist, finden wir Einheiten u_i und eindeutige Darstellungen

$$r_i = u_i \prod_{p \in \mathcal{P}} p^{m_p(r_i)}$$

für alle $1 \leq i \leq \ell$ mit $m_p(r_i) \in \mathbb{N}_0$ für alle $p \in \mathcal{P}$. Für $p \in \mathcal{P}$ setzen wir

$$m(p) := \min\{p^{m_p(r_i)} \mid i \in \{1, \ldots, \ell\}\}.$$

Man überprüft nun, dass $g := \prod_{p \in \mathcal{P}} p^{m(p)}$ ein größter gemeinsamer Teiler der r_i ist (vgl. Aufgabe 4). □

Definition. Ist R ein faktorieller Ring und $r, s \in R$. Wir sagen r und s sind **teilerfremd**, falls 1 ein größter gemeinsamer Teiler von r, s ist. Dies ist genau dann der Fall, wenn $\mathrm{ggT}(r, s) = R^\times$ gilt.

4 Polynomringe

4.1 Grundlegende Definitionen

Der Begriff des Polynoms ist uns seit der Schule geläufig. Dort werden Polynome häufig mit denen von ihnen induzierten Funktionen gleichgesetzt. Hier muss jedoch unterschieden werden, sobald man nicht mehr nur Polynome mit Koeffizienten in $\mathbb{R}$, $\mathbb{C}$ betrachtet, wie das folgende Beispiel zeigt:

Beispiel. Sei R ein kommutativer Ring und f die Funktion

$$f\colon R \longrightarrow R\,;\; r \mapsto r^2 + r + 1.$$

Für $R = \mathbb{R}$ wird die Funktion f durch das Polynom $x^2 + x + 1$ beschrieben. Mit der später entwickelten Theorie können wir zeigen, dass $x^2 + x + 1$ das einzige Polynom ist, welches die Abbildung beschreibt. Für $R = \mathbb{Z}/(2)$ beschreibt das Polynom $x^2 + x + 1$ weiterhin die Abbildung f. Jedoch beschreiben auch die Polynome 1, $x^2 + x + 1$ und $(x^2 + x + 1)^2$ die Funktion $f\colon \mathbb{Z}/(2) \longrightarrow \mathbb{Z}/(2)\,;\; r \mapsto r^2 + r + 1$.

Im Folgenden sei $R \neq \{0\}$ ein kommutativer Ring und

$$R[X] := \{\sum_{i\in\mathbb{N}_0} a_i X^i \mid a_i \in R, a_i = 0 \text{ für alle bis auf endlich viele } i \in \mathbb{N}_0\}$$

die Menge der Polynome mit Koeffizienten aus R.[1] Auf $R[X]$ erklären wir eine Addition und Multiplikation wie folgt

$$\sum_{i\in\mathbb{N}_0} a_i X^i + \sum_{i\in\mathbb{N}_0} b_i X^i := \sum_{i\in\mathbb{N}_0} (a_i + b_i) X^i,$$

$$\sum_{i\in\mathbb{N}_0} a_i X^i \cdot \sum_{i\in\mathbb{N}_0} b_i X^i := \sum_{i\in\mathbb{N}_0} c_i X^i,$$

wobei $c_i := \sum_{r,s\in\mathbb{N}_0, r+s=i} a_r b_s$. Man rechnet nach, dass $R[X]$ ein kommutativer Ring ist. Wir nennen $R[X]$ den **Polynomring in X über R**. Die Abbildung

$$R \longrightarrow R[X]; a \mapsto a \cdot X^0$$

ist ein injektiver Ringhomomorphismus. Im Folgenden fassen wir daher R Teilring von $R[X]$ auf und schreiben a anstatt $a \cdot X^0$.

[1] Polynome sind hier formale Summen und keine Abbildungen, es gibt also eine natürliche bijektive Abbildung zwischen $R[X]$ und der Menge der R-wertigen Folgen mit endlichem Träger

$$(a\colon \mathbb{N}_0 \longrightarrow R) \mapsto \sum_{i=0} a_i X^i.$$

Definition. Für ein Polynom $f = \sum_{i \in \mathbb{N}_0} a_i X^i \in R[X]$ heißt

$$\deg(f) := \begin{cases} \max\{i \in \mathbb{N}_0 \mid a_i \neq 0\} & , f \neq 0 \\ -\infty & , f = 0 \end{cases}$$

der **Grad** des Polynoms f. Gilt $f \neq 0$, so heißt $a_{\deg(f)}$ der **Leitkoeffizient** von f. Weiter heißt f **normiert**, falls $a_{\deg(f)} = 1$ gilt.

Beispiele.

(1) Das Polynom $7X^6 + 4X^2 + 5 \in \mathbb{Z}[X]$ hat Grad 6 und Leitkoeffizienten 7.

(2) Das Polynom $(1 + (2))X + (1 + (2))X \in \mathbb{Z}/(2)[X]$ hat Grad $-\infty$.

Satz 4.1.1 (Die universelle Eigenschaft des Polynomrings)**.** *Es sei $\varphi : R \longrightarrow S$ ein Homomorphismus kommutativer Ringe und $s \in S$. Dann gibt es genau einen Homomorphismus von Ringen $\tilde{\varphi}_s : R[X] \longrightarrow S$ mit*

(i) $\tilde{\varphi}_s(r) = \varphi(r)$ für alle $r \in R$ und

(ii) $\tilde{\varphi}_s(X) = s$.

Beweis. Ist ψ ein Homomorphismus mit obigen Eigenschaften, so gilt

$$\psi(\sum_{i=0}^{m} r_i X^i) = \sum_{i=0}^{m} \psi(r_i)\psi(X)^i = \sum_{i=0}^{m} \varphi(r_i)s^i$$

für alle Polynome $\sum_{i=0}^{m} r_i X^i \in R[X]$. Insbesondere existiert höchstens ein Homomorphismus mit obigen Eigenschaften, und wir definieren notwendigerweise

$$\tilde{\varphi}_s \colon R[X] \longrightarrow S \,;\, \sum_{i=0}^{m} r_i X^i \mapsto \sum_{i=0}^{m} \varphi(r_i)s^i.$$

Man rechnet nun nach, dass $\tilde{\varphi}_s$ ein Ringhomomorphismus ist. □

4.2 Nullstellen

In diesem Abschnitt studieren wir Nullstellen von Polynomringen.

Satz 4.2.1. *Sei $R \neq \{0\}$ ein kommutativer Ring.*

(1) Es gilt $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$ für alle $f, g \in R[X]$.

(2) Es gilt $\deg(fg) \leq \deg(f) + \deg(g)$ für alle $f, g \in R[X]$.

(3) Ist R ein Integritätsbereich, so gilt $\deg(fg) = \deg(f) + \deg(g)$ für alle $f, g \in R[X]$.

(4) Ist R ein Integritätsbereich, so ist $R[X]$ ein Integritätsbereich und es gilt $R[X]^\times = R^\times$.

Beweis. Wir beweisen lediglich (4). Es seien $f, g \in R[X]$ mit $fg = 0$. Dann gilt nach (3)

$$-\infty = \deg(fg) = \deg(f) + \deg(g)$$

und somit $f = 0$ oder $g = 0$.
Klar ist $R^\times \subseteq R[X]^\times$. Sei $f \in R[X]^\times$ und $g \in R[X]$ mit $fg = 1$. Mit (3) folgt $0 = \deg(f) + \deg(g)$, das heißt $f, g \in R$ und somit $f \in R^\times$. □

Wie für Polynomringe über Körpern (siehe [5, (7.1.12)]) liefert das Verfahren der Polynomdivision:

Satz 4.2.2 (Division mit Rest). *Sei $R \neq \{0\}$ ein kommutativer Ring sowie $g \in R[X] \setminus \{0\}$ ein Polynom, sodass der Leitkoeffizient eine Einheit ist. Dann existieren zu jedem Polynom $f \in R[X]$ eindeutig bestimmte Polynome $q, r \in R[X]$ derart, dass $f = qg + r$ mit $\deg(r) < \deg(g)$ gilt.*

Korollar 4.2.3. *Sei $R \neq \{0\}$ ein kommutativer Ring. Folgende Aussagen sind äquivalent.*

(1) $R[X]$ ist ein euklidischer Ring.

(2) $R[X]$ ist ein Hauptidealring.

(3) R ist ein Körper.

Beweis. (1) ⇒ (2). Dies folgt unmittelbar aus Satz 3.4.3.
(2) ⇒ (3). Der Hauptidealring $R[X]$ ist insbesondere ein Integritätsbereich. Damit ist $R \subseteq R[X]$ ebenfalls ein Integritätsbereich. Nach Satz 4.1.1 gibt es genau einen Homomorphismus $\tilde{\varphi} : R[X] \longrightarrow R$ mit $\tilde{\varphi}(r) = r$ für alle $r \in R$ und $\tilde{\varphi}(X) = 0$. Damit ist $\tilde{\varphi}$ surjektiv und wegen $R[X]/\ker\tilde{\varphi} \cong R$ ist $\mathfrak{p} := \ker\tilde{\varphi}$ ein Primideal von $R[X]$ nach Lemma 3.2.5. Wegen $X \in \mathfrak{p}$ folgt $\mathfrak{p} \neq \{0\}$. Da R Hauptidealring ist, liefert Satz 3.4.5 die Maximalität von $\mathfrak{p}$. Erneute Anwendung von Lemma 3.2.5 zeigt, dass $R \cong R[X]/\mathfrak{p}$ ein Körper ist.
(3) ⇒ (1). Nach Satz 4.2.1 ist $R[X]$ ein Integritätsbereich. Wir definieren

$$R[X] \setminus \{0\} \longrightarrow \mathbb{N}_0, f \mapsto \deg(f).$$

Nach Satz 4.2.2 ist dies eine geeignete Gradfunktion, da R ein Körper ist und damit für jedes Polynom $g \in K[X] \setminus \{0\}$ der Leitkoeffizient eine Einheit ist. □

Definition. Sei $f = \sum_{i=0}^n a_i X^i \in R[X] \setminus \{0\}$. Ein Element $r \in R$ heißt **Nullstelle** von f, falls $\sum_{i=0}^n a_i r^i = 0$ gilt. Die Menge der Nullstellen von f in R sei mit $Z_R(f)$ bezeichnet.

Für $r \in R$ sei

$$\mathrm{ev}_r : R[X] \longrightarrow R\,;\ \sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n a_i r^i$$

der nach Satz 4.1.1 eindeutig bestimmte Homomorphismus mit $\mathrm{ev}_r(a) = a$ für alle $a \in R$ und $\mathrm{ev}_r(X) = r$. Der Homomorphismus ev_r heißt **Auswertungs-** oder **Einsetzungshomomorphismus** in r.
Es ist $r \in R$ eine Nullstelle von $f \in R[X]$ genau dann, wenn $\mathrm{ev}_r(f) = 0$ gilt. Für ein beliebiges Polynom $f = \sum_{i=0}^{n} a_i X^i$ und $r \in R$ schreiben wir von nun an

$$f(r) := \mathrm{ev}_r(f) = \sum_{i=0}^{n} a_i r^i \in R.$$

Satz 4.2.4. *Sei R ein Integritätsbereich. Dann besitzt jedes Polynom $f \in R[X]\backslash\{0\}$ höchstens $\deg(f)$ Nullstellen.*

Beweis. Wir verwenden Induktion nach $\deg(f)$, wobei der Fall $\deg(f) = 0$ trivial ist. Gilt $\deg(f) > 0$ und ist r eine Nullstelle von f, so gibt es nach Satz 4.2.2 $q, a \in R[X]$ derart, dass $f = q(X-r)+a$ mit $a = 0$ oder $\deg(a) < \deg(X-a) = 1$ gilt. Zudem haben wir

$$0 = f(r) = \mathrm{ev}_r(q(X-r)+a) = \mathrm{ev}_r(q)\,\mathrm{ev}_r(X-r) + \mathrm{ev}_r(a) = q(r)(r-r) + a(r) = a(r).$$

Wir schließen damit $a = 0$. Da R ein Integritätsbereich ist, erhalten wir mit Satz 4.2.1 $\deg(q) = \deg(f) - 1$. Weiter gilt $Z_R(f) = Z_R(q) \cup \{r\}$. Die Induktionsannahme liefert uns damit die Behauptung. □

Beispiele. (1) Das Polynom $X^2 + 1$ besitzt in $\mathbb{R}$ keine Nullstelle, in $\mathbb{C}$ hingegen gilt $X^2 + 1 = (X - i)(X + i)$.

(2) Das Polynom $(X-1)(X-2)^2 \in \mathbb{Z}[X]$ hat die Nullstellenmenge $\{1, 2\}$.

Satz 4.2.5. *Es sei K ein Körper und $U \subseteq K^\times$ eine endliche Untergruppe. Dann ist U zyklisch.*

Beweis. Es sei $g \in U$ ein Element maximaler Ordnung $n \in \mathbb{N}$. Nach Satz 2.3.3 gilt $\mathrm{ord}(u) \mid n$ für alle $u \in U$, da $U \subseteq K^\times$ abelsch ist. Also gilt $\langle g \rangle \subseteq U \subseteq Z_K(X^n - 1)$. Nach Satz 4.2.4 enthält $Z_K(X^n - 1)$ höchstens n Elemente. Mit $n = |\langle g \rangle| \leq |U| \leq |Z_K(X^n - 1)| = n$ folgt $\langle g \rangle = U$. □

Definition. (1) Sei $f \in R[X] \setminus \{0\}$ ein Polynom und $r \in R$ eine Nullstelle von f. Dann gilt $(X-r) | f$ und nach Satz 4.2.1 existiert ein $n(r) \in \mathbb{N}_{\leq \deg(f)}$ mit $(X-r)^{n(r)} | f$ und $(X-r)^{n(r)+1} \nmid f$. Dann heißt $n(r)$ die **Vielfachheit** der Nullstelle r. Eine Nullstelle r heißt **einfach**, falls $n(r) = 1$ gilt.

(2) Sei $f = \sum_{i=0}^{n} a_i X^i \in R[X]$. Dann heißt

$$f' := \sum_{i=1}^{n} i a_i X^{i-1} \in R[X]$$

die **Ableitung** von f.

Satz 4.2.6. *Sei K ein Körper, $\alpha \in K$ eine Nullstelle des Polynoms $f \in K[X] \setminus \{0\}$. Dann sind folgende Aussagen äquivalent:*

(1) $n(\alpha) = 1$.

(2) $f'(\alpha) \neq 0$.

Beweis. (1) $\Rightarrow$ (2). Nach Voraussetzung gibt es ein Polynom $q \in K[X]$ mit $f = q(X - \alpha)$ und $q(\alpha) \neq 0$. Die Produktregel liefert $f' = q'(X - \alpha) + q$. Damit erhalten wir $f'(\alpha) = q(\alpha) \neq 0$.
(2) $\Rightarrow$ (1). Sei nun $n(\alpha) \geq 2$. Dann gilt $n(\alpha) - 1 \geq 1$. Wir schreiben $f = q(X - \alpha)^{n(\alpha)}$ mit $q(\alpha) \neq 0$. Damit liefert die Produktregel

$$f' = q'(X - \alpha)^{n(\alpha)} + n(\alpha)q(X - \alpha)^{n(\alpha)-1}.$$

Es folgt $f'(\alpha) = q'(\alpha)(\alpha - \alpha)^{n(\alpha)} + n(\alpha)q(\alpha - \alpha)^{n(\alpha)-1} = 0$. □

Beispiel. Sei K ein Körper, $f = X^n - 1 \in K[X]$ mit $n \geq 2$. Dann gilt $f' = nX^{n-1}$. Ist $a \in K$ eine Nullstelle von f, so folgt $a^n = 1$ und $f'(a) = na^{n-1}$. Die Annahme $f'(a) = 0$ führt zu $n1 = 0$ und damit $\mathrm{char}(K)|n$. Andernfalls ist a eine einfache Nullstelle von f.

4.3 Irreduzible Polynome

In diesem Abschnitt untersuchen wir Polynome in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$ auf Irreduzibilität. Es sei $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in \mathbb{Z}$ mit $a_i \neq 0$ für mindestens ein $i \in \{1, \ldots, n\}$. Da $\mathbb{Z}$ faktoriell ist und $\mathbb{Z}^\times = \{-1, 1\}$ gilt, existiert nach Lemma 3.4.9 genau ein größter gemeinsamer Teiler $0 \neq g \in \mathbb{N}$ von $a_1, \ldots, a_n$. Im Folgenden schreiben wir $\mathrm{ggT}(a_0, \ldots, a_n)$ für diesen größten gemeinsamen Teiler.

Definition. Es sei $0 \neq f = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ ein Polynom.

(1) Die natürliche Zahl $c(f) := \mathrm{ggT}(a_0, \ldots, a_n) \in \mathbb{N}$ heißt **Inhalt von f**.

(2) Das Polynom f heißt **primitiv**, falls $c(f) = 1$ gilt.

Beispiel. (1) Es sei $f = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ und $b_i \in \mathbb{Z}$ die eindeutig bestimmten Elemente mit $b_i \cdot c(f) = a_i$. Das Polynom $f_0 := \sum_{i=0}^n b_i X^i \in \mathbb{Z}[X]$ erfüllt

(i) $f = c(f)f_0$, und

(ii) f_0 ist primitiv: Es sei $c \in \mathbb{N}$ ein Teiler aller b_i. Dann ist $c \cdot c(f)$ ein Teiler von $b_i \cdot c(f) = a_i$ für alle $i \in \{0, \ldots, n\}$. Damit gilt $(c \cdot c(f)) \mid \mathrm{ggT}(a_0, \ldots, a_n) = c(f)$. Es folgt $c = 1$, da $c \in \mathbb{N}$.

(2) Das Polynom $f := -60 \cdot X^3 - 20 \cdot X^2 + 100X$ hat den Inhalt $c(f) = \mathrm{ggT}(-60, -20, 100) = 20$. Es gilt $f = 20 \cdot (-3X^3 - X^2 + 5X)$.

(3) Ein Polynom $0 \neq aX^0 \in \mathbb{Z}[X]$ ist genau dann irreduzibel, wenn $a \in \mathbb{Z}$ irreduzibel (also prim) ist, das heißt $a \in \pm\mathbb{P}$ gilt.

(4) Es sei $f \in \mathbb{Z}[X]$ mit $\deg(f) \geq 1$ irreduzibel. Gilt $c(f) \neq 1$, so ist $f = c(f)f_0$ eine Zerlegung in zwei Nichteinheiten. Damit muss ein irreduzibles Polynom von Grad ≥ 1 primitiv sein.

Achtung: Die Umkehrung gilt nicht, wie schon $f = X^2$ zeigt.

Lemma 4.3.1. *(1) Es sei $p \in \mathbb{Z}$. Dann sind folgende Aussagen äquivalent.*

(i) $p \in \mathbb{Z}$ ist ein Primelement.

(ii) $p \in \mathbb{Z}[X]$ ist ein Primelement.

(2) Sind $f, g \in \mathbb{Z}[X]$ primitiv, so ist $f \cdot g$ primitiv.

Beweis. Wir können o.B.d.A. $p \notin \{-1, 0, 1\}$ annehmen.

(1) (i) $\Rightarrow$ (ii). Es ist $\mathfrak{p} := (p)_{\mathbb{Z}}$ ein Primideal in $\mathbb{Z}$. Wir betrachten die kanonische Projektion $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/\mathfrak{p}$ sowie den induzierten Homomorphismus $\pi^* : \mathbb{Z}[X] \longrightarrow (\mathbb{Z}/\mathfrak{p})[X]$. Sei $g \in \ker \pi^*$, $g = \sum_{i=0}^n r_i X^i$. Dann gilt

$$0 = \pi^*(g) = \sum_{i=0}^{n} \pi(r_i) X^i$$

und daher $r_i \in \ker \pi = \mathfrak{p}$ für $0 \leq i \leq n$. Wir schreiben $r_i = s_i p$ und setzen $h := \sum_{i=0}^n s_i X^i$. Dann gilt $g = ph$ und somit ist $\ker \pi^* = (p)_{\mathbb{Z}[X]}$ das von p in $\mathbb{Z}[X]$ erzeugte Ideal. Also induziert π^* einen Isomorphismus $\mathbb{Z}[X]/(p)_{\mathbb{Z}[X]} \xrightarrow{\sim} (\mathbb{Z}/\mathfrak{p})[X]$. Da $\mathbb{Z}/\mathfrak{p}$ ein Integritätsbereich ist, gilt dies nach Satz 4.2.1 auch für $(\mathbb{Z}/\mathfrak{p})[X]$. Damit ist $(p)_{\mathbb{Z}[X]}$ ein Primideal und p in $\mathbb{Z}[X]$ ein Primelement.

(ii) $\Rightarrow$ (i). Es seien $a, b \in \mathbb{Z}$ mit $p \mid ab$ in $\mathbb{Z}$. Damit wird ab auch von p in $\mathbb{Z}[X]$ geteilt und wir finden nach Voraussetzung o.B.d.A. $h \in \mathbb{Z}[X]$ mit $p \cdot h = a$. Es folgt $\deg(h) = \deg(p) + \deg(h) = \deg(ph) = \deg(a)$. Insbesondere gilt $h \in \mathbb{Z}$.

(2) Ist $f \cdot g$ nicht primitiv, so ist $c(f \cdot g) \in \mathbb{N}_{\geq 2}$ keine Einheit und $f \cdot g = c(f \cdot g) \cdot (f \cdot g)_0$. Da $\mathbb{Z}$ faktoriell ist, existiert $p \in \mathbb{Z}$ Primelement mit $p \mid c(f \cdot g)$. Nach (1) ist $p \in \mathbb{Z}[X]$ ein Primelement. Es gilt $p \mid c(f \cdot g) \cdot (f \cdot g)_0 = f \cdot g$ in $\mathbb{Z}[X]$. Es folgt $p \mid f$ oder $p \mid g$, ein Widerspruch.

□

Satz 4.3.2. *Es sei $0 \neq f \in \mathbb{Z}[X]$.*

(1) Ist $f = f_1 \cdots f_n$ mit $f_1, \ldots, f_n \in \mathbb{Q}[X]$, so existieren $g_1, \ldots, g_n \in \mathbb{Z}[X]$ primitiv und $\lambda_1, \ldots, \lambda_n \in \mathbb{Q}_{>0}$ mit

$$f_i = \lambda_i \cdot g_i \text{ und } \lambda := \lambda_1 \cdots \lambda_n \in \mathbb{N}.$$

(2) Ist f primitiv und $g \in \mathbb{Z}[X]$ mit $f \mid_{\mathbb{Q}[X]} g$, so gilt $f \mid_{\mathbb{Z}[X]} g$.

Beweis.

(1) Für $i \in \{1, \dots, n\}$ sei $m_i \in \mathbb{N}$ der Betrag des Produkts der Nenner der Koeffizienten $\neq 0$ von f_i. Dann ist $m_i f_i \in \mathbb{Z}[X]$, $d_i := c(m_i f_i) \in \mathbb{N}$ und es existiert $g_i \in \mathbb{Z}[X]$ primitiv mit $m_i f_i = c(m_i f_i) g_i = d_i g_i$. Wir setzen $\lambda_i := \frac{d_i}{m_i} \in \mathbb{Q}_{>0}$, $m := m_1 m_2 \cdots m_n \in \mathbb{N}$ und $d := d_1 d_2 \cdots d_n \in \mathbb{N}$. Es gilt $\lambda_1 \cdot \ldots \cdot \lambda_n = \frac{d}{m}$. Weiter ist

$$mf = (m_1 f_1)(m_2 f_2) \cdots (m_n f_n) = d g_1 g_2 \cdots g_n.$$

Da $g_1, \dots, g_n$ primitiv sind, gilt mit Lemma 4.3.1 auch $c(g_1 g_2 \cdots g_n) = 1$ und wir erhalten

$$mc(f) \overset{m \in \mathbb{N}}{=} c(mf) = c(d g_1 g_2 \cdots g_n) \overset{d \in \mathbb{N}}{=} d c(g_1 g_2 \cdots g_n) = d.$$

Das heißt $\lambda := \lambda_1 \cdot \ldots \cdot \lambda_n = \frac{d}{m} = \frac{mc(f)}{m} = c(f) \in \mathbb{N}$.

(2) Es sei $h \in \mathbb{Q}[X]$ mit $f \cdot h = g$. Nach (1) existieren Zerlegungen $f = \lambda_f f'$ und $h = \lambda_h h'$ mit $\lambda_f, \lambda_h \in \mathbb{Q}_{>0}$ und $f', h' \in \mathbb{Z}[X]$ primitiv und $\lambda_f \lambda_h \in \mathbb{N}$. Da f primitiv ist, gilt $\lambda_f = 1$ und damit $\lambda_h \in \mathbb{N}$. Wir erhalten $h = \lambda_h h \in \mathbb{Z}[X]$.

□

Satz 4.3.3. *Der Ring $\mathbb{Z}[X]$ ist faktoriell.*[a]

[a] Allgemeiner lässt sich zeigen, dass für einen Integritätsbereich R der Polynomring $R[X]$ genau dann faktoriell ist, wenn R faktoriell ist. Wir haben uns auf $\mathbb{Z}$ beschränkt, da wir das allgemeinere Resultat nicht benötigen. Der Beweis ist sehr ähnlich zum dem vorgestellten Beweis. Dabei wird $\mathbb{Q}$ durch den Quotientenkörper von R ersetzt.

Beweis. Es sei $0 \neq f \in \mathbb{Z}[X]$ keine Einheit. Nach Satz 3.4.5(2) reicht es zu zeigen, dass f ein Produkt von Primelementen in $\mathbb{Z}[X]$ ist. Dabei unterscheiden wir zwei Fälle.

(1) Gilt $\deg(f) = 0$, so ist $f \in \mathbb{Z}$ und da $\mathbb{Z}$ faktoriell ist, finden wir eine Zerlegung $f = p_1 p_2 \cdots p_n$ in Primelemente in $\mathbb{Z}$. Nach Lemma 4.3.1 sind diese auch Primelement in $\mathbb{Z}[X]$.

(2) Es sei $\deg(f) \geq 1$. Da $f \in \mathbb{Q}[X]$ als euklidischer Ring faktoriell ist, finden wir eine Zerlegung $f = f_1 f_2 \cdots f_n$ in Primelemente in $\mathbb{Q}[X]$. Anwendung von Satz 4.3.2 liefert primitive Elemente $g_1, \dots, g_n \in \mathbb{Z}[X]$ und $\lambda_1, \dots, \lambda_n \in \mathbb{Q}_{>0}$

$$f_i = \lambda_i g_i \text{ und } \lambda := \lambda_1 \lambda_2 \cdots \lambda_n \in \mathbb{N}.$$

Wie in (1) zerlegen $\lambda = q_1 q_2 \cdots q_m$ als Produkt von Primelementen in $\mathbb{Z}[X]$ und erhalten

$$f = \lambda g_1 g_2 \cdots g_n = q_1 q_2 \cdots q_m g_1 g_2 \cdots g_n.$$

Es sei $i \in \{1, \dots, n\}$ und $p, q \in \mathbb{Z}[X]$ mit $g_i \mid p \cdot q$. Da $g_i = \lambda_i^{-1} f_i$ gilt, ist $g_i \in \mathbb{Q}[X]$ ein Primelement und es folgt o.B.d.A. $g_i \mid_{\mathbb{Q}[X]} p$ in $\mathbb{Q}[X]$. Da g_i auch primitiv ist, liefert Satz 4.3.2 uns $g_i \mid_{\mathbb{Z}[X]} p$. Also ist p_i ein Primelement.

□

Bemerkung 4.3.4. Da $\mathbb{Z}$ und $\mathbb{Z}[X]$ beide faktorielle Ringe sind, sind die Primelemente genau die irreduziblen Elemente (siehe Satz 3.4.5).

Korollar 4.3.5. *Es sei $0 \neq f \in \mathbb{Z}[X]$. Folgende Aussagen sind äquivalent:*

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

(2) $\deg(f) = 0$ und $f \in \mathbb{Z}$ ist irreduzibel, oder $\deg(f) > 0$ und f ist primitiv und als Element in $\mathbb{Q}[X]$ irreduzibel.

Beweis. Nach Lemma 4.3.1 müssen wir nur den Fall $\deg(f) \geq 1$ betrachten.
(1) $\Rightarrow$ (2). Nach Beispiel (4) ist f primitiv. Wir schreiben $f = pq \in \mathbb{Q}[X]$. Es sei $\lambda \in \mathbb{N}$ mit $\lambda p \in \mathbb{Z}[X]$ und λp primitiv. Dann gilt $f = (\lambda p)(\lambda^{-1} q)$. Wir erhalten mit Satz 4.3.2 $\lambda^{-1} q \in \mathbb{Z}[X]$, also gilt o.B.d.A. $\lambda p \in \mathbb{Z}[X]^\times = \{-1, 1\}$. Das heißt $p \in \mathbb{Q} \setminus \{0\}$ ist eine Einheit. Damit ist f in $\mathbb{Q}[X]$ irreduzibel.
(2) $\Rightarrow$ (1). Es sei $\deg(f) \geq 1$ und f primitiv und irreduzibel in $\mathbb{Q}[X]$. Es sei weiter $f = pq \in \mathbb{Z}[X]$. Da f irreduzibel in $\mathbb{Q}[X]$ ist, gilt o.B.d.A. $p \in \mathbb{Q}[X]^\times \cap \mathbb{Z}[X] = (\mathbb{Q} \setminus \{0\}) \cap \mathbb{Z} = \mathbb{Z} \setminus \{0\}$. Da f primitiv ist, folgt $1 = c(f) = c(pq) = |p| c(q)$. Das heißt $|p| = 1$ und $p \in \{-1, 1\}$ ist eine Einheit. □

Beispiel.

(1) $f = 2 = 2X^0$ ist irreduzibel in $\mathbb{Z}[X]$ aber nicht in $\mathbb{Q}[X]$, da $\mathbb{Q}[X]^\times = \mathbb{Q} \setminus \{0\}$.

(2) $f = 4X^0$ ist weder in $\mathbb{Z}[X]$ noch in $\mathbb{Q}[X]$ irreduzibel.

(3) $f = X$ ist in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$ irreduzibel.

(4) $f = 2X$ ist nicht in $\mathbb{Z}[X]$ aber in $\mathbb{Q}[X]$ irreduzibel.

Satz 4.3.6 (Kriterium von Eisenstein). *Es sei $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ ein primitives Polynom vom Grad $n \geq 1$. Ist $p \in \mathbb{P}$ eine Primzahl mit $p | a_i$ für $0 \leq i \leq n-1$ und $p \nmid a_n$ sowie $p^2 \nmid a_0$. Dann ist f irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$.*

Beweis. Es seien $g, h \in \mathbb{Z}[X]$ mit $f = gh$. Wir schreiben $g = \sum_{i=0}^{k} b_i X^i$ und $h = \sum_{i=0}^{\ell} c_i X^i$ mit $b_k \neq 0 \neq c_\ell$. Es gilt $p \mid a_0 = b_0 c_0$ und damit o.B.d.A. $p \mid b_0$, da p ein Primelement ist. Mit $p^2 \nmid a_0$ folgt $p \nmid c_0$. Weiter gilt $p \nmid a_n = b_k c_\ell$ und damit $p \nmid b_k$. Wir finden also $1 \leq m \leq k \leq n$ minimal mit $p \nmid b_m$. Es gilt

$$a_m = \underbrace{b_0 c_m + b_1 c_{m-1} + b_2 c_{m-2} + \cdots + b_{m-1} c_1}_{\text{wird von } p \text{ geteilt}} + b_m c_0$$

wobei $c_i := 0$ für $i > \ell$. Weiter gilt $p \nmid b_m c_0$, da p ein Primelement ist. Es folgt $p \nmid a_m$. Nach Voraussetzung folgt $n = m \leq k \leq n$. Das heißt $k = \deg(g) = n$ und $\deg(h) = \deg(f) - \deg(g) = 0$. Damit ist $h \in \mathbb{Z} \setminus \{0\}$ und $1 = c(f) = c(gh) = |h| c(g)$. Damit gilt $h \in \{-1, 1\}$ und wir schließen, dass h eine Einheit ist. Damit ist f irreduzibel in $\mathbb{Z}[X]$. Die Irreduzibilität in $\mathbb{Q}[X]$ folgt aus Korollar 4.3.5.
□

Beispiel. (1) Es sei $f := X^3 + 3X^2 + 15$. Es ist f primitiv und nach Eisenstein mit $p = 3$ irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$.

(2) Es ist $g := 2X^3 + 6X^2 + 30$ nicht primitiv. Insbesondere ist g nicht irreduzibel in $\mathbb{Z}[X]$. Wir zerlegen $g = c(g)g_0 = 2f$. Nach (1) ist f irreduzibel in $\mathbb{Q}[X]$. Da 2 eine Einheit in $\mathbb{Q}[X]$ ist, ist $2f = g$ auch in $\mathbb{Q}[X]$ irreduzibel.

(3) Das Polynom $h := \frac{1}{2}X^3 + \frac{3}{2}X^2 + \frac{15}{2} \in \mathbb{Q}[X] \setminus \mathbb{Z}[X]$ erfüllt $h = \frac{1}{2}f$. Nach (1) ist f irreduzibel in $\mathbb{Q}[X]$. Da $\frac{1}{2} \in \mathbb{Q}[X]$ eine Einheit ist, ist damit auch h irreduzibel.

(4) Da Polynom $X^2 + 1$ ist irreduzibel in $\mathbb{Q}[X]$ und $\mathbb{Z}[X]$ (also auch primitiv in $\mathbb{Z}[X]$). Das Eisensteinkriterium ist aber nicht anwendbar.

5 Elementare Theorie der Körpererweiterungen

5.1 Körpererweiterungen

Definition. Sei L ein Körper. Ein Unterring $K \subseteq L$ heißt **Teilkörper**, falls $x^{-1} \in K$ für alle $x \in K \setminus \{0\}$ gilt. Dann nennt man L einen **Erweiterungskörper** von K und spricht von einer **Körpererweiterung** $L : K$.

Beispiele.

(1) $\mathbb{R} : \mathbb{Q}$ ist eine Körpererweiterung.

(2) $\mathbb{C} : \mathbb{R}$ ist eine Körpererweiterung.

Diese beiden Erweiterungen unterscheiden sich in fundamentaler Weise: Ist allgemein $L : K$ eine Körpererweiterung, so erhält L durch

$$r.v := rv \quad \text{für alle } r \in K, v \in L$$

die Struktur eines K-Vektorraums. Es gilt $\dim_{\mathbb{R}} \mathbb{C} = 2$, da $(1, i)$ eine $\mathbb{R}$-Basis von $\mathbb{C}$ ist.

Angenommen, $\dim_{\mathbb{Q}} \mathbb{R} < \infty$. Dann gilt $\mathbb{R} \cong \mathbb{Q}^n$ für ein $n \in \mathbb{N}$ und somit wäre die Menge $\mathbb{R}$ abzählbar, ein Widerspruch.

Definition. Sei L ein Körper, $K \subseteq L$ ein Teilkörper, $S \subseteq L$ eine Teilmenge. Dann bezeichnet

$$K(S) := \bigcap_{K \cup S \subseteq K' \subseteq L \text{ Teilkörper}} K'$$

den kleinsten Teilkörper von L, der $K \cup S$ enthält. Ferner bezeichnet $K[S] := \bigcap_{K \cup S \subseteq R \subseteq L \text{ Teilring}} R$ den kleinsten Unterring von L, der $K \cup S$ enthält.

Lemma 5.1.1. *Sei $L : K$ eine Körpererweiterung, $S \subseteq L$ eine Menge. Dann ist $K(S)$ isomorph zum Quotientenkörper $Q(K[S])$.*

Beweis. Da $K[S] \subseteq L$ ein Integritätsbereich ist, existiert der Quotientenkörper $Q(K[S])$. Der Körper $K(S)$ ist ein Unterring von L, der $K \cup S$ enthält. Daher folgt $K[S] \subseteq K(S)$. Für die kanonische Inklusion $\alpha : K[S] \longrightarrow K(S)$ gilt $\alpha(x) \in K(S)^\times$ für jedes $x \in K[S] \setminus \{0\}$. Damit existiert nach Satz 3.3.3 ein Homomorphismus $\beta : Q(K[S]) \longrightarrow K(S)$ mit $\beta(\frac{x}{1}) = \alpha(x)$ für alle $x \in K[S]$. Da $Q(K[S])$ ein Körper ist, ist β nach Satz 3.2.1 injektiv. Also ist $\beta(Q(K[S]))$ ein Teilkörper von $K(S)$, der $K \cup S$ enthält. Es folgt $\beta(Q(K[S])) = K(S)$ und damit ist β der gewünschte Isomorphismus. □

Definition. Sei L ein Körper mit Teilkörpern K und $S = \{a_1, \ldots, a_n\} \subseteq L$.

(1) Wir schreiben $K[a_1, \ldots, a_n] := K[S]$ sowie $K(a_1, \ldots, a_n) := K(S)$.

(2) Der Körper

$$P(L) := \bigcap_{A \subseteq L \text{ Teilkörper}} A$$

heißt der **Primkörper** von L.

Lemma 5.1.2. *Sei L ein Körper. Dann gilt:*

(1) Ist $\operatorname{char}(L) = p > 0$, so gilt $P(L) \cong \mathbb{Z}/(p)$.

(2) Ist $\operatorname{char}(L) = 0$, so gilt $P(L) \cong \mathbb{Q}$.

Beweis. Wir betrachten den Ringhomomorphismus $\varphi : \mathbb{Z} \longrightarrow P(L)\ ;\ n \mapsto n1$. Dann gilt nach Lemma 3.2.4 $\ker \varphi = (\operatorname{char}(L))$ und $\operatorname{char}(L) = 0$ oder $\operatorname{char}(L)$ ist eine Primzahl.

(1) Ist $\operatorname{char}(L)$ eine Primzahl p, so ist $\mathbb{Z}/\ker \varphi \cong \mathbb{Z}/(p)$ nach Satz 3.2.3 ein Körper. Also ist $\operatorname{im} \varphi \cong \mathbb{Z}/(p)$ ein Teilkörper von $P(L)$ (und damit von L) und wir erhalten $\operatorname{im} \varphi = P(L)$.

(2) Gilt $\operatorname{char}(L) = 0$, so liefert Korollar 3.3.4 einen injektiven Homomorphismus $\mathbb{Q} \longrightarrow P(L)$ und damit wie im ersten Teil $\mathbb{Q} \cong P(L)$.

□

5.2 Endliche Körpererweiterungen

Definition. Sei $L : K$ eine Körpererweiterung. Dann heißt $[L : K] := \dim_K L$ der **Grad** der Erweiterung $L : K$. Die Körpererweiterung $L : K$ heißt **endlich**, falls $[L : K] < \infty$.

Satz 5.2.1 (Turmformel)**.** *Sei $L : K$ eine Körpererweiterung.*

(1) Ist V ein L-Vektorraum mit Basis $(v_j)_{j \in J}$ und ist $(a_i)_{i \in I}$ eine Basis von L über K, so ist $(a_i v_j)_{(i,j) \in I \times J}$ eine Basis des K-Vektorraums V und es gilt

$$\dim_K V = \dim_L V [L : K].$$

(2) Ist $L' : L$ eine Körpererweiterung, so gilt $[L' : K] = [L' : L][L : K]$.

Beweis.

(1) Sei $v \in V$. Da $(v_j)_{j\in J}$ eine Basis von V über L ist, gibt es $(x_j)_{j\in J}$, $x_j \in L$ und $x_j = 0$ für alle bis auf endlich viele $j \in J$ mit $v = \sum_{j\in J} x_j v_j$. Ebenso schreiben wir $x_j = \sum_{i\in I} \lambda_{ij} a_i$ mit $\lambda_{ij} \in K$. Damit folgt also

$$v = \sum_{j\in J} \sum_{i\in I} \lambda_{ij} a_i v_j \in \langle \{a_i v_j \mid (i,j) \in I \times J\} \rangle.$$

Es seien nun $\gamma_{ij} \in K$ mit $\gamma_{ij} = 0$ für alle bis auf endlich viele $(i,j) \in I \times J$ gegeben derart, dass

$$0 = \sum_{(i,j)} \gamma_{ij} a_i v_j.$$

Dann gilt also

$$0 = \sum_{j\in J} (\sum_{i\in I} \gamma_{ij} a_i) v_j.$$

Da die v_j linear unabhängig sind, folgt

$$\sum_{i\in I} \gamma_{ij} a_i = 0 \quad \forall\, j \in J.$$

Die lineare Unabhängigkeit der a_i liefert dann $\gamma_{ij} = 0$ für alle $(i,j) \in I \times J$.

Damit ist $(a_i v_j)_{(i,j)\in I\times J}$ eine Basis von V über K und es gilt

$$\dim_K V = |I \times J| = |I||J| = [L : K] \dim_L V.$$

(2) Aus (1) folgt $[L' : K] = \dim_L L'[L : K] = [L' : L][L : K]$.

□

Definition. Sei $L : K$ eine Körpererweiterung und $a \in L$. Es heißt a **algebraisch über K**, falls es ein Polynom $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$ gibt. Andernfalls heißt $a \in L$ **transzendent über K**.

Beispiele. Wir betrachten die Körpererweiterung $\mathbb{R} : \mathbb{Q}$.

(1) Die irrationale Zahl $\sqrt{2}$ ist als Nullstelle des Polynoms $X^2 - 2 \in \mathbb{Q}[X]$ algebraisch über $\mathbb{Q}$.

(2) Ein berühmter Satz von Lindemann-Weierstrass besagt, dass $\pi \in \mathbb{R}$ transzendent über $\mathbb{Q}$ ist.

(3) Das Element $\alpha := \sqrt{2 + \sqrt{3}} \in \mathbb{R}$ ist auch algebraisch über $\mathbb{Q}$. Um ein entsprechendes Polynom zu finden, berechnen wir zunächst $\alpha^2 = 2 + \sqrt{3}$ und dann $\alpha^4 = 7 + 4\sqrt{3}$. Damit gilt $\alpha^4 - 4\alpha = -1$. Damit erfüllt $f := X^4 - 4X^2 + 1 \in \mathbb{Q}[X]$ die Gleichung $f(\alpha) = 0$.

Definition. Sei $L : K$ eine Körpererweiterung und $a \in L$ algebraisch über K ist. Dann existiert ein Polynom $\mu_a \in K[X] \setminus \{0\}$ mit folgenden Eigenschaften.

(a) $\mu_a(a) = 0$,

(b) $\deg(\mu_a) \leq \deg(f)$ für alle $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$,

(c) μ_a ist normiert.

Das Polynom $\mu_a \in K[X]$ ist eindeutig bestimmt und heißt das **Minimalpolynom** von a.

Lemma 5.2.2. *Sei $L : K$ eine Körpererweiterung sowie $a \in L$ algebraisch über K. Dann ist μ_a irreduzibel, $\{1, a, \ldots, a^{\deg(\mu_a)-1}\}$ ist eine Basis des K-Vektorraums $K[a]$ und es gilt $K[a] = K(a)$. Insbesondere gilt also $[K(a) : K] = \deg(\mu_a)$.*

Beweis. Wir betrachten den Homomorphismus $\mathrm{ev}_a : K[X] \longrightarrow K(a) \; ; \; f \mapsto f(a)$. Dann gilt $\operatorname{im} \mathrm{ev}_a = K[a]$. Da $K[X]$ nach Korollar 4.2.3 ein Hauptidealring ist und $a \in L$ algebraisch über K ist, gibt es $f_a \in K[X] \setminus \{0\}$ mit $\ker \mathrm{ev}_a = (f_a)$. Wegen $\mu_a \in \ker \mathrm{ev}_a$ existiert ein $0 \neq g \in K[X]$ mit $\mu_a = g f_a$. Damit folgt $\deg(\mu_a) = \deg(g) + \deg(f_a) \geq \deg(f_a)$ und da $\mu_a \in \ker \mathrm{ev}_a$ nach Definition minimalen Grad hat, erhalten wir $\deg(\mu_a) = \deg(f_a)$ und somit $\deg(g) = 0$. Also folgt $\ker \mathrm{ev}_a = (f_a) = (\mu_a)$.

Die Homomorphiesätze liefern nun einen Isomorphismus $K[X]/(\mu_a) \cong K[a] \subseteq K(a)$. Damit ist $K[X]/(\mu_a)$ ein Integritätsbereich und $(\mu_a) \neq \{0\}$ ein Primideal. Insbesondere ist μ_a also irreduzibel. Weiter liefert uns Satz 3.4.5, dass $K[X]/(\mu_a)$ ein Körper ist. Das heißt $K[a] = K(a)$.
Direktes Nachrechnen zeigt das $\{1, a, \ldots, a^{\deg(\mu_a)-1}\}$ eine Basis des K-Vektorraums $K[a]$ ist und damit $[K(a) : K] = \deg(\mu_a)$. □

Satz 5.2.3. *Sei $L : K$ eine Körpererweiterung, $a \in L$ ein Element. Dann sind folgende Aussagen äquivalent:*

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

(2) $K(a) = K[a]$.

(3) Die Körpererweiterung $K(a) : K$ ist endlich.

Beweis. (1) ⇒ (2). Dies wurde in Lemma 5.2.2 gezeigt.
(2) ⇒ (3). Für $a = 0$ ist nichts zu zeigen. Sei nun $a \neq 0$. Dann liefert (2) uns $a^{-1} \in K[a]$, also existiert $f \in K[X] \setminus \{0\}$ mit $a^{-1} = f(a)$. Damit ist a Nullstelle des Polynoms $g := Xf - 1 \in K[X] \setminus \{0\}$. Wir wenden Lemma 5.2.2 an.
(3) ⇒ (1). Da $\dim_K K(a) < \infty$ gilt, gibt es ein $n \in \mathbb{N}$ derart, dass $\{1, a, a^2, \ldots, a^n\}$ linear abhängig ist. Also existiert $(r_0, \ldots, r_n) \in K^{n+1} \setminus \{0\}$ mit

$$\sum_{i=0}^{n} r_i a^i = 0.$$

Es ist daher $f := \sum_{i=0}^{n} r_i X^i \in K[X] \setminus \{0\}$ ein Polynom mit $f(a) = 0$. □

Beispiel. Wir betrachten $\sqrt{d} \in \mathbb{R}$ für ein $d \in \mathbb{N}$ sowie $f_d := X^2 - d \in \mathbb{Q}[X]$. Wegen $f_d(\sqrt{d}) = 0$ ist $\sqrt{d}$ algebraisch über $\mathbb{Q}$. Es folgt mit Lemma 5.2.2: $1 \leq [\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = \deg(\mu_d) \leq \deg(f_d) = 2$. Es folgt $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$ genau dann, wenn d keine Quadratzahl ist.

5.3 Algebraische Körpererweiterungen

Definition. Eine Körpererweiterung $L : K$ heißt **algebraisch**, falls jedes Element $a \in L$ algebraisch über K ist.

Beispiele. (1) Sei $L : K$ eine endliche Körpererweiterung. Für $a \in L$ gilt $[K(a) : K] \leq [L : K]$ und Satz 5.2.3 zeigt, dass a algebraisch über K ist. Also ist $L : K$ algebraisch.

(2) Die Erweiterung $\mathbb{R} : \mathbb{Q}$ ist nicht algebraisch, da π nicht algebraisch über $\mathbb{Q}$ ist. Man kann dies aber auch ohne den Satz von Lindemann einsehen.

Satz 5.3.1. *Sei $L : K$ eine Körpererweiterung.*

(1) Gilt $L = K(a_1, \ldots, a_n)$, so ist $L : K$ algebraisch genau dann, wenn $L : K$ endlich ist.

(2) Sei $K \subseteq K' \subseteq L$ ein Zwischenkörper. Folgende Aussagen sind äquivalent.

(a) Die Erweiterungen $L : K'$ und $K' : K$ sind algebraisch.

(b) Die Erweiterung $L : K$ ist algebraisch.

(3) Die Menge

$$\hat{L} := \{x \in L \mid x \text{ ist algebraisch über } K\}$$

*ist ein Zwischenkörper von $L : K$ und heißt **algebraischer Abschluss** von K in L.*

Beweis.

(1) Für $i \in \{1, \ldots, n\}$ ist a_i algebraisch über K und damit auch über dem Körper $K(a_1, \ldots, a_{i-1})$. Wegen $K(a_1, \ldots a_i) = K(a_1, \ldots a_{i-1})(a_i)$ folgt aus Satz 5.2.3 damit die Endlichkeit der Erweiterung $K(a_1, \ldots, a_i) : K(a_1, \ldots, a_{i-1})$ für $1 \leq i \leq n$. Nun liefert Satz 5.2.1

$$[L : K] = \prod_{i=1}^{n} [K(a_1, \ldots, a_i) : K(a_1, \ldots, a_{i-1})] < \infty.$$

Da endliche Erweiterungen stets algebraisch sind, folgt die Behauptung.

(2) Es seien $L : K'$, $K' : K$ algebraisch und $a \in L$. Dann existiert $f \in K'[X] \setminus \{0\}$ mit $f(a) = 0$. Wir schreiben $f = \sum_{i=0}^{n} r_i X^i$. Dann ist a algebraisch über $K(r_0, \ldots, r_n) \subseteq K'$. Nach (1) ist die Erweiterung $K(r_0, \ldots, r_n) : K$ endlich. Damit ist nach Satz 5.2.1 und Satz 5.2.3 die Erweiterung $K(r_0, \ldots, r_n, a) : K$ ebenfalls endlich und a ist algebraisch über K.
Sei nun $L : K$ algebraisch. Dann folgt unmittelbar, dass $L : K'$ und $K' : K$ algebraisch sind.

(3) Seien $x, y \in \hat{L}$. Dann ist y algebraisch über $K(x)$. Nach Satz 5.2.3 folgt $[K(x, y) : K(x)] < \infty$ und $[K(x) : K] < \infty$. Also liefert Satz 5.2.1, dass $K(x, y) : K$ eine endliche Erweiterung ist. Wegen $x + y, xy, x^{-1} \in K(x, y)$ folgt mit Satz 5.2.3, dass diese Elemente zu $\hat{L}$ gehören. Damit ist $\hat{L}$ ein Teilkörper von L, der zudem K enthält.

□

Satz 5.3.2 (Kronecker Konstruktion). *Sei K ein Körper und $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein irreduzibles Polynom vom Grad $n \in \mathbb{N}$. Dann existiert ein Körper $K \subseteq L$ in dem f eine Nullstelle besitzt mit $[L : K] = \deg(f)$.*

Beweis. Wir betrachten dazu den Ring $L := K[X]/(f)$. Da f ein Primelement ist, ist (f) ein Primideal von $K[X]$ und L nach Satz 3.4.5 und Satz 3.2.3 ein Körper. Wir betrachten den injektiven Homomorphismus von Ringen

$$\pi\colon K \longrightarrow K[X]/(f)\ ;\ \alpha \mapsto \alpha + (f)$$

und fassen $K \cong \operatorname{im}\pi$ als Unterkörper von $K[X]/(f)$ auf.[1] Dann ist $\alpha := X+(f) \in L$ eine Nullstelle des Polynoms $\bar{f} = \sum_{i=0}^{n} \pi(a_i)T^i \in L[T]$, da

$$\bar{f}(\alpha) = \sum_{i=0}^{n} \pi(a_i)\alpha^i = \sum_{i=0}^{n} a_i X^i + (f) = f + (f) = 0_L.$$

Es sei nun $g + (f) \in L[T]$. Da $f \neq 0$ gilt, finden wir eine Darstellung $g = qf + r$ mit $q, r \in K[X]$ und $r = 0$ oder $0 \leq r < \deg(f)$. Wir schreiben $r = \sum_{i=0}^{n-1} b_i X^i$ mit $b_0, \ldots, b_{n-1} \in K$ und erhalten

$$g + (f) = qf + r + (f) = r + (f) = \sum_{i=0}^{n-1} b_i X^i + (f).$$

Damit ist $\{1_L, X + (f), \ldots, X^{n-1} + (f)\}$ ein K-Erzeugendensystem von L. Sind $c_0, \ldots, c_{n-1} \in K$ mit

$$0_L = \sum_{i=0}^{n-1} c_i(X^i + (f)) = (\sum_{i=0}^{n-1} c_i X^i) + (f),$$

dann ist $h := \sum_{i=0}^{n-1} c_i X^i \in (f)$ und damit ein Vielfaches von f. Mit $\deg(f) > \deg(h)$ folgt $h = 0$. Also ist $\{1_L, X + (f), \ldots, X^{n-1} + (f)\}$ eine K-Basis von L und $[L : K] = n = \deg(f)$. □

Beispiel. Das Polynom $X^2 + 1 \in \mathbb{R}[X]$ ist irreduzibel. Die Konstruktion liefert den Körper $L := \mathbb{R}[X]/(X^2+1)$ mit $\mathbb{R}$-Basis $\{1_L, X+(X^2+1)\}$. Das Element $X+(X^2+1) \in L$ erfüllt $(X+(X^2+1))^2 = X^2 + (X^2+1) = -1 + (X^2+1) = -1_L$, da $X^2 + 1 \in (X^2+1)$. Damit liefert die Konstruktion einen Körper in dem eine Wurzel aus -1 existiert.

[1] Wir wollen uns hier einmalig klarmachen, dass obige Identifikation von K mit $\pi(K)$ und f mit $\bar{f}$ keine Einschränkung ist. Zunächst wählen wir eine Menge $K \subseteq A$ zusammen mit einer Bijektion $\varphi\colon A \longrightarrow L$, sodass $\varphi|_K = \pi$ gilt. Nun definieren wir auf A zwei Operationen $+, \cdot\colon A \times A \longrightarrow A$ durch

$$a + b := \varphi^{-1}(\varphi(a) + \varphi(b)) \text{ und } a \cdot b := \varphi^{-1}(\varphi(a)\varphi(b)).$$

Auf diese Weise erhält $(A, +, \cdot)$ die Struktur eines Körpers. Weiter ist

$$\begin{aligned} f(\varphi^{-1}(\alpha)) &= \sum_{i=0}^{n} a_i \varphi^{-1}(\alpha)^i = \sum_{i=0}^{n} a_i \varphi^{-1}(\alpha^i) = \sum_{i=0}^{n} \varphi^{-1}(\varphi(a_i)\alpha^i) \\ &= \varphi^{-1}(\sum_{i=0}^{n} \varphi(a_i)\alpha^i) = \varphi^{-1}(\bar{f}(\alpha)) = \varphi^{-1}(0_L) = \varphi^{-1}(0_{\pi(K)}) = 0_K = 0_A. \end{aligned}$$

Definition. Es sei $\sigma\colon K \longrightarrow K'$ ein Körperisomorphismus.

(1) Wir bezeichnen mit $\sigma^*\colon K[X] \longrightarrow K'[X]$ den eindeutig bestimmten Isomorphismus von Ringen (vgl. Satz 4.1.1) gegeben durch $\sigma^*|_K = \sigma$ und $\sigma^*(X) = X$.

(2) Sind $L\colon K, L'\colon K'$ Körpererweiterungen, so heißt ein Isomorphismus von Körpern $\varphi\colon L \longrightarrow L'$ heißt **Fortsetzung** von σ, falls $\varphi|_K = \sigma$ gilt.

Lemma 5.3.3 (Fortsetzungslemma). *Es seien $L\colon K, L'\colon K'$ Körpererweiterungen und $\sigma\colon K \longrightarrow K'$ ein Isomorphismus von Körpern. Weiter sei $a \in L$ algebraisch über K mit Minimalpolynom μ_a und $a' \in L'$ eine Nullstelle von $\sigma^*(\mu_a) \in K'[X]$. Dann existiert genau eine Fortsetzung $\varphi\colon K(a) \longrightarrow K'(a')$ von σ mit $\varphi(a) = a'$. Wir sind also in folgender Situation:*

$$\begin{array}{ccc} L & & L' \\ \uparrow & & \uparrow \\ K(a) & \overset{\exists!\varphi}{\dashrightarrow} & K'(a') \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sigma} & K'. \end{array}$$

Beweis. Wir nehmen an, dass $\psi : K(a) \longrightarrow K'(a')$ eine Fortsetzung von σ mit $\psi(a) = a'$ ist. Es sei $x \in K(a) = K[a]$ (siehe Satz 5.2.3), dann existiert $f \in K[X]$ mit $f = \sum_{i=0}^n \lambda_i X^i$ und $f(a) = x$. Notwendigerweise gilt

$$\psi(x) = \psi(f(a)) = \psi(\sum_{i=0}^n \lambda_i a^i) = \sum_{i=0}^n \sigma(\lambda_i)(a')^i = \sigma^*(f)(a').$$

Wir definieren daher

$$\varphi\colon K(a) \longrightarrow K'(a')\ ;\ f(a) \mapsto \sigma^*(f)(a').$$

Dies ist wohldefiniert: Gilt $f(a) = g(a)$, so ist $f - g \in \ker \mathrm{ev}_a = (\mu_a)$ und $f - g = p\mu_a$ mit $p \in K[X]$. Wir erhalten $\sigma^*(f)(a') - \sigma^*(g)(a') = \sigma^*(f-g)(a') = \sigma^*(p\mu_a)(a') = \sigma^*(p)(a')\sigma^*(\mu_a)(a') = 0$. Direktes Nachrechnen zeigt, dass φ ein Homomorphismus von Ringen ist. Die Umkehrabbildung ist gegeben durch

$$\varphi^{-1}\colon K'(a') \longrightarrow K(a)\ ;\ h(a') \mapsto (\sigma^{-1})^*(h)(a)^2.$$

□

[2]Es ist a' nach Voraussetzung algebraisch. Weiter ist $\mu_{a'} = \sigma^*(\mu_a)$, da $\sigma^*(\mu_a)$ normiert und irreduzibel ist und a ist eine Nullstelle von $\mu_a = (\sigma^{-1})^*(\sigma^*(\mu_a)) = (\sigma^{-1})^*(\mu_{a'})$.

5.4 Zerfällungskörper

Definition. Sei K ein Körper, $f \in K[X] \setminus K$ ein Polynom vom Grad $m \geq 1$. Ein Körper $L \supseteq K$ heißt **Zerfällungskörper von f über K**, falls es Elemente $a_1, \ldots, a_m \in L$ und $c \in K \setminus \{0\}$ derart gibt, dass

(1) $f = c\prod_{i=1}^{m}(X - a_i)$, das heißt, f zerfällt über L in Linearfaktoren, und

(2) $L = K(a_1, \ldots, a_m)$.

Satz 5.4.1. *Es sei K ein Körper, $f \in K[X] \setminus K$ ein Polynom mit $n := \deg(f)$.*

(1) Es existiert ein Zerfällungskörper $\overline{K}$ von f mit $[\overline{K}\colon K] \leq n!$.

(2) Ist $\sigma\colon K \longrightarrow K'$ ein Körperisomorphismus, sowie L und L' Zerfällungskörper von f bzw. $\sigma^*(f)$. Dann existiert eine Fortsetzung $\varphi\colon L \longrightarrow L'$ von σ.

(3) Sind $\overline{K}, \overline{K}'$ Zerfällungskörper von f, so existiert ein Isomorphismus von Körpern $\varphi\colon \overline{K} \longrightarrow \overline{K}'$ mit $\varphi|_K = \mathrm{id}_K$.

Beweis.

(1) Wir beweisen die Existenz über Induktion nach $n \in \mathbb{N}$. Ist $n = 1$, so ist K ein Zerfällungskörper von f vom Grad $[K\colon K] = 1 = 1!$. Es sei nun $n > 1$. Da $K[X]$ faktoriell ist, existiert ein Primteiler p von f. Die Kronecker Konstruktion liefert nun eine Körpererweiterung $L : K$ mit $[L : K] = \deg(p) \leq n$, sodass p mindestens eine Nullstelle in L besitzt. Diese sei mit a_n bezeichnet. Wir erhalten in $L[X]$ die Zerlegung $f = (X - a_n)g$ mit $\deg(g) = \deg(f) - 1$. Nach Induktionsvoraussetzung existiert ein Zerfällungskörper L' von g über L vom Grad $[L'\colon L] \leq (n-1)!$. Das heißt es existiert $c \in L \setminus \{0\}$ und $a_1, \ldots, a_{n-1} \in L'$ mit $g = c\prod_{i=1}^{n-1}(X - a_i)$. In $L'[X]$ gilt also $f = c\prod_{i=1}^{n}(X - a_i)$. Damit ist $\overline{K} := K(a_1, \ldots, a_n) \subseteq L'$ ein Erweiterungskörper von K und $[\overline{K}\colon K] \leq [L'\colon K] = [L' : L] \cdot [L : K] \leq (n-1)! \cdot n = n!$.

(2) Wir beweisen die Existenz von φ nach Induktion über $[L : K]$, wobei der Fall $[L : K] = 1$ klar ist. Es sei nun $[L : K] > 1$. Wie in (1) finden wir einen irreduziblen und normierten Faktor p von f und $q \in K[X]$ mit $f = pq$ mit $\deg(p) \geq 2$. Da f in $L[X]$ in Linearfaktoren zerfällt, finden wir $a \in L$ mit $p(a) = 0$. Es gilt $\sigma^*(f) = \sigma^*(p)\sigma^*(q)$. Damit besitzt $\sigma^*(p)$ mindestens eine Nullstelle $a' \in L'$. Weiter ist $p = \mu_a$. Nach Lemma 5.3.3 finden wir eine Fortsetzung $\varphi\colon K(a) \longrightarrow K'(a')$ von $\sigma\colon K \longrightarrow K'$. Es gilt $K(a) \neq K$ und damit gilt $[L : K(a)] < [L : K]$ nach der Turmformel. Es sind L und L' Zerfällungskörper von f über $K(a)$ bzw. $K'(a')$. Nach Induktionsvoraussetzung existiert eine Fortsetzung $\psi\colon L \longrightarrow L'$ von φ. Damit ist ψ eine Fortsetzung von σ.

(3) Dies folgt direkt aus (2) nach Anwendung auf $\sigma = \mathrm{id}_K\colon K \longrightarrow K$.

□

5.5 Normale Erweiterungen

Definition. Eine endliche Körpererweiterung $L : K$ heißt **normal**, falls L der Zerfällungskörper für ein Polynom $f \in K[X] \setminus K$ ist.

Bemerkung 5.5.1.

(1) Man muss in der Definition nicht fordern, dass $L : K$ endlich ist. Dies folgt schon aus Satz 5.3.1 (siehe auch Satz 5.4.1.

(2) Es sei L der Zerfällungskörper von $f \in K[X]\setminus K$ über K. Ist $K \subseteq Q \subseteq L$ ein Zwischenkörper, dann ist auch L Zerfällungskörper von f aufgefasst als Polynom in $Q[X]$. Das heißt $L : K$ normal $\Rightarrow L : Q$ normal.

Satz 5.5.2. *Es sei $L : K$ eine endliche Erweiterung. Folgende Aussagen sind äquivalent:*

(1) Die Erweiterung $L : K$ ist normal.

(2) Jedes irreduzible Polynom $p \in K[X]\setminus K$, das in L eine Nullstelle besitzt, zerfällt in L vollständig in Linearfaktoren.

Beweis. (1) $\Rightarrow$ (2). Es sei L der Zerfällungskörper von $f \in K[X] \setminus K$. Es sei $p \in K[X]$ irreduzibel und $a \in L$ mit $p(a) = 0$. Wir nehmen o.B.d.A. an, dass p normiert ist. Damit gilt $p = \mu_a$. Es sei $L \subseteq M$ ein Zerfällungskörper von p (aufgefasst als Element in $L[X]$). Weiter sei $b \in M$ eine Nullstelle. Nach Lemma 5.3.3 existiert ein K-linear Isomorphismus von Körpern $\varphi\colon K(a) \longrightarrow K(b)$ mit $\varphi(a) = b$. Es ist L ein Zerfällungskörper von f über $K(a)$ und $L(b) \subseteq M$ ein Zerfällungskörper von f über $K(b)$. Da φ K-linear ist, gilt $\varphi^*(f) = f$. Nach Satz 5.4.1 existiert eine Fortsetzung $\psi\colon L \longrightarrow L(b)$ von φ. Insbesondere ist ψ K-linear und damit gilt $\dim_K L = \dim_K L(b)$. Mit $L \subseteq L(b)$ folgt $L = L(b)$, also $b \in L$. Das folgende Diagramm veranschaulicht die Situation.

$$\begin{array}{ccc} M & & M \\ \uparrow & & \uparrow \\ L & \overset{\psi}{\dashrightarrow} & L(b) \\ \uparrow & & \uparrow \\ K(a) & \overset{\varphi}{\dashrightarrow} & K(b) \\ \uparrow & & \uparrow \\ K & \xrightarrow{\mathrm{id}_K} & K. \end{array}$$

(2) $\Rightarrow$ (1). Da $L : K$ endlich ist, finden wir $a_1, \ldots, a_n \in K$ mit $L = K(a_1, \ldots, a_n)$. Es sei $f := \mu_{a_1}\mu_{a_2}\cdots\mu_{a_n}$ das Produkt der Minimalpolynome der a_i. Nach Voraussetzung, zerfällt jedes μ_{a_i} über L in Linearfaktoren und damit auch f. Weiter gilt

$$L = K(a_1, \ldots, a_n) \subseteq K(Z_L(f)) = K(\bigcup_{i=1}^{n} Z_L(\mu_{a_i})) \subseteq L.$$

Das heißt $L = K(Z_L(f))$ und damit ist L Zerfällungskörper von f über K.

□

Beispiel. Wir betrachten die Erweiterung $\mathbb{Q}(\sqrt[4]{2})\colon \mathbb{Q}$, $p := X^4 - 2 \in \mathbb{Q}[X]$ und $\alpha := \sqrt[4]{2}$. Es gilt $p(\alpha) = 0$. Mit dem Kriterium von Eisenstein zeigt man, dass $p := X^4 - 2 \in \mathbb{Q}[X]$ irreduzibel ist. Weiter gilt $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$. Es ist $\sqrt[4]{2} \cdot i \in \mathbb{C} \setminus \mathbb{R}$ auch eine Nullstelle von p. Damit ist die Erweiterung nicht normal.

Korollar 5.5.3. *Sei $L : K$ eine normale Körpererweiterung sowie $a, b \in L$. Dann sind folgende Aussagen äquivalent:*

(1) Es gibt einen Automorphismus $\sigma : L \longrightarrow L$ mit $\sigma|_K = \mathrm{id}_K$ derart, dass $\sigma(a) = b$ gilt.

(2) $\mu_a = \mu_b$.

Beweis. (1) $\Rightarrow$ (2). Es gilt $0 = \sigma(\mu_a(a)) = \sigma^*(\mu_a)(b) = \mu_a(b)$. Damit folgt $\mu_a = \mu_b$.
(2) $\Rightarrow$ (1). Siehe Beweis von Satz 5.5.2. □

5.6 Lineare Unabhängigkeit von Körperhomomorphismen

Sei A eine Menge und K ein Körper. Dann erhält die Menge $\mathrm{Abb}(A, K)$ der Abbildungen von A nach K die Struktur eines K-Vektorraums durch

$$(\varphi + \psi)(a) := \varphi(a) + \psi(a) \;\; ; \;\; (\lambda\varphi)(a) := \lambda\varphi(a) \quad \text{für alle } \varphi, \psi \in \mathrm{Abb}(A, K), a \in A, \lambda \in K.$$

Satz 5.6.1. *Es seien K', K Körper sowie $\sigma_1, \ldots, \sigma_n\colon K' \longrightarrow K$ paarweise verschiedene Homomorphismen von Körpern. Dann ist $\{\sigma_1, \ldots, \sigma_n\} \subseteq \mathrm{Abb}(K', K)$ linear unabhängig über K.*

Beweis. Wir zeigen die Behauptung über Induktion nach n, wobei der Fall $n = 1$ klar ist. Es sei daher $n \geq 2$ und $\alpha_1, \ldots, \alpha_n \in K$ mit $\sum_{i=1}^n \alpha_i\sigma_i = 0_{\mathrm{Abb}(K',K)}$. Für $g, h \in K'$ gilt

$$0_K = \sigma_n(g) \underbrace{\sum_{i=1}^{n} \alpha_i\sigma_i(h)}_{=0_K} - \underbrace{\sum_{i=1}^{n} \alpha_i\sigma_i(gh)}_{=0_K} = \sum_{i=1}^{n-1} \underbrace{\alpha_i(\sigma_n(g) - \sigma_i(g))}_{\in K} \sigma_i(h).$$

Damit folgt $\sum_{i=1}^{n-1} \alpha_i(\sigma_n(g) - \sigma_i(g))\sigma_i = 0_{\mathrm{Abb}(K',K)}$ für jedes $g \in G$ und die Induktionsannahme liefert

$$\alpha_i(\sigma_n(g) - \sigma_i(g)) = 0_K \;\text{ für }\; 1 \leq i \leq n-1,\; g \in G.$$

Da die Elemente $\sigma_1, \ldots, \sigma_n$ paarweise verschieden sind, finden wir für jedes $i \in \{1, \ldots, n-1\}$ ein g mit $\sigma_i(g) \neq \sigma_n(g)$ und damit $\alpha_i = 0$. Insgesamt folgt $0_K = \alpha_n\sigma_n$ und damit auch $\alpha_n = 0_K$. □

Definition. Sei $L : K$ eine endliche Körpererweiterung. Wir definieren

$$\mathrm{Aut}(L : K) := \{\varphi\colon L \longrightarrow L \mid \varphi \text{ ist Ringautomorphismus mit } \varphi|_K = \mathrm{id}_K\}^3.$$

und bemerken, dass $\mathrm{Aut}(L : K)$ eine Untergruppe von $\mathrm{Aut}(L)$ ist. Die Gruppe $\mathrm{Aut}(L : K)$ heißt **Galoisgruppe** der Erweiterung $L : K$. Nach Definition sind die Elemente in $\mathrm{Aut}(L : K)$ K-linear.

Beispiel. Wir betrachten die Körpererweiterung $\mathbb{C} : \mathbb{R}$. Wir wollen untersuchen, welche $\mathbb{R}$-linearen Körperisomorphismen $\mathbb{C} \longrightarrow \mathbb{C}$ existieren. Neben der Identität $\mathrm{id}_\mathbb{C}$ kennen wir noch die Komplexe Konjugation $\bar{\cdot}\colon \mathbb{C} \longrightarrow \mathbb{C}\ ;\ z \mapsto \overline{z}$, da $\overline{r} = r$ für $r \in \mathbb{R}$.

Korollar 5.6.2. *Es seien $Q : K$ und $L : K$ endliche Körpererweiterungen.*

(1) Es gilt

$$|\{\varphi\colon Q \longrightarrow L \mid \varphi \textit{ ist Homomorphismus mit } \varphi|_K = \mathrm{id}_K\}| \leq [Q : K].$$

(2) Es gilt $|\mathrm{Aut}(L : K)| \leq [L : K]$.

Beweis.

(1) Die Menge der K-linearen Abbildungen $\mathrm{Hom}_K(Q, L)$ bildet einen L-Untervektorraum des Vektorraums $\mathrm{Abb}(Q, L)$, da

$$(\alpha\varphi)(\beta a) = \alpha\varphi(\beta a) = \alpha\beta\varphi(a) = \beta(\alpha\varphi)(a)$$

für alle $\alpha \in L$, $\beta \in K$, $a \in Q$ und $\varphi \in \mathrm{Hom}_K(Q, L)$ gilt. Nun liefert Satz 5.2.1

$$\dim_L \mathrm{Hom}_K(Q, L) = \frac{\dim_K \mathrm{Hom}_K(Q, L)}{[L : K]} = \frac{[L : K][Q : K]}{[L : K]} = [Q : K].$$

Wir schließen mit $\{\varphi\colon Q \longrightarrow L \mid \varphi \text{ ist Homomorphismus mit } \varphi|_K = \mathrm{id}_K\} \subseteq \mathrm{Hom}_K(Q, L)$ und Satz 5.6.1

$$|\{\varphi\colon Q \longrightarrow L \mid \varphi \text{ ist Homomorphismus mit } \varphi|_K = \mathrm{id}_K\}| \leq [Q : K].$$

(2) Dies folgt aus (1) für $Q = L$.

□

[3] Ein Isomorphismus $\varphi\colon R \longrightarrow R$ eines Rings R heißt **Automorphismus**.

6 Galoistheorie

6.1 Galoiserweiterungen

Definition. (1) Sei L ein Körper und $G \subseteq \mathrm{Aut}(L)$ eine Gruppe. Der Teilkörper von L

$$L^G := \{a \in L \mid \forall\, \sigma \in G\colon \sigma(a) = a\}$$

heißt **Fixkörper** von G.

(2) Eine endliche Erweiterung $L : K$ heißt **Galoiserweiterung**, falls $L^{\mathrm{Aut}(L:K)} = K$ gilt.

Bemerkung 6.1.1. Es gilt stets $L^{\mathrm{Aut}(L:K)} \supseteq K$. Weiter ist $\mathrm{Aut}(L : K) \subseteq \mathrm{Aut}(L)$ nach Korollar 5.6.2 eine endliche Untergruppe von $\mathrm{Aut}(L) = \{\varphi\colon L \longrightarrow L \mid \varphi \text{ Automorphismus des Rings } L\}$.

Beispiele. (1) Nach Korollar 5.6.2 gilt $|\mathrm{Aut}(\mathbb{C} : \mathbb{R})| \leq 2$ und damit $\mathrm{Aut}(\mathbb{C} : \mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \bar{\cdot}\}$. Mit $i \notin \mathbb{C}^{\mathrm{Aut}(\mathbb{C}:\mathbb{R})}$ folgt $\mathbb{R} = \mathbb{C}^{\mathrm{Aut}(\mathbb{C}:\mathbb{R})}$. Mithin ist $\mathbb{C} : \mathbb{R}$ eine Galoiserweiterung.

(2) Wir betrachten die Erweiterung $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$. Nach Eisenstein ist $f := X^4 - 2 \in \mathbb{Q}[X]$ irreduzibel mit $f(\sqrt[4]{2}) = 0$. Das heißt $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ und $f = \mu_{\sqrt[4]{2}}$. Es sei $\varphi \in \mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q})$, dann gilt $\varphi(\sqrt[4]{2}) \in Z_{\mathbb{C}}(f) = \{i^k \sqrt[4]{2} \mid k \in \{0, 1, 2, 3\}\}$. Mit $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ folgt $\varphi(\sqrt[4]{2}) \in \{\sqrt[4]{2}, -\sqrt[4]{2}\}$ und damit $\varphi(\sqrt{2}) = \sqrt{2}$. Also ist $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})^{\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q})} \subseteq \mathbb{Q}(\sqrt[4]{2})$. Damit ist $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$ keine Galoiserweiterung.

Satz 6.1.2. *Es sei L ein Körper und $G \subseteq \mathrm{Aut}(L)$ eine endliche Untergruppe. Es gelten die folgenden Aussagen.*

(1) Die Erweiterung $L : L^G$ ist endlich, $\mathrm{Aut}(L : L^G) = G$ und $[L : L^G] = |G|$.

(2) $L : L^G$ ist eine Galoiserweiterung mit Galoisgruppe $\mathrm{Aut}(L : L^G) = G$.

(3) $L : L^G$ ist normal.

Beweis.

(1) Wir setzen $n := |G|$ und schreiben $G = \{\varphi_1, \ldots, \varphi_n\}$. Weiter definieren wir

$$\mathrm{Tr}_G\colon L \longrightarrow L\ ;\ y \mapsto \sum_{i=1}^{n} \varphi_i(y)$$

und bemerken $\mathrm{Tr}_G(y) \in L^G$ für alle $y \in L$. Weiter gilt $\mathrm{Tr}_G \neq 0$ nach Satz 5.6.1. Es seien $y_1, \ldots, y_{n+1} \in L$. Wir zeigen $\{y_1, \ldots, y_{n+1}\}$ ist linear abhängig über L^G. Dazu betrachten wir

das lineare Gleichungssystem $Ax = 0$ gegeben durch die Matrix $A = (a_{ij}) \in \mathrm{Mat}_{n\times(n+1)}(L)$ mit Einträgen

$$a_{ij} := \varphi_i^{-1}(y_j)$$

für alle $i \in \{1, \ldots, n\}$ und $j \in \{1, \ldots, n+1\}$. Das Gleichungssystem besitzt eine nicht-triviale Lösung, etwa $t = (t_1, \ldots, t_{n+1}) \in L^{n+1}$ und wir nehmen ohne Beschränkung $t_1 \neq 0$ an, da wir ansonsten die φ_i umsortieren können. Nun fixieren wir $y \in L$ mit $\mathrm{Tr}_G(y) \neq 0$ und bemerken, dass auch $z := yt_1^{-1}t = (y, yt_1^{-1}t_2, \ldots, yt_1^{-1}t_{n+1}) \in L^{n+1}$ eine nicht-triviale Lösung des Gleichungssystem ist. Zeilenweise Auswertung des Gleichungssystems $Az = 0$ ergibt

$$\varphi_i^{-1}(y_1)(y) + \sum_{j=2}^{n+1} \varphi_i^{-1}(y_j)(yt_1^{-1}t_j) = 0$$

für alle $i \in \{1, \ldots, n\}$ und Anwendung von φ_i liefert

$$y_1\varphi_i(y) + \sum_{j=2}^{n+1} y_j\varphi_i(yt_1^{-1}t_j) = 0.$$

Wir erhalten

$$0 = \sum_{i=1}^{n} y_1\varphi_i(y) + \sum_{i=1}^{n}\sum_{j=2}^{n+1} y_j\varphi_i(yt_1^{-1}t_j) = \underbrace{\mathrm{Tr}_G(y)}_{\in L^G} y_1 + \sum_{j=2}^{n+1} \underbrace{\mathrm{Tr}_G(yt_1^{-1}t_j)}_{\in L^G} y_j.$$

Es gilt $\mathrm{Tr}_G(y) \neq 0$ und damit ist $\{y_1, \ldots, y_{n+1}\}$ linear abhängig über L^G. Dies zeigt $[L : L^G] \leq |G|$. Weiter folgt mit Korollar 5.6.2 | $\mathrm{Aut}(L : L^G)| \leq [L : L^G] \leq |G|$.
Per Definition gilt $G \subseteq \mathrm{Aut}(L : L^G)$. Das heißt $G = \mathrm{Aut}(L : L^G)$ und $[L : L^G] = |G|$.

(2) Es gilt nach (1) $L^{\mathrm{Aut}(L:L^G)} = L^G$.

(3) Sei $a \in L$. Dann ist $G.a := \{\varphi(a) \mid \varphi \in G\}$ eine endliche Menge. Für $\psi \in G$ ist $G \longrightarrow G\ ;\ \varphi \mapsto \psi \circ \varphi$ eine Permutation. Insbesondere ist $G.a \longrightarrow G.a\ ;\ b \mapsto \psi(b)$ eine Permutation. Wir betrachten das Polynom $f_a := \prod_{b\in G.a}(X - b) \in L[X]$. Per Definition zerfällt f_a über L Linearfaktoren Für $\psi \in G$ sei $\psi^* \in \mathrm{Aut}(L[X])$ der induzierte Automorphismus. Dann erhalten wir

$$\psi^*(f_a) = \prod_{b\in G.a} (X - \psi(b)) = \prod_{b\in G.a} (X - b) = f_a.$$

Mithin folgt $f_a \in L^G[X]$ und wegen $f_a(a) = 0$ ist a algebraisch über L^G. Da $L^G : L$ nach (1) endlich ist, existieren $b_1, \ldots, b_m$ mit $L = L^G(b_1, \ldots, b_n)$. Wir definieren $f := \prod_{i=1}^n f_{b_i}$. Mit $b_1, \ldots, b_m \in Z_L(f)$ folgt $L = L^G(Z_L(f))$ und f zerfällt über L in Linearfaktoren. Also ist $L : L^G$ normal.

□

Satz 6.1.3. *Es sei $L : K$ eine endliche Körpererweiterung.*

(1) Folgende Aussagen sind äquivalent.

(i) $L : K$ ist eine Galoiserweiterung.

(ii) $|\operatorname{Aut}(L:K)| = [L:K]$.

(2) Ist $L:K$ eine Galoiserweiterung, so ist $L:K$ normal.

Beweis.

(1) (i) $\Rightarrow$ (ii). Nach Satz 6.1.2 gilt $[L:K] = [L:L^{\operatorname{Aut}(L:K)}] = |\operatorname{Aut}(L:K)|$.
(ii) $\Rightarrow$ (i). Nach Satz 6.1.2 gilt $[L:K] = |\operatorname{Aut}(L:K)| = [L:L^{\operatorname{Aut}(L:K)}]$. Mit $K \subseteq L^{\operatorname{Aut}(L:K)}$ und der Turmformel folgt die Behauptung.

(2) Folgt direkt aus Satz 6.1.2 angewandt auf die endliche Gruppe $\operatorname{Aut}(L:K)$.

□

Korollar 6.1.4. *Ist $L:K$ eine Galoiserweiterung und $K \subseteq Q \subseteq L$ ein Zwischenkörper.*

(1) $L:Q$ ist eine Galoiserweiterung.

(2) Es gilt $|\{\varphi\colon Q \longrightarrow L \mid \varphi \text{ ist Homomorphismus mit } \varphi|_K = \mathrm{id}_K\}| = [Q:K]$.

Beweis. Wir betrachten die endliche Gruppe $G := \operatorname{Aut}(L:K)$ und operieren auf der Menge

$$X := \{\varphi\colon Q \longrightarrow L \mid \varphi \text{ ist Homomorphismus mit } \varphi|_K = \mathrm{id}_K\}$$

durch

$$G \times X \longrightarrow X\ ;\ (\varphi, \psi) \mapsto \varphi.\psi := \varphi \circ \psi.$$

Es sei $x\colon Q \longrightarrow L$ die kanonische Inklusion. Es gilt für $\varphi \in G$ nach Definition

$$\varphi \in G_x \Leftrightarrow \varphi \circ x = x \Leftrightarrow \varphi(q) = \varphi(x(q)) = x(q) = q \text{ für alle } q \in Q \Leftrightarrow \varphi \in \operatorname{Aut}(L:Q).$$

Nach Korollar 5.6.2 ist X eine endliche Menge mit $|X| \leq [Q:K]$ und $|\operatorname{Aut}(L:Q)| \leq [L:Q]$. Wir erhalten mit der Bahnformel, Satz 6.1.3 und der Turmformel

$$[L:K] = |G| = |G_x| \cdot |G.x| \leq |\operatorname{Aut}(L:Q)| \cdot |X| \leq [L:Q] \cdot [Q:K] = [L:K].$$

Damit gilt bereits $[L:Q] = |\operatorname{Aut}(L:Q)|$ und $|X| = [Q:K]$. Insbesondere gilt (2) und Anwendung von Satz 6.1.3 zeigt, dass $L:Q$ eine Galoiserweiterung ist. □

Definition. Ist $L:K$ eine Körpererweiterung, so definieren wir die Mengen

$$\mathfrak{Z} := \{Q \mid K \subseteq Q \subseteq L \text{ Zwischenkörper}\} \quad \mathfrak{U} := \{H \mid H \subseteq \operatorname{Aut}(L:K) \text{ Untergruppe}\},$$

sowie Abbildungen

$$\gamma : \begin{cases} \mathfrak{Z} & \longrightarrow & \mathfrak{U} \\ Q & \mapsto & \operatorname{Aut}(L:Q) \end{cases} \quad \text{und} \quad \delta : \begin{cases} \mathfrak{U} & \longrightarrow & \mathfrak{Z} \\ H & \mapsto & L^H. \end{cases}$$

Lemma 6.1.5. *Es sei $L : K$ eine Körperweiterung. Es gelten die folgenden Aussagen.*

(1) Für $Q \in \mathcal{Z}$ gilt $Q \subseteq L^{\mathrm{Aut}(L:Q)} = (\delta \circ \gamma)(Q)$.

(2) Für $H \in \mathcal{U}$ gilt $H \subseteq \mathrm{Aut}(L : L^H) = (\gamma \circ \delta)(H)$.

(3) Für $Q_1, Q_2 \in \mathcal{Z}$ mit $Q_1 \subseteq Q_2$ gilt $\gamma(Q_2) \subseteq \gamma(Q_1)$.

(4) Für $H_1, H_2 \in \mathcal{U}$ mit $H_1 \subseteq H_2$ gilt $\delta(H_2) \subseteq \delta(H_1)$.

Beweis. Übung. □

Satz 6.1.6 (Hauptsatz der Galoistheorie[a])**.** *Es sei $L : K$ eine Galoiserweiterung.*

(1) Es gelten $\delta \circ \gamma = \mathrm{id}_{\mathcal{Z}}$ und $\gamma \circ \delta = \mathrm{id}_{\mathcal{U}}$.

(2) Ist $Q \in \mathcal{Z}$, so gilt $[Q : K] = \frac{[L:K]}{[L:Q]} = \frac{|\mathrm{Aut}(L:K)|}{|\mathrm{Aut}(L:Q)|}$.

(3) Ist Q in $\mathcal{Z}$ mit $\sigma(Q) = Q$ für alle $Q \in \mathrm{Aut}(L : K)$, so ist $Q : K$ eine Galoiserweiterung.

[a] Der Hauptsatz umfasst weitere Aussagen, die wir nicht diskutieren.

Beweis. Da $L : K$ eine endliche Erweiterung ist, ist $\mathrm{Aut}(L : K)$ nach Korollar 5.6.2 eine endliche Gruppe.

(1) Sei $H \in \mathcal{U}$. Satz 6.1.2 impliziert

$$(\gamma \circ \delta)(H) = \gamma(L^H) = \mathrm{Aut}(L : L^H) = H.$$

Sei $Q \in \mathcal{Z}$. Nach Korollar 6.1.4 ist $L : Q$ eine Galoiserweiterung und damit gilt

$$(\delta \circ \gamma)(Q) = \delta(\mathrm{Aut}(L : Q)) = L^{\mathrm{Aut}(L:Q)} = Q.$$

(2) Da $L : K$ und $L : Q$ Galoiserweiterungen sind, folgt die Behauptung direkt aus der Turmformel und Satz 6.1.3.

(3) Nach Voraussetzung können wir $\sigma|_Q$ als Elemente von $\mathrm{Aut}(Q : K)$ auffassen und erhalten einen Homomorphismus von Gruppen

$$\varphi\colon\ \mathrm{Aut}(L : K) \longrightarrow \mathrm{Aut}(Q : K)\ ;\ \sigma \longrightarrow \sigma|_Q.$$

Es gilt $\ker \varphi = \mathrm{Aut}(L : Q)$. Da $L : Q$ eine Galoiserweiterung ist, erhalten wird mit (2), dem Homomorphiesatz und Korollar 5.6.2

$$\begin{aligned}[Q : K] = \frac{|\mathrm{Aut}(L : K)|}{|\mathrm{Aut}(L : Q)|} = \frac{|\mathrm{Aut}(L : K)|}{|\ker \varphi|} = |\mathrm{Aut}(L : K)/\ker \varphi| \\ = |\operatorname{im} \varphi| \leq |\mathrm{Aut}(Q : K)| \leq [Q : K].\end{aligned}$$

Also folgt $[Q : K] = |\mathrm{Aut}(Q : K)|$ und $Q : K$ ist nach Satz 6.1.3 eine Galoiserweiterung.

□

6.2 Charakterisierung von Galoiserweiterungen in Charakteristik 0

Im Folgenden sei $L : K$ stets eine endliche Körpererweiterung mit $\mathrm{char}(K) = 0$ (dies ist äquivalent zu $\mathrm{char}(L) = 0$).

Lemma 6.2.1. *Es sei $L : K$ ein normale Erweiterung, $\mathrm{char}(K) = 0$ und $f \in K[X]$ ein irreduzibles Polynom, das in L eine Nullstelle besitzt. Dann besitzt f genau $\deg(f)$ verschiedene Nullstellen in L.*[a]

[a] Das Resultat lässt sich mit demselben Beweis auch $\mathrm{char}(K) > 0$ beweisen, wenn $f' \neq 0$ gilt.

Beweis. Da die Erweiterung normal ist, zerfällt f nach Satz 5.5.2 über L in Linearfaktoren $f = c\prod_{i=1}^{m}(X - \alpha_i)$ mit $c \in K^\times$. Wir zeigen $\alpha_i \neq \alpha_j$ für alle $i \neq j$. Es gilt $0 \neq f'$ und $\deg(f') < \deg(f)$. Insbesondere gilt $f \nmid f'$ und die Irreduzibilität von f liefert $1 \in \mathrm{ggT}(f, f') = K^\times$. Das heißt wir finden $s, t \in K[X]$ mit $1 = s \cdot f + t \cdot f'$[1]. Es folgt

$$1 = 1(\alpha_i) = s(\alpha_i)f(\alpha_i) + t(\alpha) \cdot f'(\alpha_i) = t(\alpha) \cdot f'(\alpha_i).$$

Anwendung von Satz 4.2.6 liefert, dass $n(\alpha_i) = 1$ für alle $i \in \{1, \ldots, m\}$ gilt. □

Satz 6.2.2 (Satz vom primitiven Element)**.** *Es sei $L : K$ eine endliche Erweiterung mit $\mathrm{char}(K) = 0$. Dann existiert $\alpha \in L$ mit $L = K(\alpha)$.*

Beweis. Aufgrund einer einfachen Induktion reicht es zu zeigen: Gilt $L = K(a, b)$, so existiert $c \in L$ mit $L = K(c)$.

Es bezeichnen $\mu_a, \mu_b \in K[X]$ die Minimalpolynome von a und b. Es sei $\mu := \mu_a \cdot \mu_b$ sowie $K \subseteq Z$ ein Zerfällungskörper von μ. Über Z zerfallen μ_a, μ_b in Linearfaktoren

$$\mu_a = \prod_{i=1}^{m}(X - a_i) \text{ und } \mu_b = \prod_{i=1}^{n}(X - b_i)$$

mit $a_1 = a$ und $b_1 = b$. Da $\mathrm{char}(K) = 0$ gilt, liefert Lemma 6.2.1, dass $b_1 = b, b_2, \ldots, b_n$ paarweise verschieden sind. Da K unendlich ist, existiert ein Element

$$u \in K \setminus \{(a_i - a)(b - b_j)^{-1} \mid 1 \leq i \leq m, 2 \leq j \leq n\}.$$

Wir setzen $c := a + ub \in L$. Klar ist $K(c) \subseteq K(a, b)$.

Wir setzen $h := \mu_a(c - u \cdot X) \in K(c)[X]$ und fixieren den normierten ggT von h und μ_b in $K(c)[X]$. Dieser sei mit $g \in K(c)[X]$ bezeichnet. Insbesondere gilt also $g \mid \mu_b \in K(c)[X]$ und damit auch $g \mid \mu_b \in Z[X]$. Also existiert eine Teilmenge $I \subseteq \{1, \ldots, n\}$ mit $g = \prod_{i \in I}(X - b_i)$ in $Z[X]$.

Es gilt $h(b) = \mu_a(c - ub) = \mu_a(a) = 0$. Weiter gilt für $2 \leq j \leq n$, dass $a + u(b - b_j) \neq a_i$ für alle $i \in \{1, \ldots, m\}$ nach Wahl von u und damit

$$h(b_j) = \mu_a(c - ub_j) = \mu_a(a + u(b - b_j)) \neq 0,$$

da die Nullstellen von μ_a gerade $a_1, \ldots, a_m$ sind.

Damit gilt $X - b = g \in K(c)[X]$. Wir schließen $b \in K(c)$ und damit $a = c - ub \in K(c)$. Es folgt $K(c) = K(a, b)$ mit $c \in L$. □

[1] Das Lemma von Bézout gilt auch in $K[X]$, da $K[X]$ ein euklidischer Ring ist.

Korollar 6.2.3. *Es sei $L : K$ eine endliche Körpererweiterung mit $\operatorname{char}(K) = 0$. Folgende Aussagen sind äquivalent:*

(1) $L : K$ ist eine Galoiserweiterung.

(2) $[L : K] = |\operatorname{Aut}(L : K)|$.

(3) $L : K$ ist eine normale Erweiterung.

Beweis. Die Äquivalenz (1) $\Leftrightarrow$ (2) gilt nach Satz 6.1.3.
(1) $\Rightarrow$ (3). Nach Satz 6.1.3 ist die Galoiserweiterung $L : K$ normal.
(3) $\Rightarrow$ (2). Nach dem Satz vom primitiven Element existiert $\alpha \in L$ mit $L = K(\alpha)$. Da $\mu_\alpha \in K[X]$ in L die Nullstelle α besitzt, folgt

$$n := [L\colon K] = [K(\alpha)\colon K] \overset{5.2.2}{=} \deg \mu_\alpha \overset{6.2.1}{=} |Z_L(\mu_\alpha)|.$$

Es seien $\alpha, \alpha_2, \ldots, \alpha_n$ die paarweise verschiedenen Nullstellen. Es gilt $\mu_\alpha = \mu_{\alpha_i}$ und damit $K(\alpha) = K(\alpha_i)$ für alle $i \in \{1, \ldots, n\}$, da $K(\alpha_i) \subseteq L$. Anwendung von Lemma 5.3.3 für $\sigma = \mathrm{id}_K$ liefert uns Automorphismen von Körpern

$$\varphi_i\colon K(\alpha) \longrightarrow K(\alpha_i) = K(\alpha)$$

mit $\varphi|_K = \sigma = \mathrm{id}_K$ und $\varphi(\alpha) = \alpha_i$. Es folgt $|\operatorname{Aut}(L\colon K)| \geq |L : K|$. Nun wenden wir Korollar 5.6.2 und Satz 6.1.3 an. □

Satz 6.2.4. *Es sei $L : K$ eine endliche Körpererweiterung mit $\operatorname{char}(K) = 0$.*

(1) Es existiert ein Erweiterungskörper N von L derart, dass $N : K$ eine Galoiserweiterung ist.

(2) Es existieren nur endliche viele Zwischenkörper $K \subseteq Q \subseteq L$.

Beweis.

(1) Nach Satz 6.2.2 finden wir $\alpha \in L$ mit $L = K(\alpha)$. Wir betrachten einen Zerfällungskörper N von $\mu_\alpha \in K[X]$. Es gilt $K \subseteq L = K(\alpha) \subseteq N$. Nun wenden wir Korollar 6.2.3 an.

(2) Wir wählen N wie in (1). Nach dem Hauptsatz der Galoistheorie, gibt es eine Bijektion zwischen Zwischenkörpern der Erweiterung $N : K$ und der endlichen Gruppe $\operatorname{Aut}(N : K)$. Es sei $K \subseteq Q \subseteq L$ ein Zwischenkörper. Dann ist Q auch ein Zwischenkörper $K \subseteq Q \subseteq N$. Es folgt die Behauptung.

□

7 Anwendungen

7.1 Der Fundamentalsatz der Algebra

Satz 7.1.1. *Der Körper der komplexen Zahlen $\mathbb{C}$ ist **algebraisch abgeschlossen**, das heißt jedes Polynom $f \in \mathbb{C}[X] \setminus \mathbb{C}$ besitzt eine Nullstelle in $\mathbb{C}$.*

Beweis. Es sei $L : \mathbb{C}$ eine endliche Erweiterung. Wir zeigen $L = \mathbb{C}$. Wir wenden Satz 6.2.4 auf die Erweiterung $L : \mathbb{R}$ an und finden einen Erweiterungskörper N von L, so dass $N : \mathbb{R}$ eine Galoiserweiterung ist. Gilt $N = \mathbb{C}$, so auch $L = \mathbb{C}$. Daher können wir annehmen, dass $L\colon \mathbb{R}$ eine Galoiserweiterung ist. Es sei $G := \operatorname{Aut}(L : \mathbb{R})$ die zugehörige Galoisgruppe und $P \subseteq G$ eine Sylow 2-Untergruppe. Wir betrachten den Teilkörper $\mathbb{R} \subseteq L^P \subseteq L$. Nach Satz 6.1.2 ist $L : L^P$ eine Galoiserweiterung mit $\operatorname{Aut}(L : L^P) = P$, also $[L\colon L^P] = |\operatorname{Aut}(L : L^P)| = |P|$. Wir erhalten

$$|G| = [L\colon \mathbb{R}] = [L\colon L^P] \cdot [L^P\colon \mathbb{R}] = |P| \cdot [L^P\colon \mathbb{R}].$$

Damit ist $[L^P\colon \mathbb{R}]$ ungerade[1]. Wir wählen $\alpha \in L^P$ und $\mu_\alpha \in \mathbb{R}[X]$ das zugehörige Minimalpolynom. Dann ist $\deg(\mu_\alpha)$ ein Teiler von $[L^P\colon \mathbb{R}]$, also ebenfalls ungerade. Ein Polynom von ungeradem Grad über $\mathbb{R}$ hat aber stets eine Nullstelle (nach dem Zwischenwertsatz). Damit folgt aufgrund der Irreduzibilität schon $\deg(\mu_\alpha) = 1$ und $\alpha \in \mathbb{R}$. Wir haben $L^p = \mathbb{R}$ gezeigt und schließen, dass $G = P$ eine 2-Gruppe ist. Damit ist auch die Galoisgruppe $\operatorname{Aut}(L : \mathbb{C}) \subseteq G$ der Galoiserweiterung $L : \mathbb{C}$ eine 2-Gruppe. Die Annahme $\operatorname{Aut}(L : \mathbb{C}) \neq \{\mathrm{id}\}$ liefert zusammen mit dem Satz von Sylow eine Untergruppe $U \subseteq \operatorname{Aut}(L : \mathbb{C})$ der Ordnung $\frac{|\operatorname{Aut}(L:\mathbb{C})|}{2}$ und damit einen Teilkörper $\mathbb{C} \subseteq L^U \subseteq L$ mit $[L^U : \mathbb{C}] = \frac{[L:\mathbb{C}]}{[L:L^U]} \overset{6.1.2}{=} \frac{|\operatorname{Aut}(L:\mathbb{C})|}{|U|} = 2$. Es sei $\alpha \in L^U \setminus \mathbb{C}$. Dann gilt $\deg(\mu_\alpha) = 2$. Dies ist ein Widerspruch, da jedes Polynom vom Grad 2 eine Nullstelle in $\mathbb{C}$ hat (dies folgt aus der p-q-Formel). Damit gilt $\operatorname{Aut}(L : \mathbb{C}) = \{\mathrm{id}\}$. Da $L : \mathbb{C}$ eine Galoiserweiterung ist, gilt damit $[L : \mathbb{C}] = 1$, also $L = \mathbb{C}$.

Es sei nun $f \in \mathbb{C}[X] \setminus \mathbb{C}$. Dann ist der Zerfällungskörper L von f über $\mathbb{C}$ eine endliche Erweiterung $L : \mathbb{C}$. Es gilt also $L = \mathbb{C}$. □

7.2 Endliche Körper

In diesem Abschnitt studieren wir endliche Körper. Nach Lemma 5.1.2 gilt $\operatorname{char}(K) = p \in \mathbb{P}$ für jeden endlichen Körper. Wir haben gesehen, dass für $p \in \mathbb{P}$ Primzahl der Ring $\mathbb{F}_p := \mathbb{Z}/(p)$ ein Körper ist. Sei nun K ein weiterer endlicher Körper der Charakteristik p. Dann gilt für den Primkörper $P(K) \cong \mathbb{Z}/(p) = \mathbb{F}_p$ und es liegt eine endliche Körpererweiterung $K : \mathbb{F}_p$ vor. Es sei $n := \dim_{\mathbb{F}_p} K$, dann gilt

$$|K| = p^{[K:\mathbb{F}_p]}$$

[1] Es gilt $|P| = 2^m$ mit $2^m \mid |G|$ und $2^{m+1} \nmid |G|$.

und $|K|$ ist damit eine p-Potenz. Da für $n > 1$, der Ring $\mathbb{Z}/(p^n)$ kein Körper ist, stellt sich die Frage, ob Körper der Ordnung p^n existieren. Im Folgenden gehen wir dieser Frage nach.

Lemma 7.2.1 (Freshman's dream). *Es sei R ein Ring der Charakteristik $p \in \mathbb{P}$, $a, b \in R$ und $m \in \mathbb{N}$. Dann gilt*

$$(a+b)^{p^m} = a^{p^m} + b^{p^m}.$$

Beweis. Es reicht den Fall $m = 1$ zu betrachten. Es gilt $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$. Für $i \in \{1, \ldots, p-1\}$ ist p ein Teiler von $\binom{p}{i} = \frac{p!}{(p-i)!i!}$, da p eine Primzahl ist. Mit $p \cdot x = 0$ für alle $x \in R$ folgt die Behauptung. □

Satz 7.2.2. *Es sei $n \in \mathbb{N}$ und $p \in \mathbb{P}$ eine Primzahl.*

(1) Es existiert (bis auf Isomorphie) genau ein Körper $\mathbb{F}_{p^n}$ der Ordnung p^n, und

(2) $\mathbb{F}_{p^n}$ ist gegeben als ein Zerfällungskörper von $f := X^{p^n} - X \in \mathbb{F}_p[X]$.

Beweis. Zunächst beweisen wir die Existenz eines Körpers mit p^n Elementen. Wir betrachten dazu einen Zerfällungskörper L des Polynoms f. Es gilt $f' = p^n X^{p^n-1} - 1 = -1$. Damit gilt $f'(a) \neq 0$ für jede Nullstelle $a \in L$ von f. Anwendung von Satz 4.2.6 liefert, dass $Z_L(f)$ genau p^n Elemente besitzt. Es gilt $0, 1 \in Z_L(f)$. Es seien $a, b \in Z_L(f)$ Nullstellen von f. Dann gilt mit Lemma 7.2.1

$$f(a+b) = (a+b)^{p^n} - (a+b) = a^{p^n} + b^{p^n} - a - b = f(a) + f(b) = 0, \text{ und}$$
$$(*) \quad f(a \cdot b) = (ab)^{p^n} - ab = a^{p^n} b^{p^n} \underbrace{-ab^{p^n} + ab^{p^n}}_{=0} - ab = b^{p^n} f(a) - a f(b) = 0.$$

Für $a \neq 0$ folgt aus $0 = f(a)$ die Gleichung $a^{p^n-1} = 1$ und damit $a^{p^n-2} = a^{-1}$, also

$$f(a^{-1}) = f(a^{p^n-2}) \overset{(*)}{=} 0.$$

Für $p \in \mathbb{P}$ ungerade gilt

$$f(-a) = (-a)^{p^n} - (-a) = (-1)^{p^n} a^{p^n} - (-a) = -a^{p^n} + a = -f(a) = 0$$

und für $p = 2$ gilt $f(-a) = f(a) = 0$. Damit ist die Nullstellenmenge $Z_L(f)$ ein Teilkörper von L und $L = Z_L(f)$ ein Körper der Mächtigkeit p^n.

Es sei nun $\mathbb{F}_p \subseteq L$ ein beliebiger Körper mit p^n Elementen. Dann ist $L^\times = L \setminus \{0\}$ nach Satz 4.2.5 eine zyklische Gruppe der Ordnung $p^n - 1$ Elemente. Es gilt also $x^{p^n-1} = 1$ für alle $x \in L \setminus \{0\}$ und damit $f(x) = x(x^{p^n-1} - 1) = 0$. Ebenso gilt $f(0) = 0$. Damit ist L gerade die Nullstellenmenge von f und damit ein Zerfällungskörper von f über $\mathbb{F}_p$. Nach Satz 5.4.1 sind alle Zerfällungskörper von f über $\mathbb{F}_p$ isomorph. □

Es sei $p \in \mathbb{P}$ und $n \in \mathbb{N}$. Dann ist

$$\mathrm{Fr}\colon \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n} \; ; \; x \mapsto x^p$$

nach Lemma 7.2.1 ein Ringhomomorphismus. Da $\mathbb{F}_{p^n}$ ein Körper ist, ist Fr injektiv und auch bijektiv, da $\mathbb{F}_{p^n}$ endlich ist. Weiter gilt für $x \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ die Gleichung $x^p = x$ (da $x^{|\mathbb{F}_p \setminus \{0\}|} = 1$), das heißt $\mathrm{Fr} \in \mathrm{Aut}(\mathbb{F}_p\colon \mathbb{F})$. Der Automorphismus Fr heißt *Frobeniusautomorphismus*.

Korollar 7.2.3. *Es sei $p \in \mathbb{P}$ und $n \in \mathbb{N}$.*

(1) Die Gruppe $\mathrm{Aut}(\mathbb{F}_{p^n} : \mathbb{F}_p)$ ist zyklisch von Ordnung n und durch Fr erzeugt.

(2) Die Erweiterung $\mathbb{F}_{p^n} : \mathbb{F}_p$ ist eine Galoiserweiterung.

(3) Es gilt $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ genau dann, wenn $m \mid n$.

Beweis.

(1) Es gilt $\mathrm{Fr}^n(x) = x^{p^n} = x$ für alle $x \in \mathbb{F}_{p^n}$. Damit gilt $\mathrm{ord}(\mathrm{Fr}) \leq n$. Weiter gilt für $x \in \mathbb{F}_{p^n}$ die Gleichung $x = \mathrm{Fr}^{\mathrm{ord}(\mathrm{Fr})}(x) = x^{p^{\mathrm{ord}(\mathrm{Fr})}}$ und x ist Nullstelle von $g := X^{p^{\mathrm{ord}(\mathrm{Fr})}} - 1 \in \mathbb{F}_p[X]$. Da g höchstens $p^{\mathrm{ord}(\mathrm{Fr})}$ Nullstellen besitzt, folgt $p^{\mathrm{ord}(\mathrm{Fr})} \geq |\mathbb{F}_{p^n}| = p^n$ und damit $\mathrm{ord}(\mathrm{Fr}) = n$. Wir schließen
$$n = \langle \mathrm{Fr} \rangle \subseteq \mathrm{Aut}(\mathbb{F}_{p^n} : \mathbb{F}_p) \leq [\mathbb{F}_{p^n} : \mathbb{F}_p] = n,$$
also $\mathrm{Aut}(\mathbb{F}_{p^n} : \mathbb{F}_p) = \langle \mathrm{Fr} \rangle \cong \mathbb{Z}/\langle n \rangle$.

(2) Folgt direkt aus (1) .

(3) Ein sei $K \subseteq \mathbb{F}_{p^n}$ ein Teilkörper mit $|K| = p^m$. Es gilt $\mathbb{F}_p \subseteq K \subseteq \mathbb{F}_{p^n}$. Nach der Turmformel gilt
$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : K] \cdot [K : \mathbb{F}_p] = [\mathbb{F}_{p^n} : K] \cdot m,$$
also $m \mid n$.

Es sei umgekehrt s ein Teiler von n. Da $\mathrm{Aut}(\mathbb{F}_{p^n} : \mathbb{F}_p)$ nach (1) zyklisch ist, existiert nach Satz 1.3.2 eine Untergruppe $U \subseteq \mathrm{Aut}(\mathbb{F}_{p^n} : \mathbb{F}_p)$ der Ordnung $|U| = \frac{n}{s}$. Nach Satz 6.1.2 ist $\mathbb{F}_{p^n} : (\mathbb{F}_{p^n})^U$ eine Galoiserweiterung mit $[\mathbb{F}_{p^n} : (\mathbb{F}_{p^n})^U] = |U| = \frac{n}{s}$. Es sei $L := (\mathbb{F}_{p^n})^U$. Dann gilt $|L| = p^{[L : \mathbb{F}_p]}$ und
$$[L : \mathbb{F}_p] = \frac{[\mathbb{F}_{p^n} : \mathbb{F}_p]}{[\mathbb{F}_{p^n} : L]} = \frac{n}{\frac{n}{s}} = s.$$

□

7.3 Einheitswurzeln

Definition. Sei K ein Körper, $n \in \mathbb{N}$. Ein Element $\zeta \in K^\times$ heißt **n-te Einheitswurzel von K**, falls $\zeta^n = 1$ gilt. Gilt zudem $\mathrm{ord}(\zeta) = n$, so nennt man ζ eine **primitive n-te Einheitswurzel**.

Bemerkungen 7.3.1. Es sei K ein Körper.

(1) Sei $n \in \mathbb{N}$. Dann ist $\mu_n(K) := \{\zeta \in K^\times \mid \zeta^n = 1\}$ eine endliche Untergruppe von $K^\times$ und nach Satz 4.2.5 zyklisch.

(2) Für $n \in \mathbb{N}$ gilt
$$\mu_n(\mathbb{C}) = \{e^{2\pi i \frac{m}{n}} \mid 0 \leq m \leq n-1\} = \mathcal{C}_n$$
und für $\ell \in \{0, \ldots, n-1\}$ ist $e^{2\pi i \frac{\ell}{n}} = (e^{\frac{2\pi i}{n}})^\ell$ genau dann eine primitive n-te Einheitswurzel, wenn $\mathrm{ggT}(\ell, n) = 1$ (vgl. Satz 1.3.1).

(3) Sei $\mathrm{char}(K) = p > 0$. Ist $\zeta \in \mu_p(K)$, so gilt nach Lemma 7.2.1

$$(\zeta - 1)^p = \zeta^p - 1^p = 0,$$

und damit $\zeta = 1$. Wir erhalten $\mu_p(K) = \{1\}$ und K besitzt keine primitiven p-ten Einheitswurzeln.

Definition. Sei $n \in \mathbb{N}$.

(1) Für einen Körper sei $\mu_n^*(K) := \{\zeta \in \mu_n(K) \mid \mathrm{ord}(\zeta) = n\}$ die Menge der primitiven n-ten Einheitswurzeln von K.

(2) Das Polynom

$$\Phi_n := \prod_{\zeta \in \mu_n^*(\mathbb{C})} (X - \zeta) \in \mathbb{C}[X]$$

heißt das n**-te Kreisteilungspolynom**.

Satz 7.3.2. *Es sei $n \in \mathbb{N}$.*

(1) Es gilt $X^n - 1 = \prod_{d|n} \Phi_d$.

(2) $\Phi_n \in \mathbb{Z}[X]$.

Beweis.

(1) Es gilt nach dem Satz von Lagrange

$$\mu_n(\mathbb{C}) = \bigsqcup_{d|n} \{\zeta \in \mu_n(\mathbb{C}) \mid \mathrm{ord}(\zeta) = d\} = \bigsqcup_{d|n} \mu_d^*(\mathbb{C}).$$

Damit erhalten wir

$$X^n - 1 = \prod_{\zeta \in \mu_n(\mathbb{C})} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mu_d^*(\mathbb{C})} (X - \zeta) = \prod_{d|n} \Phi_d.$$

(2) Die Behauptung gilt für $n = 1$. Für $n > 1$ folgt nach (1)

$$X^n - 1 = \Phi_n \Big(\prod_{d|n, d \neq n} \Phi_d \Big).$$

Induktiv können wir $f_n := \prod_{d|n, d\neq n} \Phi_d \in \mathbb{Z}[X]$ annehmen. Da f_n normiert ist, liefert Satz 4.2.2 Polynome $q, r \in \mathbb{Z}[X]$ mit

$$X^n - 1 = q f_n + r \quad \text{und} \quad 0 \leq \deg(r) < \deg(f_n) \ \text{ oder } \ r = 0.$$

Wir erhalten aus diesen Gleichungen

$$r = (\Phi_n - q) f_n,$$

was im Fall $\Phi_n \neq q$ die Ungleichung $\deg(r) \geq \deg(f_n)$ nach sich zieht, ein Widerspruch. Also gilt $\Phi_n = q \in \mathbb{Z}[X]$.

□

Satz 7.3.3. *Sei $n \in \mathbb{N}$. Dann ist Φ_n irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$, und $\deg(\Phi_n) = \varphi(n)$.*

Beweis. Wir beweisen zunächst zwei Hilfsaussagen.

(1) Es sei $\zeta \in \mu_n^*(\mathbb{C})$ sowie p eine Primzahl, die n nicht teilt. Dann gilt $\mu_{\zeta,\mathbb{Q}}, \mu_{\zeta^p,\mathbb{Q}} \in \mathbb{Z}[X]$ für die Minimalpolynome von ζ und ζ^p über $\mathbb{Q}$ und $\mu_{\zeta,\mathbb{Q}}, \mu_{\zeta^p,\mathbb{Q}}$ sind Teiler von Φ_n in $\mathbb{Z}[X]$:

Nach Satz 7.3.2 gilt $\Phi_n \in \mathbb{Z}[X]$ und $\mathbb{Z}[X]$ ist faktoriell nach Satz 4.3.3. Daher existieren irreduzible Polynome $f_1, \ldots, f_\ell \in \mathbb{Z}[X]$ mit

$$\Phi_n = f_1 \cdots f_\ell.$$

Da Φ_n normiert ist, sind die Leitkoeffizienten der f_i Einheiten von $\mathbb{Z}$ und somit Elemente von $\{1, -1\}$. Ersetzen wir gegebenenfalls f_i durch $-f_i$, so können wir annehmen, dass jedes f_i normiert ist.[2] Nach Korollar 4.3.5 ist jedes f_i irreduzibel in $\mathbb{Q}[X]$. Wegen $p \nmid n$ gilt nach Satz 1.3.1 $\zeta^p \in \mu_n^*(\mathbb{C})$ und damit $\Phi_n(\zeta) = 0 = \Phi_n(\zeta^p)$. Daher sind $\mu_{\zeta,\mathbb{Q}}$ und $\mu_{\zeta^p,\mathbb{Q}}$ Teiler von Φ_n. Es gilt also $\{\mu_{\zeta,\mathbb{Q}}, \mu_{\zeta^p,\mathbb{Q}}\} \subseteq \{f_i \mid i \in \{1, \ldots, \ell\}\} \subseteq \mathbb{Z}[X]$.

(2) Sei $\zeta \in \mu_n^*(\mathbb{C})$ sowie p eine Primzahl, die n nicht teilt. Dann gilt $\mu_{\zeta,\mathbb{Q}} = \mu_{\zeta^p,\mathbb{Q}}$:

Wir setzen $f := \mu_{\zeta,\mathbb{Q}}$ und $g := \mu_{\zeta^p,\mathbb{Q}}$. Wir nehmen $f \neq g$ an. Da $f, g \in \mathbb{Z}[X]$ irreduzibel sind, gilt nach (1) $fg \mid_{\mathbb{Z}[X]} \Phi_n$ und somit $fg \mid_{\mathbb{Z}[X]} X^n - 1$. Wegen $g(\zeta^p) = 0$ ist ζ eine Nullstelle des Polynoms $g(X^p) \in \mathbb{Z}[X]$ und es folgt $f|_{\mathbb{Q}[X]} g(X^p)$. Da f als normiertes Polynom primitiv ist, liefert Satz 4.3.2 $f|_{\mathbb{Z}[X]} g(X^p)$. Sei also $h \in \mathbb{Z}[X]$ mit $g(X^p) = fh$.

Wir betrachten die kanonische Projektion $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/(p)$ sowie den induzierten Homomorphismus $\pi^* : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/(p)[X]$. Es sei $g = \sum_{i=0}^s a_i X^i$. Dann gilt aufgrund von Lemma 7.2.1 und $\mathrm{char}((\mathbb{Z}/(p)[X]) = \mathrm{char}(\mathbb{Z}/(p)) = p$:

$$\pi^*(g)^p \quad = \quad (\sum_{i=0}^s \pi(a_i) X^i)^p = \sum_{i=0}^s \pi(a_i)^p X^{ip} = \sum_{i=0}^s \pi(a_i) X^{ip} = \pi^*(g(X^p)) = \pi^*(f)\pi^*(h).$$

Sei nun $q \in \mathbb{Z}/(p)[X]$ ein irreduzibler Faktor von $\pi^*(f)$. Dann teilt q auch $\pi^*(g)^p$ und somit $\pi^*(g)$. Also ist q^2 ein Teiler von $\pi^*(f)\pi^*(g)$ und daher auch von $X^n - 1 \in \mathbb{Z}/(p)[X]$. Wir schreiben also $X^n - 1 = q^2 r$ für ein $r \in \mathbb{Z}/(p)[X]$. Wir bilden nun die Ableitung und erhalten

$$nX^{n-1} = (q^2 r)' = 2qq'r + q^2 r' = q(2q'r + qr').$$

Wegen $p \nmid n$, gilt $n.1 \neq 0$ in $\mathbb{Z}/(p)$. Da q irreduzibel ist, gibt es also ein $m \in \mathbb{Z}$ mit $p \nmid m$ und $q = mX$. Es gilt aber $X \nmid X^n - 1$, da $0_{\mathbb{Z}/(p)}$ keine Nullstelle von $X^n - 1$ ist, ein Widerspruch.

Da Φ_n normiert und $\deg(\Phi_n) \geq 1$ ist, liefert Korollar 4.3.5 die Äquivalenz der beiden Behauptungen.

Es sei nun K_n ein Zerfällungskörper von Φ_n über $\mathbb{Q}$ sowie $\zeta \in K_n$ eine primitive n-te Einheitswurzel. Ist $\eta \in K_n$ eine weitere primitive n-te Einheitswurzel, so gibt es nach Satz 1.3.1 ein $m \in \mathbb{N}$ mit $\eta = \zeta^m$ und $\mathrm{ggT}(m, n) = 1$. Sei $m = p_1 \cdots p_r$ die Primfaktorzerlegung von m. Für $j \in \{1, \ldots, r\}$ gilt $\mathrm{ggT}(p_1 \cdots p_j, n) = 1$. Daher ist $\zeta^{p_1 \cdots p_j}$ nach Satz 1.3.1 eine primitive n-te Einheitswurzel. Wiederholte Anwendung von (2) zeigt: $\mu_{\zeta,\mathbb{Q}} = \mu_{\zeta^{p_1 \cdots p_j},\mathbb{Q}}$ für $1 \leq j \leq r$. Insbesondere folgt $\mu_{\zeta,\mathbb{Q}}(\zeta^m) = 0$. Damit hat $\mu_{\zeta,\mathbb{Q}}$ mindestens $\varphi(n)$ Nullstellen. Wegen $\Phi_n(\zeta) = 0$ folgt $\mu_{\zeta,\mathbb{Q}} | \Phi_n$. Damit gilt $\deg(\Phi_n) = \varphi(n) = \deg(\mu_{\zeta,\mathbb{Q}})$. Mithin ist $\Phi_n = \mu_{\zeta,\mathbb{Q}}$ irreduzibel.

□

[2] Da die Anzahl der f_i mit Leitkoeffizient -1 notwendig gerade ist, ist dies möglich.

7.4 Konstruktion mit Zirkel und Lineal

In diesem Abschnitt beschäftigen wir uns mit der Frage, welche Punkte sich aus einer Menge $M \subseteq \mathbb{R}^2$ nur durch Zirkel und Lineal konstruieren lassen. Wichtig ist dabei, dass das Lineal nicht beschriftet ist. Es kann also nur für das Zeichnen von (unendlich langen) Geraden benutzt werden. Der Zirkel erlaubt den Abstand r zweier bereits konstruierter Punkte zu messen und einen Kreis von Radius r um einen bereits konstruierten Punkt zu zeichnen. Wir identifizieren die Ebene $\mathbb{R}^2$ mit $\mathbb{C}$ durch $(a, b) = a + bi$. Für $z = a + bi \in \mathbb{C}$ sei wie üblich $\Re(z) := a$ und $\Im(z) := b$.

Es sei M eine Menge $\{0, 1\} \subseteq M \subseteq \mathbb{C}$. Wir bezeichnen mit $g(M)$ die Menge aller Geraden, die zwei Punkte von M enthalten und mit $o(M)$ die Menge aller Kreise, die als Mittelpunkt einen Punkt aus M enthalten, sodass der Radius einem Abstand von zwei Punkten aus M entspricht.

Wir definieren die Menge $M_1 := M \cup c(M)$, wobei $c(M)$ die Punkte sind, die sich als Schnittpunkt von zwei verschiedenen Geraden aus $g(M)$, von zwei verschiedenen Kreisen aus $o(M)$ oder von einer Geraden aus $g(M)$ und eines Kreises $o(M)$ sind.

Induktiv erhalten wir eine Folge

$$M_0 := M, M_1 := M \cup c(M), M_2 := M_1 \cup c(M_1), M_3 := M_2 \cup c(M_2), \ldots$$

und definieren die Menge der aus M *konstruierbaren Punkte*

$$\widehat{M} := \bigcup_{i \in \mathbb{N}_0} M_i.$$

Der folgende Satz wird in [3, 19.2, 19.3] bewiesen. Wir verwenden diesen ohne Beweis.

Satz 7.4.1. *Es sei $\{0, 1\} \subseteq M \subseteq \mathbb{C}$ eine Menge. Die Menge $\widehat{M} \subseteq \mathbb{C}$ besitzt folgende Eigenschaften.*

(1) $\widehat{M} \subseteq \mathbb{C}$ ist ein Teilkörper von $\mathbb{C}$.

(2) Es gilt $i \in \widehat{M}$.

(3) Für $z \in \widehat{M}$ gilt $|z|, \Re(z), \Im(z), \overline{z} \in \widehat{M}$.

*(4) Es sei $z \in \widehat{M}$. Dann sind auch die Nullstellen von $X^2 - z$ in $\widehat{M}$, das heißt $\widehat{M}$ ist **quadratisch abgeschlossen**.*

Lemma 7.4.2. *Es sei $\{0, 1\} \subseteq K \subseteq \mathbb{C}$ ein Körper mit $i \in K$ und $\overline{K} = K$ (d.h. K ist abgeschlossen unter der komplexen Konjugation). Weiter sei $z \in K \cup c(K)$.*

(1) Es existiert ein Körper $K \subseteq L \subseteq \mathbb{C}$ mit $[L : K] \leq 2$ und $z \in L$.

(2) Ist $K \subseteq L \subseteq \mathbb{C}$ ein Körper mit $[L : K] \leq 2$, so existiert ein Erweiterungskörper $L \subseteq N \subseteq \mathbb{C}$ mit $[N : L] \leq 2$ und $\overline{N} = N$.

Beweis.

(1) Es sei $\alpha \in K$. Dann gilt $\Re(\alpha) = \frac{1}{2}(\alpha + \overline{\alpha}), \Im(\alpha) = \frac{1}{2i}(\alpha - \overline{\alpha}) \in K$. Weiter gilt $|\alpha|^2 = \Re(\alpha)^2 + \Im(\alpha)^2 \in K$. Diese Eigenschaften werden im Beweis mehrmals benutzen. Nach Definition müssen wir drei Fälle unterscheiden.

(i) z ist Schnitt zweier Geraden aus $g(K)$: Wir finden $z_i \in K$ für $1 \leq i \leq 4$ und $\lambda, \mu \in \mathbb{R}$ mit $z_2 \neq 0 \neq z_4$ und

$$z_1 + \lambda z_2 = z = z_3 + \mu z_4.$$[3]

Vergleich der Real- und Imaginärteile liefert

$$\begin{aligned} \Re(z_1) + \lambda \Re(z_2) &= \Re(z_3) + \mu \Re(z_4) \\ \Im(z_1) + \lambda \Im(z_2) &= \Im(z_3) + \mu \Im(z_4) \end{aligned}$$

und damit

$$\begin{pmatrix} \Re(z_2) & -\Re(z_4) \\ \Im(z_2) & -\Im(z_4) \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} \Re(z_3) - \Re(z_1) \\ \Im(z_3) - \Im(z_1) \end{pmatrix} \in K^2.$$

Da beide Geraden nicht parallel sind, verschwindet die Determinante der Matrix nicht und ist damit in K invertierbar. Es folgt $\lambda, \mu \in K$ und damit sogar $z \in K$. Wir können $L = K$ wählen.

(ii) z ist Schnittpunkt einer Geraden aus $g(K)$ und eines Kreises aus $o(K)$: Wir finden $z_1, z_2 \neq 0, z_3 \in K$ und $\lambda \in \mathbb{R}$ sowie $r \in \mathbb{R}_{>0} \cap K$ mit $z = z_1 + \lambda z_2$ sowie $(\Re(z) - \Re(z_3))^2 + (\Im(z) - \Im(z_3))^2 = r^2$. Wir erhalten

$$(\Re(z_1) + \lambda \Re(z_2) - \Re(z_3))^2 + (\Im(z_1) + \lambda \Im(z_2) - \Im(z_3))^2 = r^2$$

und damit

$$u\lambda^2 + v\lambda + w = 0$$

für $u, v, w \in K$ mit $u = \Re(z_2)^2 + \Im(z_2)^2 \neq 0$. Also finden wir eine Gleichung $\lambda^2 + p\lambda + q = 0$ mit $p, q \in K$ und erhalten $\lambda = -\frac{p}{2} \pm \sqrt{\alpha}$ mit $\alpha = \frac{p^2}{4} - q \in K$. Das heißt $\lambda \in K(\sqrt{\alpha})$ und damit $z = z_1 + \lambda z_2 \in K(\sqrt{\alpha})$. Es gilt $[K(\sqrt{\alpha}) : K] \leq 2$, da $X^2 - \alpha \in K[X]$. Wir wählen $L = K(\sqrt{\alpha})$.

(iii) z ist Schnittpunkt zweier Kreise aus $o(K)$: Wir finden $z_1 \neq z_2 \in K$ und $r, s \in \mathbb{R}_{>0} \cap K$ mit

$$(\Re(z) - \Re(z_1))^2 + (\Im(z) - \Im(z_1))^2 = r^2 \text{ und } (\Re(z) - \Re(z_2))^2 + (\Im(z) - \Im(z_2))^2 = s^2.$$

Subtraktion beider Gleichungen liefert $u\Re(z) + v\Im(z) = w$ mit $u = 2(\Re(z_2) - \Re(z_1))$, $v = 2(\Im(z_2) - \Im(z_2)) \in K \cap \mathbb{R}$ und $w = |z_2|^2 - |z_1|^2 + r^2 - s^2 \in K \cap \mathbb{R}$. Da $z_1 \neq z_2$ gilt, ist $u \neq 0$ oder $v \neq 0$. Es gelte o.B.d.A. $u \neq 0$. Dann ist $\frac{w}{u} + 0 \cdot i + \mathbb{R}(-\frac{v}{u} + i) \in o(K)$ und $\lambda := \Im(z)$ liefert $(\frac{w}{u} + 0 \cdot i) + \lambda(-\frac{v}{u} + i) = \frac{w - v\Im(z)}{u} + \Im(z)i = \Re(z) + \Im(z)i = z$. Damit ist z Schnittpunkt einer Geraden aus $g(K)$ und eines Kreises aus $o(K)$. Wir wenden Fall (ii) an.

[3] Eine Gerade ist von der Form $w_1 + \mathbb{R}(w_1 - w_2)$ für $w_1, w_2 \in K$ mit $0 \neq w_1 - w_2 \in K$.

(2) Es $\sigma\colon \mathbb{C} \longrightarrow \mathbb{C}$ ein Automorphismus mit $\sigma(K) = K$. Damit ist $\sigma|_K\colon K \longrightarrow K$ ein Automorphismus. Wir betrachten den induzierten Isomorphismus $(\sigma|_K)^*\colon K[X] \longrightarrow K[X]$ gegeben durch $(\sigma|_K)^*(x) = \sigma(x)$ für alle $x \in K$ und $(\sigma|_K)^*(X) = X$. Es sei $f = \sum_{i=0}^n \lambda_i X^i \in K[X]$ ein irreduzibles Polynom. Dann ist $(\sigma|_K)^*(f) = \sum_{i=0}^n \sigma(\lambda_i) X^i \in K[X]$ irreduzibel mit $\deg((\sigma|_K)^*(f)) = \deg(f)$ und für eine Nullstelle $\alpha \in \mathbb{C}$ von f gilt

$$(\sigma|_K)^*(f)(\sigma(\alpha)) = \sum_{i=0}^n \sigma(\lambda_i)\sigma(\alpha)^i = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Wir wenden diese Überlegung nun auf die komplexe Konjugation $\sigma(z) = \overline{z}$ an. Nach Voraussetzungen finden wir $y \in L$ mit $K(y) = L$ und $\deg \mu_y = [L : K] \leq 2$. Dann gilt $\mu_{\overline{y}} = (\sigma|_K)^*(\mu_y)$. Das heißt $[K(\overline{y}) : K] = \deg \overline{\mu}_y = \deg(\mu_y) \leq 2$. Wir setzen $N := K(y, \overline{y})$. Es gilt

$$\overline{N} = \overline{K(y,\overline{y})} = K(\overline{y}, \overline{\overline{y}}) = K(y, \overline{y}) = N$$

und $[N : L] = [K(y, \overline{y}) : K(y)] = [L(\overline{y}) : L] \leq [K(\overline{y}) : K] \leq 2$.

□

Bemerkung 7.4.3. Es sei $x \in M_\ell \subseteq \widehat{M} = \bigcup_{n\geq 0} M_n$. Dann existieren endlich viele Punkte in $M_{\ell-1}$, die für die Konstruktion von x benötigt werden. Induktiv, folgt dass für $z \in \widehat{M}$ eine endliche Folge $z_1, \ldots, z_n = z \in \widehat{M}$ existiert, sodass jedes z_i aus $M \cup \{z_1, \ldots, z_{i-1}\}$ mit nur einer Operation konstruiert werden kann. Da $M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n$ gilt, ist weiter $z_i \in M_i$ für alle $i \in \{1, \ldots, n\}$.

Es sei $\{0, 1\} \subseteq M \subseteq \mathbb{C}$. Nach Lemma 5.1.2 ist $\mathbb{Q} \subseteq \widehat{M}$ ein Teilkörper von $\widehat{M}$. Wir definieren $\overline{M} := \{\overline{z} \mid z \in M\}$ und Satz 7.4.1 zeigt, dass

$$K_0 := \mathbb{Q}(M \cup \overline{M}) \subseteq \mathbb{C}.$$

ein Teilkörper von $\widehat{M}$ ist. Weiter gilt $\overline{K_0} = \overline{\mathbb{Q}(M \cup \overline{M})} = \mathbb{Q}(\overline{M} \cup \overline{\overline{M}}) = K_0$.

Satz 7.4.4. *Es sei $\{0, 1\} \subseteq M \subseteq \mathbb{C}$ und $K_0 := \mathbb{Q}(M \cup \overline{M}) \subseteq \widehat{M}$. Für $z \in \mathbb{C}$ sind folgende Aussagen äquivalent.*

(1) Es gilt $z \in \widehat{M}$.

(2) Es existiert $n \in \mathbb{N}_0$ und Körpererweiterungen $K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_n$ mit $z \in K_n$ und $[K_i : K_{i-1}] = 2$ für alle $i \in \{1, \ldots, n\}$ gilt.

(3) Es existiert eine Galoiserweiterung $L : K_0$ mit $z \in L \subseteq \mathbb{C}$, sodass $[L : K_0]$ eine 2er-Potenz ist.

Beweis. (1) ⇒ (2). Der Beweis ist klar für $z \in K_0$, sei daher $z \in \widehat{M} \setminus K_0$. Da $z \in \widehat{M} = \bigcup_{n\in\mathbb{N}_0} M_n$ gilt, finden wir $m \in \mathbb{N}$ und eine Folge, $z_1, \ldots, z_m = z \in \widehat{M}$, sodass für jedes $j \in \{1, \ldots, m\}$ der Punkt z_j mit nur einer Operation aus $M \cup \{z_1, \ldots, z_{j-1}\}$ konstruierbar ist, d.h.

$$z_j \in M \cup \{z_1, \ldots, z_{j-1}\} \cup c(M \cup \{z_1, \ldots, z_{j-1}\}).$$

Wir zeigen nun induktiv über j, dass ein Körperturm $K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \cdots \subsetneq K_\ell$ wie in (2) existiert, der $M \cup \{z_1, \ldots, z_j\} \subseteq K_\ell$ und $\overline{K_\ell} = K_\ell$ erfüllt. Daraus folgt die Behauptung. Da $[K_0(i) : K_0] \leq 2$ und $\overline{K_0(i)} = K_0(i)$ gilt, können wir annehmen, dass $i \in K_0$, da wir ansonsten die Induktion mit $K_0(i)$ beginnen.

Es gilt $z_1 \in M \cup c(M) \subseteq K_0 \cup c(K_0)$. Wir können $z_1 \notin K_0$ annehmen. Nach Lemma 7.4.2(1) finden wir einen Erweiterungskörper $K_0 \subseteq L$ mit $z_1 \in L$ und $[L : K_0] = 2$ (da $L \neq K_0$). Ist $\overline{L} = L$, so wählen wir $K_1 := L$. Ansonsten liefert Lemma 7.4.2(2) einen Erweiterungskörper N mit $\overline{N} = N$ und $[N : L] = 2$. Wir wählen $K_1 := L$ und $K_2 := N$.

Es sei nun $j > 1$. Dann finden wir einen Körperturm $K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \cdots \subsetneq K_\ell$ wie in (2) mit $M \cup \{z_1, \ldots, z_{j-1}\} \subseteq K_\ell$ und $\overline{K_\ell} = K_\ell$. Wir können erneut $z_j \notin K_\ell$ annehmen. Es gilt

$$z_j \in M \cup \{z_1, \ldots, z_{j-1}\} \cup c(M \cup \{z_1, \ldots, z_{j-1}\}) \subseteq K_\ell \cup c(K_\ell).$$

Nun verfahren wir analog wie für z_1.

(2) $\Rightarrow$ (1). Für $i \in \{1, \ldots, n\}$ finden wir $a_i \in K_i \setminus K_{i-1}$ mit $K_{i-1}(a_i) = K_i$ mit $a_i^2 \in K_{i-1}$. Damit ist a_i Nullstelle von $X_i^2 - a_i^2 \in K_{i-1}[X]$. Wir schließen mit $K_0 \subseteq \widehat{M}$ und Satz 7.4.1(4) $a_1 \in \widehat{M}$, also folgt $K_1 = K_0(a_1) \subseteq \widehat{M}$. Induktiv folgt $K_i = K_{i-1}(a_i) \subseteq \widehat{M}$ für alle $i \in \{1, \ldots, n\}$, also $z \in K_n \in \widehat{M}$.

(2) $\Rightarrow$ (3). Nach Satz 6.2.4 existiert ein Erweiterungskörper $K_n \subseteq N$, sodass $N \colon K_0$ eine Galoiserweiterung ist. Nach dem Satz vom primitiven Element existiert $a \in K_n$ mit $K_0(a) = K_n$. Es sei $\mathrm{Aut}(N : K_0) = \{\sigma_1, \ldots, \sigma_m\}$ mit $\sigma_1 = \mathrm{id}_N$ und wir definieren $a_i := \sigma_i(a)$ für $i \in \{1, \ldots, m\}$, sowie $L := K_0(a_1, \ldots, a_m) \subseteq N$. Für $\sigma \in \mathrm{Aut}(N : K_0)$ ist die Abbildung

$$\mathrm{Aut}(N : K_0) \longrightarrow \mathrm{Aut}(N : K_0)\ ;\ \tau \mapsto \sigma \circ \tau$$

eine Bijektion. Es folgt

$$\sigma_i(L) = \sigma_i(K_0(a_1, \ldots, a_m)) = K_0((\sigma_i \circ \sigma_1)(a), \cdots, (\sigma_i \circ \sigma_m)(a)) = K(a_1, \ldots, a_m) = L.$$

Wir zeigen induktiv nach $1 \leq \ell \leq m$, dass $[K_0(a_1, \ldots, a_\ell) : K_0]$ eine 2er-Potenz ist. Für $\ell = 1$ gilt $K_0(a_1) = K_0(a) = K_n$ und die Behauptung gilt nach Voraussetzung. Es sei nun $\ell > 1$. Es gilt

$$[K_0(a_1, \ldots, a_\ell) \colon K_0] = [K_0(a_1, \ldots, a_{\ell-1})(a_\ell) \colon K_0(a_1, \ldots, a_{\ell-1})] \cdot \underbrace{[K_0(a_1, \ldots, a_{\ell-1}) \colon K_0]}_{2er-Potenz}.$$

Es sei $f \in K_0[X]$ das Minimalpolynom von a. Dann ist f auch das Minimalpolynom von $a_\ell = \sigma_\ell(a)$, da $\sigma_\ell|_{K_0} \in \mathrm{Aut}(N \colon K_0)$. Mit $a \in K_n$ folgt, dass $\deg(f) = [K_0(a_\ell) : K_0]$ eine $2er$-Potenz ist. Es ist $f \in K_0(a_1, \ldots, a_{\ell-1})[X]$ und damit ist $[K_0(a, a_1, \ldots, a_{\ell-1})(a_\ell) \colon K_0(a, a_1, \ldots, a_{\ell-1})]$ ein Teiler von $[K_0(a_\ell) \colon K_0] = \deg(f)$.

(3) $\Rightarrow$ (2). Wir schreiben $[L : K_0] = 2^n$. Nach Satz 6.1.3 ist $G := \mathrm{Aut}(L : K_0)$ eine 2-Gruppe der Ordnung 2^n. Wiederholte Anwendung des Satzes von Sylow liefert eine Folge von Untergruppen

$$\{\mathrm{id}_L\} = G_0 \subsetneq G_1 \subsetneq G_2 \subsetneq \cdots \subsetneq G_n = G,$$

mit $G_i = 2^i$ für alle $i \in \{0, \ldots, n\}$. Die inklusionsumkehrende Bijektion aus der Galoiskorrespondenz liefert uns einen Körperturm

$$K_0 = L^G \subsetneq K_1 := L^{G_{n-1}} \subsetneq \cdots \subsetneq K_{n-1} := L^{G_1} \subsetneq K_n := L^{G_0} = L.$$

Nach 6.1.2 gilt $\mathrm{Aut}(L : L^{G_{n-i}}) = G_{n-i}$. Nach Satz 6.1.6 gilt

$$[K_i : K_0] = \frac{[L : K_0]}{[L : K_i]} = \frac{|\mathrm{Aut}(L : K_0)|}{|\mathrm{Aut}(L : L^{G_{n-i}})|} = \frac{|G|}{|G_{n-i}|} = \frac{2^n}{2^{n-i}} = 2^i$$

und die Turmformel liefert $[K_i : K_{i-1}] = \frac{[K_i : K_0]}{[K_{i-1} : K_0]} = 2$. □

Korollar 7.4.5. *Es sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$. Ist $z \in \widehat{M}$, so ist z algebraisch über K_0 und $[K_0(z)\colon K_0]$ eine 2er-Potenz.*

Natürlich lassen sich alle Zahlen in $\mathbb{C}$ konstruieren, wenn wir sie als gegeben, also als Elemente von M, voraussetzen.

Satz 7.4.6 (Quadratur des Kreises)**.** *Es sei K ein Kreis mit Mittelpunkt 0 und Radius 1, sodass nur die Punkte $0, 1 \in \mathbb{C}$ markiert sind. Es lässt sich daraus kein Quadrat Q mit dem Flächeninhalt von K konstruieren.*

Beweis. Es ist $M = \{0,1\}$ und damit $K_0 = \mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$. Der Kreis K besitzt den Flächeninhalt π. Wäre Q konstruierbar, so auch die Länge $\sqrt{\pi}$. Insbesondere, wäre $\sqrt{\pi} \in \widehat{M}$ algebraisch über $K_0 = \mathbb{Q}$ und nach Satz 5.3.1 auch π. Ein Widerspruch zum Satz von Lindemann. □

Satz 7.4.7 (Konstruierbarkeit von Einheitzwurzeln)**.** *Es sei $n \in \mathbb{N}$. Die Einheitswurzel $\zeta_n := e^{\frac{2\pi i}{n}}$ ist genau dann aus $M = \{0,1\}$ konstruierbar, wenn $\varphi(n) = |\{s \in \{1,\dots,n\} \mid \mathrm{ggT}(s,n) = 1\}|$ eine $2er$-Potenz ist.*

Beweis. Da $M = \{0,1\}$ ist, gilt $K_0 = \mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$. Nach Satz 7.3.3 ist $\mathbb{Q}(\zeta_n)\colon \mathbb{Q}$ eine Galoiserweiterung vom Grad $\varphi(n)$, also

$$[K_0(\zeta_n)\colon K_0] = [\mathbb{Q}(\zeta_n)\colon \mathbb{Q}] = \varphi(n).$$

Ist $\varphi(n)$ keine 2er-Potenz, so ist ζ_n nach Korollar 7.4.5 nicht konstruierbar. Ist umgekehrt $\varphi(n)$ eine 2er-Potenz, so ist ζ_n nach Satz 7.4.4(3) konstruierbar. □

Satz 7.4.8 (Konstruktion regelmäßiger n-Ecke)**.** *Sei $n \in \mathbb{N}_{\geq 3}$. Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal aus $M = \{0,1\}$ konstruierbar, wenn $\varphi(n)$ eine 2er-Potenz ist.*

Beweis. Das regelmäßige n-Eck ist genau dann konstruierbar, wenn $e^{\frac{2\pi i}{n}}$ konstruierbar ist. □

Satz 7.4.9 (Winkeldreiteilung)**.** *Der Winkel 20° lässt sich nicht mit Zirkel und Lineal konstruieren. Insbesondere ist die Winkeldreiteilung i.A. nicht möglich.*

Beweis. Der Winkel 20° entspricht $e^{\frac{2\pi i}{18}}$. Es gilt $\varphi(18) = \varphi(2)\varphi(3^2) = 6$. Damit ist 20° nach Satz 7.4.8 nicht aus $M := \{0,1\}$ konstruierbar,

Wäre die Winkeldreiteilung stets möglich, so wäre 20° aus 60° konstruierbar, das heißt $e^{\frac{2\pi i}{18}}$ aus $\widehat{N}$ für $N := \{0, 1, e^{\frac{2\pi i}{6}}\}$. Es gilt $\varphi(6) = 2$. Damit ist $e^{\frac{2\pi i}{6}}$ nach Satz 7.4.8 aus M konstruierbar. Das bedeutet $N \subseteq \widehat{M}$ und damit folgt $\widehat{N} = \widehat{M}$. Also ist $e^{\frac{2\pi i}{18}} \in \widehat{N} = \widehat{M}$ aus $M = \{0,1\}$ konstruierbar, ein Widerspruch. □

Literaturverzeichnis

[1] S. Bosch, *Algebra*, Springer-Verlag, 1996.

[2] H-D. Ebbinghaus, *Einführung in die Mengenlehre*, Springer-Verlag, 2021.

[3] I. Kersten, *Algebra*, Universitätsdrucke Göttingen, 2006.

[4] J.C. Jantzen and J. Schwermer, *Algebra*, Springer-Verlag, 2006.

[5] R. Weidmann, *Vorlesungsskript Lineare Algebra I/II* (2023/24).

[6] R. A. Wilson, *An elementary proof that not all principal ideal domains are Euclidean domains*, The Mathematical Gazette (2017).