Vorlesungsskript Algebra I

Wintersemester 2021
CAU Kiel

Daniel Bissinger

Version: 4. Februar 2024

Inhaltsverzeichnis

1 Grundlagen der Gruppentheorie **1**
- 1.1 Untergruppen und der Satz von Lagrange . . . 1
- 1.2 Zyklische Gruppen . . . 4
- 1.3 Homomorphismen und Normalteiler . . . 8
- 1.4 Die symmetrische Gruppe $\mathcal{S}_n$ . . . 10
- 1.5 Faktorgruppen und Isomorphiesätze . . . 13
- 1.6 Produkte von Gruppen . . . 16
- 1.7 Operationen von Gruppen und die Klassengleichung . . . 19

2 Strukturtheorie endlicher Gruppen **25**
- 2.1 p-Gruppen . . . 25
- 2.2 Die Sätze von Sylow . . . 26
- 2.3 Auflösbare Gruppen . . . 28

3 Grundlagen der Ringtheorie **33**
- 3.1 Ringe, Homomorphismen und Ideale . . . 33
- 3.2 Einheiten und Nullteiler . . . 36
- 3.3 Kommutative Ringe . . . 40
- 3.4 Ringe der Brüche . . . 43
- 3.5 Teilbarkeit in Integritätsbereichen . . . 46

4 Polynomringe **51**
- 4.1 Konstruktion von Polynomringen . . . 51
- 4.2 Polynome in einer Variablen und Nullstellen . . . 53
- 4.3 Unzerlegbare Polynome . . . 57

5 Elementare Theorie der Körpererweiterungen **64**
- 5.1 Körpererweiterungen . . . 64
- 5.2 Endliche Körpererweiterungen . . . 65
- 5.3 Algebraische Körpererweiterungen . . . 67
- 5.4 Zerfällungskörper . . . 74
- 5.5 Lineare Unabhängigkeit von Körperhomomorphismen . . . 77

6 Galoistheorie **79**
- 6.1 Galoiserweiterungen . . . 79
- 6.2 Charakterisierung von Galoiserweiterungen . . . 85
- 6.3 Einheitswurzeln . . . 90
- 6.4 Polynome der Form $X^n - a$ . . . 93
- 6.5 Auflösbarkeit von Gleichungen . . . 95

Einleitung

In der Linearen Algebra haben wir die Lösbarkeit linearer Gleichungssysteme der Form

$$Ax = b$$

mit $A \in \mathrm{Mat}_{m\times n}(k)$ und $x \in k^n, b \in k^m$ über einem Körper k untersucht. In diesem Semester werden wir die Lösbarkeit von Polynomgleichungen in einer Variablen x studieren. Genau wie die linearen Gleichungsystem, wurden auch Polynomgleichungen bereits in der Schule behandelt: Eine quadratische Gleichung

$$x^2+px+q = 0 \quad (p, q \in \mathbb{R}),$$

besitzt nach der p-q-Formel (oder Mitternachtsformel) genau die Lösungen

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \in \mathbb{C}.$$

Es stellt sich die Frage, ob man solche Formeln auch für Gleichungen der Form

$$(*) \quad x^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0 = 0$$

mit Koeffizienten in beliebigen Körpern angeben kann. Für $n=3,4$ gibt es derartige Formel, die im 16. Jahrhundert von G. Cardano (1501-1576), N. Tartaglia (1500-1557) und L. Ferrari (1522-1565) hergeleitet wurden. Ist $n\geq 5$, so hat der norwegische Mathematiker Niels Henrik Abel (1802-1829) gezeigt, dass man eine allgemeine Lösungsformel für beliebige Koeffizienten $a_0, \ldots, a_{n-1}$ nicht mehr finden kann.
Man beachte, dass dies nicht heißt, dass für jede Polynomgleichung von Grad ≥ 5 keine allgemeine Lösungsformel existiert: Etwa besitzt die Gleichung

$$x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x^1 + a_0 = 0$$

mit $a_1 = a_2 = a_3 = a_4 = 0$ über $\mathbb{C}$ die Lösungsmenge Formel $x_k = e^{\frac{2\pi ik}{5}} \sqrt[5]{-a_0}$ für $k \in \{0, \ldots, 4\}$. Évariste Galois (1811-1832) fand eine zufriedenstellende Begründung für die Entdeckung Abels und konnte sogar beweisen, wann eine Polynomgleichung der Form $(*)$ mit Koeffizienten in $\mathbb{Q}$ eine „Lösungsformel“ besitzt:

Theorem. *Die Gleichung $(*)$ besitzt eine Lösungsformel genau dann, wenn die zugehörige Gruppe $G(a_0, \ldots, a_{n-1})$ eine sogenannte **auflösbare** Gruppe ist.*

Ein Hauptziel dieser Vorlesung ist es, die notwendige Theorie zu vermitteln um den Hauptsatz von Galois präzise formulieren und beweisen zu können. Wir gehen dabei wie folgt vor:

(1) Wir beginnen mit dem Studium von Gruppen.

(2) Die Lösungen der Gleichungen sind Nullstellen von Polynomen. Deren Studium erfordert Kenntnisse der Ringtheorie.

(3) Man kann immer Lösungen konstruieren. Diese liegen in gewissen Körpern (in obigem Beispiel $\mathbb{C}$), deren Automorphismen unsere oben erwähnten Gruppen definieren. Aus diesem Grunde werden wir uns auch mit sogenannten Körpererweiterungen befassen.

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 sowohl 2019/20 als auch 2020/21 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 Untergruppen und der Satz von Lagrange

Definition. Sei $G \neq \varnothing$ eine Menge sowie $\mu : \begin{cases} G \times G & \longrightarrow & G \\ (a,b) & \mapsto & ab \end{cases}$ eine Abbildung[1]. Das Paar (G, μ) heißt **Gruppe**, falls gilt

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

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

(i) $ex = x$ für alle $x \in G$,

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

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

Lemma 1.1.1. *Sei G eine Gruppe. Dann gilt:*

(1) Sind $e, f \in G$ mit $ex = x = fe$ für alle $x \in G$, so gilt $e = f$ und $ex = x = xe$ für alle $x \in G$.

(2) Ist $x \in G$ und $x', x'' \in G$ mit $x'x = e = x''x$, so gilt $x' = x''$ und $x'x = e = xx'$.

*Man nennt e das **neutrale Element** und $x^{-1} := x'$ das zu x **inverse Element** in G.*

Beweis. (1) Sei $x \in G$, dann existiert ein $x' \in G$ mit $x'x = e$. Weiter existiert $y \in G$ mit $yx' = e$. Wir erhalten $ye = y(x'x)e = (yx')(xe) = (ex)e = xe$ und damit $xe = ye = y(x'x) = (yx')x = ex$. Sei $f \in G$ mit $fx = x$ für alle $x \in G$, so folgt $e = fe = f$.
(2) Sei $x \in G$ und $x' \in G$ mit $x'x = e$. Es existiert $y \in G$ mit $yx' = e$ und mit (1) folgt

$$y = ye = y(x'x) = (yx')x = ex = x,$$

also $xx' = yx' = e$. Seien nun $x'' \in G$ mit $e = x''x$, so folgt $x'' = x''e = x''(xx') = (x''x)x' = ex' = x'$. □

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

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

[1] Wir unterdrücken μ und schreiben ab oder $a \cdot b$ anstatt $\mu(a, b)$.

Definition. Eine Teilmenge $H \subseteq G$ einer Gruppe G heißt **Untergruppe** von G genau dann, wenn $(H, \mu_{H\times H})$ eine Gruppe ist.

Bemerkung. Ist $(H, \mu_{H\times H})$ eine Gruppe, so gilt nach Definition $h_1h_2 = \mu(h_1, h_2) \in H$. Das heißt H ist abgeschlossen unter der Verknüpfung.

Lemma 1.1.2 (Das 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. 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) Sei $n \in \mathbb{N} := \{1, 2, 3, \ldots\}$, sowie

$$\mathcal{S}_n := \{\sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\} \mid \sigma \text{ ist bijektiv.}\}$$

Dann ist $\mathcal{S}_n$ zusammen mit der Komposition von Abbildungen eine Gruppe und

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

ist für jedes $i \in \{1, \ldots, n\}$ eine Untergruppe.

(2) Sei $n \in \mathbb{N}$. Die Menge der n-ten Einheitswurzeln $\mu_n(\mathbb{C}) := \{\exp(2\pi i \frac{m}{n}) \mid 0 \leq m \leq n-1\}$ ist eine Untergruppe von $(\mathbb{C} \setminus \{0\}, \cdot)$

Lemma 1.1.3. *Sei G eine Gruppe, $\mathfrak{A}$ eine Menge von Untergruppen von G sowie $S \subseteq G$ eine Teilmenge. Dann gilt:*

(1) $\bigcap_{H\in\mathfrak{A}} H$ *is eine Untergruppe von G.*

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

$$\langle S\rangle := \bigcap_{H\in\mathfrak{A}_S} H$$

die kleinste Untergruppe von G, die S enthält.

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

Beweis.

(1) Dies folgt durch Nachprüfen des Untergruppenkriteriums.

(2) Sei $U \subseteq G$ eine Untergruppe von U die S enthält, so folgt $U \in \mathfrak{A}_S$ 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 $V \in \mathfrak{A}_S$. Sei nun $U \in \mathfrak{A}_S$. 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 $\langle S \rangle \subseteq V \subseteq \bigcap_{U \in \mathfrak{A}_S} U = \langle S \rangle$.

□

Ist S eine endliche Menge, so bezeichnen wir mit $|S|$ die Anzahl der Elemente von S. Ist G eine endliche Gruppe, d.h. 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. Analog definiert man die **Rechtsnebenklasse** von x in H als

$$Hx := \{hx \mid h \in H\}.$$

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 1.1.4 (Lagrange, 1736-1813). *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 derart, dass $[x] = xH$ für jedes $x \in G$ gerade die Äquivalenzklasse von x ist. Damit ist

$$G = \bigsqcup_{Z \in G/H} Z$$

die disjunkte Vereinigung der Äquivalenzklassen. Außerdem ist für jedes $x \in G$ die Abbildung

$$f_x : H \longrightarrow xH \;\; ; \;\; h \mapsto xh$$

bijektiv. Damit folgt $|G| = \sum_{Z \in G/H} |Z| = \sum_{Z \in G/H} |H| = [G:H]|H|$. □

Korollar 1.1.5. *Sei G eine endliche Gruppe, $K \subseteq H$ Untergruppen von G. Dann gilt*

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

Beweis. Wir wenden Satz 1.1.4 mehrfach an und erhalten

$$[G:K] = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = [G:H][H:K].$$

□

1.2 Zyklische Gruppen

Definition. Eine Gruppe G heißt **endlich erzeugt**, falls es eine endliche Menge $S \subseteq G$ mit $G = \langle S \rangle$ gibt. Die Gruppe G heißt **zyklisch**, falls es ein $x \in G$ mit $G = \langle \{x\} \rangle$ gibt. Wir schreiben dann $G = \langle x \rangle$.

Beispiele. (1) Division mit Rest zeigt, dass jede Untergruppe $H \subseteq \mathbb{Z}$ zyklisch ist.

(2) Aus dem Satz von Lagrange folgt: Ist G eine Gruppe mit $|G| \in \mathbb{P}$ Primzahl, so ist G zyklisch.

(3) $(\mathbb{Q}, +)$ 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 $z \in \mathbb{Z}$.

(4) Ähnlich wie in (3) zeigt man, dass $(\mathbb{Q}, +)$ nicht endlich erzeugt ist.

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 1.2.1. *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.

(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 $H = \langle m_0 \rangle = \{mm_0 \mid m \in \mathbb{Z}\}$. Gilt $m_0 = 0$, so folgt $H = \{0\}$ und die Abbildung

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

ist injektiv. Damit hat x unendliche Ordnung, im Widerspruch zur Annahme.

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 1.1.3(3). Sei $h \in \langle x \rangle$. Dann existiert nach Lemma 1.1.3(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 $s = t$. Mithin 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

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

Damit hat x^s endliche Ordnung. Es sei nun

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

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

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

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.

□

Satz 1.2.2. *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 1.1.3(2) folgt. Sei $h=x^n \in H$. Dann existieren $q, r \in \mathbb{Z}$ mit $n=qn_0+r$ und $r \in \{0,\dots,n_0-1\}$. Es folgt $x^r = h(x^{n_0})^{-q} \in H$. Nach Definition von n_0 impliziert dies $r=0$, und damit $h=(x^{n_0})^q \in \langle x^{n_0}\rangle$. Inbesondere ist H damit zyklisch.

(2) Wegen $d \mid n$ gilt $\frac{n}{d} = \mathrm{ggT}(n, \frac{n}{d})$ und Satz 1.2.1 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 $H=\{e\}=H_1$. 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 1.2.1(3)

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

Wie schreiben $n=qm+r$ mit $r \in \{0,\dots,m-1\}$. Dann gilt

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

Also ist x^r 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 $m=\frac{n}{d}$ und $H=G_d$.

(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. Seien $f, g \in \mathbb{S}_3$ die Permutationen gegeben durch $f(2)=1, f(1)=2$ und $g(1)=3$, $g(3)=1$. Es sind $\langle f\rangle \neq \langle g\rangle$ Untergruppen von $\mathbb{S}_3$ der Ordnung 2. Damit ist $\mathbb{S}_3$ nach Satz 1.2.2 nicht zyklisch.

Um zu sehen, dass Satz 1.2.2 zyklische Gruppen charakterisiert, benötigen wir einige Vorüberlegungen.

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

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

Die Funktion

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N} \; ; \; n \mapsto \varphi(n)$$

heißt **Eulersche φ-Funktion**.

Lemma 1.2.3. *Für jedes $n \in \mathbb{N}$ gilt*

$$n = \sum_{d|n} \varphi(d).$$

Beweis. Sei $H = \langle h \rangle$ eine zyklische Gruppe der Ordnung m, dann liefert Satz 1.2.1(3) für $y = h^s$ mit $s \in \{1, \ldots, m\}$

$$\mathrm{ord}(y) = m \Leftrightarrow \mathrm{ggT}(m, s) = 1.$$

Das heißt

$$(*) \; \varphi(m) = |\{y \in H \mid \mathrm{ord}(y) = m\}|.$$

In den Übungen wird gezeigt: Es gibt eine zyklische Gruppe G mit $|G| = n$. Sei $x \in G$ ein Erzeuger. Ist nun $y \in G$ ein Element mit $\mathrm{ord}(y) = d$, so gilt $\langle y \rangle = G_d$ und damit liefert $(*)$:

$$\varphi(d) = |\{y \in G_d \mid \mathrm{ord}(y) = d\}| = |\{y \in G \mid \mathrm{ord}(y) = d\}|.$$

Wegen

$$G = \bigsqcup_{d|n} \{y \in G \mid \mathrm{ord}(y) = d\}$$

erhalten wir $n = |G| = \sum_{d|n} \varphi(d)$. □

Definition. Sei G eine endliche Gruppe. Für $d \in \mathbb{N}$ sei mit

$$o_G(d) := |\{x \in G \mid \mathrm{ord}(x) = d\}|$$

die Anzahl der Elemente in G mit Ordnung d bezeichnet.

Satz 1.2.4. *Sei G eine endliche Gruppe derart, dass für jeden Teiler d von $|G|$ höchstens eine Untergruppe der Ordnung d existiert. Dann ist G zyklisch.*

Beweis. Sei $n := |G|$. Für $d|n$ mit $o_G(d) \neq 0$ gibt es nach Voraussetzung genau eine Untergruppe G_d von G mit $|G_d| = d$. Sei nun $y \in G$ mit $\mathrm{ord}(y) = d$. Dann gilt $\langle y \rangle = G_d$ und es folgt

$$o_G(d) = |\{x \in G \mid \mathrm{ord}(x) = d\}| = |\{x \in G_d \mid \mathrm{ord}(x) = d\}| = o_{G_d}(d).$$

Da G_d zyklisch ist, erhalten wir also (wie im Beweis von Lemma 1.2.3) $o_G(d) = o_{G_d}(d) = \varphi(d)$. Mit Lemma 1.2.3 folgt nun

$$n = \sum_{d|n} \varphi(d) \geq \sum_{d|n; o_G(d) \neq 0} \varphi(d) = \sum_{d|n; o_G(d) \neq 0} o_G(d) = n.$$

Wir erhalten $\sum_{d|n} \varphi(d) = \sum_{d|n; o_G(d) \neq 0} o_G(d)$ und damit $0 = \sum_{d|n; o_G(d) = 0} \varphi(d)$. Da $\varphi(n) \geq 1$, gilt, folgt $o_G(n) \neq 0$. Also gibt es ein $x \in G$ mit $\mathrm{ord}(x) = n$ und $G = \langle x \rangle$ ist zyklisch. □

1.3 Homomorphismen und Normalteiler

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

Lemma 1.3.1. *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) $\operatorname{im}\varphi := \{\varphi(x) \mid x \in G\}$ *ist eine Untergruppe von* G'.

(4) $\ker\varphi := \varphi^{-1}(e_{G'}) = \{x \in G \mid \varphi(x) = e_{G'}\}$ *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, 3.2.39, 3.2.37] 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 $\varphi(x^{-1}y) = \varphi(x)^{-1}\varphi(x) = e_{G'}$. Anderseits ist $\varphi(xz) = \varphi(x)\varphi(z) = \varphi(x)$ für alle $z \in \ker\varphi$. □

Bemerkung. Nach Lemma 1.3.1 ist ein Homomorphismus $\varphi\colon G \longrightarrow G'$ injektiv, genau dann, wenn $\ker\varphi = \{e_G\}$ gilt.

Definition. Es sei G eine Gruppe. Ein Isomorphismus $\varphi\colon G \longrightarrow G$ heißt **Automorphismus**. Wir bezeichnen mit $\mathcal{S}_G$ die Permutationsgruppe von der Menge G. Dann ist

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

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

Beispiele. (1) $\exp\colon (\mathbb{Z}, +) \longrightarrow (\mathbb{R}\setminus\{0\}, \cdot)\ ;\ z \mapsto \exp(z)$ ist ein Homomorphismus.

(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 $S^1 \subseteq \mathbb{C}$ der Einheitskreis und $z \in \mathbb{C}\setminus\{0\}$, so gilt

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

da $\exp(i\arg(z)) \in S^1$ und S^1 eine Untergruppe von $(\mathbb{C}\setminus\{0\}, \cdot)$ ist. Figur 1.1 zeigt die Fasern von 2 und $3,5$ unter φ in der Gaußschen Zahlenebene.

(3) Sei k ein Körper, $n \in \mathbb{N}$ und $\mathrm{GL}_n(k)$ die Menge der invertierbaren $n \times n$-Matrizen. Nach dem Determinantenproduktsatz ist die Determinantenabbildung

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

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

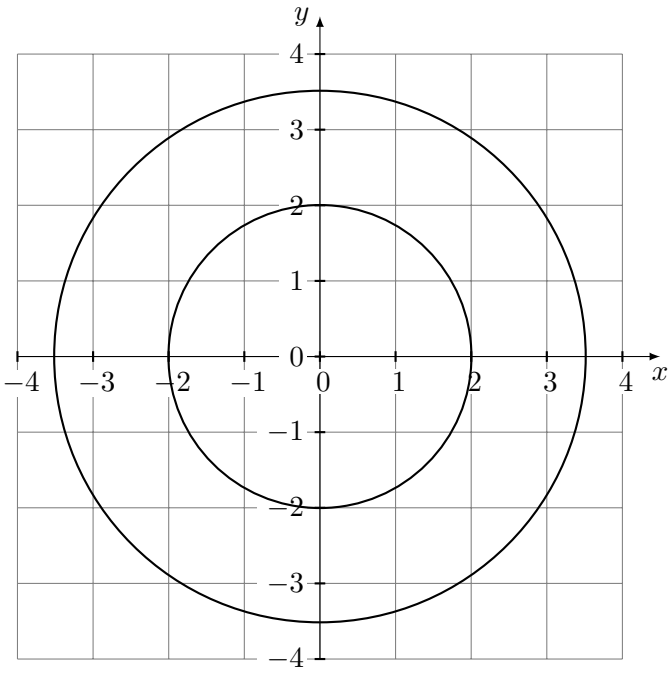


Abbildung 1.1: Fasern von 2 und 3.5 unter dem Homomorphismus φ aus Beispiel (2).

(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 der Determinante liefert $\det(A(\sigma)) = \mathrm{sgn}(\sigma)$, wobei $\mathrm{sgn}(\sigma)$ das **Signum/Vorzeichen** von σ 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 $\mathrm{sgn}\colon \mathcal{S}_n \longrightarrow (\{\pm 1\}, \cdot), \sigma \mapsto \mathrm{sgn}(\sigma)$ ein Gruppenhomomorphismus (vergleiche [5, 3.3.9]).

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

$$xNx^{-1} = N \quad \forall\, x \in G.$$

In diesem Fall schreiben wir $N \trianglelefteq G$.

Lemma 1.3.2. *Sei G eine Gruppe und $N \subseteq G$ eine Untergruppe. Folgende Bedingungen sind äquivalent:*

(1) $N \subseteq G$ ist normal in G.

(2) $xN = Nx$ für alle $x \in G$.

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

Beweis. (1) $\Longrightarrow$ (2) und (2) $\Longrightarrow$ (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

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

□

Definition. Eine Gruppe G heißt **kommutativ** oder **abelsch**, falls

$$xy = yx \quad \forall\, x, y \in G$$

gilt.

Beispiele. (1) $H := \mathrm{Stab}_{\mathcal{S}_3}(3)$ ist nicht normal in $\mathcal{S}_3$: Es sei $\tau \in H$ gegeben durch $\tau(1) = 2,\ \tau(2) = 1, \tau(3) = 3$. Für die durch $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 2$ gegebene Permutation $\sigma \in \mathcal{S}_3$ erhalten wir

$$(\sigma \circ \tau \circ \sigma^{-1})(3) = (\sigma \circ \tau)(2) = \sigma(1) = 1,$$

und somit $\sigma \circ \tau \circ \sigma^{-1} \notin H$.

(2) Ist $S \subseteq G$ eine Teilmenge mit $xSx^{-1} \subseteq \langle S \rangle$ für alle $x \in G$, so ist $\langle S \rangle$ ein Normalteiler von G.

(3) Ist G eine abelsche Gruppe, so ist jede Untergruppe von G ein Normalteiler.

(4) Ist $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus, so sind Urbilder von Normalteiler wieder Normalteiler. Insbesondere ist $\ker \varphi$ ein Normalteiler von G. Bilder von Normalteilern sind in der Regel keine Normalteiler, wie schon das einfache Beispiel $\mathrm{Stab}_{\mathcal{S}_3}(3) \subseteq \mathcal{S}_3$ zeigt.

(5) 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**.

(6) Sei G eine Gruppe. Für $x \in G$ heißt der Automorphismus

$$\iota_x : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ y & \mapsto & xyx^{-1} \end{array} \right.$$

die **Konjugation** mit x. $\mathrm{Inn}(G) := \{\iota_x \mid x \in G\}$ ist ein Normalteiler von $\mathrm{Aut}(G)$. Sind nämlich $\varphi \in \mathrm{Aut}(G)$ und $x \in G$, so gilt

$$\varphi \circ \iota_x \circ \varphi^{-1} = \iota_{\varphi(x)} \in \mathrm{Inn}(G).$$

1.4 Die symmetrische Gruppe $\mathcal{S}_n$

Unser erster Satz besagt, dass jede Gruppe G als Untergruppe der Permutationsgruppe $\mathcal{S}_G$ aufgefasst werden kann.

Proposition 1.4.1. *Sei G eine Gruppe. Dann ist $\varphi : G \longrightarrow \mathcal{S}_G$, mit*

$$\varphi(x)(y) := xy \quad \forall\, x, y \in G$$

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. □

Sei A eine Menge, $\sigma \in \mathcal{S}_A$ eine Permutation. Dann heißt

$$\mathrm{supp}(\sigma) := \{a \in A \mid \sigma(a) \neq a\}$$

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

$$(a_1, \ldots, a_m)(a) := \begin{cases} a & a \notin \{a_1, \ldots, a_m\} \\ a_{i+1} & a = a_i \,;\, 1 \leq i \leq m-1 \\ a_1 & a = a_m \end{cases}$$

definierten m-Zykel von A.

Bemerkung. Sind $\sigma, \tau \in \mathcal{S}_A$ Permutationen mit $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \varnothing$, so gilt $\sigma \circ \tau = \tau \circ \sigma$.

Folgende Resultate wurden bereits in der Linearen Algebra behandelt (siehe [5, 3.3.4]).

Satz 1.4.2. *Sei $n \in \mathbb{N}$.*

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

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_t \;\; \textit{und} \;\; \mathrm{supp}(\sigma) = \bigsqcup_{i=1}^{t} \mathrm{supp}(\sigma_i).$$

Diese Darstellung ist bis auf Reihenfolge eindeutig.

(2) Sind $a_1, \ldots, a_\ell \in \{1, \ldots, n\}$ paarweise verschieden, so gilt

$$\sigma \circ (a_1, \ldots, a_\ell) \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_\ell)) \quad \forall\, \sigma \in \mathcal{S}_n.$$

(3) Die Gruppe $\mathcal{S}_n$ wird sowohl von der Menge $\{(1,2),(1,3),\ldots,(1,n)\}$ als auch von $\{(1,2),(2,3),\ldots,(n-1,n)\}$ erzeugt.

Beweis.[2]

(1) Sei $\sigma \neq \mathrm{id} \in \mathcal{S}_n$. Wir definieren auf der Menge $[1,n] := \{1,\ldots,n\}$ eine Äquivalenzrelation vermöge

$$a \sim_\sigma b :\Leftrightarrow \exists\, i \in \mathbb{Z} \text{ mit } b = \sigma^i(a).$$

Da σ endliche Ordnung hat, gibt es zu $a \in [1,n]$ ein minimales $m_a \in \mathbb{N}$ derart, dass $\sigma^{m_a}(a) = a$. Damit ist die Äquivalenzklasse $[a]_\sigma$ von a durch

$$[a]_\sigma = \{\sigma^i(a) \mid 0 \leq i \leq m_a - 1\}\}$$

gegeben. Wir zerlegen $[1,n]$ in seine Äquivalenzklassen: Es gibt $a_1,\ldots,a_\ell \in [1,n]$ mit $[1,n] = \bigsqcup_{i=1}^{\ell} [a_i]_\sigma$. Für $j \in [1,\ell]$ mit $m_{a_j} > 1$ ist

$$\sigma_j := (a_j, \sigma(a_j), \sigma^2(a_j), \ldots, \sigma^{m_{a_j}-1}(a_j))$$

nach Wahl von m_{a_j} ein m_{a_j}-Zykel mit $\mathrm{supp}(\sigma_j) = [a_j]_\sigma$. Es sei $J := \{j \in [1,\ell] \mid m_{a_j} > 1\}$. Wegen $\sigma \neq \mathrm{id}$ gilt $J \neq \varnothing$. Wir betrachten $\tau := \prod_{j\in J} \sigma_j$. Aufgrund obiger Bemerkung spielt die Reihenfolge der Faktoren keine Rolle. Dann gilt $\mathrm{supp}(\tau) = \bigsqcup_{j\in J} \mathrm{supp}(\sigma_j) = \mathrm{supp}(\sigma)$.

Ist $a \in \mathrm{supp}(\sigma)$, so gibt es also genau ein $j_0 \in J$ mit $a \in \mathrm{supp}(\sigma_{j_0}) = [a_{j_0}]_\sigma$. Damit folgt $\sigma_j(a) = a$ für $j \in J \setminus \{j_0\}$ und wir erhalten

$$\tau(a) = [\sigma_{j_0} \circ \prod_{j \in J\setminus\{j_0\}} \sigma_j](a) = \sigma_{j_0}(a) = \sigma(a).$$

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

Ist nun $\sigma = \tau_1 \circ \cdots \circ \tau_m$ eine weitere derartige Zerlegung, so ist $\{\mathrm{supp}(\tau_i) \mid i \in [1,m]\}$ die Menge der Äquivalenzklassen von $\sim_\sigma$ mit mindestens 2 Elementen. Insbesondere gilt $m = l$ und es existiert eine Bijektion $f\colon \{1,\ldots,l\} \longrightarrow \{1,\ldots,l\}$ mit $\mathrm{supp}(\sigma_i) = \mathrm{supp}(\tau_{f(i)})$ für alle $i \in \{1,\ldots,l\}$. Sei $i \in \{1,\ldots,l\}$, dann gilt

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

und damit

$$\sigma_i(a) = \sigma_i(\sigma_1 \cdots \sigma_{i-1}\sigma_{i+1} \cdots \sigma_l)(a) = \tau_{f(i)}(\tau_1 \cdots \tau_{f(i)-1}\tau_{f(i)+1} \cdots \tau_l)(a) = \tau_{f(i)}(a)$$

für alle $a \in \mathrm{supp}(\sigma_i) = \mathrm{supp}(\tau_{f(i)})$. 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 $x \in \mathrm{supp}(\sigma \circ (a_1,\ldots,a_\ell) \circ \sigma^{-1})$. Dann gilt $[\sigma \circ (a_1,\ldots,a_\ell) \circ \sigma^{-1}](x) \neq x$ und somit

$$(a_1,\ldots,a_\ell) \circ \sigma^{-1}(x) \neq \sigma^{-1}(x).$$

[2] Der Beweis verwendet implizit Gruppenoperationen, die wir erst später behandeln werden. Es lohnt sich also diesen Beweis erneut zu lesen, wenn wir Gruppenoperationen studiert haben.

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

$$\sigma \circ (a_1, \ldots, a_\ell) \circ \sigma^{-1}(\sigma(a_j)) = \begin{cases} \sigma(a_{j+1}) & j < \ell \\ \sigma(a_1) & j = \ell. \end{cases}$$

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

(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 $1 < i < j \in [1, n]$. Aus (2) folgt

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

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

Für $\ell \geq 3$ gilt

$$(1, \ell) = (\ell-1, \ell) \circ (1, \ell-1) \circ (\ell-1, \ell).$$

Dies liefert per Induktion nach ℓ

$$(1, \ell) \in \langle \{(1, 2), (2, 3), \ldots, (\ell-1, \ell)\} \rangle$$

und damit $\mathcal{S}_n = \langle \{(1, 2), (2, 3), \ldots, (\ell-1, \ell)\} \rangle$.

□

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

(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) Es gilt für $i \geq 3$ die Gleichung $(1, i) = (i - 1, i)(1, i - 1)(i - 1, i)$.

(4) Nach Satz 1.4.2(2) sind je zwei Zyklen gleicher Länge zueinander konjugiert.

1.5 Faktorgruppen und Isomorphiesätze

Sei G eine Gruppe, $N \subseteq G$ eine normale Untergruppe. Dann erhält die Menge

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

vermöge

$$(xN).(yN) := xyN$$

die Struktur einer Gruppe. Diese Gruppe heißt **Faktorgruppe von G nach N**. Die Abbildung

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

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

Bemerkungen. (1) Obige Zuordnung ist wohldefiniert, da N ein Normalteiler von G ist: Sind g_1, g_2, h_1, h_2 mit $g_1N = g_2N$ und $h_1N = h_2N$, so gilt $g_1^{-1}g_2, h_1^{-1}h_2 \in N$ und damit

$$(g_1h_1)^{-1}(g_2h_2)N = h_1^{-1}g_1^{-1}g_2h_2N = (h_1^{-1}h_2)(h_2^{-1}(g_1^{-1}g_2)h_2)N = N,$$

da N ein Normalteiler ist. Das heißt $g_1h_1N = g_2h_2N$.

(2) Das Einselement ist durch $e_{G/N} = N$ gegeben, zudem gilt $(xN)^{-1} = x^{-1}N$ für jedes $x \in G$.

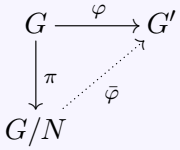
(3) $U := \mathrm{Stab}_{\mathcal{S}_3}(3)$ ist kein Normalteiler von $\mathcal{S}_3$ und die Zuordnung

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

nicht wohldefiniert: Es gilt $(1,3)U = (1,2,3)U$ aber

$$(1,3)(1,3)U = U \neq (1,2,3)U = (1,3,2)(1,3,2)U.$$

Satz 1.5.1. *Sei $\varphi : G \longrightarrow G'$ ein Homomorphismus von Gruppen, $N \subseteq G$ 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. Da π surjektiv ist, ist die Abbildung $\bar{\varphi}$ eindeutig bestimmt. Dementsprechend setzen wir

$$\bar{\varphi}(xN) := \varphi(x) \quad \forall\, x \in G.$$

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

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

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

Korollar 1.5.2. *Sei $\varphi : G \longrightarrow G'$ ein Homomorphismus. Dann ist*

$$\bar{\varphi} : \begin{cases} G/\ker\varphi & \longrightarrow & G' \\ x\ker\varphi & \mapsto & \varphi(x) \end{cases}$$

ein injektiver Homomorphismus mit $\mathrm{im}\,\bar{\varphi} = \mathrm{im}\,\varphi$.

Beweis. Nach Satz 1.5.1 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 $e_{G'} = \varphi(x)$ und damit $x \in \ker\varphi$. Das heißt $x\ker\varphi = \ker\varphi = e_{G/\ker\varphi}$ □

Beispiel. (1) Übungsaufgabe: Mithilfe von Korollar 1.5.2 lässt sich zeigen, dass für jede zyklische Gruppe G geanu ein $n \in \mathbb{N}_0$ mit $G \cong \mathbb{Z}/\langle n\rangle$ existiert.

(2) Ist $\varphi\colon G \longrightarrow G'$ ein surjektiver Homomorphismus zwischen endlichen Gruppen, so ist nach dem Satz von Lagrange und Korollar 1.5.2 die Ordnung von G' ein Teiler der Ordnung von G.

(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 $x \in \mathbb{Z}/\langle 7\rangle$.

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

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

Satz 1.5.3 (Erster Isomorphiesatz). *Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe, $N \subseteq G$ ein Normalteiler. Dann gilt:*

(1) NH ist eine Untergruppe von G.

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

(3) Die Abbildung

$$\varphi : \begin{cases} H/N\cap H & \longrightarrow & NH/N \\ x(N\cap H) & \mapsto & xN \end{cases}$$

ist ein Isomorphismus.

Beweis.

(1) Es ist $e \in NH$. Sind $n, n' \in N$ und $h, h' \in H$, so erhalten wir

$$(nh)(n'h') = (nhn'h^{-1})hh' \in NH,$$

sowie

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

(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

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

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 1.5.2 das Gewünschte. Weiter ist damit $N \cap H = \ker\sigma$ ein Normalteiler von H.

□

Satz 1.5.4 (Zweiter Isomorphiesatz). *Es seien $N \subseteq M$ Normalteiler der Gruppe G. Dann gilt:*

(1) M/N ist eine normale Untergruppe der Gruppe G/N.

(2) Es gibt einen Isomorphismus $(G/N)/(M/N) \xrightarrow{\sim} G/M$.

Beweis. Es seien $\pi_M : G \longrightarrow G/M$ und $\pi_N : G \longrightarrow G/N$ die kanonischen Projektionen. Wegen $N \subseteq M = \ker \pi_M$ liefert Theorem 1.5.1 genau einen Homomorphismus $\bar{\pi}_M : G/N \longrightarrow G/M$ derart, dass $\bar{\pi}_M \circ \pi_N = \pi_M$. Es gilt also

$$\bar{\pi}_M(xN) = xM \quad \forall\, x \in G.$$

Damit ist $\bar{\pi}_M$ surjektiv und $\ker \bar{\pi}_M = M/N$. Nach Korollar 1.5.2 ist die induzierte Abbildung $(G/N)/(M/N) \longrightarrow G/M$ ein Isomorphismus. □

1.6 Produkte von Gruppen

Es sei Λ eine Menge, $(G_\lambda)_{\lambda\in\Lambda}$ eine Familie von Gruppen. Dann erhält die Menge

$$\prod_{\lambda\in\Lambda} G_\lambda := \{(x_\lambda)_{\lambda\in\Lambda} \mid x_\lambda \in G_\lambda \ \forall\, \lambda \in \Lambda\}$$

die Struktur einer Gruppe vermöge

$$(x_\lambda)_{\lambda\in\Lambda}(y_\lambda)_{\lambda\in\Lambda} = (x_\lambda y_\lambda)_{\lambda\in\Lambda}.$$

Diese Gruppe nennt man das **(äußere) Produkt** der Familie $(G_\lambda)_{\lambda\in\Lambda}$.
Sei $\lambda_0 \in \Lambda$. Dann gilt:

- Die Abbildung
$$\iota_{\lambda_0} : G_{\lambda_0} \longrightarrow \prod_{\lambda\in\Lambda} G_\lambda \ ; \ \iota_{\lambda_0}(x)_\lambda = \begin{cases} e_{G_\lambda} & \lambda \neq \lambda_0 \\ x & \lambda = \lambda_0 \end{cases}$$
ist ein injektiver Homomorphismus.
- $\iota_{\lambda_0}(G_{\lambda_0})$ ist ein Normalteiler von $\prod_{\lambda\in\Lambda} G_\lambda$.
- $\langle \bigcup_{\lambda\in\Lambda} \iota_\lambda(G_\lambda)\rangle = \{(x_\lambda)_{\lambda\in\Lambda} \mid x_\lambda = e_{G_\lambda}$ für alle bis auf endlich viele $\lambda \in \Lambda\}$.
- $\iota_{\lambda_0}(G_{\lambda_0}) \cap \langle \bigcup_{\mu\neq\lambda_0} \iota_\mu(G_\mu)\rangle = \{e\}$.

Lemma 1.6.1. *Sei Λ eine endliche Menge, $(G_\lambda)_{\lambda\in\Lambda}$ eine Familie von normalen Untergruppen einer Gruppe G derart, dass*

(i) $G = \langle \bigcup_{\lambda\in\Lambda} G_\lambda\rangle$, und

(ii) $G_\lambda \cap \langle \bigcup_{\mu\neq\lambda} G_\mu\rangle = \{e\} \quad \forall\, \lambda \in \Lambda$.

Dann gibt es einen Isomorphismus $\prod_{\lambda\in\Lambda} G_\lambda \xrightarrow{\sim} G$.

Beweis. Aufgrund von (ii) gilt $G_\lambda \cap G_\mu = \{e\}$ für alle $\lambda \neq \mu$. Für $x \in G_\lambda$ und $y \in G_\mu$ folgt wegen der Normalität von G_λ und G_μ also

$$xyx^{-1}y^{-1} \in G_\lambda \cap G_\mu = \{e\}.$$

Dies bedeutet $xy = yx \ \forall\, x \in G_\lambda, y \in G_\mu, \lambda \neq \mu$. Wir betrachten nun die Abbildung

$$\varphi : \begin{cases} \prod_{\lambda\in\Lambda} G_\lambda & \longrightarrow & G \\ (x_\lambda)_{\lambda\in\Lambda} & \mapsto & \prod_{\lambda\in\Lambda} x_\lambda \end{cases}$$

Da Λ endlich ist, ist φ wohldefiniert. Zudem gilt

$$\begin{aligned} \varphi((x_\lambda)(y_\lambda)) &= \varphi((x_\lambda y_\lambda)) = \prod_{\lambda\in\Lambda} x_\lambda y_\lambda = (\prod_{\lambda\in\Lambda} x_\lambda)(\prod_{\lambda\in\Lambda} y_\lambda) \\ &= \varphi((x_\lambda))\varphi((y_\lambda)). \end{aligned}$$

Damit ist φ ein Gruppenhomomorphismus. Für $\lambda \in \Lambda$ erhalten wir

$$[\varphi \circ \iota_\lambda](x) = x \quad \forall\, x \in G_\lambda,$$

und daher $G_\lambda \subseteq \operatorname{im}\varphi$. Dies impliziert $\bigcup_{\lambda\in\Lambda} G_\lambda \subseteq \operatorname{im}\varphi$ und (i) liefert $G = \operatorname{im}\varphi$.

Sei nun $(x_\lambda)_{\lambda\in\Lambda} \in \ker\varphi$. Dann gilt $\prod_{\lambda\in\Lambda} x_\lambda = e$. Für $\lambda_0 \in \Lambda$ erhalten wir

$$x_{\lambda_0} = \prod_{\lambda\neq\lambda_0} x_\lambda^{-1} \in G_{\lambda_0} \cap \langle \bigcup_{\lambda\neq\lambda_0} G_\lambda \rangle \overset{(ii)}{=} \{e\}$$

und somit $(x_\lambda)_{\lambda\in\Lambda} = e_{\prod_{\lambda\in\Lambda} G_\lambda}$. Mithin ist φ injektiv und daher ein Isomorphismus. □

Lemma 1.6.2. *Seien N, H Gruppen sowie $\gamma : H \longrightarrow \operatorname{Aut}(N)$ ein Homomorphismus von Gruppen. Dann erhält $N \times H$ vermöge*

$$(n,h)(n',h') := (n\gamma(h)(n'), hh') \quad \forall\, n,n' \in N, h,h' \in H$$

die Struktur einer Gruppe.

Bemerkung. Man schreibt $N \rtimes_\gamma H$ und nennt diese Gruppe das **semidirekte Produkt** von N und H bezüglich γ. Wir werden in der Notation γ oft unterdrücken.

Beweis. Es gilt $e = (e_N, e_H)$:

$$(e_N, e_H)(n,h) = (e_N\gamma(e_H)(n), e_H h) = (\mathrm{id}_N(n), h) = (n,h).$$

Ist $(n,h) \in N \rtimes_\gamma H$ so erhalten wir

$$\begin{aligned} (\gamma(h^{-1})(n^{-1}), h^{-1})(n,h) &= (\gamma(h^{-1})(n^{-1})\gamma(h^{-1})(n), h^{-1}h) = (\gamma(h^{-1})(n^{-1}n), e_H) \\ &= (\gamma(h^{-1})(e_N), e_H) = (e_N, e_H). \end{aligned}$$

Das Assoziativgesetz folgt durch direktes Nachrechnen. □

Bemerkung. Man kann zudem zeigen:

(i) $\pi_H : N \rtimes_\gamma H \longrightarrow H \; ; \; \pi_H(n,h) = h$ ist ein surjektiver Homomorphismus.

(ii) $\iota_N : N \longrightarrow N \rtimes_\gamma H \; ; \; \iota_N(n) = (n, e_H)$ ist ein injektiver Homomorphismus derart, dass $\operatorname{im} \iota_N = \ker \pi_H$ gilt.

(iii) $\iota_H : H \longrightarrow N \rtimes_\gamma H \; ; \; \iota_H(h) = (e_N, h)$ ist ein Homomorphismus mit $\pi_H \circ \iota_H = \mathrm{id}_H$. (Insbesondere ist ι_H injektiv.)

Beispiele. (1) Es sei V ein euklidischer $\mathbb{R}$-Vektorraum sowie

$$\mathrm{Iso}(V) := \{\varphi \in \mathcal{S}_V \mid ||\varphi(x) - \varphi(y)|| = ||x - y|| \; \forall \, x, y \in V\}$$

die Gruppe der Isometrien. Dann ist $\mathcal{O}(V) := \{\varphi \in \mathrm{Iso}(V) \mid \varphi \text{ linear}\}$ eine Untergruppe von $\mathrm{Iso}(V)$ und

$$\gamma : \mathcal{O}(V) \longrightarrow \mathrm{Aut}((V,+)) \; ; \; \varphi \mapsto \varphi$$

in die Automorphismengruppe der dem Vektorraum V zugrundeliegenden abelschen Gruppe $(V,+)$ ist ein Gruppenhomomorphismus. In der Linearen Algebra zeigt man $\mathrm{Iso}(V) \cong V \rtimes \mathcal{O}(V)$, indem man die Elemente von V als Translationen interpretiert (vergleiche [5, 9.7.9]).

(2) Es sei N eine abelsche Gruppe, $H := (\pm 1, \cdot)$ die zyklische Gruppe der Ordnung 2. Dann ist

$$\gamma : H \longrightarrow \mathrm{Aut}(N) \; ; \; \gamma(1) = \mathrm{id}_N, \gamma(-1)(n) = n^{-1} \forall n \in N$$

ein Homomorphismus und $D_N := N \rtimes_\gamma H$ heißt **Diedergruppe** zu N. Es gilt also

$$(n_1, h_1)(n_2, h_2) = (n_1 h_1 n_2 h_1^{-1}, h_1 h_2).$$

Für $N = \mathbb{Z}/\langle n \rangle$ schreibt man $D_n := D_{\mathbb{Z}/\langle n \rangle}$.

Lemma 1.6.3. *Sei G eine Gruppe, $N \subseteq G$ ein Normalteiler sowie $H \subseteq G$ eine Untergruppe. mit*

(i) $NH = G$, und

(ii) $N \cap H = \{e\}$.

Dann existiert ein Homomorphismus $\iota \colon H \longrightarrow \mathrm{Aut}(N)$, sodass $\varphi : N \rtimes_\iota H \longrightarrow G \; ; \; (n,h) \mapsto nh$ ein Isomorphismus ist. Wir schreiben in diesem Fall $N \rtimes H = G$.

Beweis. Sei $h \in H$. Da N normal in G ist, ist die Abbildung

$$\iota_h : N \longrightarrow N \; ; \; n \mapsto hnh^{-1}$$

ein Automorphismus von N. Damit ist

$$\iota : H \longrightarrow \mathrm{Aut}(N) \; ; \; h \mapsto \iota_h$$

ein Homomorphismus. Es bezeichne $N \rtimes_\iota H$ das zugehörige semidirekte Produkt. Es gilt nun

$$\varphi((n_1,h_1)(n_2,h_2)) = \varphi((n_1 h_1 n_2 h_1^{-1}, h_1 h_2)) = n_1 h_1 n_2 h_2 = \varphi(n_1,h_1)\varphi(n_2,h_2).$$

Damit ist φ ein Gruppenhomomorphismus. Wegen (i) ist φ surjektiv; Eigenschaft (ii) impliziert die Injektivität von φ. $\square$.

Beispiel. Sei $n \geq 3$. Wir betrachten erneut surjektiven Homomorphismus $\operatorname{sgn}\colon \mathcal{S}_n \longrightarrow (\{\pm 1\}, \cdot)$. Der Satz von Lagrange zusammen mit Korollar 1.5.2 liefert $|\mathcal{A}_n| = |\ker \operatorname{sgn}| = \frac{|\mathcal{S}_n|}{|\{\pm 1\}|} = \frac{n!}{2}$. Für jede Transposition $\tau \in \mathcal{S}_n$ folgt mit Lemma 1.5.3 und Lemma 1.6.3 die Gleichheit $\mathcal{A}_n \rtimes \langle \tau \rangle = \mathcal{S}_n$.

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) $g.(h.x) = (gh).x \quad \forall\, g, h \in G, x \in X$,

(2) $e.x = x \;\; \forall\, x \in X$.

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 [3], das heißt

$$\sigma.i := \sigma(i) \quad \forall \sigma \in \mathcal{S}_n \quad \forall i \in X.$$

(2) Sei G eine Gruppe. Dann wird durch

$$g.x := gx \quad \forall\, g, x \in G$$

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

(3) Sei G eine Gruppe. Dann wird durch

$$g.x := gxg^{-1} \;\; \forall\, g, x \in G$$

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

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

eine Gruppenoperation.

[3] Diese Operation kam bereits im Beweis von 1.4.2 zur Anwendung.

Beweis.

(1) Für jedes $g \in G$ ist

$$\varphi(g) : \left\{ \begin{array}{ccc} X & \longrightarrow & X \\ x & \mapsto & g.x \end{array} \right.$$

eine Abbildung. Es gilt $\varphi(e) = \mathrm{id}_X$, sowie

$$(*) \quad \varphi(gh)(x) = (gh).x = g.(h.x) = [\varphi(g) \circ \varphi(h)](x) \quad \forall\, g, h \in G, x \in X.$$

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

(2) Analog.

□

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

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

die **Bahn** von x. Ferner ist

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

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

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

für die Menge der Bahnen. Weiter bezeichnen wir für $g \in G$ mit X^g die Menge

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

Die Operation heißt **transitiv**, falls ein $x \in X$ mit $G.x = X$ existiert. Weiter heißt die Operation **treu**, falls $g.x = x$ für alle $x \in X$ bereits $g = e$ impliziert.

Lemma 1.7.2 (Bahnformel und Burnsides Lemma)**.** *Sei X eine G-Menge und $x \in X$.*

(1) Die Abbildung

$$\varphi : \left\{ \begin{array}{ccc} G/G_x & \longrightarrow & G.x \\ gG_x & \mapsto & g.x \end{array} \right.$$

bijektiv.

(2) Ist G endlich, so ist $|G.x|$ ein Teiler der Gruppenordnung.

(3) Sind X und G endlich, so gilt

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Beweis.

(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 $\varphi(g) = \varphi(h)$ 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.

(3) Wir definieren auf X eine Äquivalenzrelation durch

$$x \sim y :\Leftrightarrow \exists\, g \in G \text{ mit } y = g.x.$$

Dann ist für $x \in X$, die Menge $G.x$ gerade die Äquivalenzklasse $[x]$ von x und wir erhalten

$$(*) \quad X = \bigsqcup_{G.x \in X/G} G.x.$$

Es gilt

$$\begin{aligned}\sum_{g\in G} |X^g| &= \sum_{g\in G} |\{y \in X \mid g.y = y\}| = |\{(g, y) \mid g \in G, y \in X, g.y = y\}| \\ &= \sum_{y\in X} |\{g \in G \mid g.y = y\}| = \sum_{y\in X} |G_y| \overset{(1)}{=} \sum_{y\in X} \frac{|G|}{|G.y|} \\ &\overset{(*)}{=} |G| \sum_{A\in X/G} \sum_{a\in A} \frac{1}{|G.a|} = |G| \sum_{A\in X/G} \sum_{a\in A} \frac{1}{|A|} = |G||X/G|.\end{aligned}$$

□

Definition. Sei X eine G-Menge. Dann heißt

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

die Menge der **Fixpunkte** von X.

Satz 1.7.3. *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

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

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 1.7.2 impliziert

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

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

$$Z(G) := G^G = \{x \in G \mid gx = xg \ \forall\, g \in G\}$$

das **Zentrum** von G.

Eine unmittelbare Folgerung aus Satz 1.7.3 ist die sogenannte Klassengleichung:

Korollar 1.7.4 (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.

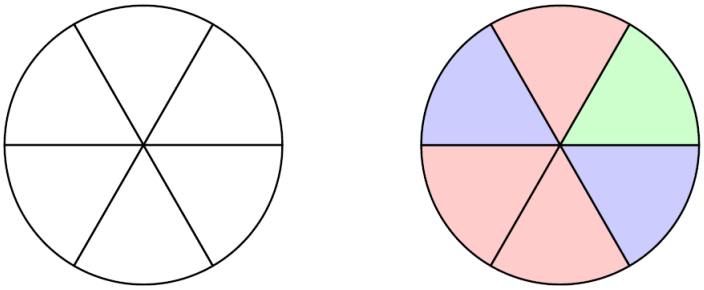


Abbildung 1.2: Farbloses Glücksrad R mit $m = 6$ Zellen und eine mögliche Färbung.

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).

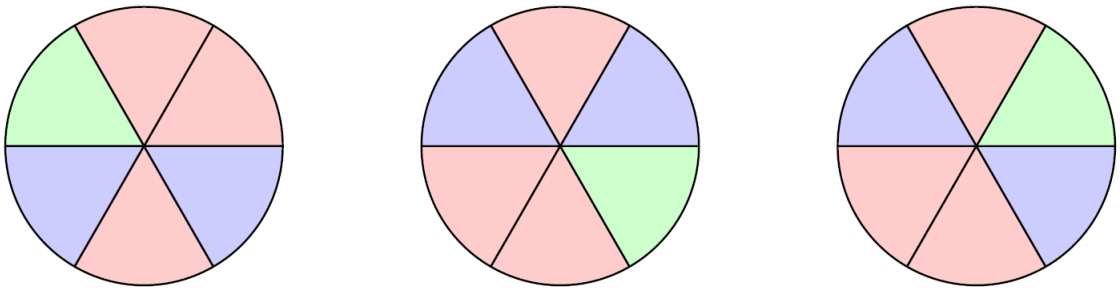


Abbildung 1.3: Drei verschiedene Einfärbungen von R. Nur die ersten beiden Einfärbungen beschreiben dasselbe bunte Glücksrad.

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 Speziallfall $m = p \in \mathbb{P}$ Primzahl auf zwei verschiedene Weisen bestimmen.
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 $1 \neq |G.x| = [G : G_x]$ ein Teiler der Gruppenordnung $|G| = p$ und somit $[G : G_x] = p$. Wir schließen mit Lemma 1.7.2

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

und somit

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

Nun berechnen wir $|X/G|$ mithilfe von Burnesides Lemma. Sei dazu $x \in X^g$ für ein $g \in G \setminus \{e\}$. Dann ist nach dem Satz von Lagrange g ein Erzeuger von G, das heißt es existiert $l \in \mathbb{N}$ mit $g^l = \sigma$. Es folgt $\sigma.x = g^l.x = x$ und somit folgt wie oben, dass jede Zelle von x dieselbe Farbe besitzt. Also gilt $|X^g| = n$ und das Lemma von Burnside liefert

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{p}(|X^e| + (p-1)n) = \frac{1}{p}(n^p + (p-1)n) = \frac{n^p + np - n}{p}.$$

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 $|G| = p^n$ gibt.

Lemma 2.1.1. *Sei $G \neq \{e\}$ eine endliche p-Gruppe. Ist X eine endliche G-Menge, so gilt*

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

Beweis. Nach 1.7.3 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. □

Korollar 2.1.2. *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 schreiben $|G| = p^n$ mit $n \in \mathbb{N}$. Die Gruppe G operiert auf $X := G \setminus \{e\}$ durch Konjugation, da $gxg^{-1} = e \Leftrightarrow x = e$ gilt. Wir erhalten mit Lemma 2.1.1 die Gleichung

$$-1 \equiv |X^G| \mod(p).$$

Das heißt $\varnothing \neq X^G = Z(G) \setminus \{e\}$.

(2) Nach (1) ist $|Z(G)| \in \{p, p^2\}$. In den Übungsserien wird 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. $Z(G) = G$.

□

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 nur natürlich folgende Fragestellungen zu untersuchen:

- Existiert für einen Teiler l von $|G|$ stets eine Untergruppe der Ordnung l?
- Wie viele Untergruppen von G derselben Ordnung gibt es?
- Sind gegebene Untergruppen derselben isomorph bzw. 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. Da $|V_4| = 2^2$ gilt, ist V_4 abelsch. Mit Satz 1.6.1 erhalten wir

$$V_4 \cong \langle (1,2)(3,4)\rangle \times \langle (1,3)(2,4)\rangle \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2) \ncong \mathbb{Z}/(4) \cong \langle (1,2,3,4)\rangle.$$

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 $N \subseteq \mathcal{A}_4$ von Ordnung 6. Damit gilt $[\mathcal{A}_4 : N] = 2$ und N ist bereits ein Normalteiler in $\mathcal{A}_4$ (!). Da $\mathcal{A}_4$ alle acht 3-Zyklen der $\mathcal{S}_4$ enthält, gibt es mindestens einen 3-Zykel in $\sigma \in \mathcal{A}_4 \setminus N$. Es gilt $|\langle\sigma\rangle| = 3$ und $N \cap \langle\sigma\rangle = \{\mathrm{id}\}$ nach dem Satz von Lagrange. Nun liefert uns Satz 1.5.3 bereits $|N\langle\sigma\rangle| = |N||\langle\sigma\rangle| = 18$, ein Widerspruch zu $N\langle\sigma\rangle \subseteq \mathcal{A}_4$.

Definition. Sei G eine endliche Gruppe.

(1) Sei $p \in \mathbb{N}$ eine Primzahl mit $|G| = p^m q \ ; \ p \nmid q$. 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.

(3) Ist $H \subseteq G$ eine Untergruppe der Gruppe G, so heißt

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}$$

der **Normalisator** von H in G. Damit ist $N_G(H)$ eine Untergruppe, die H als Normalteiler enthält.

Ist nun $S \subseteq G$ eine Sylow p-Untergruppe und gilt $|G| = p^m q$ mit $p \nmid q$, so folgt nach 1.1.5

$$[G:S] = q \ \text{ und } \ [G:N_G(S)] \mid q.$$

Satz 2.2.1 (Die Sylowschen Sätze). *Sei G eine endliche Gruppe, $p \in \mathbb{N}$ eine Primzahl mit $|G| = p^m q \ ; \ p \nmid q$. 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 $x \in G$ mit $xHx^{-1} \subseteq S$ ($\Leftrightarrow H \subseteq x^{-1}Sx$). Insbesondere ist H in einer Sylow p-Untergruppe enthalten.

(3) Es gilt $|\mathrm{Syl}_p(G)| \equiv 1 \mod(p)$ *sowie*

$$|\mathrm{Syl}_p(G)| = [G : N_G(S)] \quad \forall\, S \in \mathrm{Syl}_p(G).$$

Beweis.

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

$$X := \{S \in \mathcal{P}(G) \mid |S| = p^n\}$$

der p^n elementigen Teilmengen von G. Es wirkt G auf X vermöge

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

Wir betrachten

$$m_p \colon \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}_0, z \mapsto \max\{k \in \mathbb{N}_0 \mid p^k \text{ teilt } z\}.$$

Es gilt $|X| = \binom{|G|}{p^n} = \binom{p^n(p^l q)}{p^n}$. Nach Übungsserie 1 gilt damit $m_p(|X|) = l$. Da X die disjunkte Vereinigung seiner Bahnen ist, existiert daher ein $S \in X$ mit $p^{l+1} \nmid |G.S|$, d.h. $m_p(|G.S|) \leq l$. Wir setzen $U := \mathrm{Stab}_G(S)$ 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 $|S| = k|U|$. Insbesondere ist $|U|$ ein Teiler von p^n. Anderseits liefert die Bahnformel

$$(*) \quad |G| = |U| \cdot |G.S|$$

und damit $m_p(|U|) = m_p(|G|) - m_p(|G.S|) \geq m - l = n$. 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. Im Fall $H = \{e\}$ ist nichts zu zeigen. Andernfalls liefert Lemma 2.1.1: $|X^H| \equiv |X| \mod(p)$. Wegen $|X| = q \not\equiv 0 \mod(p)$ erhalten wir $X^H \neq \varnothing$. Damit gibt es $g \in G$ mit $hg^{-1}S = g^{-1}S$ für alle $h \in H$ und es folgt $gHg^{-1} \subseteq S$.

(3) Wir betrachten die Operation

$$G \times \mathrm{Syl}_p(G) \longrightarrow \mathrm{Syl}_p(G)\ ;\ (g, s) \mapsto gSg^{-1}.$$

Infolge (2) gilt $G.S = \mathrm{Syl}_p(G)$ für alle $S \in \mathrm{Syl}_p(G)$. Damit erhalten wir aus 1.7.2:

$$|\mathrm{Syl}_p(G)| = [G : G_S] \quad \forall\, S \in \mathrm{Syl}_p(G).$$

Definitionsgemäß gilt zudem $G_S = N_G(S)$.

Sei $S_0 \in \mathrm{Syl}_p(G)$. Wir betrachten die Operation

$$S_0 \times \mathrm{Syl}_p(G) \longrightarrow \mathrm{Syl}_p(G)\ ;\ (s, T) \mapsto sTs^{-1}.$$

Dann gilt $S_0 \in \mathrm{Syl}_p(G)^{S_0}$. Ist $T \in \mathrm{Syl}_p(G)^{S_0}$, so folgt $sTs^{-1} = T$ für alle $s \in S_0$ und somit $S_0 \subseteq N_G(T)$. Damit sind S_0 und T Sylow p-Untergruppen von $N_G(T)$ und (2) liefert ein $g \in N_G(T)$ mit $S_0 = gTg^{-1} = T$. Lemma 2.1.1 impliziert nun $|\mathrm{Syl}_p(G)| \equiv |\mathrm{Syl}_p(G)^{S_0}| = 1 \mod(p)$.

□

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 $T = gSg^{-1}$, d.h. die Operation von G auf $\mathrm{Syl}_p(G)$ durch Konjugation ist transitiv. Inbesondere ist eine Sylowgruppe $S \in \mathrm{Syl}_p(G)$ ein Normalteiler von G genau dann, $\mathrm{Syl}_p(G) = \{S\}$ gilt.*

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

Satz 2.2.3. *Sei G eine endliche Gruppe mit*

(a) $|G| = pq$ für Primzahlen $p < q$, und

(b) $p \nmid (q-1)$.

Dann gilt $G \cong \mathbb{Z}/\langle p\rangle \times \mathbb{Z}/\langle q\rangle \cong \mathbb{Z}/\langle pq\rangle$.

Beweis. Übung. □

Satz 2.2.4. *Sei $n \in \mathbb{N}_{\geq 4}$ und $S \in \mathrm{Syl}_2(\mathfrak{S}_n)$. Dann ist S nicht zyklisch.*

Beweis. Wir betrachten erneut die nicht zyklische Untergruppe

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

der Ordnung 2^2. Nach Satz 2.2.1(2) existiert eine Sylow 2-Untergruppe T von $\mathfrak{S}_n$, die V enthält. Damit ist T nach Satz 1.2.2 nicht zyklisch. Weiter liefert Korollar 2.2.2 uns $T \cong S$. Damit ist auch S nicht zyklisch. □

2.3 Auflösbare Gruppen

Sei G eine Gruppe. Eine **Normalreihe** in G ist eine Folge

$$\mathcal{G}: \quad \{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

von Untergruppen von G derart, dass G_i ein Normalteiler von G_{i+1} ist für $0 \leq i \leq n-1$. Die Gruppen G_{i+1}/G_i heißen **Faktoren** der Normalreihe.

Eine Gruppe $G \neq \{e\}$ heißt **einfach**, falls $\{e\}$ und G die einzigen Normalteiler von G sind.

Eine Normalreihe $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ von G heißt **Kompositionsreihe**, falls G_{i+1}/G_i einfach ist für $0 \leq i \leq n-1$.

Seien

$$\mathcal{G}: \quad \{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

und

$$\mathcal{H}: \quad \{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m = G$$

zwei Normalreihen von G. Dann heißt $\mathcal{H}$ **Verfeinerung** von $\mathcal{G}$ falls $\{G_i \mid 0 \leq i \leq n-1\} \subseteq \{H_i\,,\ 0 \leq i \leq m-1\}$ gilt.

Lemma 2.3.1. *Sei $\mathcal{G}: \{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ eine Normalreihe einer endlichen Gruppe G. Dann existiert eine Verfeinerung von $\mathcal{G}$, die eine Kompositionsreihe ist.*

Beweis. Wir verwenden Induktion nach $\ell := |G|$. Im Fall $\ell = 1$ ist nichts zu zeigen. Sei $i_0 := \min\{i \mid G_i = G\}$. Dann gilt $i_0 \geq 1$ und $G_{i_0-1} \neq G$ ist ein Normalteiler von G. Es sei nun H ein Normalteiler von G von maximaler Ordnung mit $G_{i_0-1} \subseteq H \subsetneq G$. Ist $N \subseteq G/H$ ein Normalteiler, so ist $U := \{g \in G \mid gH \in N\}$ ein Normalteiler[1] von G mit $H \subseteq U \subseteq G$. Nach Wahl von H gilt $U = H$ oder $U = G$. Damit erhalten wir $N = \{e\}$ oder $N = G/H$ und die Gruppe G/H ist einfach.

Wegen $|H| < \ell$ kann nach Induktionsannahme die Normalreihe $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{i_0-1} \subseteq H$ von H zu einer Kompositionsreihe $\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m = H$ von H verfeinert werden. Damit ist

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m \subseteq G$$

eine Kompositionsreihe von G, die $\mathcal{G}$ verfeinert. □

Definition. (1) Eine Normalreihe $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ einer Gruppe G heißt **abelsch**, falls jede Faktorgruppe G_{i+1}/G_i abelsch ist für $0 \leq i \leq n-1$.

(2) Eine Gruppe G heißt **auflösbar**, falls G eine abelsche Normalreihe besitzt.

Beispiele. (1) Jede abelsche Gruppe ist auflösbar.

(2) Die $\mathcal{S}_3$ ist nicht abelsch, dennoch auflösbar, da $\{\mathrm{id}\} \subseteq \mathcal{A}_3 \subseteq \mathcal{S}_3$ eine abelsche Normalreihe ist.

Satz 2.3.2. *Sei G eine Gruppe.*

(1) Ist $\varphi: G \longrightarrow G'$ ein Homomorphismus und ist G auflösbar, so ist $\varphi(G)$ auflösbar.

(2) Ist G auflösbar, so ist jede Untergruppe $H \subseteq G$ auflösbar.

(3) Ist $N \subseteq G$ ein Normalteiler, so ist G genau dann auflösbar, wenn N und G/N auflösbar sind.

Beweis.

[1] Es gilt $U = \pi^{-1}(N)$ für die kanonische Projektion $\pi: G \longrightarrow G/H$.

(1) Es sei $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ eine abelsche Normalreihe. Dann ist $\varphi(G_i)$ ein Normalteiler von $\varphi(G_{i+1})$ und

$$\bar{\varphi} : G_{i+1}/G_i \longrightarrow \varphi(G_{i+1})/\varphi(G_i) \ ; \ gG_i \mapsto \varphi(g)\varphi(G_i)$$

ist ein surjektiver Homomorphismus. Damit ist $\{e\} = \varphi(G_0) \subseteq \varphi(G_1) \subseteq \cdots \subseteq \varphi(G_n) = \varphi(G)$ eine abelsche Normalreihe von $\varphi(G)$.

(2) Ist $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ eine abelsche Normalreihe von G, so ist $H \cap G_i$ normal in $H \cap G_{i+1}$ und

$$H \cap G_{i+1}/H \cap G_i \longrightarrow G_{i+1}/G_i \ ; \ h(H \cap G_i) \mapsto hG_i$$

ist ein injektiver Homomorphismus. Damit ist $\{e\} = H \cap G_0 \subseteq H \cap G_1 \subseteq \cdots \subseteq H \cap G_n = H$ eine abelsche Normalreihe von H.

(3) Ist G auflösbar, so sind N und G/N nach (2) und (1) auflösbar. Seien nun umgekehrt N und G/N auflösbar. Dann existieren abelsche Normalreihen

$$\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_n = N \text{ und } \{e\} = G'_0 \subseteq G'_1 \subseteq \cdots \subseteq G'_m = G/N$$

von N und G/N. Es sei $\pi : G \longrightarrow G/N$ die kanonische Projektion. Dann ist $G_i := \pi^{-1}(G'_i)$ ein Normalteiler von $G_{i+1} = \pi^{-1}(G'_{i+1})$ und der Homomorphismus

$$\bar{\pi} : G_{i+1}/G_i \longrightarrow G'_{i+1}/G'_i \ \ gG_i \mapsto \pi(g)G'_i$$

ist bijektiv. Damit ist $\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_n = N = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m = G$ eine abelsche Normalreihe.

□

Korollar 2.3.3. *Sei G eine Gruppe sowie $N \subseteq G$ ein auflösbarer Normalteiler und $H \subseteq G$ eine auflösbare Untergruppe. Dann ist NH auflösbar.*

Beweis. Es ist N eine normale Untergruppe von NH und Satz 1.5.3 liefert einen Isomorphismus

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

Da H auflösbar ist, gilt dies nach Satz 2.3.2 auch für $H/H \cap N$. Damit ist NH/N auflösbar und Satz 2.3.2 liefert die Behauptung. □

Korollar 2.3.4. *Sei p eine Primzahl. Dann ist jede p-Gruppe auflösbar.*

Beweis. Sei $G \neq \{e\}$ eine p-Gruppe. Nach Korollar 2.1.2 gilt $Z(G) \neq \{e\}$. Damit ist $G' := G/Z(G)$ eine p-Gruppe kleinerer Ordnung. Wir können also induktiv annehmen, dass G' auflösbar ist. Da $Z(G)$ auflösbar ist, folgt die Behauptung mit Satz 2.3.2. □

Satz 2.3.5. *Sei G eine endliche auflösbare Gruppe. Dann existiert eine Kompositionsreihe $\{e\}=G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n=G$ und Primzahlen $p_1,\ldots,p_n \in \mathbb{N}$ mit $G_i/G_{i-1} \cong \mathbb{Z}/\langle p_i\rangle$ für $1 \leq i \leq n$.*

Beweis. Da G auflösbar ist, besitzt G eine abelsche Normalreihe. Nach Lemma 2.3.1 besitzt diese eine Verfeinerung

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots G_n = G$$

zu einer Kompositionsreihe. Diese ist dann ebenfalls abelsch. Es bleibt zu zeigen: Jede einfache abelsche Gruppe H ist zyklisch von Primzahlordnung.

Sei $|H| = m$. Da H einfach und abelsch ist, besitzt H keine Untergruppen $\neq \{e\}, H$. Gilt $x \in H \setminus \{e\}$, so ist $\langle x\rangle \neq \{e\}$ eine Untergruppe von H und es folgt $H = \langle x\rangle$. Ist $p \in \mathbb{N}$ ein Primteiler von m, so liefert Satz 2.2.1 eine Untergruppe $H_p \subseteq H$ mit $|H_p| = p$. Wir erhalten $H = H_p$ und somit $H \cong \mathbb{Z}/\langle p\rangle$. □

Definition. Sei G eine Gruppe, $x, y \in G$.

(1) $[x,y] := xyx^{-1}y^{-1}$ heißt der **Kommutator** von x und y.

(2) $D(G) := [G,G] := \langle\{[g,h] \mid g,h \in G\}\rangle$ heißt **Kommutatoruntergruppe** von G.

(3) Die durch $D^0(G) := G$, $D^n(G) := [D^{n-1}(G), D^{n-1}(G)]$ $(n \in \mathbb{N})$ induktiv definierte Folge $(D^n(G))_{n\geq 0}$ von Untergruppen von G, heißt **abgeleitete Reihe von** G.

Satz 2.3.6. *Sei G eine Gruppe. Dann sind folgende Aussagen äquivalent:*

(1) G ist auflösbar.

(2) Es existiert ein $m \in \mathbb{N}$ mit $D^m(G) = \{e\}$.

Beweis. (1) ⇒ (2). Sei H eine Gruppe und $N \subseteq H$ ein Normalteiler derart, dass H/N abelsch ist, so gilt für die kanonische Projektion $\pi : H \longrightarrow H/N$: $\pi(D(H)) \subseteq D(H/N) = \{e\}$. Damit erhalten wir $D(H) \subseteq \ker\pi = N$.

Sei nun $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m = G$ eine abelsche Normalreihe. Obige Beobachtung liefert $D(G_{i+1}) \subseteq G_i$ für alle i. Damit folgt

$$D^j(G) \subseteq G_{m-j}$$

und somit $D^m(G) = \{e\}$.

(2) ⇒ (1). Sei $\varphi \in \mathrm{Aut}(G)$ ein Automorphismus von G. Durch Induktion zeigt man

$$(*) \quad \varphi(D^j(G)) = D^j(G) \quad \forall\, j \in \mathbb{N}_0.$$

Sei $g \in G$. Dann ist

$$\iota_g : G \longrightarrow G \;;\; x \mapsto gxg^{-1}$$

ein Automorphismus von G. Nach $(*)$ ist damit $D^j(G)$ für jedes $j \in \mathbb{N}_0$ ein Normalteiler von G. Zudem ist die Faktorgruppe $D^j(G)/D^{j+1}(G)$ abelsch. Also ist

$$\{e\} = D^m(G) \subseteq D^{m-1}(G) \subseteq \cdots \subseteq D^0(G) = G$$

eine abelsche Normalreihe von G. □

Satz 2.3.7. *Sei $n \in \mathbb{N}$. Die symmetrische Gruppe $\mathcal{S}_n$ ist auflösbar, genau dann, wenn $n \in \{1,2,3,4\}$.*

Beweis. In den Übungsserien wird gezeigt, dass $\mathcal{S}_4$ auflösbar ist. Für $n \leq 4$ betrachten wir betrachten den injektiven Homomorphismus

$$\varphi_n : \mathcal{S}_n \longrightarrow \mathcal{S}_4 \ ; \ \varphi(\sigma)(j) := \begin{cases} \sigma(j) & 1 \leq j \leq n \\ j & j > n. \end{cases}$$

Also ist $\mathcal{S}_n$ isomorph zu einer Untergruppe von $\mathcal{S}_4$ und nach Satz 2.3.2 ebenfalls auflösbar. Sei nun $n \geq 5$. Seien $a,b,c,d,e \in \{1,\ldots,n\}$ fünf paarweise verschiedene Zahlen. Dann gilt für $x := (a,b,d)$ und $y := (a,c,e)$

$$(*) \quad [x,y] = (a,b,c).$$

Damit enthält $D(\mathcal{S}_n)$ sämtliche 3-Zykel und ein Ergebnis aus den Übungsserien liefert $\mathcal{A}_n \subseteq D(\mathcal{S}_n)$. Da $\mathcal{S}_n/A_n$ als Gruppe von Ordnung 2 abelsch ist, gilt andererseits $D(\mathcal{S}_n) \subseteq A_n$. Insgesamt gilt also $D(\mathcal{S}_n) = \mathcal{A}_n$. Erneute Anwendung von $(*)$ liefert $D(\mathcal{A}_n) = \mathcal{A}_n$. Nach Satz 2.3.6 ist $\mathcal{S}_n$ daher nicht auflösbar. □

3 Grundlagen der Ringtheorie

3.1 Ringe, Homomorphismen und Ideale

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 $1a = a = a1 \ \ \forall\, a \in R$.

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. Jeder Körper ist ein kommutativer Ring.

(2) Ist $(R_i)_{i \in I}$ eine Familie von Ringen, so ist $\prod_{i \in I} R_i$ ein Ring mit Operationen

$$(x_i)_{i \in I} + (y_i)_{i \in I} := (x_i + y_i)_{i \in I} \ \text{ und } \ (x_i)_{i \in I}(y_i)_{i \in I} := (x_i y_i)_{i \in I}.$$

(3) Es sei V ein $\mathbb{R}$-Vektorraum, dann erhält die Menge

$$\mathrm{End}_{\mathbb{R}}(V) = \{f \colon V \longrightarrow V \mid f \ \mathbb{R}\text{-linear}\}$$

mit den Verknüpfungen

$$(f + g)(v) = f(v) + g(v) \text{ sowie } (fg)(v) = f(g(v))$$

die Struktur eines Rings.

(4) Sei X eine Menge. Dann ist $(\mathcal{P}(X), \Delta, \cap)$ ein kommutativer Ring mit $0_{\mathcal{P}(X)} = \varnothing$ und $1_{\mathcal{P}(X)} = X$, wobei Δ die symmetrische Differenz bezeichnet.

(5) Ist R ein Ring und X eine nicht-leere Menge, dann erhält die Menge der Abbildungen $\mathrm{Abb}(X, R)$ von X nach R durch $(f + g)(x) = f(x) + g(x)$, $(f \cdot g)(x) = f(x)g(x)$ die Struktur eines Rings.

Definition. Sei R eine 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 **Linksideal** (**Rechtsideal**), falls gilt

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

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

(3) Eine Teilmenge $I \subseteq R$ ist ein **Ideal**, falls I sowohl ein Linksideal als auch ein Rechtsideal ist.

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*, $x_\ell \in I_\ell \ \forall\, \ell \in \Lambda'\}$ *ist ein Ideal von R.*

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

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

Beweis. Die Aussagen folgen durch direktes Nachrechnen. □

Definition. Ist $I \subseteq R$ ein Ideal, so definiert man induktiv

$$I^n := II^{n-1} \quad \forall\, n \geq 2.$$

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) Es sei $R := \mathrm{Mat}_2(\mathbb{Q})$ der Ring der (2×2)-Matrizen über $\mathbb{Q}$.

(a) $\mathrm{Upp}_2(\mathbb{Q}) := \{(a_{ij}) \in R \mid a_{21} = 0\}$ ist ein Unterring von R.

(b) $I := \{(a_{ij}) \in R \mid a_{12} = 0 = a_{22}\}$ ist ein Linksideal von R, das kein Rechtsideal ist.

(c) $J := \{(a_{ij}) \in R \mid a_{11} = 0 = a_{12}\}$ ist ein Rechtsideal von R, das kein Linksideal ist.

(d) $\{0\}$ und R sind die einzigen Ideale von R: Ist $I \neq \{0\}$ ein Ideal von R, so gibt es $A = (a_{ij}) \in R$ mit $a_{i_0,j_0} \neq 0$. Für $\ell, k \in \{1, 2\}$ erhalten wir

$$a_{i_0,j_0}^{-1} E_{\ell i_0} A E_{j_0,k} = E_{\ell k} \in I.$$

Hierbei ist $E_{\ell k} := (\delta_{i\ell}\delta_{jk})$. Damit folgt insbesondere $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = E_{11} + E_{22} \in I$ und somit $B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) B \in I$ für alle $B \in R$.

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

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

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

Bemerkungen. 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

$$\pi : \left\{ \begin{array}{ccc} R & \longrightarrow & R/I \\ x & \mapsto & x+I \end{array} \right.$$

  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

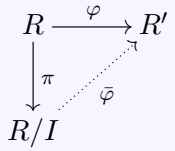
$$\varphi(xy) = \varphi(x)\varphi(y)$$

  und

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

  für alle $x, y \in \mathbb{Z}$.

Satz 3.1.2. *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. □

Ist R ein Ring, so bezeichnen wir mit $\mathrm{Id}(R)$ die Menge der Ideale von R.

Satz 3.1.3. *Sei $I \subseteq R$ ein Ideal des Rings R sowie $\mathrm{Id}_I(R) := \{J \in \mathrm{Id}(R) \mid I \subseteq J\}$. Dann ist*

$$\Pi : \begin{cases} \mathrm{Id}(R/I) & \longrightarrow & \mathrm{Id}_I(R) \\ J & \mapsto & \pi^{-1}(J) \end{cases}$$

eine inklusionserhaltende Bijektion.

Beweis.

- Π ist wohldefiniert: Für $J \in \mathrm{Id}(R/I)$ ist $\pi^{-1}(J)$ ein Ideal von R mit $I = \ker \pi \subseteq \pi^{-1}(J)$.
- Π ist surjektiv: Sei $L \in \mathrm{Id}_I(R)$. Da $\pi : R \longrightarrow R/I$ surjektiv ist, ist $\pi(L)$ ein Ideal von R/I mit $L \subseteq \pi^{-1}(\pi(L))$. Sei $x \in \pi^{-1}(\pi(L))$. Dann existiert $y \in L$ mit $\pi(x) = \pi(y)$, und damit $x - y \in \ker \pi \subseteq L$. Es folgt also $x = (x-y)+y \in L$. Wir erhalten $L = \Pi(\pi(L))$ und damit die Surjektivität von Π.
- Π ist injektiv: Seien nun $J, J' \in \mathrm{Id}(R/I)$ mit $\Pi(J) = \Pi(J')$, so liefert die Surjektivität von π

$$J = \pi(\pi^{-1}(J)) = \pi(\Pi(J)) = \pi(\Pi(J')) = \pi(\pi^{-1}(J')) = J'.$$

□

3.2 Einheiten und Nullteiler

Definition. Sei R ein Ring, $x \in R$.

(1) Ein Element $y \in R$ heißt **linksinverses** (**rechtsinverses**) Element zu x, falls gilt $yx = 1$ ($xy = 1$).

(2) Das Element $x \in R$ heißt **invertierbar** oder **Einheit** falls x ein linksinverses Element und ein rechtsinverses Element besitzt.

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

Beispiele. (1) Sei V ein endlich dimensionaler $\mathbb{R}$-Vektorraum. Besitzt $f \in \mathrm{End}_{\mathbb{R}}(V)$ ein linksinverses g, so gilt $g \circ f = \mathrm{id}_V$ und g ist insbesondere surjektiv. Da $\dim_k V$ endlich ist, folgt damit nach [5, 5.3.5] bereits die Bijektivität von g. Damit gilt $f \circ g = (g^{-1} \circ g) \circ (f \circ g) = g^{-1} \circ (g \circ f) \circ g = \mathrm{id}_V$ ist f 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 $R := \mathrm{End}_{\mathbb{R}}(V)$. Dann 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, φ besitzt ein rechtsinverses Element $\gamma \in R$. Dann gilt $\varphi \circ \gamma = \mathrm{id}_V$ und φ ist surjektiv. Aus $(1, 0, 0, \ldots) \notin \mathrm{im}\,\varphi$ erhalten wir einen Widerspruch.

Definition. Sei R ein Ring.

(1) Die Gruppe

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

heißt die **Einheitengruppe** von R.

(2) Gilt $R \neq \{0\}$ und $R^\times = R \setminus \{0\}$, so heißt R **Divisionsring** oder **Schiefkörper**. Ist R zudem kommutativ, so ist R ein **Körper**.

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

(2) Es gilt $(\mathbb{R} \times \mathbb{R})^\times = \mathbb{R}^\times \times \mathbb{R}^\times$.

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

(1) R ist ein Divisionsring.

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

(3) $\{0\}$ und R sind die einzigen Rechtsideale von R.

Beweis. (1) $\Rightarrow$ (2). Sei $I \neq \{0\}$ ein Linksideal in R. Dann gibt es $x \in I \setminus \{0\}$. Da R Divisionsring ist, existiert $r \in R$ mit $rx = 1$. Damit folgt $1 \in I$ und somit $s = s1 \in I$ für alle $s \in R$. Wir erhalten also $I = R$.

(2) $\Rightarrow$ (1). Sei $x \in R \setminus \{0\}$. Dann ist

$$Rx := \{rx \mid r \in R\}$$

ein Linksideal $\neq \{0\}$ und es folgt $Rx = R$. Also gibt es $a \in R$ mit $ax = 1$. Wegen $a \neq 0$ gibt es ebenfalls $y \in R$ mit $ya = 1$. Es folgt

$$y = y1 = y(ax) = (ya)x = 1x = x.$$

Wir erhalten $xa = 1 = xa$ und somit ist x invertierbar.
Der Beweis von (1) $\Leftrightarrow$ (2) verläuft analog. □

Bemerkung. Das Beispiel $R = \mathrm{Mat}_n(k)$ zeigt für $n \geq 2$, dass ein Ring, dessen einzige Ideale $\{0\}$ und R sind, nicht notwendig ein Divisionsring ist.

Korollar 3.2.2. *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). Dies folgt aus Satz 3.2.1.
(2) $\Rightarrow$ (3). Wegen $\varphi(1) = 1 \neq 0$ gilt $\ker \varphi \neq R$. Damit liefert (2) $\ker \varphi = \{0\}$ und φ ist injektiv.
(3) $\Rightarrow$ (1). Sei $L \subseteq R$ ein Linksideal mit $L \neq R$. Da R kommutativ ist, ist L ein Ideal und es folgt $R' := R/L \neq \{0\}$. Damit ist $\pi : R \longrightarrow R' \; ; \; x \mapsto x + L$ nach (3) injektiv und $L = \ker \pi = \{0\}$. Nach Satz 3.2.1 ist R damit ein Körper. □

Definition. Sei R ein Ring.

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

(2) Ein **Nullteiler** von R ist ein Element, welches ein Linksnullteiler oder ein Rechtsnullteiler ist.

(3) Ist $R \neq \{0\}$ ein kommutativer Ring, sodass 0 der einzige Nullteiler von R ist, 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 nämlich $\dim_{\mathbb{R}} V \geq 2$ so finden wir echte Untervektorräume $U, W \subseteq V$ mit $U \oplus W = V$. Die kanonischen Projektionen $\pi_U : V \longrightarrow V, u + w \mapsto u$, $\pi_W : V \longrightarrow V, u + w \mapsto w$ erfüllen $\pi_U \circ \pi_W$, aber $\pi_U \neq 0 \neq \pi_W$.

Lemma 3.2.3. *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

$$\ell_x : \left\{ \begin{array}{ccc} R & \longrightarrow & R \\ r & \mapsto & xr \end{array} \right.$$

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

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

(2) $\mathbb{Z}/\langle n\rangle$ ist ein Körper.

(3) n ist eine Primzahl.

Beweis. (1) ⇒ (2). Dies folgt aus Lemma 3.2.3.

(2) ⇒ (3). Seien $a, b \in \mathbb{Z}$ mit $n|ab$. Dann gilt $(a+\langle n\rangle)(b+\langle n\rangle) = ab+\langle n\rangle = 0$. Da $\mathbb{Z}/\langle n\rangle$ ein Körper ist, folgt $a+\langle n\rangle = 0$ oder $b+\langle n\rangle = 0$, also $n|a$ oder $n|b$. Damit ist n eine Primzahl.

(3) ⇒ (1). Seien $\bar{x}, \bar{y} \in \mathbb{Z}/\langle n\rangle$ mit $\bar{x}\bar{y} = 0$ gegeben. Wir schreiben $\bar{x} = x+\langle n\rangle$ sowie $\bar{y} = y+\langle n\rangle$ und erhalten $xy \in \langle n\rangle$. Da n eine Primzahl ist, folgt $n|x$ oder $n|y$ und daher $\bar{x} = 0$ oder $\bar{y} = 0$. Damit ist $\mathbb{Z}/\langle n\rangle$ ein Integritätsbereich. □

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

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

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

Definition. Die Abbildung

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & R \\ n & \mapsto & n1 \end{array} \right.$$

ist ein Ringhomomorphismus. 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 $\ker\varphi = \langle n\rangle$. Die Zahl $n =: \operatorname{char}(R)$ heißt die **Charakteristik** von R.

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

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

Lemma 3.2.5. *Sei R ein Integritätsbereich. Dann ist $\mathrm{char}(R)=0$ oder $\mathrm{char}(R)$ ist eine Primzahl.*

Beweis. Die Abbildung $\varphi : \mathbb{Z} \longrightarrow R\ ;\ n \mapsto n1$ induziert einen injektiven Homomorphismus $\bar{\varphi} : \mathbb{Z}/\langle \mathrm{char}(R)\rangle \hookrightarrow R$. Damit ist $\mathbb{Z}/\langle \mathrm{char}(R)\rangle$ ein Integritätbereich. Wegen $R \neq \{0\}$ folgt $\mathrm{char}(R) \neq 1$ und Satz 3.2.4 liefert die Behauptung. □

3.3 Kommutative Ringe

Sei R ein kommutativer Ring. Dann ist jedes Linksideal und jedes Rechtsideal von R bereits ein Ideal. Ist $X \subseteq R$ eine Teilmenge, so ist

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

ein Ideal von R. Es gilt $(X) = \bigcap_{I \in \mathrm{Id}_X(R)} I$, wobei $\mathrm{Id}_X(R) := \{I \in \mathrm{Id}(R) \ \mid\ X \subseteq I\}$. Man nennt (X) das **von X erzeugte Ideal** von R. Gilt $X = \{x_1, \ldots, x_n\}$, so schreiben wir $(X) = (x_1, \ldots, x_n)$. Im Fall $X = \{x\}$ gilt $(X) = Rx = \{rx \mid r \in R\}$. Solche Ideale heißen **Hauptideale**. Ein Ideal $I \subseteq R$ heißt **endlich erzeugt**, falls es $x_1, \ldots, x_n \in I$ mit $I = (x_1, \ldots, x_n)$ gibt.

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

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

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

Beweis.

(1) Sei $I \subseteq R$ ein maximales Ideal. Wegen $I \subsetneq R$ gilt $R/I \neq \{0\}$. Nach Satz 3.1.3 sind $\{0\}$ und R/I die einzigen Ideale von R/I. Damit zeigt Korollar 3.2.2, dass R/I ein Körper ist.

Sei umgekehrt R/I ein Körper. Dann gilt $I \neq R$. Anwendung von Satz 3.1.3 und Korollar 3.2.2 liefert $\mathrm{Id}_I(R) = \{I, R\}$. Damit ist I ein maximales Ideal von 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 $(x+I)(y+I) = 0$. 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. Da jeder Körper ein Integritätsbereich ist, liefert Lemma 3.3.1: Jedes maximale Ideal $\mathfrak{m} \subseteq R$ ist ein Primideal.

Beispiel. Sei I ein maximales Ideal von $\mathbb{Z}$. Insbesondere ist $(I, +)$ eine Untergruppe von $(\mathbb{Z}, +)$ und damit zyklisch. Also existiert $n \in \mathbb{N}_0$ mit $I = \langle x \rangle = (x)$. Da weder $\langle 1 \rangle = \mathbb{Z}$ noch $\langle 0 \rangle = \{0\}$ maximale Ideale sind, folgt $n \geq 2$ und Satz 3.2.4 liefert $n \in \mathbb{P}$. Das heißt I ist maximal genau dann, wenn eine Primzahl $p \in \mathbb{P}$ mit $I = (p)$ existiert. Ebenso zeigt man, dass ein Ideal $I \subseteq \mathbb{Z}$ ein Primideal ist genau dann, wenn $I = \{0\}$ gilt oder eine Primzahl $p \in \mathbb{N}$ mit $I = (p)$ existiert.

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.[1]

Lemma 3.3.2 (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 3.3.3. *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. Übungsaufgabe. □

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

Bemerkungen. (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.

[1] 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 3.3.4 (Chinesischer Restsatz). *Es sei R ein kommutativer Ring, $I_1, \dots, I_n \subseteq R$ paarweise teilerfremde Ideale von R. Dann gilt:*

(1) Für jedes $j \in \{1, \dots, n\}$ 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 $\varphi : R \longrightarrow \prod_{j=1}^n R/I_j \; ; \; x \mapsto (x+I_1, \dots, x+I_n)$ ist surjektiv mit $\ker \varphi = \bigcap_{j=1}^n I_j$.

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

Beweis.

(1) Sei $j \in \{1, \dots, n\}$. 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 $j \in \{1, \dots, n\}$ 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 $x_1, \dots, x_n \in R$. Wir setzen $x := \sum_{j=1}^n x_j v_j$. Für $\ell \in \{1, \dots, n\}$ 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 $\varphi(x) = (x_1 + I_1, \dots, x_n + I_n)$. 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 folgende Kongruenzgleichungen erfüllt

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

Die Ideale $(5), (6), (7)$ von $\mathbb{Z}$ sind paarweise teilerfremd. Nach Satz 3.3.4 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 existierst ein $x \in \mathbb{Z}$ mit

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

Gemäß dem Beweis von 3.3.4(3) lässt sich eine Lösung wie folgt bestimmen. Wir verwenden den erweiterten euklidischen Algorithmus (siehe etwa [7]) 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.

3.4 Ringe der Brüche

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

Definition. Eine Teilmenge $D \subseteq R$ eines kommutativen Rings R heißt **multiplikativ abgeschlossen**, falls gilt

(a) $1 \in D$, und

(b) $d_1 d_2 \in D$ für alle $d_1, d_2 \in D$.

Beispiel. Sei R ein kommutativer Ring, $\mathfrak{p} \subseteq R$ ein Primideal. Dann ist $D := R \setminus \mathfrak{p}$ multiplikativ abgeschlossen. Ist R ein Integritätsbereich, so ist insbesondere $R\setminus\{0\}$ multiplikativ abgeschlossen.

Lemma 3.4.1. *Sei R ein kommutativer Ring, $D \subseteq R$ eine multiplikativ abgeschlossene Menge. Dann wird vermöge*

$$(r_1, d_1) \sim (r_2, d_2) \quad :\Leftrightarrow \quad \exists\, u \in D \text{ mit } u(r_1 d_2 - r_2 d_1) = 0$$

auf $R \times D$ eine Äquivalenzrelation definiert.

Beweis. Übungsaufgabe. □

Für $(r, d) \in R \times D$ setzen wir

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

für die Äquivalenzklasse von (r, d). Die Menge $(R \times D)/\sim$ der Äquivalenzklassen wird mit $D^{-1}R$ bezeichnet.

Bemerkung. Ist R ein Integritätsbereich und gilt $0 \notin D$, so erhalten wir

$$\frac{r_1}{d_1} = \frac{r_2}{d_2} \quad \Leftrightarrow \quad r_1 d_2 = r_2 d_1.$$

Dies entspricht der Gleicheit von Elementen aus $\mathbb{Q}$.

Satz 3.4.2. *Sei R ein kommutativer Ring, $D \subseteq R$ eine multiplikativ abgeschlossene Menge. Dann erhält $D^{-1}R$ vermöge*

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

für $r_1, r_2 \in R$ und $d_1, d_2 \in D$ die Struktur eines kommutativen Rings.

Beweis. Der Beweis erfolgt durch direktes Nachrechnen der Ringaxiome. Wir zeigen nur exemplarisch die Wohldefiniertheit der Addition. Seien $r_i \in R, d_i \in D$ für $1 \leq i \leq 4$ mit $(r_1, d_1) \sim (r_3, d_3)$ und $(r_2, d_2) \sim (r_4, d_4)$. Dann existieren $u, v \in D$ mit $u(r_1 d_3 - r_3 d_1) = 0 = v(r_2 d_4 - r_4 d_2)$. Es folgt

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

Da $uv \in D$ gilt, erhalten wir damit $(r_1 d_2 + r_2 d_1, d_1 d_2) \sim (r_3 d_4 + r_4 d_3, d_3 d_4)$. □

Definition. Sei R ein kommutativer Ring, $D \subseteq R$ eine multiplikativ abgeschlossene Teilmenge. Dann heißt $D^{-1}R$ der **Ring der Brüche von R bezüglich D**. Ist R ein Integritätsbereich, so heißt $Q(R) := (R \setminus \{0\})^{-1}R$ der **Quotientenkörper von R**.

Bemerkung. Ist R ein Integritätsbereich, dann ist $Q(R)$ ein Körper, da für $\frac{r}{d} \in Q(R) \setminus \{0_{Q(R)}\}$ stets $r \neq 0$ gilt und damit $\frac{d}{r} \in Q(R)$ gilt.

Definition. Sei R ein kommutativer Ring und $D \subseteq R$ eine multiplikative Menge, so bezeichen wir mit ι_D den Ringhomomorphismus

$$\iota_D \colon R \longrightarrow D^{-1}R \ ; \ r \mapsto \frac{r}{1}.$$

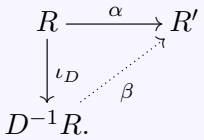
Bemerkungen. (1) Es gilt $r \in \ker \iota_D$ genau dann, wenn ein $u \in D$ mit $ur = 0$ existiert.

(2) Sei $d \in D$. Dann gilt $\iota_D(d) = \frac{d}{1}$ und

$$\iota_D(d)\frac{1}{d} = \frac{1}{1} = 1_{D^{-1}R}.$$

Damit gilt $\iota_D(d) \in (D^{-1}R)^\times$.

Satz 3.4.3 (Die universelle Eigenschaft des Rings der Brüche). *Sei R ein kommutativer Ring, $D \subseteq R$ eine multiplikativ abgeschlossene Teilmenge sowie $\alpha : R \longrightarrow R'$ ein Homomorphismus kommutativer Ringe derart, dass $\alpha(D) \subseteq (R')^\times$. Dann existiert genau ein Homomorphismus $\beta : D^{-1}R \longrightarrow R'$ mit $\beta \circ \iota_D = \alpha$. Wir erhalten also das kommutative Diagram*



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

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

Wir gehen schrittweise vor.

- $\bar{\alpha}$ ist konstant auf Äquivalenzklassen: Angenommen $(r_1, d_1) \sim (r_2, d_2)$. Dann gibt es $u \in D$ mit $u(r_1d_2 - r_2d_1)$. Also folgt $\alpha(u)\alpha(r_1d_2 - r_2d_1) = 0$ und wegen $\alpha(u) \in (R')^\times$ somit $0 = \alpha(r_1d_2 - r_2d_1) = \alpha(r_1)\alpha(d_2) - \alpha(r_2)\alpha(d_1)$. 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

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

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

- Eindeutigkeit der Abbildung: Sei nun $\gamma : D^{-1}R \longrightarrow R'$ ein weiterer Homomorphismus mit $\gamma \circ \iota_D = \alpha$. Dann gilt für $(r, d) \in R \times D$

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

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

□

Korollar 3.4.4. *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 3.4.3. 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 $\alpha(\mathbb{Z}\setminus\{0\}) \subseteq K^\times$. Damit gibt es nach Satz 3.4.3 einen Homomorphismus $\beta : Q(\mathbb{Z}) \longrightarrow K$ mit $\beta \circ \iota_{\mathbb{Z}\setminus\{0\}} = \alpha$. Da $Q(\mathbb{Z})$ ein Körper ist, ist β nach Korollar 3.2.2 injektiv. Nun wenden wir (1) an.

(3) Die Abbildung $\alpha\colon K \longrightarrow K, a \mapsto a$ erfüllt die Voraussetzung von Satz 3.4.3 und wir erhalten einen eindeutig bestimmten Ringhomomorphismus $\beta\colon Q(K) \longrightarrow K$ mit $\beta \circ \iota_{K\setminus\{0\}} = \alpha$. Da α surjektiv ist, gilt dies auch für β. Weiter ist $Q(K)$ ein Körper und damit β injektiv nach Korollar 3.2.2.

□

3.5 Teilbarkeit in Integritätsbereichen

Definition. Sei R ein Integritätsbereich.

(1) Seien $a, b \in R$. Man sagt a **teilt** b (wir schreiben in diesem Fall $a|b$), 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. Es sei R ein Integritätsbereich.

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

(2) Zwei Elemente $a, b \in R$ sind zueinander assoziiert genau dann, 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 $b = 1a$. Andernfalls erhalten wir aus $b = sa = stb$,

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

Da R ein Integritätsbereich ist, folgt nun $st = 1$ und somit $s \in R^\times$.

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

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

(2) Das Element p heißt **Primelement**, falls aus $p|ab$ stets $p|a$ 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) Wir betrachten den Unterring

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

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

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

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

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

Also erhalten wir $y_1=0=y_2$ und ohne Beschränkung $|x_1|=1$, das heißt $x_1+i\sqrt{5}y_1 \in \mathbb{Z}[\sqrt{-5}]^\times$. 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 $2|6=(1+i\sqrt{5})(1-i\sqrt{5})$, aber $2 \nmid (1\pm\sqrt{5})$, da $\mathcal{N}(2)=4$ und $\mathcal{N}(1\pm\sqrt{5})=6$.

Definition. Sei R ein Integritätsbereich.

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

(i) Für jedes $a \in R\backslash(\{0\} \cup R^\times)$ gibt es irreduzible Elemente $p_1,\ldots,p_n$ mit $a=p_1p_2\cdots p_n$.

(ii) Gilt $p_1p_2\cdots p_n = q_1q_2\cdots q_m$ mit p_i, q_j irreduzibel, so gilt $m=n$ und es gibt eine Permutation $\sigma \in \mathcal{S}_n$ mit $q_i \sim p_{\sigma(i)}$ für jedes $i \in \{1,\ldots,n\}$.

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

(3) R heißt **euklidisch**, falls eine Abbildung $\rho : R\backslash\{0\} \longrightarrow \mathbb{N}_0$ existiert derart, dass zu je zwei Elementen $a,b \in R$, $b \neq 0$ Elemente $q,r \in R$ mit $a=qb+r$ und $r=0$ oder $\rho(r)<\rho(b)$ existieren.

Satz 3.5.1. *Sei R ein Ring.*

(1) Ist R ein faktoriell, so ist jedes irreduzible Element prim.

(2) Ist R ein Hauptidealring, so ist jedes Primideal $\mathfrak{p} \neq \{0\}$ maximal und jedes irreduzible Element bereits prim.

Beweis.

(1) Sei $p \in R$ irreduzibel und $a, b \in R$ mit $p \mid ab$. Wir wollen $p \mid a$ oder $p \mid b$ nachweisen. Wir können daher 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) Sei $\mathfrak{p} \neq \{0\}$ ein Primideal. Da R ein Hauptidealring ist, gilt $\mathfrak{p} = (p)$, wobei $p \in R$ ein Primelement ist. Satz 3.3.3 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 $(p) = \mathfrak{m}$ 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 Irreduzibitlät von p_0 liefert $p_0 \sim q_0$. Also ist q_0 ein Primelement.

□

Satz 3.5.2. *Sei R ein Hauptidealring. Dann ist R faktoriell.*

Beweis. Sei $a \in R \setminus (\{0\} \cup R^\times)$. Wir gehen schrittweise vor.

- Existenz der Zerlegung: Angenommen, a besitzt keine Faktorisierung wie in (i).

  Wegen $a \in R \setminus (\{0\} \cup R^\times)$ gilt $\{0\} \subsetneq (a) \subsetneq R$ und nach Satz 3.3.3 gibt es ein maximales Ideal $\mathfrak{m}_1 \subseteq R$ mit $(a) \subseteq \mathfrak{m}_1$[2]. 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 eine Folge $(p_i)_{i \in \mathbb{N}}$ von irreduziblen Elementen mit $a_i = a_{i+1} p_{i+1}$ und $(a_i) \subsetneq (a_{i+1})$ sowie $(a_i) \subsetneq R$ für alle $i \in \mathbb{N}$. In den Übungsserien wird gezeigt, dass dies nicht sein kann.

- Eindeutigkeit der Zerlegung: Es seien $p_1, \ldots, p_n, q_1, \ldots, q_m$ irreduzible Elemente mit $p_1 \cdots p_n = q_1 \cdots q_m$. Wir beweisen die Eindeutigkeit durch Induktion nach n.

  Gilt $n = 1$, so folgt $p_1 = q_1 (q_2 \cdots q_m)$. Damit ist der zweite Faktor eine Einheit, was $m = 1$ impliziert. Sei $n > 1$. Da p_n nach Satz 3.5.1 ein Primelement ist, gibt es ein $j_n \in \{1, \ldots, m\}$ $p_n | q_{j_n}$. Da q_{j_n} irreduzibel ist, existiert eine Einheit u mit $q_{j_n} = u p_n$ und es folgt $p_n \sim q_{j_n}$. Da R ein Integritätsbereich ist, erhalten wir zudem

  $$p_1 \cdots p_{n-1} = u q_1 \cdots q_{j_n - 1} q_{j_n + 1} \cdots q_m.$$

  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

[2] 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.

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 $1 \leq i \leq n$ und R ist faktoriell.

□

Satz 3.5.3. *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 $I = (x_0)$. □

Bemerkungen. (1) Das analoge Argument wie im obigen Beweis zeigt, dass jede Untergruppe von $(\mathbb{Z}, +)$ zyklisch ist.

(2) 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].

(3) Wir haben damit folgende Implikationen für einen Ring R nachgewiesen.

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

Definition. Es sei R ein Integritätsbereich und $r_1, \ldots, r_n \in R$ mit $n \in \mathbb{N}$. Ein Element $a \in R$ heißt ggT (**größter gemeinsamer Teiler**) von $r_1, \ldots, r_n$ falls folgende Bedingungen erfüllt sind.

(1) Es gilt $a \mid r_i$ für alle $i \in \{1, \ldots, n\}$.

(2) Ist $b \in R$ mit $b \mid r_i$ für alle $i \in \{1, \ldots, n\}$, so gilt bereits $b \mid a$.

Wir bezeichnen die Menge der größten gemeinsanem Teiler von $r_1, \ldots, r_n$ mit $\mathrm{ggT}(r_1, \ldots, r_n)$.

Bemerkung. Sind $a, b \in \mathrm{ggT}(r_1, \ldots, r_n)$, so gilt $a|b$ und $b|a$. Das heißt $a \sim b$. Weiter sieht man ein, dass für jeden größten gemeinsamen Teiler $c \in \mathrm{ggT}(r_1, \ldots, r_n)$ die Gleichung

$$\mathrm{ggT}(r_1, \ldots, r_n) = cR^\times$$

gilt.

Beispiele. (1) In $\mathbb{Z}$ gilt $\mathrm{ggT}(60, 105) = \{\pm 15\} = 15\mathbb{Z}^\times$.

(2) In $\mathbb{Z}[\sqrt{-5}]$ gilt $\mathrm{ggT}(6, 2(1+i\sqrt{5})) = \varnothing$: Angenommen t ein größter gemeinsamer Teiler. Dann gilt $\mathcal{N}(t) \mid 36$ und $\mathcal{N}(t) \mid 24$, das heißt $\mathcal{N}(t) \mid 12$. Da 2 und $1 + i\sqrt{5}$ Teiler von 6 und $2(1 + i\sqrt{5})$ sind, liefert die ggT-Eigenschaft $2 \mid t$ und $1 + i\sqrt{5} \mid t$. Das heißt $12|\mathcal{N}(t)$. Damit gilt $\mathcal{N}(t) = 12$. Wir schreiben $t = a + bi\sqrt{5}$. Dann gilt $12 = \mathcal{N}(t) = a^2 + 5b^2$. Diese Gleichung besitzt in $\mathbb{Z}^2$ keine Lösung, ein Widerspruch.

(3) Es gilt $r_1 = r_2 = \cdots = r_n = 0 \Leftrightarrow ggT(r_1, \ldots, r_n) = \{0\}$.

Lemma 3.5.4. *Es sei R ein faktorieller Ring und $r_1, \ldots, r_n \in R$.*

(1) Es gilt $\varnothing \neq \mathrm{ggT}(r_1, \ldots, r_n)$.

(2) Ist $t \neq 0$ ein größter gemeinsamer Teiler der r_i und ist $ta_i = r_i$ für alle $i \in \{1, \ldots, n\}$, so gilt

$$\mathrm{ggT}(a_1, \ldots, a_n) = R^\times.$$

Beweis.

(1) Wir können annehmen, dass ein $1 \leq l \leq n$ mit $r_i \neq 0 \Leftrightarrow 1 \leq i \leq l$ existiert. Wir fixieren ein Repräsentantensystem $\mathcal{P}$ aller irreduziblen Element 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 $1 \leq i \leq l$ mit $m_p(r_i) \in \mathbb{N}_0$ für alle $p \in \mathcal{P}$. Für $p \in \mathcal{P}$ setzen wir

$$m(p) := \min\{p^{m_p(r_i)} \mid i \in \{1, \ldots, l\}\}.$$

Man überprüft nun, dass $g := \prod_{p \in \mathcal{P}} p^{m(p)}$ ein größter gemeinsamer Teiler der r_i ist.

(2) Da R faktoriell ist, existiert $g \in \mathrm{ggT}(a_1, \ldots, a_n) \neq \varnothing$. Es ist tg ein Teiler von $ta_i = r_i$ für alle $i \in \{1, \ldots, n\}$. Die ggT Eigenschaft liefert uns $tg \mid t$. Damit gilt $tg \sim t$. Das heißt es existiert eine Einheit $c \in R^\times$ mit $t(c - g) = 0$. Da $t \neq 0$ gilt, folgt $g = c$.

□

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 Konstruktion von Polynomringen

Der Begriff des Polynoms ist uns seit der Schule geläufig. Dort werden Polynome häufig mit denen von ihnen induzierten Funktionen gleichgesetzt. Hier muss jedoch unterscheiden, 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 $x^2 + x + 1$ beschreiben. 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 $f\colon \mathbb{Z}/(2) \longrightarrow \mathbb{Z}/(2)\,;\; r \mapsto r^2 + r + 1$.

Um den Unterschied der beiden Begriff klarer zu machen, führen wir dafür zunächst Polynome auf formale Weise ein und untersuchen erst im nächsten Abschnitt die induzierten Funktionen. Wir beschränken uns dabei nicht auf Polynome in einer „Variablen“ bzw. „Unbestimmten“.

Im Folgenden sei R ein kommutativer Ring und $n \in \mathbb{N}$. Wir definieren die Menge

$$R[X_1, \ldots, X_n] = R^{(\mathbb{N}_0^n)} := \{(r_\mu)_{\mu\in\mathbb{N}_0^n} \mid r_\mu \in R, r_\mu = 0 \text{ für alle bis auf endlich viele } \mu \in \mathbb{N}_0^n\}^{1}$$

und Abbildungen

$$+, \cdot\colon R[X_1, \ldots, X_n] \times R[X_1, \ldots, X_n] \longrightarrow R[X_1, \ldots, X_n]$$

durch

$$(r_\mu)_{\mu\in\mathbb{N}_0^n} + (s_\mu)_{\mu\in\mathbb{N}_0^n} := (r_\mu + s_\mu)_{\mu\in\mathbb{N}_0^n},\;\; (r_\mu)_{\mu\in\mathbb{N}_0^n} \cdot (s_\mu)_{\mu\in\mathbb{N}_0^n} := (t_\mu)_{\mu\in\mathbb{N}_0^n}$$

wobei

$$t_\mu := \sum_{\lambda,\nu\in\mathbb{N}_0^n;\lambda+\nu=\mu} r_\lambda s_\nu.$$

Direktes Nachprüfen der Ringaxiome zeigt:

Satz 4.1.1. *Sei R ein kommutativer Ring und $n \in \mathbb{N}_0$, so erhält das Tupel $(R[X_1, \ldots, X_n], +, \cdot)$ die Struktur eines kommutativen Ringes mit Einselement $(1_R\ \delta_{m0_{\mathbb{N}_0^n}})_{m\in\mathbb{N}_0^n}$.*

[1] Die betrachteten Tupel sind gerade die Funktionen $f\colon \mathbb{N}_0^n \longrightarrow R$ mit endlichem **Träger** $\operatorname{supp}(f) := \{\mu \in \mathbb{N}_0^n \mid f(\mu) \neq 0\}$.

Für $\mu \in \mathbb{N}_0^n$ sei mit $X^\mu := (1_R\, \delta_{m\mu})_{m\in\mathbb{N}_0^n} \in R[X_1, \ldots, X_n]$ das zu μ gehörige **Monom** bezeichnet. Weiter bezeichnen wir für $i \in \{1, \ldots, n\}$ mit $e_i \in \mathbb{N}_0^n$ den i-ten Einheitsvektor und definieren

$$X_i := X^{e_i}.$$

Die Elemente $X_1, \ldots, X_n$ heißen **Unbestimmte** über R. Für $i \in \{1, \ldots, n\}$ zeigt eine leichte Induktion nach $l \in \mathbb{N}_0$, dass $(X_i)^l = X^{le_i}$ gilt. Ist $\mu = (\mu_1, \ldots, \mu_n) \in \mathbb{N}_0^n$, so erhält man weiter

$$X^\mu = X^{\mu_1 e_1} \cdot X^{\mu_2 e_2} \cdots X^{\mu_n e_n} = (X_1)^{\mu_1} \cdot (X_2)^{\mu_2} \cdots (X_n)^{\mu_n}.$$

Jedes Element $(r_m)_{m\in\mathbb{N}_0^n} \in R[X_1, \ldots, X_n]$ lässt sich so auf eindeutige Weise in Unbestimmten $X_1, \ldots, X_n$ schreiben. Genauer gilt

$$(r_\mu)_{\mu\in\mathbb{N}_0^n} = \sum_{\mu\in\mathbb{N}_0^n} r_\mu X^\mu = \sum_{\mu\in\mathbb{N}_0^n} r_\mu X_1^{\mu_1} \cdots X_n^{\mu_n}.$$

Konvention: Wir schreiben von nun an

$$f = \sum_{\mu\in\mathbb{N}_0^n} r_\mu X_1^{\mu_1} \cdots X_n^{\mu_n} = \sum_{\mu\in\mathbb{N}_0^n} r_\mu X^\mu \in R[X_1, \ldots, X_n].$$

Insbesondere gilt also $r_\mu = 0$ für alle bis auf endlich viele $\mu \in \mathbb{N}_0^n$.

Obige Verknüpfungen lesen sich nun wie folgt:

$$\sum_{\mu\in\mathbb{N}_0^n} r_\mu X_1^{\mu_1} \cdots X_n^{\mu_n} + \sum_{\mu\in\mathbb{N}_0^n} s_\mu X_1^{\mu_1} \cdots X_n^{\mu_n} = \sum_{\mu\in\mathbb{N}_0^n} (r_\mu + s_\mu) X_1^{\mu_1} \cdots X_n^{\mu_n},$$

$$\sum_{\mu\in\mathbb{N}_0^n} r_\mu X_1^{\mu_1} \cdots X_n^{\mu_n} \cdot \sum_{\mu\in\mathbb{N}_0^n} s_\mu X_1^{\mu_1} \cdots X_n^{\mu_n} = \sum_{\mu\in\mathbb{N}_0^n} \left(\sum_{\lambda,\nu\in\mathbb{N}_0^n;\lambda+\nu=\mu} (r_\lambda s_\nu) \right) X_1^{\mu_1} \cdots X_n^{\mu_n}.$$

Definition. Für $\mu = (\mu_1, \ldots, \mu_n) \in \mathbb{N}_0^n$ definieren wir $|\mu| := \sum_{i=1}^n \mu_i$. Für ein Polynom $f = \sum_{\mu\in\mathbb{N}_0^n} r_\mu X^\mu$ heißt

$$\deg(f) := \begin{cases} \max\{|\mu| \mid r_\mu \neq 0\} & , f \neq 0 \\ -\infty & , f = 0 \end{cases}$$

der **Grad** des Polynoms f.

Beispiele. (1) Das Polynom $7X_1^6 + 4X_1^2 + 5 \in \mathbb{Z}[X_1]$ hat Grad 6.

(2) Das Polynom $2X_2X_4^3 + X_1X_2X_3X_4X_5 \in \mathbb{Z}[X_1, \ldots, X_6]$ hat Grad 5.

(3) Das Polynom $(1 + 2\mathbb{Z})X + (1 + 2\mathbb{Z})X \in \mathbb{Z}/(2)[X]$ hat Grad $-\infty$.

Satz 4.1.2 (Die universelle Eigenschaft des Polynomrings). *Sei $\varphi : R \longrightarrow S$ ein Homomorphismus kommutativer Ringe, $s = (s_1, \ldots, s_n) \in S^n$. Dann gibt es genau einen Homomorphismus von Ringen $\tilde{\varphi}_s : R[X_1, \ldots, X_n] \longrightarrow S$ mit*

(i) $\tilde{\varphi}_s(r) = \varphi(r) \quad \forall\, r \in R$ *und*

(ii) $\tilde{\varphi}_s(X_i) = s_i \quad \forall\, 1 \leq i \leq n$.

Beweis. Ist ψ ein Homomorphismus mit obigen Eigenschaften, so gilt

$$\psi(\sum_{\mu \in \mathbb{N}_0^n} r_\mu X^\mu) = \sum_{\mu \in \mathbb{N}_0^n} \psi(r_\mu)\psi(X_1^{\mu_1}) \cdots \psi(X_n^{\mu_n}) = \sum_{\mu \in \mathbb{N}_0^n} \varphi(r_\mu) s_1^{\mu_1} \cdots s_n^{\mu_n}$$

für alle Polynome $\sum_{\mu \in \mathbb{N}_0^n} r_\mu X^\mu$. Insbesondere existiert höchstens ein Homomorphismus mit obigen Eigenschaften und wir definieren notwendigerweise

$$\tilde{\varphi}_s \colon R[X_1, \ldots, X_n] \longrightarrow S \,;\, \sum_{\mu \in \mathbb{N}_0^n} r_\mu X^\mu \mapsto \sum_{\mu \in \mathbb{N}_0^n} \varphi(r_\mu) s_1^{\mu_1} \cdots s_n^{\mu_n}.$$

Man rechnet nun nach, dass $\tilde{\varphi}_s$ ein Ringhomomorphismus ist. □

Korollar 4.1.3. *Es sei R ein kommutativer Ring und $n \geq 2$. Es gibt einen Isomorphismus*

$$R[X_1, \ldots, X_n] \cong R[X_1, \ldots, X_{n-1}][X_n].$$

Beweis. Übungsaufgabe. □

4.2 Polynome in einer Variablen und Nullstellen

In diesem Abschnitt studieren wir Polynomringe über einem kommutativen Ring R in einer Variablen. Anstatt $R[X_1]$ schreiben wir $R[X]$ und unterscheiden nicht zwischen $\mathbb{N}_0^1$ und $\mathbb{N}_0$. Weiter identifizieren wir im Folgenden den Ring R mit den konstanten Polynomen $\{rX^0 \mid r \in R\} \subseteq R[X]$, das heißt wir fassen R als Unterring von $R[X]$ auf.

Definition. Sei $f = \sum_{i \in \mathbb{N}_0} r_i X^i \in R[X] \setminus \{0\}$, dann ist $\deg(f) \in \mathbb{N}_0$ und $r_{\deg(f)}$ der **Leitkoeffizient** von f. Das Polynom f heißt **normiert**, falls der Leitkoeffizient $r_{\deg(f)} = 1$ erfüllt.

Satz 4.2.1. *Sei R ein kommutativer Ring.*

(1) Es gilt $\deg(f+g) \leq \max\{\deg(f), \deg(g)\} \quad \forall\, f, g \in R[X]$.

(2) Es gilt $\deg(fg) \leq \deg(f) + \deg(g) \quad \forall\, f, g \in R[X]$.

(3) Ist R ein Integritätsbereich, so gilt $\deg(fg) = \deg(f) + \deg(g) \quad \forall\, f, g \in R[X]$.

(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 liefert das Verfahren der Polynomdivision:

Satz 4.2.2. *Sei R ein kommutativer Ring sowie $g \in R[X] \setminus \{0\}$ ein Polynom, dessen höchster Koeffizient 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 ein kommutativer Ring, X eine Unbestimmte über R. Dann sind folgende Aussagen 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 3.5.3.
(2) ⇒ (3). Der Hauptidealring $R[X]$ ist insbesondere ein Integritätsbereich. Damit ist $R \subseteq R[X]$ ebenfalls ein Integritätsbereich. Nach Satz 4.1.2 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 3.3.1. Wegen $X \in \mathfrak{p}$ folgt $\mathfrak{p} \neq \{0\}$. Da R Hauptidealring ist, liefert 3.5.1 die Maximalität von $\mathfrak{p}$. Erneute Anwendung von Lemma 3.3.1 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. □

Definition. Sei $f = \sum_{i=0}^n a_i X^i \in R[X] \setminus \{0\}$. Ein Element $r \in R$ heißt **Nullstelle** oder **Wurzel** von f, falls $\sum_{i=0}^n a_i r^i = 0$ gilt.

Für $r \in R$ sei

$$\mathrm{ev}_r : \left\{ \begin{array}{ccc} R[X] & \longrightarrow & R \\ \sum_{i=0}^n a_i X^i & \mapsto & \sum_{i=0}^n a_i r^i \end{array} \right.$$

der nach Satz 4.1.2 eindeutig bestimmte Homomorphismus mit $\mathrm{ev}_r(a)=a\ \forall\, a\in R$ 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 $f=\sum_{i=0}^n a_iX^i$ und $r\in R$ werden wir von nun an

$$f(r):=\mathrm{ev}_r(f)=\sum_{i=0}^n a_ir^i\in R$$

schreiben.

Satz 4.2.4. *Sei R ein Integritätsbereich. Dann besitzt jedes Polynom $f\in R[X]\backslash\{0\}$ höchstens $\deg(f)$ Nullstellen.*

Beweis. Für ein Polynom $h\in R[X]\setminus\{0\}$ bezeichen wir mit $Z_R(h)$ die Nullstellen von h in R. 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 $\deg(a)<1$ 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 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 $\{1,2\}$.

Korollar 4.2.5. *Sei K ein Körper und $G\subseteq K^\times$ eine endliche Untergruppe. Dann ist G zyklisch.*

Beweis. Sei d ein Teiler von $|G|$ sowie $G_d\subseteq G$ eine Untergruppe der Ordnung d. Für $x\in G_d$ ist $\mathrm{ord}(x)$ nach dem Satz von Lagrange ein Teiler von d. Damit folgt $x^d=1$. Also ist x eine Nullstelle von $f_d:=X^d-1\in K[X]$ und $G_d\subseteq\{x\in K\mid f_d(x)=0\}$. Satz 4.2.4 zeigt nun

$$G_d=\{x\in K\mid f_d(x)=0\}.$$

Damit besitzt G höchstens eine Untergruppe der Ordnung d und nach Satz 1.2.4 ist G damit zyklisch. □

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 $n(r)\in\mathbb{N}$ mit $(X-r)^{n(r)}|f$ und $(X-r)^{n(r)+1}\nmid f$. Dann heißt $n(r)$ die **Vielfachheit** der Nullstelle r.

(2) Sei $f=\sum_{i=0}^n a_iX^i\in R[X]$. Dann heißt

$$f':=\sum_{i=1}^n ia_iX^{i-1}\in R[X]$$

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, $f = X^n - 1 \in K[X]$ $(n \geq 1)$. 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.

Satz 4.2.7. *Sei K ein Körper, $f \in K[X]$ ein Polynom mit $\deg(f) \geq 1$.*

(1) Gilt $\mathrm{char}(K) = 0$, so folgt $\deg(f') = \deg(f) - 1$.

(2) Gilt $\mathrm{char}(K) = p > 0$, so folgt $\deg(f') \leq \deg(f) - 1$.

(3) Gilt $\mathrm{char}(K) = p > 0$, so gilt $f' = 0$ genau dann, wenn $f = \sum_{j=0}^{n} \alpha_j X^{jp}$ für $\alpha_0, \ldots, \alpha_n \in K$.

Beweis.

(1),(2) Sei $f = \sum_{i=0}^{m} a_i X^i$, $a_m \neq 0$. Wegen $f' = \sum_{i=1}^{m} i a_i X^{i-1}$ folgt $\deg(f) \leq m-1$ und $\deg(f') = m-1$ falls $\mathrm{char}(K) = 0$.

(3) Es gelte $f' = 0$, wobei $f = \sum_{i=0}^{m} a_i X^i$, $a_m \neq 0$. Dann folgt $i a_i = 0$ für $i \geq 1$, d.h. $p | i$ für $a_i \neq 0$. Wir erhalten

$$f = \sum_{i=0}^{m} a_i X^i = \sum_{i=1, a_i \neq 0}^{m} a_i X^i + a_0 X^{0p} = \sum_{i=1, a_i \neq 0} a_i X^{\frac{p}{i} p} + a_0 X^{0p}$$

Ist umgekehrt $f = \sum_{j=0}^{n} \alpha_j X^{jp}$, so folgt $f' = \sum_{j=1}^{n} pj \alpha_j X^{pj-1} = 0$.

□

4.3 Unzerlegbare Polynome

Wir haben bereits gesehen, dass für einen Körper K der Polynomring $K[X]$ ein eukldischer Ring und damit insbesondere faktoriell ist. Ziel dieses Abschnitts ist es ein allgemeineres Resultat zu beweisen: Wir werden einsehen, dass für einen faktoriellen Ring R mit Unbestimmten $X_1, \ldots, X_n$ der Polynomring $R[X_1, \ldots, X_n]$ auch faktoriell ist.

Im Folgenden sei R ein faktorieller Ring. Definitionsgemäß ist R ein Integritätsbereich und der Quotientenkörper $K := Q(R)$ enthält den Ring nach Identifikation von R mit $\operatorname{im} \iota_{R\setminus\{0\}} \cong R$.
Im Folgenden werden wir den Begriff der Assoziiertheit in Integritätsbereichen (siehe Abschnitt 3.5) in natürlicher Weise auf Quotientenkörper erweitern.

Definition. Sind $\alpha, \beta \in K$ so schreiben wir $\alpha \sim \beta$, falls ein $u \in R^\times$ mit $\beta = u\alpha$ existiert. In diesem Fall nennen wir α und β **assoziiert**.

Bemerkung. (1) $\sim$ definiert eine Äquivalenzrelation auf K.

(2) Sind $a, b \in R$. So sind a, b assoziiert aufgefasst als Elemente in K genau dann, wenn a und b assoziiert im Integritätsbereich R sind.

Beispiele. (1) Es sei $R := \mathbb{Z}$ mit $K = \mathbb{Q}$. Wegen $R^\times = \{1, -1\}$ sind zwei Elemente $\alpha, \beta \in \mathbb{Q}$ genau dann assoziiert, wenn $\alpha = \pm\beta$ gilt.

(2) Sei K ein Körper, X eine Unbestimmte über K. Wir betrachten $R := K[X]$. Wegen $R^\times = K\setminus\{0\}$ sind zwei Elemente f, g des Quotientenkörpers $K(X) := Q(K[X])$ von R genau dann assoziiert, wenn es ein $\alpha \in K\setminus\{0\}$ mit $f = \alpha g$ gibt.

Wir fixieren ein vollständiges Repräsentantensystem $\mathcal{P} \subseteq R$ der Assoziiertenklassen irreduzibler Elemente von R. Dann existiert zu jedem $r \in R\setminus\{0\}$ eine eindeutig bestimmte Folge $(m_p(r))_{p\in\mathcal{P}}$, $m_p(r) \in \mathbb{N}_0$[2] für alle $p \in \mathcal{P}$ mit

$$r \sim \prod_{p\in\mathcal{P}} p^{m_p(r)}.$$

Ist nun K der Quotientenkörper von R und $\alpha = \frac{r}{s} \in K\setminus\{0\}$, so folgt

$$\alpha \sim \prod_{p\in\mathcal{P}} p^{m_p(r)-m_p(s)}.$$

Für $p \in \mathcal{P}$ setzen wir $\nu_p(\alpha) := m_p(r) - m_p(s) \in \mathbb{Z}$ und bemerken, dass $\nu_p(\alpha)$ unabhängig von der Wahl der Darstellung von α ist. Dies liefert eine wohldefinierte Abbildung

$$\nu_p : K\setminus\{0\} \longrightarrow \mathbb{Z}, \alpha \mapsto \nu_p(\alpha)$$

mit

$$\alpha \sim \prod_{p\in\mathcal{P}} p^{\nu_p(\alpha)}$$

für alle $\alpha \in K\setminus\{0\}$.

[2] Hierbei sind alle bis auf endlich viele der $m_p(r)$ gleich Null.

Bemerkung. Seien $\alpha, \beta \in K \setminus \{0\}$. Es gilt

$$\alpha \sim \beta \Leftrightarrow \nu_p(\alpha) = \nu_p(\beta) \quad \forall\, p \in \mathcal{P}.$$

Definition. Sei $f \in K[X] \setminus \{0\}$ ein Polynom. Dann gibt es $\alpha_0, \ldots, \alpha_n \in K$ mit $f = \sum_{i=0}^{n} \alpha_i X^i$. Wir definieren den **Inhalt** $c(f)$ von f durch

$$c(f) := \prod_{p \in \mathcal{P}} p^{\nu_p(f)} \in K \setminus \{0\},$$

wobei $\nu_p(f) := \min\{\nu_p(r_i) \mid \alpha_i \neq 0\}$ für jedes $p \in \mathcal{P}$ gilt.

Bemerkungen. (1) Für $\alpha \in K \setminus \{0\}$ gilt $c(\alpha) = \prod_{p \in \mathcal{P}} p^{\nu_p(\alpha)} \sim \alpha$.

(2) Nach Konstruktion (vgl. mit dem Beweis von Lemma 3.5.4) ist für $f = \sum_{i=0}^{n} r_i X^i \in R[X] \setminus \{0\}$ der Inhalt $c(f)$ ein größter gemeinsamer Teiler der Koeffizienten, d.h. $c(f) \in \mathrm{ggT}(r_0, \ldots, r_n)$.

(3) Sei $f \in K[X] \setminus \{0\}$. Es gilt $c(f) \in R$ genau dann, wenn $f \in R[X]$.

(4) Für $f \in K[X] \setminus \{0\}$ und $\alpha \in K \setminus \{0\}$ zeigt direktes Nachrechnen $c(\alpha f) = c(\alpha)c(f) \sim \alpha c(f)$.

Beispiel. Sei $R := \mathbb{Z}$, $K := \mathbb{Q}$ sowie

$$f := 42X^2 + 28X + 6.$$

Wir wählen für $\mathcal{P}$ die Menge der (positiven) Primzahlen $\mathbb{P}$. Wegen $42 = 2 \cdot 3 \cdot 7$, $28 = 2^2 \cdot 7$ und $6 = 2 \cdot 3$ gilt $\nu_p(f) = 0$ für $p \neq 2, 3, 7$. Ferner gilt $\nu_7(f) = 0 = \nu_3(f)$ sowie $\nu_2(f) = 1$. Damit erhalten wir $c(f) = 2$. Weiter gilt $c(-\frac{3}{2} f) = 3 = c(-\frac{3}{2}) c(f)$, aber $c(-\frac{3}{2} f) = 3 \neq -\frac{3}{2} c(f)$.

Lemma 4.3.1. *Sei R ein faktorieller Ring mit Quotientenkörper K sowie $f \in K[X] \setminus \{0\}$ ein Polynom.*

(1) Es existieren $r, s \in R \setminus \{0\}$ und $f_0 \in R[X] \setminus \{0\}$ mit
   (a) $f = \frac{r}{s} f_0$,
   (b) $c(f_0) = 1$, und
   (c) $\mathrm{ggT}(r, s) = R^\times$.

(2) Die Elemente $r, s \in R$ und $f_0 \in R[X]$ sind bis auf Multiplikation mit Elementen aus $R^\times$ eindeutig bestimmt.

(3) Ist $f \in R[X]$, so gilt $s \sim 1$ und $r \sim c(f)$.

Beweis.

(1) Wir schreiben

$$f = \sum_{i=0}^{n} \frac{a_i}{b_i} X^i$$

mit $a_i, b_i \in R$, $b_i \neq 0$ für $1 \leq i \leq n$. Es ist $b := \prod_{i=1}^{n} b_i \neq 0$. Damit folgt $bf \in R[X]$ und $d := c(bf) \in R \setminus \{0\}$ ist ein größter gemeinsamer Teiler der Koeffizienten von bf. Wir setzen

$$f_0 := \frac{1}{d}(bf) \in R[X],$$

und erhalten $c(f_0) = c(\frac{1}{d})c(bf) \sim \frac{d}{d} = 1$. Mit $f_0 \in R[X]$ und der Definitions des Inhalts folgt bereits $c(f_0) = 1$.

Es sei nun t ein größter gemeinsamer Teiler von b und d. Wir setzen $s := \frac{b}{t}$ und $r := \frac{d}{t}$. Anwendung von Lemma 3.5.4 ergibt $\mathrm{ggT}(r, s) = R^\times$. Weiter gilt $f = \frac{d}{b} f_0 = \frac{r}{s} f_0$.

(2) Angenommen, $r', s' \in R$ und $f_0' \in R[X]$ erfüllen (a), (b) und (c). Dann gilt $rs' f_0 = r' s f_0'$ und wir erhalten

$$rs' = rs' c(f_0) \sim c(rs' f_0) = c(r' s f_0') \sim r' s c(f_0) = r' s.$$

Da $\mathrm{ggT}(r, s) = R^\times = \mathrm{ggT}(r', s')$ gilt, folgt $r \sim r'$ und $s \sim s'$. Insbesondere existieren Einheiten $u, v \in R$ mit $r = ur'$, $s = vs'$. Wir erhalten

$$f_0 = \frac{s}{r} f = \frac{vs'}{ur'} f = \frac{v}{u} f_0' = vu^{-1} f_0'$$

mit $vu^{-1} \in R$ Einheit.

(3) Sei $f \in R[X]$. Es gilt $\frac{r}{s} = \frac{r}{s} c(f_0) \sim c(\frac{r}{s} f_0) = c(f) \in R$ und $\mathrm{ggT}(r, s) = R^\times$ liefert $s \sim 1$. Wir erhalten damit $r \sim sc(f) \sim c(f)$.

□

Lemma 4.3.2. *Sei R ein faktorieller Ring mit Quotientenkörper K. Dann gilt*

$$c(fg) = c(f)c(g) \quad \forall\, f, g \in K[X] \setminus \{0\}.$$

Beweis. Wir wenden Lemma 4.3.1 an und schreiben

$$f = \frac{r}{s} f_0 \;\; g = \frac{r'}{s'} g_0$$

mit $\mathrm{ggT}(r, s) = R^\times = \mathrm{ggT}(r', s')$ sowie $c(f_0) = 1 = c(g_0)$. Angenommen, $c(f_0 g_0) \neq 1$. Dann existiert ein $p \in \mathcal{P}$ derart, dass p jeden Koeffizienten von $f_0 g_0 \in R[X]$ teilt. Da R faktoriell ist, ist $\mathfrak{p} := (p)$ ein Primideal von R. Wir betrachten die kanonische Projektion $\pi : R \longrightarrow R/\mathfrak{p}$ sowie den nach Satz 4.1.2 eindeutig bestimmten Homomorphismus

$$\pi^* : R[X] \longrightarrow (R/\mathfrak{p})[X]^3 \;\; ; \;\; \pi^*(\sum_{i=0}^{n} r_i X^i) = \sum_{i=0}^{n} \pi(r_i) X^i$$

[3] Eigentlich müssten wir eine Unbestimmte Y über $R/\mathfrak{p}$ wählen.

mit $\pi^*|_R = \pi$ und $\pi^*|_R(X) = X$. Dann gilt

$$0 = \pi^*(f_0 g_0) = \pi^*(f_0)\pi^*(g_0).$$

Nach Lemma 3.3.1 ist $R/\mathfrak{p}$ ein Integritätsbereich und Lemma 4.2.5 zeigt, dass $(R/\mathfrak{p})[X]$ ebenfalls ein Integritätsbereich. Damit folgt $\pi^*(f_0) = 0$ oder $\pi^*(g_0) = 0$ und somit $p|c(f_0)$ oder $p|c(g_0)$, im Widerspruch zur Definition von f_0 oder g_0. Damit erhalten wir $c(f_0 g_0) = 1$.
Insgesamt folgt

$$c(fg) = c(\frac{r}{s}\frac{r'}{s'} f_0 g_0) = c(\frac{r}{s}\frac{r'}{s'}) c(f_0 g_0) = c(\frac{r}{s}\frac{r'}{s'}) = c(\frac{r}{s}) c(f_0) c(\frac{r'}{s'}) c(g_0) = c(f)c(g).$$

□

Bemerkung. Seien $f, g \in K[X] \setminus \{0\}$ mit $fg \in R[X]$. Dann gilt

$$c(f)c(g) = c(fg) \in R.$$

Satz 4.3.3. *Sei R ein faktorieller Ring mit Quotientenkörper K. Dann gilt:*

(1) $R[X]$ ist faktoriell.

(2) Sei $f \in R[X] \setminus \{0\}$ ein Polynom. Dann sind folgende Aussagen äquivalent:

(a) $f \in R[X]$ ist irreduzibel.

(b) $\deg(f) = 0$ und $f \in R$ ist irreduzibel, oder f ist als Element in $K[X]$ irreduzibel mit $c(f) = 1$.

Beweis.

(1) Sei $f \in R[X] \setminus \{0\}$, $f \notin R[X]^\times$. Wir gehen schrittweise vor.

(i) f ist ein Produkt von Elementen aus $R[X]$, die (b) erfüllen.
`Beweis.` Sei $\deg(f) = 0$. Dann gilt $f \in R$ und f ist ein Produkt irreduzibler Elemente von R, denn R ist faktoriell.

Sei nun $\deg(f) > 0$. Dann gilt $f \notin K \setminus \{0\} = K[X]^\times$ und da $K[X]$ als Hauptidealring faktoriell ist, gibt es irreduzible Elemente $g_1, \ldots, g_n \in K[X]$ mit

$$f = g_1 \cdots g_n.$$

Lemma 4.3.1 liefert $\alpha_i \in K \setminus \{0\}$ und $h_i \in R[X] \setminus \{0\}$ mit

$$g_i = \alpha_i h_i \ , \ c(h_i) = 1 \quad 1 \le i \le n.$$

Wir erhalten

$$f = \alpha h_1 \cdots h_n \ \text{ mit } \ \alpha := \alpha_1 \cdots \alpha_n \in K^\times$$

und somit liefert Lemma 4.3.2 $\alpha \sim c(\alpha) = c(f) \in R$. Mithin ist $\alpha \in R \setminus \{0\}$. Ist α keine Einheit in R, so zerlegen wir α im faktoriellen Ring R in irreduzible Faktoren $\alpha = p_1 \cdots p_l$ und erhalten so die gewünschte Darstellung.

$$f = p_1 \cdots p_l h_1 \cdots h_n.$$

Sei daher nun $\alpha \in R^\times$. Dann gilt $c(\alpha) \sim 1$ und die Definition des Inhalts impliziert $c(\alpha) = 1$. Somit ist

$$f = (\alpha h_1)h_2 \cdots h_n$$

eine gewünschte Darstellung, da $c(\alpha h_1) = 1$ gilt und $\alpha h_1 \in R[X]$ irreduzibel in $K[X]$ ist. ◇

(ii) Sei $p \in R$ irreduzibel. Dann ist p ein Primelement von $R[X]$.
`Beweis.` Da R faktoriell ist, ist $\mathfrak{p} := (p)$ ein Primideal in R. Wir betrachten die kanonische Projektion $\pi : R \longrightarrow R/\mathfrak{p}$ sowie den induzierten Homomorphismus $\pi^* : R[X] \longrightarrow (R/\mathfrak{p})[X]$. 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 $\ker \pi^* = R[X]p$ das von p in $R[X]$ erzeugte Ideal. Also induziert π^* einen Isomorphismus $R[X]/R[X]p \xrightarrow{\sim} (R/\mathfrak{p})[X]$. Da $R/\mathfrak{p}$ ein Integritätsbereich ist, gilt dies nach Satz 4.2.1 auch für $(R/\mathfrak{p})[X]$. Damit ist $R[X]p$ ein Primideal und p in $R[X]$ ein Primelement. ◇

(iii) Sei $f \in R[X]$ derart, dass $c(f) = 1$ gilt und f in $K[X]$ irreduzibel ist. Dann ist f prim in $R[X]$.
`Beweis.` Seien $g, h \in R[X]$ mit $f | gh$. Da $K[X]$ als euklidischer Ring faktoriell ist, und damit f bereits prim in $K[X]$ ist, können wir $f | g$ annehmen. Es gibt also $\lambda \in K[X]$ mit $g = \lambda f$. Wir schreiben $\lambda = \frac{r}{s}\lambda_0$ mit $\lambda_0 \in R[X]$, $c(\lambda_0) = 1$ und $\mathrm{ggT}(r, s) = R^\times$. Nach Lemma 4.3.2 gilt dann

$$g = \frac{r}{s}(\lambda_0 f) \text{ mit } c(\lambda_0 f) = c(\lambda_0)c(f) = 1 \text{ und } \lambda_0 f \in R[X].$$

Damit liefert Lemma 4.3.1(3) $s \sim 1$ und es folgt $\lambda = r\lambda_0 \in R[X]$. Damit gilt auch $f | g$ in $R[X]$ und f ist ein Primelement von $R[X]$. ◇

Sei nun $f \in R[X]\backslash\{0\}$, $f \notin R[X]^\times$. Nach (i), (ii) und (iii) ist f ein Produkt von Primelementen von $R[X]$. Damit ist jedes irreduzible Element von $R[X]$ ein Primelement. Es verbleibt zu zeigen, dass bis auf Permutation und Assoziiertheit genau eine Zerlegung in irreduzible Elemente existiert. Da wir gezeigt haben, dass irreduzible Elemente in $R[X]$ bereits prim sind, können wir genauso wie im Beweis von Satz 3.5.2 argumentieren:
Seien also $p_1 \cdots p_n = q_1 \cdots q_m$ Zerlegungen in irreduzible Faktoren. Wir für den Beweis über Induktion nach $n + m \geq 2$. Für $n + m = 2$ ist nichts zu zeigen. Da wir nachgewiesen haben, dass jedes irreduzible Element in $R[X]$ prim ist, finden wir ein $i \in \{1, \ldots, m\}$ mit $p_1 | q_i$. Wir schreiben $q_i = ap_1$ und bemerken, dass a eine Einheit ist, da q_i irreduzibel ist. Es folgt $p_2 \cdots p_n = q_1 \cdots q_{i-1}(aq_{i+1}) \cdots q_m$ mit aq_{i+1} irreduzibel. Auf diese Gleichung können wir die Induktionsvoraussetzung anwenden. Damit ist $R[X]$ faktoriell.

(2) (a) $\Rightarrow$ (b). Gemäß (i) schreiben wir f als Produkt von Elementen aus $R[X]$, die (b) erfüllen. Wir haben in (ii) und (iii) eingesehen, dass alle Faktoren prim in $R[X]$ sind und damit insbesondere irreduzibel. Da $R[X]$ faktoriell ist, besteht das Produkt aus einem Faktor und es folgt die Behauptung. (b) $\Rightarrow$ (a). Dies folgt aus (iii).

□

Beispiel. Es sei $R = \mathbb{Z}$ mit Quotientenkörper $\mathbb{Q}$.

(1) $f = 2X^0$ ist irreduzibel in $\mathbb{Z}[X]$ aber nicht in $\mathbb{Q}[X]$.

(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.

Korollar 4.3.4. *Sei R ein faktorieller Ring und $n \in \mathbb{N}$. Dann ist der Ring $R[X_1, \ldots, X_n]$ faktoriell.*

Beweis. Die Aussage folgt induktiv unter Verwendung von Satz 4.3.3 und Korollar 4.1.3. □

Satz 4.3.5 (Kriterium von Eisenstein). *Es sei R ein faktorieller Ring mit Quotientenkörper K sowie $f = \sum_{i=0}^{n} r_i X^i \in R[X]$ ein Polynom vom Grad $n > 0$. Ist $p \in R$ irreduzibel mit $p | r_i$ für $0 \leq i \leq n-1$ und $p \nmid r_n$ sowie $p^2 \nmid r_0$. Dann ist $f \in K[X]$ irreduzibel.*

Beweis. Da $p \in R$ irreduzibel ist, ist $\mathfrak{p} := (p)$ ein Primideal von R. Damit ist $R/\mathfrak{p}$ ein Integritätsbereich und besitzt einen Quotientenkörper L. Wir betrachten die kanonische Projektion $\pi : R \longrightarrow R/\mathfrak{p}$ sowie den induzierten Homomorphismus $\pi^* : R[X] \longrightarrow (R/\mathfrak{p})[X] \subseteq L[X]$. Nach Voraussetzung gilt

$$\pi^*(f) = \sum_{i=0}^{n} \pi(r_i) X^i = \pi(r_n) X^n.$$

Angenommen, f ist nicht irreduzibel in $K[X]$. Da K ein Körper ist, gibt es Polynome $\bar{g}, \bar{h} \in K[X]$ mit $0 < \deg(\bar{g}), \deg(\bar{h}) < n$ und

$$f = gh.$$

Insbesondere gilt $n \geq 2$. Gemäß Lemma 4.3.1 schreiben wir $\bar{g} = \frac{r}{s}\bar{g}_0$, $\bar{h} = \frac{r'}{s'}\bar{h}_0$. Weiter seien $x, y \in R \setminus \{0\}$ mit $\mathrm{ggT}(x, y) = R^\times$ und $\frac{rr'}{ss'} = \frac{x}{y}$. Wir erhalten

$$f = \frac{x}{y}(\bar{g}_0 \bar{h}_0)$$

und schließen mit Lemma 4.3.2 und Lemmma 4.3.3, dass $\frac{x}{y} \in R$. Damit existiert eine Zerlegung $f = gh$ mit $g, h \in R[X]$ und $0 < \deg(g), \deg(h) < n$. Wir erhalten

$$\pi(r_n) X^n = \pi^*(f) = \pi^*(gh) = \pi^*(g)\pi^*(h).$$

Mit $n = \deg(\pi(r_n)X^n) = \deg(\pi^*(g)) + \deg(\pi^*(g))$ und $n = \deg(g) + \deg(h)$ folgt weiter $0 < \deg(g) = \deg(\pi^*(g))$ und $0 < \deg(h) = \deg(\pi^*(h))$. Insbesondere sind $\pi^*(g), \pi^*(h)$ keine Einheiten in $L[X]$. Es ist $L[X]$ als euklidischer Ring faktoriell. Da $X \in L[X]$ irreduzibel und $0 \neq \pi(r_n) \in R/\mathfrak{p} \setminus \{0\} \subseteq L^\times = L[X]^\times$ eine Einheit ist, folgt damit aus der Eindeutigkeit der Primfaktorzerlegung, dass

X ein Teiler von $\pi^*(g)$ und $\pi^*(h)$ ist. Das heißt die konstanten Terme von $\pi^*(g)$ und $\pi^*(h)$ sind $0_L = 0_{R/\mathfrak{p}}$. Der konstante Term von $\pi^*(g)$ ist $g(0) + \mathfrak{p}$. Das heißt $g(0) \in \mathfrak{p} = (p)$ und damit $p \mid g(0)$. Analog folgt $p \mid h(0)$ und insgesamt $p^2 \mid g(0)h(0) = f(0)$. Also teilt p^2 den konstanten Term von f, ein Widerspruch zur Annahme. □

Beispiel. (1) Es sei $f := X^3+3X^2+15$. Dann ist $f \in \mathbb{Q}[X]$ irreduzibel nach dem Kriterium von Eisenstein für $p = 3 \in \mathbb{Z}$. Wir wählen $\mathcal{P} = \mathbb{P}$. Wegen $c(f) = 1$ ist f auch irreduzibel in $\mathbb{Z}[X]$ aufgrund von Satz 4.3.3.

(2) Da Polynom X^2+1 ist irreduzibel in $\mathbb{Q}[X]$. 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 $x^{-1} \in K \ \forall\, x \in K \setminus \{0\}$ 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 vermöge

$$r.v := rv \quad \forall\, r \in K, v \in L$$

die Struktur eines K-Vektorraums. Man sieht sofort, dass $\dim_{\mathbb{R}} \mathbb{C} = 2$.

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.

Sei K ein Körper, $(K_i)_{i \in I}$ eine Familie von Teilkörpern von K. Dann ist $\bigcap_{i \in I} K_i$ ein Teilkörper. Damit ist folgende Definition sinnvoll:

Definition. Sei L ein Körper, $K \subseteq L$ ein Teilkörper, $S \subseteq L$ eine Teilmenge. Dann bezeichnet $K(S)$ den kleinsten Teilkörper von L, der $K \cup S$ enthält. Ferner bezeichnet $K[S]$ 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 $Q(K[S]) = (K[S] \setminus \{0\})^{-1} K[S]$. 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 3.4.3 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 Korollar 3.2.2 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, 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 $KK' := K(K') = K'(K)$ heißt das **Kompositum** von K und K' in L.

(3) 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 3.2.5 $\ker \varphi = (\operatorname{char}(L))$ 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 3.2.4 ein Körper. Also ist $\operatorname{im} \varphi \cong \mathbb{Z}/(p)$ ein Teilkörper von $P(L)$ und wir erhalten $\operatorname{im} \varphi = P(L)$.

(2) Gilt $\operatorname{char}(L) = 0$, so liefert Korollar 3.4.4 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, $a \in L$. Dann 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. Damit ist die Quadratur des Kreises unmöglich.

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 $f(a) = 0$,

(b) 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, $[K(a):K] = \deg(\mu_a)$ und es gilt $K[a] = K(a)$.*

Beweis. Wir betrachten den Homomorphismus $\mathrm{ev}_a : K[X] \longrightarrow K(a) \; ; \; f \mapsto f(a)$. Dann gilt $\mathrm{im}\,\mathrm{ev}_a = K[a]$. Da $K[X]$ 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 $g \in K[X]$ 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 3.5.1, 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 $\mathbb{Q}$. Damit folgt $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] \leq 2$. Es gilt nach Lemma 5.2.2 $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$ genau dann, wenn f_d irreduzibel ist. Dies ist genau dann der Fall, 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) Es sei K ein Körper sowie $K(X)$ der Quotientenkörper des Polynomrings $K[X]$. Dann ist $K(X):K$ keine algebraische Körpererweiterung.

(3) Die Erweiterung $\mathbb{R}:\mathbb{Q}$ ist nicht algebraisch. (Übung)

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

$$\hat{L} := \{x \in L \mid x \text{ ist algebraisch über } K\}$$

ein Zwischenkörper von $L:K$.

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.

□

Definition. Sei $L:K$ eine Körpererweiterung. Der Zwischenkörper $\hat{L}$ heißt **algebraischer Abschluss von K in L.**

Unser nächstes Ziel ist, jedem Körper K einen Körper $\bar{K} \supseteq K$ zuzuordnen, der folgende Eigenschaften hat:

(a) Die Erweiterung $\bar{K} : K$ ist algebraisch, und

(b) Jedes Polynom $f \in \bar{K}[X] \setminus \bar{K}$ hat in $\bar{K}$ eine Nullstelle.

Definition. Ein Körper K heißt **algebraisch abgeschlossen**, falls jedes Polynom $f \in K[X] \setminus K$ eine Nullstelle in K besitzt.

Satz 5.3.2. *Sei K ein Körper. Dann sind folgende Aussagen äquivalent:*

(1) K ist algebraisch abgeschlossen.

(2) Jedes Polynom $f \in K[X] \setminus K$ ist ein Produkt von Polynomen vom Grad 1.

(3) $f \in K[X]$ ist normiert und irreduzibel genau dann, wenn $f = X - a$ für ein $a \in K$ gilt.

(4) Ist $L : K$ eine algebraische Körpererweiterung, so gilt $L = K$.

Beweis. (1) $\Rightarrow$ (2). Wir verwenden Induktion nach $\deg(f)$, wobei der Fall $\deg(f) = 1$ trivial ist. Sei also $\deg(f) \geq 2$. Da K algebraisch abgeschlossen ist, gibt es eine Nullstelle $a \in K$ von f. Da $K[X]$ ein euklidischer Ring ist, finden wir eine Darstellung $f = q(X - a) + r$, wobei $\deg(r) < 1$ gilt. Damit ist r konstant und es folgt $r = r(a) = f(a) = 0$. Die Induktionsannahme sichert nun, dass q ein Produkt von Polynomen vom Grad 1 ist. Dies gilt damit auch für f.
(2) $\Rightarrow$ (3). Dies folgt unmittelbar.
(3) $\Rightarrow$ (4). Sei $L : K$ algebraisch sowie $a \in L$. Aufgrund von Lemma 5.2.2 ist $\mu_a \in K[X]$ ein normiertes, irreduzibles Polynom. Wegen (3) gibt es $b \in K$ mit $\mu_a = X - b$. Also folgt, $0 = \mu_a(a) = a - b$ und daher $a \in K$.
(4) $\Rightarrow$ (1). Da $K[X]$ faktoriell ist, genügt es zu zeigen, dass jedes irreduzible Polynom $f \in K[X]$ in K eine Nullstelle besitzt. 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 3.5.1 ein Körper. Wir betrachten den injektiven Homomorphismus

$$\pi : K \longrightarrow L \ ; \ \alpha \mapsto \alpha + (f).$$

Es ist $K' := \operatorname{im} \pi \cong K$ ein Unterkörper von L. Sei $n := \deg(f)$. Division mit Rest liefert

$$L = \langle \{1, X + (f), X^2 + (f), \ldots, X^{n-1} + (f)\} \rangle_{K'}.$$

Also ist $L : K'$ eine endliche Körpererweiterung und damit insbesondere algebraisch. Nach (4) gilt daher $K' = L$ und π ist ein Isomorphismus.[1] Damit gibt es $\alpha \in K$ mit $X + (f) = \alpha + (f)$, was $X - \alpha \in (f)$ nach sich zieht. Also gilt $f(\alpha) = 0$, da $X - \alpha$ algebraisch ist. □

Bemerkungen. (1) Eine leichte Abänderung des Beweises von (4) $\Rightarrow$ (1) zeigt: Ist K ein Körper und $f \in K[X]$ ein irreduzibles Polynom, so existiert ein Körper $K \subseteq L$ in dem f eine Nullstelle besitzt mit $[L : K] = \deg(f)$. Ein solcher Körper wird durch $L := K[X]/(f)$ gegeben indem wir K vermöge der Einbettung

$$\pi : K \longrightarrow K[X]/(f), \alpha \mapsto \alpha + (f)$$

[1] Hier muss man sich noch überlegen, dass K' die Eigenschaft (4) von K erbt.

als Unterkörper von $K[X]/(f)$ auffassen. 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

$$\bar{f}(\alpha) = \sum_{i=0}^{n} \pi(a_i)\alpha^i = \sum_{i=0}^{n} a_i X^i + (f) = f + (f) = 0_L.$$

Diese Konstruktion wird auch **Kronecker Konstruktion** genannt.

(2) 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 $+, \cdot\colon A \times A \longrightarrow A$ vermöge

$$a+b := \varphi^{-1}(\varphi(a)+\varphi(b)) \text{ und } a \cdot b := \varphi^{-1}(\varphi(a)\varphi(b)).$$

Auf diese Weise erhält $(A, +, \cdot)$ die Struktur eines Körpers.[2] 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. Sei $L\colon K$ eine Körpererweiterung und $f \in K[X]$. Es bezeichnet

$$Z_L(f) := \{a \in L \mid f(a) = 0\}$$

die Menge der Nullstellen von f in L.

Definition. Sei K ein Körper. Ein Körper $\bar{K} \supseteq K$ heißt **algebraischer Abschluss** von K, falls gilt

(a) $\bar{K}$ ist algebraisch abgeschlossen, und

(b) die Erweiterung $\bar{K}\colon K$ ist algebraisch.

Satz 5.3.3 (Beweis nach H. Bender). *Sei K ein Körper. Dann existiert ein algebraischer Abschluss $\bar{K}$ von K.*

Beweis. Zunächst beweisen wir einige Hilfsbehauptungen.

(i) Sei $L\colon K$ eine algebraische Körpererweiterung. Dann gilt $L = \bigsqcup_{f \in \mathcal{P}} Z_L(f)$, wobei $\mathcal{P} \subseteq K[X]$ die Menge der normierten, irreduziblen Polynome von $K[X]$ bezeichne.
`Beweis.` Wird in den Übungen gezeigt. ◇

[2] Diese allgemeine Konstruktion wird auch Strukturtransport genannt.

(ii) Die Mengen $\mathfrak{M}_f := \{f\} \times \mathbb{N}_0$, $f \in \mathcal{P}$ erfüllen $\mathfrak{M} := \mathcal{P} \times \mathbb{N}_0 = \bigsqcup_{f\in\mathcal{P}} \mathfrak{M}_f$.
`Beweis.` Dies folgt unmittelbar aus der Definition der Mengen. ◇

(iii) Sei $K \subseteq L \subseteq H$ algebraische Körpererweiterungen mit

(1) $L \subseteq \mathfrak{M}$, und

(2) $Z_L(f) \subseteq \mathfrak{M}_f$ für alle $f \in \mathcal{P}$.

So existiert ein Körper H' mit $L \subseteq H' \subseteq \mathfrak{M}$ derart, dass $Z_{H'}(f) \subseteq \mathfrak{M}_f \ \forall\, f \in \mathcal{P}$ gilt, und ein Homomorphismus $\varphi : H \longrightarrow H'$ mit $\varphi|_L = \mathrm{id}_L$. Die Erweiterung $H' : L$ ist algebraisch.
`Beweis.` Sei $f \in \mathcal{P}$. Wegen $Z_L(f) \subseteq Z_H(f)$, $Z_L(f) \subseteq \mathfrak{M}_f$ und $|Z_H(f)| \leq \deg(f)$ gibt es eine injektive Abbildung $\varphi_f : Z_H(f) \longrightarrow \mathfrak{M}_f$ mit $\varphi_f|_{Z_L(f)} = \mathrm{id}_{Z_L(f)}$. Nach (i) ist $\{Z_H(f) \mid f \in \mathcal{P}\}$ eine Partition von H. Also wird durch

$$\varphi : H \longrightarrow \mathfrak{M} \ ; \ \varphi|_{Z_H(f)} = \varphi_f \quad \forall\, f \in \mathcal{P}$$

eine injektive Abbildung mit $\varphi|_L = \mathrm{id}_L$ definiert.

Wir betrachten nun $H' := \varphi(H)$. Dann erhält H' vermöge

$$a+b := \varphi(\varphi^{-1}(a)+\varphi^{-1}(b)) \ \text{ und } \ ab := \varphi(\varphi^{-1}(a)\varphi^{-1}(b)).$$

die Struktur eines Körpers und $\varphi : H \longrightarrow H'$ ist ein Isomorphismus[3] mit $\varphi|_L = \mathrm{id}_L$. Insbesondere gilt also $L \subseteq H'$.

Sei nun $f \in \mathcal{P}$ und $a \in Z_{H'}(f)$. Dann gilt wegen $\varphi|_L = \mathrm{id}_L$ für $b := \varphi^{-1}(a) \in H$

$$0 = \varphi^{-1}(f(a)) = f(b)$$

und somit $b \in Z_H(f)$. Also folgt $a = \varphi(b) = \varphi_f(b) \in \mathfrak{M}_f$. Ebenso zeigt man: $H' : L$ ist algebraisch. ◇

Damit haben wir alle benötigten Hilfsaussagen beweisen. Im Folgenden fassen wir K durch die Identifikation

$$K \cong \{(X-a, 1) \ ; \ a \in K\} \subseteq \mathfrak{M}$$

als Teilmenge von $\mathfrak{M}$ auf. Sei nun

$$\mathsf{A} := \{K \subseteq L \subseteq \mathfrak{M} \ ; \ L : K \text{ ist algebraische Körpererweiterung mit } Z_L(f) \subseteq \mathfrak{M}_f \ \forall\, f \in \mathcal{P}\}.$$

Wir definieren durch

$$L \leq L' \ :\Leftrightarrow \ L \subseteq L' \text{ und } L \text{ ist ein Teilkörper von } L'$$

eine partielle Ordnung auf A. Im Folgenden zeigen wir, dass die Voraussetzungen von Zorns Lemma erfüllt sind.

Sei $\mathsf{B} \subseteq \mathsf{A}$ eine total geordnete Teilmenge, $\mathsf{B} \neq \varnothing$. Wir betrachten

$$L_{\mathsf{B}} := \bigcup_{L\in\mathsf{B}} L.$$

[3] Hier verwenden wir erneut Strukturtransport

Dann gilt $L_{\mathsf{B}} \subseteq \mathfrak{M}$ sowie $Z_{L_{\mathsf{B}}}(f) \subseteq \mathfrak{M}_f$ für jedes $f \in \mathcal{P}$. Für $x, y \in L_{\mathsf{B}}$ gibt es $L, L' \in \mathsf{B}$ mit $x \in L$ und $y \in L'$. Da B total geordnet ist, dürfen wir $L' \leq L$ annehmen. Wir setzen

$$x+y := x+_L y \text{ und } xy := x \cdot_L y.$$

Ist $\hat{L}$ ein weiterer Körper mit $x, y \in \hat{L}$, so folgt $\hat{L} \subseteq L$ oder $L \subseteq \hat{L}$. In beiden Fällen erhalten wir

$$x+_L y = x+_{\hat{L}} y \text{ und } x \cdot_L y = x \cdot_{\hat{L}} y.$$

Obige Definition hängt also nicht von der Wahl von L ab. Nun zeigt direktes Nachrechnen, dass

$$(L_{\mathsf{B}}, +, \cdot)$$

ein Körper ist. Sei $a \in L_{\mathsf{B}}$. Dann gibt es $L \in \mathsf{B}$ mit $a \in L$. Damit ist a algebraisch über K. Also ist die Erweiterung $L_{\mathsf{B}} : K$ algebraisch und es gilt $L \leq L_{\mathsf{B}}$ für alle $L \in \mathsf{B}$. Folglich ist $L_{\mathsf{B}} \in \mathsf{A}$ eine obere Schranke von B. Da weiter $\mathsf{A} \neq \varnothing$ gilt, sind die Voraussetzungen des Zornschen Lemmas (3.3.2) erfüllt und es existiert ein maximales Element $L_0 \in \mathsf{A}$. Wir zeigen nun, dass L_0 ein algebraischer Abschluss von K ist.

Da $L_0 \in \mathsf{A}$ gilt, ist die Erweiterung $L_0 : K$ algebraisch. Sei nun $H : L_0$ eine algebraische Körpererweiterung. Dann existiert nach (iii) ein Körper H' mit $L_0 \subseteq H' \subseteq \mathfrak{M}$, $Z_{H'}(f) \subseteq \mathfrak{M}_f$ für alle $f \in \mathcal{P}$ sowie ein Isomorphismus $\varphi : H \longrightarrow H'$ mit $\varphi|_{L_0} = \mathrm{id}_{L_0}$. Zudem ist $H' : L_0$ algebraisch. Es folgt also $H' \in \mathsf{A}$ sowie $L_0 \leq H'$. Aufgrund der Maximalität von L_0 gilt daher $H' = L_0$. Wegen $\varphi|_{L_0} = \mathrm{id}_{L_0}$ erhalten wir $H = L_0$. Satz 5.3.2 zeigt nun, dass L_0 algebraisch abgeschlossen ist.

□

Bemerkungen. (1) Im Fall $K = \mathbb{R}$ ist $\bar{K} := \mathbb{C}$ dem **Fundamentalsatz der Algebra** zufolge ein algebraischer Abschluss von $\mathbb{R}$.

(2) Jetzt können wir auf einfache Weise eine Körpererweiterung angeben, die algebraisch aber nicht endlich ist. Sei K ein endlicher Körper (etwa $K = \mathbb{Z}/(2)$). Dann ist $\bar{K} : K$ eine algebraische Erweiterung. Wäre die Körpererweiterung endlich, so wäre $\bar{K}$ von endlicher Ordnung $|K|^{[\bar{K}:K]}$. Wir haben in den Übungsserien gesehen, dass dies nicht möglich nicht.

(3) Sei K ein endlicher Körper mit einem algebraischen Abschluss $\bar{K}$ und ist $x \in \bar{K}^\times$, so existiert $x \in \mathbb{N}$ mit $x^n = 1$. (Übungsaufgabe).[4]

Lemma 5.3.4. *Es sei $\sigma : K \longrightarrow K'$ ein Isomorphismus von Körpern, $\sigma^* : K[X] \longrightarrow K'[X]$ der durch $\sigma^*|_K = \sigma$ und $\sigma^*(X) = X$ gegebene Isomorphismus von Polynomringen. Ferner seien $L : K$ und $L' : K'$ algebraische Körpererweiterungen.*

(1) Seien $a \in L$ und $a' \in L'$ zwei Elemente mit $\sigma^*(\mu_a) = \mu_{a'}$. Dann existiert genau ein Isomorphismus $\varphi : K(a) \longrightarrow K'(a')$ mit $\varphi|_K = \sigma$ und $\varphi(a) = a'$.

(2) Sei $a \in L$. Dann ist $|Z_{L'}(\sigma^*(\mu_a))|$ die Anzahl der Homomorphismen $\varphi : K(a) \longrightarrow L'$ mit $\varphi|_K = \sigma$.

[4] Damit ist die Gruppe $\bar{K}^\times$ eine **Torsionsgruppe**.

Beweis.

(1) Wir betrachten den Homomorphismus $\varepsilon : K[X] \longrightarrow K[a] = K(a)\ ;\ \varepsilon(f) = f(a)$. Dann gilt $\ker \varepsilon = (\mu_a)$ und

$$\bar{\varepsilon} : K[X]/(\mu_a) \longrightarrow K(a) \subseteq L \ \ ; \ \ f+(\mu_a) \mapsto f(a)$$

ist ein Isomorphimus von Ringen. Analog erhalten wir einen Isomorphismus

$$\bar{\varepsilon'} : K'[X]/(\mu_{a'}) \longrightarrow K'(a') \subseteq L' \ \ ; \ \ f+(\mu_{a'}) \mapsto f(a).$$

Wegen $\sigma^*(\mu_a) = \mu_{a'}$ induziert σ^* einen Isomorphismus

$$\bar{\sigma}^* : K[X]/(\mu_a) \longrightarrow K'[X]/(\mu_{a'}) \ \ ; \ \ \bar{\sigma}^*(f+(\mu_a)) = \sigma^*(f)+(\mu_{a'}).$$

Wir betrachten nun

$$\varphi : K(a) \longrightarrow K'(a') \quad \varphi = \bar{\varepsilon'} \circ \bar{\sigma}^* \circ \bar{\varepsilon}^{-1}.$$

Dies liefert ein kommutatives Diagramm

$$\begin{array}{ccc} K[X]/(\mu_a) & \xrightarrow{\bar{\varepsilon}} & K(a) \\ \downarrow{\scriptstyle \bar{\sigma}^*} & & \downarrow{\scriptstyle \varphi} \\ K'[X]/(\mu_{a'}) & \xrightarrow{\bar{\varepsilon'}} & K'(a'). \end{array}$$

Dann ist φ ein Isomorphismus und für $r \in K$ erhalten wir

$$\varphi(r) = \varphi(\bar{\varepsilon}(r+(\mu_a))) = \bar{\varepsilon'}(\bar{\sigma}^*(r+(\mu_a))) = \bar{\varepsilon'}(\sigma^*(r)+(\mu_{a'})) = \bar{\varepsilon'}(\sigma(r)+(\mu_{a'})) = \sigma(r).$$

Damit folgt $\varphi|_K = \sigma$. Zudem erhalten wir

$$\varphi(a) = \varphi(\bar{\varepsilon}(X+(\mu_a))) = \bar{\varepsilon'}(X+(\mu_{a'})) = a'.$$

Ist nun $\psi : K(a) \longrightarrow K'(a')$ ein weiterer Isomorphismus mit $\psi|_K = \sigma$ und $\psi(a) = a'$, so ist

$$Q := \{x \in K(a) \ \mid \ \psi(x) = \varphi(x)\}$$

ein Teilkörper von $K(a)$ mit $K \subseteq Q$ und $a \in Q$. Also folgt $Q = K(a)$ und $\psi = \varphi$.

(2) Es sei

$$G_\sigma := \{\varphi : K(a) \longrightarrow L' \ \mid \ \varphi \text{ ist Homomorphismus mit } \varphi|_K = \sigma\}.$$

Wir behaupten, dass durch

$$\Omega : G_\sigma \longrightarrow Z_{L'}(\sigma^*(\mu_a)) \ \ ; \ \ \varphi \mapsto \varphi(a)$$

eine bijektive Abbildung definiert wird.

Sei $\varphi \in G_\sigma$. Dann gilt $\sigma^*(\mu_a)(\varphi(a)) = \varphi(\mu_a(a)) = 0$. Damit ist Ω wohldefiniert. Seien $\psi, \varphi \in G_\sigma$ mit $\Omega(\psi) = \Omega(\varphi)$. Dann gilt $K, \{a\} \subseteq Q := \{x \in K(a) \mid \varphi(x) = \psi(x)\}$. Da Q ein Teilkörper von $K(a)$ ist, folgt $Q = K(a)$ und damit $\varphi = \psi$.
Sei $a' \in Z_{L'}(\sigma^*(\mu_a))$. Dann gilt $\sigma^*(\mu_a)(a') = 0$. Da $\sigma^*(\mu_a) \in K'[X]$ normiert und irreduzibel ist, folgt also $\sigma^*(\mu_a) = \mu_{a'}$. Damit liefert (1) ein $\varphi \in G_\sigma$ mit $\Omega(\varphi) = a'$. Also ist Ω surjektiv.

Insgesamt erhalten wir nun $|G_\sigma| = |Z_{L'}(\sigma^*(\mu_a))|$.

□

Satz 5.3.5. *Sei K ein Körper.*

(1) Ist $\sigma : K \longrightarrow K'$ ein Homomorphismus in einen algebraisch abgeschlossenen Körper K' und ist $L : K$ eine algebraische Körpererweiterung, so existiert ein Homomorphismus $\varphi : L \longrightarrow K'$ mit $\varphi|_K = \sigma$.

(2) Ist $\sigma : K \longrightarrow K'$ ein Isomorphismus und sind $\bar{K}, \bar{K}'$ algebraische Abschlüsse von K und K', so existiert ein Isomorphismus $\varphi : \bar{K} \longrightarrow \bar{K}'$ mit $\varphi|_K = \sigma$.

(3) Sind K_1 und K_2 algebraische Abschlüsse von K, so existiert ein Isomorphismus $\varphi : K_1 \longrightarrow K_2$ mit $\varphi|_K = \mathrm{id}_K$.

Beweis.

(1) Wir betrachten

$$\mathsf{A} := \{(Q, \psi) \mid K \subseteq Q \subseteq L \text{ Zwischenkörper}, \ \psi : Q \longrightarrow K' \text{ Homomorphismus mit } \psi|_K = \sigma\}.$$

Wegen $(K, \sigma) \in \mathsf{A}$ ist diese Menge nicht leer. Auf A definieren wir eine partielle Ordnung $\leq$ vermöge

$$(Q, \psi) \leq (Q', \psi') \ :\Leftrightarrow \ Q \subseteq Q' \text{ und } \psi'|_Q = \psi.$$

Sei nun $\mathsf{B} \subseteq \mathsf{A}$ eine total geordnete Teilmenge. Dann ist $Q_{\mathsf{B}} := \bigcup_{(Q,\psi)\in\mathsf{B}} Q$ ein Zwischenkörper und

$$\psi_{\mathsf{B}} : Q_{\mathsf{B}} \longrightarrow K' \ ; \ \psi_{\mathsf{B}}(x) = \psi(x) \quad \text{für } (Q, \psi) \in \mathsf{B} \text{ und } x \in Q$$

ist ein Homomorphismus mit $(\psi_{\mathsf{B}})|_K = \sigma$. Also ist $(Q_{\mathsf{B}}, \psi_{\mathsf{B}}) \in \mathsf{A}$ eine obere Schranke von B. Nach Lemma 3.3.2 gibt es also ein maximales Element $(Q_0, \psi_0) \in \mathsf{A}$.

Sei nun $a \in L$. Wir betrachten $Q_0' := \psi_0(Q_0) \subseteq K'$. Dann ist $\psi_0 : Q_0 \longrightarrow Q_0'$ ein Isomorphismus. Dieser induziert einen Isomorphismus $\psi_0^* : Q_0[X] \longrightarrow Q_0'[X]$. Da K' algebraisch abgeschlossen ist, besitzt das Polynom $\psi_0^*(\mu_a) \in Q_0'[X]$ in K' eine Nullstelle a'. Damit gilt $\psi_0^*(\mu_a) = \mu_{a',Q_0'}$ und Lemma 5.3.4 liefert einen Isomorphismus $\varphi_0 : Q_0(a) \longrightarrow Q_0'(a') \subseteq K'$ mit $\varphi_0|_{Q_0} = \psi_0$ und $\varphi_0(a) = a'$. Es folgt daher $(Q_0(a), \varphi_0) \in \mathsf{A}$ sowie $(Q_0, \psi_0) \leq (Q_0(a), \varphi_0)$. Da (Q_0, ψ_0) maximal ist, erhalten wir Gleichheit und somit $Q_0 = Q_0(a)$. Also folgt $a \in Q_0$. Damit gilt also $Q_0 = L$ und $\psi_0 : L \longrightarrow K'$ ist die gewünschte Fortsetzung von σ,

(2) Nach (1) gibt es einen Homomorphismus $\varphi : \bar{K} \longrightarrow \bar{K}'$ mit $\varphi|_K = \sigma$. Also ist $\varphi(\bar{K})$ isomorph zu $\bar{K}$ und somit algebraisch abgeschlossen. Da die Erweiterung $\bar{K}' : \varphi(\bar{K})$ algebraisch ist, folgt $K' = \varphi(\bar{K})$. Damit ist φ ein Isomorphismus.

(3) Dies folgt direkt aus (2).

□

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 $\sigma : K \longrightarrow K'$ ein Körperisomorphismus, $\sigma^* : K[X] \longrightarrow K'[X]$ der zugehörige Ringisomorphismus. Sei $f \in K[X]\setminus K$. Sind L und L' Zerfällungskörper von f bzw. $\sigma^*(f)$ über K bzw. K', so gibt es einen Isomorphismus $\varphi : L \longrightarrow L'$ mit $\varphi|_K = \sigma$. Für jeden derartigen Isomorphismus gilt $\varphi(Z_L(f)) = Z_{L'}(\sigma^*(f))$.*

Beweis. Es seien $\bar{L}$ und $\bar{L}'$ algebraische Abschlüsse von L bzw. L'. Da die Erweiterungen $L : K$ und $L' : K'$ algebraisch sind, sind $\bar{L}$ und $\bar{L}'$ auch algebraische Abschlüsse von K bzw. K'. Infolge Satz 5.3.5 existiert daher ein Isomorphismus $\psi : \bar{L} \longrightarrow \bar{L}'$ mit $\psi|_K = \sigma$. Für $a \in \bar{L}$ erhalten wir $\psi(f(a)) = \sigma^*(f)(\psi(a))$. Insbesondere gilt

$$\psi(Z_L(f)) = Z_{L'}(\sigma^*(f)).$$

Da L und L' Zerfällungskörper von f bzw. $\sigma^*(f)$ sind, folgt

$$\psi(L) = \psi(K(Z_L(f)) = \psi(K)(\psi(Z_L(f)) = K'(Z_{L'}(\sigma^*(f))) = L'.$$

Damit ist $\varphi := \psi|_L$ ein gewünschter Isomorphismus. □

Definition. Sei $\mathcal{F} \subseteq K[X]\setminus K$ eine Menge von Polynomen. Ein Erweiterungskörper $L \supseteq K$ von K heißt **Zerfällungskörper** von $\mathcal{F}$ über K, falls gilt:

(a) Jedes $f \in \mathcal{F}$ zerfällt über L in Linearfaktoren, und

(b) $L = K(\bigcup_{f\in\mathcal{F}} Z_L(f))$.

Satz 5.4.2. *Sei $\mathcal{F} \subseteq K[X]\setminus K$.*

(1) Ist $\bar{K} \supseteq K$ ein algebraischer Abschluß, so gibt es genau einen Zerfällungskörper $L \subseteq \bar{K}$ von $\mathcal{F}$ über K.

(2) Sind L, L' Zerfällungskörper von $\mathcal{F}$ über K, so gibt es einen Isomorphismus $\varphi : L \longrightarrow L'$ mit $\varphi|_K = \mathrm{id}_K$.

Beweis. (1) Wir definieren $L := K(\bigcup_{f\in\mathcal{F}} Z_{\bar{K}}(f))$.
(2) Dies folgt wie in Satz 5.4.1. □

Definition. Eine Körpererweiterung $L : K$ heißt **normal**, falls es eine Menge $\mathcal{F} \subseteq K[X]\setminus K$ gibt, so dass L ein Zerfällungskörper von $\mathcal{F}$ über K ist.

Bemerkung. Sei $L : K$ eine normale Erweiterung und $L = K(\bigcup_{f\in\mathcal{F}} Z_L(f))$. Da alle Elemente in $\bigcup_{f\in\mathcal{F}} Z_L(f)$ nach Definition algebraisch über K sind, gilt $K(\bigcup_{f\in\mathcal{F}} Z_L(f)) \subseteq \hat{L}$. Das heißt $L = \hat{L}$ und die Erweiterung $L : K$ ist algebraisch.

Satz 5.4.3. *Sei K ein Körper mit algebraischem Abschluß $\bar{K}$ sowie $K \subseteq L \subseteq \bar{K}$ ein Zwischenkörper. Dann sind folgende Aussagen äquivalent:*

(1) Die Erweiterung $L:K$ ist normal.

(2) Ist $\varphi : L \longrightarrow \bar{K}$ ein Homomorphismus mit $\varphi|_K = \mathrm{id}_K$, so gilt $\varphi(L) = L$.

(3) Ist $f \in K[X]$ irreduzibel mit $Z_L(f) \neq \varnothing$, so gilt $Z_{\bar{K}}(f) \subseteq L$.

Beweis. (1) $\Rightarrow$ (2). Nach Voraussetzung gibt es eine Menge $\mathcal{F} \subseteq K[X] \setminus K$ mit

(a) $L = K(\bigcup_{f\in\mathcal{F}} Z_L(f))$, und

(b) jedes $f \in \mathcal{F}$ zerfällt über L in Linearfaktoren.

Sei $\varphi : L \longrightarrow \bar{K}$ ein Homomorphismus mit $\varphi|_K = \mathrm{id}_K$, sowie $\varphi^* : L[X] \longrightarrow \bar{K}[X]$ der induzierte Homomorphismus. Ist $f \in \mathcal{F}$, so gibt es $a_1, \ldots, a_n \in L$ und $c \in K^\times$ mit $f = c\prod_{i=1}^n (X - a_i)$. Wegen $f \in K[X]$ und $\varphi|_K = \mathrm{id}_K$ folgt

$$f = \varphi^*(f) = c\prod_{i=1}^{n}(X - \varphi(a_i)).$$

Damit erhalten wir $\varphi(Z_L(f)) = Z_L(f)$ für alle $f \in \mathcal{F}$ und es folgt

$$\varphi(L) = K(\varphi(\bigcup_{f\in\mathcal{F}} Z_L(f))) = K(\bigcup_{f\in\mathcal{F}} \varphi(Z_L(f))) = L.$$

(2) $\Rightarrow$ (3). Sei $f \in K[X]$ irreduzibel und $a \in Z_L(f)$. Damit existiert $\alpha \in K^\times$ mit $f = \alpha\mu_a$.

Ist $b \in Z_{\bar{K}}(f)$, so liefert Lemma 5.3.4(1) einen Isomorphismus $\psi : K(a) \longrightarrow K(b)$ mit $\psi|_K = \mathrm{id}_K$ und $\psi(a) = b$. Nach Satz 5.3.5 gibt es eine Fortsetzung $\varphi : L \longrightarrow \bar{K}$ von ψ. Insbesondere folgt $\varphi|_K = \mathrm{id}_K$ und (2) impliziert $b = \varphi(a) \in L$.

(3) $\Rightarrow$ (1). Es sei $\mathcal{F} := \{\mu_{a,K} \mid a \in L\}$. Dann besitzt jedes $f \in \mathcal{F}$ in L eine Nullstelle und (3) impliziert $Z_{\bar{K}}(f) \subseteq L$. Also zerfällt jedes $f \in \mathcal{F}$ über L in Linearfaktoren und $L = K(\bigcup_{f\in\mathcal{F}} Z_L(f))$. Damit ist $L:K$ eine normale Körpererweiterung. □

Bemerkung. Sei $L : K$ eine normale Erweiterung mit $L = K(b_1, \ldots, b_n)$. Weiter sei $\bar{K}$ ein algebraischer Abschluss von K der L enthält. Wir setzen $f := \prod_{i=1}^n \mu_{b_i} \in K[X]$. Da alle Faktoren μ_{b_i} von f irreduzibel sind und jeweils die Nullstelle $b_i \in L$ haben, folgt mit Satz 5.4.3 bereits, dass f über L vollständig in Linearfaktoren zerfällt. Mit $\{b_1, \ldots, b_n\} \subseteq K(Z_L(f))$ folgt $L = K(Z_L(f))$.

Korollar 5.4.4. *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). Dies folgt mit den Argumenten von Satz 5.4.3. □

Satz 5.4.5. *Sei $L:K$ eine normale Körpererweiterung.*

(1) Ist $K \subseteq Q \subseteq L$ ein Zwischenkörper, so ist die Erweiterung $L:Q$ normal.

(2) Ist $E:K$ eine Körpererweiterung mit $L, E \subseteq \bar{K}$, so ist $LE:E$ normal. □

Beweis.

(1) Sei $\mathcal{F} \subseteq K[X] \setminus K$, sodass L der Zerfällungskörper von $\mathcal{F}$ über K ist. Es gilt $\mathcal{F} \subseteq Q[X] \setminus Q$ und $\mathcal{F}$ ist Zerfällungskörper von $\mathcal{F}$ über Q.

(2) Wie in (1) schreiben wir $L = K(\bigcup_{f\in\mathcal{F}} Z_L(f))$ mit $\mathcal{F} \subseteq K[X] \setminus K$, sodass jedes $f \in \mathcal{F}$ über in L in Linerfaktoren zerfällt. Es gilt $\mathcal{F} \subseteq E[X] \setminus E$ mit $LE = E(\bigcup_{f\in\mathcal{F}} Z_{LE}(f))$. Das heißt LE ist Zerfällungskörper von $\mathcal{F}$ über E.

□

5.5 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 vermöge

$$(\varphi+\psi)(a) := \varphi(a)+\psi(a) \;\; ; \;\; (\alpha\varphi)(a) := \alpha\varphi(a) \quad \forall\, \varphi, \psi \in \mathrm{Abb}(A, K), a \in A, \alpha \in K.$$

Definition. Sei G eine Gruppe. Eine Abbildung $\chi : G \longrightarrow K$ heißt **Charakter**, falls $\chi(e) = 1$ und $\chi(gh) = \chi(g)\chi(h)$ für alle $g, h \in G$ gilt.

Satz 5.5.1. *Es seien $\chi_1, \ldots, \chi_n \in \mathrm{Abb}(G, K)$ paarweise verschiedene Charaktere. Dann ist die Menge $\{\chi_1, \ldots, \chi_n\}$ linear unabhängig.*

Beweis. Wir verwenden Induktion nach n, wobei der Fall $n = 1$ trivial ist. Sei also $n > 1$ sowie $\alpha_1, \ldots, \alpha_n \in K$ mit $\sum_{i=1}^{n} \alpha_i\chi_i = 0$. Für $g, h \in G$ erhalten wir

$$0 = \sum_{i=1}^{n} \alpha_i\chi_n(g)\chi_i(h) - \sum_{i=1}^{n} \alpha_i\chi_i(gh) = \sum_{i=1}^{n-1} \alpha_i(\chi_n(g) - \chi_i(g))\chi_i(h).$$

Damit folgt $\sum_{i=1}^{n-1} \alpha_i(\chi_n(g) - \chi_i(g))\chi_i = 0$ für jedes $g \in G$. Die Induktionsannahme liefert

$$\alpha_i(\chi_n(g) - \chi_i(g)) = 0 \;\text{ für }\; 1 \leq i \leq n-1,\; g \in G.$$

Da die Charaktere paarweise verschieden sind, gibt es für jedes $i \in \{1, \ldots, n-1\}$ ein $g_i \in G$ mit $\chi_n(g_i) \neq \chi_i(g_i)$. Also folgt $\alpha_i = 0$ für $i \in \{1, \ldots, n-1\}$ und somit auch $\alpha_n = 0$. □

Korollar 5.5.2. *Sei K', K ein Körper sowie $\sigma_1, \ldots, \sigma_n \colon K' \longrightarrow K$ paarweise verschiedene Homomorphismen. Dann ist $\{\sigma_1, \ldots, \sigma_n\} \subseteq \mathrm{Abb}(K', K)$ linear unabhängig über K.*

Beweis. Es seien $\alpha_1, \ldots, \alpha_n \in K$ mit

$$\sum_{i=1}^{n} \alpha_i \sigma_i = 0.$$

Wir betrachten die Gruppe $G := (K')^\times$ sowie für $i \in \{1, \ldots, n\}$

$$\tau_i : G \longrightarrow K \;\; ; \;\; g \mapsto \sigma_i(g).$$

Dann ist jedes τ_i ein Charakter und wegen $\sigma_i(0) = 0$ sind die τ_i paarweise verschieden. Da zudem $\sum_{i=1}^{n} \alpha_i \tau_i = 0$ gilt, liefert Satz 5.5.1: $\alpha_i = 0$ für $i \in \{1, \ldots, n\}$. Also ist $\{\sigma_1, \ldots, \sigma_n\}$ linear unabhängig. □

Definition. Sei $L : K$ eine Körperweiterung. Wir definieren

$$\mathrm{Aut}(L : K) := \{\varphi \colon L \longrightarrow L \mid \varphi \text{ ist Ringautomorphismus mit } \varphi|_K = \mathrm{id}_K\}$$

und bemerken, dass $\mathrm{Aut}(L : K)$ eine Untergruppe von $\mathrm{Aut}(L)$ ist. Die Gruppe $\mathrm{Aut}(L : K)$ heißt **Galoisgruppe** der Erweiterung $L : K$.

Korollar 5.5.3. *Es seien $Q : K$ und $L : K$ endliche Körpererweiterungen.*

(1) Es gilt

$$|\{\varphi \colon Q \longrightarrow L \mid \varphi \text{ ist Homomorphismus mit } \varphi|_K = \mathrm{id}_K\}| \leq [Q : K].$$

(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 Korollar 5.5.2

$$|\{\varphi \colon Q \longrightarrow L \mid \varphi \text{ ist Homomorphismus mit } \varphi|_K = \mathrm{id}_K\}| \leq [Q : K].$$

(2) Dies folgt aus (1) für $Q = L$.

□

6 Galoistheorie

6.1 Galoiserweiterungen

Definition. (1) Sei L ein Körper, $G \subseteq \mathrm{Aut}(L)$ eine Gruppe. Dann heißt

$$L^G := \{a \in L \mid \sigma(a) = a \quad \forall\, \sigma \in G\}$$

der **Fixkörper** von G.

(2) Eine endliche Erweiterung $L : K$ heißt **Galoiserweiterung**, falls $L^{\mathrm{Aut}(L:K)} = K$ gilt.

Bemerkung. Es gilt stets $L^{\mathrm{Aut}(L:K)} \supseteq K$.

Beispiele. (1) Nach Korollar 5.5.3 gilt $|\mathrm{Aut}(\mathbb{C} : \mathbb{R})| \leq 2$ und damit $\mathrm{Aut}(\mathbb{C} : \mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \bar{\cdot}\}$, wobei $\bar{\cdot}$ die Konjugation bezeichnet. 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 $\varphi(\sqrt[4]{2}) \in Z_{\mathbb{C}}(f) = \{i^k \sqrt[4]{2} \mid k \in \{0, 1, 2, 3\}\}$. Da $\{1, \sqrt[4]{2}, \sqrt[4]{2}^2, \sqrt[4]{2}^3\}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt[4]{2})$ ist, gilt $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$. Das heißt $\varphi(\sqrt[4]{2}) \in \{\sqrt[4]{2}, -\sqrt[4]{2}\}$. Es folgt $\varphi(\sqrt{2}) = \sqrt{2}$ und somit gilt bereits $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})^{\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q})} \subseteq \mathbb{Q}(\sqrt[4]{2})$. Das heißt $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$ ist keine Galoiserweiterung.

Satz 6.1.1. *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 $G = \{\varphi_1, \ldots, \varphi_n\}$. Wir definieren

$$\mathrm{Tr}_G \colon L \longrightarrow L, y \mapsto \sum_{i=1}^{n} \varphi_i(y)$$

und bemerken $\mathrm{Tr}_G(y) \in L^G$ für alle $y \in L$. Weiter gilt $\mathrm{Tr}_G \neq 0$ nach Korollar 5.5.2. 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

$$a_{ij} = \varphi_i^{-1}(y_j)\ \forall i \in \{1,\dots,n\}, j \in \{1,\dots,n+1\}.$$

Das Gleichungssystem besitzt eine nicht-triviale Lösung, etwa $t = (t_1,\dots,t_{n+1}) \in L^{n+1}$ und wir nehmen ohne Beschränkung $t_1 \neq 0$ an. Nun fixieren wir $y \in L$ mit $\mathrm{Tr}_G(y) \neq 0$ und bemerken, dass auch $z := yt_1^{-1}t = (y, yt_1^{-1}t_2,\dots,yt_1^{-1}t_{n+1}) \in L^{n+1}$ 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 $i \in \{1,\dots,n\}$ und damit

$$y_1\varphi_i(y) + \sum_{j=2}^{n+1} y_j\varphi_i(yt_1^{-1}t_j) = 0.$$

Wir erhalten

$$0 = \sum_{i=1}^{n} y_1\varphi_i(y) + \sum_{i=1}^{n}\sum_{j=2}^{n+1} y_j\varphi_i(yt_1^{-1}t_j) = \mathrm{Tr}_G(y)y_1 + \sum_{j=2}^{n+1} \mathrm{Tr}_G(yt_1^{-1}t_j)y_j.$$

Es gilt $\mathrm{Tr}_G(y) \neq 0$ und damit ist $\{y_1,\dots,y_{n+1}\}$ linear abhängig über L^G. Dies zeigt $[L : L^G] \leq |G|$. Weiter folgt mit Satz 5.5.3 | $\mathrm{Aut}(L : L^G)| \leq [L : L^G] \leq |G|$.
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 $f_a := \prod_{b\in G.a}(X - b) \in L[X]$. 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. Definitionsgemäß erhalten wir $L = L^G(\bigcup_{a\in L} Z_L(f_a))$ und jedes Polynom f_a zerfällt über L in Linearfaktoren. Also ist $L : L^G$ normal.

□

Korollar 6.1.2. *Sei $L : K$ eine Galoiserweiterung, dann ist $L : K$ normal.*

Beweis. Die Gruppe $\mathrm{Aut}(L : K)$ ist nach Korollar 5.5.3 endlich. Nach Definition gilt $L^G = K$. Wir wenden Satz 6.1.1 an. □

Satz 6.1.3. *Es sei $L : K$ eine endliche Körperweiterung. Folgende Aussagen sind äquivalent.*

(1) $L : K$ ist eine Galoiserweiterung.

(2) $|\operatorname{Aut}(L : K)| = [L : K]$.

Beweis. (1) $\Longrightarrow$ (2). Nach Satz 6.1.1 gilt $[L : K] = [L : L^{\operatorname{Aut}(L:K)}] = |\operatorname{Aut}(L : K)|$.
(2) $\Longrightarrow$ (1). Wir wenden Satz 6.1.1 auf die Gruppe $\operatorname{Aut}(L : K)$ an und erhalten

$$[L : K] = |\operatorname{Aut}(L : K)| = [L : L^{\operatorname{Aut}(L:K)}].$$

Mit $K \subseteq L^{\operatorname{Aut}(L:K)}$ folgt die Behauptung. □

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

$$X := \{\varphi\colon Q \longrightarrow L \mid \varphi \text{ ist Homomorphismus mit } \varphi|_K = \mathrm{id}_K\}$$

vermöge

$$G \times X \longrightarrow X;\ \ (\varphi, \psi) \mapsto \varphi.\psi := \varphi \circ \psi.$$

Es sei $x\colon Q \longrightarrow L$ die kanonische Inklusion. Es gilt für $\varphi \in G$ nach Definition

$$\varphi \in G_x \Leftrightarrow \varphi \circ x = x \Leftrightarrow \varphi(q) = \varphi(x(q)) = x(q) = q\ \forall q \in Q \Leftrightarrow \varphi \in \operatorname{Aut}(L : Q).$$

Nach Satz 5.5.3 ist X eine endliche Menge mit $|X| \leq [Q : K]$ und $|\operatorname{Aut}(L : Q)| \leq [L : Q]$. Wir erhalten mit der Bahnformel und Satz 6.1.3

$$[L : K] = |G| = |G_x||G.x| \leq |\operatorname{Aut}(L : Q)||X| \leq [L : Q][Q : K] = [L : K].$$

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

$$\mathcal{Z} := \{Q \mid K \subseteq Q \subseteq L \text{ Zwischenkörper}\} \quad \mathcal{U} := \{H \mid H \subseteq \operatorname{Aut}(L\colon K) \text{ Untergruppe}\},$$

sowie Abbildungen

$$\gamma : \begin{cases} \mathcal{Z} & \longrightarrow & \mathcal{U} \\ Q & \mapsto & \operatorname{Aut}(L\colon Q) \end{cases} \quad \text{und} \quad \delta : \begin{cases} \mathcal{U} & \longrightarrow & \mathcal{Z} \\ H & \mapsto & L^H. \end{cases}$$

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 $\delta(H_2) \subseteq \delta(H_1)$.

(5) Es gilt $\varphi(L^H) = L^{\varphi H \varphi^{-1}}$ für alle $\varphi \in \mathrm{Aut}(L:K)$ und $H \in \mathcal{U}$.

(6) Es sei $K \subseteq Q \subseteq L$ ein Zwischenkörper und $\varphi \in \mathrm{Aut}(L : K)$. Dann gilt

$$\mathrm{Aut}(L : \varphi(Q)) = \varphi \,\mathrm{Aut}(L : Q)\varphi^{-1}.$$

Beweis. (1) - (4) folgen direkt aus der Definition.

(5) Seien $\varphi \in \mathrm{Aut}(L:K)$ und $H \in \mathcal{U}$. Ist $y \in \varphi(L^H)$ und $g \in \varphi H \varphi^{-1}$, so existieren $x \in L^H$ und $h \in H$ mit $y = \varphi(x)$ und $g = \varphi \circ h \circ \varphi^{-1}$. Also erhalten wir

$$g(y) = (\varphi \circ h \circ \varphi^{-1})(\varphi(x)) = \varphi(h(x)) = \varphi(x) = y.$$

Damit folgt $\varphi(L^H) \subseteq L^{\varphi H \varphi^{-1}}$. Da φ beliebig gewählt ist, folgt auch

$$L^H \subseteq \varphi^{-1}(L^{\varphi H \varphi^{-1}}) \subseteq L^{\varphi^{-1}(\varphi H \varphi^{-1})\varphi} = L^H,$$

und daher $L^H = \varphi^{-1}(L^{\varphi H \varphi^{-1}})$, also $\varphi(L^H) = L^{\varphi H \varphi^{-1}}$.

(6) Für $\psi \in \mathrm{Aut}(L : \varphi(Q))$ und $x \in Q$ gilt $(\varphi^{-1} \circ \psi \circ \varphi)(x) = \varphi^{-1}(\varphi(x)) = x$, also $\varphi^{-1} \circ \psi \circ \varphi \in \mathrm{Aut}(L : Q)$ mit $\psi = \varphi \circ (\varphi^{-1} \circ \psi \circ \varphi) \circ \varphi^{-1}$. Dies zeigt $\mathrm{Aut}(L : \varphi(Q)) \subseteq \varphi \,\mathrm{Aut}(L : Q)\varphi^{-1}$. Sei nun $\psi' \in \mathrm{Aut}(L : Q)$, dann gilt $(\varphi \circ \psi' \circ \varphi^{-1})(\varphi(x)) = \varphi(x)$. Dies zeigt $\varphi \,\mathrm{Aut}(L : Q)\varphi^{-1} \subseteq \mathrm{Aut}(L : \varphi(Q))$.

□

Satz 6.1.6 (Hauptsatz der Galoistheorie). *Es sei $L : K$ eine Galoiserweiterung.*

(1) Es gilt $\delta \circ \gamma = \mathrm{id}_{\mathcal{Z}}$, $\gamma \circ \delta = \mathrm{id}_{\mathcal{U}}$.

(2) Für $Q \in Z$ sind äquivalent:

(i) $Q : K$ ist eine Galoiserweiterung.

(ii) $Q : K$ ist normal.

(iii) $\mathrm{Aut}(L : Q) \subseteq \mathrm{Aut}(L : K)$ ist eine normale Untergruppe.

(iv) Es gilt $\varphi(Q) = Q$ für alle $\varphi \in \mathrm{Aut}(L : K)$.

(3) Ist $Q \in \mathcal{Z}$ derart, dass $Q : K$ eine Galoiserweiterung ist, so gilt

$$\mathrm{Aut}(Q{:}K) \cong \mathrm{Aut}(L{:}K)/\mathrm{Aut}(L{:}Q).$$

Beweis. Da $L : K$ eine endliche Erweiterung ist, ist $\mathrm{Aut}(L : K)$ nach Korollar 5.5.3 eine endliche Gruppe.

(1) Sei $H \in \mathcal{U}$. Satz 6.1.1 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) (i) $\Longrightarrow$ (ii). Dies ist Korollar 6.1.2.
(ii) $\Longrightarrow$ (iii). Sei $Q \in \mathcal{Z}$ und $Q : K$ normal. Dann liefert Satz 5.4.3 $\psi(Q) = Q$ für alle $\psi \in \mathrm{Aut}(L{:}K)$. Damit folgt für $h \in \mathrm{Aut}(L{:}Q)$ und $\varphi \in \mathrm{Aut}(L : K)$

$$\varphi \circ h \circ \varphi^{-1}|_Q = \varphi \circ \varphi^{-1}|_Q = \mathrm{id}_Q\,.$$

Also ist $\mathrm{Aut}(L{:}Q)$ normal in $\mathrm{Aut}(L{:}K)$.
(iii) $\Longrightarrow$ (iv). Sei $\mathrm{Aut}(L{:}Q)$ normal und $\varphi \in \mathrm{Aut}(L : K)$. Es ist $L : \varphi(Q)$ nach Korollar 6.1.4 eine Galoiserweiterung. Damit liefert Lemma 6.1.5 die Gleichung

$$\mathrm{Aut}(L : \varphi(Q)) = \varphi\,\mathrm{Aut}(L : Q)\varphi^{-1} = \mathrm{Aut}(L : Q).$$

Da auch $L : Q$ eine Galoiserweiterung ist, folgt

$$\varphi(Q) = L^{\mathrm{Aut}(L:\varphi(Q))} = L^{\mathrm{Aut}(L:Q)} = Q.$$

(iv) $\Longrightarrow$ (i). Sei $x \in Q^{\mathrm{Aut}(Q:K)} \supseteq K$ und $\varphi \in \mathrm{Aut}(L : K)$. Es ist $\varphi|_Q$ nach Voraussetzung in $\mathrm{Aut}(Q : K)$. Damit gilt $\varphi(x) = \varphi|_Q(x) = x$. Da $L : K$ eine Galoiserweiterung ist, folgt $x \in L^{\mathrm{Aut}(L:K)} = K$ und insgesamt $Q^{\mathrm{Aut}(Q:K)} = K$.

(3) Aufgrund (iv) gilt $\varphi(Q) = Q$ für alle $\varphi \in \mathrm{Aut}(L : K)$ und

$$\Gamma : \left\{ \begin{array}{ccc} \mathrm{Aut}(L{:}K) & \longrightarrow & \mathrm{Aut}(Q{:}K) \\ \varphi & \mapsto & \varphi|_Q \end{array} \right.$$

ist eine wohldefinierte Abbildung und ferner ein Gruppenhomomorphismus mit $\ker\Gamma = \mathrm{Aut}(L : Q)$. Es ist $G := \mathrm{im}\,\Gamma$ eine Untergruppe von $\mathrm{Aut}(Q : K)$. Sei $x \in Q^G$. Für $\varphi \in \mathrm{Aut}(L : K)$ gilt $x = \Gamma(\varphi)(x) = \varphi|_Q(x) = \varphi(x)$. Dies zeigt $Q^G \subseteq L^{\mathrm{Aut}(L:K)} = K$, also $Q^G = K$. Wir erhalten mit Satz 6.1.1 $G = \mathrm{Aut}(Q : Q^G) = \mathrm{Aut}(Q : K)$. Damit ist Γ surjektiv. Die Behauptung folgt damit aus dem Homomorphiesatz.

□

Beispiel. Es sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von $f := X^3 - 2 \in \mathbb{Q}[X]$ über $\mathbb{Q}$ und $\zeta := \exp(\frac{2\pi i}{3}) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Es gilt $Z_{\mathbb{C}}(f) = \{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\}$ und damit $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$. Weiter gilt $[L : \mathbb{Q}] = 6$ (Übung) und $[L : \mathbb{Q}(\sqrt[3]{2})] = 2$. Es ist L der Zerfällungskörper von $X^2(\frac{1}{\sqrt[3]{2}})^2 + X\frac{1}{\sqrt[3]{2}} + 1 \in \mathbb{Q}(\sqrt[3]{2})[X]$ mit Nullstellenmenge $\{\zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\}$. Nach Korollar 5.4.3 existiert $\varphi \in \mathrm{Aut}(L : \mathbb{Q}(\sqrt[3]{2})) \subseteq \mathrm{Aut}(L : \mathbb{Q})$ mit $\varphi(\zeta\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$. Da $|\mathrm{Aut}(L : \mathbb{Q}(\sqrt[3]{2})) \leq [L : \mathbb{Q}(\sqrt[3]{2})] = 2$ gilt, folgt $\varphi^2 = \mathrm{id}$ und damit $\varphi(\zeta^2\sqrt[3]{2}) = \zeta\sqrt[3]{2}$. Da $\varphi \in \mathrm{Aut}(L : \mathbb{Q})$ die Nullstellen von f permutiert, folgt $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$. Da $L : \mathbb{Q}$ normal ist, folgt mit analogen Elementen die Existenz von $\varphi' \in \mathrm{Aut}(L : \mathbb{Q})$ mit $\varphi'(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$.
Wir betrachten die Operation

$$\mathrm{Aut}(L : \mathbb{Q}) \times Z_{\mathbb{C}}(f) \longrightarrow Z_{\mathbb{C}}(f); (f, x) \mapsto f.x := f(x)$$

mit zugehörigem Gruppenhomomorphismus $\Gamma\colon \mathrm{Aut}(L : \mathbb{Q}) \longrightarrow \mathcal{S}_{Z_{\mathbb{C}}(f)}$. Da $L = \mathbb{Q}(Z_{\mathbb{C}}(f))$ gilt, ist Γ injektiv und damit $\mathrm{Aut}(L : \mathbb{Q})$ isomorph zu einer Untergruppe von $\mathcal{S}_X \cong \mathcal{S}_3$. Es ist $\Gamma(\varphi)$ eine Transposition und $\Gamma(\varphi') \notin \langle\Gamma(\varphi)\rangle$ nach Konstruktion. Damit folgt bereits $\mathrm{Aut}(L : \mathbb{Q}) \cong \mathrm{im}\,\Gamma = \mathcal{S}_X$ und $|\mathrm{Aut}(L : \mathbb{Q})| = 6 = [L : \mathbb{Q}]$. Damit ist $L : \mathbb{Q}$ nach Satz 6.1.3 eine Galoiserweiterung.
Da $\mathcal{S}_X \cong \mathcal{S}_3$ genau 4 echte Untergruppen besitzt, existieren nach dem Hauptsatz der Galoistheorie genau 4 echte Zwischenkörper $\mathbb{Q} \subsetneq Q \subsetneq L$. Weiter existiert genau ein echter Normalteiler von $\mathcal{S}_X$ und damit genau ein echter Zwischenkörper, sodass $Q : \mathbb{Q}$ eine Galoiserweiterung ist.
Im Folgenden berechnen wir diese Zwischenkörper:
Da Γ ein Isomorphismus ist, finden wir $\psi \in \mathrm{Aut}(L : \mathbb{Q})$ mit $\psi(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$, $\psi(\zeta^2\sqrt[3]{2}) = \sqrt[3]{2}$ und $\psi(\zeta\sqrt[3]{2}) = (\zeta\sqrt[3]{2})$. Die echten Untergruppen sind damit gegeben durch

$$U_1 = \langle\varphi\rangle, U_2 = \langle\psi\rangle, U_3 = \langle\varphi\psi\varphi\rangle, U_4 = \langle\varphi\psi\rangle,$$

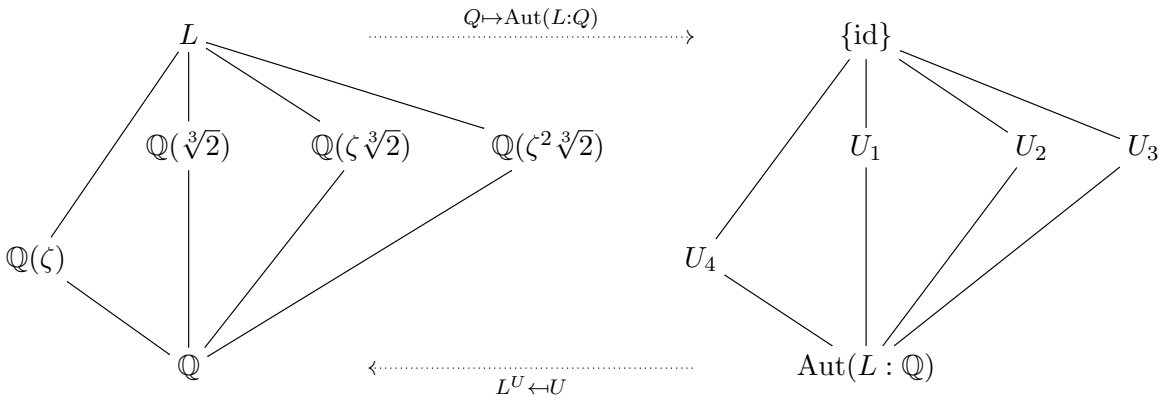
wobei $\varphi, \psi, \varphi\psi\varphi$ die Elemente der Ordnung 2 sind. Sei $i \in \{1, 2, 3\}$, dann gilt $|U_i| = 2$ gilt. Es ist $L : L^{U_i}$ eine Galoiserweiterung mit Galoisgruppe U_i. Inbesondere gilt $[L : L^{U_i}] = 2$ und damit $[L^{U_i} : \mathbb{Q}] = 3$. Analog folgt $[L : L^{U_4}] = 2$, da $|U_4| = 3$ gilt. Es sind

$$Q_1 := \mathbb{Q}(\sqrt[3]{2}), Q_2 := \mathbb{Q}(\zeta\sqrt[3]{2}), Q_3 := \mathbb{Q}(\zeta^2\sqrt[3]{2})$$

paarweise verschieden Körper mit $[Q_i : \mathbb{Q}] = 3$. Man sieht leicht $Q_i \subseteq L^{U_i}$ ein. Da $[Q_i : \mathbb{Q}] = [L^{U_i} : \mathbb{Q}]$ gilt, folgt $Q_i = L^{U_i}$ für alle $i \in \{1, 2, 3\}$. Ebenso zeigt man $L^{U_4} = \mathbb{Q}(\zeta)$. Wir fassen zusammen:

- $L : \mathbb{Q}$ ist eine Galoiserweiterung mi $\mathrm{Aut}(L : \mathbb{Q}) \cong \mathcal{S}_3$.
- $\{K, L, Q_1, Q_2, Q_3, Q_4\}$ ist die Menge der Zwischenkörper der Erweiterung $L : \mathbb{Q}$.
- Es gilt $L^{U_1} = Q_i$ und $\mathrm{Aut}(L : Q_i) = U_i$ für alle $i \in \{1, 2, 3, 4\}$, $L^{\mathrm{id}} = L$ und $L^{\mathrm{Aut}(L:Q)} = \mathbb{Q}$.
- Es gilt $\mathrm{Aut}(L : Q_i) = U_i$ für alle $i \in \{1, 2, 3, 4\}$.

Wir illustrieren unsere Ergebnisse:



Dieses Beispiel zeigt bereits, dass es schwierig sein kann, zu entscheiden, ob eine gegebene Erweiterung galoisch ist. Das Ziel des nächsten Abschnittes ist es eine Charakterisierung von Galoiserweiterungen zu beweisen, die uns diese Entscheidung erleichert.

6.2 Charakterisierung von Galoiserweiterungen

Definition. (1) Sei K ein Körper, $\bar{K}$ ein algebraischer Abschluss von K. Dann heißt $a \in \bar{K}$ **separabel über** K, wenn das Minimalpolynom $\mu_a \in K[X]$ in $\bar{K}$ nur einfache Nullstellen besitzt.

(2) Sei $L:K$ eine algebraische Körpererweiterung. Dann heißt $L:K$ **separabel**, falls jedes $a \in L$ separabel über K ist.

Bemerkung. Nach Lemma 5.3.4 und Satz 5.3.5 gilt für $a \in L$ und algebraische Abschlüsse K_1, K_2 von K mit $a \in K_1, K_2$ $|Z_{K_1}(\mu_a)| = |Z_{K_2}(\mu_a)|$. Also hängt die Separabilität von a nicht von der Wahl des algebraischen Abschlusses ab.

Lemma 6.2.1. *Sei K ein Körper, $a \in \bar{K}$. Dann sind folgende Aussagen äquivalent:*

(1) Das Element a ist separabel über K.

(2) $\mu_a' \neq 0$.

Beweis. (1) $\Rightarrow$ (2). Nach Voraussetzung ist a eine einfache Nullstelle von μ_a und Satz 4.2.6 liefert $\mu_a'(a) \neq 0$. Also folgt $\mu_a' \neq 0$.

(2) $\Rightarrow$ (1). Nach Lemma 5.2.2 ist μ_a irreduzibel. Wegen $\mu_a' \neq 0$ und $\deg(\mu_a') \leq \deg(\mu_a) - 1$ erhalten wir $\mu_a \nmid \mu_a'$. Also folgt $\mathrm{ggT}(\mu_a, \mu_a') = K[X]^\times = K^\times$ und der Satz von Bézout liefert $f, g \in K[X]$ mit $f\mu_a + g\mu_a' = 1$. Sei nun $b \in Z_{\bar{K}}(\mu_a)$. Dann folgt $1 = g(b)\mu_a'(b)$ und somit $\mu_a'(b) \neq 0$. Wegen Satz 4.2.6 hat b damit Multiplizität 1. Also ist a separabel über K. □

Satz 6.2.2. *Sei K ein Körper.*

(1) Sei $\mathrm{char}(K)=0$. Dann ist jede algebraische Erweiterung $L:K$ separabel.

(2) Sei $\mathrm{char}(K)=p>0$. Ist $L:K$ eine endliche Körpererweiterung mit $p\nmid[L:K]$, so ist $L:K$ separabel.

(3) Sei $\mathrm{char}(K)=p>0$ ein endlicher Körper und $L:K$ algebraische Erweiterung, so ist $L:K$ separabel.

Beweis.

(1) Sei $L:K$ algebraisch sowie $a\in L$. Wir schreiben

$$\mu_a=\sum_{i=0}^{n}\alpha_i X^i \quad n\geq 1 \;;\; \alpha_n=1$$

und erhalten $\mu_a'=\sum_{i=1}^{n} i\alpha_i X^{i-1}$. Für $\mathrm{char}(K)=0$ oder $p\nmid n$ folgt $n\alpha_n\neq 0$. Nach Lemma 6.2.1 ist a in beiden Fällen separabel über K.

(2) Sei $a\in L$ und $n=\deg(\mu_a)=[K(a):K]$. Mit Satz 5.2.1 folgt $n|[L:K]$. Nach Voraussetzung folgt dann $p\nmid n$. Insbesondere $\mu_a'\neq 0$ (siehe (1)).

(3) Wir betrachten den **Frobenius Morphismus**

$$\mathrm{Fr}\colon K\longrightarrow K, x\mapsto x^p.$$

Da $\mathrm{char}(K)=p>0$ eine Primzahl ist, gilt $(x+y)^p=x^p+y^p$ für alle $x,y\in K$. Also ist Fr ein Homomorphismus von Körpern und insbesondere injektiv. Nun liefert $|K|<\infty$ die Bijektivität. Sei $a\in L$. Wir nehmen an, dass a nicht separabel ist. Dann gilt nach Lemma 6.2.1 bereits $\mu_a'=0$ und Satz 4.2.7 liefert $\mu_a=\sum_{j=0}^{n}\alpha_j X^{jp}$ für geeignete $\alpha_0,\ldots,\alpha_n\in K$. Da Fr surjektiv ist, finden wir $a_0,\ldots,a_n$ mit $\mathrm{Fr}(a_j)=\alpha_j$ für alle $j\in\{0,\ldots,n\}$ und schließen

$$\mu_a=\sum_{j=0}^{n}a_j^p X^{jp}=(\sum_{j=0}^{n}a_j X^j)^p,$$

da $\mathrm{char}(K[X])=p>0$ gilt. Dies ist ein Widerspruch, da μ_a irreduzibel ist.

□

Beispiel. Sei T eine Unbestimmte über $\mathbb{Z}/(2)$ und $K:=Q(\mathbb{Z}/(2)[T])$ der Quotientenkörper von $\mathbb{Z}/(2)[T]$. Wir betrachten das Polynom $f:=X^2-T\in K[X]$. Das Polynom besitzt keine Nullstelle in K, da $T\in\mathbb{Z}/(2)[T]$ irreduzibel ist und $\mathbb{Z}/(2)[T]$ faktoriell ist. Also ist f irreduzibel. Sei L ein Zerfällungskörper von f über K und $a\in L$ eine Nullstelle von f. Mit $\mathrm{char}(L)=\mathrm{char}(K)=\mathrm{char}(\mathbb{Z}/(2))=2$ erhalten wir $(X-a)^2=X^2-a^2=X^2-T=f$. Damit ist a nicht separabel.

Definition. Sei K ein Körper mit algebraischem Abschluss $\bar{K}$. Ist $L:K$ eine algebraische Erweiterung, so heißt

$$[L:K]_s:=|\{\varphi:L\longrightarrow\bar{K}\mid \varphi\text{ Homomorphismus }\varphi|_K=\mathrm{id}_K\}|$$

der **Separabilitätsgrad** der Erweiterung $L:K$.

Bemerkung. Der Separabilitätsgrad hängt nicht von der Wahl von $\bar{K}$ ab (siehe Satz 5.3.5(2)).

Lemma 6.2.3. *Es seien $L:K$ und $M:L$ algebraische Körpererweiterungen. Dann gilt:*

(1) $[M:K]_s = [M:L]_s[L:K]_s$.

(2) Ist $L:K$ eine endliche Erweiterung, so gilt $[L:K]_s \leq [L:K]$.

Beweis.

(1) Wir wählen einen algebraischen Abschluss $\bar{K}$ von K, der M enthält und schreiben

$$\mathrm{Mor}_K(A,\bar{K}) := \{\varphi : A \longrightarrow \bar{K} \mid \varphi|_K = \mathrm{id}_K\}$$

für $A \in \{M, L\}$. Wir betrachten die Abbildung

$$\Omega : \mathrm{Mor}_K(M,\bar{K}) \longrightarrow \mathrm{Mor}_K(L,\bar{K}) \ ; \ \varphi \mapsto \varphi|_L.$$

Nach Satz 5.3.5(1) ist Ω surjektiv und es gilt daher

$$(*) \qquad \mathrm{Mor}_K(M,\bar{K}) = \bigsqcup_{\psi \in \mathrm{Mor}_K(L,\bar{K})} \Omega^{-1}(\psi).$$

Sei nun $\psi \in \mathrm{Mor}_K(L,\bar{K})$. Dann ist $\psi : L \longrightarrow \psi(L)$ ein Isomorphismus und Satz 5.3.5(2) liefert einen Automorphismus $\bar{\psi} : \bar{K} \longrightarrow \bar{K}$ mit $\bar{\psi}|_L = \psi$.
Sei $\gamma \in \Omega^{-1}(\psi)$. Dann gilt $\bar{\psi}^{-1} \circ \gamma \in \mathrm{Mor}_K(M,\bar{K})$ und $\Omega(\bar{\psi}^{-1} \circ \gamma) = \bar{\psi}^{-1} \circ \gamma|_L = \bar{\psi}^{-1} \circ \psi = \mathrm{id}_L$. Also ist

$$\zeta : \left\{ \begin{array}{ccc} \Omega^{-1}(\psi) & \longrightarrow & \Omega^{-1}(\mathrm{id}_L) \\ \gamma & \mapsto & \bar{\psi}^{-1} \circ \gamma \end{array} \right.$$

eine bijektive Abbildung mit Umkehrabbildung

$$\zeta' : \left\{ \begin{array}{ccc} \Omega^{-1}(\mathrm{id}_L) & \longrightarrow & \Omega^{-1}(\psi) \\ \gamma' & \mapsto & \bar{\psi} \circ \gamma'. \end{array} \right.$$

Damit liefert $(*)$

$$\begin{aligned} [M:K]_s &= |\mathrm{Mor}_K(M,\bar{K})| = \sum_{\psi \in \mathrm{Mor}_K(L,\bar{K})} |\Omega^{-1}(\psi)| = \sum_{\psi \in \mathrm{Mor}_K(L,\bar{K})} |\Omega^{-1}(\mathrm{id}_L)| \\ &= |\mathrm{Mor}_K(L,\bar{K})||\Omega^{-1}(\mathrm{id}_L)| = [L:K]_s[M:L]_s. \end{aligned}$$

(2) Wir betrachten zunächst den Fall $L = K(a)$. Nach Lemma 5.2.2 gilt dann $[L:K] = \deg \mu_a$. Infolge Lemma 5.3.4(3) erhalten wir $[L:K]_s = |Z_{\bar{K}}(\mu_a)|$, und daher $[L:K]_s \leq [L:K]$.

Im allgemeinen Fall gibt es $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$. Wir setzen $L_i := K(a_1, \ldots, a_i)$, $L_0 = K$, sodass $L_i = L_{i-1}(a_i)$ für $1 \leq i \leq n$. Dann folgt mit (1) und dem Spezialfall

$$[L:K]_s = \prod_{i=1}^{n} [L_i:L_{i-1}]_s \leq \prod_{i=1}^{n} [L_i:L_{i-1}]$$

und Satz 5.2.1 liefert $\prod_{i=1}^{n} [L_i:L_{i-1}] = [L:K]$.

□

Satz 6.2.4. *Sei $L:K$ eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent:*

(1) Die Erweiterung $L:K$ ist separabel.

(2) Es gibt separable Elemente $a_1,\dots,a_n \in L$ mit $L=K(a_1,\dots,a_n)$.

(3) Es gilt $[L:K]_s = [L:K]$.

Beweis. (1) $\Rightarrow$ (2). Dies folgt unmittelbar.
(2) $\Rightarrow$ (3). Für $i \in \{1,\dots,n\}$ sei $L_i := K(a_1,\dots,a_i)$. Wir zeigen induktiv: $[L_i:K]_s = [L_i:K]$. Der Fall $i=1$ folgt aus Lemma 5.3.4(2) und Lemma 5.2.2. Sei nun $i>1$. Es gilt $L_i = L_{i-1}(a_i)$. Es seien $\mu_{a_i,K}$ und $\mu_{a_i,L_{i-1}}$ die Minimalpolynome von a_i über K bzw. über L_{i-1}. Wegen $\mu_{a_i,K} \in L_{i-1}[X]$ und $\mu_{a_i,K}(a_i)=0$ folgt $\mu_{a_i,L_{i-1}} | \mu_{a_i,K}$. Also besitzt $\mu_{a_i,L_{i-1}}$ nur einfache Nullstellen und a_i ist separabel über L_{i-1}. Es folgt nun mit Lemma 6.2.3:

$$[L_i:K]_s = [L_i:L_{i-1}]_s[L_{i-1}:K]_s = [L_i:L_{i-1}][L_{i-1}:K] = [L_i:K].$$

(3) $\Rightarrow$ (1). Sei $a \in L$. Die Voraussetzung zusammen mit Lemma 6.2.3(1) liefert $[L:K(a)]_s[K(a):K]_s = [L:K] = [L:K(a)][K(a):K]$. Wegen Lemma 6.2.3(2) folgt damit $[K(a):K]_s = [K(a):K]$. Sei $\bar{K}$ ein algebraischer Abschluss von K der a enthält. Lemma 5.3.4 zeigt nun $|Z_{\bar{K}}(\mu_a)| = [K(a):K] = \deg(\mu_a)$. Also ist a separabel über K. □

Satz 6.2.5. *Sei $L:K$ eine algebraische Körpererweiterung. Es ist $L_s := \{a \in L \mid a \text{ ist separabel über } K\}$ ein Teilkörper von L, der K enthält.*

Beweis. Offenbar gilt $K \subseteq L_s$. Es seien $a,b \in L_s$. Dann ist nach Satz 6.2.4 $K(a,b):K$ separabel. Wegen $a+b, ab, a^{-1} \in K(a,b)$ gilt $a+b, ab, a^{-1} \in L_s$. Damit ist L_s ein Teilkörper von L. □

Definition. Sei $L:K$ eine algebraische Körpererweiterung. Dann heißt L_s die **separable Hülle von K in L**.

Definition. Sei K ein Körper. Ein irreduzibles Polynom $f \in K[X]$ heißt **separabel**, falls $f' \neq 0$ gilt. Ein Polynom $g \in K[X] \setminus K$ heißt **separabel** falls jeder irreduzible Faktor von g separabel ist.

Satz 6.2.6. *Sei $f \in K[X] \setminus K$ ein Polynom. Dann sind folgende Aussagen äquivalent.*

(1) Das Polynom f ist separabel.

(2) Der Zerfällungskörper von f in $\bar{K}$ ist separabel über K.

Beweis. (1) $\Rightarrow$ (2). Sei $L \subseteq \bar{K}$ der Zerfällungskörper sowie $a \in L$ eine Nullstelle von f. Dann ist μ_a ein irreduzibler Faktor von f und somit gilt $\mu_a' \neq 0$. Also ist das Element a gemäß Lemma 6.2.1 separabel über K. Damit folgt (2) aus Satz 6.2.4.

(2) $\Rightarrow$ (1). Sei $p \in K[X]$ ein irreduzibler Faktor von f. Dann besitzt p in L eine Nullstelle a und es gibt $\alpha \in K^\times$ mit $p = \alpha\mu_a$. Da a separabel über K ist, liefert Lemma 6.2.1: $p' = \alpha\mu_a' \neq 0$. Also ist f separabel. □

Korollar 6.2.7. *Es sei $L : K$ eine endliche Körpererweiterung. Folgende Aussagen sind äquivalent:*

(1) $L : K$ ist eine Galoiserweiterung.

(2) $[L : K] = |\operatorname{Aut}(L : K)|$.

(3) $L : K$ ist normal und separabel.

(4) Es existiert ein separables Polynom $f \in K[X] \setminus K$, sodass L der Zerfällungskörper von f ist.

Beweis. Die Äquivalenz (1) $\Leftrightarrow$ (2) gilt nach Korollar 6.1.3.
(1) $\Rightarrow$ (3). Nach Korollar 6.1.2 ist die Galoiserweiterung $L : K$ normal. Weiter gilt nach (2) und Lemma 6.2.3

$$[L : K] = |\operatorname{Aut}(L : K)| \leq [L : K]_s \leq [L : K],$$

also $[L : K]_s = [L : K]$. Wir wenden nun Satz 6.2.4 an.
(3) $\Longrightarrow$ (2). Nach Satz 5.4.3 und Satz 6.2.4 gilt $|\operatorname{Aut}(L : K)| = [L : K]_s = [L : K]$.
(3) $\Leftrightarrow$ (4). Ist $L : K$ normal und separabel, so liefert die Bemerkung nach Satz 5.4.3 ein Polynom $f \in K[X]$, sodass L der Zerfällungskörper von f über K ist. Nun liefert Satz 6.2.6, dass f separabel ist. Die Umkehrung folgt unmittelbar aus Satz 6.2.6.

□

Korollar 6.2.8. *Es sei $L : K$ eine endliche Körpererweiterung mit $\operatorname{char}(K) = 0$, oder $\operatorname{char}(K) = p > 0$ und K endlich, oder $\operatorname{char}(K) = p > 0$ und $p \nmid [L:K]$. Es sind äquivalent.*

(1) $L : K$ ist eine Galoiserweiterung.

(2) $L : K$ ist eine normale Erweiterung.

Beweis. Dies folgt unmittelbar aus Satz 6.2.2 und Korollar 6.2.7. □

Satz 6.2.9. *Sei $L:K$ eine endliche separable Körpererweiterung. Dann existiert ein Erweiterungskörper N von L derart, dass $N:K$ eine Galoiserweiterung ist.*

Beweis. Nach Voraussetzung ist $L:K$ algebraisch und wir finden separable Elemente $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$. Wir wählen einen algebraischen Abschluss $K \subseteq L \subseteq \bar{K}$ und setzen $f := \prod_{i=1}^n \mu_{a_i}$ und $L \subseteq N := K(Z_{\bar{K}}(f))$. Nach Satz 5.3.1 ist $N : K$ eine endliche Erweiterung. Nach Konstruktion ist f ein separables Polynom und Korollar 6.2.7 liefert die Behauptung. □

6.3 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. 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 Korollar 4.2.5 damit zyklisch.

(2) Für $n \in \mathbb{N}$ gilt

$$\mu_n(\mathbb{C}) = \{\exp(2\pi i \frac{m}{n}) \mid 0 \leq m \leq n-1\}$$

und für $\mathrm{ggT}(\ell, n) = 1$ ist $\exp(2\pi i \frac{\ell}{n})$ eine primitive n-te Einheitswurzel.

(3) Sei $\mathrm{char}(K) = p > 0$. Ist $\zeta \in \mu_p(K)$, so gilt

$$(\zeta - 1)^p = \zeta^p - 1^p = 0,$$

und damit $\zeta = 1$. Wir erhalten $\mu_p(K) = \{1\}$ und K besitzt keine primitiven p-ten Einheitswurzeln.

Satz 6.3.1. *Es sei $n \in \mathbb{N}$ und K ein Körper mit $\mathrm{char}(K) \nmid n$ an. Dann gilt:*

(1) Der Zerfällungskörper $K_n \subseteq \bar{K}$ des Polynoms $X^n - 1$ ist eine Galoiserweiterung von K.

(2) $\mathrm{ord}(\mu_n(K_n)) = n$ und $\varphi(n)$ ist die Anzahl der primitiven n-ten Einheitswurzeln.

Beweis.

(1) Es sei $f := X^n - 1$, dann gilt $K_n = K(Z_{\bar{K}}(f)) = K(\mu_n(K_n))$. Es sei $\zeta \in \mu_n(K_n)$. Es gilt $f(\zeta) = 0$ und damit existiert $g \in K[X]$ mit $f = g\mu_\zeta$. Mit $p \nmid n$ folgt $0 \neq n\zeta^{n-1} = f'(\zeta) = g\mu'_\zeta(\zeta)$. Damit ist ζ nach Lemma 6.2.1 separabel. Damit liefert Satz 6.2.4 die Separabilität der Erweiterung $K_n : K$.

(2) Der Beweis von (1) zeigt auch, dass f nur einfache Nullstellen besitzt. Damit gilt

$$\mathrm{ord}(\mu_n(K_n)) = |Z_{\bar{K}}(f)| = n.$$

Da $\mu_n(K_n)$ zyklisch ist, gibt es einen Isomorphismus $\psi : \mathbb{Z}/\langle n \rangle \longrightarrow \mu_n(K_n)$. Die Anzahl der primitiven n-ten Einheitswurzeln stimmt also mit der Zahl der Erzeuger von $\mathbb{Z}/\langle n \rangle$ überein. Nach Satz 1.2.1 ist dies gerade der Wert $\varphi(n)$ der Eulerschen φ-Funktion an der Stelle n.

□

Definition. Sei $n \in \mathbb{N}$.

(1) Für einen Körper sei $\mu_n^*(K) := \{\zeta \in \mu_n(K) \mid \operatorname{ord}(\zeta) = n\}$ 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 6.3.2. *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
$$\mu_n(\mathbb{C}) = \bigsqcup_{d|n} \{\zeta \in \mu_n(\mathbb{C}) \mid \operatorname{ord}(\zeta) = d\} = \bigsqcup_{d|n} \mu_d^*(\mathbb{C}).$$
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
$$X^n - 1 = q f_n + r \quad \text{und} \quad 0 \leq \deg(r) < \deg(f_n) \quad \text{oder} \quad r = 0.$$
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. Also gilt $\Phi_n = q \in \mathbb{Z}[X]$.

□

Lemma 6.3.3. *Sei $\zeta \in \mu_n^*(\mathbb{C})$ sowie p eine Primzahl, die n nicht teilt. Dann gilt $\mu_{\zeta,\mathbb{Q}} = \mu_{\zeta^p,\mathbb{Q}}$ für die Minimalpolynome von ζ und ζ^p über $\mathbb{Q}$.*

Beweis.

Wir beweisen zunächst: $\mu_{\zeta,\mathbb{Q}}, \mu_{\zeta^p,\mathbb{Q}} \in \mathbb{Z}[X]$.
`Beweis.` Nach Satz 6.3.2 gilt $\Phi_n \in \mathbb{Z}[X]$. Zudem zeigt Satz 4.3.3, dass $\mathbb{Z}[X]$ faktoriell ist. 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.[1] Nach Satz 4.3.3 ist jedes f_i irreduzibel in $\mathbb{Q}[X]$. Wegen $p \nmid n$ gilt nach Satz 1.2.1 $\zeta^p \in \mu_n^*(\mathbb{C})$ 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 $\{\mu_{\zeta,\mathbb{Q}}, \mu_{\zeta^p,\mathbb{Q}}\} \subseteq \{f_i \mid i \in \{1, \ldots, \ell\}\} \subseteq \mathbb{Z}[X]$. ◇

Wir setzen $f := \mu_{\zeta,\mathbb{Q}}$ und $g := \mu_{\zeta^p,\mathbb{Q}}$ und nehmen $f \neq g$ an. Dann gilt $fg \mid \Phi_n$ und somit $fg \mid X^n - 1$. Wegen $g(\zeta^p) = 0$ ist ζ eine Nullstelle des Polynoms $g(X^p) \in \mathbb{Z}[X]$ (siehe obige Überlegung) und es folgt $f | g(X^p)$ in $\mathbb{Q}[X]$. Wie in Satz 6.3.2 zeigt man: $f | g(X^p)$ in $\mathbb{Z}[X]$. 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 $\mathrm{char}((\mathbb{Z}/(p)[X]) = p$

$$\pi^*(g)^p \quad = \quad (\sum_{i=0}^{s} \pi(a_i) X^i)^p = \sum_{i=0}^{s} \pi(a_i)^p X^{ip} = \sum_{i=0}^{s} \pi(a_i) X^{ip} = \pi^*(g(X^p)) = \pi^*(f)\pi^*(h).$$

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 $q = mX$. Dies widerspricht $q^2 | (X^n - 1)$. □

Satz 6.3.4. *Sei $n \in \mathbb{N}$. Dann ist Φ_n irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$.*

Beweis. Da Φ_n normiert ist, liefert 4.3.3 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 1.2.1 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 1.2.1 eine primitive n-te Einheitswurzel. Wiederholte Anwendung von Lemma 6.3.3 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. □

[1] Da die Anzahl der f_i mit Leitkoeffizient -1 notwendig gerade ist, ist dies möglich.

Satz 6.3.5. *Sei K ein Körper, $n \in \mathbb{N}$ und $K_n \subseteq \bar{K}$ ein Zerfällungskörper von $X^n - 1$ über K.*

(1) Gilt $\mathrm{char}(K) \nmid n$, so ist $\mathrm{Aut}(K_n : K)$ zu einer Untergruppe von $(\mathbb{Z}/(n))^\times$ isomorph.

(2) Ist $K = \mathbb{Q}$, so gilt $\mathrm{Aut}(K_n : K) \cong (\mathbb{Z}/(n))^\times$.

Beweis.

(1) Nach Satz 6.3.1 existiert eine primitive n-te Einheitswurzel $\zeta \in K_n$. Sei $\sigma \in \mathrm{Aut}(K_n : K)$. Dann ist $\sigma(\zeta)$ eine primitive n-te Einheitswurzel von K_n und es existiert ein $m \in \mathbb{N}$ mit $\sigma(\zeta) = \zeta^m$ und $\mathrm{ggT}(m, n) = 1$. Sei $l \in \mathbb{Z}$. Nach Satz 1.2.1 gilt $\zeta^l = \zeta^m = \sigma(\zeta)$ genau dann, wenn $l \in m + (n)$. Weiter liefert $\mathrm{ggT}(m, n) = 1$ uns $m + (n) \in (\mathbb{Z}/(n))^\times$. Wir definieren $\Theta(\sigma) := m + (n)$. Wir erhalten die Abbildung

$$\Theta : \mathrm{Aut}(K_n : K) \longrightarrow (\mathbb{Z}/(n))^\times; \sigma \mapsto \Theta(\sigma).$$

Seien $\sigma, \tau \in \mathrm{Aut}(K_n : K)$ und $a, b \in \mathbb{Z}$ mit $\Theta(\sigma) = a + (n)$, $\Theta(\tau) = b + (n)$. Es folgt $(\sigma \circ \tau)(\zeta) = \sigma(\zeta^b) = (\zeta^a)^b = \zeta^{ab}$. Dies zeigt $\Theta(\sigma \circ \tau) = ab + (n) = (a + (n))(b + (n)) = \Theta(\sigma)\Theta(\tau)$. Sei $\sigma \in \ker \Theta$. Dann gilt $\sigma(\zeta) = \zeta$ und wegen $K = K(\zeta)$ folgt $\sigma = \mathrm{id}_{K_n}$. Damit ist Θ injektiv.

(2) Sei nun $K = \mathbb{Q}$. Nach Satz 6.3.1 ist $K_n : K$ eine Galoiserweiterung. Da $K_n = K(\zeta)$ gilt, schließen wir mit Satz 6.3.4, Lemma 5.2.2 und Übungsserie 7 Aufgabe 4:

$$|\mathrm{Aut}(K_n : K)| = [K_n : K] = \deg \Phi_n = \varphi(n) = |(\mathbb{Z}/(n))^\times|.$$

Damit ist Θ ein Isomorphismus.

□

6.4 Polynome der Form $X^n - a$

Definition. Sei K ein Körper, $n \in \mathbb{N}$ sowie $a \in K \setminus \{0\}$. Ist $L : K$ eine Körpererweiterung und ist $\alpha \in L$ ein Element mit $\alpha^n = a$, so nennt man $\alpha = \sqrt[n]{a}$ ein **Radikal von** a (in L).

Lemma 6.4.1. *Sei K ein Körper mit algebraischem Abschluss $\bar{K}$ sowie $n \in \mathbb{N}, \zeta \in \bar{K}$ eine primitive n-te Einheitswurzel.*

(1) Ist $a \in K \setminus \{0\}$ und $\sqrt[n]{a} \in \bar{K}$ ein Radikal von a, so ist $K(\sqrt[n]{a}, \zeta)$ ein Zerfällungskörper des Polynoms $X^n - a \in K[X]$.

(2) $K(\sqrt[n]{a}, \zeta) : K$ ist eine Galoiserweiterung.

Beweis.

(1) Wir setzen $\alpha := \sqrt[n]{a}$. Sei $Z \subseteq \bar{K}$ der Zerfällungskörper von $X^n - a \in K[X]$. Da $\alpha\zeta$ eine Wurzel von $X^n - a$ ist, liegen α und ζ in Z und es gilt $K(\sqrt[n]{a}, \zeta) \subseteq Z$.

Sei $\beta \in \bar{K}$ mit $\beta^n = a$. Dann gilt $(\frac{\beta}{\alpha})^n = 1$ und es existiert ein $m \in \mathbb{N}_0$ mit $\frac{\beta}{\alpha} = \zeta^m$. Mithin folgt $\beta \in K(\sqrt[n]{a}, \zeta)$ und wir erhalten $Z \subseteq K(\sqrt[n]{a}, \zeta)$.

(2) Es reicht den Fall $\mathrm{char}(K) = p > 0$ zu betrachten. Gilt $n = pm$ für ein $m \in \mathbb{N}$, so folgt

$$0 = \zeta^n - 1 = (\zeta^m - 1)^p$$

und damit $\zeta^m = 1$. Also ist ζ keine primitive n-te Einheitswurzel. Damit gilt also $p \nmid n$. Aufgrund von $n \nmid p$ gilt $(X^n - a)' = nX^{n-1} \neq 0$. Damit ist $X^n - a$ separabel und (1) liefert die Behauptung.

□

Satz 6.4.2. *Sei K ein Körper, $n \in \mathbb{N}$. Der Körper K enthalte eine primitive n-te Einheitswurzel ζ.*

(1) Sei $a \in K \setminus \{0\}$ mit Radikal $\sqrt[n]{a} \in \bar{K}$. Dann ist $K(\sqrt[n]{a}) : K$ eine Galoiserweiterung mit zyklischer Galoisgruppe, deren Ordnung n teilt.

(2) Ist $L : K$ eine Galoiserweiterung vom Grad $[L : K] = n$ mit zyklischer Galoisgruppe, so existiert ein Element $a \in K \setminus \{0\}$ derart, dass L ein Zerfällungskörper von $X^n - a$ ist.

Beweis.

(1) Wegen $\zeta \in K$ folgt $K(\sqrt[n]{a}, \zeta) = K(\sqrt[n]{a})$ (in $\bar{K}$). Nach Lemma 6.4.1 ist $K(\sqrt[n]{a}) : K$ eine Galoiserweiterung. Es sei $\alpha := \sqrt[n]{a}$. Die Zuordnung

$$\Theta : \mathrm{Aut}(K(\alpha) : K) \longrightarrow \mu_n(K) \ ; \ \sigma \mapsto \sigma(\alpha)\alpha^{-1}$$

ist eine wohldefinierte Abbildung. Wie im Beweis von Satz 6.3.5 lässt sich zeigen, dass Θ injektiver Gruppenhomomorphismus ist. Damit ist $\mathrm{Aut}(K(\sqrt[n]{a}) : K)$ isomorph zu einer Untergruppe von $\mu_n(K)$ und damit zyklisch. Wegen $\mathrm{ord}(\mu_n(K)) = n$ ist $\mathrm{ord}(\mathrm{Aut}(K(\sqrt[n]{a}) : K))$ ein Teiler von n.

(2) Nach Voraussetzung existiert $\sigma \in \mathrm{Aut}(L : K)$ mit $\mathrm{Aut}(L : K) = \langle\sigma\rangle$. Dann gilt $\mathrm{ord}(\sigma) = n$, und die Automorphismen $\mathrm{id}_L, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ sind paarweise verschieden. Damit zeigt Korollar 5.5.2: $\sum_{i=0}^{n-1} \zeta^{-i}\sigma^i \neq 0$. Es gibt also ein Element $c \in L \setminus \{0\}$ mit $b := \sum_{i=0}^{n-1} \zeta^{-i}\sigma^i(c) \neq 0$. Es folgt

$$\sigma(b) = \sum_{i=0}^{n-1} \zeta^{-i}\sigma^{i+1}(c) = \sum_{i=1}^{n} \zeta^{-i+1}\sigma^i(c) = \zeta b$$

und somit

$$\sigma^j(b) = \zeta^j b \quad 0 \leq j \leq n-1.$$

Wir erhalten also $\sigma^i(b) \neq \sigma^j(b)$ für $0 \leq i < j \leq n-1$ und daher

$$n \leq [K(b) : K]_s \leq [K(b) : K] \leq [L : K] = n$$

und damit $L = K(b)$. Wir betrachten nun $a := b^n$. Dann gilt

$$\sigma(a) = \sigma(b)^n = \zeta^n b^n = b^n = a$$

und somit $a \in L^{\mathrm{Aut}(L:K)} = K$. Also gilt $X^n - a \in K[X]$ und $K(b)$ ist der Zerfällungskörper von $X^n - a$, da $\zeta \in K$ und $\zeta^j b$ $(0 \leq j \leq n-1)$ Nullstellen von $X^n - a$ sind.

□

6.5 Auflösbarkeit von Gleichungen

Definition. Sei $L : K$ eine Körpererweiterung. Dann heißt $L : K$ **durch Radikale auflösbar**, falls es $u_1, \ldots, u_r \in \bar{K}$ und $m_1, \ldots, m_r \in \mathbb{N}$ gibt, mit

(a) $L \subseteq K(u_1, \ldots, u_r)$, und

(b) $u_1^{m_1} \in K$ und $u_i^{m_i} \in K(u_1, \ldots, u_{i-1})$ für $2 \leq i \leq r$.

Bemerkung. Es gibt in der Literatur unterschiedliche Definitionen für den Begriff „durch Radikale auflösbar". Manchmal wird anstatt Bedingung (a) auch $L = K(u_1, \ldots, u_r)$ gefordert.

Satz 6.5.1. *Sei $L : K$ eine endliche Körpererweiterung, $\mathrm{char}(K) = 0$. Dann sind folgende Aussagen äquivalent:*

(1) Die Erweiterung $L : K$ ist durch Radikale auflösbar.

(2) Es gibt eine endliche Körpererweiterung $M : L$ derart, dass $M : K$ eine Galoiserweiterung mit auflösbarer Galoisgruppe $\mathrm{Aut}(M : K)$ ist.

Beweis. (1) $\Rightarrow$ (2). Wir beweisen zunächst

Es existiert ein Teilkörper $L \subseteq M' \subseteq \bar{K}$ sowie $v_1, \ldots, v_s \in M'$, $n_1, \ldots, n_s \in \mathbb{N}$ mit

(a) $M' = K(v_1, \ldots, v_s)$.

(b) $M' : K$ ist normal.

(c) $v_i^{n_i} \in K(v_1, \ldots, v_{i-1})$ $\quad 2 \leq i \leq s, \;\; v_1^{n_1} \in K$.

`Beweis.` Nach Voraussetzung gibt es $u_1, \ldots, u_t \in \bar{K}$, $m_1, \ldots, m_t \in \mathbb{N}$ sodass $M := K(u_1, \ldots, u_t)$ die Bedingungen (a) und (c) erfüllt und zudem $M \supseteq L$ gilt.

Wir beweisen $(*)$ durch Induktion nach $n := [M : K]$. Der Fall $n = 1$ ist trivial; sei also $n \geq 2$. Wir setzen

$$t_0 := \min\{s \in \{1, \ldots, t\} \mid K(u_1, \ldots, u_s) = M\}.$$

Dann gilt für $M_0 := K(u_1, \ldots, u_{t_0 - 1})$:

(i) $K \subseteq M_0 \subsetneq M$ und $M_0(u_{t_0}) = M$.

Nach Induktionsannahme gibt es eine normale Erweiterung $M_0 \subseteq M_0' \subseteq \bar{K}$, die durch sukzessive Adjunktion von Radikalen (Eigenschaften (a),(c)) entsteht. Wir betrachten nun das Polynom

$$f := \prod_{\sigma \in \mathrm{Aut}(M_0':K)} (X^{m_{t_0}} - \sigma(u_{t_0}^{m_{t_0}})) \in M_0'[X].$$

Für $\sigma \in \mathrm{Aut}(M_0' : K)$ sei $\sigma^* : M_0'[X] \longrightarrow M_0'[X]$ der induzierte Automorphismus. Wegen $\sigma^*(f) = f$ für alle $\sigma \in \mathrm{Aut}(M_0' : K)$ folgt $f \in {M_0'}^{\mathrm{Aut}(M_0':K)}[X]$. Da $\mathrm{char}(K) = 0$ gilt, ist $M_0' : K$ eine Galoiserweiterung und damit gilt $f \in K[X]$,

Sei nun $M' \subseteq \bar{K}$ der Zerfällungskörper von f über M_0'. Wegen $f(u_{t_0}) = 0$ folgt $M = M_0(u_{t_0}) \subseteq M'$. Da $M_0' : K$ eine endliche, normale Körpererweiterung ist, gibt es ein Polynom $g \in K[X]$ derart, dass M_0' der Zerfällungskörper von g ist. Dann ist M' der Zerfällungskörper von $fg \in K[X]$ und die Erweiterung $M' : K$ ist normal.

Nach Definition ist die Erweiterung $M' : M_0'$ durch Radikale auflösbar. Dies gilt dann auch für die Erweiterung $M' : K$. ◇

Es sei nun also $L \subseteq M \subseteq \bar{K}$ ein Teilkörper derart, dass (a)-(c) für M gelten. Damit gibt es eine Kette

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = M$$

von Teilkörpern mit $K_i = K_{i-1}(u_i)$; $u_i^{m_i} \in K_{i-1}, m_i \in \mathbb{N}$ für $1 \leq i \leq s$. Es sei nun $m := \mathrm{kgV}(m_1, \ldots, m_s)$ sowie $\zeta \in \bar{K}$ eine primitive m-te Einheitswurzel. Wir setzen $K_i' := K_i(\zeta)$ für $0 \leq i \leq s$. Dann gilt

$$K(\zeta) = K_0' \subseteq K_1' \subseteq \cdots \subseteq K_s' = M(\zeta),$$

wobei $K_i' = K_{i-1}'(u_i)$; $u_i^{m_i} \in K_{i-1}'$ $\forall\, i \in \{1, \ldots, s\}$.

Da $\mathrm{char}(K) = 0$ gilt, ist die Erweiterung $M(\zeta) : K$ separabel. Ferner ist $M : K$ normal und da ζ eine primitive Einheitswurzel ist, ist $M(\zeta) : K$ ebenfalls normal. Nach Satz 6.4.2 ist für jedes $i \in \{1, \ldots, s\}$ $K_i' : K_{i-1}'$ eine Galoiserweiterung mit zyklischer Galoisgruppe. Zudem ist $M(\zeta) : K_i'$ normal und separabel. Wir setzen $G_i := \mathrm{Aut}(M(\zeta) : K_i')$ $\forall\, i \in \{0, \ldots, s\}$. Nach Satz 6.1.6(5),(6) ist G_i normal in G_{i-1} und es gilt $G_i / G_{i-1} \cong \mathrm{Aut}(K_i' : K_{i-1}')$ für $i \in \{1, \ldots, s\}$. Wegen Satz 6.3.5 ist $K(\zeta) : K$ ebenfalls eine Galoiserweiterung mit zyklischer Galoisgruppe. Damit ist G_0 normale Untergruppe von $\mathrm{Aut}(M(\zeta) : K)$ und $\mathrm{Aut}(M(\zeta) : K)/G_0$ ist zyklisch. Wir erhalten also eine abelsche Normalreihe

$$\mathrm{Aut}(M(\zeta) : K) \supseteq G_0 \supseteq \cdots \supseteq G_s = \{e\}.$$

Damit ist $\mathrm{Aut}(M(\zeta) : K)$ auflösbar.

(2) ⇒ (1). Nach Voraussetzung gibt es einen Körper $L \subseteq M$ derart, dass $M : K$ eine Galoiserweiterung mit auflösbarer Galoisgruppe $\mathrm{Aut}(M : K)$ ist. Wir setzen $n := [M : K]$ und wählen eine primitive n-te Einheitswurzel $\zeta \in \bar{K}$. Dann ist die Erweiterung $M(\zeta) : K$ ebenfalls normal und wegen $\mathrm{char}(K) = 0$ eine Galoiserweiterung.

Sei $\sigma \in \mathrm{Aut}(M(\zeta) : K(\zeta))$. Da $M : K$ normal ist, folgt $\sigma(M) = M$ und wir erhalten einen Gruppenhomomorphismus

$$\mathrm{res} : \left\{ \begin{array}{ccc} \mathrm{Aut}(M(\zeta) : K(\zeta)) & \longrightarrow & \mathrm{Aut}(M : K) \\ \sigma & \mapsto & \sigma|_M. \end{array} \right.$$

Für $\sigma \in \ker \mathrm{res}$ gilt $\sigma|_M = \mathrm{id}_M$ und $\sigma|_{K(\zeta)} = \mathrm{id}_{K(\zeta)}$. Damit folgt $\sigma = \mathrm{id}_{M(\zeta)}$. Also ist res injektiv und $\mathrm{Aut}(M(\zeta):K(\zeta))$ auflösbar. Damit liefert 2.3.5 eine abelsche Normalreihe

$$\mathrm{Aut}(M(\zeta):K(\zeta)) = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_s = \{e\},$$

deren Faktoren G_i/G_{i+1} zyklisch von Primzahlordnung p_i sind. Nach Satz 6.1.6 gibt es also Zwischenkörper

$$K(\zeta) = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{s-1} \subseteq K_s = M(\zeta)$$

mit $\mathrm{Aut}(K_{i+1}:K_i) \cong G_i/G_{i+1}$. Wegen $p_i = [K_{i+1}:K_i] | n$ enthält K_i eine primitive p_i-te Einheitswurzel. Damit existiert gemäß Satz 6.4.2 ein Element $u_{i+1} \in K_{i+1}$ mit $K_{i+1} = K_i(u_{i+1})$ und $u_{i+1}^{p_i} \in K_i$.

Es folgt $L \subseteq K(u_1, \ldots, u_s) = M(\zeta)$ und damit ist $L:K$ durch Radikale auflösbar. □

Korollar 6.5.2. *Sei $L:K$ eine endliche Galoiserweiterung eines Körpers K der Charakteristik 0. Dann ist $L:K$ genau dann durch Radikale auflösbar, wenn die Galoisgruppe $\mathrm{Aut}(L:K)$ auflösbar ist.*

Beweis. Angenommen, $L:K$ ist durch Radikale auflösbar. Nach Satz 6.5.1 gibt es eine endliche Galoiserweiterung $M:K$ mit $L \subseteq M$ und auflösbarer Galoisgruppe $\mathrm{Aut}(M:K)$. Wegen Satz 6.1.6 gilt $\mathrm{Aut}(L:K) \cong \mathrm{Aut}(M:K)/\mathrm{Aut}(M:L)$, und damit ist $\mathrm{Aut}(L:K)$ nach Satz 2.3.2 auflösbar. Ist $\mathrm{Aut}(L:K)$ auflösbar, so folgt aus Satz 6.5.1, dass $L:K$ durch Radikale auflösbar ist. □

Wir wollen abschließend andeuten, wie Satz 6.5.1 mit der Frage der Existenz von Lösungsformeln zusammenhängt. Dazu benötigen wir zunächst Informationen über Untergruppen symmetrischer Gruppen.

Lemma 6.5.3. *Sei p eine Primzahl, $G \subseteq \mathcal{S}_p$ eine Untergruppe derart, dass G eine Transposition und einen p-Zykel enthält. Dann gilt $G = \mathcal{S}_p$.*

Beweis. Ohne Einschränkung können wir annehmen, dass $\sigma := (1, 2 \ldots, p-1, p) \in G$. Wir interpretieren die Zahlen als Elemente von $\mathbb{Z}/(p)$ und erhalten $\sigma(j) = j+1$ für alle $j \in \mathbb{Z}/(p)$. Damit folgt $\sigma^\ell(j) = j+\ell \;\; \forall\, j \in \mathbb{Z}/(p), \ell \in \mathbb{Z}$. Nach Voraussetzung gibt es $i, q \in \mathbb{Z}/(p), q \neq 0$ mit $\tau := (i, i+q) \in G$. Dann folgt aus 1.4.2:

$$(*) \qquad (i+\ell, i+q+\ell) = \sigma^\ell \circ \tau \circ \sigma^{-\ell} \in G$$

für $\ell \in \{0, \ldots, p-1\}$.

Sei nun $n \in \{1, \ldots, p-2\}$ gegeben mit $(i, i+nq) \in G$. Wegen $i+nq \neq i \neq i+(n+1)q$ folgt aus (I.1.4.2) und $(*)$

$$(i, i+(n+1)q) = (i+nq, i+(n+1)q) \circ (i, i+nq) \circ (i+nq, i+(n+1)q) \in G.$$

Damit erhalten wir

$$(i, i+nq) \in G \quad \forall\, n \in \{1, \ldots, p-1\}.$$

Da die Abbildung $\mathbb{Z}/(p) \longrightarrow \mathbb{Z}/(p) \;\; ; \;\; n \mapsto nq$ bijektiv ist, folgt $(i, r) \in G$ für alle $r \in \mathbb{Z}/(p) \setminus \{i\}$. Für $i \neq 1$ gilt

$$(1, r) = (i, 1) \circ (i, r) \circ (i, 1) \in G \quad \forall\, r \in \mathbb{Z}/(p) \setminus \{i\}.$$

Die Behauptung folgt nun mit Satz 1.4.2. □

Korollar 6.5.4. *Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom mit Zerfällungskörper $L \subseteq \mathbb{C}$. derart, dass $\deg(f) =: p$ eine Primzahl ist. Besitzt f genau zwei nicht-reelle Nullstellen, so gilt $\mathrm{Aut}(L:\mathbb{Q}) \cong \mathcal{S}_p$.*

Beweis. Es sei $Z := \{\zeta_1, \dots, \zeta_p\}$ die Menge der Nullstellen von f in L. Da f irreduzibel ist, gilt $|Z| = p$. Wir nehmen $\zeta_1, \zeta_2 \in \mathbb{C} \setminus \mathbb{R}$ an. Es bezeichne $\kappa \in \mathrm{Aut}(\mathbb{C}:\mathbb{R})$ die komplexe Konjugation. Es gilt $\kappa(\zeta_i) \neq \zeta_i$ für $i \in \{1,2\}$. Da $\kappa|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ gilt, sind $\kappa(\zeta_1), \kappa(\zeta_2) \in \mathbb{C} \setminus \mathbb{R}$ Nullstellen von f. Wir erhalten $\kappa(\zeta_1) = \kappa(\zeta_2)$, $\kappa(\zeta_2) = \kappa(\zeta_1)$ sowie $\kappa(\zeta_i) = \zeta_i$ für $i \in \{3, \dots, p\}$. Insbesondere folgt $\kappa|_L \in \mathrm{Aut}(L:\mathbb{Q})$. Da f irreduzibel ist, gilt $[\mathbb{Q}(\zeta_1):\mathbb{Q}] = p$. Damit liefert Satz 5.2.1: $p|[L:\mathbb{Q}] = |\mathrm{Aut}(L:\mathbb{Q})|$. Es gilt $\sigma|_Z \in \mathcal{S}_Z$ für alle $\sigma \in \mathrm{Aut}(L:\mathbb{Q})$ und

$$\Omega : \mathrm{Aut}(L:\mathbb{Q}) \longrightarrow \mathcal{S}_Z \cong \mathcal{S}_p \ ; \ \sigma \mapsto \sigma|_Y$$

ist ein injektiver Gruppenhomomorphismus. Sei $G := \mathrm{im}\,\Omega$. Nach obigen Bemerkungen ist $\Omega(\kappa|_L) \in G$ eine Transposition. Wegen $p|\,\mathrm{ord}(G)$ enthält G ein Element g der Ordnung p. Nach Übungsserie 4 ist g ein p-Zykel. Nun liefert Lemma 6.5.3 $G = \mathcal{S}_p$; also ist Ω der gewünschte Isomorphismus. □

Definition. Es sei $f \in K[X]$ und $K \subseteq L \subseteq \bar{K}$ ein Zerfällungskörper von f über K. Dann heißt f **auflösbar (durch Radikale)** über K, falls $L : K$ durch Radikale auflösbar ist.

Satz 6.5.5. *Das Polynom $f := X^5 - 6X + 3 \in \mathbb{Q}[X]$ ist nicht auflösbar.*

Beweis. Das Polynom ist nach dem Eisensteinkriterium irreduzibel. Die Ableitung $f' = 5X^4 - 6$ besitzt genau die reellen Nullstellen $\pm\sqrt[4]{\frac{6}{5}}$. Nach dem Eisensteinkriterium ist $f' \in \mathbb{Q}[X]$ irreduzibel mit $f'(\sqrt[4]{\frac{6}{5}}) = 0$. Mithin ist $\pm\sqrt[4]{\frac{6}{5}} \in \mathbb{R} \setminus \mathbb{Q}$ und damit $f(\sqrt[4]{\frac{6}{5}}) = (\frac{6}{5} - 6)\sqrt[4]{\frac{6}{5}} + 3 \neq 0$. Ebenso gilt $f(-\sqrt[4]{\frac{6}{5}}) \neq 0$. Damit sind alle Nullstellen von f einfache Nullstellen.
Weiter gilt

$$f(-2) < 0, f(0) = 3, f(1) < 0 \text{ und } f(2) > 0.$$

Damit besitzt f nach dem Zwischenwertsatz mindestens drei verschiedene Nullstellen in $\mathbb{R}$. Da zwischen zwei reellen Nullstellen die Ableitung stets verschwinden muss, folgt, dass f genau drei reelle Nullstellen besitzt.
Es sei L der Zerfällungskörper von f in $\mathbb{C}$. Wir erhalten mit Korollar 6.5.4 $\mathrm{Aut}(L : \mathbb{Q}) \cong \mathcal{S}_5$ und Satz 6.5.1 liefert, dass $L : \mathbb{Q}$ nicht durch Radikale auflösbar ist, da $\mathcal{S}_5$ nach Satz 2.3.7 eine nicht auflösbare Gruppe ist.

□

Literaturverzeichnis

[1] S. Bosch, *Algebra*, Springer-Verlag, 1996.

[2] H-D. Ebbinghaus, *Einführung in die Mengenlehre*, Springer-Verlag, 2021.

[3] J.C. Jantzen and J. Schwermer, *Algebra*, Springer-Verlag, 2006.

[4] K. Meyberg, *Algebra*: *Teil 2*, Carl Hanser Verlag, 1976.

[5] R. Weidmann, *Vorlesungsskript Lineare Algebra I/II* (2020/21).

[6] R. A. Wilson, *An elementary proof that not all principal ideal domains are Euclidean domains*, The Mathematical Gazette (2017).

[7] Wikipedia, *Erweiterer Euklidischer Algorithmus*, https://de.wikipedia.org/wiki/Erweiterter_euklidischer_Algorithmus.