Skript zur Vorlesung

Algebra

SS 2012

Peter Junghanns

Hinweis: Das vorliegende Skript stellt nur ein Gerüst zu den Inhalten der Vorlesung dar. Die Vorlesung selbst bietet weiterführende Erläuterungen, Beweise und die ausführliche Behandlung der Beispiele.

Inhaltsverzeichnis

Literaturverzeichnis

[1] E. Artin, Galoissche Theorie, Verlag Harry Deutsch, Frankfurt am Main, 1988.

[2] M. Artin, Algebra, Birkhäuser Verlag, Basel, Boston, Berlin, 1993.

[3] C. Karpfinger, K. Meyberg, Algebra (Gruppen - Ringe - Körper), Spektrum Akademischer Verlag, Heidelberg, 2009.

[4] K. Meyberg, Algebra, Teil 1 und Teil 2, Carl Hanser Verlag, München, Wien.

Kapitel 1

Gruppen

Bezeichnungen:

- $\mathbb{N} := \{1, 2, \ldots\}$ - die Menge der natürlichen Zahlen ohne die Null
- $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$ - die Menge der natürlichen Zahlen mit der Null
- $\mathbb{Z} := \{0, \pm 1, \pm 2, \ldots\}$ - die Menge der ganzen Zahlen
- $\mathbb{Q}$ - Menge der rationalen Zahlen
- $\mathbb{R}$ - Menge der reellen Zahlen
- $\mathbb{C}$ - Menge der komplexen Zahlen

1.1 Grundlegende Begriffe

Definition 1.1 *Unter einer* **Gruppe G** *verstehen wir eine nichtleere Menge* $\mathbf{G}$ *versehen mit einer binären Verknüpfung, d.h. mit einer Abbildung* $\mathbf{G} \times \mathbf{G} \longrightarrow \mathbf{G}$, $(a, b) \mapsto ab$, *die folgenden Axiomen genügt:*

(G1) *Für beliebige* $a, b, c \in \mathbf{G}$ *gilt* $(ab)c = a(bc)$.

(G2) *Es existiert ein* **Einselement** $e \in \mathbf{G}$, *d.h.* $ae = ea = a \;\forall\, a \in \mathbf{G}$.

(G3) *Für jedes* $a \in \mathbf{G}$ *existiert ein zu* a **inverses Element** $b =: a^{-1} \in \mathbf{G}$ *mit* $ab = ba = e$.

Eine Gruppe ist also ein geordnetes Paar $(\mathbf{G}, \cdot)$ aus einer nichtleeren Menge $\mathbf{G}$ und einer auf dieser definierten binären Verknüpfung, die den Gruppenaxiomen (G1) – (G3) genügt.

Das Einselement und das Inverse zu einem Element sind eindeutig bestimmt, denn wäre e' ein weiteres Einselement, so folgt $e' = e'e = e$, und aus $ab = ca = e$ folgt $c = ce = cab = eb = b$.

Rechenregeln:

- $\left(a^{-1}\right)^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$
- $m \in \mathbb{N}$: $a^0 := e$, $a^m := a^{m-1}a$, $a^{-m} := \left(a^{-1}\right)^m$ (ganzzahlige Potenzen)
- $m, n \in \mathbb{Z}$: $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$, $(ab)^m = a^m b^m$ falls $ab = ba$ (Potenzgesetze)
- $\dfrac{a}{b} := a\, b^{-1}$
- $ac = bc \implies a = b$, $\quad ca = cb \implies a = b$ (Kürzungsregeln)

Eine Gruppe entsprechend Definition 1.1 nennt man auch **multiplikative Gruppe**. Schreibt man die Verknüpfung in der Form $(a, b) \mapsto a + b$, so spricht man von einer **additiven Gruppe**. Die Gruppenaxiome schreiben sich dann wie folgt:

(G1) Für beliebige $a, b, c \in \mathbf{G}$ gilt $(a + b) + c = a + (b + c)$.

(G2) Es existiert ein **Nullelement** $\theta \in \mathbf{G}$, d.h. $a + \theta = \theta + a = a \;\forall\, a \in \mathbf{G}$.

(G3) Für jedes $a \in \mathbf{G}$ existiert ein zu a **entgegengesetztes Element** $b =: -a \in \mathbf{G}$ mit $a + b = b + a = \theta$.

Rechenregeln in einer additiven Gruppe:

- $-(-a) = a$, $-(a + b) = (-b) + (-a)$
- $m \in \mathbb{N} : 0a := \theta$, $ma := (m - 1)a + a$, $(-m)a := m(-a)$ (ganzzahlige Vielfache)
- $m, n \in \mathbb{Z}$: $ma + na = (m + n)a$, $n(ma) = (nm)a$, $m(a + b) = ma + mb$ falls $a + b = b + a$
- $a - b := a + (-b)$
- $a + c = b + c \implies a = b$, $\quad c + a = c + b \implies a = b$

Man nennt eine Gruppe **kommutativ** bzw. **abelsch**, wenn für die Verknüpfung das Kommutativgesetz gilt. Unter einer **Untergruppe** einer Gruppe $(\mathbf{G}, \diamond)$ versteht man eine nichtleere Teilmenge $\mathbf{U} \subset \mathbf{G}$, so dass $(\mathbf{U}, \diamond)$ selbst eine Gruppe ist.

Beispiele:

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ - additive abelsche Gruppen
- $(\mathbb{Z}_m, +)$ - additive abelsche Gruppe der Restklassen modulo m ($m \in \mathbb{N}$)
- $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, - multiplikative abelsche Gruppen
- $(\mathbb{Z}_m^{\text{prim}}, \cdot)$ - multiplikative abelsche Gruppe der primen Restklassen modulo m

- $G\mathbb{Q}^{m\times m}$, $G\mathbb{R}^{m\times m}$, $G\mathbb{C}^{m\times m}$ - Die Mengen invertierbarer Matrizen der Ordnung m sind Beispiele nichtkommutativer Gruppen.
- Sind $M \neq \emptyset$ und $\mathcal{S}(M) := \{f : M \longrightarrow M \text{ bijektiv}\}$, so ist $(\mathcal{S}(M), \circ)$ eine Gruppe, die **Permutationsgruppe** oder **symmetrische Gruppe** über M .

  Insbesondere: $\mathcal{S}_n := \mathcal{S}(\{1, \ldots, n\})$.

Satz 1.2 *Eine nichtleere Teilmenge* $\mathbf{U} \subset \mathbf{G}$ *der Gruppe* $\mathbf{G}$ *ist genau dann Untergruppe von* $\mathbf{G}$, *wenn eine der folgenden Bedingungen erfüllt ist:*

(a) $a, b \in \mathbf{U}$ *impliziert* $a^{-1}b \in \mathbf{U}$.

(b) $a, b \in \mathbf{U}$ *impliziert* $ab \in \mathbf{U}$ *und* $a^{-1} \in \mathbf{U}$.

Beispiele:

- $m \in \mathbb{N}_0$, $(m) := \{nm : n \in \mathbb{Z}\}$ ist Untergruppe von $(\mathbb{Z}, +)$.
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist Untergruppe von $(\mathbb{R} \setminus \{0\}, \cdot)$ und diese wiederum von $(\mathbb{C} \setminus \{0\}, \cdot)$.

Folgerung 1.3 *Der Durchschnitt beliebig vieler Untergruppen einer Gruppe ist wieder eine Untergruppe.*

Sind $\mathbf{G}$ eine Gruppe und $X \subset \mathbf{G}$ eine nichtleere Teilmenge, so nennt man $\langle X \rangle := \bigcap_{\mathbf{U}\in\mathcal{G}} \mathbf{U}$, wobei

$$\mathcal{G} = \{\mathbf{U} : \mathbf{U} \text{ ist Untergruppe von } \mathbf{G} \text{ mit } X \subset \mathbf{U}\} ,$$

die von X erzeugte Untergruppe von $\mathbf{G}$. Man kann zeigen, dass $\langle X \rangle$ aus allen endlichen Produkten von Elementen aus $X \cup X^{-1}$ besteht. Eine von einem Element erzeugte Gruppe $\mathbf{G}$, d.h.

$$\exists g \in \mathbf{G} : \mathbf{G} = \langle g \rangle = \{g^n : n \in \mathbb{Z}\} ,$$

heißt **zyklische Gruppe**. (in additiver Schreibweise: $\langle g \rangle = \{ng : n \in \mathbb{Z}\}$)

Unter der **Ordnung** einer Gruppe $\mathbf{G}$ versteht man ihre Mächtigkeit $|G|$. Wir schreiben $|G| = \infty$, falls G unendlich viele Elemente hat. Ist $g \in \mathbf{G}$, so nennt man $\operatorname{ord} g := |\langle g \rangle|$ die **Ordnung** des Elementes g .

Beispiele:

- $(\mathbb{Z}, +)$ ist zyklische Gruppe unendlicher Ordnung, $\mathbb{Z} = \langle 1 \rangle$.
- $(\mathbb{Z}_m, +)$ ist zyklische Gruppe der Ordnung m , $\mathbb{Z}_m = \langle [1]_m \rangle$.
- $|\mathcal{S}_n| = n!$
- $|\mathbb{Q}| = \infty$

Satz 1.4 *Jede Untergruppe einer zyklischen Gruppe ist zyklisch.*

Folgerung 1.5 *Ist* $\mathbf{U}$ *eine Untergruppe von* $(\mathbb{Z}, +)$, *so existiert ein* $m \in \mathbb{N}_0$ *mit* $\mathbf{U} = (m)$.

Satz 1.6 *Es seien* $\mathbf{G}$ *eine Gruppe und* $g \in \mathbf{G}$ *mit* $\operatorname{ord} g = n \in \mathbb{N}$. *Dann gilt:*

(a) $\langle g \rangle = \left\{e, g, \ldots, g^{n-1}\right\}$, *und* n *ist die kleinste positive ganze Zahl mit* $g^n = e$.

(b) *Es gilt* $g^k = e$ *genau dann, wenn* $k \in (n)$.

(c) *Ist* $m \in \mathbb{N}$, *so* $\operatorname{ord} g^m = \dfrac{n}{\operatorname{ggT}(m, n)}$, *wobei* $\operatorname{ggT}(m, n)$ *den größten gemeinsamen Teiler von* m *und* n *bezeichnet.*

(d) *Für* $m \in \mathbb{N}$ *ist* $\langle g^m \rangle = \langle g \rangle$ *genau dann, wenn* $\operatorname{ggT}(m, n) = 1$.

(e) *Zu jedem Teiler* d *von* n *gibt es genau eine Untergruppe von* $\langle g \rangle$ *der Ordnung* d.

1.2 Homomorphismen

Definition 1.7 *Eine Abbildung* $\varphi : \mathbf{G}_1 \longrightarrow \mathbf{G}_2$ *zwischen zwei Gruppen* $\mathbf{G}_1$ *und* $\mathbf{G}_2$ *heißt* (*Gruppen-*)**Homomorphismus**, *wenn sie strukturverträglich ist, d.h., für beliebige* $a, b \in \mathbf{G}_1$ *gilt* $\varphi(ab) = \varphi(a)\varphi(b)$.

Beispiele:

- $(\mathbb{R}, +) \longrightarrow (\mathbb{R} \setminus \{0\}, \cdot)$, $x \mapsto e^x$
- $(\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_m, +)$, $x \mapsto [x]_m = x + (m)$

Definition 1.8 *Einen Homomorphismus* $\varphi : \mathbf{G}_1 \longrightarrow \mathbf{G}_2$ *nennt man*

- **Monomorphismus**, *wenn er injektiv ist,*
- **Epimorphismus**, *wenn er surjektiv ist,*
- **Isomorphismus**, *wenn er bijektiv ist,*
- **Endomorphismus**, *wenn* $\mathbf{G}_1 = \mathbf{G}_2$ *(mit der gleichen Verknüpfung) gilt,*
- **Automorphismus**, *wenn er ein bijektiver Endomorphismus ist.*

Definition 1.9 *Zwei Gruppen* $\mathbf{G}_1$ *und* $\mathbf{G}_2$ *nennt man zueinander* **isomorph**, *wenn ein Isomorphismus* $\varphi : \mathbf{G}_1 \longrightarrow \mathbf{G}_2$ *existiert. In Zeichen:* $\mathbf{G}_1 \cong \mathbf{G}_2$

Es seien $\varphi : \mathbf{G}_1 \longrightarrow \mathbf{G}_2$ ein Homomorphismus und e_j das neutrale Element in $\mathbf{G}_j$. Dann gelten folgende Aussagen:

1. $\varphi(e_1) = e_2$.
2. $\varphi(a^{-1}) = [\varphi(a)]^{-1}$, $a \in \mathbf{G}_1$,
3. $\varphi(a^n) = [\varphi(a)]^n$, $a \in \mathbf{G}_1$, $n \in \mathbb{Z}$,
4. Sind $\mathbf{G}_1' \subset \mathbf{G}_1$ und $\mathbf{G}_2' \subset \mathbf{G}_2$ Untergruppen von $\mathbf{G}_1$ bzw. $\mathbf{G}_2$, so sind das **Bild** $\varphi(\mathbf{G}_1') = \{\varphi(a) : a \in \mathbf{G}_1'\}$ und das **Urbild** $\varphi^{-1}(\mathbf{G}_2') = \{a \in \mathbf{G}_1 : \varphi(a) \in \mathbf{G}_2'\}$ Untergruppen von $\mathbf{G}_2$ bzw. $\mathbf{G}_1$.
5. Der **Kern** $\ker\varphi = \{a \in \mathbf{G}_1 : \varphi(a) = e_2\}$ des Homomorphismus φ ist eine Untergruppe der Gruppe $\mathbf{G}_1$.
6. Der Homomorphismus $\varphi : \mathbf{G}_1 \longrightarrow \mathbf{G}_2$ ist genau dann injektiv, wenn $\ker\varphi = \{e_1\}$ gilt.
7. Ist $\varphi : \mathbf{G}_1 \longrightarrow \mathbf{G}_2$ ein Isomorphismus, so gilt dies auch für $\varphi^{-1} : \mathbf{G}_2 \longrightarrow \mathbf{G}_1$.

Offenbar ist die Verkettung von Homomorphismen ein Homomorphismus, also die Verkettung von Isomorphismen ein Isomorphismus, woraus unter Verwendung von 7. folgt, dass "$\cong$" (vgl. Definition 1.9) eine Äquivalenzrelation auf der Menge der Gruppen definiert.

Mit $(\mathrm{Aut}\,\mathbf{G}, \circ)$ bezeichnen wir die **Automorphismengruppe** der Gruppe $\mathbf{G}$, die ja eine Untergruppe der symmetrischen Gruppe $(S(\mathbf{G}), \circ)$ ist. Spezielle Elemente der Automorphismengruppe sind die **inneren Automorphismen**. Das sind die Automorphismen $\varphi : \mathbf{G} \longrightarrow \mathbf{G}$, für die ein $x \in \mathbf{G}$ existiert, so dass $\varphi(b) = xbx^{-1} =: \varphi_x(b)$ für alle $b \in \mathbf{G}$ gilt. Die Abbildung $\Phi : \mathbf{G} \longrightarrow \mathrm{Aut}\,\mathbf{G}$, $x \mapsto \varphi_x$ ist ein Homomorphismus. Der Kern dieses Homomorphismus ist gleich

$$\ker\Phi = \{x \in \mathbf{G} : xy = yx \ \forall y \in \mathbf{G}\} =: Z(\mathbf{G})$$

und wird **Zentrum** der Gruppe $\mathbf{G}$ genannt.

Satz 1.10 *Sind M_1 und M_2 nichtleere Mengen gleicher Mächtigkeit, so gilt $\mathcal{S}(M_1) \cong \mathcal{S}(M_2)$.*

Satz 1.11 (Cayley) *Jede Gruppe $\mathbf{G}$ ist isomorph zu einer Untergruppe von $\mathcal{S}(\mathbf{G})$.*

Folgerung 1.12 *Jede Gruppe der Ordnung $n \in \mathbb{N}$ ist isomorph zu einer Untergruppe von $\mathcal{S}_n$.*

Beispiel 1.13 *Sind $\mathbf{G}$ eine Gruppe, $f : X \longrightarrow \mathbf{G}$ eine bijektive Abbildung und*

$$x \circ y := f^{-1}\big(f(x)f(y)\big),$$

so ist $(X, \circ)$ eine zu $\mathbf{G}$ isomorphe Gruppe.

1.3 Faktorgruppen und Isomorphiesätze

Satz 1.14 *Es seien* $\mathbf{G}$ *eine Gruppe und* $\mathbf{U} \subset \mathbf{G}$ *eine Untergruppe.*

(a) *Die Relation* $\mathcal{R} = \mathcal{R}_{\mathbf{U}} = \left\{(x,y) \in \mathbf{G} \times \mathbf{G} : xy^{-1} \in \mathbf{U}\right\}$ *ist eine Äquivalenzrelation auf* $\mathbf{G}$, *die mit der Multiplikation auf* $\mathbf{G}$ **rechtsverträglich** *ist, d.h.* $(xg, yg) \in \mathcal{R}_{\mathbf{U}}\ \forall (x,y) \in \mathcal{R}_{\mathbf{U}}$, $\forall g \in \mathbf{G}$.

(b) *Für die Äquivalenzklassen gilt* $[x]_{\mathcal{R}} = \mathbf{U}x := \{ux : u \in \mathbf{U}\}$.

(c) *Die Abbildung* $\mathbf{U}x \longrightarrow \mathbf{U}y$, $ux \mapsto uy$ *ist korrrekt definiert und bijektiv.*

(d) $|\mathbf{U}x| = |\mathbf{U}| \quad \forall x \in \mathbf{G}$.

Die Äquivalenzklassen $\mathbf{U}x$ nennt man **Rechtsnebenklassen modulo U**.

Folgerung 1.15 *Es seien* $\mathbf{G}$ *eine Gruppe und* $\mathbf{U} \subset \mathbf{G}$ *eine Untergruppe.*

(a) $\mathbf{G} = \bigcup\limits_{x \in \mathbf{G}} \mathbf{U}x$

(b) $\mathbf{U}x \cap \mathbf{U}y \neq \emptyset \iff xy^{-1} \in \mathbf{U} \iff \mathbf{U}x = \mathbf{U}y$

(c) $\mathbf{U}x = \mathbf{U} \iff x \in \mathbf{U}$

Beispiele:

- $m \in \mathbb{N}$: $\mathbf{G} = (\mathbb{Z}, +)$, $\mathbf{U} = (m)$
- $\mathbf{G} = \mathcal{S}_4$, $\mathbf{U} = \{\sigma \in \mathcal{S}_4 : \sigma(1) = 1\}$

Definition 1.16 *Unter dem* **Index** *einer Untergruppe* $\mathbf{U}$ *einer Gruppe* $\mathbf{G}$ *versteht man die Anzahl der verschiedenen Rechtsnebenklassen modulo* $\mathbf{U}$ *und bezeichnet diese Zahl mit* $|\mathbf{G} : \mathbf{U}|$.

Satz 1.17 (Lagrange) *Es seien* $\mathbf{U}$ *eine Untergruppe der Gruppe* $\mathbf{G}$ *und wenigstens zwei der Zahlen* $|\mathbf{G}|$, $|\mathbf{U}|$ *und* $|\mathbf{G} : \mathbf{U}|$ *endlich. Dann gilt* $|\mathbf{G}| = |\mathbf{G} : \mathbf{U}| \cdot |\mathbf{U}|$.

Folgerung 1.18 *Es seien* $\mathbf{G}$ *eine endliche Gruppe und* $\mathbf{U} \subset \mathbf{G}$ *eine Untergruppe. Dann gilt*

(a) $|\mathbf{U}|$ *ist Teiler von* $|\mathbf{G}|$,

(b) $\operatorname{ord} g$ *ist Teiler von* $|\mathbf{G}|$ *für jedes* $g \in \mathbf{G}$,

(c) $x^{|\mathbf{G}|} = e \quad \forall x \in \mathbf{G}$ (**kleiner Fermat'scher Satz**).

(d) *Ist* $|\mathbf{G}|$ *eine Primzahl, so ist* $\mathbf{G}$ *zyklisch.*

(e) *Ist* $\mathbf{V} \subset \mathbf{G}$ *eine weitere Untergruppe von* $\mathbf{G}$ *mit zu* $|\mathbf{U}|$ *teilerfremder Ordnung, so gilt* $\mathbf{U} \cap \mathbf{V} = \{e\}$.

(f) *Sind* $\mathbf{V} \subset \mathbf{U}$ *eine weitere Untergruppe von* $\mathbf{G}$ *und wenigstens zwei der Zahlen* $|\mathbf{G} : \mathbf{U}|$, $|\mathbf{G} : \mathbf{V}|$ *und* $|\mathbf{U} : \mathbf{V}|$ *endlich, so gilt* $|\mathbf{G} : \mathbf{V}| = |\mathbf{G} : \mathbf{U}| \cdot |\mathbf{U} : \mathbf{V}|$.

Analog zu Satz 1.14 kann man die Menge der Linksnebenklassen modulo $\mathbf{U}$ definieren. Der Satz von Lagrange (Satz 1.17) zeigt, dass die Zahl der Linksnebenklassen gleich der der Rechtnebenklassen ist und dass somit die Definition des Index $|\mathbf{G} : \mathbf{U}|$ unabhängig davon ist, ob man rechts- oder Linksnebenklassen betrachtet.

Definition 1.19 *Wir nennen eine Untergruppe* $\mathbf{U}$ *einer Gruppe* $\mathbf{G}$ **Normalteiler**, *wenn für alle* $g \in \mathbf{G}$ *gilt* $g\mathbf{U}g^{-1} \subset \mathbf{U}$.

Beispiele:

- Jede Untergruppe einer abelschen Gruppe ist Normalteiler, z.B. $(m) \subset (\mathbb{Z}, +)$.
- $\mathbf{G} = G\mathbb{C}^{m\times m}$, $\mathbf{U} = \{A \in \mathbf{G} : \det(A) = 1\}$

Folgende Bedingungen sind zur Normalteilereigenschaft äquivalent:

- $g\mathbf{U}g^{-1} = \mathbf{U} \quad \forall g \in \mathbf{G}$
- $g\mathbf{U} = \mathbf{U}g \quad \forall g \in \mathbf{G}$
- $g\mathbf{U} \subset \mathbf{U}g \quad \forall g \in \mathbf{G}$
- $\forall x, y \in \mathbf{G}$: $xy^{-1} \in \mathbf{U} \iff x^{-1}y \in \mathbf{U}$

Ist $\mathbf{U}$ ein Normalteiler in $\mathbf{G}$, so bezeichnen wir mit $\mathbf{G}/\mathbf{U}$ die Menge aller Nebenklassen modulu $\mathbf{U}$ und versehen diese mit der Vernüpfung $(\mathbf{G}/\mathbf{U}) \times (\mathbf{G}/\mathbf{U}) \longrightarrow \mathbf{G}/\mathbf{U}$, $(x\mathbf{U}, y\mathbf{U}) \mapsto (xy)\mathbf{U}$.

Satz 1.20 *Ist* $\mathbf{U}$ *ein Normalteiler in* $\mathbf{G}$, *so ist* $(\mathbf{G}/\mathbf{U}, \cdot)$ *eine Gruppe, die* **Faktorgruppe** G *modulo* $\mathbf{U}$, *wobei* $|\mathbf{G}/\mathbf{U}| = |\mathbf{G} : \mathbf{U}|$. *Die Abbildung* $\pi : \mathbf{G} \longrightarrow \mathbf{G}/\mathbf{U}$, $g \mapsto g\mathbf{U}$ *ist ein Epimorphismus mit* $\ker \pi = \mathbf{U}$.

Den Epimorphismus π nennt man auch **kanonischen Epimorphismus**.

Folgerung 1.21 *Es seien* $\mathbf{G}$ *eine Gruppe und* $\mathbf{U} \subset \mathbf{G}$ *eine Untergruppe.*

(a) $\mathbf{U}$ *ist genau dann Normalteiler in* $\mathbf{G}$, *wenn ein Homomorphismus* $\varphi : \mathbf{G} \longrightarrow \mathbf{H}$ *mit* $\ker \varphi = \mathbf{U}$ *existiert.*

(b) *Ist* $\varphi : \mathbf{G} \longrightarrow \mathbf{H}$ *ein Homomorphismus, so gilt* $\mathbf{G}/\ker \varphi \cong \varphi(\mathbf{G})$. (**Homomorphiesatz**)

(c) *Für jedes* $n \in \mathbb{N}$ *existiert genau eine* (*bis auf Isomorphie*) *zyklische Gruppe der Ordnung* n, *nämlich* $(\mathbb{Z}_n, +)$. *Jede unendliche zyklische Gruppe ist isomorph zu* $(\mathbb{Z}, +)$.

(d) *Ist* $\varphi : \mathbf{G} \longrightarrow \mathbf{H}$ *ein Monomorphismus, so gilt* $\mathbf{G} \cong \varphi(\mathbf{G})$.

(e) *Ist* $\mathbf{V}$ *ein Normalteiler in* $\mathbf{G}$, *so sind* $\mathbf{UV}$ *eine Untergruppe von* $\mathbf{G}$ *und* $\mathbf{U} \cap \mathbf{V}$ *ein Normalteiler in* $\mathbf{U}$. *Dabei gilt* $\mathbf{UV}/\mathbf{V} \cong \mathbf{U}/(\mathbf{U} \cap \mathbf{V})$. (**erster Isomorphiesatz**)

(f) *Sind* $\mathbf{U}$ *und* $\mathbf{V}$ *Normalteiler in* $\mathbf{G}$ *mit* $\mathbf{U} \subset \mathbf{V}$, *so ist* $\mathbf{V}/\mathbf{U}$ *Normalteiler in* $\mathbf{G}/\mathbf{U}$, *wobei* $(\mathbf{G}/\mathbf{U})/(\mathbf{V}/\mathbf{U}) \cong \mathbf{G}/\mathbf{V}$ *gilt.* (**zweiter Isomorphiesatz**)

Beispiel 1.22 *Es gibt* (*bis auf Isomorphie*) *genau zwei Gruppen der Ordnung* 4, *die zyklische Gruppe der Ordnung* 4 *und die* **Klein'sche Vierergruppe** $\mathbf{V}_4$.

Beispiel 1.23 *Es seien* $\mathbf{G} = (\mathbb{R}, +)$, $\mathbf{H} = (\mathbb{T}, \cdot)$ ($\mathbb{T}$ - *Einheitskreis*) *und* $\varphi : \mathbf{G} \longrightarrow \mathbf{H}$, $x \mapsto e^{2\pi \mathbf{i} x}$. *Es folgt* $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$.

Beispiel 1.24 *Es seien* $\mathbf{G} = (\mathbf{O}\mathbb{R}^{m\times m}, \cdot)$ *die Gruppe der orthogonalen Matrizen der Ordnung* m, $\mathbf{H} = (\{-1, 1\}, \cdot)$ *und* $\varphi : \mathbf{G} \longrightarrow \mathbf{H}$, $A \mapsto \det(A)$. *Es folgt*

$$\ker \varphi = \left\{ A \in \mathbf{O}\mathbb{R}^{m\times m} : \det(A) = 1 \right\} =: \mathbf{SO}\mathbb{R}^{m\times m}$$

und $\mathbf{O}\mathbb{R}^{m\times m}/\mathbf{SO}\mathbb{R}^{m\times m} \cong \mathbf{H} \cong (\mathbb{Z}_1, +)$.

1.4 Die Sylow'schen Sätze

Definition 1.25 *Man sagt, eine Gruppe* $\mathbf{G}$ **operiert** *auf einer nichtleeren Menge* X, *wenn eine Abbildung* $\mathbf{G} \times X \longrightarrow X$, $(g, x) \mapsto g \bullet x$ *mit folgenden Eigenschaften gegeben ist:*

(O1) $h \bullet (g \bullet x) = (hg) \bullet x \ \forall\, h, g \in \mathbf{G}, \forall\, x \in X$,

(O2) $e \bullet x = x \ \forall\, x \in X$.

Beispiele:

(B1) Mittels $g \bullet x := x$ operiert jede Gruppe $\mathbf{G}$ auf jeder nichtleeren Menge X.

(B2) Die Gruppe $\mathbf{G} = (\mathbb{R}, +)$ operiert auf $X = \mathbb{R}^2$ mittels $t \bullet x := x + t x_0$, wobei $x_0 \in \mathbb{R}^2 \setminus \{\Theta\}$ ein fest gewählter Vektor ist.

(B3) Die Gruppe $\mathbf{G} = (\mathbb{R}, +)$ operiert auf $X = \mathbb{C}$ mittels $t \bullet z := e^{\mathbf{i}t} z$.

Operiert $\mathbf{G}$ auf X, so ist

$$R(\mathbf{G}) = \{(x, y) \in X \times X : \exists\, g \in \mathbf{G} \text{ mit } g \bullet x = y\}$$

eine Äquivalenzrelation auf X. Die Äquivalenzklassen bzgl. $R(\mathbf{G})$ nennt man **Orbits**. Für $x \in X$ ist

$$[x]_{R(\mathbf{G})} = \{g \bullet x : g \in \mathbf{G}\} =: \mathbf{G} \bullet x\,.$$

Im Beispiel (B1) sind die Orbits alle einelementigen Teilmengen von X, im Beispiel (B2) sind es zueinander parallele Geraden, und im Beispiel (B3) sind es die Kreislinien um den Koordinatenursprung.

Beispiel:

(B4) Die Gruppe $\mathbf{G} = (\mathbb{Z}^2, +)$ operiert auf $X = \mathbb{R}^2$ mittels $(m,n) \bullet (x,y) := (x+m, y+n)$. Die Orbits sind Punktegitter $[(x,y)]_{R(\mathbf{G})} = \big\{(x+m, y+n) : (m,n) \in \mathbb{Z}^2\big\}$.

Operiert $\mathbf{G}$ auf X, so nennt man $\mathbf{G}_x := \{g \in \mathbf{G} : g \bullet x = x\}$ den **Stabilisator** von $x \in X$ in $\mathbf{G}$. Er ist eine Untergruppe von $\mathbf{G}$. Die Abbildung $g \bullet x \mapsto g\mathbf{G}_x$ ist eine wohldefinierte und bijektive Abbildung des Orbits $\mathbf{G} \bullet x$ auf die Menge der Linksnebenklassen modulo $\mathbf{G}_x$. Es gilt also

$$|\mathbf{G} \bullet x| = |\mathbf{G} : \mathbf{G}_x| \quad \forall\, x \in \ X\,. \tag{1.1}$$

Im Fall einer endlichen Gruppe $\mathbf{G}$ ist also $|\mathbf{G} \bullet x|$ ein Teiler der Gruppenordnung $|\mathbf{G}|$. Unter einem **Repräsentantensystem** $V \subset X$ verstehen wir eine Menge, die aus jedem Orbit genau ein Element enthält. Ein $x \in X$ heißt **Fixpunkt** unter der vorliegenden Gruppenoperation, wenn $g \bullet x = x$ für alle $g \in \mathbf{G}$ gilt. Die Menge aller dieser Fixpunkte bezeichnen wir mit $\mathrm{Fix}_{\mathbf{G}}(X)$. Ist V ein Repräsentantensystem, so gilt

$$|X| = |\mathrm{Fix}_{\mathbf{G}}(X)| + \sum_{x \in V : |\mathbf{G}:\mathbf{G}_x| > 1} |\mathbf{G} : \mathbf{G}_x|\,. \tag{1.2}$$

Satz 1.26 *Es sei p eine Primzahl. Eine Gruppe $\mathbf{G}$ der Ordnung p^r operiere auf der endlichen Menge X. Dann gilt*

$$|X| \equiv |\mathrm{Fix}_{\mathbf{G}}(X)| \mod p\,.$$

Sind außerdem $|X|$ und p teilerfremd, so existiert wenigstens ein Fixpunkt.

Beispiele:

(B5) Es seien $\mathbf{G}$ eine Gruppe, $X \subset \mathbf{G}$ nichtleer und $X_{\mathbf{G}} = \big\{gXg^{-1} : g \in \mathbf{G}\big\}$ die Menge der zu X **konjugierten** Teilmengen von $\mathbf{G}$. Die Gruppe $\mathbf{G}$ operiert auf $X_{\mathbf{G}}$ mittels $h \bullet Y := hYh^{-1}$. Es folgt $\mathbf{G} \bullet Y = X_{\mathbf{G}}$ für alle $Y \in X_{\mathbf{G}}$. Es gibt also nur einen Orbit, $X_{\mathbf{G}}$ selbst. Der Stabilisator von X in $\mathbf{G}$ ist gleich

$$\mathbf{G}_X = \big\{g \in \mathbf{G} : gXg^{-1} = X\big\} = \{g \in \mathbf{G} : gX = Xg\} =: \mathbf{N}(X)\,.$$

$\mathbf{N}(X)$ wird der **Normalisator** von X in $\mathbf{G}$ genannt. Es folgt

$$|X_{\mathbf{G}}| = |\mathbf{G} : \mathbf{N}(X)|\,. \tag{1.3}$$

(B6) Eine Gruppe $\mathbf{G}$ operiert auf sich selbst ($X = \mathbf{G}$) vermöge der Abbildungsvorschrift $g \bullet x := gxg^{-1}$. Die Orbits sind hierbei Klassen zueinander **konjugierter** Elemente, $\mathbf{G} \bullet x = \left\{gxg^{-1} : g \in \mathbf{G}\right\}$. Der Stabilisator $\mathbf{G}_x$ ist gleich dem Normalisator $\mathbf{N}(x)$ von $x \in \mathbf{G}$ in $\mathbf{G}$, $\mathbf{N}(x) = \{g \in \mathbf{G} : gx = xg\}$. Aus $\mathrm{Fix}_{\mathbf{G}}(\mathbf{G}) = \left\{x \in \mathbf{G} : gxg^{-1} = x \,\forall\, g \in \mathbf{G}\right\} = Z(\mathbf{G})$ und (1.2) folgt

$$|G| = |Z(\mathbf{G})| + \sum_{x \in V : |\mathbf{G}:\mathbf{N}(x)| > 1} |\mathbf{G} : \mathbf{N}(x)| \tag{1.4}$$

für jedes Repräsentantensystem $V \subset \mathbf{G}$.

Aus den Beispielen (B5) und (B6) ergeben sich zwei Folgerungen.

Folgerung 1.27 *Die Anzahl der zu einer Untergruppe $\mathbf{U} \subset \mathbf{G}$ konjugierten Untergruppen ist gleich dem Index des Normalisators von $\mathbf{U}$ in $\mathbf{G}$.*

Folgerung 1.28 *Ist $\mathbf{G}$ eine Gruppe der Ordnung p^r, p - Primzahl, $r \in \mathbb{N}$, so hat $\mathbf{G}$ ein nichttriviales Zentrum.*

Lemma 1.29 *Sind $m, n, r \in \mathbb{N}$, p eine Primzahl, $n = p^r m$ und $\mathrm{ggT}(p, m) = 1$, so ist p^{r-s+1} kein Teiler von $\binom{n}{p^s}$ für jedes $s \in \{1, \ldots, r\}$.*

Satz 1.30 (Erster Sylow'scher Satz) *Es seien $m, r \in \mathbb{N}$, p eine Primzahl, $\mathrm{ggT}(p, m) = 1$ und $\mathbf{G}$ eine Gruppe der Ordnung $n = p^r m$. Dann gibt es zu jedem $s \in \{1, \ldots, r\}$ eine Untergruppe von $\mathbf{G}$ der Ordnung p^s.*

Folgerung 1.31 (Satz von Cauchy) *Ist die Primzahl p Teiler der Gruppenordnung $|\mathbf{G}|$, so gibt es in $\mathbf{G}$ ein Element der Ordnung p.*

Definition 1.32 *Es sei p eine Primzahl. Man nennt eine Gruppe $\mathbf{G}$ eine* **p-Gruppe**, *wenn die Ordnung eines jeden Elementes von $\mathbf{G}$ eine Potenz von p ist. Eine Untergruppe $\mathbf{U} \subset \mathbf{G}$ heißt* **p-Sylow-Gruppe** *von $\mathbf{G}$, wenn $\mathbf{U}$ eine p-Gruppe ist und es keine $\mathbf{U}$ echt umfassende p-Untergruppe von $\mathbf{G}$ gibt.*

Nach Satz 1.6,(b) gilt $a^k = e$ genau dann, wenn k ein Vielfaches der Ordnung von a ist. Deshalb ist $\mathbf{G}$ genau dann eine p-Gruppe, wenn zu jedem $a \in \mathbf{G}$ ein $k \in \mathbb{N}_0$ existiert, so dass $a^{p^k} = e$ ist.

Folgerung 1.33 *Es seien $\mathbf{G}$ eine endliche Gruppe und p eine Primzahl.*

(a) *$\mathbf{G}$ ist genau dann eine p-Gruppe, wenn $|\mathbf{G}|$ eine Potenz von p ist.*

(b) *Ist $|\mathbf{G}| = p^r m$, $\mathrm{ggT}(p, m) = 1$, so ist jede Untergruppe von $\mathbf{G}$ der Ordnung p^r eine p-Sylow-Gruppe von $\mathbf{G}$, wobei wenigstens eine solche p-Sylow-Gruppe existiert.*

(c) *Ist* $\mathbf{U} \subset \mathbf{G}$ *eine p-Untergruppe (bzw. p-Sylow-Gruppe) von* $\mathbf{G}$, *so ist jede zu* $\mathbf{U}$ *konjugierte Untergruppe p-Untergruppe (bzw. p-Sylow-Gruppe) von* $\mathbf{G}$. *(Hierbei muss* $\mathbf{G}$ *nicht endlich sein!)*

Satz 1.34 (Zweiter Sylow'scher Satz) *Es seien* p *eine Primzahl,* $r, m \in \mathbb{N}$, $|\mathbf{G}| = p^r m$, $\mathrm{ggT}(p, m) = 1$ *und* $\mathbf{U} \subset \mathbf{G}$ *eine p-Sylow-Gruppe von* $\mathbf{G}$. *Ist* $\mathbf{V} \subset \mathbf{G}$ *eine p-Gruppe, so existiert ein* $a \in \mathbf{G}$ *mit* $a\mathbf{V}a^{-1} \subset \mathbf{U}$.

Folgerung 1.35 *Unter den Voraussetzungen von Satz 1.34 gilt:*

(a) *Alle p-Sylow-Gruppen von* $\mathbf{G}$ *sind zueinander konjugiert und haben die Ordnung* p^r.

(b) *Eine p-Sylowgruppe von* $\mathbf{G}$ *ist genau dann Normalteiler in* $\mathbf{G}$, *wenn sie die einzige p-Sylow-Gruppe von* $\mathbf{G}$ *ist.*

Lemma 1.36 *Es seien* $\mathbf{U} \subset \mathbf{G}$ *eine p-Sylow-Gruppe von* $\mathbf{G}$ *und* $a \in \mathbf{G}$. *Dann gilt:*

(a) *Ist* $a \in N(\mathbf{U})$ *und hat* $[a]_{\mathbf{U}} \in N(\mathbf{U})/\mathbf{U}$ *eine p-Potenz als Ordnung, so ist* $[a]_{\mathbf{U}} = \mathbf{U}$.

(b) *Hat* a *eine p-Potenz als Ordnung und ist* $a\mathbf{U}a^{-1} = \mathbf{U}$, *so folgt* $a \in \mathbf{U}$.

Satz 1.37 (Dritter Sylow'scher Satz) *Es sei* $\mathbf{G}$ *eine endliche Gruppe, deren Ordnung durch die Primzahl* p *teilbar ist. Dann ist die Anzahl der p-Sylow-Gruppen von* $\mathbf{G}$ *ein Teiler von* $|\mathbf{G}|$ *und von der Form* $1 + kp$ *mit einem* $k \in \mathbb{N}_0$.

Beispiele zur Anwendung der Sylow'schen Sätze: Es sei stets p eine Primzahl.

(A1) Eine Gruppe der Ordnung p^2 ist abelsch.

(A2) Ist eine Gruppe der Ordnung p^2 nicht zyklisch, so ist sie isomorph zu $\mathbb{Z}_p \times \mathbb{Z}_p$.

(A3) Jede Gruppe $\mathbf{G}$ der Ordnung p^r, $r \in \mathbb{N}$ besitzt einen Normalteiler der Ordnung p^{r-1}. Es gibt somit eine Folge von Untergruppen

$$\{e\} = \mathbf{U}_0 \subset \mathbf{U}_1 \subset \ldots \subset \mathbf{U}_{r-1} \subset \mathbf{U}_r = \mathbf{G},$$

so dass $|\mathbf{U}_j| = p^j$ und $\mathbf{U}_{j-1}$ Normalteiler in $\mathbf{U}_j$ ist.

(A4) Sind p und q Primzahlen mit $p < q$ und $\mathbf{G}$ eine Gruppe der Ordnung pq, so gibt es genau eine q-Sylow-Gruppe von $\mathbf{G}$. Gilt außerdem $q \notin \{1 + kp : k \in \mathbb{N}\}$, so gibt es auch nur eine p-Sylow-Gruppe von $\mathbf{G}$. In diesem Fall ist $\mathbf{G}$ isomorph zur Gruppe $\mathbb{Z}_p \times \mathbb{Z}_q$, die wiederum isomorph zu $\mathbb{Z}_{pq}$ ist.

1.5 Die symmetrischen Gruppen $\mathcal{S}_n$

Wir fassen $\mathcal{S}_n$ auch als Untergruppe von $\mathcal{S}(\mathbb{N})$ auf.

Definition 1.38 *Eine Permutation $f \in \mathcal{S}(\mathbb{N})$ nennen wir r-**Zykel**, wenn r paarweise verschiedene Zahlen $j_1, \ldots, j_r \in \mathbb{N}$ existieren, so dass*

$$f(j_k) = j_{k+1}\,,\ k = 1, \ldots, r-1\,, \quad f(j_r) = j_1 \quad \textit{und} \quad f(m) = m\ \forall\, m \in \mathbb{N} \setminus \{j_1, \ldots, j_r\}$$

gilt. Wir schreiben dann f in der Form $(j_1, \ldots, j_r)$. Ein 2-Zykel (j_1, j_2) heißt **Transposition**. *Für die identische Abbildung $f = \mathrm{id}$ schreiben wir (1). Wir sagen, dass zwei Zykeln $(j_1, \ldots, j_r)$ und $(k_1, \ldots, k_s)$* **disjunkt** *sind, wenn $\{j_1, \ldots, j_r\} \cap \{k_1, \ldots, k_s\} = \emptyset$ gilt.*

Rechenregeln:

(Z1) $(j_1, j_2, \ldots, j_r) = (j_2, j_3, \ldots, j_r, j_1) = \ldots = (j_r, j_1, \ldots, j_{r-1})$,

(Z2) $(j_1, \ldots, j_r) = (j_1, \ldots, j_k) \circ (j_k, \ldots, j_r)\,,\ 2 \le k \le r-1$,

(Z3) $(j_1, \ldots, j_r) = (j_1, j_2) \circ (j_2, j_3) \circ \ldots \circ (j_{r-1}, j_r)$,

(Z4) $(j_1, \ldots, j_r)^m = \begin{pmatrix} j_1, \ldots, j_r \\ j_{m+1}, \ldots, j_{m+r} \end{pmatrix}$, wobei $j_{m+s} := j_{(m+s \mod r)}$, also $\operatorname{ord}(j_1, \ldots, j_r) = r$,

(Z5) $(j_1, \ldots, j_r)^{-1} = (j_r, \ldots, j_1)$,

(Z6) $f \circ (j_1, \ldots, j_r) \circ f^{-1} = \big(f(j_1), \ldots, f(j_r)\big)\ \forall\, f \in \mathcal{S}(\mathbb{N})$.

(Z7) Disjunkte Zykeln sind vertauschbar.

Folgerung 1.39 *Für $n \in \mathbb{N}$ definieren wir $f_k = (k, n+1)$, $k \in \{1, \ldots, n\}$ und $f_{n+1} = (1)$. Dann sind die Nebenklassen $f_k \circ \mathcal{S}_n$, $k = 1, \ldots, n$ paarweise disjunkt, und es gilt*

$$\mathcal{S}_{n+1} = \bigcup_{k=1}^{n+1} f_k \circ \mathcal{S}_n\,.$$

Folgerung 1.40 *Sei $n \in \mathbb{N}$.*

(a) $|\mathcal{S}_{n+1} : \mathcal{S}_n| = n+1$ *und* $|\mathcal{S}_n| = n!$

(b) $\mathcal{S}_n = \langle \{(1,2), (1,3), \ldots, (1,n)\} \rangle$

Sind $g \in \mathcal{S}_n$, $\alpha = \operatorname{ord} g$ und $\mathbf{G} = \langle g \rangle$, so operiert $\mathbf{G}$ auf $X = \{1, 2, \ldots, n\}$ mittels $(h, m) \mapsto h \bullet m := h(m)$. Die Orbits sind dabei von der Gestalt

$$\mathbf{G} \bullet m = \{h(m) : h \in \langle g \rangle\} = \big\{m, g(m), \ldots, g^{\alpha-1}(m)\big\}\ .$$

Ist $g = (j_1, \ldots, j_r)$ ein Zykel mit $r \ge 2$, so ist $\{j_1, \ldots, j_r\}$ der einzige Orbit, der mehr als ein Element von X enthält. Ist umgekehrt $\mathbf{G} \bullet j = \big\{j, g(j), \ldots, g^{\beta-1}(j)\big\}$ der einzige Orbit mit mehr als einem Element, so folgt $g = \big(j, g(j), \ldots, g^{\beta-1}(j)\big)$.

Folgerung 1.41 *Jede Permutation $f \in \mathcal{S}_n$ ist (bis auf die Reihenfolge der Faktoren) eindeutig als Produkt paarweise disjunkter Zykeln darstellbar (***kanonische Faktorisierung** *einer Permutation).*

Beweis. Seien also $f \in \mathcal{S}_n$, $\mathbf{G} = \langle f \rangle$, $X = \{1, 2, \ldots, n\}$ und $X = \bigcup_{k=1}^{s} X_k$ mit paarweise disjunkten Orbits $X_k = \left\{ f^i(m_k) : i = 0, \ldots, \operatorname{ord} f - 1 \right\}$ (bzgl. obiger Operation $\mathbf{G} \times X \longrightarrow X$, $m \mapsto h \bullet m := h(m)$). Wir definiern $f_k \in S_n$ durch

$$f_k(j) = \begin{cases} f(j) & : \quad j \in X_k \,, \\ j & : \quad j \notin X_k \,. \end{cases}$$

Besteht X_k aus nur einem Element, so ist $f|_{X_k} = \mathrm{id}$, also $f_k = \mathrm{id}$. Seien o.E.d.A. $X_1, \ldots, X_r$ die Orbits, die mehr als ein Element enthalten. Dann sind nach obigen Überlegungen die f_k, $k = 1, \ldots, r$ paarweise disjunkte Zykeln und $f = f_1 \circ \ldots \circ f_r$.

Es sei nun $f = g_1 \circ \ldots \circ g_t$ eine weitere Faktorisierung von f in paarweise disjunkte Zykeln. Mit Y_k bezeichnen wir den nichtrivialen orbit des Zykels g_k. Dann ist Y_k auch (nichttrivialer) Orbit von f, und f hat keine weiteren nichttrivialen Orbits, so dass (nach evtl. Umnumerierung) $Y_k = X_k$, $k = 1, \ldots, t = r$. Nun ist aber auch

$$g_k(j) = \left\{ \begin{array}{rcl} f(j) & : & j \in Y_k = X_k \\ j & : & j \notin Y_k = X_k \end{array} \right\} = f_k(j) \,, \quad j \in \{1, \ldots, n\} \,, \; k = 1, \ldots, r \,,$$

also $g_k = f_k$, $k = 1, \ldots, r$. □

Beispiele:

- $\begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 2\,5\,6\,4\,7\,3\,1 \end{pmatrix} = (1, 2, 5, 7) \circ (3, 6)$
- $(1, 4, 7, 6, 3) \circ (2, 4, 3) \circ (4, 5, 8, 1) = (2, 7, 6, 3) \circ (4, 5, 8)$
- $[(2, 4, 3) \circ ((1, 5, 6, 8)]^{17} = (2, 3, 4) \circ (1, 5, 6, 8)$

Beispiel 1.42 *Wir bestimmen verschiedene Untergruppen der $\mathcal{S}_3$ und der $\mathcal{S}_4$.*

Satz 1.43 *Sei $n \in \mathbb{N} \setminus \{1\}$. Die Abbildung*

$$\varepsilon : \mathcal{S}_n \longrightarrow \{1, -1\} \,, \quad f \mapsto \varepsilon(f) := \prod_{1 \le j < k \le n} \frac{f(j) - f(k)}{j - k}$$

ist ein Epimorphismus von $\mathcal{S}_n$ auf die Untergruppe $(\{1, -1\}, \cdot)$ der Gruppe $(\mathbb{R} \setminus \{0\}, \cdot)$. Dabei gilt $\varepsilon(f) = (-1)^r$, falls f als Produkt von r Transpositionen darstellbar ist.

Man nennt $\varepsilon(f)$ die **Signatur** der Permutation $f \in \mathcal{S}_n$ und f **gerade** bzw. **ungerade**, falls $\varepsilon(f) = 1$ bzw. $\varepsilon(f) = -1$ ist.

Beispiel:

- (1) ist gerade.
- $\varepsilon((j_1,\ldots,j_r)) = \varepsilon((j_1,j_2)\circ\ldots\circ(j_{r-1},j_r)) = \varepsilon((j_1,j_2))\cdots\varepsilon((j_{r-1},j_r)) = (-1)^{r-1}$

Die Menge aller geraden Permutation $\mathcal{A}_n \subset \mathcal{S}_n$ ist ein Normalteiler in $\mathcal{S}_n$ der Ordnung $n!/2$ und wird **alternierende Gruppe** vom Grad n genannt.

Eine Gruppe **G** heißt **einfach**, wenn sie mindestens zwei Elemente enthält und nur $\{e\}$ und **G** als Normalteiler besitzt.

Beispiel:

- Die alternierende Gruppe $\mathcal{A}_4$ ist Untergruppe der Ordnung 12 der $\mathcal{S}_4$.

Folgerung 1.44 *Sei $n \in \mathbb{N}\setminus\{1,2\}$.*

(a) *Die Gruppe $\mathcal{A}_n$ wird von 3-Zykeln erzeugt.*

(b) *Für $n \geq 5$ existiert zu jedem Paar $f,g \in \mathcal{A}_n$ von 3-Zykeln ein $h \in \mathcal{A}_n$ mit $f = h\circ g\circ h^{-1}$.*

(c) *Für $n \geq 5$ ist $\mathcal{A}_n$ einfach.*

Beispiel:

- Die alternierende Gruppe $\mathcal{A}_5$ besitzt keine Untergruppe der Ordnung 30, die alternierende Gruppe $\mathcal{A}_4$ keine Untergruppe der Ordnung 6.

Kapitel 2

Ringe und Körper

2.1 Ringe

Definition 2.1 *Ein* **Ring R** *ist eine additive abelsche Gruppe mit mindestens zwei Elementen, in der zusätzlich eine assoziative Multiplikation* $(a, b) \mapsto ab$ *erklärt ist, so dass die Distributivgesetze* $a(b + c) = ab + ac$ *und* $(a + b)c = ac + bc$ *für alle* $a, b, c \in \mathbf{R}$ *erfüllt sind.*

Ist auch die Multiplikation in einem Ring kommutativ, so spricht man von einem **kommutativen Ring**. Existiert in $\mathbf{R}$ ein neutrales Element (mit 1 bezeichnet) bezüglich der Multiplikation, so sprechen wir von einem **Ring mit Einselement**.

Beispiele:

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind kommutative Ringe mit Einselement.
- $(\mathbb{Z}_m, +, \cdot)$ ist der Restklassenring modulo m mit der Null $[0]_m$ und der Eins $[1]_m$.
- $(\mathbf{R}^X, +, \cdot)$: Hierbei sind X eine nichtleere Menge, $\mathbf{R}$ ein Ring, $\mathbf{R}^X = \{f : X \longrightarrow \mathbf{R}\}$ die Menge aller Abbildungen von X in $\mathbf{R}$ und

  $$(f + g)(x) := f(x) + g(x), \quad (fg)(x) = f(x)g(x), \quad f, g \in \mathbf{R}^X, \ x \in X.$$

  Spezialfall: $\mathbf{R}^{\{1,\ldots,n\}} =: \mathbf{R}^n$,
- $(\mathbf{R}^{n\times n}, +, \cdot)$ mit

  $$\left[\ a_{jk}\ \right]_{j,k=1}^{n} + \left[\ b_{jk}\ \right]_{j,k=1}^{n} := \left[\ a_{jk} + b_{jk}\ \right]_{j,k=1}^{n}$$

  und

  $$\left[\ a_{jk}\ \right]_{j,k=1}^{n} \left[\ b_{jk}\ \right]_{j,k=1}^{n} := \left[\ \sum_{i=1}^{n} a_{ji} b_{ik}\ \right]_{j,k=1}^{n}$$

Rechenregeln in einem Ring $(\mathbf{R}, +, \cdot)$: Für alle $x, y \in \mathbf{R}$ gilt

- $0x = x0 = 0$,
- $(-x)y = y(-x) = -(xy)$,
- $(-x)(-y) = xy$,
- $x - y := x + (-y)$,
- $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$, $n \in \mathbb{N}$, falls $xy = yx$.

Definition 2.2 *Sind* $(\mathbf{R}, +, \cdot)$ *und* $\mathbf{S}, +, \cdot)$ *Ringe, so nennen wir eine Abbildung* $\varphi : \mathbf{R} \longrightarrow \mathbf{S}$ *einen* **Ringhomomorphismus**, *wenn* $\varphi : (\mathbf{R}, +) \longrightarrow (\mathbf{S}, +)$ *ein Gruppenhomomorphismus ist und* $\varphi(xy) = \varphi(x)\varphi(y)$ *für alle* $x, y \in \mathbf{R}$ *gilt.*

Die Bezeichnungen Monomorphismus, usw. aus der Gruppentheorie werden auch hier verwendet. Eine Teilmenge $\mathbf{U}$ eines Ringes $\mathbf{R}$, die mindestens zwei Elemente enthält, heißt **Unterring** von $\mathbf{R}$, wenn $\mathbf{U} + \mathbf{U} \subset \mathbf{U}$ und $\mathbf{U} \cdot \mathbf{U} \subset \mathbf{U}$ gilt, was genau dann der Fall ist, wenn aus $x, y \in \mathbf{U}$ folgt $x - y \in \mathbf{U}$ und $xy \in \mathbf{U}$.

Beispiele:

- (m) ist ein Unterring von $(\mathbb{Z}, +, \cdot)$.
- Sind $\mathbf{R}$ und $\mathbf{S}$ Ringe, $\mathbf{U} \subset \mathbf{R}$ und $\mathbf{V} \subset \mathbf{S}$ Unterringe sowie $\varphi : \mathbf{R} \longrightarrow \mathbf{S}$ ein Ringhomomorphismus, so sind $\varphi(\mathbf{U})$ und $\varphi^{-1}(\mathbf{V})$ Unterringe von $\mathbf{S}$ bzw. $\mathbf{R}$ oder gleich $\{0\}$. Somit sind auch $\ker \varphi$ und $\varphi(\mathbf{R})$ Unterringe oder gleich $\{0\}$.

Definition 2.3 *Eine nichtleere Teilmenge* $\mathbf{J}$ *eines Ringes* $\mathbf{R}$ *nennt man* **Linksideal** (*bzw.* **Rechtsideal**) *von* $\mathbf{R}$, *wenn* $(\mathbf{J}, +)$ *Untergruppe von* $(\mathbf{R}, +)$ *ist und wenn* $xu \in \mathbf{J}$ (*bzw.* $ux \in \mathbf{J}$) *für alle* $x \in \mathbf{R}$ *und alle* $u \in \mathbf{J}$ *gilt. Ist* $\mathbf{J}$ *Links- und Rechtsideal, so nennt man* $\mathbf{J}$ *ein* **Ideal**.

Beispiele:

- (m) ist ein Ideal in $(\mathbb{Z}, +, \cdot)$.
- Seien $x_0 \in X$ und $\mathbf{R}_{x_0}^X = \left\{ f \in \mathbf{R}^X : f(x_0) = 0 \right\}$. Dann ist $\mathbf{R}_{x_0}^X$ ein Ideal in $\mathbf{R}$.

Satz 2.4 *Es seien* $\mathbf{J}_1 \subset \mathbf{R}$ *und* $\mathbf{J}_2 \subset \mathbf{S}$ *Ideale sowie* $\varphi : \mathbf{R} \longrightarrow \mathbf{S}$ *ein Ringhomomorphismus. Dann ist* $\varphi^{-1}(\mathbf{J}_2)$ *ein Ideal in* $\mathbf{R}$, *also auch* $\ker \varphi$. *Ist* φ *surjektiv, so ist auch* $\varphi(\mathbf{J}_1)$ *ein Ideal in* $\mathbf{S}$.

Sei $\mathbf{J} \subset \mathbf{R}$ ein Ideal im Ring $\mathbf{R}$. Wir nennen zwei Elemente $x, y \in \mathbf{R}$ **kongruent** modulo $\mathbf{J}$, wenn $x - y \in \mathbf{J}$ gilt, in Zeichen $x \equiv y \mod \mathbf{J}$. Dies definiert eine Äquivalenzrelation auf $\mathbf{R}$, die zugehörigen Äquivalenzklassen sind von der Gestalt $x + \mathbf{J}$ und werden **Restklassen**

modulo $\mathbf{J}$ genannt. Die Menge aller dieser Restklassen bezeichnen wir mit $\mathbf{R}/\mathbf{J}$. Definiert man $(x+\mathbf{J})+(y+\mathbf{J}) := (x+y)+\mathbf{J}$ und $(x+\mathbf{J})(y+\mathbf{J}) := xy+\mathbf{J}$, so erhält man einen Ring, den **Restklassenring** modulo $\mathbf{J}$. Die Abbildung $\pi : \mathbf{R} \longrightarrow \mathbf{R}/\mathbf{J}$, $x \mapsto x+\mathbf{J}$ ist ein Epimorphismus und wird **kanonischer Epimorphismus** genannt. Dabei gilt $\ker \pi = \mathbf{J}$.

Satz 2.5 *Es seien* $\mathbf{R}$ *und* $\mathbf{S}$ *Ringe.*

(a) *Eine Menge* $\mathbf{J} \subset \mathbf{R}$ *ist genau dann ein Ideal, wenn sie Kern eines Ringhomomorphismus ist.*

(b) *Ist* $\varphi : \mathbf{R} \longrightarrow \mathbf{S}$ *ein Ringhomomorphismus, so gilt* $\mathbf{R}/\ker\varphi \cong \varphi(\mathbf{R})$.
(**Homomorphiesatz**)

(c) *Sind* $\mathbf{U} \subset \mathbf{R}$ *ein Unterring und* $\mathbf{J} \subset \mathbf{R}$ *ein Ideal, so ist* $\mathbf{U} \cap \mathbf{J}$ *ein Ideal in* $\mathbf{U}$, *wobei* $(\mathbf{U}+\mathbf{J})/\mathbf{J} \cong \mathbf{U}/(\mathbf{U}\cap\mathbf{J})$ *gilt.* (**erster Isomorphiesatz**)

(d) *Sind* $\mathbf{J}_1$ *und* $\mathbf{J}_2$ *Ideale in* $\mathbf{R}$ *mit* $\mathbf{J}_1 \subset \mathbf{J}_2$, *so ist* $\mathbf{J}_2/\mathbf{J}_1$ *ein Ideal in* $\mathbf{R}/\mathbf{J}_1$. *Dabei gilt* $(\mathbf{R}/\mathbf{J}_1)/(\mathbf{J}_2/\mathbf{J}_1) \cong \mathbf{R}/\mathbf{J}_2$. (**zweiter Isomorphiesatz**)

Da der Durchschnitt beliebig vieler Ideale eines Ringes $\mathbf{R}$ wieder ein Ideal ist, kann man das von einer nichtleeren Menge $X \subset \mathbf{R}$ erzeugte Ideal (X) als den Durchschnitt aller Ideale in $\mathbf{R}$ definieren, die X enthalten. Das von $X \subset \mathbf{R}$ erzeugte Ideal (X) besteht aus allen endlichen Summen von Produkten der Form nu, xu, uy und xuy, wobei $u \in X$, $x, y \in \mathbf{R}$ und $n \in \mathbb{Z}$ beliebig sind. Ein Ideal, welches von einem Element erzeugt wird, heißt **Hauptideal**. Für $(\{u\})$ schreiben wir auch nur (u).

Folgerung 2.6 *Ist* $\mathbf{R}$

(a) *ein Ring mit Eins, so besteht* (X) *aus allen endlichen Summen von Produkten der Form* xuy *mit* $u \in X$, $x, y \in \mathbf{R}$, *z.B.* $(u) = \mathbf{R}u\mathbf{R}$,

(b) *ein kommutativer Ring, so besteht* (X) *aus allen endlichen Summen von Produkten der Form* xu *und* nu *mit* $u \in X$, $x \in \mathbf{R}$ *und* $n \in \mathbb{Z}$, *z.B.* $(u) = \mathbf{R}u + \mathbb{Z}u$,

(c) *ein kommutativer Ring mit Eins, so besteht* (X) *aus allen endlichen Summen von Produkten der Form* xu *mit* $u \in X$ *und* $x \in \mathbf{R}$, *z.B.* $(u) = \mathbf{R}u$.

Definition 2.7 *Ein Element* $x \in \mathbf{R} \setminus \{0\}$ *eines Ringes* $\mathbf{R}$ *nennen wir* **Nullteiler**, *wenn ein* $y \in \mathbf{R} \setminus \{0\}$ *mit* $xy = 0$ *oder* $yx = 0$ *existiert. Der Ring* $\mathbf{R}$ *heißt* **nullteilerfrei** , *wenn er keine Nullteiler besitzt.*

Beispiel 2.8 *Der Ring der ganzen Zahlen* $\mathbb{Z}$ *ist nullteilerfrei. Der Restklassenring* $\mathbb{Z}_m$ *modulo* m $(m \in \mathbb{N} \setminus \{1\})$ *ist genau dann nullteilerfrei, wenn* m *eine Primzahl ist.*

Man beachte: Ist $a \in \mathbf{R} \setminus \{0\}$ kein Nullteiler, so gelten die Kürzungsregeln

$$ax = ay \implies x = y \quad \text{und} \quad xa = ya \implies x = y\,.$$

Definition 2.9 *Man sagt, dass ein Ring* $\mathbf{R}$ *die* **Charakteristik** $\operatorname{char}\mathbf{R} = 0$ *hat, wenn es in der Gruppe* $(\mathbf{R}, +)$ *keine von Null verschiedenen Elemente endlicher Ordnung gibt. Sonst setzt man*

$$\operatorname{char}\mathbf{R} = \min\{n \in \mathbb{N} : \exists\, x \in \mathbf{R} \setminus \{0\} \text{ mit } nx = 0\}\ .$$

Satz 2.10 *Ein nullteilerfreier Ring* $\mathbf{R}$ *mit Einselemt* 1 *hat entweder die Charakteristik* 0 *oder eine Primzahl* p *als Charakteristik, die gleich der Ordnung von* 1 *in* $(\mathbf{R}, +)$ *ist und für die außerdem* $px = 0$ *für alle* $x \in \mathbf{R}$ *gilt.*

2.2 Integritätsringe

Einen nullteilerfreien kommutativen Ring nennt man **Integritätsring**.

Man beachte: Während $\mathbb{Z}$ ein Integritätsring ist, sind seine homomorphen Bilder $\mathbb{Z}_m$ im Fall, dass $m \in \mathbb{N} \setminus \{1\}$ keine Primzahl ist, keine Integritätsringe.

Unter einem **Primideal** $\mathbf{J} \subset \mathbf{R}$ eines kommutativen Ringes $\mathbf{R}$ versteht man ein Ideal $\mathbf{J} \neq \mathbf{R}$, für welches aus $x, y \in \mathbf{R}$ und $xy \in \mathbf{J}$ folgt $x \in \mathbf{J}$ oder $y \in \mathbf{J}$.

Folgerung 2.11 *In einem kommutativen Ring* $\mathbf{R}$ *ist* (0) *genau dann ein Primideal, wenn* $\mathbf{R}$ *ein Integritätsring ist. Somit ist* (0) *in* $\mathbb{Z}$ *ein Primideal. Weiter ist* (p), $p \in \mathbb{N}$ *genau dann ein Primideal in* $\mathbb{Z}$, *wenn* p *eine Primzahl ist.*

Folgerung 2.12 *Es seien* $\mathbf{R}$ *ein kommutativer Ring und* $\mathbf{J} \subset \mathbf{R}$ *ein Ideal mit* $\mathbf{J} \neq \mathbf{R}$. *Folgende Aussagen sind dann äquivalent:*

(a) $\mathbf{J}$ *ist ein Primideal.*

(b) $\mathbf{R}/\mathbf{J}$ *ist ein Integritätsring.*

(c) *Es gibt einen Ringhomomorphismus* $\varphi : \mathbf{R} \longrightarrow \mathbf{S}$ *in einen Integritätsring* $\mathbf{S}$, *wobei* $\ker\varphi = \mathbf{J}$ *gilt.*

Definition 2.13 *Seien* $\mathbf{R}$ *ein Integritätsring mit Eins und* $x, y \in \mathbf{R}$. *Man sagt* x **teilt** y *(in Zeichen:* $x|y$*), oder* x *ist* **Teiler** *von* y, *oder* y *ist* **Vielfaches** *von* x, *wenn ein* $z \in \mathbf{R}$ *mit* $y = zx$ *existiert.*

Regeln: Es gilt

- $1|x$, $x|0$ und $x|x$ für alle $x \in \mathbf{R}$,
- $x|1$ genau dann, wenn x invertierbar ist, also eine sogenannte **Einheit** in $\mathbf{R}$ ist,
- $x|y \implies xz|yz\ \forall\, z \in \mathbf{R}$,

- $x|y_k\,,\ k=1,\ldots,n \implies x|(z_1y_1+\ldots+z_ny_n\ \forall\, z_k\in\mathbf{R}\,,$
- $x|y\,,\ y|x \implies x|z\,,$
- $x|y \iff y\in(x) \iff (y)\subset(x)\,,$
- $x|y\,,\ y|x \iff (y)=(x) \iff y=xz$ mit einer Einheit $z\,.$

Die Menge der Einheiten eines Ringes $\mathbf{R}$ mit Eins bezeichnen wir mit $\mathbf{R}^*$. Zwei Elemente $x,y\in\mathbf{R}$ nennen wir **assoziiert**, wenn ein $z\in\mathbf{R}^*$ mit $x=yz$ existiert, in Zeichen: $x\sim y$. Es gilt also: $x\sim y \iff (x)=(y)$. Ein Element $p\in\mathbf{R}\setminus(\mathbf{R}^*\cup\{0\})$ heißt **Primelement**, wenn aus $x,y\in\mathbf{R}$ und $p|xy$ folgt $p|x$ oder $p|y$. Man nennt $p\in\mathbf{R}\setminus(\mathbf{R}^*\cup\{0\})$ **irreduzibel**, wenn aus $x,y\in\mathbf{R}$ und $p=xy$ folgt $x\in\mathbf{R}^*$ oder $y\in\mathbf{R}^*$. Wir nennen einen Teiler x von y einen **echten Teiler**, wenn x weder zu $\mathbf{R}^*$ gehört noch assoziiert zu y ist. Ein p ist also irreduzibel, wenn es keine echten Teiler besitzt.

Folgerung 2.14 *Es seien* $\mathbf{R}$ *ein Integritätsring mit* 1 *und* $p\in\mathbf{R}\setminus(\mathbf{R}^*\cup\{0\})$. *Dann ist*

(a) p *genau dann ein Primelement, wenn* (p) *ein Primideal ist,*

(b) p *genau dann irreduzibel, wenn aus* $(p)\subset(x)\neq\mathbf{R}$ *folgt* $(p)=(x)\,,$

(c) *jedes Primelement irreduzibel.*

Definition 2.15 *Es sei* $\mathbf{R}$ *ein Integritätsring mit* 1. *Ein gemeinsamer Teiler* d *der Elemente* $x_1,\ldots,x_n\in\mathbf{R}$ *heißt* **größter gemeinsamer Teiler** *der* $x_1,\ldots,x_n$, *wenn jeder gemeinsame Teiler der* $x_1,\ldots,x_n$ *auch Teiler von* d *ist. Die Menge der größten gemeinsamen Teiler von* $x_1,\ldots,x_n$ *bezeichnen wir mit* $\mathrm{ggT}(x_1,\ldots,x_n)$. *Die Elemente* $x_1,\ldots,x_n$ *heißen* **relativ prim** *oder* **teilerfremd**, *wenn* $\mathrm{ggT}(x_1,\ldots,x_n)\subset\mathbf{R}^*$ *gilt.*

Beachte: Aus $d_1,d_2\in\mathrm{ggT}(x_1,\ldots,x_n)$ folgt $d_1\sim d_2\,.$

Einen Integritätsring mit 1, in dem jedes Ideal ein Hauptideal ist, nennen wir **Hauptidealring** Das von $x_1,\ldots,x_n\in\mathbf{R}$ erzeugte Ideal bezeichnen wir mit $(x_1,\ldots,x_n)$.

Satz 2.16 *Es seien* $\mathbf{R}$ *ein Hauptidealring und* $x_1,\ldots,x_n\in\mathbf{R}$.

(a) *Es gilt* $d\in\mathrm{ggT}(x_1,\ldots,x_n)$ *genau dann, wenn* $(d)=(x_1,\ldots,x_n)\,.$

(b) *Es ist* $\mathrm{ggT}(x_1,\ldots,x_n)\neq\emptyset\,,$ *und für* $d\in\mathrm{ggT}(x_1,\ldots,x_n)$ *existieren* $r_1,\ldots,r_n\in\mathbf{R}$ *mit* $d=r_1x_1+\ldots+r_nx_n\,.$

(c) *Die* $x_1,\ldots,x_n$ *sind genau dann relativ prim, wenn* $r_1,\ldots,r_n\in\mathbf{R}$ *existieren, so dass* $1=r_1x_1+\ldots+r_nx_n$ *gilt.*

(d) *Sind* $a,b\in\mathbf{R}$ *teilerfremd, so folgt aus* $a|bc\,,$ *dass* $a|c\,,$ *sowie aus* $a|c$ *und* $b|c\,,$ *dass* $ab|c\,.$

Ein Ideal $\mathbf{J} \neq \mathbf{R}$ im Ring $\mathbf{R}$ heißt **maximal**, wenn für jedes Ideal $\mathbf{J}_1 \subset \mathbf{R}$ mit $\mathbf{J} \subset \mathbf{J}_1 \neq \mathbf{R}$ folgt $\mathbf{J} = \mathbf{J}_1$. Ein Ring $\mathbf{R}$ heißt **einfach**, wenn er nur die trivialen Ideale $\{0\}$ und $\mathbf{R}$ besitzt.

Folgerung 2.17 *Ist* $\mathbf{R}$ *ein einfacher kommutativer Ring mit* 1, *so gilt* $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$.

Folgerung 2.18 *Sei* $\mathbf{J} \neq \mathbf{R}$ *ein Ideal im Ring* $\mathbf{R}$.

(a) *Sind* $\mathbf{J}$ *maximal und* $\mathbf{J}_1 \subset \mathbf{R}$ *ein nicht in* $\mathbf{J}$ *enthaltenes Ideal, so gilt* $\mathbf{J} + \mathbf{J}_1 = \mathbf{R}$.

(b) $\mathbf{J}$ *ist genau dann maximal, wenn* $\mathbf{R}/\mathbf{J}$ *einfach ist.*

(c) *Ist* $\mathbf{R}$ *ein Hauptidealring, so ist* $p \in \mathbf{R}$ *genau dann ein Primelement, wenn es irreduzibel ist, und das ist genau dann der Fall, wenn* (p) *maximal ist.*

(d) *Ist* $\mathbf{R}$ *ein Hauptidealring, so ist jedes* $x \in \mathbf{R} \setminus (\mathbf{R}^* \cup \{0\})$ *als Produkt endlich vieler Primelemente darstellbar.*

Sind $\mathbf{R}$ ein Integritätsring mit 1 und $p \in \mathbf{R}$ ein Primelement sowie $x \in \mathbf{R}$ beliebig, so ist p Teiler von x oder p und x sind teilerfremd. Insbesondere sind zwei Einheiten assoziiert oder teilerfremd. Hieraus kann man schließen, dass die in Folgerung 2.18,(d) erwähnte Faktorisierung bis auf die Reihenfolge der Faktoren und bis auf Einheiten eindeutig ist.

Einen Integritätsring $\mathbf{R}$ nennt man **Euklidischen Ring**, wenn eine Abbildung $h : \mathbf{R} \setminus \{0\} \longrightarrow \mathbb{N}_0$ mit folgender Eigenschaft existiert: Für beliebige $a, b \in \mathbf{R}$ mit $b \neq 0$ existieren $q, r \in \mathbf{R}$, so dass $a = bq + r$ und $r = 0$ oder $h(r) < h(b)$ (**Division mit Rest**).

Folgerung 2.19 *Jeder Euklidische Ring ist ein Hauptidealring.*

Beispiel 2.20 $\mathbb{Z}[\sqrt{2}] = \left\{x + y\sqrt{2} : x, y \in \mathbb{Z}\right\}$ *ist ein Unterring von* $\mathbb{R}$ *und somit ein Integritätsring (mit* 1*). Zusammen mit der Abbildung* $h : \mathbb{Z}[\sqrt{2}] \setminus \{0\} \longrightarrow \mathbb{N}$, $x + y\sqrt{2} \mapsto |x^2 - 2y^2|$ *erweist sich dieser als Euklidischer Ring.*

Beispiel 2.21 $\mathbb{Z}[\sqrt{-5}] = \left\{x + \mathbf{i}\sqrt{5} : x, y \in \mathbb{Z}\right\}$ *ist Unterring von* $\mathbb{C}$. *Die einzigen Einheiten in* $\mathbb{Z}[\sqrt{-5}]$ *sind* ± 1. *Die Zahl* 3 *ist irreduzibel in* $\mathbb{Z}[\sqrt{-5}]$, *aber kein Primelement. Somit ist* $\mathbb{Z}[\sqrt{-5}]$ *auch kein Hauptidealring (vgl. Folgerung 2.18).*

2.3 Körper

Definition 2.22 *Unter einem* **Schiefkörper** *verstehen wir einen Ring* $(\mathbf{R}, +, \cdot)$ *mit Eins* 1, *für den* $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$ *gilt. Ein kommutativer Schiefkörper heißt* **Körper**. *Einen Unterring eines Ringes* $\mathbf{R}$ *nennen wir* **Unterkörper** *bzw.* **Teilkörper** *von* $\mathbf{R}$, *wenn er selbst ein Schiefkörper ist.*

Ein Ring $\mathbf{R}$ ist somit genau dann ein Schiefkörper, wenn $(\mathbf{R} \setminus \{0\}, \cdot)$ eine Gruppe ist.

Beispiel 2.23 *Es seien* $\mathbf{R}$ *ein Integritätsring mit* 1 *und* $\mathcal{F}(\mathbf{R}) = \left\{(x,y) \in \mathbf{R}^2 : y \neq 0\right\}$ *. Durch*

$$(x_1,y_1) \sim (x_2,y_2) \iff_{\text{def}} x_1y_2 = x_2y_1$$

wird auf $\mathcal{F}(\mathbf{R})$ *eine Äquivalenzrelation definiert. Die Menge der Äquivalenzklassen* $[(x,y)]_\sim$ *bezeichnen wir mit* $\mathcal{Q}(\mathbf{R})$ *und definieren*

$$[(x_1,y_1)]_\sim + [x_2,y_2)]_\sim := [(x_1y_2 + x_2y_1, y_1y_2)]_\sim\,, \quad [(x_1,y_1)]_\sim \cdot [x_2,y_2)]_\sim := [(x_1x_2, y_1y_2)]_\sim\,.$$

Dann ist $(\mathcal{Q}(\mathbf{R}),+,\cdot)$ *ein Körper, der* **Quotientenkörper** *des Integritätsringes* $\mathbf{R}$*. Die Abbildung*

$$\varphi : \mathbf{R} \longrightarrow \mathcal{Q}(\mathbf{R})\,,\ x \mapsto [(x,1)]_\sim$$

ist ein Ringmonomorphismus. Man kann deshalb $\mathbf{R}$ *mit dem Bild* $\varphi(\mathbf{R})$ *in* $\mathcal{Q}(\mathbf{R})$ *identifizieren.*

Unter dem **Primkörper** $P(\mathbf{R})$ eines Schiefkörpers $\mathbf{R}$ versteht man den kleinsten in $\mathbf{R}$ enthaltenen Unterkörper, d.h. den Durchschnitt aller Unterkörper von $\mathbf{R}$ (die ja $\{0,1\}$ enthalten). Ist die Charakteristik von $\mathbf{R}$ gleich 0, so ist $P(\mathbf{R})$ isomorph zu $(\mathbb{Q},+,\cdot)$. Ist die Charakteristik von $\mathbf{R}$ gleich $p \neq 0$ (also eine Primzahl, vgl. Satz 2.10), so ist $P(\mathbf{R})$ isomorph zu $(\mathbb{Z}_p,+,\cdot)$.

Sind $\varphi : \mathbf{K} \longrightarrow \mathbf{R}$ ein Ringhomomorphismus und $\mathbf{K}$ ein Körper, so ist φ entweder injektiv oder identisch Null, weil es in einem Körper nur triviale Ideale gibt und somit $\ker\varphi$ nur gleich $\{0\}$ oder gleich $\mathbf{K}$ sein kann.

2.4 Polynomringe

Es sei $\mathbf{R}$ ein kommutativer Ring mit 1. Mit $\mathbf{R}[[t]]$ bezeichnen wir die Menge aller Folgen $f = (f_0, f_1, \dots) = (f_k)_{k=0}^\infty$ mit $f_k \in \mathbf{R}$ und versehen diese mit den Verknüpfungen

$$f+g := (f_k+g_k)_{k=0}^\infty \quad \text{und} \quad fg := \left(\sum_{j=0}^k f_{k-j}g_j\right)_{k=0}^\infty = \left(\sum_{j,\ell\in\mathbb{N}_0, j+\ell=k} f_\ell g_j\right)_{k=0}^\infty .$$

Dann ist $(\mathbf{R}[[t]],+,\cdot)$ ein kommutativer Ring mit Eins, der **Ring der formalen Potenzreihen** über $\mathbf{R}$. Man kann nämlich $(f_k)_{k=0}^\infty$ mit der formalen Potenzreihe $\sum_{k=0}^\infty f_k t^k$ identifizieren. Mit $\mathbf{R}[t]$ bezeichnen wir den Unterring von $\mathbf{R}[[t]]$ der Folgen $f \in \mathbf{R}[[t]]$, für die ein $m = m(f) \in \mathbb{N}_0$ existiert, so dass $f_k = 0$ für alle $k > m$ gilt. Man nennt $\mathbf{R}[t]$ den **Polynomring** über $\mathbf{R}$ in der Veränderlichen t. Die Elemente von $\mathbf{R}[t]$ nennt man **Polynome** und schreibt sie auch in der Form $f(t) = \sum_{k=0}^{m(f)} f_k t^k$. Für $f \in \mathbf{R}[t] \setminus \{0\}$ definieren wir $\deg f = \max\{k \in \mathbb{N}_0 : f_k \neq 0\}$. Es gilt

$$\deg(fg) = \deg f + \deg g \quad \forall\, f,g \in \mathbf{R}[t] \setminus \{0\}$$

genau dann, wenn $\mathbf{R}$ ein Integritätsring ist. Für $f \in \mathbf{R}[t] \setminus \{0\}$ nennt man $f_{\deg f}$ den **Leitkoeffizienten** des Polynoms f. Das Polynom $f \in \mathbf{R}[t] \setminus \{0\}$ heißt **monisch**, wenn $f_{\deg f} = 1$ gilt.

Der Polynomring $\mathbf{R}[t]$ ist genau dann ein Integritätsring, wenn $\mathbf{R}$ ein solcher Ring ist. In diesem Fall ist der Quotientenkörper $\mathbf{R}(t) := \mathcal{Q}(\mathbf{R}[t])$ der **Körper der rationalen Funktionen** in der Veränderlichen t, und ein Polynom $f \in \mathbf{R}[t]$ ist genau dann in $\mathbf{R}[t]$ invertierbar, wenn $f_0 \in \mathbf{R}^*$ und $f_k = 0$, $k > 0$ gilt. In diesem Sinne kann man $(\mathbf{R}[t])^* = \mathbf{R}^*$ schreiben. Für ein festes $g \in \mathbf{R}[t]$ betrachten wir den Homomorphismus $\Phi_g : \mathbf{R}[t] \longrightarrow \mathbf{R}[t]$, $f(t) \mapsto f(g(t))$, d.h.

$$(\Phi_g f)(t) = \sum_{k=0}^{\deg f} f_k \left(\sum_{j=0}^{\deg g} g_j t^j \right)^k ,$$

auch die durch g induzierte **Polynomabbildung** genannt.

Folgerung 2.24 *Ist* $\mathbf{R}$ *ein Integritätsring mit Eins, so ist* $\Phi_g : \mathbf{R}[t] \longrightarrow \mathbf{R}[t]$ *genau dann ein Isomorphismus, wenn* $\deg g = 1$ *und* $g_1 \in \mathbf{R}^*$ *gilt.*

Satz 2.25 (Division mit Rest) *Es seien* $\mathbf{R}$ *ein kommutativer Ring mit* 1, $f, g \in \mathbf{R}[t]$ *mit* $g(t) = \sum_{k=0}^{n} g_k t^k$ *und* $g_n \in \mathbf{R}^*$. *Dann existieren eindeutig bestimmte* $q, r \in \mathbf{R}[t]$ *mit* $f = gq + r$ *und* $r = 0$ *oder* $\deg r < \deg g$.

Folgerung 2.26 *Es sei* $\mathbf{K}$ *ein Körper. Dann gilt:*

(a) $\mathbf{K}[t]$ *ist ein Euklidischer Ring.*

(b) $\mathbf{K}[t]$ *ist ein Hauptidealring.*

(c) *Jedes* $f \in \mathbf{K}[t]$ *mit* $\deg f > 0$ *lässt sich in der Form* $f = ap_1p_2 \dots p_r$ *mit* $a \neq 0$ *und irreduziblen monischen Polynomen* p_k *auf (bis auf die Reihenfolge der Faktoren) eindeutige Weise darstellen.*

(d) *Es ist* $p \in \mathbf{K}[t]$ *genau dann irreduzibel, wenn* $\mathbf{K}[t]/(p)$ *ein Körper ist.*

Folgerung 2.27 *Für einen kommutativen Ring* $\mathbf{R}$ *mit Eins sind folgende Aussagen äquivalent:*

(a) $\mathbf{R}$ *ist ein Körper.*

(b) $\mathbf{R}[t]$ *ist ein Euklidischer Ring.*

(c) $\mathbf{R}[t]$ *ist ein Hauptidealring.*

Wir betrachten nun folgende Situation: Es seien $\mathbf{R}$ ein kommutativer Ring mit 1 und $\mathbf{S} \supset \mathbf{R}$ ein kommutativer Erweiterungsring. Sind $f \in \mathbf{R}[t]$, $f(t) = \sum_{k=0}^{\deg f} f_k t^k$ und $x \in \mathbf{S}$, so verstehen wir unter $f(x)$ das Element $f(x) = \sum_{k=0}^{\deg f} f_k x^k \in \mathbf{S}$. Ein Element $x \in \mathbf{S}$ heißt **Nullstelle** oder **Wurzel** des Polynoms $f \in \mathbf{R}[t]$, wenn $f(x) = 0$ gilt.

Folgerung 2.28 *Sind* $\mathbf{R}$ *ein Integritätsring mit* 1 *und* $f \in \mathbf{R}[t]$ *mit* $\deg f = n > 0$, *so hat* f *höchstens* n *verschiedene Wurzeln in* $\mathbf{R}$. *Ist* $x \in \mathbf{R}$ *eine solche Wurzel, so ist das Polynom* $t - x$ *ein Teiler von* f.

Im Weiteren schreiben wir für $y^{-1}x$ auch $\dfrac{x}{y}$.

Folgerung 2.29 *Es seien* $\mathbf{K}$ *ein Körper mit* $|\mathbf{K}| = \infty$ *und* $x_1, \ldots, x_n \in \mathbf{K}$ *paarweise verschiedene Elemente sowie* $y_1, \ldots, y_n \in \mathbf{K}$ *beliebig. Dann ist*

$$f(t) = \sum_{k=0}^{n} y_k \frac{(t - x_1) \cdots (t - x_{k-1})(t - x_{k+1}) \cdots (t - x_n)}{(x_k - x_1) \cdots (x_k - x_{k-1})(x_k - x_{k+1}) \cdots (x_k - x_n)}$$

das eindeutig bestimmte Polynom in $\mathbf{K}[t]$ *mit* $\deg f < n$ *und* $f(x_k) = y_k$, $k = 1, \ldots, n$.

Folgerung 2.30 *Es sei* $\mathbf{K}$ *ein Körper.*

(a) *Ist* $\mathbf{G}$ *eine endliche Untergruppe von* $(\mathbf{K}^*, \cdot)$, *so ist* $\mathbf{G}$ *zyklisch.*

(b) *Ist* $|\mathbf{K}| < \infty$, *so ist* $(\mathbf{K}^*, \cdot)$ *zyklisch.*

Kapitel 3

Körpertheorie

3.1 Körpererweiterungen

Im Weiteren seien $\mathbf{K}$, $\mathbf{L}$ und $\mathbf{M}$ Körper. Ist $\mathbf{K} \subset \mathbf{L}$ ein Unterkörper von $\mathbf{L}$, so nennt man $\mathbf{L}$ einen **Erweiterungskörper** von $\mathbf{K}$ und spricht von der **Körpererweiterung** $\mathbf{L} : \mathbf{K}$. Der Körper $\mathbf{M}$ heißt **Zwischenkörper** der Erweiterung $\mathbf{L} : \mathbf{K}$, wenn $\mathbf{M}$ Unterkörper von $\mathbf{L}$ mit $\mathbf{K} \subset \mathbf{M} \subset \mathbf{L}$ ist.

Die Abbildung $F : \mathbf{K} \longrightarrow \mathbf{K}$, $x \mapsto x^p$ mit $p = \operatorname{char} \mathbf{K} > 0$ nennt man **Frobenius-Abbildung**.

Beispiel:

- Ist p Primzahl, so gilt $\operatorname{char} \mathbb{Z}_p = p$ und $[x]_p^p = [x]_p$, d.h. $F = \mathrm{id}$.

Folgerung 3.1 *Ist* $|\mathbf{K}| < \infty$, *so ist* $F : \mathbf{K} \longrightarrow \mathbf{K}$ *ein Automorphismus.*

Folgerung 3.2 *Für* $\operatorname{char} \mathbf{K} = p > 0$ *gilt* $P(\mathbf{K}) = \{x \in \mathbf{K} : x^p = x\}$.

Ist $\mathbf{L} : \mathbf{K}$ eine Körpererweiterung, so folgt $P(\mathbf{L}) = P(\mathbf{K})$ und $\operatorname{char} \mathbf{L} = \operatorname{char} \mathbf{K}$. Ferner kann $\mathbf{L}$ als Vektorraum über $\mathbf{K}$ betrachtet werden. Die Dimension dieses Vektorraumes wird **Grad** der Körpererweiterung genannt und mit $[\mathbf{L} : \mathbf{K}]$ bezeichnet. Je nachdem, ob $[\mathbf{L} : \mathbf{K}] < \infty$ oder $[\mathbf{L} : \mathbf{K}] = \infty$ gilt, sprechen wir von einer endlichen oder unendlichen Körpererweiterung.

Beispiele:

- $[\mathbb{C} : \mathbb{R}] = 2$,
- $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$,
- $[\mathbf{K}(t) : \mathbf{K}] = \infty$, wobei $\mathbf{K}(t)$ den Quotientenkörper zu $\mathbf{K}[t]$ bezeichnet.

Folgerung 3.3 *Sind* $|\mathbf{K}| < \infty$ *und* $n = [\mathbf{K} : P(\mathbf{K})]$, *so gilt* $|\mathbf{K}| = (\operatorname{char}\mathbf{K})^n$.

Satz 3.4 *Ist* $\mathbf{M}$ *ein Zwischenkörper von* $\mathbf{L} : \mathbf{K}$, *so gilt*

$$[\mathbf{L} : \mathbf{K}] = [\mathbf{L} : \mathbf{M}] \cdot [\mathbf{M} : \mathbf{K}] .$$

Definition 3.5 *Unter der* **Adjunktion** $\mathbf{K}(A)$ *einer Teilmenge* $A \subset \mathbf{L}$ *an den Körper* $\mathbf{K}$ *verstehen wir den kleinsten Zwischenkörper der Erweiterung* $\mathbf{L} : \mathbf{K}$, *der* A *umfasst, d.h.*

$$\mathbf{K}(A) = \bigcap \{\mathbf{M} : \mathbf{M} \text{ ist Zwischenkörper von } \mathbf{L} : \mathbf{K},\ A \subset \mathbf{M}\} .$$

Offenbar gilt

- $\mathbf{K}(A) = \mathbf{K}(\mathbf{K} \cup A)$,
- $\mathbf{K}(A_1 \cup A_2) = \big(\mathbf{K}(A_1)\big)(A_2) = \big(\mathbf{K}(A_2)\big)(A_1)$,
- $\mathbf{K} \subset \mathbf{M} \subset \mathbf{L}$ und $A \subset \mathbf{L}$ implizieren $\mathbf{K}(A) \subset \mathbf{M}(A)$.

Wir verwenden die Schreibweise $\mathbf{K}(a_1, \ldots, a_n)$ für $\mathbf{K}(\{a_1, \ldots, a_n\})$. Eine Körpererweiterung $\mathbf{L} : \mathbf{K}$ wird **einfach** genannt, wenn ein $a \in \mathbf{L}$ existiert, so dass $\mathbf{L} = \mathbf{K}(a)$ gilt. In diesem Fall heißt a **primitives Element** der Erweiterung $\mathbf{L} : \mathbf{K}$. So sind z.B. $\mathbb{C} : \mathbb{R}$ und $\mathbb{R}(t) : \mathbb{R}$ einfach.

Folgerung 3.6 *Jede endliche Erweiterung* $\mathbf{L} : \mathbf{K}$ *eines endlichen Körpers* $\mathbf{K}$ *ist einfach.*

Definition 3.7 *Es sei* $\mathbf{L} : \mathbf{K}$ *eine Körpererweiterung. Man nennt* $a \in \mathbf{L}$ **algebraisch** *über* $\mathbf{K}$, *wenn es ein* $f \in \mathbf{K}[t]$ *mit* $f(a) = 0$ *gibt. Sonst heißt* a **transzendent** *über* $\mathbf{K}$.

Offenbar gilt für eine Körpererweiterung $\mathbf{L} : \mathbf{K}$, $a \in \mathbf{L}$ und $\mathbf{K}[a] := \{f(a) : f \in \mathbf{K}[t]\}$ stets $\mathbf{K}[a] \subset \mathbf{L}$. Die Abbildung $\varphi_a : \mathbf{K}[t] \longrightarrow \mathbf{L}$, $f \mapsto f(a)$ ist ein Homomorphismus. Nach dem Homomorphiesatz gilt $\mathbf{K}[t]/\ker\varphi_a \cong \mathbf{K}[a]$.

Folgerung 3.8 *Es seien* $\mathbf{K}(a) : \mathbf{K}$ *eine Körpererweiterung und* $a \in \mathbf{L}$ *transzendent über* $\mathbf{K}$. *Dann gilt:*

(a) $\mathbf{K}(a) \cong \mathbf{K}(t)$,

(b) $[\mathbf{K}(a) : \mathbf{K}] = \infty$,

(c) a^2 *ist transzendent über* $\mathbf{K}$, $\mathbf{K}(a^2) \subset \mathbf{K}(a)$ *und* $\mathbf{K}(a^2) \neq \mathbf{K}(a)$,

(d) $\mathbf{K}(a) : \mathbf{K}$ *besitzt unendlich viele Zwischenkörper.*

In Folgerung 3.8 haben wir eine sogenannte transzendente einfache Körpererweiterung $\mathbf{K}(a) : \mathbf{K}$ betrachtet. Es sei nun $\mathbf{K}(a) : \mathbf{K}$ eine algebraische Körpererweiterung, d.h., $a \in \mathbf{L}$ ist algebraisch über $\mathbf{K}$. Dies ist gleichbedeutend mit $\ker \varphi_a \neq \{0\}$. Da das erzeugende Element des Hauptideals $\ker \varphi_a$ ($\mathbf{K}[t]$ ist Hauptidealring, siehe Folgerung 2.26) bis auf Einheiten eindeutig bestimmt ist (siehe Regeln nach Definition 2.13), gilt $\ker \varphi_a = (m_a(t))$ mit dem eindeutig bestimmten monischen Polynom $m_a(t)$ kleinsten Grades in $\ker \varphi_a$. Das Polynom $m_a(t)$ heißt **Minimalpolynom** des Elementes $a \in \mathbf{L}$ über $\mathbf{K}$, und $\deg_{\mathbf{K}} a := \deg m_a(t)$ wird **Grad** von a über $\mathbf{K}$ genannt.

Beispiel:

- $\mathbf{i} \in \mathbb{C}$ über $\mathbb{R}$: $m_{\mathbf{i}}(t) = t^2 + 1$, $\deg_{\mathbb{R}} \mathbf{i} = 2$

Folgerung 3.9 *Es seien $a \in \mathbf{L}$ algebraisch über $\mathbf{K}$ und $m_a(t)$ das entsprechende Minimalpolynom. Dann gilt:*

(a) $f \in \mathbf{K}[t]$, $f(a) = 0 \implies m_a | f$.

(b) *Das Polynom $m_a(t)$ ist irreduzibel in $\mathbf{K}[t]$.*

(c) *Ist $f \in \mathbf{K}[t]$ monisch und irreduzibel mit $f(a) = 0$, so folgt $f(t) = m_a(t)$.*

Folgerung 3.10 *Unter den Voraussetzungen von Folgerung 3.9 gilt:*

(a) $\mathbf{K}(a) = \mathbf{K}[a] \cong \mathbf{K}[t]/(m_a)$,

(b) $\left\{a^k : k = 0, 1, \ldots, \deg_{\mathbf{K}} a - 1\right\}$ *ist Basis in* $\mathbf{K}(a) : \mathbf{K}$,

(c) $[\mathbf{K}(a) : \mathbf{K}] = \deg_{\mathbf{K}} a$.

Wir nennen eine Körpererweiterung $\mathbf{L} : \mathbf{K}$ **algebraisch**, wenn jedes $a \in \mathbf{L}$ algebraisch über $\mathbf{K}$ ist. Sonst heißt die Erweiterung **transzendent**.

Folgerung 3.11 *Für eine Körpererweiterung $\mathbf{L} : \mathbf{K}$ gilt:*

(a) *Das Element $a \in \mathbf{L}$ ist genau dann algebraisch, wenn $[K(a) : \mathbf{K}]$ endlich ist.*

(b) *Ist $[\mathbf{L} : \mathbf{K}]$ endlich, so ist $\mathbf{L} : \mathbf{K}$ algebraisch.*

(c) *Es gilt $[\mathbf{L} : \mathbf{K}] < \infty$ genau dann, wenn endlich viele $a_1, \ldots, a_m \in \mathbf{L}$ existieren mit $\mathbf{L} = \mathbf{K}(a_1, \ldots, a_m)$.*

(d) *Sind $a \in \mathbf{L}$ algebraisch, $\mathbf{M}$ ein Zwischenkörper von $\mathbf{K}(a) : \mathbf{K}$ und $m_a(t) = \sum_{k=0}^{n} a_k t^k \in \mathbf{M}[t]$ das Minimalpolynom von a über $\mathbf{M}$, so gilt $\mathbf{M} = \mathbf{K}(a_0, \ldots, a_{n-1})$.*

(e) *Die Erweiterung $\mathbf{L} : \mathbf{K}$ ist genau dann einfach und algebraisch, wenn $\mathbf{L} : \mathbf{K}$ nur endlich viele Zwischenkörper besitzt.*

(f) *Sind* $\mathbf{L} : \mathbf{K}$ *einfach und algebraisch sowie* $\mathbf{M}$ *ein Zwischenkörper von* $\mathbf{L} : \mathbf{K}$, *so ist* $\mathbf{M} : \mathbf{K}$ *einfach und algebraisch.*

(g) *Ist* $\mathbf{M}$ *ein Zwischenkörper von* $\mathbf{L} : \mathbf{K}$, *so ist* $\mathbf{L} : \mathbf{K}$ *genau dann algebraisch, wenn* $\mathbf{L} : \mathbf{M}$ *und* $\mathbf{M} : \mathbf{K}$ *algebraisch sind.*

(h) *Die Menge* $A(\mathbf{L} : \mathbf{K}) := \{a \in \mathbf{L} : a \text{ ist algebraisch über } \mathbf{K}\}$ *ist ein algebraischer Erweiterungskörper von* $\mathbf{K}$.

3.2 Konstruktionen mit Zirkel und Lineal

Gegeben seien uns nur die zwei Punkte 0 und 1, die wir als reelle Zahlen 0 und 1 interpretieren können.

Konstruktionsregeln:

(1) Durch zwei gegebene oder konstruierte Punkte kann man die Gerade legen.

(2) Um jeden gegebenen oder konstruierten Punkt kann man einen Kreis schlagen mit einem Radius, den man zwischen zwei gegebenen oder konstruierten Punkten abgreift.

(3) Konstruierte Punkte sind Schnittpunkte zweier Geraden, zweier Kreise oder eines Kreises und einer Geraden.

Abgeleitete Konstruktionsschritte:

1. Errichten der zu einer Geraden Senkrechten in einem Punkt dieser Geraden. Das erlaubt uns, 0 und 1 als Punkte auf der Abszisse zu betrachten und in einem kartesischen Koordinatensystem zu arbeiten.
2. Lot von einem Punkt auf eine Gerade.
3. Parallelverschiebung einer Geraden in einen gegebenen Punkt.
4. Mittelsenkrechte einer Verbindungsstrecke zweier Punkte.
5. Halbkreis über der Verbindungsstrecke zweier Punkte.

Wir sehen, dass $(a, 0)$ und $(b, 0)$ genau dann konstruiert werden können, wenn dies für (a, b) der Fall ist.

Definition 3.12 *Wir nennen eine reelle Zahl* a **konstruierbar**, *wenn der Punkt* $(a, 0)$ *in endlich vielen Schritten nach den Regeln* (1), (2) *und* (3) *konstruierbar ist. Die Menge dieser Zahlen bezeichnen wir mit* $\mathbb{K}$.

Folgerung 3.13 *Für die Menge* $\mathbb{K}$ *der konstruierbaren reellen Zahlen gilt:*

(a) $\mathbb{K}$ *ist Zwischenkörper von* $\mathbb{R} : \mathbb{Q}$.

(b) *Die reelle Zahl* a *gehört genau dann zu* $\mathbb{K}$, *wenn Zwischenkörper* $\mathbb{K}_j$ *von* $\mathbb{R} : \mathbb{Q}$ *existieren, so dass* $\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n \subset \mathbb{R}$, $\mathbb{K}_{j+1} = \mathbb{K}_j(\sqrt{b_j})$, $b_j \in \mathbb{K}_j$, $b_j \geq 0$, $j = 0, \ldots, n-1$ *und* $a \in \mathbb{K}_n$ *gilt.*

(c) *Ist* $a \in \mathbb{K}$, *so gehört* a *zu einem Zwischenkörper von* $\mathbb{R} : \mathbb{Q}$, *dessen Grad über* $\mathbb{Q}$ *eine Zweierpotenz ist.*

(d) *Ist* $a \in \mathbb{R}$ *transzendent über* $\mathbb{Q}$, *so ist* $a \notin \mathbb{K}$.

(e) *Sind* $a \in \mathbb{R}$ *algebraisch über* $\mathbb{Q}$ *und* $\deg_{\mathbb{Q}} a$ *keine Zweierpotenz, so gilt* $a \notin \mathbb{K}$.

Beispiel 3.14 $\sqrt[3]{2} \notin \mathbb{K}$.

Ein Polynom $f \in \mathbb{Z}[t]$ nennt man **primitiv**, wenn $\mathrm{ggT}(f_0, f_1, \ldots, f_{\deg f}) = 1$. Es gilt nun:

- Sind $f, g \in \mathbb{Z}[t]$ primitive Polynome, so auch $h = fg$.
- Ist $f \in \mathbb{Z}[t]$ mit $\deg f > 0$ irreduzibel, so ist $f(t)$ auch über $\mathbb{Q}$ irreduzibel.

Beispiel 3.15 *Wir zeigen, dass* $a = \cos \frac{\pi}{9} \notin \mathbb{K}$.

3.3 Körpererweiterungen (Fortsetzung)

Definition 3.16 *Es seien* $\mathbf{K}$ *ein Körper und* $f \in \mathbf{K}[t] \setminus \mathbf{K}$. *Eine Körpererweiterung* $\mathbf{L} : \mathbf{K}$ *heißt* **Zerfällungskörper** *von* f , *wenn Elemente* $a_1, \ldots, a_m \in \mathbf{L}$ *und* $b \in \mathbf{K}$ *existieren, so dass* $f(t) = b(t - a_1) \cdots (t - a_m)$ *und* $\mathbf{L} = \mathbf{K}(a_1, \ldots, a_m)$ *gilt.*

Satz 3.17 *Es sei* $\mathbf{K}$ *ein Körper.*

(a) *Für jedes irreduzible Polynom* $p \in \mathbf{K}[t]$ *gibt es eine Körpererweiterung* $\mathbf{L} : \mathbf{K}$, *in der* $p(t)$ *eine Wurzel hat und für die* $[\mathbf{L} : \mathbf{K}] = \deg p$ *gilt.*

(b) *Für jedes Polynom* $f \in \mathbf{K}[t] \setminus \mathbf{K}$ *gibt es eine Körpererweiterung* $\mathbf{L} : \mathbf{K}$, *in der* $f(t)$ *eine Wurzel hat und für die* $[\mathbf{L} : \mathbf{K}] \leq \deg f$ *gilt.*

(c) *Für jedes Polynom* $f \in \mathbf{K}[t] \setminus \mathbf{K}$ *gibt es einen Zerfällungskörper* $\mathbf{L} : \mathbf{K}$, *für den* $[\mathbf{L} : \mathbf{K}] \leq (\deg f)!$ *gilt.*

Für $f \in \mathbf{K}[[t]]$, $f(t) = \sum_{n=0}^{\infty} f_n t^n$, definieren wir $f'(t) = \sum_{n=1}^{\infty} n f_n t^{n-1}$.

Folgerung 3.18 *Es sei* $\mathbf{K}$ *ein Körper.*

(a) *Das Polynom* $f \in \mathbf{K}[t]$ *hat genau dann mehrfache Wurzeln (in einem Erweiterungskörper* $\mathbf{L} : \mathbf{K}$*), wenn* f *und* f' *einen nicht konstanten gemeinsamen Teiler in* $\mathbf{K}[t]$ *besitzen.*

(b) *Ein irreduzibles Polynom* $f \in \mathbf{K}[t]$ *hat genau dann mehrfache Wurzeln, wenn* $f' = 0$ *gilt.*

(c) *Sind* $f \in \mathbf{K}[t]$ *irreduzibel und* $\operatorname{char} \mathbf{K} = 0$ *, so hat* f *nur einfache Wurzeln.*

Im Weiteren seien $\mathbf{K}$ ein Körper, $\mathbf{P}$ sein Primkörper und $n \in \mathbb{N}$. Unter einer **n-ten Einheitswurzel über $\mathbf{K}$** verstehen wir eine beliebige Wurzel des Polynoms $e_n(t) = t^n - 1$ $(\in \mathbf{P}[t])$. Der Zerfällungskörper $\mathbf{P}_n : \mathbf{P}$ von e_n heißt **n-ter Kreisteilungskörper** über $\mathbf{P}$. Die Menge aller n-ten Einheitswurzeln über $\mathbf{P}$ im Kreisteilungskörper $\mathbf{P}_n$ bezeichen wir mit $E_n = E_n(\mathbf{P})$. Es gilt also $\mathbf{P}_n = \mathbf{P}(E_n)$ (vgl. Definition 3.16).

Folgerung 3.19 *Für* E_n *gilt:*

(a) $|E_n| \leq n$, $E_n \subset E_{nm}$ $\forall\, m \in \mathbb{N}$.

(b) E_n *ist zyklische Untergruppe von* $(P_n^*, \cdot)$.

(c) $\operatorname{char} P = p \neq 0 \implies E_n = E_{np}$ $\forall\, n \in \mathbb{N}$.

(d) $\operatorname{char} P = 0$ *oder* $\operatorname{ggT}(\operatorname{char} P, n) = 1 \implies |E_n| = n$.

Im Weiteren seien die Voraussetzungen von Folgerung 3.19,(d) erfüllt. Dann ist E_n eine zyklische Gruppe der Ordnung n . Jedes erzeugende Element dieser Gruppe nennt man **primitive n-te Einheitswurzel** . Für eine solche primitive n-te Einheitswurzel w gilt also (vgl. Folgerung 3.10 und beachte, dass w algebraisch über $\mathbf{P}$ ist)

$$\mathbf{P}_n = \mathbf{P}(E_n) = \mathbf{P}(w) = \mathbf{P}[w] .$$

Nach Satz 1.6 gibt es genau $\varphi(n)$ primitive n-te Einheitswurzeln, wobei $\varphi(n)$ gleich der Anzahl der zu n teilerfremden Zahlen aus $\{1, \ldots, n\}$ ist (**Euler'sche φ-Funktion**). Mit F_n bezeichnen wir die Menge der primitiven n-ten Einheitswurzeln. Wir haben also $|F_n| = \varphi(n)$.

Folgerung 3.20 *Es gilt für* $\operatorname{char} P = 0$ *oder* $\operatorname{ggT}(n, \operatorname{char} P) = \operatorname{ggT}(m, \operatorname{char} P) = 1$

(a) $F_m \cap F_n = \emptyset$ *für* $m \neq n$,

(b) $E_n = \bigcup_{d \in \mathbb{N} \,:\, d \mid n} F_d$,

(c) $n = \sum_{d \in \mathbb{N} \,:\, d \mid n} \varphi(d)$.

Wir bemerken, dass die Eulersche φ-Funktion folgende Eigenschaften besitzt:

(Φ1) $\mathrm{ggT}(m,n)=1 \implies \varphi(mn)=\varphi(m)\varphi(n)$.

(Φ2) Ist p Primzahl, so gilt $\varphi(p^k)=p^{k-1}(p-1)$.

Wir haben also $F_n=\{w_1,\ldots,w_{\varphi(n)}\}$ bzw. $F_n=\{w^k : 1\le k\le n,\ \mathrm{ggT}(k,n)=1\}$ mit einem $w\in F_n$. Das Polynom $\varphi_n(t)=(t-w_1)\cdots(t-w_{\varphi(n)})\in \mathbf{P}_n[t]$ heißt n**-tes Kreisteilungspolynom** über $\mathbf{P}$.

Folgerung 3.21 *Es seien wieder* $\mathrm{char}\,P=0$ *oder* $\mathrm{ggT}(n,\mathrm{char}\,P)=\mathrm{ggT}(m,\mathrm{char}\,P)=1$. *Dann gilt*

(a) $t^n-1=\displaystyle\prod_{d\in\mathbb{N}\,:\,d|n}\varphi_d(t)$,

(b) $\varphi_p(t)=t^{p-1}+\ldots+t+1$, *falls* p *eine Primzahl ist,*

(c) $\varphi_n(t)=\dfrac{t^n-1}{\displaystyle\prod_{1\le d<n\,:\,d|n}\varphi_d(t)}$.

Unter Verwendung von Folgerung 3.21 erhalten wir $\varphi_1(t)=t-1$, $\varphi_2(t)=t+1$, $\varphi_3(t)=t^2+t+1$, $\varphi_4(t)=t^2+1$, $\varphi_5(t)=t^4+t^3+t^2+t+1$, $\varphi_6(t)=t^2-t+1$.

Satz 3.22 *Das* n*-te Kreisteilungspolynom über* $\mathbb{Q}$ *gehört zu* $\mathbb{Z}[t]$ *und ist irreduzibel über* $\mathbb{Z}$ *und somit auch über* $\mathbb{Q}$.

Bemerkung. Bezeichnen wir mit $\mathbb{K}_0$ die Menge der mit Zirkel und Lineal konstruierbaren komplexen Zahlen, so bleiben die Aussagen von Folgerung 3.13 gültig, wenn man dort $\mathbb{K}$ durch $\mathbb{K}_0$ und $\mathbb{R}$ durch $\mathbb{C}$ ersetzt.

Satz 3.23 *Ist das regelmäßige* n*-Eck mit Zirkel und Lineal konstruierbar, so gilt* $n=2^k p_1\cdots p_r$ *mit paarweise verschiedenen Fermat'schen Primzahlen* $p_1,\ldots,p_r$, *d.h.* $p_j=2^{m_j}+1$ *mit* $m_j\in\mathbb{N}$.

3.4 Die Galois-Gruppe einer Körpererweiterung

Sind $X\neq\emptyset$ eine beliebige Menge und $\mathbf{K}$ ein Körper, so bezeichnen wir mit $\mathcal{F}(X,\mathbf{K})$ die Menge der Abbildungen $f: x\longrightarrow \mathbf{K}$. Vereinbaren wir für $f,g\in\mathcal{F}(X,\mathbf{K})$ und $\alpha,\beta\in\mathbf{K}$

$$(\alpha f+\beta g)(x):=\alpha f(x)+\beta g(x),$$

so wird $\mathcal{F}(X,\mathbf{K})$ zu einem linearen Raum über $\mathbf{K}$.

Satz 3.24 *Ist* $(\mathbf{G},\cdot)$ *eine Gruppe und sind* $\varphi_1,\ldots,\varphi_n : \mathbf{G} \longrightarrow \mathbf{K}^*$ *Gruppenhomomorphismen, so sind diese genau dann in* $\mathcal{F}(\mathbf{G},\mathbf{K})$ *linear unabhängig, wenn sie paarweise verschieden sind.*

Sind $\mathbf{L}_1 : \mathbf{K}$ und $\mathbf{L}_2 : \mathbf{K}$ Körpererweiterungen mit $[\mathbf{L}_1 : \mathbf{K}] < \infty$, so ist die Menge der $\mathbf{K}$-linearen Abbildungen $L_{\mathbf{K}}(\mathbf{L}_1,\mathbf{L}_2)$ von $\mathbf{L}_1 : \mathbf{K}$ nach $\mathbf{L}_2 : \mathbf{K}$ ein endlichdimensionaler linearer Teilraum von $\mathcal{F}(\mathbf{L}_1,\mathbf{L}_2)$ der Dimension $[\mathbf{L}_1 : \mathbf{K}]$. Beachte: Wir betrachten hier $L_{\mathbf{K}}(\mathbf{L}_1,\mathbf{L}_2)$ als linearen Teilraum des linearen Raumes $\mathcal{F}(\mathbf{L}_1,\mathbf{L}_2)$ mit dem Skalarkörper $\mathbf{L}_2$.

Ein Monomorphismus $\varphi : \mathbf{L}_1 \longrightarrow \mathbf{L}_2$ gehört genau dann zu $L_{\mathbf{K}}(\mathbf{L}_1,\mathbf{L}_2)$, wenn $\varphi(x) = x$ für alle $x \in \mathbf{K}$ gilt.

Folgerung 3.25 *Sind* $\mathbf{L}_1 : \mathbf{K}$ *und* $\mathbf{L}_2 : \mathbf{K}$ *Körpererweiterungen mit* $[\mathbf{L}_1 : \mathbf{K}] < \infty$ *und* $\varphi_1,\ldots,\varphi_n : \mathbf{L}_1 \longrightarrow \mathbf{L}_2$ *paarweise verschiedene Monomorphismen mit* $\varphi_j|_{\mathbf{K}} = \mathrm{id}_{\mathbf{K}}$, $j = 1,\ldots,n$, *so gilt* $n \leq [\mathbf{L}_1 : \mathbf{K}]$.

Definition 3.26 *Es sei* $\mathbf{L}_{\mathbf{K}}$ *eine Körpererweiterung. Die Menge* $\mathcal{G}(\mathbf{L} : \mathbf{K})$ *der Automorphismen von* $\mathbf{L}$, *deren Einschränkung auf* $\mathbf{K}$ *gleich der Identität in* $\mathbf{K}$ *ist, ist offenbar eine Untergruppe der Automorphismengruppe von* $\mathbf{L}$. *Sie wird* **Galois-Gruppe** *von* $\mathbf{L} : \mathbf{K}$ *genannt.*

Folgerung 3.27 *Ist* $\mathbf{L} : \mathbf{K}$ *eine endliche Körpererweiterung, so gilt* $|\mathcal{G}(\mathbf{L} : \mathbf{K})| \leq [\mathbf{L} : \mathbf{K}]$.

Eine Erweiterung $\mathbf{L} : \mathbf{K}$ nennt man **normal** , wenn sie algebraisch ist und wenn jedes irreduzible Polynom $f \in \mathbf{K}[t]$, für welches ein $a \in \mathbf{L}$ mit $f(a) = 0$ existiert, über $\mathbf{L}$ in Linearfaktoren zerfällt.

Ein Polynom $f \in \mathbf{K}[t]$ heißt **separabel**, wenn jeder irreduzible Faktor von f nur einfache Wurzeln hat. Der Körper $\mathbf{K}$ wird **vollkommen** genannt, wenn jedes Polynom aus $\mathbf{K}[t]$ separabel ist.

Folgerung 3.28 *Es sei* $\mathbf{K}$ *ein Körper. Dann gilt:*

(a) *Ist die Erweiterung* $\mathbf{L} : \mathbf{K}$ *normal und endlich, so existiert ein* $f \in \mathbf{K}[t]$, *für welches* $\mathbf{L} : \mathbf{K}$ *Zerfällungskörper ist.*

(b) *Ist* $\mathrm{char}\,\mathbf{K} = 0$, *so ist* $\mathbf{K}$ *vollkommen.*

(c) *Ist* $\mathrm{char}\,\mathbf{K} = p > 0$, *so ist* $\mathbf{K}$ *genau dann vollkommen, wenn die Frobenius-Abbildung* $F : \mathbf{K} \longrightarrow \mathbf{K}$, $x \mapsto x^p$ *surjektiv ist.*

(d) *Ist* $|\mathbf{K}| < \infty$, *so ist* $\mathbf{K}$ *vollkommen.*

Bemerkung *Es gilt auch die Umkehrung zu Folgerung 3.28,(a), d.h., ist* $\mathbf{L} : \mathbf{K}$ *Zerfällungskörper eines Polynoms* $f \in \mathbf{K}[t]$, *so ist die Erweiterung* $\mathbf{L} : \mathbf{K}$ *normal.*

Ist $\mathbf{L} : \mathbf{K}$ eine Körpererweiterung, so nennt man ein $a \in \mathbf{L}$ **separabel** über $\mathbf{K}$, wenn a Wurzel eines separablen Polynoms aus $\mathbf{K}[t]$ ist. Die Erweiterung $\mathbf{L} : \mathbf{K}$ heißt **separabel**, wenn jedes $a \in \mathbf{L}$ separabel über $\mathbf{K}$ ist.

Folgerung 3.29 *Für eine algebraische Körpererweiterung* $\mathbf{L} : \mathbf{K}$ *gilt:*

(a) *Ist* $\mathbf{K}$ *vollkommen, so ist* $\mathbf{L} : \mathbf{K}$ *separabel.*

(b) *Ist* $|\mathbf{K}| < \infty$, *so ist* $\mathbf{L} : \mathbf{K}$ *separabel.*

(c) *Ist* $\operatorname{char} \mathbf{K} = 0$, *so ist* $\mathbf{L} : \mathbf{K}$ *separabel.*

Folgerung 3.30 *Es seien* $\mathbf{L} : \mathbf{K}$ *eine Körpererweiterung und* $a \in \mathbf{L}$ *algebraisch über* $\mathbf{K}$ *mit Minimalpolynom* $m_a \in \mathbf{K}[t]$. *Dann sind folgende Aussagen äquivalent:*

(a) a *ist separabel.*

(b) m_a *ist separabel.*

(c) a *ist einfache Wurzel von* m_a.

(d) $m_a' \neq 0$.

Folgerung 3.31 *Jede endliche, normale und separable Körpererweiterung* $\mathbf{L} : \mathbf{K}$ *ist Zerfällungskörper eines separablen Polynoms aus* $\mathbf{K}[t]$.

Satz 3.32 (Satz vom primitiven Element) *Es seien* $\mathbf{L} : \mathbf{K}$ *eine Körpererweiterung,* $a \in \mathbf{L}$ *separabel und* $b \in \mathbf{L}$ *algebraisch. Dann existiert ein* $c \in \mathbf{L}$ *mit* $\mathbf{K}(a, b) = \mathbf{K}(c)$.

Satz 3.33 *Ist* $\mathbf{L} : \mathbf{K}$ *eine endliche, normale und separable Körpererweiterung, so gilt*

$$|\mathcal{G}(\mathbf{L} : \mathbf{K})| = [\mathbf{L} : \mathbf{K}] .$$

In Anlehnung an den Beweis von Satz 3.32 findet man folgendes: Sind $\mathbf{L} = \mathbf{K}(a)$ und $n = \deg m_a(t)$, so sind die Elemente $\varphi \in \mathcal{G}(\mathbf{L} : \mathbf{K})$ gegeben durch

$$\varphi(x) = \varphi_j(x) = \sum_{k=0}^{n-1} \xi_k a_j^k , \quad x = \sum_{k=0}^{n-1} \xi_k a^k \in \mathbf{L} = \mathbf{K}(a) , \quad j = 1, \ldots, r ,$$

wobei $\{a_1, \ldots, a_r\}$ die Menge der Wurzeln von $m_a(t)$ in $\mathbf{L}$ bezeichnet.

Beispiel 3.34 *Unter Anwendung der vorhergehenden Aussage erhalten wir*

(a) $\mathcal{G}(\mathbb{C} : \mathbb{R}) = \{\varphi_1, \varphi_2\}$ *mit* $\varphi_1(z) = z$, $\varphi_2(z) = \overline{z}$,

(b) $\mathcal{G}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = \left\{\mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}\right\}$,

(c) $\mathcal{G}(\mathbf{L} : \mathbf{P}) = \mathrm{Aut}\,\mathbf{L}$, *wobei* $\mathbf{P}$ *der Primkörper von* $\mathbf{L}$ *und* $\mathrm{Aut}\,\mathbf{L}$ *die Gruppe der Automorphismen über* $\mathbf{L}$ *sind,*

(d) $\mathcal{G}(\mathbb{R} : \mathbb{Q}) = \{\mathrm{id}_{\mathbb{R}}\}$,

(e) $\mathcal{G}(\mathbb{Q}(\omega) : \mathbb{Q}) \cong \mathbb{Z}_n^*$, *wobei* $\omega = e^{\frac{2\pi \mathrm{i}}{n}}$ *primitive n-te Einheitswurzel und somit* $\mathbb{Q}(\omega)$ *der n-te Kreisteilungskörper über* $\mathbb{Q}$ *sind.*

Unter der **Galois-Gruppe** $\mathcal{G}(f, \mathbf{K})$ eines Polynoms $f \in \mathbf{K}[t] \backslash \mathbf{K}$ versteht man die Galois-Gruppe $\mathcal{G}(\mathbf{L} : \mathbf{K})$ des Zerfällungskörpers $\mathbf{L} : \mathbf{K}$ von f . Nach Beispiel 3.34,(e) ist die Galois-Gruppe $\mathcal{G}(\varphi_n, \mathbb{Q})$ des n-ten Kreisteilungspolynoms $\varphi_n(t)$ isomorph zur primen Restklassengruppe $\mathbb{Z}_n^*$.

Sind $f \in \mathbf{K}[t]$, $\mathbf{L} : \mathbf{K}$ der Zerfällungskörper von f und $a_1, \ldots, a_r \in \mathbf{L}$ die verschiedenen Wurzeln von f , so ist $\mathcal{G}(f, \mathbf{K})$ isomorph zu einer Untergruppe der symmetrischen Gruppe $\mathcal{S}_r$. Nutzt man die Tatsache aus, dass für eine Primzahl p die symmetrische Gruppe $\mathcal{S}_p$ durch $(1, \ldots, p)$ und eine Transposition $(1, k)$ erzeugt wird, so erhält man folgendes Resultat: Sind p eine Primzahl, $f \in \mathbf{K}[t]$ irreduzibel, $\deg f = p$, und enthält $\mathcal{G}(f, \mathbf{K})$ ein Element der Ordnung p und eine Transposition, so ist $\mathcal{G}(f, \mathbf{K})$ isomorph zu $\mathcal{S}_p$.

Folgerung 3.35 *Sind* $f \in \mathbb{Q}[t]$ *irreduzibel,* $p = \deg f$ *eine Primzahl, und hat* f *nur zwei nicht reelle Wurzeln, so gilt* $\mathcal{G}(f, \mathbf{K}) \cong \mathcal{S}_p$.

Dies ergibt sich aus dem vorhergehenden Resultat wie folgt: Die Abbildung $z \to \overline{z}$, eingeschränkt auf die Menge der Wurzeln von f , liefert die Transposition. Sind $\mathbf{L}$ der Zerfällungskörper von f über $\mathbb{Q}$ und $a \in \mathbf{L}$ eine Wurzel von f , so gilt wegen der Irreduzibilität von f und Satz 3.4 sowie Folgerung 3.10,(c)

$$[\mathbf{L} : \mathbb{Q}] = [\mathbf{L} : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}] = [\mathbf{L} : \mathbb{Q}(a)] \cdot p \,.$$

Also ist p Teiler von $[\mathbf{L} : \mathbb{Q}] = |\mathcal{G}(f, \mathbb{Q})|$ (siehe Satz 3.33, Folgerung 3.29, Folgerung 3.28,(b) und die Bemerkung nach Folgerung 3.28). Nach Folgerung 1.31 besitzt $\mathcal{G}(f, \mathbb{Q})$ somit auch ein Element der Ordnung p .

Sind $\mathbf{G} = (\mathbf{G}, \cdot)$ eine Gruppe und $a, b \in \mathbf{G}$, so nennt man $[a, b] := aba^{-1}b^{-1}$ den **Kommutator** von a und b . Man beachte, dass $ab = [a, b]ba$ gilt. Mit $K(\mathbf{G})$ bezeichnen wir die von allen Kommutatoren $[a, b]$, $a, b \in \mathbf{G}$ erzeugte Untergruppe von $\mathbf{G}$. Wegen $[a, b]^{-1} = [b, a]$ besteht $K(\mathbf{G})$ aus allen endlichen Produkten von Kommutatoren.

(A) $K(\mathbf{G})$ ist ein Normalteiler in $\mathbf{G}$.

(B) Ist $\mathbf{N}$ eine Normalteiler in $\mathbf{G}$, so ist $\mathbf{G}/\mathbf{N}$ genau dann abelsch, wenn $K(\mathbf{G}) \subset \mathbf{N}$ gilt.

Für die symmetrischen Gruppen $\mathcal{S}_n$ und die alternierenden Gruppen $\mathcal{A}_n$ gilt $K(\mathcal{S}_n) = \mathcal{A}_n$, $n \geq 2$, $K(\mathcal{A}_2) = \{(1)\}$, $K(\mathcal{A}_3) = \{(1)\}$, $K(\mathcal{A}_4) = \mathbf{V}_4$ und $K(\mathcal{A}_n) = \mathcal{A}_n$, $n \geq 5$. Wir definieren $K_0(\mathbf{G}) := \mathbf{G}$, $K_{n+1}(\mathbf{G}) := K(K_n(\mathbf{G}))$, $n \in \mathbb{N}_0$. Eine Gruppe $\mathbf{G}$ heißt **auflösbar**, wenn ein $m \in \mathbb{N}$ existiert, so dass $K_m(\mathbf{G}) = \{e\}$ gilt. Somit sind die symmetrischen Gruppen $\mathcal{S}_n$ für $n \geq 5$ nicht auflösbar, aber für $n \leq 4$.

Eine Körpererweiterung $\mathbf{L} : \mathbf{K}$ nennt man **Radikalerweiterung**, wenn es Zwischenkörper $\mathbf{K}_j$ gibt, so dass

$$\mathbf{K} = \mathbf{K}_1 \subset \mathbf{K}_2 \subset \ldots \subset \mathbf{K}_m = \mathbf{L}\,, \quad \mathbf{K}_{j+1} = \mathbf{K}_j(b_j)\,,\ j = 1, \ldots, m-1\,,$$

gilt, wobei b_j Wurzel eines Polynoms $t^{n_j} - a_j \in \mathbf{K}_j[t]$ ist. Ein Polynom $f \in \mathbf{K}[t]$ heißt über $\mathbf{K}$ **durch Radikale lösbar**, wenn eine Radikalerweiterung $\mathbf{L} : \mathbf{K}$ existiert, die alle Wurzeln von $f(t)$ enthält.

Satz 3.36 *Ist $\mathbf{K}$ ein Körper der Charakteristik Null, so ist $f \in \mathbf{K}[t]$ genau dann über $\mathbf{K}$ durch Radikale lösbar, wenn die Galois-Gruppe $\mathcal{G}(f, \mathbf{K})$ auflösbar ist.*

Ist also $\mathcal{G}(f, \mathbf{K})$ abelsch, so ist $f(t)$ über $\mathbf{K}$ durch Radikale auflösbar. Insbesondere gilt (vgl. Bsp. 3.34,(e))

Folgerung 3.37 *Die Kreisteilungspolynome $\varphi_n(t)$ sind über $\mathbb{Q}$ durch Radikale auflösbar.*

Beispiel 3.38 *Das Polynom $f(t) = t^5 - 6t^3 + 3 \in \mathbb{Q}[t]$ ist über $\mathbb{Q}$ nicht durch Radikale lösbar.*

Sei $\operatorname{char} \mathbf{K} = 0$. Wir betrachten $a_1, \ldots, a_n$ als Unbestimmte. Das Polynom $f(t) = t^n + a_1 t^{n-1} + \ldots + a_{n-1}t + a_n \in \mathbf{K}(a_1, \ldots, a_n)[t]$ nennt man **allgemeines Polynom** n-ten Grades. Die dazugehörige Galoisgruppe $\mathcal{G}(f, \mathbf{K}(a_1, \ldots, a_n))$ ist isomorph zu $\mathcal{S}_n$. Somit ist das allgemeine Polynom n-ten Grades für $n \geq 5$ nicht durch Radikale lösbar, aber für $n \leq 4$.

Bemerkung: Verzichtet man auf die Vorausetzung $\operatorname{char} \mathbf{K} = 0$, so gilt (vgl. Satz 3.36): Ist $f \in \mathbf{K}[t]$ über $\mathbf{K}$ duch Radikale lösbar, so ist die Galois-Gruppe $\mathcal{G}(f, \mathbf{K})$ auflösbar.

3.5 Anhang

Für eine Teilmenge $\mathcal{A} \subset \mathcal{G}(\mathbf{L} : \mathbf{K})$ definieren wir

$$F(\mathbf{L}, \mathcal{A}) := \{x \in \mathbf{L} : \varphi(x) = x\ \forall\, \varphi \in \mathcal{A}\}\ .$$

Es zeigt sich, dass $F(\mathbf{L}, \mathcal{A})$ ein Zwischenkörper von $\mathbf{L} : \mathbf{K}$ ist, der sogenannte **Fixkörper** von $\mathcal{A}$ in $\mathbf{L}$. Wir bezeichen mit $U := U(\mathbf{L} : \mathbf{K})$ die Menge aller Untergruppen von $\mathcal{G}(\mathbf{L} : \mathbf{K})$, mit $\mathcal{Z} := \mathcal{Z}(\mathbf{L} : \mathbf{K})$ die Menge aller Zwischenkörper von $\mathbf{L} : \mathbf{K}$ und definieren die Abbildungen

$$\Phi : U \longrightarrow \mathcal{Z}\,, \quad \mathcal{U} \mapsto F(\mathbf{L} : \mathcal{U}) \quad \text{sowie} \quad \Gamma : \mathcal{Z} \longrightarrow U\,, \quad \mathbf{M} \mapsto \mathcal{G}(\mathbf{L} : \mathbf{M})\,.$$

Für $\mathbf{M}, \mathbf{M}_1, \mathbf{M}_2 \in \mathcal{Z}$ und $\mathcal{U}, \mathcal{U}_1, \mathcal{U}_2 \in U$ gilt dann

(1) $\mathbf{M} \subset \Phi(\Gamma(\mathbf{M}))\,,$

(2) $\mathcal{U} \subset \Gamma(\Phi(\mathcal{U}))\,,$

(3) $\mathbf{M}_1 \subset \mathbf{M}_2 \implies \Gamma(\mathbf{M}_2) \subset \Gamma(\mathbf{M}_1)\,,$

(4) $\mathcal{U}_1 \subset \mathcal{U}_2 \implies \Phi(\mathcal{U}_2) \subset \Phi(\mathcal{U}_1)$.

Hieraus kann man schließen, dass $\Gamma \circ \Phi \circ \Gamma = \Gamma$ und $\Phi \circ \Gamma \circ \Phi = \Phi$ gilt.

Man nennt eine Körpererweiterung $\mathbf{L} : \mathbf{K}$ **Galois-Erweiterung** oder **galoisch**, wenn $\mathbf{K} = F(\mathbf{L}, \mathcal{G}(\mathbf{L} : \mathbf{K}))$ gilt. Die Erweiterung $\mathbb{C} : \mathbb{R}$ ist galoisch, ebenso die in Beispiel 3.34,(e) betrachtete Erweiterung $\mathbb{Q}(\omega) : \mathbb{Q}$. Der Hauptsatz der Galois-Theorie besagt nun Folgendes.

Satz 3.39 *Ist* $\mathbf{L} : \mathbf{K}$ *eine endliche Galois-Erweiterung, so sind* $\Phi : U \longrightarrow \mathcal{Z}$ *und* $\Gamma : \mathcal{Z} \longrightarrow U$ *bijektive Abbildungen und zueinander invers. Für jeden Zwischenkörper* $\mathbf{M}$ *von* $\mathbf{L} : \mathbf{K}$ *und jede Untergruppe* $\mathcal{U}$ *von* $\mathcal{G}(\mathbf{L} : \mathbf{K})$ *gilt*

$$[\mathbf{M} : \mathbf{K}] = [\mathcal{G}(\mathbf{L} : \mathbf{K}) : \Gamma(\mathbf{M})] \quad \textit{und} \quad [\mathbf{L} : \Phi(\mathcal{U})] = |\mathcal{U}|\,.$$

Für $\mathbf{M} \in \mathcal{Z}(\mathbf{L} : \mathbf{K})$ *ist* $\mathbf{M} : \mathbf{K}$ *genau dann galoisch, wenn* $\Gamma(\mathbf{M}) = \mathcal{G}(\mathbf{L} : \mathbf{M})$ *ein Normalteiler in* $\mathcal{G}(\mathbf{L} : \mathbf{K})$ *ist. Dabei gilt* $\mathcal{G}(\mathbf{M} : \mathbf{K}) \cong \mathcal{G}(\mathbf{L} : \mathbf{K})/\mathcal{G}(\mathbf{L} : \mathbf{M})$.

Index