Algebra I - Kurzskript - WS 2003/04

Dozent: Prof. Dr. Kreuzer
LaTeX-Abschrift: Ingo Manfraß

16. Oktober 2004

Dieses Kurzskript ist aus einer Mitschrift der Vorlesung Algebra I bei *Professor Dr. Kreuzer* im Wintersemester 2003/04 entstanden. Ich habe versucht alles richtig wiederzugeben, kann allerdings keine Garantie darauf geben. Es ist deshalb wahrscheinlich, dass dieses Skriptum Fehler enthält.

Inhaltsverzeichnis

Kapitel I - Gruppentheorie 4

1 Grundlagen 4

2 Kristallographie 10

3 Restklassengruppen 13
A. Operationen von Gruppen auf Mengen 13
B. Normalteiler 17
C. Die Noetherschen Isomorphiesätze 19

4 Konstruktion von Gruppen 20
A. Produkte 20
B. Präsentationen 23

5 Abelsche Gruppen 26
A. Zyklische Gruppen 26
B. Endlich erzeugte Abelsche Gruppen 28

6 p-Gruppen 30
A. Der Satz von Cauchy 30
B. Die Sätze von Sylow 31

7 Auflösbare Gruppen 34

Kapitel II - Galoistheorie 36

8 Grundlagen 36
A. Ringe 36
B. Körper 41

9 Konstruktionen mit Zirkel und Lineal 44

10 Auflösung algebraischer Gleichungen 47

11 Ringe und Algebren 48
A. Teilbarkeitstheorie in Ringen 48
B. Polynomringe 50
C. Kommutative Algebren 53

12 Algebraische Körpererweiterungen 55
A. Endliche algebraische Körpererweiterungen 55
B. Der algebraische Abschluß eines Körpers 58

13 Separable Körpererweiterungen **60**

14 Normale Körpererweiterung **63**

15 Galoische Körpererweiterung **65**
A. Grundlagen 65
B. Der Hauptsatz der Galoistheorie 67
C. Der Satz vom primitiven Element 69

16 Kreisteilungskörper **70**
A. Grundlagen 70
B. Konstruktion regulärer n-Ecke 73

17 Weitere Anwendungen der Galoistheorie **74**
A. Endliche Körper 74
B. Der Fundamentalsatz der Algebra 75
C. Auflösung von Gleichungen durch Radikale 75

Index **79**

Kapitel I
Gruppentheorie

1 Grundlagen

Definition 1.1 Sei G eine Menge und $\circ : G \times G \to G$ eine Verknüpfung auf G.

a) $(G, \circ)$ heißt *Halbgruppe*, wenn das *Assoziativgesetz* gilt:

$$(a \circ b) \circ c = a \circ (b \circ c) \qquad \forall\, a, b, c \in G$$

b) $(G, \circ)$ heißt *Monoid*, wenn G eine Halbgruppe ist und ein *neutrales Element* besitzt, d.h.

$$\exists\, e \in G :\ e \circ a = a \circ e = a \qquad \forall\, a \in G$$

c) $(G, \circ)$ heißt eine *Gruppe*, wenn G ein Monoid ist und jedes Element $a \in G$ ein *inverses Element*
indexinverses Element a^{-1} besitzt, d.h.

$$\exists\, a^{-1} \in G :\ a^{-1} \circ a = a \circ a^{-1} = e$$

d) Eine Halbgruppe / ein Monoid / eine Gruppe heißt *Abelsch* (oder kommutativ), wenn gilt

$$\forall\, a, b \in G :\ a \circ b = b \circ a$$

Beispiel 1.2

a) $\mathbb{N} = \{0, 1, 2, \dots\}$ ist bzgl. $+$ ein Monoid.

b) $(\mathbb{Z}, +)$ ist eine Gruppe.

c) $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ ist eine Gruppe bzgl. $+$.
Die Elemente von $\mathbb{Z}/_{n\mathbb{Z}}$ sind die *Restklassen* $a + n\mathbb{Z}$ mit $a \in \mathbb{Z}$. Verschiedene Restklassen erhält man für $a \in \{0, \dots, n-1\}$. Die Addition ist definiert durch $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$.
Die Gruppe $\mathbb{Z}/_{n\mathbb{Z}}$ heißt die *zyklische Gruppe* der

Ordnung n. Die Restklasse $a + n\mathbb{Z}$ ist die Menge $\{a + nb \mid b \in \mathbb{Z}\}$.

d) Sei M eine Menge. Dann ist:

$$\mathrm{Abb}(M, M) = \{f : M \to M \text{ Abbildung}\}$$

bzgl. der Komposition $\circ$ ein Monoid.
Die Menge

$$\mathrm{Bij}(M,M) = \{f : M \to M \text{ bijektive Abbildung}\}$$

ist eine Gruppe bzgl. $\circ$. Sie heißt die *Transformationsgruppe* von M.
Im Allgemeinen gilt hier das Kommutativgesetz nicht!

e) Sei p eine Primzahl, so ist $\mathbb{F}_p = \mathbb{Z}/_{p\mathbb{Z}}$ ein Körper und $\mathbb{F}_p \setminus \{0\}$ ist bzgl. der Multiplikation $(a+p\mathbb{Z})\cdot(b+p\mathbb{Z}) = ab+p\mathbb{Z}$ eine Gruppe. Das inverse Element $(a+p\mathbb{Z})^{-1}$ einer Restklasse $a+p\mathbb{Z}$ findet man dabei mit Hilfe des erweiterten Euklidischen Algorithmus.

$$(a+p\mathbb{Z})(\tilde{a}+p\mathbb{Z}) = 1+p\mathbb{Z} \qquad \Leftrightarrow \qquad a\tilde{a}+cp = 1$$

Notation 1.3 a) Für eine kommutative Gruppe verwendet man meist die sogenannte *additive Notation*:
Die Verknüpfung heißt $+$, das neutrale Element heißt 0 und das inverse Element zu $a \in G$ heißt $-a$.

b) Bei der *multiplikativen Notation* heißt die Verknüpfung $\cdot$, das neutrale Element 1, und das inverse Element zu $a \in G$ heißt a^{-1}.

c) Im ersten Fall setzen wir

$$n \cdot a = \begin{cases} \underbrace{a+a+\cdots+a}_{n\text{-mal}} & \text{für } n \geq 0 \\ -(-n)\cdot a & \text{für } n < 0 \end{cases}$$

Im zweiten Fall setzen wir

$$a^n = \begin{cases} \underbrace{a\cdot a\cdot \ldots \cdot a}_{n\text{-mal}} & \text{für } n \geq 0 \\ (a^{-n})^{-1} & \text{für } n < 0 \end{cases}$$

Satz 1.4 *Einfache Eigenschaften von Gruppen*
Sei $(G,\circ)$ eine Gruppe.

a) Das neutrale Element e ist eindeutig bestimmt.

b) Zu jedem $a \in G$ ist das inverse Element a^{-1} eindeutig bestimmt.

c) Für $a,b \in G$ gilt $(a\circ b)^{-1} = b^{-1}\circ a^{-1}$

d) Es gelten die *Kürzungsregeln*:

d1) $a\circ b = a\circ c \quad \Rightarrow \quad b = c \qquad \forall\, a,b,c \in G$

d2) $b \circ a = c \circ a \quad \Rightarrow \quad b = c \qquad \forall\, a, b, c \in G$

e) Für jedes Element $a \in G$ sind die *Rechtstranslation* um a

$$\rho_a : \begin{array}{ccc} G & \to & G \\ b & \mapsto & b \circ a \end{array}$$

und die *Linkstranslation* um a

$$\lambda_a : \begin{array}{ccc} G & \to & G \\ b & \mapsto & a \circ b \end{array}$$

bijektive Abbildungen.

Bemerkung 1.5 *Gruppentafeln*
Ist $(G, \circ)$ eine endliche Gruppe, so kann man die Verknüpfung $\circ$ (und damit die Gruppenstruktur) beschreiben durch die *Gruppentafel*:
Sei $G = \{a_1, \ldots, a_n\}$

	a_1	a_2	$\cdots$	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	$\cdots$	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	$\cdots$	$a_2 \circ a_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	$a_n \circ a_1$	$a_n \circ a_2$	$\cdots$	$a_n \circ a_n$

Definition 1.6 Seien $(G, \circ)$ und $(H, \star)$ zwei Gruppen.

a) Eine nicht leere Teilmenge $U \subseteq G$ heißt eine *Untergruppe* von G, wenn gilt

1.) $a \circ b \in U \qquad \forall\, a, b \in U$

2.) $a \in U \quad \Rightarrow \quad a^{-1} \in U$

b) Eine Abbildung $f : G \to H$ heißt ein *Gruppenhomomorphismus* oder ein *Homomorphismus von Gruppen*, wenn gilt:

$$f(a \circ b) = f(a) \star f(b) \qquad \forall\, a, b \in G$$

c) Ein bijektiver Gruppenhomomorphismus $f : G \to H$ heißt auch *Isomorphismus* von Gruppen.

d) Gibt es einen Isomorphismus von Gruppen $f : G \to H$, so heißen G und H *isomorph*.

e) Ein Isomorphismus von Gruppen $f : G \to G$ heißt auch ein *Automorphismus* der Gruppe G.

Beispiel 1.7

a) $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$.

b) Zu jeder Gruppe G ist $\{e\}$ eine Untergruppe. Sie heißt die *triviale Untergruppe*.

c) Zu jeder Gruppe G ist G eine Untergruppe.

d) Betrachte die Gruppe $(\mathbb{Z}, +)$. Für jedes $n \in \mathbb{Z}$ ist dann

$$\mu_n : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ a & \mapsto & n \cdot a \end{array}$$

ein Gruppenhomorphismus.

e) Sei G die Gruppe $(\mathbb{R}, +)$ und H die Gruppe $(\mathbb{R}_+, \cdot)$. dann sind G und H isomorph. Die Exponentialfunktion

$$\exp : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R}_+ \\ x & \mapsto & e^x \end{array}$$

ist ein Isomorphismus von Gruppen.

Satz 1.8 *Eigenschaften von Untergruppen und Gruppenhomomorphismen*
Seien $(G, \circ)$ und $(H, \star)$ Gruppen mit neutralen Elementen e_G bzw. e_H. Weiter sei $f : G \to H$ ein Gruppenhomomorphismus.

a) Ist $U \subseteq G$ eine Untergruppe, so ist U bzgl. $\circ|_U : U \times U \to U$ selbst eine Gruppe. Insbesondere ist $\iota : U \hookrightarrow G$ ein Gruppenhomomorphismus.

b) Es gilt $f(e_G) = e_H$.

c) Ist $U \subseteq G$ eine Untergruppe, so ist $f(U) \subseteq H$ eine Untergruppe.

d) Ist $V \subseteq H$ eine Untergruppe, so ist $f^{-1}(V) \subseteq G$ eine Untergruppe.

e) Für alle $a \in G$ gilt $f(a)^{-1} = f(a^{-1})$.

f) Genau dann ist f injektiv, wenn $\ker(f) = \{e_G\}$ gilt.
Hierbei gilt $\ker(f) = f^{-1}(\{e_H\})$.

g) Ist $f : G \to H$ ein Isomorphismus von Gruppen, so ist $f^{-1} : H \to G$ ebenfalls ein Isomorphismus von Gruppen.

Beispiel 1.9 *Symmetrische Gruppe*
Sei $M = \{1, 2, \ldots, n\}$ mit $n \geq 1$. Die Gruppe $\mathrm{Bij}(M, M)$ wird auch mit $\mathcal{S}_n$ bezeichnet und heißt die *n-te symmetrische Gruppe* oder die n-te *Permutationsgruppe*. Die Elemente von $\mathcal{S}_n$ heißen *Permutationen*.
Statt

$$\sigma : \begin{array}{ccc} \{1,2,\ldots,n\} & \to & \{1,2,\ldots,n\} \\ i & \mapsto & \sigma(i) \end{array}$$

schreiben wir auch

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

a) Es gilt $\#\mathcal{S}_n = n!$

b) Für $n \geq 3$ ist $\mathcal{S}_n$ nicht Abelsch.

c) Eine Permutation der Form

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & i-1 & i & i+1 & \cdots & j-1 & j & j+1 & \cdots & n \\ 1 & 2 & \cdots & i-1 & j & i+1 & \cdots & j-1 & i & j+1 & \cdots & n \end{pmatrix}$$

mit $1 \leq i < j \leq n$ heißt eine *Transposition*.
Jede Permutation ist als Produkt von Transpositionen darstellbar. Diese Darstellung ist jedoch nicht eindeutig.

d) Besitzt eine Permutation eine Darstellung als Produkt einer geraden (bzw. ungeraden) Anzahl von Transpositionen, so heißt sie eine *gerade* (bzw. *ungerade*) Permutation. Diese Eigenschaft hängt nicht ab von der Wahl der Darstellung.

e) Die Abbildung

$$\mathrm{sign} : \begin{array}{ccc} \mathcal{S}_n & \to & \{1,-1\} \\ \sigma & \mapsto & \begin{cases} 1 & \text{falls } \sigma \text{ gerade} \\ -1 & \text{falls } \sigma \text{ ungerade} \end{cases} \end{array}$$

heißt *Signum*. Sie ist ein surjektiver Gruppenhomomorphismus.

f) Die Untergruppe $\mathcal{A}_n = \ker(\mathrm{sign}) \subseteq \mathcal{S}_n$ heißt die *n-te alternierende Gruppe*. Für jede ungerade Permutation $\sigma \in \mathcal{S}_n$ gilt:

$$\mathcal{S}_n = \mathcal{A}_n \cup \sigma\mathcal{A}_n = \mathcal{A}_n \cup \mathcal{A}_n\sigma$$

Insbesondere folgt $\#\mathcal{A}_n = \frac{1}{2}n!$

Definition 1.10 a) Sei G eine Gruppe und $a \in G$. Dann heißt die Zahl

$$\mathrm{ord}_G(a) = \begin{cases} \min\{i > 0 \mid a^i = e\} & \text{falls dieses Minimum existiert} \\ \infty & \text{sonst} \end{cases}$$

die *Ordnung* von a in G.

b) Ist G eine endliche Gruppe, so heißt

$$\mathrm{ord}(G) = \#G$$

auch die *Ordnung* von G.

Satz 1.11 *Kleiner Fermatscher Satz*
Sei G eine endliche Gruppe und sei $a \in G$ der Ordnung $r = \mathrm{ord}_G(a)$.

a) Die Menge $U = \{e, a, a^2, \dots\} = \{e, a, a^2, \dots, a^{r-1}\}$ ist eine Abelsche Untergruppe von G.
Sie heißt die von a erzeugte zyklische Untergruppe $U =< a >$.

b) Die Zahl $r = \mathrm{ord}_G(a)$ teilt $\mathrm{ord}(G) = \#G$.

Beispiel 1.12 Sei p eine Primzahl. Das Element $a+p\mathbb{Z} \in (\mathbb{Z}/_{p\mathbb{Z}} \setminus \{0\}, \cdot) = (\mathbb{F}_p^\star, \cdot)$ heißt eine *primitive Restklasse* modulo p, wenn $\mathrm{ord}_{\mathbb{F}_p^\star}(a + p\mathbb{Z}) = p - 1$, d.h. wenn $a + p\mathbb{Z}$ die Gruppe $\mathbb{F}_p^\star$ erzeugt.

Definition 1.13 Eine Gruppe G heißt *zyklisch*, wenn es ein $a \in G$ gibt, so dass

$$G = \{a^i \mid i \in \mathbb{Z}\}$$

gilt. In diesem Fall heißt a ein *primitives Element* oder ein *erzeugendes Element* von G. Wir schreiben

$$G =< a >$$

Offenbar sind zyklische Gruppen stets kommutativ.

Satz 1.14 *Eigenschaften zyklischer Gruppen*
Sei G eine zyklische Gruppe mit primitivem Element a.

a) Gilt $\mathrm{ord}_G(a) = \infty$, so ist

$$\varphi : \begin{array}{ccc} \mathbb{Z} & \to & G \\ i & \mapsto & a^i \end{array}$$

ein Isomorphismus von Gruppen.

b) Gilt $n = \mathrm{ord}_G(a) < \infty$, so ist

$$\psi : \begin{array}{ccc} \mathbb{Z}/_{n\mathbb{Z}} & \to & G \\ i + n\mathbb{Z} & \mapsto & a^i \end{array}$$

ein Isomorphismus von Gruppen.

c) Sei G endlich. Ist $U \subseteq G$ eine nichttriviale Untergruppe und $n = \mathrm{ord}(G) < \infty$, so gilt

$$U \cong \{0 + n\mathbb{Z}, m + n\mathbb{Z}, 2m + n\mathbb{Z}, \dots\}$$

Insbesondere ist jede Untergruppe einer zyklischen Gruppe zyklisch.

d) Sei $n = \mathrm{ord}(G) < \infty$. Ein Element $b = \psi(m+n\mathbb{Z})$ ist ein primitives Element von G genau dann, wenn $\mathrm{ggT}(m, n) = 1$ gilt.

e) Sei $n = \mathrm{ord}(G) < \infty$. Dann besitzt G genau $\varphi(n)$ primitive Elemente, wobei $\varphi(n) = \#\{0 < m < n \mid \mathrm{ggT}(m, n) = 1\}$ die *Eulersche Phi-Funktion* ist.

f) Sei $n = \mathrm{ord}(G) < \infty$ und $m \in \mathbb{Z}$ mit $\mathrm{ggT}(m, n) = 1$.
Dann gilt $\mathrm{ord}_G(a^m) = \mathrm{ord}_G(a) = n$.

2 Kristallographie

Definition 2.1 a) Ein *Kristall* ist ein anisotroper homogener Körper, der eine 3-dimensionale Anordnung der Bausteine besitzt (d.h. eine Kristallstruktur)

anisotrop verschiedene Beiträge einer physikalischen Eigenschaft in verschiedenen Richtungen

homogen gleiches Verhalten in parallelen Richtungen

b) Ein *Raumgitter* ist eine 3-dimensionale periodische Anordnung von Punkten. Sind p, q zwei Punkte des Raumgitters, so heißt die Gerade $\overline{pq}$ eine *Gittergerade*. Ist p ein Punkt eines Gitters und sind $\overline{pq}$ und $\overline{pq'}$ zwei verschiedene durch p gehende Gittergeraden, so heißt die Ebene $< p, q, q' >$ eine *Gitterebene* oder *Netzebene*.

c) Sei R ein Raumgitter und $p_0 = (0, 0, 0)$ ein Gitterpunkt. Drei Gitterpunkte p_1, p_2, p_3 liefern sogenannte *kristallographische Achsen* $\overline{p_0p_1}, \overline{p_0p_2}, \overline{p_0p_3}$, wenn die Translationen $p_1 - p_0, p_2 - p_0, p_3 - p_0$ das Gitter R in sich überführen und keine Gitterpunkte auf den Strecken $]p_0, p_1[,]p_0, p_2[,]p_0, p_3[$ liegen.

d) Die Punktmenge $E = \{a_1p_1 + a_2p_2 + a_3p_3 \in \mathbb{R}^3 \mid a_i \in [0, 1]\}$ heißt die *Elementarzelle* des Gitters. Die Einteilung der Elementarzelle in Bausteine des Kristalls nennt man die *Kristallbasis*.

e) Eine *Kristallstruktur* besteht aus einem Raumgitter und einer Kristallbasis der Elementarzelle des Gitters.

Beispiel 2.2 siehe Folien zur Kristallographie

Definition 2.3 Sei R ein Raumgitter im $\mathbb{R}^3$.
Eine orthogonale Abbildung $f : \mathbb{R}^3 \to \mathbb{R}^3$ heißt eine *Symmetrieoperation* (oder *Symmetrie*) von R, wenn $f(R) = R$ gilt.

Beispiel 2.4 Sei $R \subseteq \mathbb{R}^3$ ein Raumgitter.

a) Sind $\overline{p_0p_1}, \overline{p_0p_2}, \overline{p_0p_3}$ kristallographische Achsen von R, so sind alle Translationen um v mit $v \in \mathbb{Z}p_1 + \mathbb{Z}p_2 + \mathbb{Z}p_3$ Symmetrieoperationen von R.

b) Drehungen und Spiegelungen können ebenfalls Symmetrieoperationen sein. Ist f eine Drehung um eine Raumgerade um einen Winkel α und ist 2π ein Vielfaches von α, so heißt $\frac{2\pi}{\alpha}$ die *Zähligkeit* der Drehung.

Satz 2.5 Ist eine Drehung f eine Symmetrieoperation eines Raumgitters R, so ist sie 2-zählig, 3-zählig, 4-zählig oder 6-zählig.

Definition 2.6 Ein *Kristallsystem* besteht aus allen Kristallstrukturen, deren kristallographische Achsen dieselbe Gruppe von Symmetrieoperationen besitzen.

Satz 2.7

a) Es gibt 7 Kristallsysteme. Abhängig von den Längen der Kanten des Elementarbereichs $a = ||p_1 - p_0||, b = ||p_2 - p_0||, c = ||p_3 - p_0||$ und den Winkeln zwischen diesen Kanten $\alpha = \angle p_2p_0p_3 = \angle(b, c); \beta = \angle(a, c); \gamma = \angle(a, b)$ kann man diese Kristallsysteme wie folgt beschreiben:

1) Triklines Kristallsystem: $a \neq b, b \neq c, c \neq a$
$\alpha \neq \beta, \beta \neq \gamma, \gamma \neq \alpha$

2) Monoklines Kristallsystem: $a \neq b, b \neq c, c \neq a$
$\alpha = \gamma = 90°, \beta > 90°$

3) Orthorhombisches Kristallsystem: $a \neq b, b \neq c, c \neq a$
$\alpha = \beta = \gamma = 90°$

4) Tetragonales Kristallsystem: $a = b, b \neq c$
$\alpha = \beta = \gamma = 90°$

5) Trigonales Kristallsystem: $a = b, b \neq c$
$\alpha = \beta = 90°, \gamma = 120°$
(3-zählige Drehsymmetrie)

6) Hexagonales Kristallsystem: $a = b, b \neq c$
$\alpha = \beta = 90°, \gamma = 120°$
(6-zählige Drehsymmetrie)

7) Kubisches Kristallsystem: $a = b = c$
$\alpha = \beta = \gamma = 90°$

b) Die Symmetrie eines Kristallsystems bilden jeweils eine Gruppe. Es treten folgende Gruppen auf:

1) triklin: 2 Elemente
$$G_1 = \{I_3, -I_3\} \cong \mathbb{Z}/_{2\mathbb{Z}}$$

2) monoklin: 6 Elemente
$$G_2 = \{I_3, -I_3, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}\}$$

3) orthorombisch: 8 Elemente
$$G_3 = \{I_3, -I_3, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}\}$$

4) tetragonal: 16 Elemente
$$G_4 = G_3 \cup \{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}\}$$

5) trigonal: 24 Elemente

6) hexagonal: 24 Elemente

7) kubisch: 48 Elemente

Definition 2.8 Eine *Punktgruppe* ist eine Gruppe von Symmetrieoperationen, bei denen mindestens ein Punkt Fixpunkt ist.

Bemerkung 2.9

a) Zu jedem Kristallgitter gehören mehrere mögliche Punktgruppen. Aus der Invarianz der kristallographischen Achsen folgt die Invarianz des Nullpunkts. Punkte des Raumgitters, die innerhalb des Elementarbereichs liegen, können jedoch verschieden abgebildet (permutiert) werden.

b) Die verschiedenen Punktgruppen eines Kristallsystems sind Untergruppen der Gruppe der Symmetrieoperationen des Kristallsystems.

Satz 2.10 Es gibt insgesamt 32 verschiedene Punktgruppen. Sie verteilen sich wie folgt auf die 7 Kristallsysteme:

1) (triklin) 2 Punktgruppen: $\{I_3\}$ und G_1

2) (monoklin) 3 Punktgruppen: G_2, C_2, C_5

3) (orthorhombisch) 3 Punktgruppen: $G_3 = D_{2h}, D_2, C_{2v}$

4) (tetragonale) 7 Punktgruppen: $G_4 = D_{4h}, C_4, S_4, C_{4h}, D_4, C_{4v}, D_{2d}$

5) (trigonal) 5 Punktgruppen: $D_{3d}, C_3, C_{3i}, D_3, C_{3v}$

6) (hexagonal) 7 Punktgruppen: $D_{6h}, C_6, C_{3h}, C_{6h}, D_6, C_{6v}, D_{3h}$

7) (kubisch) 5 Punktgruppen: O_h, T, T_h, O, T_d

Definition 2.11 Die Gruppe der Symmetrieoperationen einer Kristallstruktur (unter Einschluß der Gittertranslationen) nennt man ihre *Raumgruppe*.

Bemerkung 2.12

a) Jede Raumgruppe enthält die zugehörige Punktgruppe als Untergruppe.

b) Es gibt insgesamt 230 Raumgruppen.

3 Restklassengruppen

A. Operationen von Gruppen auf Mengen

Im Folgenden sei $(G, \circ)$ eine Gruppe und M eine Menge.

Definition 3.1 a) Eine *Operation* von G auf M ist eine Abbildung

$$\alpha : \begin{array}{ccc} G \times M & \to & M \\ (g, m) & \mapsto & g(m) \end{array},$$

so dass die folgenden Bedingungen gelten:

1) $e(m) = m \qquad \forall\, m \in M$
2) $(g' \circ g)(m) = g'(g(m)) \qquad \forall\, g, g' \in G, m \in M$

b) Eine Operation $\alpha : G \times M \to M$ heißt *treu*, wenn für alle $g, g' \in G$ gilt:

$$g(m) = g'(m) \quad \forall\, m \in M \qquad \Rightarrow \qquad g = g'$$

Beispiel 3.2

a) Ist G eine Untergruppe von $\mathrm{Bij}(M, M)$, so operiert G auf M mittels

$$\alpha : \begin{array}{ccc} G \times M & \to & M \\ (g, m) & \mapsto & g(m) \end{array} ,$$

wobei $g(m)$ die Anwendung der Abbildung $g \in \mathrm{Bij}(M, M)$ auf das Element m bezeichnet.

b) Die Abbildung

$$\lambda : \begin{array}{ccc} G \times G & \to & G \\ (g, g') & \mapsto & g \circ g' \end{array} ,$$

definiert eine treue Operation von G auf G. Man sagt, G operiert auf sich durch *Linkstranslation*.

c) Ebenso operiert G auf sich durch *Rechtstranslation* mittels

$$\rho : \begin{array}{ccc} G \times G & \to & G \\ (g, g') & \mapsto & g' \circ g^{-1} \end{array}$$

d) Die Gruppe G operiert auf sich durch *Konjugation* mittels

$$\kappa : \begin{array}{ccc} G \times G & \to & G \\ (g, g') & \mapsto & g \circ g' \circ g^{-1} \end{array}$$

e) Sei $\mathfrak{U}$ die Menge der Untergruppen von G. Für $g \in G$ und $U \in \mathfrak{U}$ ist $g \circ U \circ g^{-1} = \{g \circ u \circ g^{-1} \mid u \in U\}$ eine Untergruppe von G.
Also hat man eine Operation von G auf $\mathfrak{U}$ durch *Konjugation* mittels

$$\bar{\kappa} : \begin{array}{ccc} G \times \mathfrak{U} & \to & \mathfrak{U} \\ (g, U) & \mapsto & g \circ U \circ g^{-1} \end{array}$$

Definition 3.3 Sei $\alpha : G \times M \to M$ eine Operation.

a) Ist $N \subseteq M$ eine Teilmenge, so heißt die Untergruppe

$$G_N = \{g \in G \mid g(n) = n \quad \forall\, n \in N\}$$

die *Isotropiegruppe* von N.

b) Ein Element $m \in M$ heißt *Fixpunkt* der Operation α, wenn

$$G_{\{m\}} = G \quad ,$$

d.h.

$$g(m) = m \quad \forall\, g \in G$$

c) Für ein Element $m \in M$ heißt

$$G_m = \{g(m) \mid g \in G\} \subseteq M$$

die *Bahn* von m unter der Operation α.

d) Die Operation α heißt *transitiv*, wenn sie nur eine Bahn besitzt, d.h.

$$\forall\, m, m' \in M\ \exists\, g \in G :\ m' = g(m)$$

Beispiel 3.4

a) Die Gruppe G operiert auf sich durch Konjugation.
Für eine Teilmenge $H \subseteq G$ heißt die Isotropiegruppe

$$G_H = \{g \in G \mid gh = hg\ \forall\, h \in H\}$$

auch der *Zentralisator* von H. Speziell heißt

$$Z(G) = G_G = \{g \in G \mid gh = hg\ \forall\, h \in G\}$$

das *Zentrum* von G.

b) Die Gruppe G operiert auf der Menge $\mathfrak{U}$ ihrer Untergruppen durch Konjugation. Für ein $U \in \mathfrak{U}$ heißt die Isotropiegruppe

$$N(U) = G_{\{U\}} = \{g \in G \mid gUg^{-1} = U\}$$

auch der *Normalisator* von U.

c) Sei G die Gruppe der Drehungen in $\mathbb{R}^2$ um den Nullpunkt. Dann sind die Bahnen gerade die Sphären mit Radius $r \geq 0$. Der Nullpunkt ist der einzige Fixpunkt.

d) Operiert G auf sich durch Konjugation und ist $g \in G$, so heißt die Bahn

$$G_g = \{hgh^{-1} \mid h \in G\}$$

auch die *Konjugationsklasse* von g.

e) Operiert G auf der Menge $\mathfrak{U}$ ihrer Untergruppen durch Konjugation und ist $U \in \mathfrak{U}$, so heißt die Bahn

$$G \cdot U = \{gUg^{-1} \mid g \in G\}$$

auch die *Konjugationsklasse* von U. Sie besteht aus allen zu U konjugierten Untergruppen gUg^{-1}.

Satz 3.5 Sei $\alpha : G \times M \to M$ eine Operation.

a) Die Menge M ist die disjunkte Vereinigung der Bahnen.

b) Sei G endlich und $m \in M$. Dann gilt:

$$\#G = \#(G_m) \cdot \#(G_{\{m\}})$$

Definition 3.6 G operiere auf sich bzw. auf der Menge ihrer Untergruppen $\mathfrak{U}$ durch Linkstranslation bzw. Rechtstranslation.

a) Die Bahn

$$U \cdot g = \{u \cdot g \mid u \in U\}$$

eines Elements $g \in G$ heißt die *Rechtsnebenklasse* von g bzgl. U.

b) Die Bahn

$$g \cdot U = \{g \cdot u^{-1} \mid u \in U\} = \{gu \mid u \in U\}$$

heißt die *Linksnebenklasse* von g bzgl. U.

c) Die Menge der Linksnebenklassen von Elementen von G bzgl. U wird mit G/U bezeichnet. (Sprich „G modulo U“)
Also gilt

$$G/U = \{gU \mid g \in G\}$$

d) Die Bahn von $U \in \mathfrak{U}$ unter der Operation von G auf $\mathfrak{U}$ durch Linkstranslation ist genau die Menge der Linksnebenklassen $G/U = \{gU \mid g \in G\}$. Die Zahl

$$[G : U] = \begin{cases} \#(G/U) & \text{falls } \#(G/U) < \infty \\ \infty & \text{sonst} \end{cases}$$

heißt der *Index* von U in G.

Korollar 3.7 *Der Satz von Lagrange*
Sei G eine endliche Gruppe und $U \subseteq G$ eine Untergruppe. Dann gilt:

$$\#G = (\#U) \cdot [G : U]$$

Korollar 3.8 *Die Klassengleichung*
Eine endliche Gruppe G operiere auf sich durch Konjugation.
Seien $g_1, \ldots, g_r \in G$, so dass $G = \overset{r}{\underset{i=1}{\cup}} Gg_i$ die disjunkte Vereinigung der Konjugationsklassen ist. Dann gilt:

$$\#G = \sum_{i=1}^{r} [G : Z(g_i)] = \#Z(G) + \sum_{\{i \mid\ [G:Z(g_i)]>1\}} [G : Z(g_i)]$$

B. Normalteiler

Frage: Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Kann man auf $G/U = \{gU \mid g \in G\}$ eine Gruppenstruktur definieren ?

Antwort: Im Allgemeinen nein!

Problem: Die Eigenschaft, in der gleichen Linksnebenklasse zu liegen, ist eine Äquivalenzrelation. Aber die Menge dieser Äquivalenzklassen ist bzgl. der natürlichen Verknüpfung $[g] \circ [h] = [g \circ h]$ im Allgemeinen keine Gruppe.

Beispiel 3.9 Sei $G = \mathcal{S}_3$ und $U = \{\mathrm{id}, \tau_{12}\}$, wobei τ_{ij} die Vertauschung von i und j bezeichne. G/U ist nun keine Gruppe.

Satz 3.10 Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann sind die folgenden Bedingungen äquivalent:

a) $\forall\, g, h \in G: \quad (g \cdot U) \cdot (h \cdot U) = (g \cdot h)U$

b) $\forall\, g \in G: \quad gU = Ug$

c) $\forall\, g \in G: \quad gUg^{-1} = U$

d) $\forall\, g \in G: \quad gUg^{-1} \subseteq U$

Definition 3.11 Eine Untergruppe $U \subseteq G$ heißt *Normalteiler* von G, wenn sie die äquivalenten Bedingungen von Satz 3.10 erfüllt. In diesem Fall schreiben wir auch $U \triangleleft G$.

Beispiel 3.12

a) Ist G eine Abelsche Gruppe, so ist *jede* Untergruppe U von G ein Normalteiler.

b) Ist $f : G \to H$ ein Gruppenhomomorphismus, so ist $\ker(f) \triangleleft G$ ein Normalteiler.

c) Für alle $n \geq 1$ ist $\mathcal{A}_n \triangleleft \mathcal{S}_n$ ein Normalteiler.

Satz 3.13 Sei $U \triangleleft G$ ein Normalteiler.

a) Die Menge G/U ist bzgl. der Verknüpfung

$$\circ : \begin{array}{ccc} G/U \times G/U & \to & G/U \\ (gU, hU) & \mapsto & ghU \end{array}$$

eine Gruppe. Sie heißt die *Restklassengruppe* (oder *Faktorgruppe* oder *Quotientengruppe*) von G modulo U.

b) Die Abbildung

$$\varepsilon : \begin{array}{ccc} G & \to & G/U \\ g & \mapsto & gU \end{array}$$

ist ein surjektiver Gruppenhomomorphismus. Sie heißt der *kanonische Epimorphismus* auf die Restklassengruppe.

c) Ist G endlich, so gilt:

$$\#(G/U) = \frac{\#G}{\#U} = [G : U]$$

Beispiel 3.14

a) Sei $n \geq 1$ und $U = n\mathbb{Z} \subseteq G = \mathbb{Z}$. Dann ist U ein Normalteiler von G, da G Abelsch ist. Die Gruppe $G/U = \mathbb{Z}/_{n\mathbb{Z}}$ ist die zyklische Gruppe modulo n.

b) Für $U = \mathcal{A}_n \subseteq G = \mathcal{S}_n$ gilt $G/U = \{\mathcal{A}_n, \sigma\mathcal{A}_n\}$ mit einer ungeraden Permutation σ. Die Abbildung

$$\varphi : \begin{array}{ccc} \mathcal{S}_n/\mathcal{A}_n & \to & \mathbb{Z}/_{2\mathbb{Z}} \\ \mathcal{A}_n & \mapsto & \bar{0} \\ \sigma\mathcal{A}_n & \mapsto & \bar{1} \end{array}$$

ist dann ein Isomorphismus von Gruppen.

Satz 3.15 *Die universelle Eigenschaft der Restklassengruppe*
Sei G eine Gruppe und $U \triangleleft G$ ein Normalteiler. Sei $\varphi : G \to H$ ein Gruppenhomomorphismus in eine weitere Gruppe H und es gelte $U \subseteq \ker(\varphi)$. Dann gibt es einen eindeutig bestimmten Gruppenhomomorphismus

$$\psi : G/U \to H \quad ,$$

so dass $\varphi = \psi \circ \varepsilon$ gilt.

C. Die Noetherschen Isomorphiesätze

Satz 3.16 *Der Homomorphiesatz für Gruppen*
Sind G, H Gruppen und ist $\varphi : G \to H$ ein surjektiver Gruppenhomomorphismus, so induziert φ einen Isomorphismus von Gruppen

$$\bar{\varphi} : G/\ker(\varphi) \to H$$

mit $\bar{\varphi}(g \cdot \ker(\varphi)) = \varphi(g)$.

Satz 3.17 *Normalteiler und Gruppenhomomorphismus*
Seien G, H Gruppen und $\varphi : G \to H$ sei ein Gruppenhomomorphismus.

a) Ist $V \triangleleft H$ ein Normalteiler, so ist $\varphi^{-1}(V) \triangleleft G$ ein Normalteiler.

b) Ist $U \triangleleft G$ ein Normalteiler und φ surjektiv, so ist $\varphi(U) \triangleleft H$ ein Normalteiler.

c) Ist φ surjektiv, so liefert φ eine Bijektion zwischen der Menge der Normalteiler von G die $\ker(\varphi)$ umfaßt und der Menge der Normalteiler von H.

Lemma 3.18 Seien G, H Gruppen; seien $N \triangleleft G$ und $N' \triangleleft H$ Normalteiler und sei $\varphi : G \to H$ ein Gruppenhomomorphismus.

a) Die Komposition

$$\alpha : G \xrightarrow{\varphi} H \xrightarrow{\varepsilon'} H/N'$$

von φ mit dem kanonischen Epimorphismus ε' liefert einen injektiven Homomorphismus von Gruppen

$$\bar{\alpha} : G/\varphi^{-1}(N') \to H/N'$$

Ist φ surjektiv, so ist $\bar{\alpha}$ ein Isomorphismus von Gruppen, d.h. u.a.

$$G/\varphi^{-1}(N') \cong H/N'$$

b) Ist $U \subseteq G$ eine Untergruppe und ist $U \cdot N = \{u \cdot n \mid u \in U, n \in N\}$, so ist $U \cdot N$ eine Untergruppe von G mit $N \lhd U \cdot N$. Ferner ist $N \cap U$ ein Normalteiler von U.

Satz 3.19 *Der 1. Noethersche Isomorphiesatz*
Sei G eine Gruppe, sei $N \lhd G$ ein Normalteiler und sei $U \subseteq G$ eine Untergruppe.
Dann wird durch den Gruppenhomomorphismus

$$\varphi : \begin{array}{ccc} U & \to & G/N \\ u & \mapsto & uN \end{array}$$

ein Isomorphismus von Gruppen

$$\bar{\varphi} : U/_{U \cap N} \xrightarrow{\sim} U \cdot N/_N$$

induziert.

Kommentar: V VR, U, U' UVRe $\Rightarrow$ $U/_{U \cap U'} \cong (U + U')/_{U'}$

Satz 3.20 *Der 2. Noethersche Isomorphiesatz*
Sei G eine Gruppe und seien $N_1, N_2 \lhd G$ Normalteiler mit $N_2 \subseteq N_1 \subseteq G$.
Dann induziert die Komposition kanonischer Epimorphismen

$$\psi : G \xrightarrow{\alpha} G/N_2 \to (G/N_2)/_{(N_1/N_2)}$$

einen Isomorphismus von Gruppen

$$\bar{\psi} : G/N_1 \xrightarrow{\sim} (G/N_2)/_{(N_1/N_2)}$$

4 Konstruktion von Gruppen

A. Produkte

Im Folgenden sei I eine Menge und für jedes $i \in I$ sei eine Gruppe G_i gegeben.

Definition 4.1 Die Menge aller Tupel $(g_i)_{i \in I}$ mit $g_i \in G_i$ für $i \in I$ heißt das *direkte Produkt* der Mengen $\{G_i\}_{i \in I}$ und wird mit $\prod_{i \in I} G_i$ bezeichnet.
Im Fall $I = \{1, \ldots, n\}$ schreibt man auch $G_1 \times G_2 \times \cdots \times G_n$.

Satz 4.2

a) Das direkte Produkt $G = \prod_{i \in I} G_i$ ist bzgl. der Verknüpfung

$$\circ : \begin{array}{ccc} G \times G & \to & G \\ ((g_i)_{i \in I}, (h_i)_{i \in I}) & \mapsto & (g_i h_i)_{i \in I} \end{array}$$

eine Gruppe.

b) Für jedes $j \in I$ ist die Abbildung

$$\varphi_j : \begin{array}{ccc} G_j & \to & \prod\limits_{i\in I} G_i \\ g_j & \mapsto & (\tilde{g}_i)_{i\in I} \end{array}$$

mit

$$\tilde{g}_j = \begin{cases} g_i & \text{falls } j = i \\ e_{G_i} & \text{sonst} \end{cases}$$

ein injektiver Gruppenhomomorphismus.

c) Für jedes $j \in I$ ist $\varphi_j(G_j) \triangleleft G$ ein zu G_j isomorpher Normalteiler von G.

d) Für jedes $j \in I$ ist

$$\psi_j : \begin{array}{ccc} \prod\limits_{i\in I} G_i & \to & G_j \\ (g_i)_{i\in I} & \mapsto & g_j \end{array}$$

ein surjektiver Gruppenhomomorphismus. (*Projektion auf den j-ten Faktor*)

Satz 4.3 *Universelle Eigenschaft des direkten Produkts*
Sei H eine Gruppe und für jedes $i \in I$ gebe es einen Gruppenhomomorphismus $\eta_i : H \to G_i$. Dann gibt es genau einen Gruppenhomomorphismus $\Phi : H \to \prod\limits_{i\in I} G_i$ mit $\eta_j = \psi_j \circ \Phi$ für alle $j \in I$.

Satz 4.4 Seien N_1, N_2 Untergruppen einer Gruppe G und sei $N_1 \times N_2$ ihr direktes Produkt. Dann sind die folgenden Bedingungen äquivalent

a) Die Abbildung

$$\iota : \begin{array}{ccc} N_1 \times N_2 & \to & G \\ (n_1, n_2) & \mapsto & n_1 \cdot n_2 \end{array}$$

ist ein Isomorphismus von Gruppen.

b) Es gelten die folgenden drei Bedingungen

1) Jedes Element $g \in G$ ist von der Form $g = g_1 \cdots g_r$ mit $g_i \in N_1 \cup N_2$ für $i = 1, \ldots, r$
2) N_1 und N_2 sind Normalteiler von G.
3) $N_1 \cap N_2 = \{e\}$

Sind diese Bedingungen erfüllt, so sagen wir, G sei das *innere direkte Produkt* von N_1 und N_2 und schreiben $G = N_1 \times N_2$.

Beispiel 4.5 Sei $m, n \in \mathbb{N}_+$.
Genau dann ist

$$\begin{array}{ccc} \mathbb{Z}/_{mn\mathbb{Z}} & \to & \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}} \\ a + mn\mathbb{Z} & \mapsto & (a + m\mathbb{Z}, a + n\mathbb{Z}) \end{array}$$

ein Isomorphismus von Gruppen, wenn $\mathrm{ggT}(m, n) = 1$ gilt.

Definition 4.6 Die Menge aller Tupel $(g_i)_{i\in I}$ mit $g_i = e_{G_i}$ für fast alle i (d.h. für alle bis auf höchstens endlich viele) heißt die *direkte Summe* der Menge $\{G_i\}_{i\in I}$ und wird mit $\coprod_{i\in I} G_i$ bezeichnet.
Ist $I = \{1, \ldots, n\}$, so schreibt man auch $G_1 \oplus \cdots \oplus G_n$.

Satz 4.7

a) Die direkte Summe $G = \coprod_{i\in I} G_i$ ist bzgl. der Verknüpfung

$$\circ : \begin{array}{ccc} G \times G & \to G \\ ((g_i)_{i\in I}, (h_i)_{i\in I}) & \mapsto & (g_i h_i)_{i\in I} \end{array}$$

eine Gruppe.

b) Für jedes $j \in I$ ist die Abbildung

$$\varphi_j : \begin{array}{ccc} G_j & \to & \coprod_{i\in I} G_i \\ g_j & \mapsto & (g_i \delta_{ij})_{i\in I} \end{array}$$

ein injektiver Gruppenhomomorphismus.

c) Für jedes $j \in I$ ist $\varphi_j(G_j)$ ein Normalteiler von $\coprod_{i\in I} G_i$

d) Für jedes $j \in I$ ist

$$\psi_j : \begin{array}{ccc} \coprod_{i\in I} G_i & \to & G_j \\ (g_i)_{i\in I} & \mapsto & g_j \end{array}$$

ein surjektiver Gruppenhomomorphismus.

Satz 4.8 *Die universelle Eigenschaft der direkten Summe*
Sei H eine Gruppe und für jedes $i \in I$ gebe es einen Gruppenhomomorphismus $\eta_i : G_i \to H$. Dann gibt es genau einen Gruppenhomomorphismus $\Psi : \coprod_{i\in I} G_i \to H$ mit $\eta_j = \Psi \circ \varphi_j$ für alle $j \in I$.

Bemerkung 4.9 Ist I endlich, so ist die Inklusion

$$\coprod_{i\in I} G_i \to \prod_{i\in I} G_i$$

ein Isomorphismus von Gruppen.

Definition 4.10 Seien G_1, G_2 zwei Gruppen.

a) Die Menge aller Isomorphismen von Gruppen $G_1 \to G_1$ ist bzgl. der Komposition $\circ$ eine Gruppe (und zwar eine Untergruppe von $\mathrm{Bij}(G_1, G_1)$). Sie heißt die *Automorphismengruppe* von G_1 und wird mit $\mathrm{Aut}(G_1)$ bezeichnet.

b) Sei $\varphi : G_2 \to \mathrm{Aut}(G_1)$ ein Gruppenhomomorphismus.
Wir definieren auf $G_1 \times G_2$ eine Verknüpfung

$$\circ : \begin{array}{ccc} (G_1 \times G_2) \times (G_1 \times G_2) & \to & G_1 \times G_2 \\ ((g_1, g_2), (h_1, h_2)) & \mapsto & (g_1 \varphi(g_2)(h_1), g_2 h_2) \end{array}$$

Die Menge $G_1 \times G_2$ mit dieser Verknüpfung heißt das *semidirekte Produkt* von G_1 und G_2 bzgl. φ und wird mit $G_1 \times_\varphi G_2$ bezeichnet.

Satz 4.11 Seien G_1, G_2 Gruppen und $\varphi : G_2 \to \mathrm{Aut}(G_1)$ ein Gruppenhomomorphismus.

a) Das semidirekte Produkt $G_1 \times_\varphi G_2$ ist eine Gruppe.

b) Die Teilmengen $\{e\} \times G_2$ und $G_1 \times \{e\}$ sind Untergruppen von $G_1 \times_\varphi G_2$.

c) Genau dann ist $G_1 \times_\varphi G_2$ Abelsch, wenn G_1 und G_2 Abelsch sind und φ der triviale Gruppenhomomorphismus ist.

d) Genau dann ist $G_1 \times_\varphi G_2$ gleich dem direkten Produkt $G_1 \times G_2$, wenn $\varphi : G_2 \to \mathrm{Aut}(G_1)$ der triviale Gruppenhomomorphismus ist (also $g_2 \mapsto \mathrm{id}_{G_1}$).

B. Präsentationen

Definition 4.12 Sei G eine Gruppe und $M \subseteq G$ eine Teilmenge. Die Menge aller Produkte $a_1 \cdots a_r$ mit $r \geq 0$ und $a_i \in M$ oder $a_i^{-1} \in M$ für $i = 1, \ldots, r$ ist offensichtlich eine Untergruppe von G.
Wir nennen sie die *von M erzeugte Untergruppe* von G und bezeichnen sie mit $< M >$. Im Fall $M = \{g_1, \ldots, g_s\}$ schreiben wir auch $< g_1, \ldots, g_s >$ statt $< M >$.

Satz 4.13 Sei G eine Gruppe.

a) Ist I eine Menge und $\{G_i\}_{i \in I}$ eine Menge von Untergruppen von G, so ist $\bigcap_{i \in I} G_i$ eine Untergruppe von G.

b) Sei $M \subseteq G$. Dann ist $< M >$ der Durchschnitt aller Untergruppen von G, die M enthalten. Insbesondere ist $< M >$ die kleinste Untergruppe von G, die M enthält.

Beispiel 4.14

a) Die von $\{2\}$ erzeugte Untergruppe von $\mathbb{Z}$ ist $2\mathbb{Z}$. Die von $\{4, 6\}$ erzeugte Untergruppe von $\mathbb{Z}$ ist $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$.

b) Die Gruppe $\mathcal{S}_n$ wird von den Transpositionen erzeugt, d.h. die von $M = \{\tau_{ij} \mid 1 \leq i < j \leq n\}$ erzeugte Untergruppe ist $< M >= \mathcal{S}_n$.

Definition 4.15 Sei Σ eine Menge. Ferner sei $\tilde{\Sigma}$ eine weitere Menge und $\iota : \Sigma \to \tilde{\Sigma}$ eine bijektive Abbildung.

a) Die Menge $M(\Sigma)$ bestehe aus allen endlichen Tupeln mit $n \geq 0$ und $x_1, \ldots, x_n \in \Sigma$.
Im Fall $n = 0$ bezeichnen wir das leere Tupel mit e.

b) Auf der Menge $M(\Sigma)$ definieren wir eine Verknüpfung durch *Konkatenation*

$$\begin{array}{rccc} \circ : & M(\Sigma) \times M(\Sigma) & \to & M(\Sigma) \\ & ((x_1, \ldots, x_n), (y_1, \ldots, y_m)) & \mapsto & (x_1, \ldots, x_n, y_1, \ldots, y_m) \end{array}$$

c) Ein Element aus $M(\Sigma \cup \tilde{\Sigma})$ heißt *reduziert*, wenn es kein $i \in \{1, \ldots, n-1\}$ gibt mit $x_{i+1} = \iota(x_i)$ oder $x_i = \iota(x_{i+1})$.

d) Ist ein Element $(x_1, \ldots, x_n) \in M(\Sigma \cup \tilde{\Sigma})$ nicht reduziert, d.h. gibt es ein $i \in \{1, \ldots, n-1\}$ mit $x_{i+1} = \iota(x_i)$ oder $x_i = \iota(x_{i+1})$, so sagen wir, das Element $(x_1 \ldots, x_{i-1}, x_{i+2}, \ldots, x_n) \in M(\Sigma \cup \tilde{\Sigma})$ folgt aus $(x_1, \ldots, x_n)$ durch einen *elementaren Reduktionsschritt*.

e) Sei $\sim$ die durch die elementaren Reduktionsschritte erzeugte Äquivalenzrelation auf $M(\Sigma \cup \tilde{\Sigma})$. Mit anderen Worten, wir setzen $(x_1, \ldots, x_n) \sim (y_1, \ldots, y_m)$, wenn es Elemente $w_1, \ldots, w_r \in M(\Sigma \cup \tilde{\Sigma})$ gibt, so dass gilt:

1) $w_1 = (x_1, \ldots, x_n)$
2) $w_r = (y_1, \ldots, y_m)$
3) Für $i = 1, \ldots, r-1$ entsteht w_i aus w_{i+1} oder w_{i+1} aus w_i durch einen elementaren Reduktionsschritt.

Satz 4.16 In der Situation von Definition 4.15 gilt:

a) Die Menge $M(\Sigma)$ ist bzgl. $\circ$ ein Monoid mit neutralem Element e.
Sie heißt das *freie Monoid* über dem *Alphabet* Σ.

b) Die Konkatenation liefert eine wohldefinierte Verknüpfung

$$\begin{array}{rccc} \circ : & M(\Sigma \cup \tilde{\Sigma})/_\sim \times M(\Sigma \cup \tilde{\Sigma})/_\sim & \to & M(\Sigma \cup \tilde{\Sigma})/_\sim \\ & ([(x_1, \ldots, x_n)], [(y_1, \ldots, y_m)]) & \mapsto & [(x_1, \ldots, x_n, y_1, \ldots, y_m)] \end{array}$$

auf der Menge der Äquivalenzklassen $M(\Sigma \cup \tilde{\Sigma})/_\sim$.

c) Die Menge der Äquivalenzklassen $M(\Sigma \cup \tilde{\Sigma})/_\sim$ ist bzgl $\circ$ eine Gruppe.
Sie heißt die *freie Gruppe* über dem Alphabet Σ.

Notationen

1) Für $x \in \Sigma$ schreiben wir statt $\iota(x)$ auch x^{-1}.

2) Statt $\tilde{\Sigma}$ schreiben wir auch Σ^{-1}.

3) Elemente von $M(\Sigma \cup \tilde{\Sigma})$ heißen *Wörter* über dem Alphabet.

4) Statt $M(\Sigma \cup \Sigma^{-1})$ schreiben wir auch Σ^+

5) Die freie Gruppe über dem Alphabet Σ bezeichnen wir mit $F(\Sigma)$.

Beispiel 4.17

a) Besitzt Σ nur ein Element x, so gilt $F(\Sigma) \cong \mathbb{Z}$.
Der Isomorphismus von Gruppen ist gegeben durch

$$[\underbrace{(x, x, \ldots, x)}_{i\text{-mal}}] \mapsto i$$

bzw.

$$[\underbrace{(x^{-1}, x^{-1}, \ldots, x^{-1})}_{i\text{-mal}}] \mapsto -i$$

b) Für $\Sigma = \emptyset$ gilt $F(\Sigma) = \{e\}$, d.h. $F(\Sigma)$ ist die triviale Gruppe.

Schreibweise
Für die Äquivalenzklasse $[(x_1, \ldots, x_n)] \in F(\Sigma)$ schreiben wir auch $x_1 \cdots x_n$.

Satz 4.18 *Universelle Eigenschaft der freien Gruppe*
Sei $\Sigma \neq \emptyset$ eine Menge, sei H eine Gruppe und sei $f : \Sigma \to H$ eine Abbildung.
Dann gibt es einen eindeutig bestimmten Gruppenhomomorphismus

$$\varphi : F(\Sigma) \to H$$

mit

$$\varphi(x) = f(x) \quad \forall\, x \in \Sigma$$

Korollar 4.19 Sei G eine Gruppe und $M \subseteq G$ ein Erzeugendensystem von G, d.h. es gelte $G =< M >$.
Dann gibt es einen eindeutig bestimmten Gruppenhomomorphismus

$$\varphi : F(M) \to G$$

mit

$$\varphi(x) = x \quad \forall\, x \in M$$

Insbesondere gilt

$$G \cong F(M)/\ker(\varphi)$$

Einen solchen Isomorphismus von G nennt man eine *Präsentation* von G durch *Erzeugende* M und *Relation* $\ker(\varphi)$.

Beispiel 4.20

a) Ist $G =< a >$ eine zyklische Gruppe, so gibt es einen eindeutig bestimmten surjektiven Gruppenhomomorphismus

$$\varphi : \mathbb{Z} \cong F(\{a\}) \to G$$

und eine Präsentation

$$G \cong \mathbb{Z}/\ker(\varphi) \cong \begin{cases} \mathbb{Z} & \text{falls } \ker(\varphi) = \{0\} \\ \mathbb{Z}/_{n\mathbb{Z}} & \text{sonst} \end{cases}$$

b) Es gilt

$$\mathcal{S}_3 \cong F(a,b)/ \ll a^3, b^2, abab^{-1} \gg$$

mit

$$\begin{array}{rcl} a & \mapsto & \sigma \\ b & \mapsto & \tau_{23} \end{array}$$

wobei $\ll M \gg$ der Normalisator der von $M = \{a^3, b^2, abab^{-1}\}$ erzeugten Untergruppe von $F(a,b)$ ist.

c) Für die Gruppe D_6 aus Blatt 1, Aufgabe 2 gilt:

$$D_6 \cong F(a,b)/ \ll a^6, b^2, abab^{-1} \gg$$

5 Abelsche Gruppen

A. Zyklische Gruppen

Wiederholung 5.1 a) Eine Gruppe G heißt *zyklisch*, wenn es ein $a \in G$ gibt mit $G =< a >= \{a^i \mid i \in \mathbb{Z}\}$.

b) Ist G zyklisch, so gilt

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

Insbesondere sind zyklische Gruppen stets abelsch.

c) Untergruppen zyklischer Gruppen sind zyklisch.

Beispiel 5.2 Sei $n \geq 2$.
In der komplexen Zahlenebene $\mathbb{C} = \{a + \mathrm{i}b \mid a, b \in \mathbb{R}\}$ betrachte die Punkte $p_j = e^{\frac{2\pi \mathrm{i}}{n} j} = \cos(\frac{2\pi}{n} j) + \mathrm{i} \sin(\frac{2\pi}{n} j)$ mit $j = 0, \ldots, n-1$.
Dann ist $G = \{p_0, \ldots, p_{n-1}\}$ eine multiplikative Untergruppe von $\mathbb{C} \setminus \{0\}$.
Die Abbildung

$$\varphi : \begin{array}{ccc} G & \to & \mathbb{Z}/_{n\mathbb{Z}} \\ p_j & \mapsto & j + n\mathbb{Z} \end{array}$$

ist ein Isomorphismus von Gruppen.
Die Zahlen $\{p_0, \ldots, p_{n-1}\}$ heißen die *n-ten Einheitswurzeln*. Sie sind die n Lösungen der Gleichung $z^n = 1$.
Die Gruppe G heißt die *n-te Einheitswurzelgruppe*.

Satz 5.3 Sei G eine Gruppe und sei $g \in G$ mit $\mathrm{ord}_G(g) = n < \infty$.

a) $(\exists\, m \in \mathbb{Z} :\ g^m = e) \quad \Rightarrow \quad n|m$

b) $m|n \quad \Rightarrow \quad \mathrm{ord}_G(g^m) = \frac{n}{m}$

c) Es gilt $< g >= \{e, g, g^2, \ldots, g^{n-1}\}$ und $\# < g >= n$

d) G endlich $\quad \Rightarrow \quad \mathrm{ord}_G(g) | \# G$

e) $\mathrm{ord}_G(g^k) = \frac{n}{\mathrm{ggT}(n,k)} \quad \forall\, k \in \mathbb{Z}$

Satz 5.4 Sei G eine Gruppe, seien $g, h \in G$ und $n = \mathrm{ord}_G(g) < \infty$, sowie $m = \mathrm{ord}_G(h) < \infty$.
Kommutieren g und h und gilt $\mathrm{ggT}(n, m) = 1$, so folgt

$$\mathrm{ord}_G(gh) = \mathrm{ord}_G(g) \cdot \mathrm{ord}_G(h)$$

Definition 5.5 Sei G eine endliche Gruppe. Dann heißt

$$\mathrm{Expo}(G) = \mathrm{kgV}\{\mathrm{ord}_G(g) \mid g \in G\}$$

der *Exponent* von G.
Für alle $g \in G$ gilt also

$$g^{\mathrm{Expo}(G)} = e$$

Satz 5.6 Jede endliche Abelsche Gruppe enthält ein Element der Ordnung $\mathrm{Expo}(G)$.

Satz 5.7 Sei R ein Integritätsring und sei G eine endliche Untergruppe von $(R \setminus \{0\}, \cdot)$. Dann ist G zyklisch.

Kommentar: Ein Integritätsring ist ein Ring mit $r_1 \cdot r_2 = 0 \ \Rightarrow \ r_1 = 0 \ \vee \ r_2 = 0$

Korollar 5.8

a) Ist K ein endlicher Körper, so ist $(K \setminus \{0\}, \cdot)$ eine zyklische Gruppe. Insbesondere ist $\mathbb{F}_p^\star = \mathbb{Z}/_{p\mathbb{Z}} \setminus \{0\}$ eine zyklische Gruppe.

b) Für jede Primzahl p und alle $n \in \mathbb{Z}$, $i \in \mathbb{N}$ gilt:

$$n^{p^i} \equiv n \mod p$$

Satz 5.9 Sei G endliche zyklische Gruppe und $n = \#G$.
Zu jedem Teiler d von n gibt es dann genau eine Untergruppe U von G mit

$$\#U = d$$

B. Endlich erzeugte Abelsche Gruppen

In diesem Unterabschnitt sei G stets eine endlich erzeugte Abelsche Gruppe. Wir verwenden die additive Notation.

Definition 5.10 a) Eine Menge $\{g_1, \ldots, g_r\}$ heißt eine *Basis* von G, wenn jedes $g \in G$ eine eindeutige Darstellung

$$g = a_1 g_1 + \cdots + a_r g_r$$

mit $a_1, \ldots, a_r \in \mathbb{Z}$ besitzt.

b) Besitzt G eine Basis, so heißt G eine (endlich erzeugte) *freie Abelsche Gruppe*.

Satz 5.11 Sei G eine freie Abelsche Gruppe mit Basis $\{g_1, \ldots, g_r\}$.

a) Die Abbildung

$$\begin{array}{rccc} & G & \to & \mathbb{Z}^r = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ mal}} \\ \varphi: & & & \\ & a_1 g_r + \cdots + a_r g_r & \mapsto & (a_1, \ldots, a_r) \end{array}$$

ist ein Isomorphismus von Gruppen.

b) Ist $\{h_1, \ldots, h_s\}$ eine weitere Basis von G, so gilt $s = r$.
Die Zahl $\mathrm{Rang}(G) = \mathrm{rk}(G) = r$ ist also eindeutig bestimmt. Sie heißt der *Rang* von G.

Theorem 5.12 *Der Hauptsatz für freie Abelsche Gruppen*
Sei G eine freie Abelsche Gruppe vom Rang r und sei $U \subseteq G$ eine Untergruppe.
Dann gibt es eine Basis $\{g_1, \ldots, g_r\}$ von G und eine Zahl $s \leq r$ und Zahlen $\varepsilon_1, \ldots, \varepsilon_s \in \mathbb{N}_+$ mit $\varepsilon_1 | \varepsilon_2, \varepsilon_2 | \varepsilon_3, \ldots, \varepsilon_{s-1} | \varepsilon_s$, so dass $\{\varepsilon_1 g_1, \ldots, \varepsilon_s g_s\}$ eine Basis von U ist.
Insbesondere ist U eine freie Abelsche Gruppe vom Rang $s \leq r$.

Theorem 5.13 *Der Hauptsatz für endlich erzeugte Abelsche Gruppen*
Sei G eine endlich erzeugte Abelsche Gruppe.

a) Es gibt eine Zahl $r \geq 0$, sowie Zahlen $\varepsilon_1, \ldots, \varepsilon_s \in \mathbb{N}_+$ mit $\varepsilon_1 > 1$ und $\varepsilon_1 | \varepsilon_2, \varepsilon_2 | \varepsilon_3, \ldots, \varepsilon_{s-1} | \varepsilon_s$ und einen Isomorphismus von Gruppen
$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}/_{\varepsilon_1 \mathbb{Z}} \oplus \cdots \oplus \mathbb{Z}/_{\varepsilon_s \mathbb{Z}}$$
Insbesondere ist G eine endliche direkte Summe zyklischer Gruppen.

b) Die Zahl r ist eine Invaraiante von G.
Mit anderen Worten, ist $G \cong \mathbb{Z}^{r'} \oplus \mathbb{Z}/_{\varepsilon_1' \mathbb{Z}} \oplus \cdots \oplus \mathbb{Z}/_{\varepsilon_s' \mathbb{Z}}$ ein weiterer Isomorphismus von Gruppen wie in a), so gilt $r' = r$. Die Zahl r heißt der *Rang* von G und wird mit $\mathrm{Rang}(G) = \mathrm{rk}(G)$ bezeichnet.

c) Ist G eine endliche Gruppe, so gilt
$$r = 0 \quad \text{und} \quad \varepsilon_s = \mathrm{Expo}(G)$$
Insbesondere ist ε_s eine Invariante von G.

Als nächstes zeigen wir, dass alle Zahlen $\varepsilon_1, \ldots, \varepsilon_s$ in Theorem 5.13 a) Invarianten von G sind. Sie heißen die *Elementarteiler* von G.

Definition 5.14 Sei G eine Abelsche Gruppe. Dann ist die Menge
$$T(G) = \{g \in G \mid \mathrm{ord}_G(g) < \infty\}$$
eine Untergruppe von G. Sie heißt die *Torsionsgruppe* von G.

Satz 5.15 Sei G eine endlich erzeugte Abelsche Gruppe und
$$\psi : G \xrightarrow{\sim} \mathbb{Z}^r \oplus \mathbb{Z}/_{\varepsilon_1 \mathbb{Z}} \oplus \cdots \oplus \mathbb{Z}/_{\varepsilon_s \mathbb{Z}}$$
ein Isomorphismus von Gruppen wie in Theorem 5.13 a)

a) Dann gilt:
$$T(G) = \psi^{-1}(0 \oplus \cdots \oplus 0 \oplus \mathbb{Z}/_{\varepsilon_1 \mathbb{Z}} \oplus \cdots \oplus \mathbb{Z}/_{\varepsilon_s \mathbb{Z}})$$
Insbesondere ist die Zahl
$$\varepsilon_1 \varepsilon_2 \cdots \varepsilon_s$$
eine Invariante von G.

b) Die Zahlen $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s$ sind Invarianten von G.

Korollar 5.16 Ist G *torsionsfrei* (d.h. gilt $T(G) = 0$), so ist G frei.

Satz 5.17 *Der Chinesische Restsatz*
Gegeben seien Zahlen $n_1, \ldots, n_s \in \mathbb{N}_+$ mit $s \geq 2$ und mit $\mathrm{ggT}(n_i, n_j) = 1$ für $1 \leq i < j \leq s$. Ferner sei $N = n_1 \cdots n_s$.

a) Der kanonische Homomorphismus von Ringen

$$\varphi : \begin{array}{ccc} \mathbb{Z}/_{N\mathbb{Z}} & \to & \mathbb{Z}/_{n_1\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{n_s\mathbb{Z}} \\ a + N\mathbb{Z} & \mapsto & (a + n_1\mathbb{Z}, \ldots, a + n_s\mathbb{Z}) \end{array}$$

ist ein Isomorphismus.

b) Die Abbildung φ induziert einen Isomorphismus von (multiplikativen) Gruppen.

$$\psi : (\mathbb{Z}/_{N\mathbb{Z}})^\times \xrightarrow{\sim} (\mathbb{Z}/_{n_1\mathbb{Z}})^\times \times \cdots \times (\mathbb{Z}/_{n_s\mathbb{Z}})^\times$$

Korollar 5.18 Ist G eine endliche Abelsche Gruppe und m ein Teiler von $n = \#G$, so gibt es eine Untergruppe $U \subseteq G$ mit $\#U = m$.

Satz 5.19 *Klassifikation endlicher Abelscher Gruppen*
Sei $n \geq 2$. Schreibe $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ mit $\alpha_1, \ldots, \alpha_r \in \mathbb{N}_+$ und paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$. Für $i = 1, \ldots, r$ sei $A(p_i^{\alpha_i})$ die Anzahl der *Partitionen* $\alpha_i = \alpha_{i1} + \cdots + \alpha_{ik}$ mit $1 \leq \alpha_{i1} \leq \cdots \leq \alpha_{ik}$.
Dann gibt es (bis auf Isomorphie) genau $A(n) = A(p_1^{\alpha_1}) \cdots A(p_r^{\alpha_r})$ verschiedene Abelsche Gruppen der Ordnung n.

Es gilt

$$U_i = T_{p_i}(G) = \{g \in G \mid \mathrm{ord}_G(g) \text{ ist } p_i\text{-Potenz}\}$$

6 p-Gruppen

Im folgenden sei p stets eine Primzahl.

A. Der Satz von Cauchy

Definition 6.1 Eine Gruppe G heißt *p-Gruppe*, falls die Ordnung jedes Elements von G eine Potenz von p ist.

Beispiel 6.2 Ist G eine endliche Gruppe und $\#G = p^n$ für ein $n \geq 1$, so ist G eine p-Gruppe.

Ziel: Zeige, dass auch die Umkehrung von Beispiel 6.2 gilt.

Satz 6.3 Ist G eine endliche Gruppe mit p^n Elementen, so gilt $Z(G) \neq \{e\}$, d.h. G hat ein nichttriviales Zentrum.

Lemma 6.4 Eine Gruppe mit p^n Elementen operiere auf einer Menge M. Sei M^G die Menge der Fixpunkte dieser Operation. Dann gilt:

$$\#M = \#M^G \mod p$$

Satz 6.5 *Der Satz von Cauchy*
Sei G eine endliche Gruppe und p eine Primzahl. Ist $\#G$ durch p teilbar, so enthält G ein Element der Ordnung p.

Korollar 6.6 Sei G eine endliche Gruppe.

$$G \text{ } p\text{-Gruppe} \quad \Leftrightarrow \quad \exists\, n \in \mathbb{N}_+ :\ \#G = p^n$$

Insbesondere besitzt jede endliche p-Gruppe ein nicht-triviales Zentrum.

Beispiel 6.7 Jede Gruppe mit $\#G = p^2$ ist Abelsch.

B. Die Sätze von Sylow

Frage: Sei G endlich und $m|\#G$.
Gibt es stets eine Untergruppe $U \subseteq G$ mit $\#U = m$?

Antwort: Ja, falls G abelsch ist. Eindeutig, falls G zyklisch. Jedoch im Allgemeinen ist die Antwort *Nein*, wie Beispiel 6.8 zeigt.

Frage: Für welche Teiler $m|\#G$ gibt es eine Untergruppe $U \subseteq G$ mit $\#U = m$?

Beispiel 6.8 In $\mathcal{A}_4 \subseteq \mathcal{S}_4$ gibt es keine Untergruppe mit 6 Elementen, obwohl $\#\mathcal{A}_4 = 12$ gilt.

Definition 6.9 Eine *p-Sylowuntergruppe* von G ist eine (bzgl. der Inklusion) maximale p-Untergruppe von G.

Lemma 6.10 *Lemma von Zorn*
Sei M eine nichtleere, *induktiv geordnete Menge*, d.h. eine Menge mit einer partiellen Ordnung $\leq$, so dass jede Kette $m_1 \leq m_2 \leq \ldots$ eine obere Schranke m besitzt (also ein Element m mit $m_i \leq m$ für alle $i \geq 1$).
Dann besitzt M mindestens ein maximales Element bzgl. $\leq$.

Satz 6.11 *Existenz von p-Sylowgruppen*
Sei G eine Gruppe und p Primzahl.

a) Es gibt eine p-Sylowuntergruppe von G.

b) Ist G Abelsch, so gibt es genau eine p-Sylowuntergruppe von G.
Diese ist gegeben durch die p-Torsion:

$$T_p(G) = \{g \in G \mid \mathrm{ord}_G(g) \text{ ist Potenz von } p\}$$

Beispiel 6.12 Sei $G = \mathcal{S}_3$.
Jede 2-Sylowuntergruppe von G hat die Ordnung 2. Es gibt genau drei 2-Sylowuntergruppen, nämlich

$$U_1 = \{\mathrm{id}, \tau_{12}\},\ U_2 = \{\mathrm{id}, \tau_{13}\},\ U_3 = \{\mathrm{id}, \tau_{23}\}$$

Insbesondere ist die p-Sylowuntergruppe von G im Allgemeinen nicht eindeutig bestimmt!

Bemerkung 6.13 Sei G eine Gruppe.

a) Ist $U \subseteq G$ eine p-Sylowuntergruppe und $g \in G$, so ist auch gUg^{-1} eine p-Sylowuntergruppe von G.

b) Besitzt G nur eine p-Sylowuntergruppe, so ist diese ein Normalteiler.

Lemma 6.14 Sei $U \subseteq G$ eine p-Untergruppe und

$$N(U) = \{g \in G \mid gUg^{-1} = U\} \supseteq U$$

ihr Normalisator. Dann gilt:

a) $[N(U) : U] \equiv [G : U] \mod p$

b) Ist p Teiler von $[G : U]$, so gilt $N(U) \neq U$.

Theorem 6.15 *Der erste Satz von Sylow*
Sei G eine endliche Gruppe und $\#G = p^n m$ mit $p \nmid m$.

a) Für jedes $i \in \{0, \ldots, n\}$ besitzt G eine Untergruppe der Ordnung p^i.
Insbesondere besitzt jede p-Sylowuntergruppe von G die Ordnung p^n.

b) Sei $i \in \{0, \ldots, n-1\}$.
Jede Untergruppe der Ordnung p^i von G ist Normalteiler in einer Untergruppe der Ordnung p^{i+1}.

Beispiel 6.16 Sei G eine Gruppe der Ordnung 15. Dann haben die 3-Sylowgruppen von G je 3 Elemente und die 5-Sylowgruppen von G je 5 Elemente. Unter anderem gilt $G \cong \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{5\mathbb{Z}} \cong \mathbb{Z}/_{15\mathbb{Z}}$, d.h. jede Gruppe der Ordnung 15 ist zyklisch.

Theorem 6.17 *Der zweite Satz von Sylow*
Sei G eine endliche Gruppe und seien U, V zwei p-Sylowuntergruppen von G. Dann gibt es ein $g \in G$ mit $V = gUg^{-1}$. Mit anderen Worten, zwei p-Sylowuntergruppen von G sind zueinander konjugiert.

Beispiel 6.18 Sei p eine Primzahl und G eine Gruppe der Ordnung $2p$.

a) $p = 2 \quad \Rightarrow \quad \#G = 4$ und $G \cong \mathbb{Z}/_{4\mathbb{Z}} \ \vee \ G \cong V_4$

b) Sei $p \geq 3$. Es gibt genau eine p-Sylowuntergruppe $U \subseteq G$ mit $\#U = p$. Es gilt $U \lhd G$. Ferner gibt es eine 2-Sylowuntergruppe $V \subseteq G$ mit $\#V = 2$. Sei $U =< a >$ und $V =< b >$, so gilt $G =< ab > \cong \mathbb{Z}/_{2p\mathbb{Z}}$ oder $G \cong D_p$ (Diedergruppe).

Theorem 6.19 *Der dritte Satz von Sylow*
Sei G eine endliche Gruppe und sei s_p die Zahl der Sylowgruppen von G. Dann gilt:

a) $\#G \equiv 0 \mod s_p$
Genauer: Schreibt man $\#G = p^n m$ mit $p \not| m$, so ist s_p ein Teiler von m.

b) $s_p \equiv 1 \mod p$

Beispiel 6.20 Seien p, q Primzahlen mit $p > q$ und $q \not| p - 1$. (Insbesondere gilt $q > 2$). Sei G eine Gruppe der Ordnung pq.

1) Nach dem 1.Satz von Sylow gibt es $a, b \in G : \ \mathrm{ord}_G(a) = p \ \wedge \ \mathrm{ord}_G(b) = q$

2) Aus dem 3. Satz von Sylow folgert man $s_p = 1$.

3) Ebenso folgt $s_q = 1$.

4) Jede Gruppe der Ordnung pq ist zyklisch.

Beispiel 6.21 Sei G eine Gruppe der Ordnung 45.

a) Es gilt $s_3 | 5$ und $3 | s_3 - 1$, also $s_3 = 1$

b) Es gilt $s_5 | 9$ und $5 | s_5 - 1$, also $s_5 = 1$

c) Somit gilt $G = U \times V$ mit $U \lhd G$ eindeutige 3-Sylowuntergruppe und $V \lhd G$ eindeutige 5-Sylowuntergruppe. Offenbar gilt $V \cong \mathbb{Z}/_{5\mathbb{Z}}$.

d) Nach Beispiel 6.7 ist U Abelsch, d.h. es gilt $U \cong \mathbb{Z}/_{9\mathbb{Z}}$ oder $U \cong \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$.

e) Insgesamt folgt $G \cong \mathbb{Z}/_{45\mathbb{Z}}$ oder $G \cong \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{15\mathbb{Z}}$.

7 Auflösbare Gruppen

Definition 7.1 Eine Gruppe G heißt *auflösbar*, wenn es eine Kette

$$\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_l = G$$

gibt, so dass für $i = 1, \ldots, l$ gilt:

a) $N_i \subseteq G$ Untergruppe

b) $N_{i-1} \lhd N_i$ Normalteiler

c) N_i/N_{i-1} Abelsch

Beispiel 7.2

a) Ist G eine Abelsche Gruppe, so ist G auflösbar, wie die Kette

$$\{e\} = N_0 \subseteq N_1 = G$$

zeigt.

b) Ist G eine nicht-Abelsche *einfache Gruppe* (d.h. die einzigen Normalteiler sind $\{e\}$ und G), so ist G nicht auflösbar.

Satz 7.3 Sei G eine endliche p-Gruppe. Dann ist G auflösbar.

Definition 7.4 Sei G eine Gruppe.
Eine Kette von Untergruppen $\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_l = G$ mit $N_{i-1} \lhd N_i$ für $i = 1, \ldots, l$ heißt *Normalreihe* von G. Also ist G genau dann auflösbar, wenn G eine Normalreihe mit Abelschen Restklassengruppen N_i/N_{i-1} besitzt.

Satz 7.5 Sei G eine auflösbare Gruppe.

a) Ist $U \subseteq G$ eine Untergruppe, so ist U auflösbar.

b) Ist $U \lhd G$ ein Normalteiler, so ist G/U auflösbar.

Bemerkung 7.6

a) Ist G eine endlich erzeugte Abelsche Gruppe, so gibt es eine Normalreihe $\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_l = G$ mit zyklischen Restklassengruppen N_i/N_{i-1}.

b) Ist G eine endliche Abelsche Gruppe, so gibt es sogar eine Normalreihe $\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_l = G$ mit N_i/N_{i-1} zyklisch von Primzahlordnung.

Satz 7.7 Sei G eine endliche auflösbare Gruppe und $N \lhd G$ ein Normalteiler. Dann gibt es eine Normalreihe $\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_l = G$ mit folgenden Eigenschaften:

a) Für $i = 1, \ldots, l$ ist N_i/N_{i-1} zyklisch von Primzahlordnung.

b) $N \in \{N_0, \ldots, N_l\}$

Bemerkung 7.8

a) Ist G eine einfache auflösbare Gruppe, so ist G zyklisch von Primzahlordnung.

b) Die Gruppen $\mathbb{Z}/_{p\mathbb{Z}}$ sind als „Atome“ anzusehen, aus denen sich jede endliche auflösbare Gruppe zusammensetzt. Ist im Satz $N_i/N_{i-1} \cong \mathbb{Z}/_{p_i\mathbb{Z}}$, so gilt $\#G = p_1 \cdots p_l$. Die auftretenden Primzahlen hängen also nur von $\#G$ ab, und nicht von der Wahl der Normalteiler.

Ziel: Zeige, dass $\mathcal{S}_n$ für $n \geq 5$ nicht auflösbar ist.

Lemma 7.9 Sei $n \geq 3$ und $a, b \in \{1, \ldots, n\}$ mit $a \neq b$. Dann wird die alternierende Gruppe $\mathcal{A}_n$ erzeugt von den Dreierzykeln

$$\sigma_{abk} = \begin{pmatrix} 1 & \ldots & a & \ldots & b & \ldots & k & \ldots & n \\ 1 & \ldots & b & \ldots & k & \ldots & a & \ldots & n \end{pmatrix}$$

mit $k \in \{1, \ldots, n\} \setminus \{a, b\}$ erzeugt.

Lemma 7.10 Sei $n \geq 3$ und $N \lhd \mathcal{A}_n$ ein Normalteiler, der einen Dreierzyklus enthält. Dann gilt:

$$N = \mathcal{A}_n$$

Satz 7.11

a) Für alle $n \neq 4$ ist $\mathcal{A}_n$ eine einfache Gruppe, d.h. ihre einzigen Normalteiler sind $\{e\}$ und $\mathcal{A}_n$.

b) Für alle $n \geq 5$ ist $\mathcal{S}_n$ nicht auflösbar. (Für $n \leq 4$ ist $\mathcal{S}_n$ auflösbar.)

Kapitel II
Galoistheorie

8 Grundlagen

A. Ringe

Definition 8.1 a) Ein *Ring* $(R, +, \cdot)$ ist eine Menge R zusammen mit zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$, so dass gilt:

1) $(R, +)$ ist eine Abelsche Gruppe
2) $(R, \cdot)$ ist eine Halbgruppe
3) Distributivgesetze

b) Ein Ring heißt *kommutativ*, wenn $\cdot$ kommutativ ist.

c) Gibt es bzgl. $\cdot$ ein neutrales Element, so bezeichnen wir dieses mit 1 (oder 1_R) und nennen R einen *Ring mit Einselement*.

Sofern es im Folgenden nicht ausdrücklich anders festgelegt ist, seien alle Ringe kommutativ mit Einselement.

Beispiel 8.2

a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/_{n\mathbb{Z}}$ für $n \geq 1$

b) Polynomring (vgl. später)

c) Der *Nullring* $R = \{0\}$ mit $1_R = 0$.

Definition 8.3 Sei R ein Ring.

a) R heißt *nullteilerfrei* oder *Integritätsring* oder *Bereich*, wenn

$$\forall\, a, b \in R : \quad (\ ab = 0 \ \Rightarrow\ a = 0 \ \vee\ b = 0\ )$$

b) Eine Teilmenge $S \subseteq R$ heißt *Unterring*, wenn $(S, +)$ eine Untergruppe von $(R, +)$ ist und $S \cdot S \subseteq S$ gilt.

c) Eine Teilmenge $I \subseteq R$ heißt *Ideal* von R, wenn $(I, +)$ eine Untergruppe von $(R, +)$ ist und $R \cdot I \subseteq I$ gilt.

Beispiel 8.4

a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Integritätsringe.

b) $\mathbb{Z}/_{n\mathbb{Z}}$ ist genau dann ein Integritätsring, wenn n eine Primzahl ist.

c) Jedes Ideal ist ein Teilring von R. Jedoch ist z.B. $\mathbb{Q}[x^2] \subseteq \mathbb{Q}[x]$ ein Teilring, aber kein Ideal.

d) $I = \{0\}$ *Nullideal*, $I = R$ *Einheitsideal* gibt es in jedem Ring.

e) Die Ideale von $\mathbb{Z}$ sind die Teilmengen $n\mathbb{Z}$ mit $n \in \mathbb{N}$.

Definition 8.5 Sei R ein Ring.

a) Ist $\{a_\lambda\}_{\lambda\in\Lambda}$ eine Familie von Elementen von R, so ist

$$I = \{\sum_{i=1}^{s} r_i a_{\lambda_i} \mid s \geq 0, \{r_1, \ldots, r_s\} \subseteq R, \{\lambda_1, \ldots, \lambda_s\} \subseteq \Lambda\}$$

ein Ideal von R.
Es heißt das von $\{a_\lambda\}_{\lambda\in\Lambda}$ *erzeugte Ideal*. Die Menge $\{a_\lambda\}_{\lambda\in\Lambda}$ heißt ein *Erzeugendensystem* von I. Wir schreiben $I = (\{a_\lambda\}_{\lambda\in\Lambda})$ bzw. $I = (a_1, \ldots, a_n)$ falls $\Lambda = \{1, \ldots, n\}$.

b) Besitzt ein Ideal $J \subseteq R$ ein endliches Erzeugendensystem, so heißt J ein *endlich erzeugtes Ideal* oder *endlich erzeugt*.

c) Gibt es ein $a \in R$ mit $I = (a) = R \cdot a$, so heißt I ein *Hauptideal*.

d) Ist jedes Ideal in R ein Hauptideal, so heißt R ein *Hauptidealring*.

Beispiel 8.6

a) $\mathbb{Z}$ und $K[x]$ mit K Körper sind Hauptidealringe.

b) In einem Körper sind (0) und $K = (1)$ die einzigen Ideale. Also ist jeder Körper K ein Hauptidealring.

c) $r \in R$ *Einheit* (d.h. r ist bzgl. $\cdot$ invertierbar) $\quad\Leftrightarrow\quad (r) = R$

Definition 8.7 Seien R, S Ringe und $f : R \to S$ eine Abbildung.

a) Die Abbildung f heißt ein *Ringhomomorphismus* oder ein *Homomorphismus von Ringen*, wenn für alle $r, r' \in R$ gilt:

1) $f(r + r') = f(r) + f(r')$
2) $f(rr') = f(r)f(r')$

b) Ein bijektiver Ringhomomorphismus heißt auch ein *Isomorphismus von Ringen*.

c) Der *Kern* eines Ringhomomorphismus $f : R \to S$ ist die Menge

$$\mathrm{Kern}(f) = \ker(f) = \{r \in R \mid f(r) = 0\}$$

Offenbar ist der Kern ein Ideal in R.

Beispiel 8.8

a) $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ sind injektive Ringhomomorphismen.

b) Die Nullabbildung

$$f : \begin{array}{ccc} R & \to & S \\ r & \mapsto & 0 \end{array}$$

ist stets ein Ringhomomorphismus. Das Bild von f ist der *Nullring*.

c) Die Abbildung

$$g : \begin{array}{ccc} K[x] & \to & K \\ f & \mapsto & f(a) \end{array}$$

mit Körper K, $a \in K$ ist ein Ringhomomorphismus und heißt *Einsetzungshomomorphismus* mit

$$\mathrm{Kern}(g) = (x - a)$$

Definition 8.9 Sei R ein Ring und $I \subseteq R$ ein Ideal.

a) Definiert man

$$a \sim_I b \quad \Leftrightarrow \quad a - b \in I$$

für $a, b \in R$, so ist $\sim_I$ eine Äquivalenzrelation auf R. Die Äquivalenzklasse eines Elements $a \in R$ ist

$$a + I = \{a + b \mid b \in I\}$$

Wir nennen $a + I$ die *Restklasse* von a *modulo* I.

b) Sei $R/I = \{a + I \mid a \in R\}$ die Menge aller Restklassen modulo I. In §3 haben wir gesehen, dass R/I durch die Verknüpfung

$$+ : \begin{array}{ccc} R/I \times R/I & \to & R/I \\ (a + I, b + I) & \mapsto & a + b + I \end{array}$$

zu einer Abelschen Gruppe wird.

Satz 8.10 Sei R ein Ring und $I \subseteq R$ ein Ideal.

a) Definiert man

$$\cdot : \begin{array}{ccc} R/I \times R/I & \to & R/I \\ (a+I, b+I) & \mapsto & ab+I \end{array},$$

so ist dies eine wohldefinierte Verknüpfung auf R/I. Hierdurch wird R/I zu einem Ring. Er heißt der *Restklassenring* von R modulo I.

b) Die Abbildung

$$\varepsilon : \begin{array}{ccc} R & \to & R/I \\ a & \mapsto & a+I \end{array}$$

ist ein surjektiver Ringhomomorphismus. Sie heißt der *kanonische Epimorphismus* auf dem Restklassenring.

c) Es gilt

$$I = \mathrm{Kern}(\varepsilon)$$

Beispiel 8.11

a) Ist $R = \mathbb{Z}$ und $I = n\mathbb{Z}$ mit $n \geq 1$, so gilt

$$R/I = \mathbb{Z}/_{n\mathbb{Z}} = \{0 + n\mathbb{Z}, \ldots, n-1+n\mathbb{Z}\}$$

Dieser Ring besitzt n Elemente und die Ringoperationen entsprechen dem üblichen „Rechnen modulo n“.

b) Sei K ein Körper, sei $R = K[x]$ und $I \subseteq R$ das von einem Polynom $f \in R$ erzeugte Hauptideal.

1. Fall: $f \equiv 0$:
$K[x] \cong R/I$

2. Fall: $f \equiv a$ mit $a \in K \setminus \{0\}$:
Es gilt $I = (f) = R$ und $R/I \cong \{0\}$

3. Fall: $f \in K[x] \setminus K$:
Es gilt

$$R/I = \{g + (f) \mid g \in K[x]_{\leq n-1}\}$$

mit $n = \deg(f)$. Der K-Vektorraum $K[x]/(f)$ besitzt die Basis

$$\{1 + (f), x + (f), \ldots, x^{n-1} + (f)\}$$

Somit folgt

$$\dim_K(K[x]/(f)) = n$$

Satz 8.12 *Die universelle Eigenschaft des Restklassenringes*
Seien R, S Ringe, sei $I \subseteq R$ ein Ideal und sei $\varphi : R \to S$ ein Ringhomomorphismus mit $I \subseteq \ker(\varphi)$.
Dann gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\psi : R/I \to S$$

mit

$$\varphi = \psi \circ \varepsilon$$

Die Abbildung ψ heißt der *induzierte Ringhomomorphismus*.

Satz 8.13 *Der Homomorphiesatz für Ringe*
Sind R, S Ringe und ist $\varphi : R \to S$ ein surjektiver Ringhomomorphismus, so induziert φ einen Isomorphismus von Ringen

$$\bar{\varphi} : \begin{array}{ccc} R/\ker(\varphi) & \xrightarrow{\sim} & S \\ a + \ker(\varphi) & \mapsto & \varphi(a) \end{array}$$

Satz 8.14 Ist R ein Ring, so gibt es genau einen Ringhomomorphismus

$$\varphi : \mathbb{Z} \to R$$

mit

$$\varphi(1) = 1_R$$

Er heißt der *Strukturhomomorphismus* von R. Der Unterring $\varphi(\mathbb{Z})$ heißt der *Primring* von R.

Definition 8.15 Sei R ein Ring und $\varphi : \mathbb{Z} \to R$ sein Strukturhomomorphismus. Dann heißt die eindeutig bestimmte Zahl $n \in \mathbb{N}$ mit $\ker(\varphi) = n\mathbb{Z}$ die *Charakteristik* von R und wird mit $\mathrm{char}(R)$ bezeichnet.

Beispiel 8.16

a) $R = \mathbb{Z}/_{n\mathbb{Z}}$ hat die Charakteristik n.

b) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ haben die Charakteristik 0.

Satz 8.17 *Ideale und Ringhomomorphismen*
Seien R, S Ringe, sei $\varphi : R \to S$ ein Ringhomomorphismus, sei $I \subseteq R$ ein Ideal und sei $J \subseteq S$ ein Ideal.

a) Die Teilmenge $\varphi^{-1}(J) \subseteq R$ ist ein Ideal.

b) Ist φ surjektiv, so ist $\varphi(I) \subseteq S$ ein Ideal.

c) Ist φ surjektiv, so definieren $I \mapsto \varphi(I)$ und $J \mapsto \varphi^{-1}(J)$ eine Bijektion zwischen der Menge der Ideale von R, die $\ker(\varphi)$ umfaßt, und der Menge der Ideale von S.

d) Ist φ surjektiv, so induziert die Komposition

$$R \xrightarrow{\varphi} S \xrightarrow{\varepsilon} S/J$$

einen Isomorphismus von Ringen

$$R/_{\varphi^{-1}(J)} \xrightarrow{\sim} S/J$$

e) Die Ideale von R/I sind genau die Ideale $\tilde{I}/I$, wobei $\tilde{I} \subseteq R$ ein Ideal ist, das I umfaßt.

Satz 8.18 *Der 2. Noethersche Isomorphiesatz für Ringe*
Sei R ein Ring und seien I, J Ideale von R mit $I \subseteq J$.
Dann induziert die Komposition kanonischer Epimorphismen

$$R \xrightarrow{\varepsilon} R/I \xrightarrow{\tilde{\varepsilon}} (R/I)/_{(J/I)}$$

einen Isomorphismus von Ringen

$$\varphi : R/J \xrightarrow{\sim} (R/I)/_{(J/I)}$$

B. Körper

Definition 8.19 Ein *Körper* $(K, +, \cdot)$ ist ein kommutativer Ring mit Einselement, bei dem $(K \setminus \{0\}, \cdot)$ eine Gruppe ist.

Bemerkung 8.20

a) Ein Körper ist ein Integritätsring.

b) Die einzigen Ideale in einem Körper K sind $(0) = \{0\}$ und $(1) = K$. Insbesondere ist K ein Hauptidealring.

c) Die Charakteristik eines Körpers ist 0 oder eine Primzahl.

Beispiel 8.21

a) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper der Charakteristik 0.

b) Ist p eine Primzahl, so ist $\mathbb{F}_p = \mathbb{Z}/_{p\mathbb{Z}}$ ein Körper der Charakteristik p.

Definition 8.22 Sei K ein Körper.

a) Ist $L \subseteq K$ ein Teilring und $(L\backslash\{0\}, \cdot)$ eine Gruppe, so heißt L ein *Teilkörper* von K und $K|L$ ist eine *Körpererweiterung*.

b) Sind K und L zwei Körper und ist $\varphi : K \to L$ ein Ringhomomorphismus, so heißt φ ein *Körperhomomorphismus* falls $\varphi \neq 0$ ist. Insbesondere gilt dann $\varphi(1) = 1$ und $\ker(\varphi) = (0)$, d.h. jeder Körperhomomorphismus ist injektiv.

c) Ein bijektiver Körperhomomorphismus $\varphi : K \to K$ heißt auch ein *Automorphismus* von K. Die Gruppe der Automorphismen von K wird mit $\mathrm{Aut}(K)$ bezeichnet.

Beispiel 8.23

a) Die komplexe Konjugation

$$\begin{array}{rccc} - : & \mathbb{C} & \to & \mathbb{C} \\ & a + \mathrm{i}b & \mapsto & a - \mathrm{i}b \end{array}$$

ist ein Automorphismus von $\mathbb{C}$.

b) Der Körper $\mathbb{R}$ ist ein Teilkörper von $\mathbb{C}$. Dabei ist $\mathbb{C}$ ein 2-dimensionaler $\mathbb{R}$-Vektorraum.

c) Es gilt $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$ und $\mathrm{Aut}(\mathbb{F}_p) = \{\mathrm{id}\}$.

Definition 8.24 a) Ist R ein Ring mit Strukturhomomorphismus $\varphi : \mathbb{Z} \to R$, so heißt der Teilring $\varphi(\mathbb{Z})$ auch der *Primring* von R.

b) Ist K ein Körper, so heißt der kleinste Teilkörper, der $\{0, 1\}$ enthält, der *Primkörper* von K.

- Ist $\mathrm{char}(K) = 0$, so ist sein Primkörper isomorph zu $\mathbb{Q}$.
- Ist $\mathrm{char}(K) = p > 0$ Primzahl, so ist sein Primkörper isomorph zu $\mathbb{F}_p$.

Satz 8.25 Sei K ein Körper und sei $\{L_\lambda\}_{\lambda\in\Lambda}$ eine Familie von Teilkörpern von K. Dann ist auch

$$L = \bigcap_{\lambda\in\Lambda} L_\lambda$$

ein Teilkörper von K.

Definition 8.26 Sei K ein Körper und $M \subseteq K$ eine Teilmenge.

a) Der von M *erzeugte Teilkörper* von K ist der Durchschnitt aller Teilkörper von K, die M enthalten.

b) Sei $L \subseteq K$ ein Teilkörper. Dann bezeichnen wir den von $L \cup M$ erzeugten Teilkörper von K mit $L(M)$. Wir sagen, der Körper $L(M)$ entstehe aus L durch *Adjunktion* von M.

Beispiel 8.27

a) Der von $M = \{0, 1\}$ erzeugte Teilkörper von K ist sein Primkörper.

b) Sei $K|L$ eine Körpererweiterung und $M \subseteq K$.
Dann besteht $L(M)$ aus allem Elementen der Form

$$\frac{f(a_1, \ldots, a_n)}{g(b_1, \ldots, b_m)} \in K$$

mit $f \in L[x_1, \ldots, x_n]$ und $g \in L[y_1, \ldots, y_m]$ und $a_1, \ldots, a_n, b_1, \ldots, b_m \in M$ und $g(b_1, \ldots, b_m) \neq 0$.

c) Ist $d \in \mathbb{Q}$ kein Quadrat einer rationalen Zahl, so ist

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$$

eine Körpererweiterung von $\mathbb{Q}$. Sie stellt einen 2-dimensionalen $\mathbb{Q}$-Vektorraum dar. Körper der Form $\mathbb{Q}(\sqrt{d})$ heißen *quadratische Zahlenkörper*.

Satz 8.28 Sei R ein Integritätsring. Wir betrachten die Menge $R \times (R \setminus \{0\})$ und rechnen sie mit der Relation

$$(r, s) \sim (r', s') \quad \Leftrightarrow \quad rs' - sr' = 0$$

a) Die Relation $\sim$ ist eine Äquivalenzrelation.

b) Sei $K = \big(R \times (R \setminus \{0\})\big)/_\sim$ die Menge der Äquivalenzklassen. Für die Äquivalenzklassen von (r, s) schreiben wir auch $\frac{r}{s}$.
Definiert man auf K zwei Verknüpfungen

$$+ : \begin{array}{ccc} K \times K & \to & K \\ (\frac{r}{s}, \frac{r'}{s'}) & \mapsto & \frac{rs'+r's}{ss'} \end{array}$$

und

$$\cdot : \begin{array}{ccc} K \times K & \to & K \\ (\frac{r}{s}, \frac{r'}{s'}) & \mapsto & \frac{rr'}{ss'} \end{array}$$

so wird K hierdurch zu einem Körper. Der Körper heißt der *Quotientenkörper* von R und wird mit $Q(R)$ bezeichnet.

Beispiel 8.29

a) Es gilt $\mathbb{Q} = Q(\mathbb{Z})$.

b) Ist $R = K[x_1, \ldots, x_n]$ ein Polynomring über einem Körper K, so heißt

$$Q(R) = \{\frac{f}{g} \mid f, g \in R \text{ und } g \neq 0\}$$

der *Körper der rationalen Funktionen* in n Unbestimmten über K und wird mit $K(x_1, \ldots, x_n)$ bezeichnet.

9 Konstruktionen mit Zirkel und Lineal

In der Zeichenebene können mit Zirkel und Lineal folgende Grundoperationen ausgeführt werden

1) Konstruktion der Geraden durch zwei gegebene Punkte

2) Konstruktion eines Kreises mit vorgegebenem Mittelpunkt und mit einem Radius, der gleich dem Abstand zweier gegebener Punkte ist.

3) Bestimmung des Schnittpunkts zweier bereits konstruierter Geraden (falls er existiert).

4) Bestimmung eventueller Schnittpunkte einer bereits konstruierten Geraden mit einem bereits konstruierten Kreis.

5) Bestimmung eventueller Schnittpunkte zweier bereits konstruierter Kreise.

Definition 9.1 Eine *Konstruktionsaufgabe* besteht aus der Angabe einer (meist endlichen) Punktmenge und der Frage, ob man einen (oder mehrere) bestimmten weiteren Punkt/Gerade/Kreis durch endlich viele Anwendungen der Grundoperationen 1) - 5) konstruieren kann.

Beispiel 9.2 Konstruiere ein Dreieck mit vorgegebenen Seitenlängen a, b, c, wobei die $\triangle$-Ungleichung für die Seiten erfüllt ist.

Beispiel 9.3 *Delisches Problem der Würfelverdopplung*
Zu einem durch seine Seitenlänge a gegebenen Würfel soll ein Würfel doppelten Volumens konstruiert werden, d.h. es soll eine Strecke der Länge $a\sqrt[3]{2}$ konstruiert werden.

Kommentar: Wir zeigen später, dass es keine Lösung gibt.

Beispiel 9.4 Zu einer gegebenen Strecke a und einer gegebenen rationalen Zahl $\frac{p}{q} > 0$ soll eine Strecke der Länge $\frac{p}{q} \cdot a$ konstruiert werden. $(p, q \in \mathbb{N}_+)$

Kommentar: Es lassen sich somit aus $0, 1$ alle rationalen Zahlen konstruieren.

Beispiel 9.5 *Winkeldreiteilung*
Zu zwei vorgegebenen Geraden G_1, G_2, die sich im Winkel φ schneiden, soll eine dritte Gerade durch den Schnittpunkt so konstruiert werden, dass sie mit G_1 den Winkel $\frac{\varphi}{3}$ einschließt.

Kommentar: Wir werden zeigen, dass dies im Allgemeinen unmöglich ist.

Beispiel 9.6 *Quadratur des Kreises*
Zu einem gegebenen Kreis soll ein flächengleiches Quadrat konstruiert werden. Mit anderen Worten: zu einer gegebenen Strecke der Länge r soll eine Strecke der Länge $r\sqrt{\pi}$ konstruiert werden.

Kommentar: Wir werden zeigen, dass dies unmöglich ist!

Beispiel 9.7 *Konstruktion regulärer n-Ecke*
In einen gegebenen Kreis soll ein reguläres (d.h. gleichseitiges) n-Eck eingeschrieben werden ($n \geq 3$). Mit anderen Worten: gesucht sind Punkte $P_1, \ldots, P_n$ auf dem Kreis mit $\overline{P_1P_2} = \overline{P_2P_3} = \cdots = \overline{P_{n-1}P_n} = \overline{P_nP_1}$

Kommentar: Wir werden die Zahlen n, für die dies möglich ist, charakterisieren.

Im Folgenden identifizieren wir die Zeichenebene mit der komplexen Zahlenebene

$$\mathbb{C} = \{a + \mathrm{i}b \mid a, b \in \mathbb{R}\}$$

Satz 9.8 Sei $M \subseteq \mathbb{C}$ eine Teilmenge mit $\{0, 1\} \subseteq M$.
Dann ist die Menge $\hat{M}$ der aus M konstruierbaren Zahlen ein Teilkörper von $\mathbb{C}$. Insbesondere gilt $\mathbb{Q} \subseteq \hat{M}$.
Hierbei heißt ein $z \in \mathbb{C}$ *aus M konstruierbar*, wenn der ihr entsprechende Punkt der Zeichenebene durch endlich viele Anwendungen der Operationen 1) - 5) aus den Punkten von M gewonnen werden kann.

Satz 9.9 Sei $\{0, 1\} \subseteq M \subseteq \mathbb{C}$ und sei $z \in \hat{M}$ eine aus M konstruierbare Zahl. Dann ist auch $\sqrt{z}$ eine aus M konstruierbare Zahl.

Im Folgenden sei $M \subseteq \mathbb{C}$ eine Teilmenge mit $\{0, 1\} \subseteq M$, sei $\overline{M} = \{\bar{z} \mid z \in M\}$ und $\hat{M}$ sei die Menge der aus M konstruierbaren Zahlen.

Satz 9.10 Sei $K_0 = \mathbb{Q}(M \cup \overline{M})$, dann gilt:

a) $K_0 \subseteq \hat{M}$

b) $K_0 = \overline{K_0}$

Satz 9.11 Sei $L \subseteq \mathbb{C}$ ein Teilkörper mit $L = \overline{L}$.

a) Für $z \in L$ gilt:
$$\mathrm{Re}(z), \mathrm{Im}(z) \in L$$

b) Sind G_1, G_2 Geraden durch je zwei verschiedene Punkte von L und ist $G_1 \cap G_2$ nicht leer, so ist auch der Punkt $G_1 \cap G_2$ in L enthalten.

c) Sei G eine Gerade durch zwei verschiedene Punkte aus L und K ein Kreis mit Mittelpunkt aus L und Radius aus L.
Ist $z \in G \cap K$, so gibt es ein $y \in L$ mit $z \in L(\sqrt{y})$

d) Sind K_1, K_2 Kreise mit Mittelpunkten in L und Radien aus L und ist $z \in K_1 \cap K_2$, so gibt es ein $y \in L$ mit $z \in L(\sqrt{y})$.

Definition 9.12 Sei $L|K$ eine Körpererweiterung.
Wir sagen, dass L aus K durch *sukzessive Adjunktion von Quadratwurzeln* entsteht, wenn es $a_1, \ldots, a_n \in L$ gibt, so dass gilt:

a) $L = K(a_1, \ldots, a_n)$

b) $a_i^2 \in K(a_1, \ldots, a_{i-1})$ für $i = 1, \ldots, n$

Korollar 9.13 Eine Zahl $z \in \mathbb{C}$ ist genau dann aus M konstruierbar, wenn z in einem Teilkörper L von $\mathbb{C}$ enthalten ist, der aus $K_0 = \mathbb{Q}(M \cup \overline{M})$ durch sukzessive Adjunktion von Quadratwurzeln entsteht.

Korollar 9.14 Sei $K_0 = \mathbb{Q}(M \cup \overline{M})$ und für alle $n \geq 1$ sei
$$K_n = K_{n-1}(\sqrt{K_{n-1}}) = K_{n-1}(\{\sqrt{a} \mid a \in K_{n-1}\})$$
Dann gilt
$$\hat{M} = \bigcup_{n=0}^{\infty} K_n$$

Beispiel 9.15

a) *Würfelverdopplung*
Sei $M = \{0, 1\}$. Genau dann ist das Konstruktionsproblem lösbar, wenn $\sqrt[3]{2}$ aus M konstruierbar ist.

b) *Quadratur des Kreises*
Genau dann ist das Konstruktionsproblem lösbar, wenn $\sqrt{\pi}$ aus $M = \{0, 1\}$ konstruierbar ist. Dies ist äquivalent damit, dass π konstruierbar ist.

c) *Winkeldreiteilung*
Ein Winkel φ sei gegeben durch $M = \{0, 1, e^{\mathrm{i}\varphi}\}$. Die Frage ist nun, ob $e^{\mathrm{i}\frac{\varphi}{3}}$ in einem Teilkörper von $\mathbb{C}$ enthalten ist, der aus $K_0 = \mathbb{Q}(e^{\mathrm{i}\varphi})$ durch sukzessive Adjunktion von Quadratwurzeln entsteht.

d) *Konstruktion regulärer n-Ecke*
Sei $M = \{0, 1\}$.
Das reguläre n-Eck ist genau dann konstruierbar, wenn $e^{\frac{2\pi\mathrm{i}}{n}}$ aus M konstruierbar ist.

10 Auflösung algebraischer Gleichungen

Gegeben sei eine Gleichung

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

mit $a_0, \ldots, a_n \in \mathbb{C}$, wobei $n \geq 1$ gelte, sowie $a_n \neq 0$.
Nach dem Fundamentalsatz der Algebra besitzt diese Gleichung stets eine Lösung. Zählt man die Lösungen mit geeigneten Vielfachheiten, so besitzt die Gleichung genau n Lösungen.

Problem: Finde Formeln, mit deren Hilfe man aus den Koeffizienten $a_0, \ldots, a_n$ die Lösungen berechnen kann.

Beispiel 10.1

a) Ist $n = 1$, so ist $x_1 = -\frac{a_0}{a_1}$ die eindeutig bestimmte Lösung der Gleichung.

b) Ist $n = 2$, so sind $x_{1/2} = -\frac{a_1}{2a_2} \pm \sqrt{\frac{a_1^2}{4a_2^2} - \frac{a_0}{a_2}}$ die beiden (nicht notwendig verschiedenen) Lösungen der Gleichung.

Beispiel 10.2 Sei $n = 3$, d.h. es sei die Gleichung

$$a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$$

gegeben. Als Lösung ergeben sich die Formeln von Cardano (1545 in Nürnberg publiziert).

Beispiel 10.3 Sei $n = 4$. Wir betrachten die Gleichung

$$a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$$

Dann führen die Formeln von Ferrari, einem Schüler Cardanos, zum Ziel.

Definition 10.4 Sei $L|K$ eine Körpererweiterung. Der Körper L heißt eine *Radikalerweiterung* von K, wenn gilt:

a) Es gibt $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$

b) Es gibt $r_1, \ldots, r_n \in \mathbb{N}_+$ mit $(a_i)^{r_i} \in K(a_1, \ldots, a_{i-1})$ für $i = 1, \ldots, n$

Mit anderen Worten: Der Körper L entsteht aus K durch sukzessive Adjunktion von Wurzeln.

Definition 10.5 Sei K ein Körper.
Eine Gleichung $a_n x^n + \cdots + a_0 = 0$ mit $a_0, \ldots, a_n \in K$ und $a_n \neq 0$ heißt *durch Radikale auflösbar*, wenn es eine Radikalerweiterung $L|K$ gibt, so dass die Lösungen der Gleichung in L liegen.

Bemerkung 10.6

a) Gleichungen vom Grad ≤ 4 sind im Fall $K = \mathbb{Q}$ durch Radikale auflösbar.

b) Für $K = \mathbb{Q}$ und $n = 5$ ist nicht jede Gleichung durch Radikale auflösbar (Satz von Abel). Man kann sogar eine konkrete, nicht auflösbare Gleichung angeben (Galois).

11 Ringe und Algebren

A. Teilbarkeitstheorie in Ringen

Im Folgenden sei R ein kommutativer Ring mit Einselement.

Definition 11.1 a) Ein Element $r \in R$ heißt *Einheit*, wenn es ein $r' \in R$ gibt mit $r \cdot r' = 1$. Die Einheiten von R bilden eine Gruppe, die wir mit $R^\times$ bezeichnen und die *Einheitengruppe* nennen.

b) Ein Element $r \in R$ heißt *Teiler* eines Elements $s \in R$, wenn es ein $r' \in R$ gibt mit $rr' = s$. In diesem Fall schreiben wir $r|s$.

c) Zwei Elemente $r, s \in R$ heißen *assoziiert*, wenn $r|s$ und $s|r$ gilt. In diesem Fall schreiben wir $r \sim s$.

d) Ein Element $r \in R$ heißt ein *echter Teiler* eines Elements $s \in R$, wenn $r|s$ gilt und r ist nicht assoziiert zu s.

e) Ein Element $r \in R \setminus \{0\}$ heißt *irreduzibel*, wenn es keine Einheit ist und keine echten Teiler besitzt.

f) Ein Element $r \in R \setminus \{0\}$ heißt *Primelement*, wenn es keine Einheit ist und aus $r|ss'$ folgt $r|s$ oder $r|s'$ für $s, s' \in R$.

Beispiel 11.2

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

b) Sei K ein Körper. Dann gilt

$$K[x]^\times = K \setminus \{0\}$$

c) Sei $I = [a, b] \subseteq \mathbb{R}$ ein abgeschlossenes Intervall und $R = \mathcal{C}^0(I)$ der Ring der stetigen Funktionen $f : I \to \mathbb{R}$. Dann besteht $\mathcal{C}^0(I)^\times$ aus genau den stetigen Funktionen $f : I \to \mathbb{R}$, die keine Nullstellen besitzen.

d) Sei K ein Körper und $f \in K[x] \setminus K$

$$f \text{ irreduzibel} \quad \Leftrightarrow \quad \nexists\, g \in K[x] : \; g|f \;\wedge\; 0 < \deg g < \deg f$$

Satz 11.3 *Regeln für Teiler und echter Teiler*
Sei R ein Ring und seien $r, s, t, u, v \in R$.

a) Es gilt $r|r$ und $r|0$.

b) $r|s,\ r|t \quad \Rightarrow \quad r|(\lambda s + \mu t) \quad \forall\, \lambda, \mu \in R$

c) $r|s,\ s|t \quad \Rightarrow \quad r|t$

d) $r|s,\ s \in R^\times \quad \Rightarrow \quad r \in R^\times$

e) $r|s,\ t \in R^\times \quad \Rightarrow \quad rt|s$

f) Unterscheiden sich r und s nur um eine Einheit, so gilt $r \sim s$. Ist R ein Integritätsring, so gilt hiervon auch die Umkehrung.

g) Ist r ein echter Teiler von s und gilt $s|t$, so ist r ein echter Teiler von t.

h) Sei R ein Integritätsring. Ist r ein echter Teiler von s und gilt $u|v$, so ist ru ein echter Teiler von sv.

i) Sei R ein Integritätsring. Gilt $r = st$ und ist s ein echter Teiler von r, so ist auch t ein echter Teiler von r.

Satz 11.4 *Eigenschaften von irreduziblen Elementen und Primelementen*
Sei R ein Integritätsring und seien $p, q, r, s \in R$.

a) Ist r irreduzibel und $r \sim s$, so ist auch s irreduzibel.

b) Sind r, s irreduzibel und gilt $r|s$, so folgt $r \sim s$.

c) Jedes Primelement ist irreduzibel.

d) Ist p ein Primelement und $p \sim q$, so ist auch q ein Primelement.

e) Sind p, q Primelemente und gilt $p|q$, so folgt $p \sim q$.

f) Ist p ein Primelement und gilt $p|a_1 \cdots a_n$ mit $a_1, \ldots, a_n \in R$, so gibt es ein $i \in \{1, \ldots, n\}$ mit $p|a_i$.

Definition 11.5 Sei R ein Integritätsring. Wir nennen R einen *faktoriellen Ring* (oder *ZPE-Ring*), wenn jedes Element $r \in R \setminus (\{0\} \cup R^\times)$ eine Darstellung als endliches Produkt von Primelementen besitzt.

Satz 11.6 Sei R ein Integritätsring, in dem der *Teilerkettensatz* für Elemente gilt, d.h. aus $r_1|r_0, r_2|r_1, \ldots$ folgt $r_n \sim r_{n+1} \sim \ldots$ für ein $n \in \mathbb{N}_+$.
Dann besitzt jedes Element von $R\setminus(\{0\}\cup R^\times)$ eine Darstellung als endliches Produkt irreduzibler Elemente.

Korollar 11.7 Der Ring $\mathbb{Z}$ ist faktoriell.

Satz 11.8 *Eindeutigkeit der Primfaktorzerlegung*
Sei R ein Integritätsring und sei $r \in R$ geschrieben als Produkt von Primelementen $r = p_1 \cdots p_m = q_1 \cdots q_n$.
Dann gilt $m = n$ und bei geeigneter Numerierung ist $p_i \sim q_i$ für $i = 1, \ldots, n$.

B. Polynomringe

Ziele:

- Zeige, dass auch $K[x]$ faktoriell ist.
- Studiere seine Primelemente.

Satz 11.9 Sei K ein Körper und $R = K[x]$.

a) In R gilt der Teilerkettensatz für Elemente.

b) Jedes irreduzible Polynom $f \in R$ ist ein Primelement.

c) Der Ring R ist faktoriell.

Bemerkung 11.10 In Algebra II wird sogar gezeigt:

$$R \text{ faktoriell} \quad \Rightarrow \quad R[x] \text{ faktoriell}$$

Insbesondere ist also $K[x_1, \ldots, x_n]$ faktoriell.

Im Folgenden ist R ein faktorieller Ring und $P = R[x]$.

Bemerkung 11.11

a) Ein lineares Polynom $f = r_1x + r_0$ mit $r_0, r_1 \in R$ und $r_1 \neq 0$ ist irreduzibel, wenn kein Primelement von R sowohl r_0 als auch r_1 teilt.

b) Ein Polynom $f \in P$ mit $\deg(f) = 2$ ist genau dann irreduzibel, wenn kein Primelement von R alle Koeffizienten teilt und f keine Nullstelle in R besitzt.

c) Ein Polynom $f \in P$ mit $\deg(f) = 3$ ist genau dann irreduzibel, wenn kein Primelement von R alle Koeffizienten teilt und f keine Nullstelle in R besitzt.

Beispiel zu Bem. 11.11 b) Das ganzzahlige Polynom

$$4x^2 - 1 = (2x - 1)(2x + 1)$$

ist reduzibel über $\mathbb{Z}$, besitzt aber keine Nullstellen in $\mathbb{Z}$.

Satz 11.12 *Das Eisenstein-Kriterium*
Sei

$$f = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in P$$

mit $a_0, \ldots, a_n \in R$ und $n = \deg(f) \geq 1$.
Ferner seien folgende Bedingungen erfüllt:

1) Es gibt kein Primelement von R, das alle Koeffizienten von f teilt.

2) Es gibt ein Primelement $p \in R$ mit $p|a_0, p|a_1, \ldots, p|a_{n-1}$.

3) $p^2 \not| a_0$

Dann ist $f \in P$ ein irreduzibles Polynom.

Beispiel 11.13

a) Ist $p \in R$ Primelement, so ist das Polynom $x^n \pm p \in R[x]$ irreduzibel.

b) Das Polynom $x^5 - 12 \in \mathbb{Z}[x]$ ist irreduzibel.

c) Das Polynom $x^3 + y + 1 \in K[x, y]$ ist irreduzibel.

d) Ebenso ist $x^3 + 3x^2y + 3x^2 + y + 1$ irreduzibel in $\mathbb{Q}[x, y]$.

Satz 11.14 *Irreduzibilität unter Ringhomomorphismen*
Sei R ein faktorieller Ring, S ein Integritätsring und $\varphi : R[x] \to S$ ein Ringhomomorphismus, der kein Polynom positiven Grades auf eine Einheit von S abbildet. Ferner sei $f \in R[x]$ ein Polynom mit $\deg(f) > 0$, so dass kein Primelement von R alle Koeffizienten von f teilt.

$$\varphi(f) \in S \quad \text{irreduzibel} \qquad \Rightarrow \qquad f \in R[x] \quad \text{irreduzibel}$$

Korollar 11.15 Ist $\psi : R \to R'$ ein Ringhomomorphismus, so ist

$$\begin{array}{rccc} & R[x] & \to & R'[x] \\ \varphi : & \sum\limits_i a_i x^i & \mapsto & \sum\limits_i \psi(a_i) x^i \end{array}$$

ein Ringhomomorphismus, der die Voraussetzung von Satz 11.14 erfüllt.

Irreduzibilitätskriterium modulo p
Sei

$$f = f_0 + f_1 x + \cdots + f_k x^k \in \mathbb{Z}[x] \setminus \mathbb{Z}$$

ein ganzzahliges Polynom mit positivem Grad, dessen Koeffizienten keinen gemeinsamen Teiler besitzen (d.h. keine Primzahl teile alle Koeffizienten). Sei p eine Primzahl, die den Höchstkoeffizienten f_k nicht teilt.
Sei $\phi : \mathbb{Z} \to \mathbb{Z}_p$ der Ring-Epimorphismus, der jede ganze Zahl auf ihre Restklasse modulo p abbildet. Sei weiter

$$\begin{array}{rccc} & \mathbb{Z}[x] & \to & \mathbb{Z}_p[x] \\ \psi : & \sum\limits_i a_i x^i & \mapsto & \sum\limits_i \phi(a_i) x^i \end{array}$$

die Fortsetzung von ϕ auf die Polynomringe.
Ist $\psi(f)$ irreduzibel über $\mathbb{Z}_p[x]$, so ist f irreduzibel über $\mathbb{Z}[x]$.

- Informelle Version: Ist unter den angegebenen Voraussetzungen f irreduzibel über $\mathbb{Z}_p$, so ist f irreduzibel über $\mathbb{Z}$.
- Für monische Polynome sind die Primzahlvoraussetzungen automatisch erfüllt.

Beispiel 11.16 Das Polynom $f = x^3 + 7x^2 - 7x + 2 \in \mathbb{Z}[x]$ ist irreduzibel.

Korollar 11.17 Sei $\psi : R \to S$ ein Ringhomomorphismus und $b \in S$.
Dann ist

$$\begin{array}{rccc} & R[x] & \to & S \\ \varphi : & \sum\limits_i a_i x^i & \mapsto & \sum\limits_i \psi(a_i) b^i \end{array}$$

ein Ringhomomorphismus. Er heißt ein *Substitutionshomomorphismus*.
Sind alle $\sum\limits_{i=0}^{n} \psi(a_i) b^i$ mit $n > 0, a_n \neq 0$ Nicht-Einheiten in S, so ist Satz 11.14 anwendbar.

Beispiel 11.18 Sei $p \in \mathbb{Z}$ eine Primzahl. Dann ist das Polynom

$$f = 1 + x + x^2 + \cdots + x^{p-1} \in \mathbb{Z}[x]$$

irreduzibel.

Frage: Sei $f \in \mathbb{Z}[x]$ irreduzibel. Ist dann auch $f \in \mathbb{Q}[x]$ irreduzibel?

Lemma 11.19 Sei R ein faktorieller Ring und $K = Q(R)$ sein Quotientenkörper. Zu jedem Polynom $g \in K[x]\backslash\{0\}$ gibt es dann ein $a \in K\backslash\{0\}$ mit $ag \in R[x]$, so dass kein Primelement von R alle Koeffizienten von ag teilt.

Kommentar: „minimale Nennerbeseitigung“

Lemma 11.20 Sei R ein Integritätsring und $p \in R$ ein Primelement. Dann ist auch $p \in R[x]$ ein Primelement.

Satz 11.21 *Der Satz von Gauß*
Sei R ein faktorieller Ring und $K = Q(R)$ sein Quotientenkörper.
Ist $f \in R[x] \setminus R$ ein irreduzibles Polynom, so ist auch $f \in K[x]$ irreduzibel.

Beispiel 11.22 Mit Hilfe des Satzes von Gauß folgt aus obigen Beispielen:

a) Ist $p \in \mathbb{Z}$ Primzahl, so ist $x^n \pm p \in \mathbb{Q}[x]$ irreduzibel.

b) $x^3 - 7x^2 + 7x - 2 \in \mathbb{Q}[x]$ irreduzibel

c) Ist $p \in \mathbb{Z}$ Primzahl, so ist $1 + x + \cdots + x^{p-1} \in \mathbb{Q}[x]$ irreduzibel.

C. Kommutative Algebren

Im Folgenden seien R, S kommutative Ringe mit Einselement.

Definition 11.23 a) Ist ein Ringhomomorphismus $\varphi : R \to S$ gegeben, so sagen wir auch S ist eine *R-Algebra* bzw. S/R ist eine *Algebra*. Der Ringhomomorphismus φ heißt der *Strukturhomomorphismus* von S/R.

b) Sind S/R und T/R zwei R-Algebren mit Strukturhomomorphismen $\varphi : R \to S$ und $\psi : R \to T$, so heißt ein Ringhomomorphismus $\Phi : S \to T$ ein *R-Algebrenhomomorphismus* oder ein *Homomorphismus von R-Algebren*, wenn $\psi = \Phi \circ \varphi$ gilt.

c) Sei S/R eine Algebra und $I \subseteq S$ ein Ideal, so ist S/I eine R-Algebra mit Strukturhomomorphismus

$$R \xrightarrow{\varphi} S \xrightarrow{\varepsilon} S/I$$

Die R-Algebra S/I heißt die *Restklassenalgebra* von S modulo I.

Bemerkung 11.24 Eine R-Algebra S ist nichts anderes als ein kommutativer Ring S, der die Struktur eines R-*Modules* besitzt:
Man hat eine Skalarmultiplikation

$$\begin{array}{ccc} R \times S & \to & S \\ (r, s) & \mapsto & \varphi(r) \cdot s \end{array}$$

Diese ist treu (d.h. $1 \cdot s = s$) und erfüllt die Distributivgesetze, sowie das Assoziativgesetz.

Beispiel 11.25

a) Ist $L|K$ eine Körpererweiterung, so ist L eine K-Algebra.

b) Sei R ein Ring. Dann ist der Polynomring $R[x]$ eine R-Algebra, wobei der Strukturhomomorphismus die Inklusion

$$R \hookrightarrow R[x]$$

ist. Allgemeiner ist $R[x_1, \ldots, x_n]$ eine R-Algebra bzgl. $R \hookrightarrow R[x_1, \ldots, x_n]$.

c) Ist R ein Ring und $I \subseteq R$ ein Ideal, so ist R/I eine R-Algebra mit Strukturhomomorphismus

$$\varepsilon : \begin{array}{ccc} R & \to & R/I \\ r & \mapsto & r + I \end{array}$$

Satz 11.26 *Die universelle Eigenschaft des Polynomrings*
Sei S/R eine Algebra und seien $s_1, \ldots, s_n \in S$. Dann gibt es einen eindeutig bestimmten R-Algebrenhomomorphismus

$$\Phi : \begin{array}{ccc} R[x_1, \ldots, x_n] & \to & S \\ x_i & \mapsto & s_i \end{array}$$

Definition 11.27 Sei S/R eine Algebra und sei $\{s_\lambda \mid \lambda \in \Lambda\}$ eine Menge von Elementen von S

a) Die kleinste R-Unteralgebra von S, die $\varphi(R)$ und $\{s_\lambda \mid \lambda \in \Lambda\}$ enthält, heißt die von $\{s_\lambda \mid \lambda \in \Lambda\}$ *erzeugte R-Unteralgebra* von S.
Sie wird mit $R[\{s_\lambda \mid \lambda \in \Lambda\}]$ bezeichnet.

b) Im Fall $\Lambda = \{1, \ldots, n\}$ schreiben wir auch $R[s_1, \ldots, s_n]$ statt $R[\{s_\lambda \mid \lambda \in \Lambda\}]$ und sagen R entstehe aus S durch *Ringadjunktion* von $s_1, \ldots, s_n$ an R.

c) Ist $S = R[\{s_\lambda \mid \lambda \in \Lambda\}]$, so heißt $\{s_\lambda \mid \lambda \in \Lambda\}$ ein *(Algebra-)Erzeugendensystem* von S/R.
Besitzt S/R ein endliches Algebraerzeugendensystem, so heißt S eine *endlich erzeugte R-Algebra* oder eine *R-Algebra von endlichem Typ*.

Satz 11.28 Sei S/R eine Algebra und $\{s_1, \ldots, s_n\} \subseteq S$.

a) Die erzeugte R-Algebra $R[s_1, \ldots, s_n]$ ist das Bild des kanonischen R-Algebrahomomorphismus

$$\Phi : \begin{array}{ccc} R[x_1, \ldots, x_n] & \to & S \\ x_i & \mapsto & s_i \end{array}$$

b) Die R-Unteralgebra $R[s_1, \ldots, s_n]$ von S besteht aus den Elementen der Form

$$\sum_{i_1, \ldots, i_n \in \mathbb{N}} \varphi(c_{i_1, \ldots, i_n}) s_1^{i_1} \cdots s_n^{i_n}$$

mit $c_{i_1, \ldots, i_n} \in R$.

c) Die R-Algebra $R[s_1, \ldots, s_n]$ ist der Durchschnitt aller R-Unteralgebren von S, die $\{s_1, \ldots, s_n\}$ enthalten.

d) Es gibt ein Ideal $I \subseteq R[x_1, \ldots, x_n]$ und einen Isomorphismus von R-Algebren

$$\varphi : R[x_1, \ldots, x_n]/_I \to R[s_1, \ldots, s_n]$$

Beispiel 11.29 Sei $S = R[x, y]$.
Dann besteht $R[x^2, xy, y^2] \subseteq S$ aus allen Polynomen, in denen nur Monome geraden Grades auftreten. Der Kern des kanonischen R-Algebrenhomomorphismus

$$\Phi : \begin{array}{ccc} R[z_1, z_2, z_3] & \to & S \\ z_1 & \mapsto & x^2 \\ z_2 & \mapsto & xy \\ z_3 & \mapsto & y^2 \end{array}$$

ist das Hauptideal $I = (z_1 z_3 - z_2^2)$. Somit erhalten wir:

$$R[x^2, xy, y^2] \cong R[z_1, z_2, z_3]/_{(z_1 z_3 - z_2^2)}$$

12 Algebraische Körpererweiterungen

A. Endliche algebraische Körpererweiterungen

Im Folgenden sei stets $L|K$ eine Körpererweiterung.

Definition 12.1 a) Ein Element $a \in L$ heißt *algebraisch* über K, wenn es ein Polynom $f \in K[x] \setminus \{0\}$ gibt mit $f(a) = 0$. Ist $a \in L$ nicht algebraisch über K, so heißt a ein *transzendentes Element* über K.

b) Ist $a \in L$ algebraisch über K, so ist $\{f \in K[x] \mid f(a) = 0\}$ ein von Null verschiedenes Ideal in $K[x]$. Das eindeutig bestimmte normierte Polynom, das dieses Hauptideal erzeugt, heißt das *Minimalpolynom* von a über K und wird mit μ_a bezeichnet.

c) Ist $a \in L$ algebraisch über K, so heißt $\deg(\mu_a)$ der *Grad* von a über K und wird mit $\deg(a|K)$ bezeichnet.

d) Ist $a \in L$ transzendent über K, so setzen wir $\mu_a = 0$ und $\deg(a|K) = \infty$.

Beispiel 12.2

a) Ist $K = \mathbb{Q}$ und $L = \mathbb{C}$, so heißen die über K algebraischen Elemente von L auch *algebraische Zahlen*. Z.B. sind $\sqrt{3}, \sqrt[3]{2}, \mathrm{i} = \sqrt{-1}, \frac{1}{2}(1+\sqrt{5}), \ldots$ algebraische Zahlen.
Transzendente Elemente von $L|K$ heißen hier auch *transzendente Zahlen*. Z.B. sind $e, \pi, \ln(2)$ transzendente Zahlen. **Kommentar:** Beweis: schwierig!

b) Die n-ten Einheitswurzeln $a_j = e^{\frac{2\pi \mathrm{i}}{n} j} \in \mathbb{C}$ mit $j \in \{0, \ldots, n-1\}$ sind genau die Nullstellen des Polynoms $x^n - 1$, also algebraische Zahlen.

c) Für $a \in L$ gilt:
$$\deg(a|K) = 1 \quad \Leftrightarrow \quad a \in K$$

d) Es gilt $\deg(\sqrt[3]{2}|\mathbb{Q}) = 3$.

Definition 12.3 Sei $L|K$ eine Körpererweiterung.

a) Der *Grad* von $L|K$ ist die Vektorraumdimension $\dim_K(L)$ und wird mit $[L : K]$ bezeichnet.

b) Der Körper L heißt *algebraisch* über K oder $L|K$ heißt eine *algebraische Körpererweiterung*, wenn jedes $a \in L$ über K algebraisch ist.

c) Ist $L|K$ nicht algebraisch, so heißt $L|K$ eine *transzendente Körpererweiterung*.

d) Die Körpererweiterung $L|K$ heißt *endlich*, wenn $\dim_K(L) < \infty$ gilt.

e) Die Körpererweiterung $L|K$ heißt *einfach*, wenn es ein $a \in L$ gibt mit $L = K(a)$.

Beispiel 12.4

a) $\mathbb{R}|\mathbb{Q}$ ist eine transzendente Körpererweiterung.

b) $\mathbb{C}|\mathbb{R}$ ist eine endliche algebraische Körpererweiterung vom Grad 2. Sie ist auch einfach, denn $\mathbb{C} = \mathbb{R}(\mathrm{i})$.

Satz 12.5 *Einfache Regeln für den Grad von Körpererweiterungen*
Sei $L|K$ eine Körpererweiterung.

a) Ist $L|K$ endlich, so ist $L|K$ algebraisch.

b) Ist $L|K$ endlich, so gilt
$$\deg(a|K) \leq [L:K]$$
für jedes $a \in L$. Hierbei gilt Gleichheit genau dann, wenn $L = K(a)$ ist.

c) Ist $L|K$ einfach, so gilt
$$[L:K] = \deg(a|K)$$
Im Fall $n = [L:K] < \infty$ gilt genau
$$L = K \oplus Ka \oplus \cdots \oplus Ka^{n-1}$$

Kommentar: $L|K$ algebraisch $\Rightarrow$ $K[a] = K(a)$

Definition 12.6 Sei $L|K$ eine Körpererweiterung. Ist $Z \subseteq L$ ein Teilkörper mit $Z \supseteq K$, so heißt Z ein *Zwischenkörper* von $L|K$.

Satz 12.7 *Die Gradformel*
Sei $L|K$ eine Körpererweiterung und Z ein Zwischenkörper von $L|K$. Dann gilt:
$$[L:K] = [L:Z] \cdot [Z:K]$$
Insbesondere ist $[Z:K]$ ein Teiler von $[L:K]$ falls $L|K$ endlich ist. Ferner ist $\deg(a|K)$ in diesem Fall für alle $a \in L$ Teiler von $[L:K]$.

Korollar 12.8 Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ und sei $z \in \mathbb{C}$ aus M mit Zirkel und Lineal konstruierbar. Ferner sei $K_0 = \mathbb{Q}(M \cup \overline{M})$.
Dann ist $K_0(z)|K_0$ eine endliche algebraische Körpererweiterung und es gilt
$$\deg(z|K_0) = 2^m \quad \text{für ein } m \in \mathbb{N}$$

Beispiel 12.9 *Würfelverdopplung*
Das Minimalpolynom von $\sqrt[3]{2}$ ist $x^3 - 2$. Insbesondere gilt $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Nach Korollar ist $\sqrt[3]{2}$ somit nicht aus $\{0,1\}$ mit Zirkel und Lineal konstruierbar. Also ist das Delische Problem der Würfelverdopplung nicht lösbar.

Beispiel 12.10 *Die Quadratur des Kreises*
Man kann zeigen, dass π eine transzendente Zahl ist. Daher ist $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ und die Quadratur des Kreises ist mit Zirkel und Lineal unmöglich.

Satz 12.11 Sei $L|K$ eine endlich erzeugte Körpererweiterung, d.h.

$$\exists\, a_1, \ldots, a_n \in L: \quad L = K(a_1, \ldots, a_n)$$

Betrachte folgende Bedingungen:

a) $L|K$ endlich

b) $L|K$ algebraisch

c) $L = K[a_1, \ldots, a_n]$

Dann gilt „a) $\Leftrightarrow$ b) $\Rightarrow$ c)“.

Die Implikation „c) $\Rightarrow$ b)“ wird in Algebra II bewiesen. (Körpertheoretische Version des Hilbertschen Nullstellensatzes)

B. Der algebraische Abschluß eines Körpers

Satz 12.12 Sei $L|K$ eine Körpererweiterung. Dann ist die Menge aller über K algebraischen Elemente von L ein Zwischenkörper von $L|K$.

Definition 12.13 Sei $L|K$ eine Körpererweiterung.

a) Der Körper M aller über K algebraischen Elemente von L heißt der *algebraische Abschluß von K in L*.

b) Der algebraische Abschluß von $\mathbb{Q}$ in $\mathbb{C}$ heißt der *Körper der algebraischen Zahlen* und wird mit $\overline{\mathbb{Q}}$ bezeichnet.

c) Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes Polynom $f \in K[x] \setminus \{0\}$ eine Nullstelle in K besitzt.

Satz 12.14 Sei $L|K$ eine Körpererweiterung, wobei L algebraisch abgeschlossen ist. Ferner sei M der algebraische Abschluß von K in L. Dann ist M algebraisch abgeschlossen.

Beispiel 12.15

a) Nach dem Fundamentalsatz der Algebra ist $\mathbb{C}$ ein algebraisch abgeschlossener Körper.

b) Für jeden Teilkörper $K \subseteq \mathbb{C}$ ist der algebraische Abschluß $\overline{K}$ von K in $\mathbb{C}$ ein algebraisch abgeschlossener Körper. Insbesondere ist der Körper $\overline{\mathbb{Q}}$ der algebraischen Zahlen ein algebraisch abgeschlossener Körper.

Satz 12.16 *Charakterisierung algebraisch abgeschlossener Körper*
Für einen Körper K sind die folgenden Bedingungen äquivalent:

a) K ist algebraisch abgeschlossen.

b) Die irreduziblen Polynome in $K[x]$ sind die Polynome vom Grad 1.

c) Jedes Polynom $f \in K[x] \setminus \{0\}$ besitzt eine eindeutige Darstellung

$$f = c(x - a_1)^{\mu_1} \cdots (x - a_n)^{\mu_n}$$

mit $c \in K \setminus \{0\}, \mu_i \in \mathbb{N}_+$ und $a_i \in K$ paarweise verschieden.

d) Ist $L|K$ eine algebraische Körpererweiterung, so gilt $L = K$.

Definition 12.17 Sei K ein Körper. Ein Erweiterungskörper $\overline{K}$ von K heißt ein *algebraischer Abschluß* von K, wenn $\overline{K}|K$ algebraisch ist und $\overline{K}$ ist algebraisch abgeschlossen.

Frage:

a) Besitzt jeder Körper K einen algebraischen Abschluß $\overline{K}$?

b) Ist der algebraische Abschluß $\overline{K}$ von K bis auf Isomorphie eindeutig bestimmt?

Lemma 12.18

a) Sind $M|L$ und $L|K$ algebraische Körpererweiterungen, so ist auch $M|K$ algebraisch.

b) Ist $f \in K[x]$ irreduzibel, so ist $L = K[x]/_{(f)}$ eine endliche algebraische Körpererweiterung von K vom Grad $[L : K] = \deg(f)$.

c) Sind $f_1, \ldots, f_n \in K[x] \setminus K$, so gibt es eine algebraische Körpererweiterung $L|K$, so dass jedes f_i eine Nullstelle in L besitzt.

Theorem 12.19 *Existenz des algebraischen Abschlusses - Steinitz 1910*
Zu jedem Körper K gibt es einen algebraischen Abschluß $\overline{K}$ von K.

Ziel: Wir zeigen noch die Eindeutigkeit von $\overline{K}$.

Satz 12.20 Sei $\overline{K}$ ein algebraischer Abschluß von K, sei $L|K$ eine algebraische Körpererweiterung und sei Z ein Zwischenkörper von $L|K$. Ferner sei $\varphi : Z \to \overline{K}$ ein K-Homomorphismus, d.h. ein Körperhomomorphismus mit $\varphi|_K = \mathrm{id}_K$. Dann gibt es eine Fortsetzung $\overline{\varphi} : L \to \overline{K}$, d.h. einen K-Homomorphismus $\overline{\varphi}$ mit $\overline{\varphi}|_Z = \varphi$.
Im Fall $Z = K$ gilt also insbesondere, dass jede algebraische Körpererweiterung $L|K$ in $\overline{K}$ eingebettet werden kann.

Korollar 12.21

a) Ist $\overline{K}$ ein algebraischer Abschluß von K und $L|K$ algebraisch, so gibt es einen K-Homomorphismus $\varphi : L \hookrightarrow \overline{K}$.

b) Sind $\overline{K}$ und $\tilde{K}$ zwei algebraische Abschlüsse von K, so gibt es einen K-Isomorphismus $\varphi : \overline{K} \xrightarrow{\sim} \tilde{K}$. Der algebraische Abschluß von K ist also bis auf einen K-Isomorphismus eindeutig bestimmt.

13 Separable Körpererweiterungen

Im Folgenden sei K ein Körper.

Definition 13.1 a) Ein irreduzibles Polynom $f \in K[x]$ heißt *separabel*, wenn f in $\overline{K}$ keine mehrfachen Nullstellen besitzt.

b) Ein beliebiges Polynom $f \in K[x]$ heißt *separabel*, wenn alle seine irreduziblen Faktoren separabel sind.

c) Ist $f \in K[x]$ nicht separabel, so heißt f *inseparabel*.

d) Der Körper K heißt *vollkommen*, wenn alle Polynome $f \in K[x]$ separabel sind.

Beispiel 13.2 In Charakteristik 0 ist jedes Polynom separabel, d.h. Körper der Charakteristik 0 sind vollkommen.

Beispiel 13.3 Sei p eine Primzahl und $K = \mathbb{F}_p(t) = Q(\mathbb{F}_p[t])$.
Betrachte $f = x^p + t \in K[x]$. Dann ist f inseparabel, aber irreduzibel in $K[x]$, d.h. $\mathbb{F}_p(t)$ ist kein vollkommener Körper.

Definition 13.4 Sei R ein Ring.

a) Ist $f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$, so heißt

$$f' = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1} \in R[x]$$

die *formale Ableitung* von f.

b) Ist $\mathrm{char}(R) = p$ Primzahl, so heißt die Abbildung

$$F : \begin{array}{ccc} R & \to & R \\ r & \mapsto & r^p \end{array}$$

der *Frobenius-Endomorphismus* von R.

Satz 13.5 Sei R ein Ring, $r \in R$ und $f, g \in R[x]$.

a) Ist $\deg(f) > 0$, so gilt $\deg(f') < \deg(f)$. Hierbei sei $\deg(0) = -1$.

b) Ist $\deg(f) = 0$, so gilt $f' = 0$.

c) Es gilt
$$(f+g)' = f' + g'$$

d) Es gilt die *Produktregel*:
$$(f \cdot g)' = f \cdot g' + f' \cdot g$$

Satz 13.6 Sei R ein Ring und $\mathrm{char}(R) = p$ eine Primzahl. Dann ist der Frobenius-Endomorphismus
$$F : \begin{array}{ccc} R & \to & R \\ r & \mapsto & r^p \end{array}$$
ein Ringhomomorphismus, d.h. für alle $a, b \in R$ gilt:

a) $(a+b)^p = a^p + b^p$

b) $(ab)^p = a^p b^p$

Satz 13.7 *Charakterisierung inseparabler Polynome*
Sei K ein Körper und $f \in K[x] \setminus K$ irreduzibel. Dann sind die folgenden Bedingungen äquivalent.

a) f ist inseparabel.

b) $f' = 0$

c) $\mathrm{char}(K) = p$ Primzahl und es gibt ein irreduzibles, separables Polynom $g \in K[x]$, sowie ein $e \in \mathbb{N}_+$ mit
$$f(x) = g(x^{p^e})$$

Definition 13.8 Sei $L|K$ eine Körpererweiterung.

a) Ein Element $a \in L$ heißt *separabel algebraisch* über K, wenn a über K algebraisch ist und $\mu_a \in K[x]$ separabel ist.

b) Ist $a \in L$ nicht separabel algebraisch, so heißt a *inseparabel*.

c) $L|K$ heißt *separabel algebraisch*, wenn alle $a \in L$ separabel algebraisch über K sind. Andernfalls heißt $L|K$ inseparabel.

Satz 13.9 Ist $L|K$ separabel algebraisch und ist Z ein Zwischenkörper von $L|K$, so sind auch $L|Z$ und $Z|K$ separabel algebraische Körpererweiterungen.

Lemma 13.10 Seien K_1, K_2 Körper und $\varphi : K_1 \hookrightarrow K_2$ ein injektiver Ringhomomorphismus. Sei $L = K_1[a]$ ein einfacher algebraischer Erweiterungskörper von K_1. Für das Minimalpolynom

$$\mu_a = c_0 + c_1 x + \cdots + c_n x^n$$

habe

$$\varphi(c_0) + \varphi(c_1)x + \cdots + \varphi(c_n)x^n$$

genau m verschiedene Nullstellen in K_2. Dann läßt sich φ auf genau m Arten zu einem Homomorphismus

$$\overline{\varphi} : L \hookrightarrow K_2$$

fortsetzen.

Satz 13.11 Sei $L|K$ eine endliche Körpererweiterung von Grad $n = [L : K]$ und sei $\overline{K}$ der algebraische Abschluß von K.

a) Es gibt höchstens n Einbettungen von L in $\overline{K}$ (also K-Homomorphismen $L \hookrightarrow \overline{K}$).

b) Genau dann ist $L|K$ separabel algebraisch, wenn es n Einbettungen von L in $\overline{K}$ gibt.

Korollar 13.12

a) Ist $M|K$ eine weitere algebraische Körpererweiterung, so gibt es höchstens n verschiedene K-Homomorphismen $\varphi : L \hookrightarrow M$.

b) Ist $L = K[a_1, \ldots, a_r]$ und ist a_i separabel über $K[a_1, \ldots, a_{i-1}]$ für $i = 1, \ldots, r$, so ist $L|K$ separabel.

c) Sind $M|L$ und $L|K$ separabel algebraische Körpererweiterungen, so ist $M|K$ separabel algebraisch.

d) Die Menge L_{sep} aller Elemente von L, die über K separabel algebraisch sind, bildet einen Zwischenkörper von $L|K$. Er heißt der *separable Abschluß* von K in L.
Die Zahl $[L_{sep} : K]$ heißt der *Separabilitätsgrad* von $L|K$.

Satz 13.13 Sei K ein Körper der Charakteristik $p > 0$.

a) Genau dann ist K vollkommen, wenn $K^p = K$ gilt.

b) Ist K endlich, so ist K vollkommen.

14 Normale Körpererweiterung

Im Folgenden sei $L|K$ eine Körpererweiterung.

Definition 14.1 Die Menge $\mathcal{G}al(L|K)$ aller K-Automorphismen von L, d.h. aller Körpererweiterungen $\varphi : L \xrightarrow{\sim} L$ mit $\varphi|_K = \mathrm{id}_K$, bildet bzgl. der Komposition eine Gruppe. Sie heißt die *Galoisgruppe* von $L|K$.

Bemerkung 14.2

a) Ist $L|K$ endlich, so gilt

$$\#\mathcal{G}al(L|K) \leq [L : K]$$

nach Korollar 13.12 a).

b) Ist $L = K[a]$ eine einfache algebraische Erweiterung von K, so ist $\#\mathcal{G}al(L|K)$ gleich der Zahl der verschiedenen Nullstellen von μ_a in $\overline{K}$.
Jeder K-Homomorphismus $\varphi : L \to \overline{K}$ bildet nämlich a ab auf eine Nullstelle von μ_a in $\overline{K}$ und liefert genau einen K-Automorphismus

$$\varphi : L \xrightarrow{\sim} \varphi(L) \subseteq \overline{K}$$

Beispiel 14.3 Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}[\sqrt{d}]$, wobei $d \in \mathbb{Z} \setminus \{0, 1\}$ eine quadratfreie ganze Zahl sei. Dann hat $a = \sqrt{d}$ das Minimalpolynom $\mu_a = x^2 - d \in \mathbb{Q}[x]$ und es gilt

$$\#\mathcal{G}al(L|K) = [L : K] = 2$$

Beispiel 14.4 Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[3]{2})$. Das Minimalpolynom von $a = \sqrt[3]{2}$ über $\mathbb{Q}$ ist $\mu_a = x^3 - 2 \in \mathbb{Q}[x]$. In $\overline{\mathbb{Q}}$ gilt $\mu_a = (x - a)(x - \rho a)(x - \rho^2 a)$ mit $\rho = -\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}$. Wegen $L \subseteq \mathbb{R}$ und $\rho a, \rho^2 a \notin \mathbb{R}$ gilt:

$$\mathcal{G}al(L|K) = \{\mathrm{id}_L\}$$

Definition 14.5 Die Körpererweiterung $L|K$ heißt *normal*, wenn $L|K$ algebraisch ist und wenn jedes Polynom $f \in K[x]$, das eine Nullstelle in L besitzt, in $L[x]$ in Linearfaktoren zerfällt.

Beispiel 14.6

a) Die Körpererweiterung $\mathbb{Q}(\sqrt{d})|\mathbb{Q}$ in Beispiel 14.3 ist normal, denn die Wurzeln von $x^2 - d$ liegen beide in $\mathbb{Q}(\sqrt{d})$.

b) Die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ ist nicht normal, denn die Wurzeln von $x^3 - 2$ liegen nur teilweise in $\mathbb{Q}(\sqrt[3]{2})$.

Satz 14.7 *Charakterisierung normaler Körpererweiterungen*
Sei $L|K$ eine algebraische Körpererweiterung und sei $\overline{L}$ der algebraische Abschluß von L (und damit auch von K). Dann sind die folgenden Bedingungen äquivalent:

a) $L|K$ ist normal.

b) Es gibt eine Menge von Polynomen $\{f_\lambda\}_{\lambda\in\Lambda} \subseteq K[x]$, so dass L aus K durch Adjunktion aller Wurzeln aller Polynome f_λ entsteht.
Sprechweise: Die Nullstellen eines Polynoms $f \in L[x]$ in $\overline{L}$ werden im Folgenden auch die *Wurzel* von f genannt.

c) Für jeden K-Homomorphismus $\sigma : L \to \overline{L}$ gilt:

$$\sigma(L) = L$$

D.h. σ induziert einen K-Automorphismus $\tilde{\sigma} : L \hookrightarrow L$.

Korollar 14.8 Ist $L|K$ normal und Z ein Zwischenkörper von $L|K$, so ist $L|Z$ normal.

Bemerkung 14.9 Ist $L|K$ normal und Z ein Zwischenkörper von $L|K$, so braucht $Z|K$ nicht normal zu sein. Z.B. ist $\overline{\mathbb{Q}}|\mathbb{Q}$ normal, aber $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ ist nicht normal.

Definition 14.10 Sei $f \in K[x]$.
Ein *Zerfällungskörper* von f ist ein Erweiterungskörper $L|K$ mit folgenden Eigenschaften:

a) f zerfällt in $L[x]$ in Linearfaktoren.

b) Sind $a_1, \ldots, a_n \in L$ die Nullstellen von f, so gilt:

$$L = K[a_1, \ldots, a_n]$$

Satz 14.11 *Existenz und Eindeutigkeit des Zerfällungskörpers*
Sei $f \in K[x] \setminus K$.

a) Es gibt einen Zerfällungskörper L von f.

b) Sind $L, \tilde{L}$ zwei Zerfällungskörper von f, so gibt es einen K-Isomorphismus

$$\varphi : L \xrightarrow{\sim} \tilde{L}$$

Mit anderen Worten, bis auf einen K-Isomorphismus ist der Zerfällungskörper von f eindeutig bestimmt.

c) Ist L der Zerfällungskörper von f, so gilt

$$[L : K] \leq (\deg f)!$$

Satz 14.12 *Charakterisierung endlicher normaler Körpererweiterungen*
Sei $L|K$ eine endliche Körpererweiterung. Genau dann ist $L|K$ normal, wenn $L|K$ der Zerfällungskörper eines Polynoms $f \in K[x] \setminus K$ ist.

Satz 14.13 Sei $L|K$ eine algebraische Körpererweiterung.

a) Es gibt eine Körpererweiterung $N|L$, so dass $N|K$ normal ist und so dass jeder Zwischenkörper Z von $N|L$ für den $Z|K$ normal ist, gleich N sein muß. Der Körper N heißt eine *normale Hülle* von $L|K$.

b) Ist $\tilde{N}|L$ eine weitere normale Hülle von $L|K$, so gibt es einen L-Isomorphismus $\varphi : N \xrightarrow{\sim} \tilde{N}$. Mit anderen Worten, die normale Hülle von $L|K$ ist bis auf einen L-Isomorphismus eindeutig bestimmt.

c) Sind $N, \tilde{N}$ zwei normale Hüllen von $L|K$ und ist $\varphi : N \to \tilde{N}$ ein L-Isomorphismus, so ist die Abbildung

$$\psi : \begin{array}{ccc} \mathcal{G}al(N|K) & \xrightarrow{\sim} & \mathcal{G}al(\tilde{N}|K) \\ \sigma & \mapsto & \varphi\sigma\varphi^{-1} \end{array}$$

ein Isomorphismus von Gruppen. Mit anderen Worten, die Galoisgruppe der normalen Hülle von $L|K$ ist bis auf einen Gruppenisomorphismus eindeutig bestimmt.

15 Galoische Körpererweiterung

A. Grundlagen

Im Folgenden sei $L|K$ eine Körpererweiterung.

Definition 15.1 Die Körpererweiterung $L|K$ heißt *Galoissch* oder eine *Galoiserweiterung*, wenn sie endlich, separabel und normal ist.

Beispiel 15.2 Sei $f \in K[x] \setminus K$ ein separables Polynom und sei L der Zerfällungskörper von f. Dann ist $L|K$ Galoissch.
In diesem Fall heißt

$$\mathcal{G}al(f) = \mathcal{G}al(L|K)$$

auch die *Galoisgruppe von* f.

Beispiel 15.3 Sei $K = \mathbb{Q}$ und $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Dann ist $L = \mathbb{Q}(\sqrt{d})$ eine Galoiserweiterung von K und $\mathcal{G}al(L|K) \cong \mathbb{Z}/_{2\mathbb{Z}}$.

Satz 15.4 *Charakterisierung von Galoiserweiterungen*
Sei $L|K$ eine Körpererweiterung. Dann sind die folgenden Bedingungen äquivalent:

a) $L|K$ ist Galoissch.

b) L ist der Zerfällungskörper eines separablen Polynoms $f \in K[x] \setminus K$.

c) Es gilt:
$$[L : K] < \infty \quad \text{und} \quad \#\mathcal{G}al(L|K) = [L : K]$$

Korollar 15.5

a) Sei K ein Körper der Charakteristik 0. Genau dann ist $L|K$ Galoissch, wenn L der Zerfällungskörper eines Polynoms aus $K[x]$ ist.

b) Sei $L|K$ Galoissch und Z ein Zwischenkörper von $L|K$. Dann ist auch $L|Z$ Galoissch und $\mathcal{G}al(L|Z) \subseteq \mathcal{G}al(L|K)$ eine Untergruppe.

Bemerkung 15.6 *Eigenschaften von $\mathcal{G}al(f)$*
Sei $f \in K[x] \setminus K$ separabel und $n = \deg(f) > 0$.

a) Jedes $\sigma \in \mathcal{G}al(f)$ permutiert die Wurzeln von f und ist durch diese Permutation eindeutig festgelegt. Somit erhalten wir einen injektiven Gruppenhomomorphismus $\mathcal{G}al(f) \hookrightarrow \mathcal{S}_n$. Insbesondere gilt $\#\mathcal{G}al(f) \leq n!$

b) Die Wurzeln eines irreduziblen Faktors von f werden durch ein $\sigma \in \mathcal{G}al(f)$ unter sich permutiert.

c) Ist f irreduzibel, so operiert $\mathcal{G}al(f)$ transitiv auf den Wurzeln von f, d.h. für $a_1, a_2 \in \overline{K}$ mit $f(a_1) = f(a_2) = 0$ gibt es ein $\sigma \in \mathcal{G}al(f)$ mit $\sigma(a_1) = a_2$.

d) Ist f irreduzibel, so gilt $n|\#\mathcal{G}al(f)$.

Beispiel 15.7 Das Polynom $f = x^3 - 2 \in \mathbb{Q}[x]$ ist irreduzibel, separabel und besitzt die Wurzeln $a = \sqrt[3]{2}, \rho a, \rho^2 a$ mit $\rho = -\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$. Dann ist $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ die normale Hülle von $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$. Sie ist eine Galoiserweiterung von $\mathbb{Q}$. Es gilt sogar $\mathcal{G}al(f) \cong \mathcal{S}_3$. Mit anderen Worten, alle Permutationen der Wurzeln von f definieren $\mathbb{Q}$-Automorphismen von L.

Definition 15.8 Sei G eine Gruppe. Ein Gruppenhomomorphismus
$$\chi : G \to K^\times$$
heißt auch ein *(linearer) Charakter* von G in K.

Beispiel 15.9

a) Seien K_1, K_2 Körper und $\sigma : K_1 \to K_2$ ein Ringhomomorphismus $\neq 0$. Dann induziert σ einen Gruppenhomomorphismus $\sigma|_{K_1^\times} : K_1^\times \to K_2^\times$ und somit einen Charakter von $K_1^\times$ in $K_2^\times$.

b) Jeder Automorphismus $\sigma : L \to L$ liefert einen Charakter $\sigma|_{L^\times} : L^\times \to L^\times$.

Satz 15.10 *Lineare Unabhängigkeit der Charaktere*
Sei G eine Gruppe, sei K ein Körper und seien $\sigma_1, \ldots, \sigma_n : G \to K^\times$ paarweise verschiedene Charaktere.
Sind $a_1, \ldots, a_n \in K$ mit

$$\underbrace{(a_1\sigma_1 + \cdots + a_n\sigma_n)(g)}_{=a_1\sigma_1(g)+\cdots+a_n\sigma_n(g)} = 0$$

für alle $g \in G$, so folgt

$$a_1 = a_2 = \cdots = a_n = 0$$

B. Der Hauptsatz der Galoistheorie

Theorem 15.11 Sei L ein Körper und sei G eine endliche Untergruppe von $\mathrm{Aut}(L)$. Ferner sei

$$K = \{a \in L \mid \sigma(a) = a \ \forall\, \sigma \in G\}$$

die Menge der G-invarianten Elemente von L.

a) Dann ist K ein Teilkörper von L.

b) Es gilt

$$[L : K] = \#G$$

c) $L|K$ ist Galoissch mit $\mathcal{G}al(L|K) = G$.

Definition 15.12 Sei $L|K$ eine Galoiserweiterung und sei $G = \mathcal{G}al(L|K)$

a) Die Menge der Zwischenkörper von $L|K$ bezeichnen wir mit $\mathfrak{Z}_{L|K}$ oder einfach mit $\mathfrak{Z}$.

b) Die Menge der Untergruppen von G bezeichnen wir mit $\mathfrak{U}_{L|K}$ oder einfach mit $\mathfrak{U}$.

c) Für $U \in \mathfrak{U}_{L|K}$ heißt

$$L_U = \{a \in L \mid \sigma(a) = a \ \forall\, \sigma \in U\}$$

der *Fixkörper* von U. Nach Theorem 15.11 ist L_U ein Zwischenkörper von $L|K$.

d) Für $Z \in \mathfrak{Z}_{L|K}$ heißt

$$G_Z = \{\sigma \in G \mid \sigma(a) = a \ \forall\, a \in Z\}$$

die *Isotropiegruppe* von Z. Offenbar gilt $G_Z \in \mathfrak{U}_{L|K}$.

Theorem 15.13 *Der Hauptsatz der Galoistheorie*
Sei $L|K$ eine Galoiserweiterung mit Galoisgruppe $G = \mathcal{G}al(L|K)$.

a) Die Abbildungen

$$\Phi : \begin{array}{ccc} \mathfrak{U} & \to & \mathfrak{Z} \\ U & \mapsto & L_U \end{array}$$

und

$$\Psi : \begin{array}{ccc} \mathfrak{Z} & \to & \mathfrak{U} \\ Z & \mapsto & G_Z \end{array}$$

sind bijektiv und zueinander invers. Somit entsprechen sich die Zwischenkörper von $L|K$ und die Untergruppen von G eindeutig.

b) Die Abbildungen Φ und Ψ sind inklusionsumkehrend.

- Für $Z_1, Z_2 \in \mathfrak{Z}$ mit $Z_1 \subseteq Z_2$ gilt also $\Psi(Z_1) \supseteq \Psi(Z_2)$, d.h. $G_{Z_1} \supseteq G_{Z_2}$
- Für $U_1, U_2 \in \mathfrak{U}$ mit $U_1 \subseteq U_2$ gilt also $\Phi(U_1) \supseteq \Phi(U_2)$, d.h. $L_{U_1} \supseteq L_{U_2}$

c) Für jedes $Z \in \mathfrak{Z}$ ist $L|Z$ Galoissch und G_Z ist die Galoisgruppe von $L|Z$.

d) Für jedes $U \in \mathfrak{U}$ ist

$$[L : L_U] = \#U$$

und $L|L_U$ ist Galoissch mit Galoisgruppe

$$U = \mathcal{G}al(L|L_U)$$

e) Für jedes $Z \in \mathfrak{Z}$ und $\sigma \in \mathcal{G}al(L|K)$ gilt

$$G_{\sigma(Z)} = \sigma G_Z \sigma^{-1}$$

f) Für $Z \in \mathfrak{Z}$ ist $Z|K$ genau dann Galoissch, wenn $G_Z \triangleleft G$ ein Normalteiler ist. In diesem Fall gilt

$$\begin{array}{ccc} G/G_Z & \xrightarrow{\sim} & \mathcal{G}al(Z|K) \\ \sigma G_Z & \mapsto & \sigma|_Z \end{array}$$

Korollar 15.14

a) Sei $L|K$ eine endliche separable Körpererweiterung. Dann besitzt $L|K$ nur endlich viele Zwischenkörper.

b) Ist $L|K$ Galoissch und $\mathcal{G}al(L|K)$ Abelsch und $Z \in \mathfrak{Z}_{L|K}$, so ist auch $Z|K$ Galoissch.

Bemerkung 15.15 *Das Umkehrproblem der Galoistheorie* fragt, ob jede endliche Gruppe G realisiert werden kann als Galoisgruppe einer endlichen Erweiterung von $\mathbb{Q}$. Für viele Gruppen ist dies bereits bewiesen, z.B. für auflösbare Gruppen (Insbesondere für endliche abelsche Gruppen).

Definition 15.16 Sei $L|K$ eine Körpererweiterung.

a) $L|K$ heißt *zyklisch*, wenn $L|K$ Galoissch ist und $\mathcal{G}al(L|K)$ zyklisch ist.

b) $L|K$ heißt *Abelsch*, wenn $L|K$ Galoissch ist und $\mathcal{G}al(L|K)$ Abelsch ist.

c) $L|K$ heißt *auflösbar*, wenn $L|K$ Galoissch ist und $\mathcal{G}al(L|K)$ auflösbar ist.

Bemerkung 15.17

a) Ist $L|K$ zyklisch vom Grad n, so entsprechen die Zwischenkörper von $L|K$ eineindeutig den Teilern von n.

b) Ist $L|K$ Abelsch, so gibt es zu jedem Teiler m von $n = [L : K]$ einen Zwischenkörper Z von $L|K$ mit $m = [Z : K]$. Für $Z \in \mathfrak{Z}_{L|K}$ sind dabei $L|Z$ und $Z|K$ Abelsch.

c) Ist $L|K$ auflösbar und $Z \in \mathfrak{Z}_{L|K}$, so ist $L|Z$ auflösbar.

d) Ist $L|K$ Galoissch und $[L : K] = p^r$ mit einer Primzahl p und $r \geq 1$, so ist $L|K$ auflösbar.

e) Ist $L|K$ Galoissch mit $\mathcal{G}al(L|K) \cong \mathcal{S}_n$ mit $n \geq 5$, so ist $L|K$ nicht auflösbar.

Beispiel 15.18 Gesucht ist $\mathcal{G}al(f)$ für $f = x^4 - x^2 - 1 \in \mathbb{Q}[x]$.

Kommentar: Der Körper $Z_2 = \mathbb{Q}[\mathrm{i}, \sqrt{5}]$ ist der einzige Zwischenkörper vom Grad 4 über $\mathbb{Q}$ mit $Z_2|\mathbb{Q}$ Galoissch.

C. Der Satz vom primitiven Element

Theorem 15.19 *Der Satz vom primitiven Element*
Für eine algebraische Körpererweiterung $L|K$ sind die folgenden Bedingungen äquivalent:

a) $L|K$ ist einfach, d.h. es gibt ein primitives Element $a \in L$ mit $L = K(a)$.

b) $L|K$ besitzt nur endlich viele Zwischenkörper.

c) Es gibt $a_1, \ldots, a_n \in L$, so dass $a_2, \ldots, a_n$ über K separabel sind und so dass $L = K[a_1, \ldots, a_n]$ gilt.

Korollar 15.20 Sei $\mathrm{char}(K) = p > 0$.
Dann sind die Bedingungen a) - c) auch äquivalent mit:

d) Es gilt $[L : K] < \infty$ und $[L : K(L^p)] \leq p$

Korollar 15.21

a) Jede endliche separable Körpererweiterung ist einfach.

b) Jede Galoiserweiterung ist einfach.

c) Ist $\mathrm{char}(K) = 0$, so ist jede endliche Körpererweiterung von K einfach.

d) Ist K vollkommen, so ist jede endliche Körpererweiterung von K einfach.

e) Jeder algebraische Zahlkörper ist eine einfache Erweiterung von $\mathbb{Q}$.

Beispiel 15.22 Die Erweiterung $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2})|\mathbb{Q}$ ist einfach mit primitivem Element $a = \sqrt[3]{2} + \sqrt{2}$.

16 Kreisteilungskörper

A. Grundlagen

Im Folgenden sei K ein Körper und $n \in \mathbb{N}_+$.

Definition 16.1 Der n-te *Kreisteilungskörper* (oder *Einheitswurzelkörper* oder *zyklotomische Körper*) ist der Zerfällungskörper L des Polynoms

$$f = x^n - 1 \in K[x]$$

Die Nullstellen von f in L heißen *n-ten Einheitswurzeln* über K.

Bemerkung 16.2

a) Die n-ten Einheitswurzeln über K bilden eine (endliche) Untergruppe von $L^\times$.

b) Die Gruppe der n-ten Einheitswurzeln ist zyklisch.

c) Ist $a \in L$ ein primitives Element dieser Gruppe, so gilt $L = K[a]$.

d) Ist $K = \mathbb{Q}$, so gilt $L = \mathbb{Q}[e^{\frac{2\pi i}{n}}]$.

e) Ist $\mathrm{char}(K) = p > 0$ und gilt $p|n$, so schreibe $n = p^\lambda m$ mit $\lambda > 0$, $m > 0$ und $p \nmid m$ und erhalte $x^n - 1 = (x^m)^{p^\lambda} - 1 = (x^m - 1)^{p^\lambda}$. Also ist jede n-te Einheitswurzel auch eine m-te Einheitswurzel. Somit können wir im Folgenden annehmen, dass p kein Teiler von n ist.

Satz 16.3 Sei $\mathrm{char}(K)$ kein Teiler von n und $L|K$ der n-te Kreisteilungskörper. Dann ist $L|K$ eine Galoiserweiterung.

Frage:

1) Was ist $[L : K]$?

2) Was ist $\mathcal{G}al(L|K)$?

Definition 16.4 Sei $L|K$ der n-te Kreisteilungskörper.

a) Ein erzeugendes Element a der Gruppe der n-ten Einheitswurzeln heißt eine *primitive n-te Einheitswurzel*. Da eine zyklische Gruppe der Ordnung n genau $\varphi(n)$ primitive Elemente besitzt, gibt es genau $\varphi(n)$ primitive n-te Einheitswurzeln $a_1, \ldots, a_{\varphi(n)}$.

b) Das Polynom
$$\Phi_n = \prod_{i=1}^{\varphi(n)} (x - a_i) \in L[x]$$
heißt das *n-te Kreisteilungspolynom*.

Beispiel 16.5

a) Sei $K = \mathbb{Q}$ und $n = 6$. Dann besitzt $\mathbb{Z}/_{6\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{5}\}$ genau $\varphi(6) = 2$ primitive Elemente, nämlich $\bar{1}$ und $\bar{5}$. Also sind $a_1 = e^{\frac{2\pi i}{6} \cdot 1} = \frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}$ und $a_2 = e^{\frac{2\pi i}{6} \cdot 5} = \frac{1}{2} - \frac{\sqrt{3}}{2}\mathrm{i}$ die primitiven 6-ten Einheitswurzeln und es gilt
$$\Phi_6 = (x - a_1)(x - a_2) = x^2 - x + 1$$

b) Sei $K = \mathbb{Q}$ und $n = p$ eine Primzahl. Dann gilt $\varphi(n) = n - 1$ und die primitiven n-ten Einheitswurzeln sind alle n-ten Einheitswurzeln außer 1. Es folgt
$$\Phi_n = \frac{x^n - 1}{x - 1} = 1 + x + \cdots + x^{n-1}$$

c) Es gilt
$$\Phi_1 = x - 1$$
Der 1-te Kreisteilungskörper ist $L = K$.

Satz 16.6 *Eigenschaften des n-ten Kreisteilungspolynoms*

a) Es gilt:
$$x^n - 1 = \prod_{d|n} \Phi_d$$

b) Sei $K_0 \subseteq K$ der Primkörper (d.h. $K_0 = \mathbb{Q}$, falls $\mathrm{char}(K) = 0$ oder $K_0 = \mathbb{Z}/_{p\mathbb{Z}}$, falls $\mathrm{char}(K) = p > 0$). Dann gilt
$$\Phi_n \in K_0[x]$$

c) Ist $K = \mathbb{Q}$, so ist $\Phi_n \in \mathbb{Q}[x]$ irreduzibel.

Kommentar: Ist a eine primitive Einheitswurzel, so gilt in c) $\Phi_n = \mu_a$ mit dem Minimalpolynom μ_a zu a.

Satz 16.7 Sei $\mathrm{char}(K)$ kein Teiler von n und $L|K$ sei der n-te Kreisteilungskörper.

a) $\mathcal{G}al(L|K)$ ist isomorph zu einer Untergruppe zu $(\mathbb{Z}/_{n\mathbb{Z}})^\times$. Insbesondere ist $L|K$ Abelsch.

b) Ist $K = \mathbb{Q}$, so gilt
$$\mathcal{G}al(L|K) \cong (\mathbb{Z}/_{n\mathbb{Z}})^\times$$
und
$$[L : \mathbb{Q}] = \varphi(n)$$

Beispiel 16.8

a) Es gilt
$$\mathcal{G}al(\mathbb{Q}[e^{\frac{2\pi \mathrm{i}}{6}}]|\mathbb{Q}) \cong (\mathbb{Z}/_{6\mathbb{Z}})^\times \cong \mathbb{Z}/_{2\mathbb{Z}} \cong \mathcal{G}al(\mathbb{Q}[\sqrt{-3}]|\mathbb{Q})$$

b) Es gilt
$$\mathcal{G}al(\mathbb{Q}[e^{\frac{2\pi \mathrm{i}}{4}}]|\mathbb{Q}) = \mathcal{G}al(\mathbb{Q}[\mathrm{i}]|\mathbb{Q}) \cong \mathbb{Z}/_{2\mathbb{Z}}$$

c) Es gilt
$$\mathcal{G}al(\mathbb{Q}[e^{\frac{2\pi \mathrm{i}}{5}}]|\mathbb{Q}) \cong (\mathbb{Z}/_{5\mathbb{Z}})^\times \cong \mathbb{Z}/_{4\mathbb{Z}}$$

Kommentar: Bei $\mathbb{Z}/_{4\mathbb{Z}} \cong (\mathbb{Z}/_{5\mathbb{Z}})^\times$ gilt $\bar{1} \mapsto \bar{2}$.

Lemma 16.9 *Dirichlet*
Sei $q > 1$. Dann gibt es in der Restklasse $1 + q\mathbb{Z}$ unendlich viele Primzahlen.

Satz 16.10 Ist G eine endliche Abelsche Gruppe, so gibt es eine Galoiserweiterung $L|\mathbb{Q}$ mit
$$\mathcal{G}al(L|\mathbb{Q}) \cong G$$

B. Konstruktion regulärer n-Ecke

Frage: Für welche $n \geq 2$ kann man den Einheitskreis mit Zirkel und Lineal in n gleiche Bögen unterteilen ? („Kreisteilung“)

Satz 16.11 Sei $L|K$ eine Körpererweiterung und seien Z_1, Z_2, Z_3 Zwischenkörper von $L|K$ mit $Z_1 \subseteq Z_2$ und $Z_2|Z_1$ Galoissch.

a) Die Menge $Z_1 \cdot Z_3 = K(Z_1 \cup Z_3)$ und die Menge $Z_2 \cdot Z_3$ sind Zwischenkörper von $L|K$ mit $Z_1Z_3 \subseteq Z_2Z_3$. Der Körper Z_1Z_3 heißt das *Kompositum* der Erweiterungen $Z_1|K$ und $Z_3|K$.

b) Die Erweiterung $Z_2Z_3|Z_1Z_3$ ist Galoissch und $\mathcal{G}al(Z_2Z_3|Z_1Z_3)$ ist isomorph zu einer Untergruppe von $\mathcal{G}al(Z_2|Z_1)$.

Definition 16.12 Sei p eine Primzahl.
Eine Körpererweiterung $L|K$ heißt *p-metazyklisch*, wenn es eine Kette

$$K = Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_r = L$$

von Zwischenkörpern gibt, so dass $Z_i|Z_{i-1}$ für $i = 1, \ldots, r$ zyklisch von Grad p ist.

Korollar 16.13 Sei p eine Primzahl und $L|K$ eine Körpererweiterung.

a) Sind Z_1, Z_2 Zwischenkörper von $L|K$, so dass $Z_1|K$ und $Z_2|K$ p-metazyklisch ist, so ist auch $Z_1Z_2|K$ p-metazyklisch.

b) Ist $L|K$ p-metazyklisch und ist $N|L$ die Galoissche Hülle von $L|K$, so ist $\mathcal{G}al(N|K)$ eine p-Gruppe.

c) Ist $\mathrm{char}(K) \neq 2$ und L der Zerfällungskörper eines separablen Polynoms μ_a mit $a \in L$, so ist a genau dann in einem zweimetazyklischen Zwischenkörper Z von $L|K$ enthalten, wenn $[L : K]$ eine Zweierpotenz ist.

Theorem 16.14 *Charakterisierung konstruierbarer Zahlen*
Sei $M \subseteq \mathbb{C}$ mit $\{0, 1\} \subseteq M$ und sei $K_0 = \mathbb{Q}(M \cup \overline{M})$. Eine komplexe Zahl $z \in \mathbb{C}$ sei algebraisch über K_0 mit Minimalpolynom $\mu_z \in K_0[x]$. Dann sind die folgenden Bedingungen äquivalent:

a) Die Zahl z ist aus M mit Zirkel und Lineal konstruierbar.

b) Ist L der Zerfällungskörper von μ_z, so ist $[L : K_0]$ eine Zweierpotenz.

c) $\mathcal{G}al(\mu_z)$ ist eine 2er-Gruppe.

Beispiel 16.15 Sei $p > 2$ eine Primzahl.
Das reguläre p-Eck ist genau dann konstruierbar, wenn

$$[\mathbb{Q}[e^{\frac{2\pi i}{p}}] : \mathbb{Q}] = \varphi(p) = p - 1$$

eine Zweierpotenz ist, also wenn $p = 2^n + 1$ eine *Fermatsche Primzahl* ist.

Satz 16.16 *Gauß*
Das reguläre n-Eck ist genau dann konstruierbar, wenn n von der Form

$$n = 2^m p_1 \cdots p_r$$

ist mit $m \geq 0$ und paarweise verschiedenen Fermatschen Primzahlen $p_1, \ldots, p_r$.

Bemerkung 16.17 Ist $p = 2^m + 1$ eine Fermatsche Primzahl, so muß $m = 2^k$ eine Zweierpotenz sein. Für $k = 0, 1, 2, 3, 4$ erhält man die Fermat-Primzahlen $3, 5, 17, 257$ und 65537.

17 Weitere Anwendungen der Galoistheorie

A. Endliche Körper

Sei K ein endlicher Körper. Dann ist $\mathrm{char}(K) = p > 0$ eine Primzahl. Der Primkörper von K ist $\mathbb{F}_p = \mathbb{Z}/_{p\mathbb{Z}}$. Ferner wissen wir bereits, dass $K^\times$ zyklisch ist und dass K vollkommen ist.

Satz 17.1 Sei K ein endlicher Körper und $p = \mathrm{char}(K)$.

a) Es gibt ein $e > 0$ mit $\#K = p^e$.

b) Die Körpererweiterung $K|\mathbb{F}_p$ ist Galoissch.

c) Es gibt bis auf Isomorphie genau einen Körper mit p^e Elementen.

Definition 17.2 Sei p eine Primzahl und $e > 0$.
Den Körper mit $q = p^e$ Elementen bezeichnen wir mit $\mathbb{F}_q$ und nennen ihn den *Galoiskörper* der Ordnung q.

Satz 17.3 Sei p eine Primzahl, $e > 0$ und $q = p^e$. Dann ist $\mathcal{G}al(\mathbb{F}_q|\mathbb{F}_p)$ eine zyklische Gruppe der Ordnung e. Sie wird erzeugt vom Frobenius-Automorphismus

$$F : \begin{array}{ccc} \mathbb{F}_q & \to & \mathbb{F}_q \\ x & \mapsto & x^p \end{array}$$

Korollar 17.4 Ist $L|K$ eine Erweiterung endlicher Körper, so ist $L|K$ zyklisch von der Ordnung $[L:K]$. Die Zwischenkörper von $L|K$ entsprechen eineindeutig den Teilern von $[L:K]$.

Korollar 17.5 Ist K ein endlicher Körper und $f \in K[x]$ irreduzibel vom Grad $e = \deg(f)$, so ist f separabel und $\mathcal{G}al(f)$ zyklisch. Im Fall $K = \mathbb{F}_p$ gilt insbesondere

$$\mathbb{F}_q = \mathbb{F}_p[x]/_{(f)}$$

mit

$$q = p^e$$

B. Der Fundamentalsatz der Algebra

Theorem 17.6 *Der Fundamentalsatz der Algebra*
Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

C. Auflösung von Gleichungen durch Radikale

Frage: Für welche $f \in K[x]$ sind die Wurzeln von f in $\overline{K}$ durch Radikale darstellbar ?

Im Folgenden sei K ein Körper.

Definition 17.7 Eine Gleichung $x^n - a = 0$ mit $n \geq 1$ und $a \in K^\times$ heißt eine *reine Gleichung*. Ist $\mathrm{char}(K)$ kein Teiler von n, so ist $x^n - a$ ein separables Polynom.

Satz 17.8 *Die Galoisgruppe reiner Gleichungen*
Sei $n \in \mathbb{N}_+$, sei $\mathrm{char}(K)$ kein Teiler von n und seien die n-ten Einheitswurzeln in K enthalten.

a) Die Galoisgruppe eines Polynoms $f = x^n - a$ mit $a \in K^\times$ ist zyklisch.

b) Zu jeder zyklischen Erweiterung $L|K$ vom Grad n gibt es ein $b \in L$ mit $b^n = a \in L^\times$ und $L = K[b]$.

c) Ist $f = x^n - a$ mit $a \in K^\times$ irreduzibel, so ist $\mathcal{G}al(f)$ zyklisch von der Ordnung n.

Beispiel 17.9 Sei K ein algebraisch abgeschlossener Körper und sei $\mathrm{char}(K)$ kein Teiler von $n \in \mathbb{N}_+$. Dann ist $K(x)|K(x^n)$ eine zyklische Erweiterung vom Grad n, denn $y^n - x^n \in K(x^n)[y]$ ist das Minimalpolynom von x über $K(x^n)$ und der Satz ist anwendbar.

Definition 17.10 Eine Körpererweiterung $L|K$ heißt *metazyklisch*, wenn es eine Kette von Zwischenkörpern $K = Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_l = L$ gibt, so dass $Z_i|Z_{i-1}$ für $i = 1, \ldots, l$ eine zyklische Körpererweiterung ist. Eine Galoiserweiterung $L|K$ ist offenbar genau dann metazyklisch, wenn $\mathcal{G}al(L|K)$ auflösbar ist.

Theorem 17.11 Sei $\mathrm{char}(K) = 0$ und sei $f \in K[x]$ irreduzibel. Dann sind die folgenden Bedingungen äquivalent:

a) Die Gleichung $f = 0$ ist durch Radikale auflösbar.

b) Die Galoisgruppe $\mathcal{G}al(f)$ ist auflösbar.

Fragen:

1) Gibt es nicht auflösbare Gleichungen ?

2) Welche ?

Definition 17.12 Sei R ein Ring und $P = R[x_1, \ldots, x_n]$ ein Polynomring über R.

a) Die symmetrische Gruppe $\mathcal{S}_n$ operiert auf P vermöge

$$\begin{array}{ccc} \mathcal{S}_n \times P & \to & P \\ (\sigma, f) & \mapsto & f(x_{\sigma(1)}, \ldots, x_{\sigma(n)} = f^\sigma \end{array}$$

D.h. mittels Permutation der Unbestimmten.

b) Ein Polynom $f \in P$ heißt *symmetrisch*, wenn für alle $\sigma \in \mathcal{S}_n$ gilt $f = f^\sigma$.

c) Für $i = 1, \ldots, n$ heißt

$$\varepsilon_i = \sum_{1 \le j_1 < j_2 < \cdots < j_i \le n} x_{j_1} \cdot x_{j_2} \cdots x_{j_i}$$

das i-te *elementarsymmetrische Polynom* in n Unbestimmten.

Bemerkung 17.13 *Eigenschaften!elementarsymmetrische Polynome*
Sei R ein Ring und $P = R[x_1, \ldots, x_n]$.

a) Es gilt

$$z_1 = x_1 + x_2 + \cdots + x_n$$

und

$$\varepsilon_n = x_1 x_2 \cdots x_n$$

Für $n = 3$ gilt z.B. $\varepsilon_2 = x_1x_2 + x_1x_3 + x_2x_3$.

b) Für jedes $i \in \{1, \ldots, n\}$ ist ε_i ein symmetrisches Polynom.

c) Sei y eine weitere Unbestimmte. Dann gilt in $P[y]$:

$$(y - x_1)(y - x_2) \cdots (y - x_n) = y^n - \varepsilon_1 y^{n-1} + \varepsilon_2 y^{n-2} - + \cdots + (-1)^n \varepsilon_n$$

d) Die Menge aller symmetrischen Polynome ist ein Unterring von P. Wir bezeichnen ihn mit P^{sym}.

e) Sei jetzt R ein Integritätsring mit Quotientenkörper $K = Q(R)$.
Jeder R-Automorphismus $\sigma : P \to P$ liefert einen K-Automorphismus

$$\bar{\sigma} : K(x_1, \ldots, x_n) \to K(x_1, \ldots, x_n)$$

mit

$$\bar{\sigma}(\frac{f}{g}) = \frac{\sigma(f)}{\sigma(g)}$$

für $f, g \in R[x_1, \ldots, x_n]$. Der Fixkörper von $\{\bar{\sigma} \mid \sigma \in \mathcal{S}_n\}$ ist ein Teilkörper von $K(x_1, \ldots, x_n)$ und heißt der *Körper der symmetrischen Funktionen*.

Satz 17.14 *Hauptsatz über die elementarsymmetrischen Polynome*
Sei R ein Ring und $P = R[x_1, \ldots, x_n]$.

a) Es gilt

$$P^{sym} = R[\varepsilon_1, \ldots, \varepsilon_n]$$

Hierbei ist $\{\varepsilon_1, \ldots, \varepsilon_n\}$ *algebraisch unabhängig*, d.h. der kanonische surjektive R-Algebrenhomomorphismus

$$\begin{array}{ccc} R[y_1, \ldots, y_n] & \to & R[\varepsilon_1, \ldots, \varepsilon_n] \\ y_i & \mapsto & \varepsilon_i \end{array}$$

ist ein Isomorphismus.

b) Ist R ein Integritätsring und $K = Q(R)$, so ist $K(\varepsilon_1, \ldots, \varepsilon_n)$ der Körper der symmetrischen Funktionen und $K(x_1, \ldots, x_n)/K(\varepsilon_1, \ldots, \varepsilon_n)$ ist eine Galoiserweiterung vom Grad $n!$ mit Galoisgruppe $\mathcal{S}_n$.

Definition 17.15 Sei K ein Körper und $L = K(x_1, \ldots, x_n)$. Dann heißt

$$f = y^n + x_1 y^{n-1} + x_2 y^{n-2} + \cdots + x_n \in L[y]$$

das *allgemeine Polynom* n-ten Grades über K.

Bemerkung 17.16 Ist $\tilde{f} \in K[y]$ ein normiertes Polynom n-ten Grades, so gibt es einen K-Algebrenhomomorphismus $\varphi : L \to K$, so dass für die Fortsetzung $\bar{\varphi} : L[y] \to K[y]$ gilt $\bar{\varphi}(f) = \tilde{f}$.

Kommentar: f ist das allgemeine Polynom.

Satz 17.17 Sei K ein Körper, $L = K(x_1, \ldots, x_n)$ und $f \in L[y]$ das allgemeine Polynom n-ten Grades.

a) Es gilt
$$\mathcal{G}al(f) \cong \mathcal{S}_n$$

b) *(Abel)* Für $n \geq 5$ ist die allgemeine Gleichung n-ten Grades
$$f = 0$$
nicht durch Radikale auflösbar.

Beispiel 17.18 Betrachte das Polynom $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$, so gilt
$$\mathcal{G}al(f) \cong \mathcal{S}_5$$

Korollar 17.19 *Galois*
Das Polynom $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ liefert die Gleichung $f = 0$, die nicht durch Radikale auflösbar ist.

Index

p-Gruppe, 30
p-Sylowuntergruppe, 31
    Existenz, 32

Abel, 78
    Satz von, 48
Abelsch, 4, 69
    endlich erzeugte Gruppe
        Hauptsatz, 29
    freie Gruppe, 28
        Hauptsatz, 29
Ableitung, formale, 60
Abschluß
    algebraischer, 59
        Existenz, 59
    separable, 62
Abschluß, algebraische, 58
Adjunktion, 43
    Ring-, 54
    sukzessive, 46
Algebra, 53
    -Erzeugendensystem, 54
    endlichem Typ, 54
    endlich erzeugte, 54
    erzeugte Unter-, 54
    Fundamentalsatz, 75
    Restklassen-, 53
algebraisch, 55, 56
    abgeschlossen, 58
    Abschluß, 58, 59
        Existenz, 59
    Körpererweiterung, 56
    separabel, 61
    Zahlen, 56
        Körper der, 58
Algebrenhomomorphismus, 53
allgemeine Polynom, 77
Alphabet, 24
anisotrop, 10
Assoziativgesetz, 4
assoziiert, 48
Atome, 35
auflösbar, 34, 69
    durch Radikale, 48
Automorphismengruppe, 23
Automorphismus, 6, 42

Bahn, 15
Basis, 28
Bausteine, 10
Bereich, 36

Cardano, 47
Cauchy, Satz, 31
Charakter
    linearer, 66
    Lineare Unabhängigkeit, 67
Charakterisierung
    algebraisch abgeschlossener Körper, 58
    endliche normale Körpererweiterung, 65
    Galoiserweiterung, 66
    inseparable Polynome, 61
    konstruierbare Zahlen, 73
    normale Körpererweiterung, 64
Charakteristik, 40
Chinesische Restsatz, 30

Delisches Problem, 44
Diedergruppe, 33
direkte
    Produkt, 20
        universelle Eigenschaft, 21
    Summe, 22
        universelle Eigenschaft, 22
Dirichlet, 72

echter Teiler, 48
    Regeln, 49
Eigenschaften

Gal(f), 66
irreduzible Elemente, 49
Kreisteilungspolynom, 72
Primelemente, 49
einfach, 56
einfache Gruppe, 34
Einheit, 48
Einheitsideal, 37
Einheitswurzel, 27
-körper, 70
primitive, 71
Einheitswurzelgruppe, 27
Einselement, 36
Einsetzungshomomorphismus, 38
Eisenstein-Kriterium, 51
Element
erzeugendes, 9
neutrales, 4
Prim-, 49
primitives, 9
Satz vom primitiven, 69
transzendentes, 55
elementarer Reduktionsschritt, 24
elementarsymmetrische Polynom, 76
Eigenschaften, 76
Hauptsatz, 77
Elementarteiler, 29
Elementarzelle, 10
endlich, 56
endlich erzeugt, 37
endlich erzeugte
Abelsche Gruppe
Hauptsatz, 29
Algebra, 54
Ideal, 37
Endomorphismus, Frobenius-, 60
Epimorphismus, kanonischer, 18
Erweiterung
algebraische Körper-, 56
Galois-, 65
Charakterisierung, 66
Radikal-, 48
transzendente Körper-, 56
Erzeugende, 26
Erzeugendensystem, 37
Algebra-, 54
erzeugte
Ideal, 37
Teilkörper, 42
Unteralgebra, 54
Untergruppe, 23
Euklidische Algorithmus, 5
Eulersche Phi-Funktion, 10
Existenz, p-Sylowgruppen, 32
Exponent, 27
Exponentialfunktion, 7

Faktorgruppe, 18
faktorieller Ring, 50
Fermat
kleiner Satz, 9
Primzahl, 74
Ferrari, 47
Fixkörper, 68
Fixpunkt, 15
frei
Abelsche Gruppe, 28
Hauptsatz, 29
Gruppe, 25
universelle Eigenschaft, 25
Monoid, 24
nullteiler-, 36
torsions-, 30
Frobenius-Endomorphismus, 60
Fundamentalsatz der Algebra, 75

Galois, 48, 78
-erweiterung, 65
-gruppe, 63, 65
-gruppe reiner Gleichungen, 75
-körper, 74
Galoissch, 65
Galoistheorie
Hauptsatz, 68
Umkehrproblem, 69
Gauß, 53, 74

Gitterebene, 10
Gittergerade, 10
Grad, 56
Gradformel, 57
Gruppe, 4
  p-Gruppe, 30
  alternierende, 8
  Automorphismen-, 23
  einfache, 34
  Einheiten-, 48
  Einheitswurzel-, 27
  endlich erzeugte Abelsche
    Hauptsatz, 29
  freie, 25
    universelle Eigenschaft, 25
  freie Abelsche, 28
    Hauptsatz, 29
  Galois-, 63, 65
  Homomorphiesatz, 19
  p-Sylowunter-, 31
  Permutations-, 8
  symmetrische, 8
  Torsions-, 29
Gruppenhomomorphismus, 6, 19
Gruppentafel, 6

Halbgruppe, 4
Hauptideal, 37
  -ring, 37
Hauptsatz
  elementarsymmetrische Polynome,
    77
  endlich erzeugte Abelsche Grup-
    pen, 29
  freie Abelsche Gruppen, 29
  Galoistheorie, 68
hexagonal, 12
homogen, 10
Homomorphiesatz
  Gruppen, 19
  Ringe, 40
Homomorphismus
  Algebren-, 53
  Einsetzungs-, 38
  Gruppen-, 6, 19
  Körper-, 42
  Ring-, 37, 40
  Struktur-, 40, 53
  Substitutions-, 52

Ideal, 36, 40
  Einheits-, 37
  endlich erzeugtes, 37
  erzeugtes, 37
  Haupt-, 37
  Null-, 37
Index, 16
induktiv geordnet, 31
induzierte Ringhomomorphismus, 40
inseparabel, 60, 61
Integritätsring, 36
irreduzibel, 48
Irreduzibilität unter Ringhomomorphis-
    men, 52
isomorph, 6
Isomorphiesatz
  1. Noethersche, 20
  2. Noethersche, 20
    für Ringe, 41
Isomorphismus, 6
  Ring-, 38
Isotropiegruppe, 14, 68

Körper, 41
  -erweiterung, 42
    algebraische, 56
    Regeln für den Grad, 57
    transzendente, 56
  -homomorphismus, 42
  algebraischen Zahlen, 58
  Einheitswurzel-, 70
  Galois-, 74
  Kreisteilungs-, 70
  Prim-, 42
  quadratische Zahlen-, 43
  Quotienten-, 43

rationalen Funktionen, 44
symmetrische Funktionen, 77
Zerfällungs-, 64
Zwischen-, 57
zyklotomische, 70
Körpererweiterungen
Grad, 57
Kürzungsregeln, 5
kanonischer Epimorphismus, 18, 39
Kern, 7, 38
Klassengleichung, 17
kommutativ, 4, 36
komplexe Zahlenebene, 45
Kompositum, 73
Konjugation, 14
Konjugationsklasse, 15, 16
Konkatenation, 24
konstruierbar, 45
Konstruktion regulärer n-Ecke, 45, 47
Konstruktionsaufgabe, 44
Kreisteilungskörper, 70
Kreisteilungspolynom, 71
Eigenschaften, 72
Kristall, 10
Kristallbasis, 10
kristallographische Achsen, 10
Kristallstruktur, 11
Kristallsystem, 11
hexagonales, 12
kubisches, 12
monoklines, 11
orthorhombisches, 11
tetragonales, 11
trigonales, 11
triklines, 11
kubisch, 12

Lagrange, 16
Lemma von Zorn, 31
linearer Charakter, 66
Lineare Unabhängigkeit der Charaktere, 67
Linksnebenklasse, 16
Linkstranslation, 6, 14

Menge
symmetrische Polynome, 77
Untergruppen, 67
Zwischenkörper, 67
metazyklisch, 73, 76
minimale Nennerbeseitigung, 53
Minimalpolynom, 56
Modul, 54
modulo, 16, 38
Monoid, 4
frei, 24
monoklin, 11

Nennerbeseitigung, minimale, 53
Netzebene, 10
Noethersche Isomorphiesatz
1., 20
2., 20
2. für Ringe, 41
normal, 63
Normalisator, 15
Normalreihe, 34
Normalteiler, 17, 19
Notation
additive, 5
multiplikative, 5
Nullideal, 37
Nullring, 36, 38
nullteilerfrei, 36

Operation, 13
Ordnung, 4, 9
orthorhombisch, 11

Permutation, 8
gerade, 8
ungerade, 8
Permutationsgruppe, 8
Polynomring, 36
universelle Eigenschaft, 54
Präsentation, 26
Prim

-element, 49
Eigenschaften, 49
-körper, 42
-ring, 40, 42
Primfaktorzerlegung, Eindeutigkeit, 50
primitive
Einheitswurzel, 71
Element, Satz, 69
Produkt
-regel, 61
direkte, 20
universelle Eigenschaft, 21
semidirekte, 23
Projektion, 21
Punktgruppe, 12

quadratische Zahlenkörper, 43
Quadratur des Kreises, 45, 46, 57
Quadratwurzeln, sukzessive Adjunktion von, 46
Quotienten
-gruppe, 18
-körper, 43

Radikale, auflösbar durch, 48
Radikalerweiterung, 48
Rang, 28, 29
rationalen Funktionen, Körper der, 44
Raumgitter, 10
Raumgruppe, 13
Rechtsnebenklasse, 16
Rechtstranslation, 6, 14
Reduktionsschritt, elementar, 24
reduziert, 24
Regeln
Grad von Körpererweiterungen, 57
Teiler und echter Teiler, 49
reine Gleichung, 75
Galoisgruppe, 75
Relation, 26
Restklassen, 4, 38
-algebra, 53
-gruppe, 18
universelle Eigenschaft, 19
-ring, 39
universelle Eigenschaft, 40
primitive, 9
Restsatz, Chinesische, 30
Ring, 36
-Isomorphismus, 38
-adjunktion, 54
-homomorphismus, 37, 40
induzierte, 40
faktorieller, 50
Hauptideal-, 37
Homomorphiesatz, 40
Integritäts-, 36
mit Einselement, 36
Null-, 38
Prim-, 40, 42
Restklassen-, 39
universelle Eigenschaft, 40
Unter-, 36
ZPE-, 50

Satz
1. Noethersche Isomorphie-, 20
1. Sylow, 32
2. Noethersche Isomorphie-, 20
für Ringe, 41
2. Sylow, 33
3. Sylow, 33
Abel, 48
Cauchy, 31
Chinesische Rest-, 30
Fundamentalsatz der Algebra, 75
Gauß, 53
Hauptsatz
elementarsymmetrische Polynome, 77
endlich erzeugte Abelsche Gruppen, 29
freie Abelsche Gruppen, 29
Galoistheorie, 68
Homomorphiesatz
für Gruppen, 19

für Ringe, 40
kleiner Fermatscher, 9
Lagrange, 16
primitives Element, 69
Teilerketten-, 50
semidirekte Produkt, 23
separabel, 60
algebraisch, 61
Separabilitätsgrad, 62
separable Abschluß, 62
Skalarmultiplikation, 54
Steinitz, 59
Strukturhomomorphismus, 40, 53
Substitutionshomomorphismus, 52
sukzessive Adjunktion, 46
Summe
direkt, 22
universelle Eigenschaft, 22
Sylow
-untergruppe, 31
Existenz, 32
1. Satz, 32
2. Satz, 33
3. Satz, 33
Symmetrie, 11
Symmetrieoperation, 11
symmetrisch, 76
symmetrische Polynom, Menge, 77

Teiler, 48
echter, 48
Regeln, 49
Teilerkettensatz, 50
Teilkörper, 42
erzeugte, 42
tetragonal, 11
torsionsfrei, 30
Torsionsgruppe, 29
Transformationsgruppe, 5
transitiv, 15
Transposition, 8
transzendent
Element, 55
Körpererweiterung, 56
Zahlen, 56
treu, 14
trigonal, 11
triklin, 11
Typ, Algebra von endlichem, 54

Umkehrproblem der Galoistheorie, 69
universelle Eigenschaft
direktes Produkt, 21
direkte Summe, 22
freie Gruppe, 25
Polynomring, 54
Restklassengruppe, 19
Restklassenring, 40
Unteralgebra, erzeugte, 54
Untergruppe, 6
erzeugte, 23
Menge der, 67
triviale, 7
Unterring, 36

vollkommen, 60

Wörter, 25
Würfelverdopplung, 44, 46, 57
Winkeldreiteilung, 45, 47
Wurzel, 64
Einheits-, 27

Zähligkeit, 11
Zahlenebene, komplexe, 45
Zahlenkörper, quadratische, 43
Zentralisator, 15
Zentrum, 15
Zerfällungskörper, 64
Zorn, 31
ZPE-Ring, 50
Zwischenkörper, 57
Menge der, 67
zyklisch, 9, 26, 69
meta-, 73, 76
zyklische Gruppe, 4
zyklotomische Körper, 70