Basiswissen Algebra

Andreas Nickel

Dies ist eine knappe Auflistung von wichtigen Definitionen und Sätzen der Algebra, die ich für Lehramtsstudierende (Lehramt an Gymnasien in Bayern) zusammengetragen habe bzw. gerade zusammentrage. Sie erhebt keinen Anspruch auf Vollständigkeit.

1 Gruppentheorie

Definition 1.1 *Eine Menge G zusammen mit einer Verknüpfung $\circ : G \times G \to G$ heißt eine* **Gruppe**, *falls*

1. $\forall x, y, z \in G : \ (x \circ y) \circ z = x \circ (y \circ z)$ (*"***Assoziativität***"*)
2. $\exists e \in G : \ x \circ e = e \circ x = x \ \forall x \in G$ (*"***neutrales Element***"*)
3. $\forall x \in G \ \exists y \in G : \ x \circ y = e$ (*"***Inverses***"*)

Eine Gruppe G heißt **abelsch**, *falls $x \circ y = y \circ x$ für alle $x, y \in G$.*

Das Element $e \in G$ bezeichnen wir auch häufig mit 1 und schreiben kurz xy für $x \circ y$. Für abelsches G notieren wir die Verknüpfung gelegentlich auch mit $+$, bezeichnen in diesem Fall das neutrale Element aber mit 0.

Definition 1.2 *Eine Teilmenge U von einer Gruppe G, die bezüglich der in G erklärten Verknüpfung selbst eine Gruppe ist, heißt eine* **Untergruppe** *von G. In Zeichen: $U \leq G$. Zwei Untergruppen U und V von G heißen* **konjugiert**, *falls ein $g \in G$ existiert mit $U = V^g := g^{-1}Vg = \{g^{-1}vg | v \in V\}$.*
Gilt $gug^{-1} \in U$ für alle $g \in G$, $u \in U$ (also $U^g = U \ \forall g \in G$), so heißt U ein **Normalteiler** *in G. In Zeichen: $U \lhd G$.*

Definition 1.3 *Die Anzahl $|G|$ aller Elemente in G heißt die* **Ordnung** *von G. Für $g \in G$ ist*

$$\langle g \rangle := \{g^n | n \in \mathbb{N}\}$$

eine Untergruppe von G, und man definiert die Ordnung von g als $\operatorname{ord}(g) = |g| := |\langle g \rangle|$. Ist $|G| = p^n$ für eine Primzahl p und ein $n \in \mathbb{N}$, so heißt G eine **p-Gruppe**.

Lemma 1.4 *Sei G eine endliche Gruppe und $U \leq G$. Dann ist $|U|$ ein Teiler von $|G|$.*

Das rechtfertigt die folgende

Definition 1.5 *Die Zahl* $[G:U] := \frac{|G|}{|U|} \in \mathbb{Z}$ *heißt der* **Index** *von* U *in* G.

Beispiele (mit kleinen Folgerungen):

1. Ist $G = \langle g \rangle$ für ein $g \in G$ der Ordnung $n \in \mathbb{N}$, so nennen wir G **zyklisch** der Ordnung n und schreiben $G \simeq C_n$. Typisch ist $G = \mathbb{Z}/n\mathbb{Z}$.

2. Die Gruppe $D_{2n} = \langle x, y | x^2 = 1, y^n = 1, xyx^{-1} = y^{-1} \rangle$ heißt die **Diedergruppe** der Ordnung $2n$.

3. Die Gruppe $Q_8 = \langle i, j | i^4 = 1, j^4 = 1, ij = j^3 i \rangle$ heißt die **Quaternionengruppe** der Ordnung 8.

4. Sei Ω eine Menge mit n Elementen. Die Gruppe aller **Permutationen** auf Ω bezeichnen wir mit S_n. Z.B. ist
$$S_3 = \langle \sigma, \tau | \sigma^3 = 1, \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^2 \rangle.$$

5. Seien G und H Gruppen. Dann ist
$$G \times H = \{(g,h) | g \in G, h \in H\}$$
mit der Verknüpfung $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ wieder eine Gruppe, das **direkte Produkt** von G und H.

6. Die Menge $Z(G) := \{g \in G | gh = hg \ \forall h \in G\} \lhd G$ heißt das **Zentrum** von G. Es gilt:
$$Z(G) = G \iff G \text{ abelsch.}$$

7. Ist G eine Gruppe, $U \leq G$, $N \lhd G$, so ist die Menge
$$UN := \{un | u \in U, n \in N\}$$
eine Untergruppe von G.

8. Ist $N \lhd G$, so ist $\overline{G} = G/N := \{\overline{g} | g \in G\}$ mit der neuen Gleichheit
$$\overline{g} = \overline{h} \iff gh^{-1} \in N$$
wieder eine Gruppe, die **Faktorgruppe** mod N. Man nennt G/N auch einen **Quotienten** von G.

9. Das **Kommutatorerzeugnis** $G' := \langle ghg^{-1}h^{-1} | g, h \in G \rangle$ ist normal in G. Für $N \lhd G$ gilt:
$$G/N \text{ abelsch} \iff G' \subset N.$$
Insbesondere ist also G/G' der größte abelsche Quotient von G.

Definition 1.6 *Seien G und H Gruppen. Eine Abbildung $\phi : G \to H$ heißt ein* **Gruppenhomomorphismus**, *falls $\phi(xy) = \phi(x)\phi(y)$ für alle $x, y \in G$. Die Menge*

$$\ker(\phi) := \{g \in G | \phi(g) = 1\}$$

ist normal in G und heißt der **Kern** *von ϕ. Das* **Bild** *von ϕ ist definiert als*

$$\mathrm{im}\,(\phi) := \{h \in H | \exists g \in G : \phi(g) = h\} \leq H.$$

ϕ heißt ein **Epimorphismus**, *falls $\mathrm{im}\,(\phi) = H$, ein* **Monomorphismus**, *falls ϕ injektiv, ein* **Isomorphismus**, *falls ϕ bijektiv ist. Im Falle $H = G$ spricht man von einem* **Endomorphismus**. *Ein bijektiver Endomorphismus heißt* **Automorphismus**. *Die Menge aller Automorphismen auf G bezeichnen wir mit $\mathrm{Aut}(G)$.*

Lemma 1.7 *Ein Gruppenhomomorphismus $\phi : G \to H$ ist injektiv genau dann, wenn $\ker(\phi) = 1$.*

Definition 1.8 *Gegeben seien zwei Gruppen G und H, sowie ein Gruppenhomomorphismus*

$$\eta : H \to \mathrm{Aut}(G), h \mapsto \eta(h) = [g \mapsto g^h].$$

Dann heißt

$$G \rtimes H = \{(g, h) | g \in G,\ h \in H\}$$

zusammen mit der Verknüpfung $(g_1, h_1)(g_2, h_2) = (g_1 g_2^{h_1^{-1}}, h_1 h_2)$ das **semidirekte Produkt** *aus G und H und η.*

Dabei gilt: $G \lhd G \rtimes H$ und $H \leq G \rtimes H$ über die natürlichen Einbettungen. Außerdem ist $|G \rtimes H| = |G| \cdot |H|$. Im Spezialfall, dass η jedes $h \in H$ auf die Identitätsabbildung in G abbildet, erhalten wir das direkte Produkt $G \times H$.

Satz 1.9 (1. Isomorphiesatz) *Jeder Gruppenhomomorphismus $\phi : G \to H$ induziert einen Isomorphismus*

$$G/\ker(\phi) \xrightarrow{\simeq} \mathrm{im}\,(\phi), \quad \overline{g} \mapsto \phi(g).$$

Satz 1.10 *Jedes $N \lhd G$ induziert einen Epimorphismus $\phi_N : G \to \overline{G} = G/N$. Es gilt:*

1. *(***2. Isomorphiesatz***) Für $U \leq G$ ist $\overline{U} := U/U \cap N \leq \overline{G}$ und*

   $$\overline{U} \simeq UN/N.$$

2. *(***3. Isomorphiesatz***) $U \lhd G \Longrightarrow \overline{U} \lhd \overline{G}$ und*

   $$G/U \simeq \overline{G}/\overline{U},\ g \bmod U \mapsto \overline{g} \bmod \overline{U}$$

3. *Die Untergruppen $U \leq G$ mit $N \subset U$ entsprechen eineindeutig den Untergruppen $\overline{U} \leq \overline{G}$. Dabei ist $U = \phi_N^{-1}(\overline{U})$.*

Wir schieben an dieser Stelle ein wichtiges Beispiel ein: die **symmetrische Gruppe** S_n.
Wir fassen S_n als die Gruppe aller Permutationen auf der Menge $M = \{1, \ldots, n\}$ auf. Ist $\{i_1, \ldots, i_k\}$ eine Teilmenge von M mit k Elementen ($2 \leq k \leq n$), und definiert man $\sigma \in S_n$ via $\sigma(j) = j$ für $j \in M \setminus \{i_1, \ldots, i_k\}$, $\sigma(i_j) = i_{j+1}$ für $j < k$ und $\sigma(i_k) = i_1$, so nennen wir σ einen **k-Zykel** und schreiben $\sigma = (i_1 \ldots i_k)$. Ein 2-Zykel heißt auch **Transposition**. Zwei Zykel $(i_1, \ldots, i_k)$ und $(j_1, \ldots, j_l)$ heißen **disjunkt**, falls $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset$.

Die Abbildung $\operatorname{sgn} : S_n \to \{\pm 1\}$ ("**Signum**") definiert durch

$$\prod_{1 \leq i < j \leq n} (i - j) = \operatorname{sgn}(\pi) \prod_{1 \leq i < j \leq n} (\pi(i) - \pi(j))$$

für $\pi \in S_n$ ist ein surjektiver Homomorphismus von Gruppen. Der Kern A_n heißt die **alterniernde Gruppe** auf n Elementen.

Satz 1.11 *1.* $|S_n| = n!$

2. *Für $n \geq 3$ ist S_n nicht abelsch.*
3. *Die Ordnung eines k-Zykels ist k.*
4. *Jedes $\pi \in S_n$ ist eindeutig als Produkt von paarweise disjunkten Zykeln darstellbar; die Faktoren vertauschen.*
5. *Zwei Permutationen π_1, $\pi_2 \in S_n$ sind konjugiert (d.h. es gibt ein $\rho \in S_n$ mit $\rho\pi_1\rho^{-1} = \pi_2$) genau dann, wenn die Zykelzerlegungen von π_1 und π_2 die selben Längen aufweisen. Für k-Zykel gilt $\rho(i_1, \ldots, i_k)\rho^{-1} = (\rho(i_1), \ldots, \rho(i_k))$.*
6. *Jedes $\pi \in S_n$ ist ein Produkt von Transpositionen.*
7. *Jede endliche Gruppe G lässt sich in S_n (für geeignetes n) einbetten. Wähle etwa $n = |G|$ und bilde ein $g \in G$ auf die Permutation π_g ab mit $\pi_g(h) = gh$ für $h \in G$. Hier ist π_g also eine Permutation auf der n-elementigen Menge G.*
8. $\operatorname{sgn}((i_1, \ldots, i_k)) = (-1)^{k+1}$.
9. $A_n \lhd S_n$
10. $|A_n| = \frac{n!}{2}$.
11. *Für $n \geq 3$ ist A_n von den 3-Zykeln erzeugt.*
12. *Sei p prim und $U \leq S_p$. Enthält U eine Transposition und gilt $p \mid |U|$, so folgt $U = S_p$.*

Die folgenden vier Sätze enthalten die wichtigsten Fakten über endliche abelsche Gruppen:

Satz 1.12 *Sei $G \simeq C_n$ zyklisch der Ordnung n. Dann gilt:*

1. *Jede Untergruppe und jede Faktorgruppe von G ist zyklisch.*
2. *Zu jedem $d|n$ existiert genau eine Untergruppe und genau eine Faktorgruppe von G der Ordnung d.*
3. *$C_n \times C_m \simeq C_{nm} \iff \mathrm{ggT}(n,m) = 1$.*

Satz 1.13 *Sei G zyklisch der Ordnung n. Dann gilt:*

1. *Die Automorphismengruppe $\mathrm{Aut}(G)$ ist abelsch.*
2. *Ist $n = p^k$ für eine Primzahl p, so ist $\mathrm{Aut}(G)$ zyklisch.*
3. *Ist $n = p^k$ für eine Primzahl $p \neq 2$, so ist*

$$\mathrm{Aut}(G) \simeq (\mathbb{Z}/n\mathbb{Z})^\times = \langle w_p^{p^{k-1}}(1+p) \bmod p^k \rangle$$

   *mit einem Erzeuger (einer "***Primitivwurzel***") w_p von $(\mathbb{Z}/p\mathbb{Z})^\times$.*

4. *Für $p = 2$, $k \geq 3$ ist*

$$(\mathbb{Z}/2^k\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z} = \langle -1 \bmod 2^k \rangle \times \langle 5 \bmod 2^k \rangle.$$

Definition 1.14 *Die Funktion $\phi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$ heißt die* **Eulersche ϕ-Funktion**.

Es gilt: $\phi(nm) = \phi(n)\phi(m)$, falls $\mathrm{ggT}(n,m) = 1$, und $\phi(p^k) = (p-1)p^{k-1}$ für Primzahlen p und $k \in \mathbb{N}$. Außerdem ist $\mathrm{ggT}(n, \phi(n)) = 1$ äquivalent zu der Aussage, dass jede Gruppe der Ordnung n zyklisch ist (bis auf Isomorphie existiert in diesem Fall also nur die zyklische Gruppe der Ordnung n).

Satz 1.15 *Sei G eine endliche abelsche Gruppe. Für jede Primzahl p definiere Untergruppen $G_p := \{g \in G | \mathrm{ord}\,(g) = p^n$ für ein $n \in \mathbb{N}\} \leq G$. Dann ist G_p eine p-Gruppe und G zerlegt sich in*

$$G = \bigtimes_{p||G|} G_p.$$

Satz 1.16 (Hauptsatz über endliche abelsche Gruppen) *Sei G eine endliche abelsche Gruppe. Dann existieren $r \in \mathbb{N}$ und zyklische Untergruppen $1 \neq Z_i \leq G$ der Ordnung $z_i = |Z_i|$, $1 \leq i \leq r$ mit*

$$G = Z_1 \times \ldots \times Z_r \text{ und } z_1|z_2| \ldots |z_r.$$

*Dabei sind r und die z_i ("***Elementarteiler***") eindeutig durch G bestimmt.*

Zum Bestimmen aller Gruppen von vorgegebener endlicher Ordnung spielen die folgenden Gruppen eine besondere Rolle.

Definition 1.17 *Sei G eine endliche Gruppe der Ordnung n und p eine Primzahl. Eine Untergruppe $P \leq G$ heißt eine* **p-Sylowuntergruppe** *von G, falls $|P| = p^s$ und $n = p^s \cdot m$ mit $p \nmid m$.*

Definition 1.18 *Sei $U \leq G$. Dann heißt die Untergruppe*

$$\mathfrak{N}_G(U) := \left\{ g \in G | gUg^{-1} = U \right\} \leq G$$

der **Normalisator** *von U in G.*

Insbesondere ist $U \lhd \mathfrak{N}_G(U) \leq G$, und der Normalisator ist maximal mit dieser Eigenschaft.

Satz 1.19 (Sylowsätze) *Sei G eine Gruppe der Ordnung $n = p^s \cdot m$ mit $p \nmid m$ und n_p die Anzahl der p-Sylowuntergruppen von G. Dann gilt:*

1. *$n_p \equiv 1 \mod p$. Insbesondere existiert also immer mindestens eine p-Sylowuntergruppe.*
2. *Ist P eine p-Sylowuntergruppe von G, dann ist $n_p = [G : \mathfrak{N}_G(P)]$. Insbesondere gilt $n_p | m$.*
3. *Ist P eine p-Sylowuntergruppe von G und $Q \leq G$ eine p-Gruppe, dann existiert ein $g \in G$ mit $Q \leq gPg^{-1}$. Insbesondere sind je zwei p-Sylowuntergruppen von G konjugiert.*
4. *Ist $0 \leq k \leq s$, so existiert eine Untergruppe $U_k \leq G$ der Ordnung p^k.*

Ebenfalls sehr wichtig bei der Bestimmung aller Gruppen von vorgegebener Ordnung ist der folgende

Satz 1.20 (Schur-Zassenhaus) *Sei G eine endliche Gruppe und $N \lhd G$ mit $\mathrm{ggT}(|N|, [G : N]) = 1$. Dann existiert ein $U \leq G$ mit $G = NU$ und $N \cap U = 1$, also $G = N \rtimes U$.*

Der Beweis des Satzes benutzt das folgende hilfreiche

Lemma 1.21 (Frattini-Argument) *Ist $N \lhd G$ und P eine p-Sylowuntergruppe von N. Dann gilt $G = N \cdot \mathfrak{N}_G(P)$.*

Im Zusammenhang mit den Sylowsätzen kommen auch die folgenden Definitionen ins Spiel:

Definition 1.22 *Eine Gruppe G* **operiert** *auf einer Menge M vermittels einer Abbildung*

$$\begin{aligned} G \times M &\to M \\ (g, m) &\mapsto gm, \end{aligned}$$

falls $1m = m$ *für alle* $m \in M$ *und* $(gh)m = g(hm)$ *für alle* $g, h \in G$, $m \in M$. *Für ein* $m \in M$ *heißt die Menge*

$$B_m := \{gm : g \in G\} \subset M$$

die **Bahn** *von* m *und die Untergruppe*

$$G_m := \{g \in G | gm = m\} \leq G$$

der **Stabilisator** *von* m. *Außerdem definiert man*

$$M^G := \{m \in M | gm = m \ \forall g \in G\}.$$

Satz 1.23 *Sei* G *eine endliche Gruppe und* M *eine endliche Menge.*

1. *Seien* $m_1, m_2 \in M$. *Dann sind die Bahnen* B_{m_1} *und* B_{m_2} *entweder gleich oder disjunkt. Insbesondere lässt sich eine Teilmenge* $M' \subset M$ *finden, so dass* M *die disjunkte Vereinigung der* $B_{m'}$, $m' \in M'$ *ist:*

$$M = \dot{\bigcup_{m' \in M'}} B_{m'}$$

2. *Es gilt:* $|B_m| = [G : G_m]$.
3. *Ist* G *eine* p*-Gruppe, so gilt* $|M| \equiv |M^G| \bmod p$.

Noch ein paar Resultate über p-Gruppen:

Satz 1.24 *Sei* G *eine* p*-Gruppe. Dann gilt:*

1. *Für* $1 \neq N \lhd G$ *ist* $N \cap Z(G) \neq 1$. *Insbesondere ist* $Z(G) \neq 1$.
2. *Ist* $U \leq G$ *mit* $[G : U] = p$, *so ist* U *sogar normal in* G.
3. *Ist* $|G| = p^2$, *so ist* G *abelsch.*

Ähnlich wie die zweite Aussage des Satzes ist das folgende

Lemma 1.25 *Ist* G *eine endliche Gruppe und* $U \leq G$ *mit* $[G : U] = 2$. *Dann ist* $U \lhd G$.

Definition 1.26 *Eine endliche Gruppe* G *heißt* **nilpotent**, *falls jede Sylowuntergruppe normal in* G *ist. Sie heißt* **auflösbar**, *falls es eine Kette*

$$G = G_0 \geq G_1 \geq \cdots \geq G_r \geq G_{r+1} = 1$$

von Untergruppen $G_i \leq G$ *gibt mit* $G_i' \leq G_{i+1}$ *für* $1 \leq i \leq r$.
G *heißt* **einfach**, *falls* 1 *und* G *die einzigen Normalteiler in* G *sind.*

Satz 1.27 *Sei* G *eine endliche Gruppe,* $U \leq G$ *und* $N \lhd G$. *Dann gilt:*

1. *G nilpotent $\Longrightarrow$ G auflösbar*
2. *G ist nilpotent genau dann, wenn G ein direktes Produkt von p-Gruppen ist.*
3. (a) *G auflösbar $\Longrightarrow$ U und G/N auflösbar*
   (b) *G nilpotent $\Longrightarrow$ U und G/N nilpotent*
   (c) *G auflösbar $\Longleftrightarrow$ N und G/N auflösbar*
4. *G ist auflösbar genau dann, wenn eine Kette*

$$G = G_0 \geq G_1 \geq \cdots \geq G_s \geq G_{s+1} = 1$$

von Untergruppen $G_i \leq G$ existiert mit $G_i \lhd G_{i+1}$ und G_{i+1}/G_i ist zyklisch von Primzahlordnung für $1 \leq i \leq s$.

Satz 1.28 *Sei $n \geq 5$. Dann ist die alternierende Gruppe A_n einfach; insbesondere ist die symmetrische Gruppe S_n nicht auflösbar.*

2 Ringe und Körper

Definition 2.1 *Eine nicht-leere Menge R zusammen mit zwei inneren Verknüpfungen $+$ und $\cdot$ heißt ein (kommutativer)* **Ring**, *falls*

1. *$(R, +)$ ist eine kommutative Gruppe.*
2. $\exists 1 \in R : \ 1 \cdot r = r \ \forall r \in R$ *(“***neutrales Element***”)*
3. $r \cdot s = s \cdot r \ \forall r, s \in R$ *(“***Kommutativität***”)*
4. $r \cdot (s \cdot t) = (r \cdot s) \cdot t \ \forall r, s, t \in R$ *(“***Assoziativität***”)*
5. $r \cdot (s + t) = r \cdot s + r \cdot t \ \forall r, s, t \in R$ *(“***Distributivität***”)*

Das neutrale Element bzgl. $+$ bezeichnen wir mit 0; wir schreiben meistens rs für $r \cdot s$. Sind R und S Ringe mit $R \subset S$ mit den selben $+, \cdot, 0, 1$, so heißt S/R eine **Ringerweiterung**.

Definition 2.2 *Eine nicht-leere Menge K mit zwei inneren Verknüpfungen $+$ und $\cdot$ heißt ein* **Körper**, *falls*

1. *$(K, +, \cdot)$ ist ein kommutativer Ring.*
2. $1 \neq 0$
3. $\forall 0 \neq x \in K \ \exists y \in K : \ x \cdot y = 1$ *(“***inverses Element***”)*

Im Falle $xy = 1$ schreiben wir für y auch x^{-1}. Sind K und L Körper mit $K \subset L$ mit den selben $+, \cdot, 0, 1$, so nennen wir L/K eine **Körpererweiterung**.

Definition 2.3 *Sei K ein Körper. Für $n \in \mathbb{N}$ definiert man*

$$n \cdot 1 := \underbrace{1 + \ldots + 1}_{n \text{ mal}}.$$

Existiert eine kleinste Zahl $p \in \mathbb{N}$ mit $p \cdot 1 = 0$, so nennen wir p die **Charakteristik** *von K. In Zeichen: $p = \mathrm{Char}(K)$. Existiert keine solche Zahl, so setzt man $\mathrm{Char}(K) = 0$.*

Satz 2.4 *Die Charakteristik eines Körpers ist entweder 0 oder eine Primzahl.*

Beispiele:

1. Körper der Charakteristik 0 sind die **rationalen Zahlen** $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ und die komplexen Zahlen $\mathbb{C}$.
2. Jeder Körper ist auch ein Ring.
3. Die Menge der **ganzen Zahlen** $\mathbb{Z}$ bildet einen Ring.
4. Sei $n \in \mathbb{Z}$. Dann ist die Menge $\mathbb{Z}/n\mathbb{Z}$ mit der von $\mathbb{Z}$ vererbten Addition und Multiplikation wieder ein Ring. Ist $n = p$ eine Primzahl, so ist $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ sogar ein Körper mit $\mathrm{Char}(\mathbb{F}_p) = p$.
5. Ist R ein Ring, so bildet die Menge aller **Polynome** $R[x]$ in einer Unbestimmten x mit Koeffizienten in R wieder einen Ring.
6. Seien $n \in \mathbb{N}$ und $R_1, \ldots, R_n$ Ringe. Dann ist $R_1 \times \ldots \times R_n$ mit komponentenweiser Addition und Multiplikation wieder ein Ring, das **äußere direkte Produkt** der R_i.
7. Sei $0, 1 \neq d \in \mathbb{Z}$ quadratfrei. Dann ist die Menge $\mathbb{Q}(\sqrt{d}) = \left\{a + b\sqrt{d} | a, b \in \mathbb{Q}\right\}$ ein Körper. Die Teilmenge $\mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d} | a, b \in \mathbb{Z}\right\}$ bildet einen Ring.

Definition 2.5 *Sei R ein kommutativer Ring.*

1. *Ein Element $0 \neq r \in R$ heißt ein* **Nullteiler**, *falls ein $0 \neq s \in R$ existiert mit $rs = 0$.*
2. *R heißt* **nullteilerfrei**, *falls in R keine Nullteiler existieren. In diesem Fall nennt man R auch einen* **Integritätsring** *oder* **Integritätsbereich**.

Beispiel: Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist genau dann nullteilerfrei, wenn n eine Primzahl ist.

Definition 2.6 *Sei R ein Integritätsring. Dann heißt der kleinste Körper K, der R enthält der* **Quotientenkörper** *von R. Wir schreiben $K = Quot(R)$.*

Definition 2.7 *Sei R ein Ring. Ein Element $r \in R$ heißt eine* **Einheit** *in R, falls ein $s \in R$ existiert mit $rs = 1$. Die Menge aller Einheiten bezeichnen wir mit $R^\times$.*

$R^\times$ ist stets eine Gruppe bzgl. der Multiplikation in R.

Beispiele:

1. $\mathbb{Z}^\times = \{\pm 1\}$.
2. Für einen Körper K gilt $K^\times = K \setminus \{0\}$.
3. $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \bmod n | \mathrm{ggT}(a, n) = 1\}$.

Satz 2.8 *Jeder endliche nullteilerfreie Ring ist ein Körper.*

Definition 2.9 *Eine nicht-leere Teilmenge $\mathfrak{a}$ von einem Ring R heißt ein* **Ideal** *von R, falls*

1. $\forall a, b \in \mathfrak{a} : \ a - b \in \mathfrak{a}$
2. $\forall r \in R, a \in \mathfrak{a} : ra \in \mathfrak{a}$.

In Zeichen: $\mathfrak{a} \lhd R$.

In jedem Ring R existieren die trivialen Ideale $\mathfrak{a} = R$ und $\mathfrak{a} = \{0\}$.

Definition 2.10 (Verknüpfungen von Idealen) *Seien $\mathfrak{a}, \mathfrak{b}$ Ideale in einem Ring R. Dann heißt*

1. $\mathfrak{a} + \mathfrak{b} := \{a + b | a \in \mathfrak{a}, b \in \mathfrak{b}\}$ *die* **Summe**,
2. $\mathfrak{ab} = \{\sum_{i=1}^n a_i b_i | n \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$ *das* **Produkt** *und*
3. $\mathfrak{a} \cap \mathfrak{b} = \{x \in R | x \in \mathfrak{a}, x \in \mathfrak{b}\}$ *der* **Schnitt**

von $\mathfrak{a}$ und $\mathfrak{b}$.

Lemma 2.11 *Seien $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ Ideale eines Ringes R. Dann sind $\mathfrak{a}+\mathfrak{b}$, $\mathfrak{ab}$ und $\mathfrak{a}\cap\mathfrak{b}$ wieder Ideale [1] von R und es gilt:*

$$\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$$

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}.$$

Definition 2.12 *Sei R ein Ring und A eine Teilmenge von R. Dann heißt*

$$(A) := \bigcap_{\substack{\mathfrak{a} \lhd R \\ A \subset \mathfrak{a}}} \mathfrak{a} = \left\{ \sum_{i=1}^n r_i a_i | n \in \mathbb{N}, r_i \in R, a_i \in A \right\}$$

das von A **erzeugte Ideal**. *Ist $A = \{a_1, \ldots, a_n\}$ so schreibt man auch $(a_1, \ldots, a_n)$ anstatt (A).*

[1] Es ist sogar der Schnitt jeder Familie von Idealen wieder ein Ideal.

Definition 2.13 *Sei R ein Ring.*

1. *Ein Ideal $\mathfrak{a} \lhd R$ heißt* **endlich erzeugt**, *falls eine endliche Teilmenge $A \subset R$ existiert mit $\mathfrak{a} = (A)$.*
2. *Ein Ideal $\mathfrak{a} \lhd R$ heißt ein* **Hauptideal**, *falls ein $a \in R$ existiert mit $\mathfrak{a} = (a)$.*
3. *R heißt* **noethersch**, *falls jedes Ideal in R endlich erzeugt ist.*
4. *R heißt ein* **Hauptidealring**, *falls R ein Integritätsring ist und jedes Ideal in R ein Hauptideal ist.*

Beispiele:

1. $\mathbb{Z}$ und $\mathbb{Z}[i]$ sind Hauptidealringe.
2. Für jeden Körper K ist der Polynomring $K[x]$ ein Hauptidealring.
3. Seien $\mathfrak{a} = (a)$ und $\mathfrak{b} = (b)$ Ideale in $\mathbb{Z}$. Dann gilt:
   - $\mathfrak{a} \subset \mathfrak{b} \iff b \mid a$
   - $\mathfrak{a} + \mathfrak{b} = (\mathrm{ggT}(a, b))$
   - $\mathfrak{a}\mathfrak{b} = (ab)$
   - $\mathfrak{a} \cap \mathfrak{b} = (\mathrm{kgV}(a, b))$

Dieses Beispiel motiviert die folgende

Definition 2.14 *Zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ in einem Ring R heißen* **teilerfremd**, *falls $\mathfrak{a} + \mathfrak{b} = R$.*

Lemma 2.15 *Sind $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise teilerfremde Ideale in einem Ring R, so gilt*

$$\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n.$$

Definition 2.16 *Seien R und S Ringe. Eine Abbildung $\phi : R \to S$ heißt ein* **Ringhomomorphismus**, *falls $\phi(x + y) = \phi(x) \dotplus \phi(y)$ für alle $x, y \in R$. Die Menge*

$$\ker(\phi) := \{r \in R | \phi(r) = 0\}$$

ist ein Ideal in R und heißt der **Kern** *von ϕ. Das* **Bild** *von ϕ ist definiert als*

$$\mathrm{im}\,(\phi) := \{s \in S | \exists r \in R : \phi(r) = s\}$$

und ist ein Teilring von S. ϕ heißt ein **Epimorphismus**, *falls* $\mathrm{im}\,(\phi) = S$, *ein* **Monomorphismus**, *falls ϕ injektiv, ein* **Isomorphismus**, *falls ϕ bijektiv ist. Im Falle $R = S$ spricht man von einem* **Endomorphismus**. *Ein bijektiver Endomorphismus heißt* **Automorphismus**.

Lemma 2.17 *Ein Ringhomomorphismus $\phi : R \to S$ ist injektiv genau dann, wenn* $\ker(\phi) = 0$.

Lemma 2.18 *Seien K und L Körper und $\phi : K \to L$ ein Ringhomomorphismus. Dann ist* $\mathrm{im}\,(\phi)$ *entweder* 0 *oder ein Teilkörper von L;* $\ker(\phi)$ *ist entweder* 0 *oder ganz K.*

Definition 2.19 *Sei $\mathfrak{a}$ ein Ideal in einem Ring R. Dann ist*

$$R/\mathfrak{a} := \{\overline{r} | r \in R\}$$

mit der neuen Gleichheit $\overline{r}_1 = \overline{r}_2 \iff r_1 - r_2 \in \mathfrak{a}$ und den Verknüpfungen

$$\overline{r}_1 \dot{+} \overline{r}_2 = \overline{r_1 \dot{+} r_2}$$

wieder ein Ring, der **Restklassenring** *von R modulo $\mathfrak{a}$.*

Satz 2.20 (1. Isomorphiesatz) [2] *Jeder Ringhomomorphismus $\phi : R \to S$ induziert einen Isomorphismus*

$$R/\ker(\phi) \xrightarrow{\simeq} \mathrm{im}\,(\phi), \quad \overline{r} \mapsto \phi(r).$$

Satz 2.21 [3] *Jedes $\mathfrak{a} \lhd R$ induziert einen Epimorphismus $\phi_\mathfrak{a} : R \to \overline{R} = R/\mathfrak{a}$. Es gilt:*

1. *(***2. Isomorphiesatz***) Für einen Teilring S von R ist $S \cap \mathfrak{a}$ ein Ideal in S und $S + \mathfrak{a}$ ein Teilring von R. Es gilt:*

$$S/(S \cap \mathfrak{a}) \simeq (S + \mathfrak{a})/\mathfrak{a}.$$

2. *(***3. Isomorphiesatz***) Ist $\mathfrak{b} \lhd R$ mit $\mathfrak{a} \subset \mathfrak{b}$, dann ist $\overline{\mathfrak{b}} = \mathfrak{b}/\mathfrak{a}$ ein Ideal in $\overline{R}$ und*

$$\overline{R}/\overline{\mathfrak{b}} \simeq R/\mathfrak{b}.$$

3. *Die Ideale $\mathfrak{b} \lhd R$ mit $\mathfrak{a} \subset \mathfrak{b}$ entsprechen eineindeutig den Idealen $\overline{\mathfrak{b}} \lhd \overline{R}$. Dabei ist $\mathfrak{b} = \phi_\mathfrak{a}^{-1}(\overline{\mathfrak{b}})$.*

Satz 2.22 (Chinesischer Restsatz) *Seien R ein Ring und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise teilerfremde Ideale von R. Dann gibt es eine kanonische Isomorphie*

$$R/(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n) \simeq R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n.$$

Den Chinesischen Restsatz kann man zum Lösen simultaner Kongruenzen benutzen. Sind etwa $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremde Ideale, also $\mathfrak{a} + \mathfrak{b} = R$, so können wir $1 = a + b$ mit $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ schreiben. Dann ist $x = r_1 a + r_2 b$ eine Lösung der simultanen Kongruenzen

$$\begin{aligned} x &\equiv r_2 \bmod \mathfrak{a} \\ x &\equiv r_1 \bmod \mathfrak{b}. \end{aligned}$$

[2] vgl. Satz 1.9
[3] vgl. Satz 1.10

Definition 2.23 *Sei R ein Ring. Ein Ideal $\mathfrak{p} \subsetneq R$ heißt*

1. *ein* **Primideal**, *falls für alle $a, b \in R$ mit $ab \in \mathfrak{p}$ gilt, dass $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.*
2. *ein* **maximales Ideal**, *falls es kein Ideal $\mathfrak{a}$ von R gibt mit $\mathfrak{p} \subsetneq \mathfrak{a} \subsetneq R$.*

Lemma 2.24 *Sei R ein Ring und $\mathfrak{a} \subsetneq R$ ein Ideal. Dann gilt:*

1. *$\mathfrak{a}$ ist ein Primideal $\iff$ $R/\mathfrak{a}$ ist ein Integritätsbereich.*
2. *$\mathfrak{a}$ ist ein maximales Ideal $\iff$ $R/\mathfrak{a}$ ist ein Körper.*

Insbesondere ist jedes maximale Ideal auch ein Primideal.

BEISPIEL: In $R = K[x, y]$ mit einem Körper K ist das Hauptideal $\mathfrak{a} = (x)$ prim, aber nicht maximal, da $R/\mathfrak{a} \simeq K[y]$. Das Ideal $\mathfrak{m} = (x, y)$ hingegen ist auch maximal, da $R/\mathfrak{m} \simeq K$.

Satz 2.25 *Sei $\mathfrak{a} \subsetneq R$ ein Ideal in einem Ring R. Dann existiert ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subset \mathfrak{m} \subsetneq R$.*

Dies folgt aus dem folgenden mengentheoretischen Resultat:

Satz 2.26 (Lemma von Zorn) *Jede nicht leere induktiv geordnete Menge besitzt mindestens ein maximales Element.*

Dabei heißt eine (halbgeornete) Menge M **induktiv geordnet** bezüglich einer Relation $\leq$, falls jede **Kette**[4] in M eine obere Schranke in M besitzt.

Definition 2.27 *Sei R ein Ring und $a, b \in R$. Falls ein $c \in R$ existiert mit $b = ca$, so heißt a ein* **Teiler** *von b. Ist c sogar eine Einheit (also $c \in R^\times$), so heißen a und b* **assoziiert**.

Definition 2.28 *Sei R nullteilerfrei und $0 \neq p \in R$ keine Einheit. Dann heißt p*

1. **prim**, *falls für alle $a, b \in R$ gilt, dass $p \mid ab \Longrightarrow p \mid a$ oder $p \mid b$.*
2. **irreduzibel**, *falls für alle $a, b \in R$ gilt, dass $p = ab \Longrightarrow a \in R^\times$ oder $b \in R^\times$.*
3. **reduzibel**, *falls p nicht irreduzibel ist.*

BEMERKUNG: Ein Element $p \in R$ ist genau dann prim, wenn das Hauptideal (p) ein Primideal ist.

Satz 2.29 1. *Sei R nullteilerfrei. Dann gilt: prim $\Longrightarrow$ irreduzibel.*

2. *Sei R ein Hauptidealring. Dann gilt: prim = irreduzibel.*

[4] das ist eine Teilmenge K von M, so dass für alle $a, b \in K$ folgt, dass $a \leq b$ oder $b \leq a$.

Definition 2.30 *Ein Ring R heißt* **faktoriell** *oder ein* **ZPE-Ring**[5]*, falls jedes $0 \neq r \in R$, $r \notin R^\times$ bis auf Assoziiertheit eindeutig als endliches Produkt von irreduziblen Faktoren p_i darstellbar ist: $r = p_1 \cdot \ldots \cdot p_n$.*

Beispiele: Aus den beiden folgenden Sätzen ergibt sich:

1. $\mathbb{Z}$ und $\mathbb{Z}[i]$ sind faktoriell.
2. Die Polynomringe $K[x_1, \ldots, x_n]$ über einem Körper K (oder allgemeiner über einem faktoriellen Ring R) sind faktoriell.

Satz 2.31 *Jeder Hauptidealring ist faktoriell.*

Satz 2.32 *Ist R faktoriell, so auch der Polynomring $R[x]$.*

Definition 2.33 *Sei R faktoriell und $0 \neq f = \sum_{i=0}^{n} r_i x^i \in R[x]$. Dann heißt*

$$I(f) := \mathrm{ggT}(r_1, \ldots, r_n)$$

der **Inhalt** *von f. Im Fall $I(f) = 1$ nennt man f* **primitiv**.

Lemma 2.34 (Lemma von Gauss) *Sei R faktoriell und seien $f, g \in R[x] \setminus \{0\}$ primitiv. Dann ist auch fg primitiv.*

Satz 2.35 *Sei R ein faktorieller Ring mit Quotientenkörper K, sowie $f \in R[x]$ ein Polynom von Grad ≥ 1. Dann gilt: f irreduzibel in $R[x] \Longrightarrow f$ irreduzibel in $K[x]$.*

Satz 2.36 (Eisenstein) *Sei R faktoriell mit Quotientenkörper K und $f = \sum_{i=0}^{n} r_i x^i \in R[x]$ ein primitives Polynom von Grad n. Es gebe ein Primelement $p \in R$ mit $p \nmid r_n$, $p \mid r_0, \ldots p \mid r_{n-1}$ und $p^2 \nmid r_0$. Dann ist f irreduzibel in $R[x]$, also wegen Satz 2.35 auch irreduzibel in $K[x]$.*

Bemerkung: Häufig ist $r_n = 1$, und f somit automatisch primitiv.

In diesem Zusammenhang drei weitere Irreduzibilitätskriterien:

Satz 2.37 *Sei R faktoriell, $\mathfrak{p} \lhd R$ ein Primideal und $\overline{R} = R/\mathfrak{p}$. Dann definiert*

$$\begin{array}{rcl} R[x] & \longrightarrow & \overline{R}[x] \\ f = \sum_{i=0}^{n} r_i x^i & \mapsto & \overline{f} = \sum_{i=0}^{n} \overline{r_i} x^i \end{array}$$

einen Ringepimorphismus und es gilt: $\overline{f}$ irreduzibel in $\overline{R}[x] \Longrightarrow f$ irreduzibel in $R[x]$.

Satz 2.38 (Artin-Schreier) *Sei K ein Körper der Charakteristik $p \neq 0$. Dann ist $f(x) = x^p - x + a \in K[x]$ entweder irreduzibel oder zerfällt in $K[x]$.*

[5] ZPE = eindeutige Primfaktorzerlegung

Satz 2.39 *Sei $f \in \mathbb{Z}[x]$ und $n \in \mathbb{Z}$. Dann ist f irreduzibel genau dann, wenn $f(x+n)$ irreduzibel ist.*

Damit beweist man z.B. auch den

Satz 2.40 *Sei p eine Primzahl. Dann ist das* **Kreisteilungspolynom**

$$f_{(p)}(x) = \sum_{i=0}^{p-1} x^i$$

irreduzibel in $\mathbb{Z}[x]$, also auch in $\mathbb{Q}[x]$.

Definition 2.41 *Ein nullteilerfreier Ring R zusammen mit einer Abbildung*

$$d : R \setminus \{0\} \to \mathbb{N}_0$$

heißt ein **euklidischer Ring**, *falls es für alle $a, b \in R \setminus \{0\}$ Elemente $v, r \in R$ gibt mit*

1. $a = vb + r$
2. $r \neq 0 \Longrightarrow d(r) < d(b)$.

Beipiele:

1. $R = \mathbb{Z}$ mit $d(x) = |x|$.
2. $R = \mathbb{Z}[i]$ und $R = \mathbb{Z}[\sqrt{2}]$ mit $d(x) = |x|$, dem komplexen Betrag.
3. $R = K[x]$ über einem Körper K mit $d(f) =$ Grad von f.

Satz 2.42 *Jeder euklidische Ring ist ein Hauptidealring.*

In einem euklidischen Ring R lässt sich der ggT zweier Zahlen $a_1, a_2 \in R$ mit $d(a_1) > d(a_2)$ durch sukzessives Dividieren mit Rest (**Euklidischer Algorithmus**) berechnen:

$$\begin{aligned}
a_1 &= v_1 a_2 + r_1 && \text{mit} && d(r_1) < d(a_2) \\
a_2 &= v_2 r_1 + r_2 && \text{mit} && d(r_2) < d(r_1) \\
r_1 &= v_3 r_2 + r_3 && \text{mit} && d(r_3) < d(r_2) \\
&\vdots \\
r_{n-2} &= v_n r_{n-1} + r_n && \text{mit} && d(r_n) < d(r_{n-1}) \\
r_{n-1} &= v_{n+1} r_n && \text{und} && r_{n+1} = 0
\end{aligned}$$

Dann ist $r_n = \mathrm{ggT}(a_1, a_2)$. Indem man die Gleichungen rückwärts liest, kann man so auch eine Darstellung $r_n = s \cdot a_1 + t \cdot a_2$ mit $s, t \in R$ berechnen.

Definition 2.43 *Sei R ein Ring. Eine abelsche Gruppe M heißt ein R-***Modul***, falls es eine Funktion*

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

gibt, so dass

$$1m = m,\ (r_1 + r_2)m = r_1 m + r_2 m,$$

$$(r_1 r_2)m = r_1(r_2 m),\ r(m_1 + m_2) = rm_1 + rm_2$$

für alle $m, m_1, m_2 \in M$ und $r, r_1, r_2 \in R$.

Der Begriff des Moduls verallgemeinert also den des Vektorraums.
BEISPIELE:

1. Jede abelsche Gruppe A ist ein $\mathbb{Z}$-Modul via $(z, a) \mapsto a^z$.
2. Jeder Ring R ist ein Modul über sich selbst via $(r_1, r_2) \mapsto r_1 \cdot r_2$.
3. Die direkte Summe von n Kopien von R, nämlich $R^n = R \oplus \ldots \oplus R$ ist ein R-Modul via $(r, (r_1, \ldots, r_n)) \mapsto (r \cdot r_1, \ldots, r \cdot r_n)$, der **freie** R-Modul von Rang n.
4. Jedes Ideal $\mathfrak{a}$ in einem Ring R ist ein R-Modul via $(r, a) \mapsto r \cdot a$.

Definition 2.44 *Sei $p \in \mathbb{Z}$ eine Primzahl. Für $z \in \mathbb{Z}$ definiere*

$$\left(\frac{z}{p}\right) = \begin{cases} 0, & p \mid z \\ 1, & z \bmod p \text{ ist ein Quadrat in } \mathbb{F}_p \\ -1, & z \bmod p \text{ ist kein Quadrat in } \mathbb{F}_p \end{cases}$$

Satz 2.45 (Quadratisches Reziprozitätsgesetz) *Seien p und q Primzahlen und $z, z_1, z_2 \in \mathbb{Z}$. Dann gilt:*

1. $z_1 \equiv z_2 \bmod p \Longrightarrow \left(\frac{z_1}{p}\right) = \left(\frac{z_2}{p}\right)$.
2. $\left(\frac{z_1 z_2}{p}\right) = \left(\frac{z_1}{p}\right)\left(\frac{z_2}{p}\right)$.
3. $\left(\frac{z}{p}\right) \equiv z^{\frac{p-1}{2}} \bmod p$.
4. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \bmod 4 \\ -1, & p \equiv 3 \bmod 4 \end{cases}$.
5. $\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0$.
6. $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, *falls* $p \equiv 1 \bmod 4$ *oder* $q \equiv 1 \bmod 4$.
7. $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$, *falls* $p \equiv q \equiv 3 \bmod 4$.

8. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Definition 2.46 *Sei K ein Körper. Dann ist der Schnitt aller Körper $k \subset K$ wieder ein Körper, der* **Primkörper** *von K. Er ist der kleinste in K gelegene Körper.*

Satz 2.47 *Sei K ein Körper.*

1. *Ist $\mathrm{Char}(K) = 0$, so ist der Primkörper von K isomorph zu den rationalen Zahlen $\mathbb{Q}$.*
2. *Ist $\mathrm{Char}(K) = p > 0$, so ist der Primkörper von K isomorph zu $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

Definition 2.48 *Sei L/K eine Körpererweiterung. Dann heißt*

$$[L : K] := \dim_K(L)$$

der **Grad** *der Körpererweiterung.*

Lemma 2.49 *Seien $K \subset L \subset F$ Körper. Dann gilt:*

$$[F : K] = [F : L] \cdot [L : K].$$

Satz 2.50 *Sei K ein endlicher Körper der Charakteristik p. Dann besteht K aus genau $|K| = p^n$ Elementen, wobei n der Grad von K über seinem Primkörper ist.*

Definition 2.51 *Sei L/K eine Körpererweiterung und A eine Teilmenge von L. Dann bezeichnen wir den Schnitt über alle Teilkörper von L, die K und A enthalten, mit $K(A)$. $K(A)$ ist wieder ein Körper und heißt die* **Körperadjunktion** *von A zu K. Ist $A = \{a_1, \ldots, a_n\}$ endlich, schreiben wir auch $K(A) = K(a_1, \ldots, a_n)$.*

Definition 2.52 *Sei K ein Körper. Ein Element a in einem Erweiterungskörper von K heißt* **algebraisch** *über K, falls $[K(a) : K]$ endlich ist. Ansonsten heißt a* **transzendent**.

Definition 2.53 *Sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Dann heißt das normierte Polynom $f_a(x) \in K[x]$ kleinsten Grades mit Nullstelle a das* **Minimalpolynom** *von a.*

Lemma 2.54 *Ist a algebraisch über K, so ist $f_a(x)$ irreduzibel und es gilt $K(a) \simeq K[x]/f_a(x)$. Insbesondere ist $[K(a) : K] = \deg(f_a)$.*

Definition 2.55 *Sei K ein Körper.*

1. *Ein Polynom $f(x) \in K[x]$ heißt* **separabel**, *falls f keine mehrfache Nullstelle in einer Erweiterung L/K besitzt.*
2. *Ein Element a heißt* **separabel** *über K, falls a algebraisch über K mit separablem Minimalpolynom $f_a(x) \in K[x]$ ist.*

3. *Eine Körpererweiterung L/K heißt algebraisch (separabel), falls jedes Element $a \in L$ algebraisch (separabel) über K ist.*

BEISPIELE:

1. Sei ζ_n eine primitive n-te Einheitswurzel. So ist die Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ algebraisch und separabel. Ist p eine Primzahl, so ist

$$f_{\zeta_p}(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Z}[x]$$

das Minimalpolynom von ζ_p über $\mathbb{Q}$. Allgemeiner ist

$$f_{\zeta_n}(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \neq n}} f_{\zeta_d}(x)} \in \mathbb{Z}[x].$$

Es ist $\deg(f_{\zeta_n}) = \phi(n)$.

2. Sei $L = k(x) := Quot(k[x])$ der **rationale Funktionenkörper** in einer Unbestimmten über k. Ist $\mathrm{Char}(k) = 2$ und $K = k(x^2)$, dann ist die Erweiterung L/K algebraisch, aber nicht separabel, da $f_x(T) = T^2 - x^2 = (T - x)^2$.

Definition 2.56 *Sei K ein Körper und $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$. Dann heißt $f'(x) := \sum_{i=1}^{n} i a_i x^{i-1}$ die* **formale Ableitung** *von f.*

Satz 2.57 *Sei K ein Körper und $f(x) \in K[x]$.*

1. *f ist genau dann separabel, falls $\mathrm{ggT}(f, f') = 1$.*
2. *Ist $f(x)$ irreduzibel in $K[x]$ und $\mathrm{Char}(K) = 0$ oder $|K| < \infty$, so ist f separabel.*

Satz 2.58 *Seien $K \subset L \subset F$ Körper. Dann gilt:*

1. *F/K ist genau dann algebraisch (separabel), wenn F/L und L/K algebraisch (separabel) sind.*
2. *Summen, Produkte, Differenzen und Quotienten über K algebraischer (separabler) Elemente sind wieder algebraisch (separabel).*

Satz 2.59 *Sei L/K eine endliche algebraische Körpererweiterung. Dann existiert ein $a \in L$ mit $L = K(a)$. Jedes solche a heißt ein* **primitives Element**.

Satz 2.60 *Sei L/K eine Köpererweiterung. Dann existiert genau dann ein über K algebraisches $a \in L$ mit $L = K(a)$, wenn die Erweiterung L/K nur endlich viele Zwischenkörper besitzt.*

Definition 2.61 *Ein Körper K heißt* **algebraisch abgeschlossen**, *falls jedes Polynom $f(x) \in K[x]$ vollständig in $K[x]$ zerfällt.*

Satz 2.62 *$\mathbb{C}$ ist algebraisch abgeschlossen.*

Satz 2.63 *Zu jedem Körper K existiert ein bis auf K-Isomorphie eindeutig bestimmter Erweiterungskörper K^c mit:*

1. *K^c/K ist algebraisch.*
2. *K^c ist algebraisch abgeschlossen.*

K^c heißt der **algebraische Abschluss** *von K.*

Satz 2.64 *Ein Punkt $a \in \mathbb{C}$ ist genau dann mit Zirkel und Lineal (aus den rationalen Zahlen) konstruierbar, wenn es einen Körperturm $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$ mit $a \in K_n$ und $[K_i : K_{i-1}] = 2$ für $i = 1, \ldots n$ gibt.*

Dabei verwendet man das folgende

Lemma 2.65 *Sei L/K eine Körpererweiterung von Grad 2 und $\mathrm{Char}(K) \neq 2$. Dann existiert ein $\alpha \in K$ mit $L = K(\sqrt{\alpha})$.*

Beispiel: Ein regelmäßiges n-Eck ist genau dann konstruierbar, wenn

$$n = 2^k p_1 \cdot \ldots \cdot p_r$$

mit paarweise verschiedenen Primzahlen p_i der Form $p_i = 2^{m_i} + 1$ ist. Solche p_i heißen **Fermatsche Primzahlen**.

Satz 2.66 *Sei K ein Körper und $f(x) \in K[x]$ nicht konstant. Dann existiert ein Erweiterungskörper L von K mit $[L : K] \leq \deg(f)$, so dass f in L eine Nullstelle besitzt. Ist f irreduzibel, so ist $[L : K] = \deg(f)$.*

Definition 2.67 *Sei K ein Körper und $f(x) \in K[x]$ nicht konstant. Ein Erweiterungskörper L von K heißt ein* **Zerfällungskörper** *von f, falls f über L in Linearfaktoren zerfällt:*

$$f(x) = c \prod_{i=1}^{\deg(f)} (x - a_i),\ a_i \in L$$

Satz 2.68 *Sei K ein Körper und $f(x) \in K[x]$ nicht konstant. Dann existiert ein Zerfällungskörper von f.*

Sei nun L/K eine endliche Körpererweiterung. Dann gibt es $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$. Sei F ein Körper der alle a_i und auch alle anderen Nullstellen der Minimalpolynome f_{a_i} enthalte.

Definition 2.69 *Die Menge*

$$I(L/K) := \{\sigma | \sigma : L \to F \text{ injektiv und } \sigma(x) = x\ \forall x \in K\}$$

heißt die **Isomorphismenmenge** *von L/K.*

ACHTUNG: Genau genommen besteht die Isomorphismenmenge also nur aus Monomorphismen.

Satz 2.70 *Sei L/K eine Körpererweiterung.*

1. *$I(L/K)$ hängt nicht von F ab.*
2. *$|I(L/K)| \leq [L:K]$.*
3. *$|I(L/K)| = [L:K] \iff L/K$ separabel.*
4. *Sei L_1 ein Zwischenkörper der Erweiterung L/K. Dann lässt sich jedes $\sigma_1 \in I(L_1/K)$ zu einem $\sigma \in I(L/K)$ fortsetzen.*

Lemma 2.71 (Artin) *Die $\sigma \in I(L/K)$ sind linear unabhängig über F.*

Ein Nachtrag zu Satz 2.59: Sei L/K endlich separabel. Dann ist $L = K(\lambda)$ genau dann, wenn $\sigma(\lambda) \neq \lambda$ für alle $1 \neq \sigma \in I(L/K)$.

3 Galoistheorie

Definition 3.1 *Eine endliche Körpererweiterung L/K heißt*

1. **normal**, *falls $\sigma(L) \subset L$ für alle $\sigma \in I(L/K)$.*
2. **galoissch**, *falls L/K separabel und normal ist.*

Satz 3.2 (Hauptsatz der Galoistheorie) *Sei L/K eine endliche galoissche Erweiterung. Dann ist $G = G(L/K) := I(L/K)$ eine Gruppe, und die Zwischenkörper der Erweiterung entsprechen eins zu eins den Untergruppen von G.*
Dabei gehört zu einem Zwischenkörper Z die Untergruppe $U = \{\sigma \in G | \sigma(z) = z \ \forall z \in Z\}$. Umgekehrt gehört zu einer Untergruppe U der Zwischenkörper $L^U := \{z \in L | \sigma(z) = z \ \forall \sigma \in U\}$. Die Erweiterung L/L^U ist wieder galoissch mit Gruppe U.

Satz 3.3 *Sei L/K eine endliche galoissche Erweiterung mit Gruppe G und Z ein Zwischenkörper mit zugehöriger Untergruppe U, also $\mathrm{Gal}(L/Z) = U$. Dann ist die Erweiterung Z/K genau dann galoissch, wenn U normal in G ist. In diesem Fall ist $\mathrm{Gal}(Z/K) = G/U$.*

Satz 3.4 *Sei L/K eine endliche galoissche Erweiterung mit Gruppe G und Z_1 und Z_2 Zwischenkörper mit den zugehörigen Untergruppen U_1 und U_2.*

1. *Zu der Untergruppe $U_1 \cap U_2$ gehört der Zwischenkörper $Z_1 Z_2$, dem kleinsten Körper, der Z_1 und Z_2 enthält.*
2. *Zum Zwischenkörper $Z_1 \cap Z_2$ gehört die Untergruppe $\bigcap_{U \leq G, U_1, U_2 \subset U} U$, der kleinsten Untergruppe von G, die U_1 und U_2 enthält.*

Satz 3.5 (Translationssatz) *Seien L_1/K und L_2/K endliche Körpererweiterungen. Dann gilt:*

1. *Ist L_1/K galoissch, so auch L_1L_2/L_2 und $G(L_1L_2/L_2) \simeq G(L_1/K)$.*
2. *Sind L_1/K und L_2/K galoissch, so auch L_1L_2/K und $G(L_1L_2/K)$ ist isomorph zu einer Untergruppe von $G(L_1/K) \times G(L_2/K)$. Ist zusätzlich $L_1 \cap L_2 = K$, so gilt $G(L_1L_2/K) \simeq G(L_1/K) \times G(L_2/K)$.*

Galoissche Erweiterungen können so klassifiziert werden:

Satz 3.6 *Sei L/K eine endliche Erweiterung. Dann ist L/K genau dann galoissch, wenn L der Zerfällungskörper[6] eines separablen Polynoms $f(x) \in K[x]$ ist.*

Satz 3.7 (Satz von der Normalbasis) *Sei L/K galoissch mit Gruppe G. Dann existiert ein $\lambda \in L$, so dass die $\sigma(\lambda)$, $\sigma \in G$ eine K-Basis von L bilden.*

Beispiele:

1. Sei $0, 1 \neq d \in \mathbb{Z}$ quadratfrei. Dann ist die Erweiterung $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ galoissch von Grad 2 mit Gruppe $G = \langle\sigma\rangle$, wobei $\sigma(\sqrt{d}) = -\sqrt{d}$. Dann ist eine geeignete Wahl von λ etwa $\lambda = 1 + \sqrt{d}$. Die Wahl $\lambda = \sqrt{d}$ führt jedoch zu keiner Normalbasis, da $\sqrt{d}$ und $-\sqrt{d}$ linear abhängig über $\mathbb{Q}$ sind.
2. Die Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ist galoissch mit Gruppe $G \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. Gehört $\sigma_a \in G$ zu $a \bmod n$, dann gilt $\sigma_a(\zeta_n) = \zeta_n^a$. Ist $n = p$ eine Primzahl, so erzeugt $\lambda = \zeta_p$ eine Normalbasis.

Etwas allgemeiner als das letzte Beispiel gilt:

Satz 3.8 *Ist $L = K(\zeta_n)$, so ist L/K galoissch, wobei die Galoisgruppe isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ ist.*

Satz 3.9 *1. Sei K ein endlicher Körper der Charakteristik p, $q = |K| = p^n$ und L/K eine endliche Erweiterung. Dann gilt:*

   (a) K ist der Zerfällungskörper des Polynoms $x^q - x$ über $\mathbb{F}_p$.
   (b) $K^\times$ ist zyklisch.
   (c) $L = K(a)$ für ein geeignetes primitives Element $a \in L$.
   (d) L/K ist galoissch mit zyklischer Gruppe $G(L/K) = \langle\phi\rangle$.
   (e) $\phi(\lambda) = \lambda^q$ für alle $\lambda \in L$. ϕ heißt der **Frobeniusautomorphismus**.

2. Sind K_1 und K_2 zwei endliche Körper der Charakteristik p und $|K_i| = p^{n_i}$, $i = 1, 2$, so gilt:

$$K_1 \subset K_2 \iff n_1 \mid n_2.$$

[6] Mit *dem* Zerfällungskörper meint man immer den kleinsten Zerfällungskörper, der aus K durch Adjunktion aller Wurzeln von f entsteht.

3. *Zu jedem $n \in \mathbb{N}$ gibt es ein irreduzibles Polynom $f(x) \in \mathbb{F}_p[x]$ von Grad n. Insbesondere gibt es zu jeder Primzahlpotenz $q = p^n$ genau einen endlichen Körper $K = \mathbb{F}_q$ mit q Elementen.*

Der zweite Punkt von (1) ist hierbei ein Spezialfall des folgenden Satzes:

Satz 3.10 *Ist K ein Körper und G eine endliche Untergruppe von $K^\times$. Dann ist G zyklisch.*

Satz 3.11 *Sei K ein Körper der Charakteristik 0 mit $\zeta_n \in K$ und L/K eine galoissche Erweiterung. Dann ist L/K genau dann zyklisch von Grad $d \mid n$, wenn $L = K(\sqrt[d]{a})$ für ein $a \in K$.*

Definition 3.12 *Sei K ein Körper, $f(x) \in K[x]$ ein separables Polynom und L_f der Zerfällungskörper von f.*

1. *f heißt* **auflösbar**, *wenn die Galoisgruppe $G_f := G(L_f/K)$ auflösbar ist.*

2. *Über L_f zerfällt f in Linearfaktoren, $f(x) = \prod_{i=1}^{\deg(f)}(x - \omega_i)$. Dann heißt*

$$d_f := \prod_{i<j}(\omega_i - \omega_j)^2 \in K$$

die **Diskriminante** *von f.*

Mit Satz 1.28 folgt

Satz 3.13 *Polynome von Grad ≥ 5 sind im Allgemeinen nicht auflösbar.*

Satz 3.14 *Sei K ein Körper, $f(x) \in K[x]$ ein separables Polynom und L_f der Zerfällungskörper von f. Dann ist die Galoisgruppe G_f stets eine Untergruppe der symmetrischen Gruppe S_n. Weiter gilt*

$$G_f \leq A_n \iff \sqrt{d_f} \in K.$$

BEMERKUNG: Sei $f(x) = x^3 + a_2x^2 + a_1x + a_0 \in K[x]$. Die Substitution

$$x \mapsto x - \frac{1}{3}a_2$$

ändert die Diskriminante von f nicht und lässt den Koeffizienten bei x^2 verschwinden:

$$\tilde{f}(x) = x^3 + px + q.$$

Dann ist $d_f = d_{\tilde{f}} = -4p^3 - 27q^2$; man kann nun direkt überprüfen, ob $\sqrt{d_f} \in K$.

Das folgende Hilfsmittel führt bei der Bestimmung von G_f in Verbindung mit Satz 1.11 (12) häufig zum Ziel.

Satz 3.15 *Sei* $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ *separabel und* p *eine Primzahl. Ist auch* $\overline{f}(x) = \sum_{i=0}^{n} \overline{a_i} x^i \in \mathbb{F}_p[x]$ *separabel, so ist* $G_{\overline{f}} \leq G_f$.

Noch genauer ist der

Satz 3.16 *Mit den Voraussetzungen und Bezeichnung aus Satz 3.15 sei*

$$\overline{f} = \overline{f}_1 \cdot \ldots \cdot \overline{f}_k$$

die Zerlegung von $\overline{f}$ *in irreduzible Faktoren. Dann enthält* G_f *ein Produkt* $\sigma_1 \cdot \ldots \cdot \sigma_k$ *von paarweise disjunkten Zykeln der Längen* $\deg(\overline{f}_i)$, $i = 1, \ldots, k$.