Protokoll zur Vorlesung Algebra WS 18/19

W. Bley

7. Februar 2019

1 Gruppentheorie

1.1 Grundlegende Definitionen

Definition 1.1.1 Eine Halbgruppe ist eine nicht-leere Menge G zusammen mit einer binären Operation $G \times G \to G, (a, b) \mapsto ab$, so daß gilt:

$$(i) \qquad a(bc) = (ab)c, \forall a, b, c \in G \quad \text{(Assoziativität)}$$

Ein Monoid ist eine Halbgruppe G, die ein Element e enthält, so daß gilt:

$$(ii) \qquad ae = ea = a, \forall a \in G \quad \text{(Existenz der Identität)}$$

Eine Gruppe ist ein Monoid G, so daß es zu jedem $a \in G$ ein Inverses $a^{-1} \in G$ gibt mit

$$(iii) \qquad aa^{-1} = a^{-1}a = e.$$

Eine Halbgruppe heißt abelsch oder kommutativ, falls für all $a, b \in G$ gilt: $ab = ba$.

Wichtige Beispiele:
1) Die Diedergruppe $D_4 = \{\sigma^i\tau^j \mid 0 \leq i \leq 3, 0 \leq j \leq 1, \tau\sigma = \sigma^3\tau\}$. Dies ist die Gruppe der Symmetrien eines regelmäßigen Vierecks. σ kann man sich als die Drehung um 90 Grad vorstellen; τ ist etwa die Spiegelung an der x-Achse.
2) Die symmetrischen Gruppen S_n der Permutationen von n Symbolen. Es gilt: $|S_n| = n!$.

An dieser Stelle sei an die Definition einer Äquivalenzrelation erinnert. Konsultieren Sie dazu zum Beispiel das Buch von S. Bosch, Lineare Algebra, Kapitel 2.2.

Satz 1.1.2 *Sei $\sim$ eine Äquivalenzrelation auf dem Monoid G, so daß für alle $a, b, c, d \in G$ gilt: $a \sim b, c \sim d \implies ac \sim bd$. Dann ist die Menge $\bar{G} := G/\sim$ der Äquivalenzklassen ein Monoid unter der binären Operation $\bar{a}\bar{b} := \overline{ab}$, wobei für $a \in G$ die Äquivalenzklasse $\{b \in G \mid a \sim b\}$ mit $\bar{a}$ bezeichnet wird.*
Falls G eine Gruppe ist, so auch $\bar{G}$. Ebenso vererbt sich die Eigenschaft abelsch.

Wichtiges Beispiel: Sei $G = \mathbb{Z}$ bezüglich $+$ oder $\cdot$ und m eine natürliche Zahl. Dann definiert man: $a \sim b :\iff m \mid a - b$. Wir schreiben dafür: $a \equiv b (\text{mod } m)$ und $\mathbb{Z}/m\mathbb{Z} := \bar{G}$. Bezüglich $+$ ist $\mathbb{Z}/m\mathbb{Z}$ eine abelsche Gruppe, bezüglich $\cdot$ ein Monoid.

Definition 1.1.3 Sei G eine Gruppe und $n \in \mathbb{Z}$. Dann setzt man:

$$a^n := \begin{cases} a \cdots a \quad (n \text{ Faktoren}), & \text{if } n > 0, \\ a^{-1} \cdots a^{-1} \quad (-n \text{ Faktoren}), & \text{if } n < 0, \\ e, & \text{if } n = 0. \end{cases}$$

Es gelten dann die üblichen Rechenregeln:

$$a^m b^n = a^{m+n}, \quad (a^n)^m = a^{mn}, \quad a \in G, m, n \in \mathbb{Z}.$$

1.2 Homomorphismen und Untergruppen

Definition 1.2.1 Seien G, H Gruppen. Eine Abbildung $f : G \to H$ heißt Homomorphismus (von Gruppen), falls für alle $a, b \in G$ gilt $f(ab) = f(a)f(b)$. Man benützt die üblichen, aus der linearen Algebra bekannten Bezeichnungen Monomorphismus, Epimorphismus und Isomorphismus.

Bemerkungen
1) Das Kompositum von zwei (oder mehreren) Homomorphismen ist stets wieder ein Homomorphismus.
2) Es gilt: $f(e_G) = e_H$ und $f(a^{-1}) = f(a)^{-1}, \forall a \in G$.

Definition 1.2.2 Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann heißt

$$\ker(f) := \{g \in G \mid f(g) = e_H\}$$

der Kern von f, $f(G)$ heißt das Bild von f und $f^{-1}(B)$ das Urbild der Teilmenge $B \subseteq H$ unter f.

Kern und Bild sind stets wieder Gruppen. Falls $B \subseteq H$ eine Untergruppe von H ist, so ist das Urbild eine Untergruppe von G.

Satz 1.2.3 *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:*
(i) f ist ein Monomorphismus $\iff \ker(f) = \{e_G\}$.
(ii) f ist ein Isomorphismus $\iff \exists$Homomorphismus $f^{-1} : H \to G$ mit $f \circ f^{-1} = id_H, f^{-1} \circ f = id_G$.

Definition 1.2.4 Sei H eine nicht-leere Teilmenge der Gruppe G, die abgeschlossen unter der Gruppenoperation ist. Fall H selbst eine Gruppe ist, so heißt H Untergruppe von G (in Zeichen: $H \leq G$).

Bemerkung: $\{e\}$ bezeichnen wir als die triviale Untergruppe. Für ein Homomorphismus $f : G \to H$ ist $\ker(f)$ stets eine Untergruppe von G.

Satz 1.2.5 *Sei H eine nicht-leere Teilmenge einer Gruppe G. Dann gilt:*

$$H \leq G \iff ab^{-1} \in H, \forall a, b \in H.$$

1.3 Zyklische Untergruppen

Definition 1.3.1 a) Sei G eine Gruppe und $a \in G$. Dann heißt $< a >:= \{a^k \mid k \in \mathbb{Z}\}$ die von a erzeugte zyklische Untergruppe von G. Die Zahl $\text{ord}(a) := | < a > |$ heißt die Ordnung von a.
b) Die Gruppe G heißt zyklisch, falls es ein $a \in G$ gibt, so dass $G =< a >$ gilt.

Satz 1.3.2 *Sei G eine Gruppe und $a \in G$. Falls a unendliche Ordnung hat, so gilt:*

(i) $a^k = e \iff k = 0$.

(ii) $a^k = a^l \iff k = l$.

Falls a endliche Ordnung $m \in \mathbb{N}$ hat, so gilt:

(iii) *m ist die kleinste positive ganze Zahl mit $a^m = e$.*

(iv) $a^k = e \iff m \mid k$.

(v) $a^k = a^l \iff k \equiv l (\text{mod } m)$.

(vi) $< a >= \{a^0, a^1, \ldots, a^{m-1}\}$.

(vii) $ord(a^k) = m/k$, *falls* $k \mid m$.

Folgerung 1.3.3 *Jede unendliche zyklische Gruppe ist isomorph zu* $\mathbb{Z}$. *Jede endliche zyklische Gruppe der Ordnung* m *ist isomorph zu* $\mathbb{Z}/m\mathbb{Z}$.

Satz 1.3.4 *Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Genauer: Ist* H *Untergruppe von* $G =< a >$, *so gilt:*

$$H =< a^k > \text{ mit } k := \min\{s \in \mathbb{N} \mid a^s \in H\}.$$

Satz 1.3.5 *Sei* $G =< a >$ *eine zyklische Gruppe. Falls* $ord(a) = \infty$, *so sind* a *und* $-a$ *die einzigen Erzeuger von* G. *Falls* $ord(a) = m < \infty$, *so gilt:*

$$< a >=< a^k > \iff \text{ggT}(m, k) = 1.$$

Genauer gilt: $ord(a^k) = m/\text{ggT}(k, m)$.

1.4 Nebenklassen und Untergruppen

Definition 1.4.1 Sei H eine Untergruppe von G und $a, b \in G$. Dann heißt a (rechts-)kongruent zu b, in Zeichen $a \equiv_r b (\text{mod } H)$, falls $ab^{-1} \in H$.

Bemerkung: Für $G = \mathbb{Z}, H = m\mathbb{Z}$ ist dies die bereits bekannte Kongruenz.

Satz 1.4.2 *(i)* $\equiv_r$ *ist eine Äquivalenzrelation auf* G.
(ii) Die Äquivalenzklasse von $a \in G$ *ist gerade die sogenannte Rechtsnebenklasse*

$$Ha = \{ha \mid h \in H\}.$$

(iii) Alle Nebenklassen haben diesselbe Kardinalität, nämlich $|H|$.

Definition 1.4.3 Sei $H \leq G$. Dann heißt die Anzahl der Rechtsnebenklassen der Index von H in G. In Zeichen: $[G : H]$.

Bemerkung: Sei $H \leq G$. Dann schreibt man $H \setminus G$ für die Menge der Rechtsnebenklassen. Völlig analog definiert man G/H für die Menge der Linksnebenklassen. Hier liegt dann die Definition

$$a \equiv_l b (\text{mod } H) : \iff a^{-1}b \in H$$

zugrunde. Es gilt: Die Anzahl der Linksnebenklassen ist gleich der Anzahl der Rechtsnebenklassen. Der Index kann also auch als die Anzahl der Linksnebenklassen definiert werden

Satz 1.4.4 *Seien* $K \leq H \leq G$ *Gruppen. Dann verhält sich der Index multiplikativ, d.h.* $[G : K] = [G : H][H : K]$. *Falls zwei dieser Indizes endlich sind, so auch der dritte.*

Satz 1.4.5 *(Lagrange) Falls* $H \leq G$, *so gilt:* $|G| = [G : H]|H|$. *Falls also* $|G| < \infty$, *so teilt* $|H|$ *stets* $|G|$.

Folgerung 1.4.6 *Sei* G *eine Gruppe der Ordnung* $m < \infty$. *Dann gilt für alle* $a \in G$:

$$ord(a) \mid m \text{ und } a^m = e.$$

Satz 1.4.7 *Seien* H, K *endliche Untergruppen eine Gruppe* G. *Dann gilt:*

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Hierbei ist $HK := \{ab \mid a \in H, b \in K\}$.

Achtung: HK ist im allgemeinen keine Gruppe.

In diesem Abschnitt wurde großer Wert darauf gelegt, zu zeigen, daß im Allgemeinen

- Rechtsnebenklassen nicht mit Linksnebenklassen übereinstimmen.
- die natürlich definierte binäre Struktur auf der Menge der Rechtsnebenklassen (bzw. Linksnebenklassen) nicht wohldefiniert ist.

Dies führt uns zum Studium von Untergruppen mit einer zusätzlichen Eigenschaft, den sogenannten Normalteilern, wo dann obige "Defizite" nicht mehr auftreten.

1.5 Normale Untergruppen und Quotienten

ZIEL: Studium derjenigen Untergruppen $N \leq G$ für die gilt: $aN = Na$ (oder gleichbedeutend: für die $\equiv_r$ und $\equiv_l$ übereinstimmen).

Satz 1.5.1 *Für eine Untergruppe $N \leq G$ sind folgende Eigenschaften äquivalent:*

a) $aN = Na, \forall a \in G.$

b) $aNa^{-1} \subseteq N, \forall a \in G.$

c) $aNa^{-1} = N, \forall a \in G.$

Definition 1.5.2 Eine Untergruppe N von G, die diesen äquivalenten Eigenschaften genügt, heißt Normalteiler von G. In Zeichen: $N \lhd G$.

Bemerkungen:
1) $\equiv_r$ und $\equiv_l$ stimmen überein, falls N normal in G ist. Wir schreiben daher kurz: $\equiv$.
2) Für eine Normalteiler N erfüllt $\equiv$ die zusätzliche Eigenschaft aus Satz 1.2. Also ist $\bar{G} = G/N = N \setminus G$ eine Gruppe.

Satz 1.5.3 *Seien K, N, G Gruppen mit $K \leq G, N \lhd G$. Dann gilt:*

(i) $N \cap K$ *ist normal in* K.

(ii) $NK = KN$ *ist eine Untergruppe von* G.

(iii) Falls ebenfalls $K \lhd G$ *und* $K \cap N = \{e\}$, *so folgt:* $nk = kn, \forall n \in N, k \in K$.

Satz 1.5.4 *Sei $N \lhd G$. Dann ist G/N eine Gruppe der Ordnung $[G : N]$ unter der binären Operation $aN \cdot bN = abN, a, b \in G$.*

Die Gruppe G/N heißt Quotientengruppe oder Faktorgruppe von G modulo N.

Satz 1.5.5 *Sei $f : G \to H$ ein Homomorphismus. Dann gilt:*
(i) $\ker(f) \lhd G$.
(ii) Jeder Normalteiler N ist Kern eines Homomorphismus, nämlich von der sogenannten kanonischen Projektion

$$\pi : G \longrightarrow G/N, \quad g \mapsto gN.$$

Satz 1.5.6 *Sei $f : G \to H$ ein Homomorphismus und $N \lhd G$ mit $N \subseteq \ker(f)$. Dann ist die kanonische Abbildung*

$$\bar{f} : G/N \longrightarrow H, \quad gN \mapsto f(g)$$

ein wohldefinierter Homomorphismus und es gilt: $\ker(\bar{f}) = \ker(f)/N,\ im(\bar{f}) = im(f)$. *Der Homomorphismus $\bar{f}$ ist also genau dann injektiv, wenn $N = \ker(f)$.*

Folgerung 1.5.7 *(1. Isomorphiesatz) Sei $f : G \to H$ ein Homomorphismus. Dann induziert f einen Isomorphismus*

$$\bar{f} : G/\ker(f) \xrightarrow{\simeq} im(f), \quad g\ker(f) \mapsto f(g).$$

Folgerung 1.5.8 *Sei $f : G \to H$ ein Homomorphismus und $N \lhd G, M \lhd H$ mit $f(N) \leq M$. Dann induziert f einen Homomorphismus*

$$\bar{f} : G/N \longrightarrow H/M, \quad gN \mapsto f(g)M.$$

Es gilt:
(a) $\bar{f}$ ist surjektiv $\iff$ $im(f)M = H$.
(b) $\bar{f}$ ist injektiv $\iff$ $f^{-1}(M) \subseteq N$.

Folgerung 1.5.9 *(2. Isomorphiesatz) Seien $K, N \leq G, N \lhd G$. Dann ist $(K \cap N) \lhd K$ und die Abbildung*

$$K/(K \cap N) \longrightarrow KN/N, \quad k(K \cap N) \mapsto kN$$

ist ein Isomorphismus.

Folgerung 1.5.10 *(3. Isomorphiesatz) Seien $H, N \lhd G$ mit $N \leq H$. Dann ist $H/N \lhd G/N$ und die Abbildung*

$$G/H \longrightarrow \frac{G/N}{H/N}, \quad gH \mapsto gN \cdot (H/N)$$

ist ein Isomorphismus.

Satz 1.5.11 *Sei $f : G \to H$ ein Epimorphismus. Dann ist die Zuordnung $U \mapsto f(U)$ eine Bijektion zwischen der Menge der Untergruppen U von G mit $\ker(f) \subseteq U$ und der Menge der Untergruppen V von H. Dabei entsprechen normale Untergruppen wieder normalen Untergruppen.*
Ferner gilt: Falls $\ker(f) \leq U_2 \lhd U_1 \leq G$ so ist $f(U_2) \lhd f(U_1)$ und

$$U_1/U_2 \simeq f(U_1)/f(U_2), \quad uU_2 \mapsto f(u)f(U_2).$$

1.6 Normalreihen und Auflösbarkeit

Definition 1.6.1 (a) Sei G eine Gruppe. Eine Kette

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_r = \{e\}$$

von Untergruppen G_i von G mit $G_i \lhd G_{i-1}$ heißt Normalreihe von G. Die Gruppen G_{i-1}/G_i heißen die Faktoren der Normalreihe.
(b) G heißt auflösbar, falls G eine Normalreihe mit abelschen Faktoren besitzt.

Zum Beispiel sind alle abelschen Gruppen auflösbar.

Satz 1.6.2 *Sei G eine Gruppe. Dann gilt:*
a) G auflösbar, $H \leq G \implies H$ auflösbar.
b) G auflösbar, $N \lhd G \implies G/N$ auflösbar.
c) Sei $N \lhd G$. Dann gilt:

$$G \text{ auflösbar} \iff G/N \text{ und } N \text{ auflösbar.}$$

d) Sei G eine endliche p-Gruppe (p Primzahl). Dann ist G auflösbar.

Der Beweis von d) ist eine direkte Konsequenz von Satz 1.6.4. Dazu folgende Begriffsbildung.

Definition 1.6.3 Sei G eine Gruppe. Dann heißt

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

das Zentrum von G.

Offensichtlich ist $Z(G)$ ein Normalteiler von G.

Satz 1.6.4 *Sei G eine nicht-triviale endliche p-Gruppe. Dann hat G ein nicht-triviales Zentrum.*

In der Literatur wird Auflösbarkeit oft durch die Existenz einer Normalreihe mit zyklischen Faktoren definiert. Der nächste Satz zeigt die Äquivalenz zu unserer Definition.

Satz 1.6.5 *Sei G endlich und auflösbar. Dann besitzt G eine Normalreihe mit zyklischen Faktoren.*

Wir wollen nun eine weitere Charakterisierung auflösbarer Gruppen herleiten.

Definition 1.6.6 (a) Sei G eine Gruppe und $a, b \in G$. Dann heißt $[a, b] := aba^{-1}b^{-1}$ der Kommutator von a und b.
(b) Seien $H_1, H_2 \leq G$. Dann setzt man

$$[H_1, H_2] := \langle [a, b] : a \in H_1, b \in H_2 \rangle.$$

$[H_1, H_2]$ ist also die von allen Kommutatoren $[a, b]$, $a \in H_1, b \in H_2$ erzeugte Untergruppe.
(c) $G' := [G, G]$ heißt Kommutatoruntergruppe von G.

Bemerkung 1.6.7 (a) Die Gruppe G ist genau dann abelsch, wenn $G' = \{e\}$ gilt.
(b) Die Kommutatoruntergruppe besteht aus allen (endlichen) Produkten von Kommutatoren.
(c) G' ist ein Normalteiler von G und in Verallgemeinerung von (a) gilt für alle Normalteiler N von G:

$$G/N \text{ ist abelsch} \iff G' \subseteq N$$

Wir iterieren nun die Kommutatorbildung und definieren

$$D^0G := G, \quad D^{i+1}G := [D^iG, D^iG], \quad i \geq 0.$$

Beobachtungen (a) $G = D^0G \supseteq D^1G \supseteq \ldots \supseteq D^iG \supseteq \ldots$
(b) $D^{i+1}G \lhd D^iG$ und der Quotient $D^iG/D^{i+1}G$ ist abelsch.

Satz 1.6.8 *Sei G eine Gruppe. Dann gilt:*

$$G \textit{ ist auflösbar} \iff \textit{es gibt ein } n \in \mathbb{N} \textit{ mit } D^nG = \{e\}.$$

Im nächsten Abschnitt wollen wir einsehen, dass die symmetrische Gruppe S_n für $n \geq 5$ nicht auflösbar ist. Diese Tatsache wird Anwendungen für die Auflösbarkeit von allgemeinen Gleichungen vom Grad n haben. Den Zusammenhang wird die sogenannte Galoistheorie herstellen.
Um zu zeigen, dass die S_n nicht auflösbar ist, reicht es zu zeigen, dass die alternierende Gruppe A_n für $n \geq 5$ nicht auflösbar ist. Dies ist eine direkte Konsequenz aus dem folgenden Resultat, dass wir im nächsten Abschnitt beweisen werden

Satz 1.6.9 *Für $n \geq 5$ gilt*

$$[A_n, A_n] = A_n.$$

Wir schließen den Abschnitt mit einer wichtigen Definition.

Definition 1.6.10 Eine nicht-triviale Gruppe G heißt einfach, falls G keine Normalteiler außer $\{e\}$ und G besitzt.

Tatsächlich kann man zeigen, dass die alternierenden Gruppen A_n für $n \geq 5$ einfach sind (Übung).

1.7 Die symmetrischen Gruppen S_n

Definition 1.7.1 Sei $X_n = \{1, 2, \ldots, n\}$ und seien $a_1, \ldots a_s, s \leq n$, paarweise verschiedene Elemente aus X_n. Dann bezeichnet $(a_1, a_2, \ldots, a_s)$ diejenige Permutation für die gilt:

$$a_1 \mapsto a_2, a_2 \mapsto a_3, \ldots, a_{s-1} \mapsto a_s, a_s \mapsto a_1,$$
$$a \mapsto a, \forall a \in X_n \setminus \{a_1, a_2, \ldots, a_s\}.$$

$(a_1, a_2, \ldots, a_s)$ heißt Zyklus der Länge s oder s-Zyklus; ein 2-Zyklus heißt Transposition.

Beobachtung Zwei disjunkte Zyklen vertauschen.

Satz 1.7.2 *Jede nicht-triviale Permutation ist eindeutig (bis auf Vertauschung) als Produkt von disjunkten Zyklen darstellbar.*

Folgerung 1.7.3 *Die Ordnung einer Permutation $\sigma \in S_n$ ist gleich dem kleinsten gemeinsamen Vielfachen der Längen der disjunkten Zyklen in der eindeutigen Produktdarstellung.*

Satz 1.7.4 *Jedes $\sigma \in S_n$ kann als Produkt von Transpositionen geschrieben werden. Diese Darstellung ist nicht eindeutig, jedoch ist die Parität der Anzahl der Transpositionen unabhängig von der Darstellung.*

Zum Beweis haben wir die Signatur

$$sgn : S_n \to \{\pm 1\}$$

definiert durch

$$sgn(\sigma) = \det(e_{\sigma(e_1)} \cdots e_{\sigma(e_n)}),$$

wobei $e_1, \ldots, e_n$ die Standardbasis des $\mathbb{R}^n$ bezeichnet. Die Signatur $sgn : S_n \to \{\pm 1\}$ ist ein surjektiver Gruppenhomomrphismus.
Sei weiter $\sigma \in S_n$ und $\sigma = \tau_1 \cdots \tau_s$, wobei sämtliche τ_i Transpositionen sind. Dann gilt

$$sgn(\sigma) = (-1)^s.$$

Definition 1.7.5 Der Normalteiler $A_n := \ker(sgn)$ heißt die alternierende Gruppe.

Lemma 1.7.6 *A_n, $n \geq 3$, wird durch die 3-Zyklen erzeugt.*

Satz 1.7.7 *A_n ist der einzige Normalteiler der S_n vom Index 2.*

Satz 1.7.8 *Es gilt:*
a) $[S_n, S_n] = A_n$ für alle $n \geq 2$.
b)

$$[A_n, A_n] = \begin{cases} 1, & n = 2, 3, \\ V_4, & n = 4, \\ A_n, & n \geq 5. \end{cases}$$

Hierbei ist $V_4 = \langle (1,2)(3,4), (1,3)(2,4) \rangle$.

Folgerung 1.7.9 *S_n und A_n sind für $n \geq 5$ nicht auflösbar.*

Wir werden im Rahmen der Übungen sehen, dass die A_5 die kleinnste nicht auflösbare Gruppe ist. Ferner sei nochmals daran erinnert, dass man zeigen kann, dass die A_n fr $n \geq 5$ sogar einfach ist.

1.8 Gruppenoperationen

Definition 1.8.1 Sei M eine Menge und G eine Gruppe. Dann operiert G auf M, falls es eine Abbildung $G \times M \to M, (g, s) \mapsto gs$ gibt, so daß gilt

$$(g_1 g_2)m = g_1(g_2 m) \text{ und } em = m, \forall g_1, g_2 \in G, m \in M.$$

Man sagt dann auch: M ist eine G-Menge.

Zwei wichtige Beispiele erhält man für $M = G$:
a) G wirkt durch Konjugation auf G, d.h. $G \times G \longrightarrow G, (g, s) \mapsto gsg^{-1}$.
b) G wirkt durch Translation auf G, d.h. $G \times G \longrightarrow G, (g, s) \mapsto gs$.

Bezeichnung: Für eine Menge M bezeichne $S(M)$ die Gruppe der Permutationen von M.

Falls M eine G-Menge ist, so wird für jedes $g \in G$ durch die Setzung $T_g(m) := gm$ ein Element $T_g \in S(M)$ definiert.

Lemma 1.8.2 *Sei M eine G-Menge. Dann ist die Abbildung $T\colon G \longrightarrow S(M), g \mapsto T_g$, ein Gruppenhomomorphismus.*

Läßt man eine Gruppe durch Translation auf sich selbst wirken, so liefert dies den

Satz 1.8.3 *(Cayley) Jede Gruppe der Ordnung n ist isomorph zu einer Untergruppe der S_n.*

Definition 1.8.4
a) Sei M eine G-Menge und $x \in M$. Dann heißt $Gx := \{gx \mid g \in G\}$ die Bahn oder der Orbit von x unter G.
b) Man sagt G operiert transitiv auf M, falls M nur aus einem einzigen Orbit besteht.

Durch $m_1 \sim m_2 : \Longleftrightarrow \exists g \in G : gm_1 = m_2$ ist eine Äquivalenzrelation auf M definiert, wobei die Äquivalenzklassen genau die Bahnen sind. Man erhält daher

Satz 1.8.5 *Sei M eine G-Menge.*
a) M ist die disjunkte Vereinigung über die verschiedenen G-Bahnen.
b) Falls $|M| < \infty$, so gilt: $|M| = \sum_C |C|$, wobei über die verschiedenen Bahnen summiert wird.

Definition 1.8.6 Sei M eine G-Menge und $x \in M$. Dann heißt

$$G_x = Stab_G(x) := \{g \in G \mid gx = x\}$$

der Stabilisator von x in G. Weitere Bezeichnung: Standunterruppe.

Die Bijektion $G/Stab_G(x) \to Gx, gStab_G(x) \mapsto gx$ liefert

Satz 1.8.7 *(Bahnengleichung) Sei M eine endliche G-Menge und sei $x_1, \ldots, x_s$ ein vollständiges Vertretersystem der verschiedenen G-Bahnen. Dann gilt:*

$$|M| = \sum_{i=1}^{s} [G : Stab_G(x_i)].$$

1.9 Die Sylowsätze und Anwendungen

Definition 1.9.1 Sei G eine endliche Gruppe und p ein Primteiler der Gruppenordnung. Es gelte: $p^r \mid |G|, p^{r+1} \nmid |G|$. Dann nennt man jede Untergruppe $U \leq G$ mit $|U| = p^r$ eine p-Sylowuntergruppe von G.

Satz 1.9.2 *Sei G eine endliche Gruppe und p ein Primteiler der Gruppenordnung. Dann existiert eine p-Sylowuntergruppe.*

Der Beweis dazu erfolgt über Induktion nach der Gruppenordnung. Benötigt wird dazu

Lemma 1.9.3 *Sei G eine endliche abelsche Gruppe und $p \mid |G|$, p Primzahl. Dann hat G eine Untergruppe der Ordnung p.*

Satz 1.9.4 *(Sylowsätze) Sei G eine endliche Gruppe und P eine p-Sylowuntergruppe.*
(i) Sei H eine p-Untergruppe von G. Dann ist H in einer p-Sylowuntergruppe enthalten. Genauer: es gibt $x \in G$ mit $H \leq x^{-1}Px$.
(ii) Alle p-Sylowuntergruppe sind konjugiert.
(iii) Sei n_p die Anzahl der verschiedenen p-Sylowuntergruppen. Dann gilt:

$$n_p \equiv 1 (\text{mod } p) \text{ und } n_p = |G/N_G(P)|.$$

Hierzu ist folgende Definition nachzutragen:

Definition 1.9.5 Sei $H \leq G$. Dann heißt $N_G(H) := \{g \in G \mid gHg^{-1} \subseteq H\}$ der Normalisator von H in G.

Offensichtlich ist $N_G(H)$ eine Untergruppe von G, die H enthält. Zusammen mit (iii) impliziert dies:

$$n_p \mid m \text{ falls } |G| = p^r m, p \nmid m.$$

Als Anwendung der Sylowsätze klassifizieren wir die Gruppen der Ordnung pq, $p > q$ Primzahlen.

Satz 1.9.6 *Seien p, q Primzahlen mit $p > q$.*
a) Falls $q \nmid (p-1)$, so ist jede Gruppe der Ordnung pq zyklisch.
b) Falls $q \mid (p-1)$, so gibt es bis auf Isomorphie genau zwei Gruppen der Ordnung pq, nämlich C_{pq} und

$$< a, b \mid a^p = e = b^q, ba = a^s b >, \text{ wobei } s \not\equiv 1 (\text{mod } p), s^q \equiv 1 (\text{mod } p).$$

Zusatz: Gruppen der Ordnung pq, $p \neq q$, sind stets auflösbar.

Beim Beweis geht ein, daß für die zyklische Gruppe C_n gilt: $\text{Aut}(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. Ferner haben wir benutzt: $(\mathbb{Z}/p\mathbb{Z})^\times, p$ Primzahl, ist zyklisch. Dies werden wir später in der Ringtheorie beweisen.

Folgerung 1.9.7 *Sei $p > 2$ eine Primzahl und $|G| = 2p$. Dann ist G zyklisch oder isomorph zur Diedergruppe der Ordnung $2p$.*

Definition 1.9.8 Seien G und H Gruppen und $\varphi : H \to \text{Aut}(G)$ ein Homomorphismus. Dann wird das kartesische Produkt $G \times H$ mit der binären Operation

$$(g, h)(g', h') := (g\varphi(h)(g'), hh'), \quad g, g' \in G, h, h' \in H,$$

zu einer Gruppe. Diese heißt das semi-direkte Produkt von G und H. Man schreibt: $G \rtimes H$ oder $G \times_\varphi H$.

Beobachtung: G ist ein Normalteiler in $G \rtimes H$.

Bemerkung 1.9.9 Mit Hilfe semi-direkter Produkte kann man nicht-abelsche Gruppen der Ordnung p^3, p eine Primzahl, konstruieren

1.10 Abelsche Gruppen

Wir werden abelsche Gruppen stets additiv notieren. Falls $A_1, \ldots, A_n$ abelsche Gruppen sind, so schreiben wir $A_1 \oplus \ldots \oplus A_n$ für das kartesische Produkt. Die binäre Struktur hierauf wird komponentenweise definiert.
In diesem Zusammenhang sei auch an die folgende Definition (etwa aus der Theorie der Vektorräume) erinnert: Sei A eine abelsche Gruppe und $A_1, A_2 \leq A$. Dann schreibt man $A = A_1 \oplus A_2$, falls $A = A_1 + A_2$ und $A_1 \cap A_2 = \{0\}$. Äquivalent dazu: Für alle $a_1, a_1' \in A_1, a_2, a_2' \in A_2$ gilt: $a_1 + a_2 = a_1' + a_2' \iff a_1 = a_1'$ und $a_2 = a_2'$.

Definition 1.10.1 Eine abelsche Gruppe F heißt frei vom Rang n, $n \in \mathbb{N}$, falls $F \simeq \mathbb{Z}^n$.

Lemma 1.10.2 *(a) Sei $F = \oplus_{i=1}^n \mathbb{Z}e_i$ eine freie abelsche Gruppe und A eine abelsche Gruppe. Seien $a_1, \ldots, a_n \in A$ gegeben. Dann gibt es genau einen Gruppenhomomorphismus $f\colon F \longrightarrow A$ mit $f(e_i) = a_i, i = 1, \ldots, n$.*
(b) Seien F und A wie in (a) und $f\colon A \longrightarrow F$ ein Epimorphismus. Dann gibt es eine Untergruppe $B \leq A$ mit

$$A = \ker(f) \oplus B \text{ und } B \simeq F.$$

Definition 1.10.3 Sei A eine abelsche Gruppe.
(a) Ein Element $a \in A$ heißt Torsionselement, falls es ein $m \in \mathbb{Z}, m \neq 0$, gibt, so daß $ma = 0$.
(b) Die Menge

$$T(A) := \{a \in A \mid a \text{ ist Torsionselement } \}$$

heißt Torsionsuntergruppe von A.
(c) A heißt torsionsfrei, falls $T(A) = \{0\}$.

Man beachte, daß $T(A)$ tatsächlich eine Untergruppe von A ist.

Satz 1.10.4 *Sei F eine freie abelsche Gruppe vom Rang n und $A \leq F$ eine Untergruppe. Dann ist A frei vom Rang $\leq n$.*

Definition 1.10.5 Eine abelsche Gruppe heißt endliche erzeugt, falls es $a_1, \ldots, a_n \in A$ gibt, $n \in \mathbb{N}$, mit $A = \langle a_1, \ldots, a_n \rangle_{\mathbb{Z}}$.

Satz 1.10.6 *a) Sei M eine endlich erzeugte abelsche Gruppe. Dann gilt:*

$$M \text{ ist frei } \iff M \text{ ist torsionsfrei.}$$

b) Sei M eine endlich erzeugte abelsche Gruppe. Dann ist

$$M \simeq T(M) \oplus \mathbb{Z}^k,$$

wobei r der Rang des freien Moduls $M/T(M)$ ist.

Für eine endlich erzeugte abelsche Gruppe $A = \langle a_1, \ldots, a_n \rangle_{\mathbb{Z}}$ betrachten wir den Epimorphismus

$$\pi\colon \mathbb{Z}^n \longrightarrow A, \quad \sum_{i=1}^n n_i e_i \mapsto \sum_{i=1}^n n_i a_i,$$

Sei $F := \mathbb{Z}^n$ und $N := \ker(\pi)$. Dann ist nach dem Isomorphiesatz $A \simeq F/N$. Die Struktur von F/N wird durch den folgenden Satz eindeutig bestimmt.

Satz 1.10.7 *Sei F eine freie abelsche Gruppe vom Rang n und N eine Untergruppe von F. Dann gibt es $\mathbb{Z}$-Basen $u_1, \ldots, u_n$ von F und $v_1, \ldots, v_m$ von N mit $m \leq n$ und*

$$v_i = \epsilon_i u_i, \quad i = 1, \ldots, m, \epsilon_i \in \mathbb{N},$$
$$\epsilon_1 \mid \epsilon_2 \mid \ldots \mid \epsilon_m.$$

Der Beweis ist algorithmisch und kann als Verallgemeinerung des Gaußschen Algorithmus aufgefasst werden. Sei zunächst eine beliebige Basis $u_1, \ldots, u_n$ von F gegeben und beliebige Erzeugende $v_1, \ldots, v_k$ von N. Schreibe

$$v_k = \sum_{i=1}^{n} \alpha_{ik} u_i \text{ mit } \alpha_{ik} \in \mathbb{Z}.$$

Sei $A = (\alpha_{ik}) \in \mathbb{Z}^{n \times k}$. Wir werden die Matrix A durch schrittweises Abändern der Basis $u_1, \ldots, u_n$ und des Erzeugendensystems $v_1, \ldots, v_k$ in die Form

$$\left(\begin{array}{ccc|c} \epsilon_1 & & & \\ & \ddots & & 0 \\ & & \epsilon_m & \\ \hline & 0 & & 0 \end{array}\right)$$

transfromieren. Erlaubte Abänderungen sind dabei:
(1) Vertauschung zweier u oder v. Dies entspricht der Vertauschung zweier Zeilen oder Spalten.
(2) Ersetzung eines u_i durch $u_i + \lambda u_j, \lambda \in \mathbb{Z}, i \neq j$. Wegen

$$v_k = \sum_{l=1}^{n} \alpha_{lk} u_l = \sum_{l=1, l \neq i,j}^{n} \alpha_{lk} u_l + \alpha_{ik}(u_i + \lambda u_j) + (\alpha_{jk} - \alpha_{ik}\lambda) u_j$$

entspricht dies der Ersetzung der j-ten Zeile durch j-te Zeile minus λ mal i-te Zeile.
(3) Ersetzung eines v_i durch $v_i - \lambda v_j, \lambda \in \mathbb{Z}, i \neq j$. Dies entspricht der Ersetzung der i-ten Spalte durch i-te Spalte minus λ mal j-te Spalte.

Wir wenden nun den folgenden Algorithmus auf die Matrix A an:
Schritt 1: Durch Vertauschen von Zeilen und Spalten bringe man das Element ungleich Null von kleinstem Betrag an die Stelle $(1, 1)$.
Schritt 2: Durch Subtraktion geeigneter Vielfacher der ersten Zeile, kann man erreichen, dass A von der Form

$$A = \begin{pmatrix} \alpha_{11} & * & \ldots & * \\ \gamma_2 & & & \\ \vdots & & * & \\ \gamma_n & & & \end{pmatrix}$$

ist, wobei jedes γ_i entweder gleich Null ist oder $|\gamma_i| < |\alpha_{11}|$ gilt. Falls alle γ_i gleich Null sind, so gehe zu Schritt 3. Andernfalls gehe zu Schritt 1.
Schritt 3: Durch Subtraktion geeigneter Vielfacher der ersten Spalte, kann man sodann erreichen, dass A von der Form

$$A = \left(\begin{array}{c|ccc} \alpha_{11} & \gamma_1 & \ldots & \gamma_k \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right)$$

ist, wobei jedes γ_i entweder gleich Null ist oder $|\gamma_i| < |\alpha_{11}|$ gilt. Falls alle γ_i gleich Null sind, so gehe zu Schritt 4. Andernfalls gehe zu Schritt 1.
Schritt 4: Falls $A' = 0$ so beende den Algorithmus.
Schritt 5: Falls alle Einträge von A' durch α_{11} teilbar sind, so gehe mit A' in Schritt 1.
Schritt 6: Sei α_{ik} ein Koeffizient in A', der nicht durch α_{11} teilbar ist. Teile mit Rest,

$$\alpha_{ik} = \alpha_{11}\beta + \gamma, \gamma \neq 0, |\gamma| < |\alpha_{11}|.$$

Addiere nun die erste Zeile zur i-ten Zeile und subtrahiere dann β mal 1. Spalte von der k-ten Spalte. Dann kommt an der Stelle (i, k) gerade γ zu stehen. Gehe mit A in Schritt 1.

Der Algorithmus endet nach endlich vielen Schritten, da in den Schritten 2,3 und 5 der minimale Betrag der Elemente ungleich 0 von A verringert wird.
Als Folgerung hieraus (bis auf die Eindeutigkeit) erhalten wir den

Satz 1.10.8 *(Hauptsatz über endlich erzeugte abelsche Gruppen) Sei A eine endlich erzeugte abelsche Gruppe. Dann gibt es eindeutig bestimmte $\epsilon_1, \ldots, \epsilon_s \in \mathbb{N}$, $\epsilon_i > 1$, mit $\epsilon_1 \mid \epsilon_2 \mid \ldots \mid \epsilon_s$, so dass*

$$A \simeq \oplus_{i=1}^{s} \mathbb{Z}/\epsilon_i\mathbb{Z} \oplus \mathbb{Z}^r, \quad r = Rang(A/T(A)).$$

Definition 1.10.9 $\epsilon_1, \ldots, \epsilon_s$ nennt man die Invariantenteiler von A. Falls

$$\epsilon_i = \prod_{j=1}^{t} p_j^{e_{ij}}, \quad e_{ij} \in \mathbb{N}_0,$$

die eindeutige Primzahlzerlegung der ϵ_i ist, so nennt man die $p_j^{e_{ij}}$ die Elementarteiler von A.

Remarks 1.10.10 1) Nach dem Chinesischen Restsatz folgt

$$A \simeq \mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t} \mathbb{Z}/p_j^{e_{ij}}\mathbb{Z} \simeq \mathbb{Z}^r \oplus \bigoplus_{j=1}^{t} \bigoplus_{i=1}^{s} \mathbb{Z}/p_j^{e_{ij}}\mathbb{Z}.$$

Es gilt:

$$T_{p_j}(A) \simeq \bigoplus_{i=1}^{s} \mathbb{Z}/p_j^{e_{ij}}\mathbb{Z},$$

wobei wir für eine Primzahl p definieren:

$$T_p(A) := \{a \in A \mid \text{ es gibt } k \in \mathbb{N} \text{ mit } p^k a = 0\}.$$

2) Invariantenteiler und Elementarteiler entsprechen sich eineindeutig.

2 Ringtheorie

2.1 Ringe und Ringhomomorphismen

Definition 2.1.1 Ein Ring ist eine nicht-leere Menge R zusammen mit zwei binären Operationen $+$ und $\cdot$, so daß gilt:

(i) $(R, +)$ ist eine abelsche Gruppe.
(ii) $(R, \cdot)$ ist ein Monoid.
(iii) $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot b + a \cdot c, \forall a, b, c \in R.$

Die Regeln unter (iii) sind die Distributivgesetze. Falls zusätzlich gilt:

$$(iv) a \cdot b = b \cdot a, \forall a, b \in R,$$

so heißt der Ring kommutativ.

Definition 2.1.2 Sei R ein Ring.
a) Elemente $x \neq 0, y \neq 0$ heißen Nullteiler, falls gilt: $xy = 0$.
b) Ein Element $a \in R$ heißt invertierbar, falls es ein $b \in R$ gibt mit $ab = ba = 1$. Man nennt dann a auch eine Einheit. Die Menge der Einheiten von R bildet eine Gruppe und wird mit $R^\times$ bezeichnet.
c) Ein Integritätsbereich ist ein nullteilerfreier, kommutativer Ring.
d) Falls in R jedes Element $a \neq 0$ invertierbar ist, so ist R ein Schiefkörper. Falls R zusätzlich auch kommutativ ist, so nennt man R einen Körper.

Beispiele von Ringen sind allgegenwärtig in der Mathematik. Angesprochen wurden hier $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, Matrizenringe und die Hamiltonschen Quaternionen.

Satz 2.1.3 *Sei $R = \mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$. Dann gilt:*

$$\begin{array}{ll} (a) & \bar{k} \text{ ist Nullteiler} \iff (k,n) > 1. \\ (b) & \bar{k} \text{ ist Einheit} \iff (k,n) = 1. \end{array}$$

Insbesondere gilt also:

$$\mathbb{Z}/n\mathbb{Z} \text{ ist ein Körper} \iff n \text{ ist Primzahl.}$$

Definition 2.1.4 a) Seien R und S Ringe. Eine Abbildung $f : R \to S$ ist ein Ringhomomorphismus, falls für alle $a, b \in R$ gilt:

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b).$$

b) Die Teilmenge $\ker(f) := \{r \in R \mid f(r) = 0\}$ heißt der Kern von f.

Achtung: Es gilt zwar stets $f(0) = 0$, jedoch i. a. nicht $f(1) = 1$.
Es gilt: f ist injektiv $\iff \ker(f) = \{0\}$.

2.2 Ideale

Ideale spielen in der Ringtheorie die Rolle der Normalteiler in der Gruppentheorie.

Definition 2.2.1 Sei R ein Ring und I eine Teilmenge von R. Dann heißt I ein R-Linksideal (bzw. R-Rechtsideal), falls für alle $r, a, b \in R$ gilt:

$$\begin{array}{ll} (i) & a, b \in I \implies a + b \in I, \\ (ii) & a \in I, r \in R \implies ra \in I \quad (\text{bzw. } ar \in I). \end{array}$$

I heißt (beidseitiges) Ideal, falls I sowohl Rechts-, als auch Linksideal ist.

Definition 2.2.2 Sei R ein kommutativer Ring und $X \subseteq R$.
a) Die Menge

$$(X) := \left\{ \sum_{x \in X} r_x x \mid r_x \in R, \text{ fast alle } r_x = 0 \right\},$$

heißt das von X erzeugte Ideal. Falls $X = \{x_1, \ldots, x_n\}$ eine endliche Menge ist, so schreibt man auch $(x_1, \ldots, x_n)$ anstelle von (X). Falls $X = \{x\}$, so heißt (x) das von x erzeugte Hauptideal.
b) Ein Hauptidealring ist ein nullteilerfreier, kommutativer Ring, in dem jedes Ideal ein Hauptideal ist.

Satz 2.2.3 *Der Ring der ganzen Zahlen $\mathbb{Z}$ ist ein Hauptidealring.*

Beispiel: Die Teilmenge $\mathbb{Q}(\sqrt{-5}) := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Q}\}$ ist ein Teilkörper der komplexen Zahlen. Wir betrachten den Ring $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ sowie $I := 3\mathbb{Z} + (1 + \sqrt{-5})\mathbb{Z}$. Dann ist I ein Ideal in R. Durch Normbetrachtungen haben wir gezeigt, dass I kein Hauptideal ist.

Definition 2.2.4 Sei R ein Ring und I, J Ideale in R. Dann definiert man:

$$\begin{array}{rcl} I + J & := & \{a + b \mid a \in I, b \in J\}, \\ IJ & := & \{ \sum\limits_{\text{endlich}} a_i b_i \mid a_i \in I, b_i \in J\}. \end{array}$$

IJ heißt das Produkt der Ideale I und J, $I+J$ die Idealsumme oder oft auch der größte gemeinsame Teiler von I und J.

Bemerkung: IJ und $I + J$ sind Ideale von R. Offensichtlich ist auch der Durchschnitt $I \cap J$ ein Ideal.

Für einen Ring R und ein Ideal I in R bezeichnen wir die Menge der Äquivalenzklassen bezüglich der additiven Struktur wie in der Gruppentheorie mit R/I. Sei $a \in R$. Dann schreiben wir $\bar{a} = a+I$ für die Restklasse von a modulo I. R/I ist durch vertreterweise Addition eine abelsche (additive) Gruppe.

Satz 2.2.5 *Durch $(a + I) \cdot (b + I) := ab + I$ wird auf R/I eine Ringstruktur definiert.*

Satz 2.2.6 *Sei R ein Ring. Dann sind die Ideale genau die Kerne von Ringhomomorphismen.*

Ersetzt man in den Isomorphiesätzen für Gruppen den Begriff "Gruppen" durch "Ringe" und "Normalteiler" durch "Ideale", so ergeben sich mit demselben Beweis die entsprechenden Isomorphiesätze für Ringe. Wegen der offensichtlichen Analogie werden diese hier nicht noch einmal aufgeführt.

Definition 2.2.7 Sei R ein kommutativer Ring und $P \subseteq R, P \neq R$ ein Ideal. Dann heißt P prim oder ein Primideal, falls für alle $a, b \in R$ gilt:

$$ab \in P \implies a \in P \text{ oder } b \in P.$$

Der folgende Satz liefert eine äquivalente Charakterisierung.

Satz 2.2.8 *Sei R ein kommutativer Ring und P ein Ideal in R mit $P \neq R$. Dann gilt:*

$$P \text{ ist Primideal} \iff R/P \text{ ist nullteilerfrei.}$$

Definition 2.2.9 Sei R ein kommutativer Ring und $M \subseteq R, M \neq R$ ein Ideal. Dann heißt M maximal, falls für alle Ideale I von R gilt: $M \subseteq I, M \neq I \implies I = R$.

Satz 2.2.10 *Sei R ein kommutativer Ring und $I \subseteq R$, $I \neq R$, ein Ideal. Dann gilt:*

$$I \text{ ist maximal} \iff R/I \text{ ist ein Körper.}$$

Insbesondere ist also jedes maximale Ideal ein Primideal.

Um zu beweisen, daß maximale Ideale stets existieren, benötigen wir das Zornsche Lemma. Sei dazu $(A, \leq)$ eine partiell geordnete Menge (z.B. die Menge der natürlichen Zahlen mit der Teilbarkeitsrelation). Ein Element $a \in A$ heißt maximal, falls für alle mit a vergleichbaren $b \in A$ gilt: $b \leq a$. Sei $B \subseteq A$. Dann heißt $d \in A$ eine obere Schranke für B, falls alle $b \in B$ mit d vergleichbar sind und gilt: $b \leq d$. Eine Kette in A ist eine linear geordnete Sequenz $a_0 \leq a_1 \leq a_2 \leq \ldots$ von Elementen $a_i \in A$.

Zornsches Lemma: Sei A eine nicht-leere partiell geordnete Menge, so daß jede Kette in A eine obere Schranke in A hat. Dann existieren maximale Elemente in A.

Man kann zeigen, daß das Zornsche Lemma äquivalent ist zu

Auswahlaxiom: Sei I ein nicht-leere Indexmenge und $\{S_i \mid i \in I\}$ eine Familie von nicht-leeren Mengen S_i. Dann gilt: $\prod_{i \in I} S_i \neq \emptyset$.

Als Anwendung erhalten wir

Satz 2.2.11 *Sei R ein kommutativer Ring und $I \subseteq R, I \neq R$, ein Ideal. Dann ist I in einem maximalen Ideal enthalten. Insbesondere existieren also maximale Ideale.*

Satz 2.2.12 *Sei $\{R_i \mid i \in I\}$ eine Familie von Ringen und $\prod_{i\in I} R_i$ das kartesische Produkt der R_i. Dann ist $\prod_{i\in I} R_i$ mit komponentenweiser Addition und Multiplikation ein Ring.*

Satz 2.2.13 *(Chinesischer Restsatz) Sei R ein Ring und seien $I_1, \ldots, I_n$ Ideale in R mit $I_k + I_l = R$ für $k \neq l$. Seien weiter $b_1, \ldots, b_n \in R$ gegeben. Dann gibt es ein $b \in R$ mit $b \equiv b_k \pmod{I_k}, k = 1, \ldots, n$. b ist dabei eindeutig bestimmt modulo $I_1 \cap \ldots \cap I_n$.*

Folgerung 2.2.14 *Sei R ein Ring und seien $I_1, \ldots, I_n$ Ideale in R mit $I_k + I_l = R$ für $k \neq l$. Sei $I = I_1 \cap \ldots \cap I_n$. Dann ist*

$$\begin{array}{rcl} R/I & \longrightarrow & R/I_1 \times \ldots \times R/I_n, \\ a + I & \mapsto & (a + I_1, \ldots, a + I_n) \end{array}$$

ein Isomorphismus von Ringen.

Die Folgerung ist tatsächlich äquivalent zum Chinesischen Restsatz. Die Surjektivität entspricht der Existenzaussage, die Injektivität der Eindeutigkeitsaussage im Chinesischen Restsatz.
Eine häufig verwendete Konsequenz aus dem Chinesischen Restsatz ist

Folgerung 2.2.15 *Sei $m \in \mathbb{N}$ eine natürliche Zahl, $m \geq 2$. Sei*

$$m = p_1^{e_1} \cdots p_s^{e_s}$$

die Primzahlzerlegung von m mit paarweise verschiedenen Primzahlen p_i. Dann ist

$$\begin{array}{rcl} \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_s^{e_s}\mathbb{Z}, \\ a + m\mathbb{Z} & \mapsto & (a + p_1^{e_1}\mathbb{Z}, \ldots, a + p_s^{e_s}\mathbb{Z}) \end{array}$$

ein Isomorphismus von Ringen.

2.3 Faktorisierung in kommutativen Ringen

ZIEL: Satz von der eindeutigen Primzahlzerlegung in Hauptidealringen.

Definition 2.3.1 Sei R ein kommutativer Ring und $0 \neq a, b \in R$. Dann heißen a und b zueinander assoziiert, in Zeichen $a \sim b$, falls $a \mid b$ und $b \mid a$.

Satz 2.3.2 *Sei R ein komm. Ring und $a, b, u \in R$. Dann gilt:*

$$\begin{array}{ll} (i) & a \mid b \iff (b) \subseteq (a) \\ (ii) & a \sim b \iff (a) = (b) \\ (iii) & u \in R^\times \iff u \mid r, \forall r \in R \\ (iv) & u \in R^\times \iff (u) = R \\ (v) & a = bu, u \in R^\times \implies a \sim b. \end{array}$$

Falls R nullteilerfrei ist, so gilt in (v) auch die Rückrichtung.

Definition 2.3.3 Sei R ein kommutativer Ring.
a) Ein Element $0 \neq c \in R \setminus R^\times$ heißt irreduzibel, falls für alle $a, b \in R$ gilt:

$$c = ab \implies a \in R^\times \text{ oder } b \in R^\times.$$

b) Ein Element $0 \neq p \in R \setminus R^\times$ heißt prim, falls für alle $a, b \in R$ gilt:

$$p \mid ab \implies p \mid a \text{ oder } p \mid b.$$

Satz 2.3.4 *Sei R ein nullteilerfreier, komm. Ring. Dann gilt:*

- *p ist prim $\iff$ (p) ist Primideal.*
- *p prim $\implies$ p irreduzibel.*
- *Falls R ein Hauptidealring ist, so gilt:*

$$p \text{ prim} \iff p \text{ irreduzibel}$$

Definition 2.3.5 Sei R ein nullteilerfreier, komm. Ring. Dann heißt R faktoriell oder ZPE-Ring, falls gilt:
(i) Jedes Element $a \neq 0, a \notin R^\times$ kann man als Produkt $a = c_1 \cdots c_n, c_i$ irreduzibel, schreiben.
(ii) Falls $a = d_1 \cdots d_m, d_j$ irreduzibel, eine weitere solche Darstellung ist, so gilt $n = m$ und (bis auf Numerierung) $d_i \sim c_i$.

Bemerkung: In einem faktoriellen Ring ist jedes irreduzible Element prim.

Beispiel: $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell.

Satz 2.3.6 *Jeder Hauptidealring ist faktoriell.*

Definition 2.3.7 Ein euklidischer Ring ist ein nullteilerfreier, kommutativer Ring R mit einer Funktion $\varphi : R \to \mathbb{N}_0$, so daß gilt:
(i) $\varphi(a) = 0 \iff a = 0$.
(ii) zu $a, b \in R, b \neq 0$, gibt es Elemente $v, r \in R$ mit $a = vb + r$ und $\varphi(r) < \varphi(b)$.

Das Standardbeispiel hierfür ist $\mathbb{Z}$ zusammen mit dem Absolutbetrag. Wie für $\mathbb{Z}$ zeigt man

Satz 2.3.8 *Jeder euklidische Ring ist ein Hauptidealring.*

Definition 2.3.9 Sei R ein Hauptidealring und $a, b \in R$. Dann heißt jeder Erzeuger d von $(a)+(b)$ ein größter gemeinsamer Teiler von a und b. Jeder Erzeuger k von $(a) \cap (b)$ heißt ein kleinstes gemeinsames Vielfaches von a und b.

In euklidischen Ringen hat man durch den euklidischen Algorithmus ein (schnelles) Verfahren zur Berechnung des ggT und kann mit dem erweitereten euklidischen Algorithmus auch eine Darstellung

$$\text{ggT}(a, b) = xa + yb \text{ mit } x, y \in R$$

berechnen.

2.4 Polynomringe

Satz 2.4.1 *Sei R ein kommutativer Ring und $f, g \in R[x]$. Sei der führende Koeffizient von g eine Einheit in R. Dann gibt es eindeutig bestimmte Polynome $q, r \in R[x]$ mit der Eigenschaft:*

$$f = qg + r \text{ mit } r = 0 \text{ oder } deg(r) < deg(g).$$

Folgerung 2.4.2 *Sei K ein Körper. Dann ist $K[x]$ ein euklidischer Ring.*

Satz 2.4.3 *Seien $R \subseteq S$ nullteilerfreie kommutative Ringe und $f \in R[x]$ ein Polynom vom Grad n. Dann hat f höchstens n Nullstellen in S.*

Definition 2.4.4 Sei R ein nullteilerfreier kommutativer Ring und $f \in R[x]$. Sei $c \in R$ eine Nullstelle von f. Dann heißt

$$max\{m \in \mathbb{N} \mid (x-c)^m \text{ teilt } f\}$$

die Vielfachheit der Nullstelle c.

Satz 2.4.5 *Sei R ein nullteilerfreier kommutativer Ring. Sei $R \subseteq S$ und $c \in S$, wobei S ebenfalls ein nullteilerfreier kommutativer Ring ist. Dann gilt:*
(i) c ist mehrfache Nullstelle $\iff f(c) = f'(c) = 0$.
(ii) Sei R ein Körper. Dann hat f keine mehrfachen Nullstellen in S, falls $(f, f') = 1$.
(iii) Sei R ein Körper und f irreduzibel. Dann gilt:

$$f \text{ hat mehrfache Nullstellen in } S \implies f' = 0.$$

Definition 2.4.6 Sei R ein faktorieller Ring. Sei $f = a_n x^n + a_{n-1}x^{n-1} + \dots a_1^x + a_0 \in R[x]$. Dann heißt $c(f) := (a_0, a_1, \dots, a_n)$ der Inhalt von f. Falls $c(f) \in R^\times$, so heißt f primitiv.

Bemerkungen:
1) $c(f)$ ist nur bis auf Assoziiertheit bestimmt.
2) Jedes Polynom g läßt sich in der Form $g = c(g)g_1$ mit primitivem g_1 schreiben.

Satz 2.4.7 *(Gaußsches Lemma) Sei R faktoriell und $f, g \in R[x]$. Dann gilt: $c(fg) \sim c(f)c(g)$. Insbesondere ist also das Produkt von primitiven Polynomen wieder primitiv.*

Satz 2.4.8 *Sei R faktoriell und $K = Quot(R)$ der Quotientenkörper. Sei $f \in R[x]$ ein nichtkonstantes, primitives Polynom. Dann gilt:*

$$f \text{ irreduzibel in } K[x] \iff f \text{ irreduzibel in } R[x]$$

Bemerkung: Der Quotientenkörper wurde bislang nur informell definiert. Dies wird noch nachgeholt.

Satz 2.4.9 *(Eisensteinkriterium) Sei R faktoriell und $K = Quot(R)$. Sei $f = a_n x^n + a_{n-1}x^{n-1} + \dots a_1 x + a_0 \in R[x]$, $deg(f) \geq 1$. Sei $p \in R$ irreduzibel und es gelte*

$$p \nmid a_n, \quad p \mid a_i,\ i = 0, \dots, n-1, \quad p^2 \nmid a_0.$$

Dann ist f irreduzibel in $K[x]$. Falls f zusätzlich primitiv ist, so ist f auch irreduzibel in $R[x]$.

Satz 2.4.10 *Sei R faktoriell. Dann ist auch $R[x_1, \dots, x_n]$ faktoriell.*

Im folgenden Einschub holen wir die Definition des Quotientenkörpers nach, gehen dabei aber etwas allgemeiner vor:

Definition 2.4.11 Sei R ein kommutativer Ring und $S \subseteq R$ eine nicht-leere Teilmenge. Dann heißt S multiplikativ, falls gilt: (i) $0 \notin S$, (ii) $a, b \in S \implies ab \in S$.

Satz 2.4.12 *Sei S eine multiplikative Teilmenge eines kommutativen Rings R. Dann ist durch*

$$(r, s) \sim (r_1, s_1) : \iff \exists t \in S : t(rs_1 - r_1 s) = 0$$

eine Äquivalenzrelation auf $R \times S$ definiert.

Bemerkung: Falls R nullteilerfrei ist, so gilt einfacher:

$$(r, s) \sim (r_1, s_1) : \iff rs_1 - r_1 s = 0$$

Die Äquivalenzklasse von (r, s) bezeichnen wir suggestiv mit $\frac{r}{s}$; $S^{-1}R$ bezeichnet die Menge der Äquivalenzklassen.

Satz 2.4.13 *Sei S eine multiplikative Teilmenge des kommutativen Rings R. Dann gilt:*
(i) $S^{-1}R$ ist ein kommutativer Ring mit den binären Operationen

$$\frac{r}{s} + \frac{r_1}{s_1} := \frac{rs_1 + r_1 s}{ss_1}, \quad \frac{r}{s} \cdot \frac{r_1}{s_1} := \frac{rr_1}{ss_1}$$

(ii) Falls R nullteilerfrei ist, so auch $S^{-1}R$.
(iii) Falls R nullteilerfrei ist und $S = R \setminus \{0\}$, so ist $S^{-1}R$ ein Körper.

Bemerkung: Der Körper in (iii) heißt der Quotientenkörper von R und wird im weiteren mit $Quot(R)$ bezeichnet.

Satz 2.4.14 *Sei S eine multiplikative Teilmenge des kommutativen Rings R. Dann gilt:*
(i) Die Abbildung $\varphi_S : R \to S^{-1}R, r \mapsto \frac{rs}{s}$, $s \in S$ beliebig, ist ein wohldefinierter Ringhomomorphismus. Für alle $s \in S$ gilt:

$$\varphi_S(s) \in \left(S^{-1}R\right)^\times.$$

(ii) Falls S keine Nullteiler enthält, so ist φ_S injektiv. Insbesondere kann man also jeden kommutativen nullteilerfreien Ring in seinen Quotientenkörper einbetten.
(iii) Falls $S \subseteq R^\times$, so ist φ_S ein Isomorphismus. Falls R ein Körper ist, so ist insbesondere $Quot(R) = R$.

3 Die Struktur von $(\mathbb{Z}/m\mathbb{Z})^\times$

3.1 Die Eulersche φ-Funktion

Definition 3.1.1 Sei $m \in \mathbb{N}$. Dann heißt $\varphi(m) := \left|(\mathbb{Z}/m\mathbb{Z})^\times\right|$ Eulersche φ-Funktion.

Satz 3.1.2 *a) Die Eulersche φ-Funktion ist multiplikativ in folgendem Sinn:*

$$\varphi(mn) = \varphi(m)\varphi(n), \text{ falls } (m,n) = 1.$$

Insbesondere gilt also:

$$\varphi(m) = \prod_{i=1}^{t} \varphi(p_t^{\alpha_t})$$

falls die eindeutige Primzahlzerlegung von m durch $m = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ gegeben ist.
b) Sei p eine Primzahl. Dann gilt: $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.

Eine direkte Folgerung aus der Definition der φ-Funktion ist der sogenannte "kleine Satz von Fermat":

Satz 3.1.3 *Für $a \in \mathbb{Z}$ mit $(a,m) = 1$ gilt $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m)$.*

Eine einfache, aber im täglichen Leben sehr wichtige Anwendung des kleinen Satzes von Fermat, ist das sogenannte RSA-Kryptographie-Verfahren.

3.2 Primitivwurzeln

Um die Struktur der abelschen Gruppen $(\mathbb{Z}/m\mathbb{Z})^\times$ zu bestimmen, genügt es nach dem chinesischen Restsatz die Struktur der Gruppen $(\mathbb{Z}/p^\alpha)^\times$ für Primzahlen p zu bestimmen.

Satz 3.2.1 *Sei $p \neq 2$ eine Primzahl und $\alpha \in \mathbb{N}$. Dann ist $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ zyklisch von der Ordnung $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$. Die Gruppe $(\mathbb{Z}/2^\alpha)^\times$ ist für $\alpha > 2$ bizyklisch. Explizit hat man*

$$(\mathbb{Z}/2^\alpha)^\times \simeq \begin{cases} 1, & \text{falls } \alpha = 1, \\ \langle -1 \rangle, & \text{falls } \alpha = 2, \\ \langle -1 \rangle \times \langle 5 \rangle, & \text{falls } \alpha > 2. \end{cases}$$

Zum Beweis benötigen wir den

Satz 3.2.2 *Sei K ein Körper und $G \subseteq K^\times$ eine endliche Untergruppe. Dann ist G zyklisch. Insbesondere ist also $(\mathbb{Z}/p\mathbb{Z})^\times$ für jede Primzahl p eine zyklische Gruppe.*

Der Beweis des letzten Satzes beruht wesentlich auf

Lemma 3.2.3 *Sei G eine abelsche Gruppe und $x, y \in G$. Dann gibt es ein Element $z \in G$ mit $ord(z) = \mathrm{kgV}(ord(x), ord(y))$.*

4 Körpertheorie

4.1 Die Gradformel

Falls E/K eine Körpererweiterung ist, so kann man E in natürlicher Weise als K-Vektorraum auffassen.

Definition 4.1.1 a) Sei E/K eine Körpererweiterung. Dann heißt die Dimension

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

der Grad von E über K.
b) Sei E/K eine Körpererweiterung und $\alpha \in E$. Dann ist $K(\alpha)$ definiert als der kleinste Teilkörper von E, der K und α enthält. Man sagt "K adjungiert α".

Satz 4.1.2 *(Gradfromel) Sei $E/F/K$ ein Körperturm. Dann gilt:*

$$[E : K] = [E : F][F : K]$$

4.2 Algebraische Körpererweiterungen

Definition 4.2.1 Sei E/K eine Körpererweiterung. Ein Element $\alpha \in E$ heißt algebraisch über K, falls es ein Polynom $f(x) \neq 0$ in $K[x]$ gibt, so daß $f(\alpha) = 0$.
Falls α nicht algebraisch ist, so heißt α transzendent über K.

Der Begriff "algebraisch" läßt sich folgendermaßen charakterisieren.

Satz 4.2.2 *Sei E/K eine Körpererweiterung und $\alpha \in E$. Dann gilt:*

$$\alpha \text{ ist algebraisch}/K \iff [K(\alpha) : K] < \infty.$$

Eine wesentliche Rolle im Beweis spielt das sogenannte Minimalpolynom.

Definition 4.2.3 Sei E/K eine Körpererweiterung und $\alpha \in E$ algebraisch über K. Dann heißt das normierte Polynom $m(x) \in K[x]$ kleinsten Grades mit der Eigenschaft $m(\alpha) = 0$ das Minimalpolynom von α über K.

Bemerkung 4.2.4 1) Für jedes Polynom $f(x) \in K[x]$ mit $f(\alpha) = 0$ gilt $m(x) \mid f(x)$.
2) Das Minimalpolynom $m(x)$ ist irreduzibel.
3) $[K(\alpha) : K] = \deg(m(x))$.
4) Faßt man die Multiplikation mit α als Endomorphismus des K-Vektorraums E auf, so ist $m(x)$ ein Teiler des charakteristischen Polynoms.

Definition 4.2.5 Eine Körpererweiterung E/K heißt algebraisch, falls jedes Element $\beta \in E$ algebraisch über K ist. Andernfalls heißt E transzendent.

Satz 4.2.6 *1) Jede endliche Körpererweiterung E/K (d.h. $[E : K] < \infty$) ist algebraisch.*
2) Es gilt: $\alpha \in E$ ist algebraisch über $K \iff K(\alpha)/K$ ist algebraisch.
3) Sei $\alpha \in E$ algebraisch über K mit Minimalpolynom $m(x)$. Dann gilt: $\deg(m(x)) \mid [E : K]$.

Man beachte, daß die Umkehrung von 1) falsch ist. Jedoch gilt

Satz 4.2.7

$$E = K(\alpha_1, \ldots, \alpha_m), \alpha_1, \ldots, \alpha_m \text{ alg. } /K \iff [E : K] < \infty.$$

Der folgende Satz besagt, daß der Begriff "algebraisch" transitiv ist.

Satz 4.2.8 *Sei $E/L/K$ ein Körperturm. Dann gilt:*

$$E/K \text{ ist algebraisch} \iff E/L \text{ und } L/K \text{ sind algebraisch.}$$

Definition 4.2.9 Sei E/K eine Körpererweiterung. Dann heißt

$$\{\alpha \in E \mid \alpha \text{ ist algebraisch über } K\}$$

der algebraische Abschluß von K in E.

Satz 4.2.10 *Sei E/K eine Körpererweiterung. Dann ist der algebraische Abschluß von K in E ein Teilkörper von E.*

Definition 4.2.11 Sei E/K eine Körpererweiterung und $K \subseteq L_1, L_2 \subseteq E$ seien Zwischenkörper. Dann heißt $L_1L_2 := L_1(L_2) = L_2(L_1)$ das Kompositum von L_1 und L_2. Also ist L_1L_2 der kleinste Teilkörper von E, der L_1 und L_2 enthält.

Satz 4.2.12 *Sei $K \subseteq L_1, L_2 \subseteq E$. Dann gilt:*
a) L_1/K algebraisch $\implies L_1L_2/L_2$ algebraisch.
b) L_1/K endlich $\implies L_1L_2/L_2$ endlich, genauer: $[L_1L_2 : L_2] \leq [L_1 : K]$.
c) $L_1/K, L_2/K$ algebraisch $\implies L_1L_2/K$ algebraisch.
d) $L_1/K, L_2/K$ endlich $\implies L_1L_2/K$ endlich, genauer: $[L_1L_2 : K] \leq [L_1 : K][L_2 : K]$. Falls zusätzlich $ggT([L_1 : K], [L_2 : K]) = 1$, so gilt in der Ungleichung sogar Gleichheit.

4.3 Einfache Körpererweiterungen

Definition 4.3.1 Eine Körpererweiterung L/K heißt einfach, falls $\alpha \in L$ existiert, so daß $L = K(\alpha)$. Jedes solche α heißt primitives Element.

Es sei nun L/K eine Körpererweiterung und $\alpha \in L$. Dann definieren wir

$$K[\alpha] := \{g(\alpha) \mid g \in K[X]\}.$$

Lemma 4.3.2 *Es gilt:*

$$\alpha \text{ ist algebraisch/} K \iff K(\alpha) = K[\alpha] \iff K[\alpha] \text{ ist ein Körper.}$$

Im Gegensatz hierzu gilt:

Lemma 4.3.3 *Folgende Aussagen sind äquivalent:*
(i) α *ist transzendent.*
(ii) Die Abbildung $\varphi : K[X] \longrightarrow K[\alpha], g(X) \mapsto g(\alpha)$ *ist ein Isomorphismus.*
(iii) $K[\alpha]$ *ist kein Körper.*

Definition 4.3.4 Der Körper $K(X) := Quot(K[X])$ heißt der rationale Funktionenkörper. Es gilt:

$$K(X) = \left\{ \frac{f(X)}{g(X)} \mid f, g \in K[X], g \neq 0 \right\}.$$

Satz 4.3.5 *Sei* L/K *eine Körpererweiterung und* $\alpha \in L$ *sei transzendent. Dann ist* $K(\alpha)$ *isomorph zu* $K(X)$*.*

Wir erinnern nochmals an einfache Konsequenzen aus der Definition des Minimalpolynoms.

Lemma 4.3.6 *Sei* L/K *eine Körpererweiterung und* $\alpha \in L$ *algebraisch. Dann gilt:*
a) Mipo_α *ist irreduzibel.*
b) Sei $f \in K[X]$ *irreduzibel und normiert und es gelte* $f(\alpha) = 0$*. Dann ist* $f = \mathrm{Mipo}_\alpha$*.*

Satz 4.3.7 *Sei* L/K *eine einfache algebraische Erweiterung und* $\alpha \in L$ *ein primitives Element, d.h.* $L = K(\alpha)$*. Dann gilt:*

$$K[X]/\left(\mathrm{Mipo}_\alpha(X)\right) \xrightarrow{\simeq} K(\alpha) = K[\alpha]$$

Umgekehrt gilt

Satz 4.3.8 *Sei* $f \in K[X]$ *irreduzibel. Dann is* $K[X]/(f(X))$ *eine algebraische Körpererweiterung von* K *vom Grad* $\deg(f)$*. (Hierbei identifizieren wir* K *mit dem Bild von* K *in* $K[X]/(f(X))$*.)*

4.4 Zerfällungskörper von Polynomen

Definition 4.4.1 Seien E_1, E_2 Erweiterungskörper von K. Dann nennt man einen Körperhomomorphismus $\sigma : E_1 \longrightarrow E_2$ mit $\sigma|_K = id$ einen K-Homomorphismus von E_1 in E_2. Man schreibt dann auch $\sigma : E_1/K \longrightarrow E_2/K$.

K-Homomorphismen sind stets injektiv. Sei $E_1 = K(\alpha)$ mit $f = \mathrm{Mipo}_\alpha$. Sei $\sigma : E_1/K \longrightarrow E_2/K$ und es sei $\sigma(\alpha) = \beta$. Dann ist β ebenfalls eine Nullstelle von f.

Lemma 4.4.2 *(Fortsetzungslemma) Seien* E/K *und* E'/K' *Körpererweiterungen und* $\sigma : K \longrightarrow K'$ *ein Homomorphismus von Körpern.*
a) σ *induziert einen Ringhomomorphismus*

$$\begin{aligned} \sigma : K[X] &\longrightarrow K'[X], \\ f = \sum a_i X^i &\mapsto f^\sigma = \sigma f := \sum \sigma(a_i) X^i. \end{aligned}$$

b) Jeder Homomorphismus $\tau : E \longrightarrow E'$*, der* σ *fortsetzt (d.h.* $\tau|_K = \sigma$*), führt Nullstellen von* f *in Nullstellen von* σf *über.*
c) Sei $\sigma : K \longrightarrow K'$ *ein Isomorphismus. Sei* $\alpha \in E$ *algebraisch und* $f = \mathrm{Mipo}_\alpha$*. Sei* $\alpha' \in E'$ *eine Nullstelle von* σf*. Dann gibt es genau eine Fortsetzung* $\tau : K(\alpha) \longrightarrow K(\alpha')$ *von* σ *mit* $\tau(\alpha) = \alpha'$*.*

Definition 4.4.3 Ein Körper C heißt algebraisch abgeschlossen, falls jedes nicht-konstante Polynom $f \in C[X]$ eine Nullstelle in C besitzt.

Satz 4.4.4 *Folgende Aussagen sind äquivalent:*
(i) C ist algebraisch abgeschlossen.
(ii) Jedes irreduzible Polynom in $C[X]$ ist linear.
(iii) Jedes Polynom $f \in C[X]$ vom Grad ≥ 1 zerfällt vollständig in Linearfaktoren.
(iv) Ist E/C eine algebraische Körpererweiterung, so gilt $E = C$.

Satz 4.4.5 *Sei K ein beliebiger Körper. Dann gibt es einen Erweiterungskörper C/K mit folgenden Eigenschaften:*

(i) C ist algebraisch abgeschlossen.

(ii) C/K ist algebraisch.

Der Körper C ist bis auf K-Isomorphie eindeutig bestimmt.

Definition 4.4.6 Der Körper C aus vorigem Satz heißt der algebraische Abschluß von K. Oft schreibt man $C = \bar{K}$.

Die Existenz eines algebraischen Abschluß ist im allgemeinen nicht ganz einfach zu beweisen. Falls $K \subseteq \mathbb{C}$, so können wir einfach

$$C := \{\alpha \in \mathbb{C} | \alpha \text{ ist algebraisch über } K\}$$

wählen.

Satz 4.4.7 *Sei E/K algebraisch und C ein algebraischer Abschluss von E. Sei $\tau\colon E \longrightarrow C$ ein K-Homomorphismus und C' ein Körper mit $E \subseteq C' \subseteq C$. Dann gibt es eine Fortsetzung $\hat{\tau}\colon C' \longrightarrow C$ von τ.*

Definition 4.4.8 Sei $f \in K[X]$ ein nicht-konstantes Polynom. Sei C ein algebraischer Abschluß von K und $\{\alpha_1, \ldots, \alpha_n\}$ die Menge der Nullstellen von f in C. Dann heißt $E := K(\alpha_1, \ldots, \alpha_n)$ ein Zerfällungskörper von f.

Unsere Definition ist abhängig von der Wahl eines algebraischen Abschluss C. Der Zerfällungskörper von f ist jedoch eindeutig bis auf K-Isomorphie.

Einschub: Sei C ein fixierter algebraischer Abschluss von $\mathbb{F}_p$. Sei $K/\mathbb{F}_p$ eine K"orpererweiterung von $\mathbb{F}_p$ mit $K \subseteq C$ und $[K : \mathbb{F}_p] = n < \infty$. Dann gilt $|K| = q := p^n$ und K ist der Zerf"allungsk"orper des Polynoms $g(x) := x^q - x$. Umgekehrt kann man leicht zeigen, dass

$$N := \{\alpha \in C \mid g(\alpha) = 0\}$$

ein K"orper ist. (Beachte dazu: $(\alpha_1 + \alpha_2)^q = \alpha_1^q + \alpha_2^q$.) Bis auf Isomorphie gibt es also genau einen K"orper $\mathbb{F}_q$ mit $q = p^n$ Elementen.

Definition 4.4.9 Eine Körpererweiterung E/K heißt normal, falls für jedes irreduzible Polynom $f \in K[X]$ gilt: Hat f eine Nullstelle in E, so liegen sämtliche Nullstellen (die a priori in einem algebraischen Abschluß C von E liegen) im Körper E.

Der folgende Satz charakterisisiert den wichtigen Begriff "normal".

Satz 4.4.10 *Sei E/K algebraisch und C ein algebraischer Abschluß von E (und damit auch von K). Dann sind folgende Aussagen äquivalent:*

(i) E/K *ist normal.*

(ii) *Für jeden* K*-Homomorphismus* $\sigma : E \longrightarrow C$ *gilt* $\sigma(E) \subseteq E$.

(iii) *Für jeden* K*-Homomorphismus* $\sigma : C \longrightarrow C$ *gilt* $\sigma(E) \subseteq E$.

(iv) *Es gibt eine Menge von Polynomen* $M \subseteq K[X]$*, so daß* $E = K(N)$*, wobei* $N = \{\alpha \in C \mid \alpha$ *ist Nullstelle eines* $f \in M\}$ *die Gesamtheit der Nullstellen in* C *der Polynome in* M *bezeichnet.*

Bemerkung 4.4.11 Insbesondere ist also der Zerfällungskörper eines Polynoms $f \in K[X]$ stets normal über K.

Bemerkung 4.4.12 In (ii) und (iii) kann man jeweils $\sigma(E) \subseteq E$ ersetzen durch $\sigma(E) = E$. Dies folgt aus der folgenden allgemeinen Beobachung: Sei E/K algebraisch und $\sigma\colon E/K \longrightarrow E/K$ eine K-Homomorphismus. Dann ist σ ein Isomorphismus.

Satz 4.4.13 *Sei* E/K *algebraisch.*
a) Es gibt einen Erweiterungskörper E'/E *mit den folgenden Eigenschaften:*

(i) E'/K *ist normal.*

(ii) *Falls* $E'/L/K$ *und* L/K *normal ist, so ist* $E' = L$.

b) Sind E' *und* E'' *zwei solche Körper, so gibt es einen* K*-Isomorphismus*

$$\sigma\colon E'/K \longrightarrow E''/K.$$

c) Ist $[E : K] < \infty$*, so auch* $[E' : K] < \infty$

Definition 4.4.14 Den Körper E' aus Satz 4.4.13 nennt man die normale Hülle von E/K.

4.5 Separabilität

Definition 4.5.1 Sei K ein Körper und C ein algebraischer Abschluß von K. Zwei Elemente $\alpha, \beta \in C$ heißen zueinander konjugiert über K, falls es einen Homomorphismus $\tau : C/K \longrightarrow C/K$ mit $\tau(\alpha) = \beta$ gibt.

Lemma 4.5.2 *Folgende Aussagen sind äquivalent:*
(i) α *und* β *sind zueinander konjugiert über* K.
(ii) β *ist eine Nullstelle von* Mipo_α.
(iii) Es gibt einen Isomorphismus $\tau : K(\alpha)/K \longrightarrow K(\beta)/K$ *mit* $\tau(\alpha) = \beta$.
(iv) $\mathrm{Mipo}_\alpha = \mathrm{Mipo}_\beta$.

Als Konsequenz aus dem Lemma ergibt sich

Folgerung 4.5.3 *Jedes* $\alpha \in C$ *hat höchstens* $\deg(\mathrm{Mipo}_\alpha) = [K(\alpha) : K]$ *viele verschiedene Konjugierte über* K.

Definition 4.5.4 Sei $\alpha \in C$ und $f = \mathrm{Mipo}_\alpha$. Dann heißt die Anzahl der verschiedenen Nullstellen von f in C der Separabilitätsgrad von α (in Zeichen: $[K(\alpha) : K]_s$). Ein Element α heißt separabel über K, falls gilt: $[K(\alpha) : K]_s = [K(\alpha) : K]$. Andernfalls heißt α inseparabel.

Definition 4.5.5 Sei E/K algebraisch. Dann heißt E/K separabel, falls jedes Element $\alpha \in E$ über K separabel ist. Sonst heißt E/K inseparabel.

Die folgenden Bemerkungen sind offensichtlich.

Bemerkung 4.5.6 1) α ist separabel $\iff$ Mipo_α hat nur einfache Nullstellen in C.
2) $[K(\alpha):K]_s \leq [K(\alpha):K]$.
3) $\alpha \in K$ ist stets separabel über K.

Definition 4.5.7 1) Seien E_1 und E_2 zwei Körpererweiterungen von K. Dann bezeichnet $G(E_1/K, E_2/K)$ die Menge der K-Homomorphismen von E_1 in E_2. Falls $E_1 = E_2 = E$, so schreiben wir kürzer $G(E/K) = G(E_1/K, E_2/K)$.
2) Falls E/K algebraisch ist, so nennt man $G(E/K)$ auch die Automorphismengruppe von E/K.

Der folgende Satz ist grundlegend.

Satz 4.5.8 *Sei $[E:K] = n < \infty$ und C ein algebraischer Abschluß von E. Dann gilt:*
i) $|G(E/K, C/K)| \leq n$.
ii) $|G(E/K, C/K)| = n \iff E/K$ ist separabel.

Ein wesentliches Hilfsmittel im Beweis des vorherigen Satzes ist das folgende Lemma.

Lemma 4.5.9 *Sei F ein Zwischenkörper der algebraischen Erweiterung E/K und C der algebraische Abschluss von E. Dann hat man eine Bijektion*

$$G(E/K, C/K) \xrightarrow{\simeq} G(F/K, C/K) \times G(E/F, C/F).$$

Setzen wir $[E:K]_s := |G(E/K, C/K)|$, so erh"alt man

Folgerung 4.5.10 *Sei F ein Zwischenkörper der algebraischen Erweiterung E/K. Dann gilt:*

$$[E:K]_s = [E:F]_s \cdot [F:K]_s$$

Folgerung 4.5.11 *Sei $\alpha \in C$. Dann gilt:*

$$\alpha \text{ ist separabel über } K \iff K(\alpha)/K \text{ ist separabel.}$$

Der Begriff der Separabilität ist transitiv.

Satz 4.5.12 *Sei E/K algebraisch und $K \subseteq L \subseteq E$. Dann gilt:*

$$E/K \text{ ist separabel} \iff E/L \text{ und } L/K \text{ sind separabel.}$$

Satz 4.5.13 *Sei E/K eine Körpererweiterung. Dann sind die folgenden Aussagen äquivalent:*
i) E/K ist endlich und separabel.
ii) Es gibt separable algebraische Elemente $\alpha_1, \ldots, \alpha_n \in E$, so daß $E = K(\alpha_1, \ldots, \alpha_n)$.

Wir erinnern daran, daß für irreduzible Polynome $f \in K[X]$ folgende Äquivalenz gilt:

$$f \text{ separabel} \iff f' \neq 0. \tag{1}$$

Dies impliziert:

Satz 4.5.14 *Sei $char(K) = 0$. Dann ist jedes irreduzible Polynom $f \in k[X]$ separabel. Insbesondere ist jede algebraische Erweiterung von K separabel.*

Eine weitere Konsequenz aus (1) ist das folgende Resultat.

Folgerung 4.5.15 *Sei $char(K) = p > 0$. Sei $f \in K[x]$ irreduzibel. Dann gilt:*

$$f \text{ ist separabel} \iff f \notin K[x^p].$$

Definition 4.5.16 Ein Körper K heißt vollkommen oder perfekt, falls jede algebraischen Erweiterung E/K separabel ist.

Körper K der Charakteristik 0 sind also vollkommen. Wir werden auf dem Übungsblatt zeigen, dass auch alle endlichen Körper K vollkommen sind. Wir notieren hier die Resultate.

Satz 4.5.17 *Sei $char(K) = p > 0$. Sei $K^p := \{\alpha^p \mid \alpha \in K\}$. Dann gilt:*

$$K \text{ ist vollkommen} \iff K^p = K$$

Für eine Körper K der Charakteristik $p > 0$ betrachten wir den sogenannten Frobenius-Homomorphismus

$$\sigma_p \colon K \longrightarrow K, \quad \alpha \mapsto \alpha^p.$$

Falls K endlich ist, so ist σ_p ein Automorphismus und wir erhalten das folgende Korollar.

Folgerung 4.5.18 *Sei $|K| < \infty$. Dann ist K vollkommen.*

5 Galoistheorie

5.1 Der Hauptsatz der Galoistheorie

Definition 5.1.1 Sei E/K eine algebraische Körpererweiterung und $G \leq G(E/K)$. Dann nennt man

$$E^G := \{\alpha \in E \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\}$$

den Fixkörper von E unter G.

Definition 5.1.2 Eine algebraische Erweiterung heißt galoissch, falls $E^{G(E/K)} = K$ gilt.

Der nächste Satz liefert eine äquivalente definierende Eigenschaft.

Satz 5.1.3 *Sei E/K algebraisch. Dann gilt:*

$$E/K \text{ ist galoissch} \iff E/K \text{ ist separabel und normal.}$$

Folgerung 5.1.4 *Sei $f \in K[X]$ separabel und E der Zerfällungskörper von f. Dann ist E/K eine endliche galoissche Erweiterung.*

Sei nun E/K galoissch und F ein Zwischenkörper. Es ist leicht zu beweisen, daß dann E/F ebenfalls galoissch ist. Ferner ist die Zuordung

$$\begin{array}{rccc} \psi\colon \text{Menge der Zwischenkörper von } E/K & \longrightarrow & \text{Menge der Untergruppen von } G(E/K), \\ F & \mapsto & G(E/F) \end{array}$$

injektiv.

Bemerkung 5.1.5 Falls E/K eine endliche Erweiterung ist, so ist $G(E/K)$ eine endliche Gruppe. Wegen der Injektivität von ψ folgt, dass es nur endlich viele Zwischenkörper von E/K gibt.

Man beachte, daß F/K im allgemeinen nicht galoissch ist. Hier gilt:

Satz 5.1.6 *Sei E/K galoissch und F ein Zwischenkörper. Sei $\sigma \in G(E/K)$. Dann gilt:*

$$G(E/\sigma(F)) = \sigma G(E/F)\sigma^{-1}.$$

Ferner sind die folgenden Aussagen äquivalent:
(i) F/K ist galoissch.
(ii) $\sigma(F) = F, \forall \sigma \in G(E/K)$.
(iii) $G(E/F) \lhd G(E/K)$.
In diesem Fall induziert die Restriktion eine Isomorphie von Gruppen

$$G(E/K)/G(E/F) \xrightarrow{\simeq} G(F/K).$$

Lemma 5.1.7 *Sei E/K algebraisch und separabel. Dann ist die normale Hülle E'/K von E/K ebenfalls separabel. Insbesondere ist also E'/K eine Galoiserweiterung.*

Ein wichtiger Schritt auf dem Weg zum Hauptsatz der Galoistheorie ist der sogenannte Satz vom primitiven Element, der auch für sich allein von Bedeutung ist.

Satz 5.1.8 *(Satz vom primitiven Element) Sei E/K endlich und separabel. Dann gibt es ein Element $\alpha \in E$, so daß $E = K(\alpha)$. Man sagt dann auch, die Erweiterung E/K ist einfach.*

Der folgende Satz faßt im wesentlichen unsere bisherigen Resultate dieses Abschnitts zusammen. Neu hinzu kommt nur die Aussage zur Surjektivität im ersten Teil des Satzes.

Satz 5.1.9 *(Hauptsatz der Galoistheorie) Sei E/K eine endliche galoissche Erweiterung. Dann ist die Abbildung*

$$F \mapsto G(E/F)$$

eine Bijektion zwischen der Menge der Zwischenkörper F von E/K und der Menge der Untergruppen U von $G(E/K)$. Ferner gilt:
(i) E/F ist galoissch und $|G(E/F)| = [E : F]$.
(ii) $F_1 \subseteq F_2 \iff G(E/F_2) \leq G(E/F_1)$.
(iii) F/K ist galoissch $\iff G(E/F) \lhd G(E/K)$.
(iv) Falls F/K galoissch ist, so induziert die Restriktion einen Isomorphismus

$$G(E/K)/G(E/F) \xrightarrow{\simeq} G(F/K).$$

Bemerkung 5.1.10 Sei E/K eine endliche Erweiterung. Dann gilt:

$$E/K \text{ ist galoissch} \iff |G(E/K)| = [E : K].$$

Wir haben in der Vorlesung nur die Hinrichtung gezeigt. Die Rückrichtung wird in den Übungen bewiesen.

Der Satz vom primitiven Element impliziert

Folgerung 5.1.11 *Die endlichen galoisschen Erweiterungen E/K sind genau die Zerfällungskörper von separablen Polynomen $f \in K[X]$.*

Definition 5.1.12 Sei $f \in K[X]$ separabel und E/K der Zerfällungskörper von f. Dann nennt man die Galoisgruppe $G(E/K)$ auch die Galoisgruppe von f über K.

Wichtige Beispiele für Galoiserweiterungen sind die Kreisteilungskörper $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ und die endlichen Erweiterungen E/K mit endlichen Körpern K. Diese werden in den nächsten Abschnitten besprochen.

6 Endliche Körper

6.1 Grundlegendes

Lemma 6.1.1 *Sei K ein endlicher Körper und $\mathrm{char}(K) = p > 0$. Dann ist K in natürlicher Weise eine Körpererweiterung von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Sei $d = \dim_{\mathbb{F}_p}(K)$. Dann gilt: $|K| = p^d$.*

Folgerung 6.1.2 *Sei $|K| = q = p^d$. Dann ist K ein Zerfällungskörper von $x^q - x \in \mathbb{F}_p[x]$. Damit ist K durch p und d bis auf Isomorphie eindeutig bestimmt.*

Satz 6.1.3 *Sei C ein algebraischer Abschluss von $\mathbb{F}_p$. Dann gibt es zu jedem $d \in \mathbb{N}$ genau einen Körper $K \subseteq C$ mit p^d Elementen, nämlich den Zerfällungskörper von $x^{p^d} - x$. Der Körper K besteht genau aus den Nullstellen von f.*

Folgerung 6.1.4 *Sei K ein endlicher Körper. Dann gibt es zu jedem $d \in \mathbb{N}$ bis auf Isomorphie genau einen Erweiterungskörper E von K mit $[E : K] = d$.*

Bemerkung 6.1.5 Sei K ein endlicher Körper und $d \in \mathbb{N}$. Dann gibt es in $K[x]$ irreduzible Polynome vom Grad d.

Schließlich untersuchen wir Erweiterungen endlicher Körper hinsichtlich ihrer Galoistheorie.

Satz 6.1.6 *Sei E/K eine Erweiterung von endlichen Körpern. Sei $|K| = q = p^d$. Dann ist E/K galoissch mit zyklischer Galoisgruppe $G(E/K) = \langle \sigma_q \rangle$, wobei $\sigma_q(\alpha) = \alpha^q$ für alle $\alpha \in E$ ist.*

Der Automorphismus σ_q heißt Frobenius-Automorphismus von E/K.

7 Kreisteilungskörper

7.1 Grundlegendes

Definition 7.1.1 Sei K ein Körper und $n \in \mathbb{N}$. Dann heißt

$$W_n(K) := \{\zeta \in K \mid \zeta^n = 1\}$$

Gruppe der n-ten Einheitswurzeln in K. Die Gruppe

$$W(K) := \bigcup_{n \in \mathbb{N}} W_n(K)$$

heißt Gruppe der Einheitswurzeln in K. Eine Einheitswurzel $\zeta \in W_n(K)$ nennt man primitiv (von der Ordnung n), falls $\mathrm{ord}(\zeta) = n$.

Lemma 7.1.2 *Sei K ein Körper und $n \in \mathbb{N}$. Dann ist $W_n(K)$ eine zyklische Gruppe mit*

$$|W_n(K)| \text{ teilt } n.$$

Falls $\mathrm{char}(K) = p > 0$, so ist $W_{np}(K) = W_n(K)$.

Definition 7.1.3 Sei K ein Körper und $n \in \mathbb{N}$. Dann heißt der Zerfällungskörper E von $x^n - 1$ der Körper der n-ten Einheitswurzeln. Wir schreiben kurz $E = K(\sqrt[n]{1})$.

Bemerkung 7.1.4 Sei C ein algebraischer Abschluß von K. Dann gilt: $K(\sqrt[n]{1}) = K(W_n(C))$.

7.2 Galoistheorie von Kreisteilungskörpern

Satz 7.2.1 *Sei $E = K(\sqrt[n]{1})$. Dann ist E/K eine endliche galoissche Erweiterung. Falls* $\mathrm{char}(K) \nmid n$, *so ist die Automorphismengruppe $G(E/K)$ isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$. Insbesondere ist $G(E/K)$ stets abelsch (auch im Fall* $\mathrm{char}(K) \mid n$*).*

Satz 7.2.2 *Sei $E = \mathbb{Q}(\sqrt[n]{1})$. Dann gilt:*

$$G(E/K) \simeq (\mathbb{Z}/n\mathbb{Z})^\times .$$

Insbesondere ist $[E : \mathbb{Q}] = \varphi(n)$ mit der Eulerschen phi-Funktion φ.

Bemerkung 7.2.3 Sei ζ eine primitive n-te Einheitswurzel. Dann ist der Isomorphismus im Satz 7.2.2 gegeben durch

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow G(E/K), \quad \bar{k} \mapsto \sigma_k,$$

wobei σ_k eindeutig festgelegt ist durch $\sigma_k(\zeta) = \zeta^k$. Entscheidend ist, dass man hier eine primitive Einheitswurzel ζ zugrunde legt.

7.3 Kreisteilungspolynome

Im Folgenden sei stets $C = \bar{\mathbb{Q}}$ der algebraische Abschluss von $\mathbb{Q}$ in $\mathbb{C}$.

Definition 7.3.1 Sei $n \in \mathbb{N}$. Das Polynom

$$F_n(x) = \prod_{\zeta \in W_n(C), \mathrm{ord}(\zeta) = n} (x - \zeta)$$

nennt man das n-te Kreisteilungspolynom.

Satz 7.3.2 *a) F_n ist ein normiertes Polynom vom Grad $\varphi(n)$.*
b) Es gilt:

$$x^n - 1 = \prod_{d \mid n} F_d(x).$$

c) $F_n(x) \in \mathbb{Z}[x]$.

Folgerung 7.3.3 *Das n-te Kreisteilungspolynom ist irreduzibel in $\mathbb{Q}[x]$. Sei ζ eine primitive n-te Einheitswurzel. Dann ist F_n das Minimalpolynom von ζ.*

Als Anwendung haben wir uns (zum Teil nur intuitiv) klar gemacht, dass folgender Satz gilt.

Satz 7.3.4 *Das regelmäßige n-Eck kann man genau dann mit Zirkel und Lineal konstruieren, wenn gilt:*

$$n = 2^e p_1 p_2 \cdots p_r$$

mit $e \in \mathbb{N}_0$ und paarweise verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$ von der Gestalt

$$p_i = 1 + 2^{m_i}.$$

7.4 Vertiefungen der Galoistheorie

Satz 7.4.1 *(Translationssatz der Galoistheorie) Sei E/K eine Galoiserweiterung und K'/K eine beliebige Erweiterung. Sei $F := E \cap K'$. Dann gilt:*
a) EK'/K' ist galoissch.
b) Die Restriktionsabbildung $\mathrm{res}\colon G(EK'/K') \longrightarrow G(K/F)$ *ist ein Gruppenisomorphismus.*
c) Falls E/K endlich ist, so auch EK'/K' und $[EK' : K']$ teilt $[E : K]$.

Bemerkung 7.4.2 Vollständig bewiesen haben wir den Translationssatz nur unter der Voraussetzung, dass E/K endlich ist. Im unendlichen Fall funktioniert der Beweis analog, wenn man den Hauptssatz der Galoistheorie auch für unendliche Erweiterungen formuliert und beweist. Dazu muss man zunächst $G(E/K)$ mit einer Topologie versehen, der sogenannten Krulltopologie, und im Hauptsatz der Galoistheorie beliebige Untergruppen H durch abgeschlossene Untergruppen H ersetzen.

Satz 7.4.3 *(Kompositionssatz der Galoistheorie) Seien E_1/K und E_2/K galoissch. Dann gilt:*
a) E_1E_2/K ist galoissch.
b) Der Gruppenhomomorphismus

$$h\colon G(E_1E_2/K) \longrightarrow G(E_1/K) \times G(E_2/K), \quad \sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2})$$

ist injektiv. Das Bild von h ist gegeben durch

$$\Delta := \{(\sigma, \tau) \in G(E_1/K) \times G(E_2/K) \mid \sigma|_{E_1 \cap E_2} = \tau|_{E_1 \cap E_2}\}.$$

Auch diesen Satz haben wir nur unter der Voraussetzung, dass E_1/K und E_2/K endlich sind vollständig bewiesen.