Staatsexamenskurs Algebra LA (vertieft)

Skript: Gruppentheorie 1.

1 Gruppen

Definition 1.1. Eine *Gruppe* ist eine Menge G zusammen mit einer Verknüpfung $\circ\colon G \times G \to G$ so dass

a) $\forall x, y, z \in G : (x \circ y) \circ z = x \circ (y \circ z)$;

b) $\exists e \in G : e \circ x = x = x \circ e \quad \forall x \in G$; ($e$ heißt neutrale Element)

c) $\forall x \in G, \exists y \in G : x \circ y = e = y \circ x$. ($y$ ist das inverse Element x^{-1})

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

Definition 1.2. Eine Teilmenge $U \subseteq G$ heißt eine *Untergruppe* von G falls U selbst eine Gruppe bezüglich der Verknupfung $\circ_G$ ist. Man schreibt $U \leq G$.

Äquivalent: $\emptyset \neq U \subseteq G$ und $\forall h_1, h_2 \in U : h_1 \circ h_2^{-1} \in U$.

Definition 1.3. Die Anzahl $|G|$ der Elemente einer Gruppe G heißt die *Ordnung* von G. Die *Ordnung* $\mathrm{ord}(g)$ des Elements $g \in G$ ist die kleinste $n \in \mathbb{N}$ so dass $g^n = e$, falls n existiert. Falls es keine solche n gibt, ist $\mathrm{ord}(g) = \infty$.

- Seien G eine Gruppe und $g \in G$ ein Element. Dann ist $g = e$ genau dann wenn $\mathrm{ord}(g) = 1$.
- Sei nun G endlich. Die Ordnung $\mathrm{ord}(g)$ teilt $|G|$.

Definition 1.4. Sei $H \leq G$ und $g \in G$. Die *Linksnebenklasse* von g ist $gH = \{g \circ h \mid h \in H\}$. Die *Rechtsnebenklasse* von g ist $Hg = \{h \circ g \mid h \in H\}$.

- Seien $g_1, g_2 \in G$. Ist $g_1 H = g_2 H$ genau dann wenn $g_2^{-1} \circ g_1 \in H$.
  Analog $Hg_1 = Hg_2 \iff g_2 \circ g_1^{-1} \in H$.
- Die Gruppe lässt sich als disjunkter Vereinigung von Links- (bzw. Rechts-) nebenklassen schreiben.

Definition 1.5. Sei $G/H := \{gH \mid g \in G\}$ die Menge aller Linksnebenklassen von $H \leq G$. Der *Index* $[G : H]$ von $H \leq G$ ist die Kardinalität von G/H.

Satz 1.6 (Lagrange)**.** *Sei H eine Untergruppe der endlichen Gruppe G. Dann gilt:* $|G| = [G : H] \cdot |H|$.

Definition 1.7. Eine Untergruppe $H \leq G$ heißt *Normalteiler*, falls $g \circ h \circ g^{-1} \in H$ gilt für alle $g \in G$, $h \in H$. Äquivalent: $gH = Hg$ für alle $g \in G$.
Man schreibt $H \trianglelefteq G$.

• Eine Untergruppe vom Index 2 ist ein Normalteiler.

Satz 1.8. *Sei $H \trianglelefteq G$. Die Menge G/H ist eine Gruppe bezüglich der Verknupfung*

$$(gH) \circ (g'H) = (g \circ g')H.$$

Die Gruppe G/H heißt Faktorgruppe *oder* Quotientengruppe.

Satz 1.9 (Korrespondenzsatz)**.** *Sei G eine Gruppe und N ein Normalteiler von G. Die Untergruppen (bzw. Normalteiler) von G/N entsprechen bijektiv den Untergruppen (bzw. Normalteilern) von G, die N enthalten.*

Definition 1.10.

- Eine Gruppe G heißt *einfach*, falls sie keine Normalteiler außer G und $\{e\}$ hat.
- Sei G eine Gruppe und X eine nichtleere Teilmenge von G. Die Menge $N_G(X) := \{g \in G \mid gXg^{-1} = X\}$ heißt *Normalisator* von X in G.
- Die Menge $Z(G) := \{g \in G \mid g \circ h = h \circ g\,,\ \forall h \in G\}$ heißt *Zentrum* von G.

• Normalisator und Zentrum sind Untergruppen.

2 Besondere Gruppen

a) Eine Gruppe G ist *zyklisch* falls es ein $g \in G$ gibt, so dass $G = \{g^n \mid n \in \mathbb{Z}\}$. Die Ordnung einer zyklischen Gruppe ist die Ordnung des Erzeugers g.

b) Die *Permutationsgruppe* oder *symmetrische Gruppe* von n Ziffern S_n ist die Gruppe aller bijektiven Abbildungen $\{1, \ldots, n\} \to \{1, \ldots, n\}$ $(n \geq 1)$ bezüglich der Verknüpfung *Komposition von Abbildungen*. Die Gruppe hat Ordnung $|S_n| = n!$ und ist nicht abelsch für $n \geq 3$.

- Jede Permutation kann als Produkt disjunkter Zyklen dargestellt werden.
- Die Ordnung eines Produkts disjunkter Zyklen ist das kleinste gemeinsame Vielfache der Ordnungen der Faktoren.
- Ein Zyklus z ist selbst eine Permutation der Ordnung $\text{ord}(z) = \text{Länge}(z)$.
- Seien σ,$(a_1 \ \ldots \ a_k) \in S_n$, dann $\sigma(a_1 \ \ldots \ a_k)\sigma^{-1} = (\sigma(a_1) \ \ldots \ \sigma(a_k))$.

c) Eine Permutation, die genau zwei Elemente vertauscht, heißt *Transposition*.
Sei $\sigma \in S_n$. Dann ist $\sigma = \tau_1 \cdots \tau_k$ für ein $k \in \mathbb{N}$ und Transpositionen $\tau_i \in S_n$. Die Zahl $sgn(\sigma) = (-1)^k$ heißt *Signum* von σ. Die Permutation σ heißt *gerade*, falls $sgn(\sigma) = 1$. Andernfalls heißt σ *ungerade*.

Für ein Zyklus $z \in S_n$ der Länge l gilt $sgn(z) = (-1)^{l-1}$, und die Signum-Funktion ist multiplikativ, d.h. für alle $\sigma_1, \sigma_2 \in S_n$ gilt $sgn(\sigma_1\sigma_2) = sgn(\sigma_1)sgn(\sigma_2)$.

Die *alternierende Gruppe* A_n ist die Gruppe aller geraden Permutationen in S_n. Die Gruppe $A_n \trianglelefteq S_n$ hat Index 2 und Ordnung $\dfrac{n!}{2}$. Für $n \geq 5$ ist A_n einfach.

d) Die *n-te Diedergruppe* $D_n \leq S_n$ $(n \geq 3)$ ist die Symmetriegruppe eines regelmäßigen n-Ecks im $\mathbb{R}^2$ (für $n = 3$ gilt $S_3 = D_3$). Die Gruppe

$$D_n = \langle \sigma, \tau \mid \sigma^n = \tau^2 = id,\ \tau\sigma = \sigma^{-1}\tau \rangle$$

besteht aus n Drehungen: σ^i, $i \in \{0, \ldots, n-1\}$, die eine zyklische Untergruppe der Ordnung n bilden, und n Spiegelungen: $\sigma^i\tau$, $i \in \{0, \ldots, n-1\}$, $\text{ord}(\sigma^i\tau) = 2$;

Die Gruppe hat damit Ordnung $|D_n| = 2n$, und jedes Element von D_n lässt sich *eindeutig* in der Form $\sigma^i\tau^k$ schreiben, mit $i \in \{0, \ldots, n-1\}$ und $k \in \{0, 1\}$.

Staatsexamenskurs Algebra LA (vertieft)

Skript: Gruppentheorie 2.

1 Untergruppen und Faktorgruppen von zyklischen Gruppen

Satz 1.1. *Alle Untergruppen und Faktorgruppen von zyklischen Gruppen sind zyklisch.*

Satz 1.2. *Sei $G = \langle g \rangle$ eine endliche zyklische Gruppe der Ordnung $|G| = n$, und sei $k \in \mathbb{N}$ ein Teiler von n.*
Dann gibt es genau eine Untergruppe $H \leq G$ mit $|H| = k$, und zwar $H = \langle g^{n/k} \rangle$.

2 Klassifikation endlicher abelscher Gruppen

Sei G eine endliche abelsche Gruppe. Dann ist

$$G \cong (\mathbb{Z}/p_1^{n_1}\mathbb{Z})^{s_1} \times (\mathbb{Z}/p_2^{n_2}\mathbb{Z})^{s_2} \times \cdots \times (\mathbb{Z}/p_k^{n_k}\mathbb{Z})^{s_k},$$

wobei p_i Primzahlen (nicht unbedingt verschieden!) und n_i, s_i nicht-negative ganze Zahlen sind. Die Primzahlpotenzen $p_i^{n_i}$ sind bis auf Reihenfolge eindeutig und $|G| = p_1^{n_1 s_1} \cdot p_2^{n_2 s_2} \dots p_k^{n_k s_k}$.

Alternativ, kann man G als Produkt

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_l\mathbb{Z},$$

darstellen, wobei $d_1 > 1$, d_i teilt d_{i+1} für alle $1 \leq i \leq l-1$ und $|G| = d_1 \cdot d_2 \dots d_l$.

Beispiel 1. Sei G die abelsche Gruppe $\mathbb{Z}/30\mathbb{Z} \times (\mathbb{Z}/12\mathbb{Z})^2$, dann ist

$$G \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^3 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}\,.$$

3 Homomorphismen

Definition 3.1. Seien G, H Gruppen. Eine Abbildung $\phi\colon G \to H$ heißt *Gruppenhomomorphismus* falls $\phi(g_1) \circ \phi(g_2) = \phi(g_1 \circ g_2)$ für alle $g_1, g_2 \in G$.

Das *Bild* von ϕ ist eine Untergruppe von H und der *Kern* $\ker\phi := \{g \in G \mid \phi(g) = e\}$ ist ein Normalteiler von G.
Falls ϕ bijektiv ist, heißt ϕ *Isomorphismus* und man schreibt $G \cong H$.

Satz 3.2 (Homomorphiesatz)**.** *Seien $\phi\colon G \to H$ ein Gruppenhomomorphismus und $K := \ker\phi$. Dann ist*

$$\tilde{\phi}\colon G/K \to \operatorname{Im}\phi$$

ein Isomorphismus, wobei $\tilde{\phi}(gK) := \phi(g)$.

Definition 3.3. Seien G eine Gruppe, H eine Untergruppe und N ein Normalteiler von G. Die Menge $N \cdot H := \{nh \mid n \in N,\ h \in H\}$ heißt *Komplexprodukt*, und ist eine Untergruppe von G.

Satz 3.4 (Isomorphiesatz)**.** *Seien G eine Gruppe, $H \leq G$ und $N \trianglelefteq G$.*

1. *Dann ist ein Normalteiler von $N \cdot H < G$ und $H \cap N$ ein Normalteiler von H, und es gilt $H/(H \cap N) \cong (N \cdot H)/N$.*
2. *Falls $N \subset H \triangleleft G$ dann ist N ein Normalteiler von H, H/N ein Normalteiler von G/N und es gilt $(G/N)/(H/N) \cong G/H$.*

4 Gruppenoperationen

Definition 4.1. Seien X eine Menge und G eine Gruppe. Eine *Gruppenoperation* G auf X ist eine Abbildung

$$\phi\colon G \times X \to X, \quad \phi(g, x) = g \cdot x$$

mit den folgenden Eigenschaften:

a) $\phi(g \circ h, x) = \phi(g) \cdot (\phi(h) \cdot x)$ für alle $g, h \in G$, $x \in X$;

b) $\phi(e, x) = x$ für alle $x \in X$.

Eine Gruppenoperation ist ein Gruppenhomomorphismus

$$G \to \mathrm{Sym}(X)\,, g \mapsto (x \mapsto g \cdot x)\,,$$

wobei $\mathrm{Sym}(X)$ die Gruppe aller bijektiven Abbildungen $X \to X$ ist.

Definition 4.2. Sei $x \in X$. Die *Bahn* von x ist die Menge

$$G \cdot x := \{g \cdot x \mid g \in G\} \subseteq X$$

und der *Stabilisator* von x ist die Untergruppe

$$G_x = \{g \in G \mid g \cdot x = x\} \leq G.$$

- Seien $x, y \in X$. Entweder $G \cdot x = G \cdot y$ oder $G \cdot x \cap G \cdot y = \emptyset$.
- Eine Gruppenoperation heißt *transitiv*, falls $G \cdot x = X$ für eine (alle) $x \in X$.
- Eine Gruppenoperation heißt *frei*, falls $G_x = \{e_G\}$ für alle $x \in X$.
- Operiere die Gruppe G auf der endlichen Menge X, dann gilt

$$|G \cdot x| = [G : G_x] \qquad \text{(Bahnformel)}.$$

Satz 4.3 (Bahnengleichung)**.** *Sei G eine Gruppe, die auf der endlichen Menge X operiere. Die Menge $\{G \cdot x_1, \ldots, G \cdot x_r\}$ der Bahnen ist eine Partition von X und es gilt*

$$|X| = \sum_{j=1}^{r} |G \cdot x_j|\,.$$

Staatsexamenskurs Algebra LA (vertieft)

Skript: Gruppentheorie 3.

1 Auflösbare Gruppen

Definition 1.1. Eine endliche Gruppe G heißt *auflösbar* falls es eine Reihe von Untergruppen

$$G =: U_0 \geq U_1 \geq U_2 \geq \cdots \geq U_n := \{e_G\}$$

gibt, so dass für alle $i = 0, \ldots, n-1$ es gilt $U_i \trianglerighteq U_{i+1}$ und U_i/U_{i+1} abelsch.

- Eine abelsche Gruppe ist auflösbar.
- Die symmetrische Gruppe S_n ist genau dann auflösbar, wenn $n \leq 4$ ist.
- Eine Gruppe der Ordnung 2^k ist auflösbar (eine Untergruppe vom Index 2 ist Normalteiler); i.A. ist jede endliche p-Gruppe auflösbar.
- Ist eine Gruppe G auflösbar, so ist jede Untergruppe und jede Faktorgruppe von G auflösbar.

Satz 1.2. *Sei G eine Gruppe und $H \trianglelefteq G$ ein Normalteiler. Dann ist G genau dann auflösbar, wenn G/H und H auflösbar sind.*

Satz 1.3 (Satz von Burnside)**.** *Eine endliche Gruppe der Ordnung $p^a q^b$, wobei p und q Primzahlen und $a, b \in \mathbb{Z}_{\geq 0}$ sind, ist auflösbar.*

2 Sylowsätze

Definition 2.1. Sei G eine endliche Gruppe der Ordnung $|G| = m \cdot p^k$ wobei p eine Primzahl ist und $p \nmid m$.

a) Eine Untergruppe $U \leq G$ der Ordnung p^r, $r \geq 1$ heißt *p-Untergruppe* von G.

b) Eine Untergruppe $U \leq G$ der Ordnung p^k heißt *p-Sylowgruppe* von G.

Satz 2.2 (Sylowsätze)**.** *Sei G eine Gruppe der Ordnung $|G| = m \cdot p^k$, wobei m und p teilerfremd sind, und sei n_p die Anzahl der p-Sylowgruppen von G. Dann gelten:*

1. *Es existiert eine p-Untergruppe der Ordnung p^l für alle $1 \leq l \leq k$.*

2. *Jede p-Untergruppe liegt in einer p-Sylowgruppe, und je zwei p-Sylowgruppen von G sind konjugiert, d.h. für jede U p-Untegruppe und P p-Sylowgruppe von G existiert ein $g \in G$ mit $gUg^{-1} \leq P$.*

3. *Es gilt $n_p \equiv 1 \mod p$ und $n_p \mid m$. Dazu ist $n_p = [G : N_G(P)]$, wobei P eine p-Sylowgruppe von G ist.*

Satz 2.3 (Satz von Cauchy)**.** *Sei G eine endliche Gruppe und p eine Primzahl, die $|G|$ teilt. Dann existiert ein $g \in G$ der Ordnung p.*

Bemerkung 2.4. a) Sei X die Menge aller p-Sylowgruppen in G. Aus dem 2. Satz folgt es, dass G auf X durch konjugation transitiv operiert.

b) Eine p-Sylowgruppe ist genau dann ein Normalteiler von G, wenn $n_p = 1$ gilt.

3 (Semi-)direkte Produkte

Definition 3.1. Seien N und H Gruppen und sei $\psi\colon H \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus, wobei $\mathrm{Aut}(N)$ die Gruppe aller Automorphismenvon N bezeichnet. Das kartesische Produkt $N \times H$ mit der Verknüpfung

$$(n_1, h_1) * (n_2, h_2) = (n_1 \cdot \psi(h_1)(n_2), h_1 \cdot h_2)$$

bildet eine Gruppe, die das *(äußere) semidirekte Produkte* $N \rtimes_\psi H$ genannt wird.
Es gilt: $(n, h)^{-1} = (\psi(h^{-1})(n^{-1}), h^{-1})$ für $n \in N$ und $h \in H$.

Bemerkung 3.2.

- Ist $N \rtimes_\psi H \cong N \times H$ genau dann, wenn ψ trivial ist ($\psi(h) = id_N, \forall h \in H$).
- Ist $N \rtimes_\psi H$ genau dann abelsch, wenn ψ trivial ist und N und H abelsch sind.
- Die Gruppe $G := N \rtimes_\psi H$ hat einen zu N isomorphen Normalteiler $N' := \{(n, e_H) \mid n \in N\}$ und eine zu H isomorphe Untergruppe $H' := \{(e_N, h) \mid h \in H\}$, mit $N' \cap H' = \{e_G\}$ und $N' \cdot H' = G$.

Seien G eine Gruppe, $H \leq G$ und $N \trianglelefteq G$ mit $N \cap H = \{e\}$.

- Die Elemente der Untegruppe $N \cdot H$ lassen sich eindeutig als nh mit $n \in N$ und $h \in H$ schreiben, insbesondere ist $|N \cdot H| = |N| \cdot |H|$.
- Falls $G = N \cdot H$ ist, ist die Abbildung $\phi\colon N \cdot H \to N \times H$, $nh \mapsto (n, h)$ bijektiv, und G ist das *(innere) semidirekte Produkte* $N \rtimes H$.

  Es gilt tatsächlich $N \rtimes H = N \rtimes_\psi H$, wobei der Gruppenhomomorphismus $\psi\colon H \to \mathrm{Aut}(N)$ durch konjugation gegeben ist: $\psi(h) = (n \mapsto hnh^{-1})$.
- Falls $G = N \cdot H$ und $H \trianglelefteq G$ ist, ist $N \cdot H \cong N \times H$ (ϕ ist ein Gruppenisomorphismus).

Staatsexamenskurs Algebra LA (vertieft)

Skript: Ringtheorie 1.

1 Ringe

Definition 1.1. Ein *Ring* (mit Eins) ist eine Menge R zusammen mit zwei Verknüpfungen $+, \cdot \colon R \times R \to R$ so dass

a) $(R, +)$ ist eine abelsche Gruppe,

b) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in R$,

c) es existiert $1 \in R$ so dass $1 \cdot a = a = a \cdot 1$ für alle $a \in R$,

d) $a \cdot (b + c) = a \cdot b + a \cdot c$ für alle $a, b, c \in R$,

e) $(a + b) \cdot c = a \cdot c + b \cdot c$ für alle $a, b, c \in R$.

- Der Ring R heißt *kommutativ* falls $a \cdot b = b \cdot a$ für alle $a, b \in R$.
- R heißt *Nullring* falls $0 = 1$ in R. In dem Fall ist $R = \{0\}$.

Beispiel 1. a) $(\mathbb{Z}, +, \times)$; Für $p \in \mathbb{N}$, $(\mathbb{Z}/p\mathbb{Z}, +, \times)$.

b) Sei R ein Ring. Der *Polynomring* mit Koeffizienten in R ist $R[X] = \{\sum_{i=0}^{n} a_i X^i \mid a_i \in R, n \in \mathbb{N}_0\}$

c) $\mathrm{Mat}(R, n \times n)$, der Ring der $n \times n$-Matrizen mit Einträgen in R.

d) Seien R, S Ringe. Dann ist $R \times S = \{(r, s) \mid r \in R,\ s \in S\}$ das *direkte Produkt* von R und S, wobei $(r, s) + (r', s') = (r + r', s + s')$ und $(r, s) \cdot (r', s') = (r \cdot r', s \cdot s')$.

Definition 1.2. Die Menge $U \subset R$ heißt *Unterring* von R falls $(U, +, \cdot)$ wieder ein Ring ist.

2 Ideale

Sei R ein kommutativer Ring.

Definition 2.1. Die Menge $I \subset R$ heißt *Ideal* falls es gilt:

a) $(I, +)$ ist eine Gruppe,

b) für alle $a \in R$, $x \in I$ gilt $a \cdot x \in I$.

• Seien $I, J \subseteq R$ Ideale, dann sind ihre Summe $I + J := \{a + b \mid a \in I, b \in J\}$ und ihre Schnitt $I \cap J$ noch Ideale.

Definition 2.2. Sei $I \subseteq R$ ein Ideal. Die Menge aller Nebenklassen von I

$$R/I = \{a + I \mid a \in R\}$$

ist der *Quotientenring* mit Verknüpfungen

$$(a + I) + (b + I) = (a + b) + I \text{ und } (a + I) \cdot (b + I) = (a \cdot b) + I.$$

Der *Index* von I in R ist $[R : I] := |R/I|$.

3 Ringhomomorphismen

Definition 3.1. Seien R, S kommutative Ringe. Die Abbildung $\phi\colon R \to S$ heißt *Ringhomomorphismus* falls es gilt:

a) $\phi(a) + \phi(b) = \phi(a + b)$ für alle $a, b \in R$,

b) $\phi(a) \cdot \phi(b) = \phi(a \cdot b)$ für alle $a, b \in R$,

c) $\phi(1_R) = 1_S$.

Der *Kern* von $\phi\colon R \to S$ ist das Ideal $\ker(\phi) = \{a \in R \mid \phi(a) = 0\} \subseteq R$ und das *Bild* von ϕ ist der Unterring $\mathrm{Im}(\phi) = \{\phi(a) \mid a \in R\} \subseteq S$.

Falls ϕ bijektiv ist, heißt ϕ *Ringisomorphismus* und man schreibt $R \cong S$.

Satz 3.2 (Homomorphiesatz)**.** *Sei $\phi\colon R \to S$ ein Ringhomomorphismus. Dann ist $\ker(\phi)$ ein Ideal von R und der Faktorring $R/\ker(\phi)$ ist isomorph zum Bild $\mathrm{Im}(\phi)$.*

Korollar 3.3 (Isomorphiesatz)**.** *Seien R ein kommutativer Ring und $J \subseteq I$ Ideale von R. Dann ist I/J ein Ideal von R/J und es gilt $R/I \cong (R/J)/(I/J)$.*

4 Eigenschaften von Elementen

Definition 4.1. Sei R ein kommutativer Ring.

-) Ein element $a \in R$ heißt eine *Einheit* falls es $b \in R$ existiert, sodass $a \cdot b = 1 = b \cdot a$. Die Menge R^* aller Einheiten in R ist eine Gruppe bezüglich $\cdot$, die *Einheitengruppe*.

-) Ein Element $a \in R$ heißt *nilpotent*, falls es ein $n \in \mathbb{N}$ mit $a^n = 0$ gibt.

-) Ein Element $a \in R$ ist ein *Nullteiler*, falls es ein $b \in R \setminus \{0\}$ mit $a \cdot b = 0$ gibt.

-) Der Ring $R \neq \{0\}$ heißt *Integritätsbereich*, falls 0 der einzige Nullteiler in R ist; und heißt *Körper*, falls $R^* = R \setminus \{0\}$.

• Seien $a, b \in R$ nilpotente Elemente, $c \in R$ und $e \in R^*$. Dann sind $a \pm b$ und ac nilpotent und $e \pm a$ Einheiten.

• Ein Element $a \in R \neq \{0\}$ kann nicht sowohl eine Einheit als auch ein Nullteiler sein.

Satz 4.2. *Seien $R \neq \{0\}$ ein endlicher kommutativer Ring und $a \in R$. Dann ist a entweder eine Einheit oder ein Nullteiler.*

Satz 4.3. *Jeder endlicher Integritätsbereich ist ein Körper.*

Definition 4.4. Sei R ein Integritätsbereich.

a) Ein Element $x \in R$ heißt *irreduzibel* falls es gilt: $x \neq 0$, $x \notin R^*$ und für alle $a, b \in R$ mit $a \cdot b = x$, es folgt dass $a \in R^*$ oder $b \in R^*$.

b) Ein Element $x \in R$ heißt *Primelement* falls es gilt: $x \neq 0$, $x \notin R^*$ und für alle $a, b \in R$ mit $x \mid a \cdot b$, es folgt dass $x \mid a$ oder $x \mid b$.

• Sei R ein Integritätsbereich, dann gilt: Primelemente sind irreduzibel.

Staatsexamenskurs Algebra LA (vertieft)

Skript: Ringtheorie 2.

1 Faktorielle Ringe

Definition 1.1. Ein *euklidischer Ring* R ist ein Integritätsbereich mit einer Abbildung

$$N\colon R \setminus \{0\} \to \mathbb{N}_0\,,$$

sodass für alle $a, b \in R$ mit $b \neq 0$ es existieren $q, r \in R$ mit

$$a = qb + r,\ N(r) < N(b) \text{ oder } r = 0.$$

Definition 1.2. Ein Ideal $I \subseteq R$ heißt *Hauptideal*, falls es ein Element $x \in R$ gibt, so dass $I = xR$. Ein Integritätsbereich R heißt *Hauptidealring*, falls jedes Ideal in R ein Hauptideal ist.

Definition 1.3. Ein Integritätsbereich R heißt *faktoriell*, falls sich jedes Element $x \in R$, $x \neq 0$ bis auf Assoziierte und Reihenfolge eindeutig als Produkt von irreduziblen Elementen schreiben lässt.

- Ein euklidischer Ring ist ein Hauptidealring. Ein Hauptidealring ist ein faktorieller Ring.
- Sei R ein faktorieller Ring. Ein Element $x \in R$ ist genau dann irreduzibel, wenn x ein Primelement ist.

2 Körper

Definition 2.1. Ein Integritätsbereich heißt *Körper*, wenn alle Elemente in $R \setminus \{0\}$ Einheiten sind.

Definition 2.2. a) Ein Ideal $I \subsetneq R$ heißt *Primideal*, falls für alle $x, y \in R$ es gilt: $xy \in I \Rightarrow x \in I$ oder $y \in I$.

b) Ein Ideal $I \subsetneq R$ heißt *maximales Ideal*, falls für alle Ideale J mit $I \subseteq J \subseteq R$ es gilt: $J = I$ oder $J = R$.

Satz 2.3. *Seien R ein kommutativer Ring und $I \subseteq R$ ein Ideal.*

a) Das Ideal I ist genau dann ein Primideal, wenn R/I ein Integritätsbereich ist.

b) Das Ideal I ist genau dann ein maximales Ideal, wenn R/I ein Körper ist.

Korollar 2.4. *Jedes maximales Ideal ist ein Primideal.*

Definition 2.5. Sei R ein Integritätsbereich. Der *Quotientenkörper* $\mathrm{Quot}(R)$ von R ist der Körper aller Brüche in R. Das heißt,

$$\mathrm{Quot}(R) = \left\{ \frac{a}{b} \;\middle|\; a \in R,\ b \in R \setminus \{0\} \right\} / \sim$$

wobei $\frac{a}{b} \sim \frac{c}{d}$ genau dann wenn $ad = bc$.

• Falls K ein Körper ist, ist $K[X]$ ein Hauptidealring. Insbesondere, falls $f \in K[X]$ irreduzibel ist, ist das Ideal $(f) \subseteq K[X]$ maximal.

3 Irreduzibilitätskriterien für Polynome

Satz 3.1. *Sei R ein Integritätsbereich. Es gilt $R[X]^* = R^*$.*

Beweis: Sei $\deg : R[X] \to \mathbb{N} \cup \{-\infty\}, f \mapsto \deg(f)$ die Gradabbildung. Für $a, b \in R[X]$ gilt $\deg(a \cdot b) = \deg(a) + \deg(b)$, weil R ein Integritätsbereich ist (damit kann das Produkt der Leitkoeffizienten nicht 0 werden).
Sei $u \in R[X]^*$: so existiert $v \in R[X]$ mit $1 = u \cdot v$, und so $0 = \deg(1) = \deg(u) + \deg(v)$. Falls u nicht konstant wäre, wäre $\deg(v) = -\deg(u) < 0$, unmöglich! □

Sei R ein faktorieller Ring und sei $f = \sum_{j=0}^{n} a_j x^j \neq 0$ ein Polynom mit Koeffiziente in R.

Definition 3.2. Das Polynom $f \in R[X]$ heißt *irreduzibel*, wenn $f \neq 0$ nicht invertierbar in $R[X]$ ist und für $g, h \in R[X]$ mit $f = gh$ entweder g oder h invertierbar ist.

Definition 3.3. Das Polynom f heißt *primitiv*, falls seine Koeffizienten teilerfremden sind, d.h. $\mathrm{ggT}(a_0, \ldots, a_n) \in R^*$.

Nunmehr sei f dazu nicht konstant.

Satz 3.4 (Lemma von Gauß)**.** *Das Polynom f ist genau dann irreduzibel in $R[x]$, wenn f primitiv und irreduzibel in* $\mathrm{Quot}(R)[x]$ *ist.*

Satz 3.5 (Eisensteinkriterium)**.** *Falls ein Primelement $p \in R$ existiert mit $p \nmid a_n$, $p \mid a_j$ für alle $j \in \{0, \ldots, n-1\}$ und $p^2 \nmid a_0$ existiert, dann ist f irreduzibel in* $\mathrm{Quot}(R)[x]$.

Satz 3.6. *Sei R ein Körper. Dann:*
i) ist jedes Polynom vom Grad 1 irreduzibel.
ii) ist jedes Polynom vom Grad 2 oder 3 genau dann irreduzibel, wenn es keine Nullstelle in R besitzt.

3.1 Polynome mit ganzzahlige Koeffizienten

Satz 3.7 (Satz über rationale Nullstellen)**.** *Sei $R = \mathbb{Z}$, also sei $\in \mathbb{Z}[X]$ ein Polynom vom Grad n. Ist $x_0 = \frac{p}{q}$ (wobei $p, q \in \mathbb{Z}$ teilerfremd sind) eine rationale Nullstelle von f, dann ist a_0 durch p teilbar und a_n durch q teilbar.*

Satz 3.8 (Koeffizientenreduktion)**.** *Sei $R = \mathbb{Z}$ und sei $p \in \mathbb{N}$ eine Primzahl mit $a_n \not\equiv 0 \mod p$. Ist*

$$\overline{f} = \sum_{j=0}^{n} \overline{a_j} X^j$$

irreduzibel in $\mathbb{F}_p[X]$, so ist f irreduzibel in $\mathbb{Q}[X]$.

Beispiel 1. ⋄ Das Polynom $2X^2 + 6$ ist irreduzibel in $\mathbb{Q}[X]$ nach dem Eisentsteinskriterium mit Primzahl $p = 3$, aber es ist nicht irreduzibel in $\mathbb{Z}[X]$: $2X^2 + 6 = 2 \cdot (X^2 + 3)$ und $2, X^2 + 3 \notin \mathbb{Z}[X]^* = \mathbb{Z}^* = \{\pm 1\}$.
⋄ Das Polynom $f(X) = 4X^2 + 4$ ist irreduzibel in $\mathbb{Q}[X]$ nach dem Reduktionskriterium mit $p = 3$: $\bar{f}(X) = X^2 + 1$ ist irreduzibel in $\mathbb{F}_3[X]$; aber f ist nicht irreduzibel in $\mathbb{Z}[X]$: $4X^2 + 4 = 4 \cdot (X^2 + 1)$ und $4, X^2 + 1 \notin \mathbb{Z}[X]^*$.

Staatsexamenskurs Algebra LA (vertieft)

Skript: Zahlentheorie.

1 Größte gemeinsame Teiler

Definition 1.1. Ein *größter gemeinsame Teiler* (ggT) zweier ganzer Zahlen m und n ist eine natürliche Zahl $d \in \mathbb{N}_0$ mit der Eigenschaft, dass sie Teiler sowohl von m als auch von n ist und dass jede ganze Zahl, die ebenfalls die Zahlen m und n teilt, ihrerseits Teiler von d ist.

Bemerkung 1.2. Es ist $\mathrm{ggT}(0,0) = 0$, also $\mathrm{ggT}(a,0) = |a|$ für alle $a \in \mathbb{Z}$.

Satz 1.3 (Lemma von Bézout)**.** *Seien $m, n \in \mathbb{Z}$, dann existieren $s, t \in \mathbb{Z}$ mit*

$$\mathrm{ggT}(m,n) = s \cdot m + t \cdot n\,.$$

2 Die Euler'sche φ-Funktion

Definition 2.1. Für $n \in \mathbb{N}$ ist $\varphi(n)$ als die Anzahl der zu n teilerfremden natürlichen Zahlen, die nicht größer als n sind:

$$\varphi(n) := |\{1 \le l \le n \mid \mathrm{ggT}(l,n) = 1\}|\,.$$

Die Abbildung $\varphi : \mathbb{N} \to \mathbb{N}$ heißt *Euler'sche φ-Funktion.*

$\diamond$ Falls $\mathrm{ggT}(m,n) = 1$ ist, gilt $\varphi(mn) = \varphi(m)\varphi(n)$.

$\diamond$ Falls p eine Primzahl ist, gilt $\varphi(p^k) = p^{k-1}(p-1)$ für alle $k \in \mathbb{N}$.

Satz 2.2 (Satz von Euler)**.** *Seien a, n teilerfremde natürliche Zahlen, dann*

$$a^{\varphi(n)} \equiv 1 \mod n\,,$$

wobei $\varphi(n)$ die eulersche φ-Funktion bezeichnet.

Satz 2.3 (Der kleine Fermat)**.** *Seien $a \in \mathbb{N}$ und p eine Primzahl, dann*

$$a^p \equiv a \mod p\,.$$

3 Einheiten von $\mathbb{Z}/n\mathbb{Z}$

• Sei $n \in \mathbb{N}$. Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^*$ hat Ordnung $\varphi(n)$:

$$\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^* \iff \exists b \in \mathbb{Z} : a \cdot b \equiv 1 \mod n \iff \mathrm{ggT}(a,n) = 1\,.$$

Bemerkung 3.1. Der Satz von Euler lautet einfach, dass die Ordnung von $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ die Ordnung der Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ teilt.

Satz 3.2 (Einheiten von $\mathbb{Z}/n\mathbb{Z}$)**.** *Sei $p_1^{e_1} \cdots p_k^{e_k}$ die Primfaktorzerlegung von n. Es gilt:*

- $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{e_k}\mathbb{Z})^*$;
- $(\mathbb{Z}/2^e\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z}$ *für* $e \ge 2$;
- $(\mathbb{Z}/p^e\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{e-1}\mathbb{Z}$ *für* $e \ge 1$ *und p ungerade Primzahl.*

4 Chinesischer Restsatz

Satz 4.1 (Chinesischer Restsatz)**.** *Sei R ein kommutativer Ring, und seien $I_1, \ldots, I_k$ paarweise teilerfremde Ideale von R, d.h. $I_i + I_j = R$, $i \neq j$. Dann ist die Abbildung*

$$\begin{array}{rcl} \pi\colon R/(I_1 \cap \ldots \cap I_k) & \longrightarrow & R/I_1 \times \ldots \times R/I_k \\ x + (I_1 \cap \ldots \cap I_k) & \longmapsto & (x + I_1, \ldots, x + I_k) \end{array}$$

ein Isomorphismus.

Korollar 4.2. *Seien p, q teilerfremde natürliche Zahlen. Dann ist die Abbildung*

$$f : \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}\,, \quad f(u + pq\mathbb{Z}) = (u + p\mathbb{Z}, u + q\mathbb{Z})\,.$$

ein Ringisomorphismus.

Dr. Davide Frapporti

Staatsexamenskurs Algebra LA (vertieft)

Skript: Körpertheorie 1.

1 Körpererweiterungen

Definition 1.1. Seien K, L Körpern. Eine *Körpererweiterung* ist eine inklusion $K \subseteq L$; L ist ein Vektorraum über K, und der *Grad* der Erweiterung ist $[L : K] := \dim_K L$.

Definition 1.2. $K \subseteq L$ heißt *endlich* falls $[L : K] < \infty$. Sonst heißt $K \subseteq L$ *unendlich.*

Satz 1.3 (Gradformel)**.** *Sei $K \subseteq L \subseteq M$ eine Kette von endlichen Körpererweiterungen. Dann gilt:*

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

Definition 1.4. Ein Element $\alpha \in L$ heißt *algebraisch* über K, falls es ein Polynom $f(X) \in K[X]$ gibt, mit $f(\alpha) = 0$. Falls es kein solches Polynom gibt, heißt α *tranzendent* über K.

Eine Körpererweiterung $K \subseteq L$ heißt *algebraisch*, falls α algebraisch über K ist, für alle $\alpha \in L$.

2 Einsetzungshomomorphismus

Sei $K \subseteq L$ eine Körpererweiterung und sei $\alpha \in L$. Der *Einsetzungshomomorphismus* ist

$$\phi_\alpha \colon K[X] \to L,\ g(X) \mapsto g(\alpha).$$

- Der Kern ist das Ideal aller Polynomen $f(X) \in K[X]$ mit $f(\alpha) = 0$.
- Das Bild ist der Ring aller Polynomen in α und ist mit $K[\alpha] \subseteq L$ bezeichnet.

2.1 Fall 1: α algebraisch

Definition 2.1. Sei $\alpha \in L$ algebraisch über K. Das *Minimalpolynom* von α in $K[X]$ ist ein normiertes irreduzibles Polynom $\mu(X) \in K[X]$ mit $\mu(\alpha) = 0$.

- Das Minimalpolynom $\mu(X)$ erzeugt den Kern von ϕ_α ($K[X]$ ist ein Hauptidealring und L ist ein Integritätsbereich).
- Das Bild $K[\alpha]$ ist isomorph zu $K[X]/(\mu(X))$ (Homomorphiesatz) und daher ist $K[\alpha]$ ein Körper.

Es folgt, dass $K(\alpha) = \mathrm{Quot}(K[\alpha]) = K[\alpha]$.

2.2 Fall 2: α tranzendent

Falls α tranzendent ist, ist $\ker \phi_\alpha = \{0\}$. Daher ist $K[\alpha] \cong K[X]$ und der Quotientenkörper $K(\alpha)$ ist nicht isomorph zu $K[\alpha]$.

Definition 2.2. Eine Körpererweiterung $K \subseteq K(\alpha)$ heißt *einfach.* Falls α algebraisch ist, ist $[K(\alpha) : K] = \deg \mu(X)$. Falls α tranzendent ist, ist $[K(\alpha) : K] = \infty$.

3 Endliche Körper

Sei R ein Ring mit 1 und betrachte den Ringhomomorphismus $\psi\colon \mathbb{Z} \to R, 1 \mapsto 1_R$. Dann ist $\ker\psi$ ein Ideal in $\mathbb{Z}$ und existiert $n \in \mathbb{N}_0$ mit $\ker\psi = (n)$: n heißt die *Charakteristik* von R: $n = \operatorname{char} R$.

Falls K ein Körper ist (insbesonders ein Integritätsbereich), ist die Charakteristik $\operatorname{char} K$ entweder 0 oder eine Primzahl $p > 0$.

Definition 3.1. Sei $p \in \mathbb{Z}$ eine Primzahl. Der *endliche Körper* $\mathbb{F}_p$ mit p Elementen ist isomorph zu $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ und hat Charakteristik p.

Satz 3.2. *Die Ordnung eines endlichen Körpers ist eine Primzahlpotenz.*

Umgekehrt, sei p eine Primzahl und $q = p^k$ mit $k \in \mathbb{N}_{>0}$. Sei $\mathbb{F}_q$ die Menge aller Nullstellen von $X^q - X \in \mathbb{F}_p[X]$. Dann ist $\mathbb{F}_q$ ein Körper mit q Elementen, $\operatorname{char}\mathbb{F}_q = p$ *und $\mathbb{F}_q$ ist eindeutig bis auf Isomorphie.*

Bemerkung 3.3. Für $n > 1$ ist der Ring $\mathbb{Z}/p^n\mathbb{Z}$ kein Körper. Insbesondere ist der Körper $\mathbb{F}_{p^n}$ *nicht isomorph* zu $\mathbb{Z}/p^n\mathbb{Z}$.

Satz 3.4. *Sei p eine Primzahl und $m, n \in \mathbb{N}_{>0}$. Dann gilt*

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n\,.$$

Satz 3.5. *Die Einheitsgruppe $\mathbb{F}_q^*$ des endlichen Körpers $\mathbb{F}_q$ ist eine zyklische Gruppe mit $q-1$ Elementen:* $\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$.

4 Zerfällungskörper

Definition 4.1. Sei K ein Körper und sei $P(X) \in K[X]$ ein nichtkonstantes Polynom mit Koeffizienten in K. Der *Zerfällungskörper* von P über K ist die kleinste Körpererweiterung $K \subset L$, über der P in Linearfaktoren zerfällt, d.h. P lässt sich schreiben als

$$P(X) = \lambda \cdot (X - \alpha_1) \cdots (X - \alpha_n)\,, \quad \text{mit} \quad \lambda \in K,\ \alpha_i \in L\,.$$

• Der Zerfällungskörper von $P(X)$ über K ist $L = K(\alpha_1, \ldots, \alpha_n)$, wobei α_i die Nullstellen von $P(X)$ sind; d.h. L wird durch Adjunktion der Nullstellen erzeugt.

Staatsexamenskurs Algebra LA (vertieft)

Skript: Körpertheorie 2.

1 Algebraischer Abschluss

Definition 1.1. Ein Körper K heißt *algebraisch abgeschlossen*, falls jedes nichtkonstante Polynom mit Koeffizienten in K eine Nullstelle in K besitzt.

Satz 1.2 (Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Definition 1.3. Eine algebraische Körpererweiterung $K \subseteq L$ ist ein *algebreischer Abschluss*, falls L algebraisch abgeschlossen ist.

2 Automorphismen

Definition 2.1. Sei $K \subset L$ eine Körpererweiterung. Ein *K-Automorphismus* $\phi\colon L \to L$ ist ein Körperisomorphismus sodass $\phi(\beta) = \beta$ für alle β in K gilt.

Definition 2.2. Die Gruppe $\mathrm{Aut}(L/K)$ aller K-Automorphismen $L \to L$ heißt die *Automorphismengruppe* von L über K (oder auch $\mathrm{Gal}(L/K)$ bzw. *Galoisgruppe*).

Satz 2.3 (Fortsetzungsatz)**.** *Sei $K \subset L$ eine algebraische Körpererweiterung, $\alpha \in L$ und $\mu \in K[X]$ das Minimalpolynom von α über K. Dann:*

- *Für alle $\phi \in \mathrm{Aut}(L/K)$ ist $\phi(\alpha)$ eine Nullstelle von μ.*
- *Umgekehrt, falls $\alpha' \in L$ eine Nullstelle von μ ist, existiert ein $\phi \in \mathrm{Aut}(L/K)$ mit $\phi(\alpha) = \alpha'$.*

3 Einheitswurzeln

Definition 3.1. Eine n-te *Einheitswurzel* ζ ist eine komplexe Nullstelle des Polynoms $X^n - 1 \in \mathbb{Q}[X]$.

- Es gibt genau n verschiedene n-te Einheitswurzeln: $\zeta_k = \exp(\frac{2\pi i k}{n})$, $k = 1, \ldots, n$.
- Die Menge $\mathbb{E}_n$ aller n-te Einheitswurzeln ist eine zyklische Gruppe bezüglich $\times$.

Definition 3.2. ζ heißt *primitiv*, falls $\zeta^m \neq 1$ für $m \in \{1, \ldots, n-1\}$ gilt.

• Die primitive Einheitswurzeln sind $\zeta_k = \exp(\frac{2\pi i k}{n})$, wobei $\mathrm{ggT}(k, n) = 1$.

Definition 3.3. Das n-te Kreisteilungspolynom ist

$$\Phi_n := \prod_{\substack{1 \leq k \leq n \\ \mathrm{ggT}(k,n)=1}} (X - \zeta_k)\,,$$

und hat Grad $\varphi(n)$.

Beispiel 1. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$.
Für p Primzahl ist $\Phi_p(X) = X^{p-1} + \ldots + X + 1$.

• Es gilt $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

4 Elementarsymmetrische Polynome

Die elementarsymmetrische Polynome in Unbekannten $z_1, \ldots, z_n$ sind

$$\begin{aligned}
\sigma_0 &= 1 \\
\sigma_1 &= z_1 + \cdots + z_n \\
\sigma_2 &= z_1 z_2 + z_1 z_3 + \cdots + z_{n-1} z_n \\
\sigma_3 &= z_1 z_2 z_3 + z_1 z_2 z_4 + \cdots + z_{n-2} z_{n-1} z_n \\
&\vdots \\
\sigma_n &= z_1 z_2 \cdot \cdots \cdot z_n
\end{aligned}$$

Ein Polynom $P(z_1, \ldots, z_n)$ heißt *symmetrisch* falls es gilt $P(z_{\rho(1)}, \ldots, z_{\rho(n)}) = P(z_1, \ldots, z_n)$ für alle $\rho \in S_n$.

Satz 4.1. *Jedes symmetrische Polynom $P(z_1, \ldots, z_n)$ in $k[z_1, \ldots, z_n]$ lässt sich als Polynom in $\sigma_0, \ldots, \sigma_n$ schreiben.*

Satz 4.2 (Wurzelsatz von Vieta)**.** *Es seien R ein Intrgritätsbereich,*

$$p(X) = X^n + a_1 X^{n-1} + a_2 X^{n-2} + \cdots + a_n$$

ein Polynom mit Koeffizienten in R und $x_1, \ldots, x_n$ die (mit Vielfachheit gezählten) Nullstellen von p in einem algebraischen Abschluss von dem Quotientkörper $\mathrm{Quot}(R)$*. Dann gilt*

$$a_k = (-1)^k \sigma_k(x_1, \ldots, x_n) \qquad \forall k = 1, \ldots, n.$$

Insbesondere, $a_1 = -(x_1 + \cdots + x_n)$, und $a_n = (-1)^n x_1 \cdots x_n$.

Dr. Davide Frapporti

Staatsexamenskurs Algebra LA (vertieft)

Skript: Galoistheorie.

1 Normal und separabel Körpererweiterungen

Definition 1.1. Die algebraische Körpererweiterung $k \subset L$ heißt *normal*, falls die folgende Bedingung erfüllt ist: sei $f \in k[X]$ ein irreduzibles Polynom mit einer Nullstelle in L, dann zerfällt f in Linearfaktoren über L.

Definition 1.2. Ein Polynom $f \in k[X]$ heißt *separabel*, wenn f in einem algebraischen Abschluss von k nur einfache Nullstellen hat.

Sei $k \subset L$ eine Körpererweiterung. Ein Element $\alpha \in L$ heißt *separabel* über k, falls α algebraisch ist und sein Minimalpolynom über k separabel ist.

Die Körpererweiterung heißt *separabel* falls jedes Element $\alpha \in L$ separabel über k ist.

- Ein nicht konstantes Polynom $\in k[X]$ ist genau dann separabel, wenn f und f' teilerfremd sind.
- Falls $\operatorname{char} k = 0$ ist, ist jedes irreduzibles Polynom f separabel, da f und f' teilerfremd sind.
- Jede algebraische Erweiterung des endlichen Körpers $\mathbb{F}_q$ ist separabel ($\mathbb{F}_q$ ist *perfekt* oder *vollkommen*).

2 Galoissche Körpererweiterungen

Definition 2.1. Die Körpererweiterung $k \subset L$ heißt *galoissch*, falls L normal und separabel über k ist.

- Sei k ein Körper. Der Zerfällungskörper L eines separablen Polynoms $f \in k[X]$ ist galoissch über k.
- Insbesonders falls $\operatorname{char} k = 0$ ist, ist der Zerfällungskörper eines Polynoms galoissch.

Definition 2.2. Sei k ein Körper.

i) Sei L/k eine galoissche Erweiterung. Die Menge aller k-Automorphismen $\operatorname{Gal}(L/k)$ ist eine Gruppe, und heißt die *Galoisgruppe* der Erweiterung.

ii) Sei $f \in K[X]$ ein nicht konstantes separables Polynom. Die *Galoisgruppe* $\operatorname{Gal}(f)$ *von* f ist die Galoisgruppe $\operatorname{Gal}(\operatorname{Zerf}_k(f)/k)$ des Zerfällungskörpers $\operatorname{Zerf}_k(f)$ von f über k.

- Sei $k \subset L$ endlich und galoissch. Dann ist $|\operatorname{Gal}(L/k)| = [L : k]$.
- Für ein nicht konstantes separables Polynom $f \in K[X]$ gilt: $\operatorname{Gal}(f) \leq S_{\deg(f)}$. Insbesondere gilt: $|\operatorname{Gal}(f)|$ teilt $\deg(f)$!.
- Sei Φ_n das n-te Kreisteilungspolynom, dann $\operatorname{Gal}(\Phi_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

3 Hauptsatz der Galoistheorie

Definition 3.1. Seien $k \subset L$ eine endliche Galoiserweiterung und $H \leq \mathrm{Gal}(L/k)$ eine Untergruppe. Der *Fixkörper* L^H (oder $\mathrm{Fix}(H)$) von H ist

$$L^H := \{\alpha \in L \mid \phi(\alpha) = \alpha \ \forall \phi \in H\}.$$

Satz 3.2 (Hauptsatz der Galoistheorie)**.** *Sei $k \subset L$ eine endliche Galoiserweiterung. Die Abbildung*

$$\{\textit{Untergruppen von } \mathrm{Gal}(L/k)\} \xrightarrow{\sim} \{\textit{Zwischenkörper von } L/k\}, H \mapsto L^H$$

ist eine Bijektion mit Umkehrfunktion $M \mapsto \mathrm{Gal}(L/M)$. Weiterhin:

a) Die Abbildung ist inklusionsumkehrende: $H_1 > H_2 \Leftrightarrow L^{H_1} \subset L^{H_2}$;

b) Indexe und Grade sind gleich: $[H_1 : H_2] = [L^{H_2} : L^{H_1}]$;

c) Für $\sigma \in \mathrm{Gal}(L/k)$ gilt $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$ und $\mathrm{Gal}(L/\sigma M) = \sigma \,\mathrm{Gal}(L/M)\sigma^{-1}$;

d) $\mathrm{Gal}(L/M) \trianglelefteq \mathrm{Gal}(L/k)$ ist genau dann ein Normalteiler, wenn die Erweiterung M/k normal (daher galoissch) ist. In diesem Fall gilt $\mathrm{Gal}(M/k) \cong \mathrm{Gal}(L/k)/\mathrm{Gal}(L/M)$.

Satz 3.3 (Translationssatz-Produktsatz)**.** *Seien L/k eine Körpererweiterungen von k, und seien E_1/k und E_2/k Zwischenkörper.*

a) Ist E_1/k eine endliche Galoiserweiterung, so sind auch $E_1 \cdot E_2/E_2$ und $E_1/E_1 \cap E_2$ galoissch mit $\mathrm{Gal}(E_1 \cdot E_2/E_2) \cong \mathrm{Gal}(E_1/E_1 \cap E_2)$.

b) Sind E_1/k und E_2/k endliche Galoserweiterungen, dann ist $E_1 \cdot E_2/k$ eine endliche Galoiserweiterung, und ist der Homomorphismus

$$\mathrm{Gal}(E_1 \cdot E_2/k) \to \mathrm{Gal}(E_1/k) \times \mathrm{Gal}(E_2/k), \sigma \mapsto (\sigma_{|E_1}, \sigma_{|E_2})$$

injektiv, und für $E_1 \cap E_2 = k$ sogar bijektiv.

4 Satz vom primitiven Element

Satz 4.1 (Satz vom primitiven Element)**.** *Seien $\gamma_1, \ldots, \gamma_{n-1}$ separabel über den Körper k und ist γ_n algebraisch über k, dann ist $k(\gamma_1, \ldots, \gamma_n)$ eine einfache Körpererweiterung von k; d.h. es gibt ein $\gamma \in k(\gamma_1, \ldots, \gamma_n)$ mit $k(\gamma_1, \ldots, \gamma_n) = k(\gamma)$.*

Korollar 4.2. *Jede endliche separable Körpererweiterung ist einfach.*

Satz 4.3 (Konstruktive Version des Satzes vom primitiven Element)**.**
Sei k ein unendlicher Körper und sei $L = k(\alpha, \beta)$, wobei α algebraisch und β separabel über k ist. Sei A die Menge der Nullstellen des Minimalpolynoms $M_{\alpha,k}$ von α über k und B die Menge der Nullstellen des Minimalpolynoms $M_{\beta,k}$ von β über k (im Zerfällungskörper Z von $M_{\alpha,k} \cdot M_{\beta,k}$). Wähle

$$\gamma \in k \setminus \left\{ \frac{a - \alpha}{b - \beta} \mid a \in A, \quad b \in B \setminus \{\beta\} \right\},$$

so ist $L = k(\alpha + \gamma\beta)$.