Staatsexamenskurs Algebra LA (vertieft) WS 2019/2020

Skript: Gruppentheorie 1. 15.10.2019

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 Inverseelement 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 $\mathrm{ord}(g) = \infty$.

Satz 1.4. *Sei U eine Untergruppe der endlichen Gruppe G. Dann gilt: $|U|$ teilt $|G|$.*

- 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 $|G|$.
- Eine Gruppe G ist *Zyklisch* falls es $g \in G$ gibt, so dass $G = \{g^n \mid n \in \mathbb{Z}\}$. Die Ordnung einer zyklischen Gruppe ist die Ordnung des Elements g.
- Die *Permutationsgruppe* oder *Symmetriegruppe* von n Ziffern S_n ist die Gruppe aller bijektiven Abbildungen $\{1, \ldots, n\} \to \{1, \ldots, n\}$ bezüglich der Verknupfung *komposition von Abbildungen*. Die Gruppe hat Ordnung $|S_n| = n!$

Definition 1.5. 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 $g, g' \in G$. Ist $gH = g'H$ genau dann wenn, es $h \in H$ existiert, so dass $g \circ h = g'$.
- Die Nebenklasse eH ist (mengenweise) H.
- Die Gruppe lässt sich als disjunkter Vereinigung von Linksnebenklassen (bzw. Rechts-) schreiben.

Definition 1.6. Der *Index* von $H \leq G$ ist die Anzahl der Linksnebenklassen von H in G.

Sei $G/H := \{gH \mid g \in G\}$ die Menge aller Linksnebenklassen von $H \leq G$.

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

Äquivalent: $gH = Hg$ für alle $g \in G$.
Eine Untergruppe vom Index 2 ist immer 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.

Skript: Gruppentheorie 2. 22.10.2019

1 Homomorphismen

Definition 1.1. 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* ist ein Normalteiler von G.

Falls ϕ bijektiv ist, heißt ϕ einen *Isomorphismus*. Man schreibt $G \cong H$.

Satz 1.2 (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 $\tilde{\phi}(gK) := \phi(g)$.

2 Gruppenoperationen

Definition 2.1. Sei 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 $G \to \operatorname{Sym}(X)$ wobei $\operatorname{Sym}(X)$ die Gruppe aller bijektiven Abbildungen $X \to X$ ist.

Definition 2.2. Sei $x \in X$. Die *Bahn* von x ist die Menge

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

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 $B_x = B_y$ oder $B_x \cap B_y = \emptyset$.

Die Gruppenoperation heißt *transitiv* falls $B_x = X$ für eine (alle) $x \in X$.

Die Gruppe G operiere auf der endlichen Menge X. Dann gilt

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

Satz 2.3 (Klassengleichung)**.** *Die Gruppe G operiere auf der endlichen Menge X. Sei R ein Repräsentantensystem für die Menge aller Bahnen. Dann gilt*

$$|X| = \sum_{x \in R} [G : G_x].$$

Skript: Gruppentheorie 3. 29.10.2019

1 Klassifikation endlicher abelscher Gruppen

Sei G eine endliche abelsche Gruppe. Dann ist

$$G \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_2^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z},$$

wobei p_i Primzahlen und n_i naturliche Zahlen sind. Die Primzahlpotenzen $p_i^{n_i}$ sind bis auf Reihenfolge eindeutig und $|G| = p_1^{n_1} \cdot p_2^{n_2} \dots p_k^{n_k}$.
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 $|G| = d_1 \cdot d_2 \dots d_l$.

2 Sylowsätze

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

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

Es existiert eine p-Untergruppe der Ordnung p^l für alle $1 \leq l \leq k$.
Jede p-Untergruppe liegt in einer p-Sylowgruppe.

Satz 2.3 (Sylowsätze)**.** *Sei G eine Gruppe der Ordnung $|G| = n \cdot p^k$ wobei n und p teilerfremd sind und n_p die Anzahl der p-Sylowgruppen von G. Dann gilt:*

a) $n_p \equiv 1 \mod p$, insbesondere ist $n_p \geq 1$;

b) $n_p \mid n$;

c) sind U, U' zwei p-Sylowgruppen dann existiert ein $g \in G$ so dass $U' = gUg^{-1}$.

Sei X die Menge aller p-Sylowgruppen in G. Aus Teil c) folgt es, dass G auf X durch konjugation transitiv operiert.

Definition 2.4. Der *Normalisator* von der p-Sylowgruppe $U \leq G$ ist der Stabilisator bei der konjugation Operation.

Bemerkung 2.5. Eine p-Sylowgruppe ist Normalteiler von G genau dann wenn $n_p = 1$ gilt.

2.1 Innere direkte Produkt

Seien $M \leq G$, $N \trianglelefteq G$. Dann ist $M \cdot N := \{mn \mid m \in M,\ n \in N\}$ eine Untergruppe in G.

- Falls $M \cdot N = G$ und $M \cap N = \{e\}$, ist die Abbildung $\phi\colon M \cdot N \to M \times N, m \cdot n \mapsto (m, n)$ bijektiv.
- Falls $M \trianglelefteq G$ und $M \cap N = \{e\}$, ist $M \cdot N \cong M \times N$ (ϕ ist ein Gruppenisomorphismus).

3 Auflösbare Gruppen

Definition 3.1. 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.
- Eine Gruppe der Ordnung 2^k ist auflösbar (eine Untergruppe vom Index 2 ist Normalteiler).

Satz 3.2. *Sei G eine Gruppe und $H \trianglelefteq G$ Normalteiler. Dann ist G auflösbar genau dann wenn G/H und H auflösbar sind.*

Staatsexamenskurs Algebra LA (vertieft) WS 2019/2020

Skript: Ringtheorie 1. 05.11.2019

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) $(\mathbb{Z}, +, \times)$

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) $\mathrm{Mat}(R, n \times n)$ $n \times n$-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 $a \in R$, $x \in I$ es gilt $a \cdot x \in I$.

(In einem nicht kommutativen Ring spricht man von Links-, Rechts- und beidseitigen Idealen.)

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

Seien R, S kommutative Ringe.

Definition 3.1. 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 $\mathrm{Im}(\phi) = \{\phi(a) \mid a \in R\} \subseteq S$.

4 Eigenschaften von Elementen

Sei R ein kommutativer Ring.

Definition 4.1. 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*.

Der kommutative Ring R heißt *Körper*, falls $R^* = R \setminus \{0\}$.

Definition 4.2. Ein Element $a \in R$ heißt *nilpotent*, falls es ein $n \in \mathbb{N}$ mit $a^n = 0$ gibt.
Ein Element $a \in R$ heißt *Nullteiler*, falls es ein $b \in R \setminus \{0\}$ mit $a \cdot b = 0$ gibt.
Der kommutative Ring $R \neq \{0\}$ heißt *Integritätsbereich*, falls 0 der einzige Nullteiler in R ist.

Definition 4.3. 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 $x \mid b$.

Skript: Ringtheorie 2. 12.11.2019

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 existiert $q, r \in R$ 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 Ring R heißt *Hauptidealring* falls jedes Ideal I in R ein Hauptideal ist.

Definition 1.3. Ein Ring R heißt *faktoriell* falls jedes Element $x \in R$ lässt sich als Produkt irreduzibler Elemente schreiben (eindeutig bis auf Assozitivität und Reihenfolge).

- Ein euklidischer Ring ist ein Hauptidealring. Ein Hauptidealring ist ein faktorieller Ring.
- Sei R ein faktorieller Ring. Genau dann ist $x \in R$ 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. *a) Ein Ideal $I \subseteq R$ ist ein Primideal genau dann wenn R/I ein Integritätsbereich ist.*

b) Ein Ideal $I \subseteq R$ ist ein maximales Ideal genau dann wenn R/I ein Körper ist.

Definition 2.4. 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 $ad = bc$.

Skript 6: Körpertheorie 1. 19.11.2019

1 Körpererweiterungen

Definition 1.1. Seien K, L Körpern. Eine *Körpererweiterung* ist eine inklusion $K \subseteq L$; L ist ein Vektorraum über K. 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 $f(X) \in K[X]$ sodass $f(\alpha) = 0$ gilt.
- 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 Hauptidealring und L ist 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 $K[\alpha] \cong K[X]$. 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 sei $\psi\colon \mathbb{Z} \to R$ der Ringhomomorphismus der durch $1 \mapsto 1_R$ definiert ist. Dann ist $\ker \psi$ ein Ideal in $\mathbb{Z}$. Falls R ein Körper ist (insbesonders ein Integritätsbereich), ist der Erzeuger p von $\ker(\psi)$ eine Primzahl $p > 0$; p heißt die *Charakteristik* von R.

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

Satz 3.2. *Sei p eine Primzahl und $q = p^k$ wobei $k \geq 1$. 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.*

4 Einheitswurzeln

Definition 4.1. Eine n-te *Einheitswurzel* ζ ist eine Nullstelle des Polynoms $X^n = 1$ in $\mathbb{C}$.

- Es gibt genau n verschiedene n-te Einheitswurzeln: $\zeta_k = \exp(\frac{2\pi i k}{n})$ für $k = 0, \ldots, n-1$.
- Die Menge $\mathbb{E}_n$ aller n-te Einheitswurzeln ist eine zyklische Gruppe bezüglich $\times$.

Definition 4.2. Eine Einheitswurzel ζ heißt *primitiv* falls ζ eine Einheit in $\mathbb{E}_n$ ist.

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

Skript 7: Körpertheorie 2. 26.11.2019

1 Zerfällungskörper

Definition 1.1. Sei $P(X) \in K[X]$ ein Polynom mit Koeffizienten in K. Der *Zerfällungskörper* von P über K ist der kleinste Körper $K \subset L$, sodass P sich als Linearfaktoren über L schreiben lässt.

Der Zerfällungskörper von $P(X)$ über K ist $L = K(\alpha_1, \ldots, \alpha_n)$ wobei α_i die Nullstellen von $P(X)$ sind.

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 manchmal auch $\mathrm{Gal}(L/K)$ bzw. *Galoisgruppe*).

- Sei $K \subset L$ eine Körpererweiterung, $\alpha \in L$ und $\mu(X)$ das Minimalpolynom von α über K. Für alle $\phi \in \mathrm{Aut}(L/K)$ gilt es: $\phi(\alpha)$ ist eine Nullstelle von μ.
- Umgekehrt, falls $\alpha' \in L$ eine Nullstelle von μ ist, existiert es einen K-Automorphismus $\phi \in \mathrm{Aut}(L/K)$ mit $\phi(\alpha) = \alpha'$.

Skript 8: Galoistheorie 1. 03.12.2019

1 Normal und separabel Körpererweiterungen

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

Definition 1.2. Ein Polynom $f(X) \in k[X]$ 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 Polynom $f(X) \in k[X]$ ist genau dann separabel, falls f und f' teilerfremd sind.
- Falls $\operatorname{char} k = 0$ ist, sind f und f' teilerfremd.
- 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 $f(X) \in k[X]$ ist galoissch über k.
- Insbesonders falls $\operatorname{char} k = 0$ ist, ist der Zerfällungskörper eines irreduziblen Polynoms galoissch.

Bemerkung 2.2. Sei $k \subset L$ eine galoissche Erweiterung. Die Menge aller k-Automorphismen $\operatorname{Aut}(L/k)$ ist eine Gruppe.

- Sei $k \subset L$ endlich und galoissch. Dann ist $|\operatorname{Gal}(L/k)| = [L : k]$.

3 Hauptsatz der Galoistheorie

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

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

Satz 3.2. *Sei $k \subset L$ eine endliche Galoiserweiterung. Die zwei Mengen*

$$\{\textit{Untergruppen von } \mathrm{Gal}(L/k)\} \leftrightarrow \{\textit{Zwischenkörper von } L/k\}$$

stehen in Bijektion zueinander. Die zwei Abbildungen sind $H \mapsto L^H$ und $(k \subset K \subset L) \mapsto \mathrm{Gal}(L/K)$. Die Erweiterung K/k ist normal (daher galoissch) genau dann wenn $H \trianglelefteq \mathrm{Gal}(L/k)$ ein Normalteiler ist.

Dr. Stephen Coughlan

Skript 9: Zwischenkörper und Galoisgruppen 05.12.2019

1 Elementarsymmetrische Polynome

Die elementarsymmetrische Polynome in Unbekannten $x_1, \dots, x_n$ sind

$$\begin{aligned}\sigma_0 &= 1\\ \sigma_1 &= x_1 + \cdots + x_n\\ \sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n\\ &\vdots\\ \sigma_n &= x_1x_2 \cdot \cdots \cdot x_n\end{aligned}$$

Ein Polynom $P(x_1, \dots, x_n)$ heißt *symmetrisch* falls es gilt $P(x_{\rho(1)}, \dots, x_{\rho(n)}) = P(x_1, \dots, x_n)$ für alle $\rho \in S_n$.

Satz 1.1. *Jedes symmetrische Polynom $P(x_1, \dots, x_n)$ in $k[x_1, \dots, x_n]$ lässt sich als Polynom in $\sigma_0, \dots, \sigma_n$ schreiben.*

Alternativ Man kann die Newton symmetrische Polynome verwenden:

$$s_0 = 1,\ s_i = x_1^i + \cdots + x_n^i,\ i = 1, \dots, n.$$

Es gilt der analoge Satz.

2 Beispiel $\mathbb{Q}(\zeta_9)$

Sei $\zeta_9 = \exp(\frac{2\pi i}{9})$ eine primitive 9-te Einheitswurzel. Dann ist $Z := \mathbb{Q}(\zeta)$ der Zerfällungskörper des (irreduziblen) Kreisteilungspolynoms

$$\Phi_9(X) = \frac{X^9 - 1}{X^3 - 1} = X^6 + X^3 + 1 = \prod_{\zeta^k \text{ prim.}} (X - \zeta^k) \in \mathbb{Q}[X]$$

über $\mathbb{Q}$. Die Nullstellen vom $\Phi_9(X)$ sind die primitive Einheitswurzeln ζ^k wobei $\mathrm{ggT}(k, 9) = 1$. Es gilt

$$[Z : \mathbb{Q}] = \deg \Phi_9(X) = \varphi(9) = 6$$

und

$$G := \mathrm{Gal}(Z : \mathbb{Q}) = (\mathbb{Z}/9\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z},$$

die einzige abelsche Gruppe der Ordnung $\varphi(9) = 6$.

Die Gruppe G ist von $\alpha\colon \zeta \mapsto \zeta^2$ erzeugt. Es gibt zwei echte Untergruppen, $H_1 := \left\langle \alpha^2 \right\rangle$ und $H_2 := \left\langle \alpha^3 \right\rangle$.

Daher gibt es zwei Ketten von Körpererweiterungen

$$\mathbb{Q} \overset{[G:H]}{\subset} Z^{H_i} \overset{|H_i|}{\subset} Z \longleftrightarrow G \supset H_i \supset \{id\}.$$

Fixkörper von H_1 Die Bahn von ζ unter H_1 ist $H_1 \cdot \zeta = \{\zeta, \alpha^2(\zeta), \alpha^4(\zeta)\} = \{\zeta, \zeta^4, \zeta^7\}$. Die elementarsymmetrische Polynome in $H_1 \cdot \zeta$ sind:

$$\sigma_0 = 1,\ \sigma_1 = \zeta + \zeta^4 + \zeta^7,\ \sigma_2 = \zeta \cdot \zeta^4 + \zeta \cdot \zeta^7 + \zeta^4 \cdot \zeta^7 (= \zeta^2 \sigma_2),\ \sigma_3 = \zeta \cdot \zeta^4 \cdot \zeta^7 (= \zeta^3)$$

Da $\Phi_9(\zeta) = 1 + \zeta^3 + \zeta^6 = 0$ ist, sind $\sigma_1 = \sigma_2 = 0$.

Behauptung Sei $\omega := \sigma_3 = \zeta^3$. Dann ist $Z^{H_1} = \mathbb{Q}(\omega)$.
Beweis: Zuerst, ω ist symmetrisch in den Elementen $H_1 \cdot \zeta$. Dass heißt, $\rho(\omega) = \omega$ für alle Permutationen $\rho \in H_1$. Daher ist $\omega \in Z^{H_1}$ und $\mathbb{Q}(\omega) \subset Z^{H_1}$.
Das Minimalpolynom von ω über $\mathbb{Q}$ ist $\Phi_3(X) = X^2 + X + 1$, weil ω eine primitive 3-te Einheitswurzel ist. Da der Grad $[Z^{H_1} : \mathbb{Q}] = [G : H_1] = 2$ ist, ist $\mathbb{Q}(\omega) = Z^{H_1}$.

Fixkörper von H_2 Die Bahn von ζ unter H_2 ist $H_2 \cdot \zeta = \{\zeta, \alpha^3(\zeta)\} = \{\zeta, \zeta^8\}$. Die elementarsymmetrische Polynome in $H_2 \cdot \zeta$ sind:

$$\sigma_0 = 1,\ \sigma_1 = \zeta + \zeta^8,\ \sigma_2 = \zeta \cdot \zeta^8 (= 1).$$

Sei $u := \zeta + \zeta^8 \in \mathbb{Q}(\zeta)^{H_2}$. (Eigentlich ist $u = \zeta + \bar{\zeta} = 2\cos(\frac{2\pi}{9}) \in \mathbb{R}$.)

Aufgabe Was ist das Minimalpolynom von u über $\mathbb{Q}$? Warum ist $\mathbb{Q}(\zeta)^{H_2} = \mathbb{Q}(u)$?

Aufgabe Untersuchen Sie die Galoisgruppe bzw. Zwischenkörper der Erweiterung $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$ für $n \leq 20$.

Dr. Stephen Coughlan