Zusammenfassung Algebra

Universität Regensburg

Wintersemester 2018/19

Inhaltsverzeichnis

1 Lineare Algebra: kurze Wiederholung **4**
1.1 Themen . . . 4
1.2 Einige wichtige Konzepte . . . 4

2 Gruppentheorie: kurze Wiederholung **6**
2.1 Themen . . . 6
2.2 Einige wichtige Konzepte . . . 6
2.2.1 Gruppenaxiome . . . 6
2.2.2 Untergruppen . . . 6
2.2.3 Ordnung . . . 6
2.2.4 Äquivalenzrelationen . . . 7
2.2.5 Satz von Lagrange . . . 7
2.2.6 Gruppenoperationen . . . 7
2.2.7 Bahnengleichung . . . 7
2.2.8 Konjugation . . . 8
2.2.9 Homomorphismus . . . 8
2.2.10 Normalteiler . . . 8
2.2.11 Isomorphiesätze . . . 8
2.2.12 Zyklische und einfache Gruppen . . . 9
2.2.13 Direktes Produkt . . . 9
2.2.14 Hauptsatz für endliche abelsche Gruppen . . . 9
2.2.15 Semidirektes Produkt . . . 9
2.2.16 Symmetrische Gruppen . . . 10
2.2.17 Sylow-Sätze . . . 10
2.2.18 Nilpotente Gruppen . . . 11
2.2.19 Auflösbare Gruppen . . . 11
2.3 Beispiele . . . 11
2.3.1 Beispiele für Gruppen: . . . 11
2.3.2 Beispiele für endlich erzeugte Gruppen: . . . 12
2.3.3 Beispiele für Gruppenoperationen . . . 13
2.3.4 Beispiel Konjugation . . . 14
2.3.5 Beispiele für Normalteilter . . . 14
2.3.6 Konstruktion äußerer semidirekter Produkte . . . 14
2.3.7 Beispiele: Symmetrische Gruppe . . . 15
2.3.8 Beispiele: Sylow-Sätze . . . 15
2.3.9 Beispiele: nilpotente und auflösbare Gruppen . . . 15

3 Ringtheorie: kurze Wiederholung **16**
3.1 Themen . . . 16
3.2 Einige wichtige Konzepte . . . 16
3.2.1 Ringaxiome . . . 16
3.2.2 Unterringe . . . 16
3.2.3 Ideale . . . 16
3.2.4 Ringhomomorphismen . . . 17

3.2.5 Faktorringe . . . 17
3.2.6 Polynomalgebren . . . 18
3.2.7 Einsetzungshomomorphismus . . . 18
3.2.8 Division mit Rest in $R[X]$ . . . 19
3.2.9 Integritätsringe . . . 19
3.2.10 Euklidische Ringe . . . 19
3.2.11 Quotientenringe . . . 19
3.2.12 Charakteristik . . . 20
3.2.13 Maximale Ideale . . . 20
3.2.14 Primideale . . . 20
3.2.15 Irreduzible Elemente, Primelemente . . . 20
3.2.16 kgV und ggT . . . 21
3.2.17 Faktorielle Polynomringe . . . 22
3.2.18 Irreduzibilitätskriterien . . . 22
3.2.19 Chinesischer Restsatz . . . 22
3.3 Beispiele . . . 23
3.3.1 Beispiele: Ringe . . . 23
3.3.2 Beispiele: Ideale . . . 24
3.3.3 Beispiele: Integritätsringe . . . 24
3.3.4 Beispiele: Euklidische Ringe . . . 24
3.3.5 Beispiele: Hauptidealringe . . . 24
3.3.6 Beispiele: Quotientenringe . . . 24
3.3.7 Beispiele: Maximale Ideale und Primideale . . . 25
3.3.8 Beispiele: Irreduzible Elemente . . . 25
3.3.9 Beispiele: Faktorielle Ringe . . . 25
3.3.10 Beispiele: Irreduzibilität . . . 25

4 Körpertheorie: kurze Wiederholung 26
4.1 Themen . . . 26
4.2 Einige wichtige Konzepte . . . 26
4.2.1 Endliche Körpererweiterungen . . . 26
4.2.2 Algebraische Erweiterungen . . . 26
4.2.3 Algebraischer Abschluss (in einem Oberkörper) . . . 27
4.2.4 Zerfällungskörper . . . 27
4.2.5 Normale Erweiterungen . . . 28
4.2.6 Galoisgruppe . . . 28
4.2.7 Separable Erweiterungen . . . 28
4.2.8 Endliche Körper . . . 29
4.2.9 Galoiserweiterungen . . . 29
4.2.10 Komposita als Galoiserweiterungen . . . 30
4.2.11 Kreistielungsteilungskörper . . . 31
4.2.12 Galoisgruppe von Polynomen . . . 32
4.2.13 Auflösbare Erweiterungen . . . 33
4.2.14 Konstruktionen mit Zirkel und Lineal . . . 34
4.3 Beispiele . . . 34
4.3.1 Beispiele: endliche Erweiterungen . . . 34
4.3.2 Beispiele: algebraischer Abschluß . . . 35
4.3.3 Beispiele: Zerfällungskörper . . . 35
4.3.4 Beispiele: Normale Erweiterungen . . . 35
4.3.5 Beispiele: Separable Erweiterungen . . . 36
4.3.6 Beispiele: Galoisgruppe . . . 36
4.3.7 Beispiele: Endliche Körper . . . 36
4.3.8 Beispiele: Galoiserweiterungen . . . 36
4.3.9 Beispiele: EInheitswurzeln . . . 37
4.3.10 Beispiele: Kreisteilungspolynome . . . 37
4.3.11 Beispiele Diskriminante . . . 37
4.3.12 Beispiele: Polynome vom Grad 3 . . . 38

4.3.13 Beispiele: Auflösbare Erweiterungen 38
4.3.14 Beispiele: Konstruktionen mit Zirkel und Lineal 38

1 Lineare Algebra: kurze Wiederholung

1.1 Themen

Vektorräume (Unterräume)
Homomorphismen
Basis
Matrizen
Eigenwerte
Diagonalisierbarkeit (charakteristisches Polynom, Minimalpolynom)
Allgemeine und spezielle lineare Gruppe
Jordan Normalform
Satz von Cayley–Hamilton

1.2 Einige wichtige Konzepte

Vektorraum Sei K ein Körper. Ein K-Vektorraum ist eine abelsche Gruppe $(V, +, 0)$ zusammen mit einer Abbildung $K \times V \to V, (a, v) \mapsto a.v$ so daß für alle $a, b \in K$ und $v, w \in V$ gilt

(a) $a.(v + w) = a.v + aw$

(b) $(a + b).v = a.v + b.v$

(c) $(a \cdot b).v = a.(b.v)$

(d) $1.v = v$

Jeder endliche Vektorraum ist isomorph zu K^n.

Unterraum Sei V ein K-Vektorraum. Ein Unterraum U von V ist eine nichtleere Teilmenge $\emptyset \neq U \subset V$, so daß für alle $v, w \in U$ und $\lambda \in K$ gilt $v + w \in U$ und $\lambda.v \in U$.

Basis Ein linear unabhängiges Erzeugendensystem heißt Basis. Jeder Vektorraum hat eine Basis (mit Zorn'schem Lemma). Für $K = \mathbb{R}$ findet man mit dem Gram-Schmidt'sche Orthonormierungsverfahren sogar eine Orthonormalbasis.

Dimension Die Länge einer und damit jeder Basis heißt Dimension. Ist $\dim V < \infty$ und sind $V_1, V_2 \subset V$ Unterräume, dann gilt

$$\dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim(V_1 \cap V_2).$$

Homomorphismen Eine Abbildung $f : V \to W$ zwischen K-Vektorräumen heißt Homomorphismus, falls für alle $v, w \in V$ und $\alpha \in K$ gilt

$$f(v + w) = f(v) + f(w) \quad \text{und} \quad f(\alpha.v) = \alpha.f(v)$$

Ist f injektiv, so heißt es Monomorphismus, ist es surjektiv, so heißt es Epimorphismus, ist es bijektiv, so heißt es Isomorphismus. Ist $V = W$ so sprechen wir von einem Endomorphismus, und ist f zusätzlich bijektiv, so heißt es Automorphismus. Wählt man eine Basis, so kann man die darstellende Matrix eines Homomorphismus bezüglich dieser Basis angeben: seine $\{v_1, \ldots, v_n\} \subset V$ und $\{w_1, \ldots, w_m\} \subset W$ Basen, dann kann man schreiben $f(v_j) = \sum \alpha_{ij} w_j$ und setzt $(\alpha_{ij}) = A$. Es gilt $\mathrm{Hom}_K(V, W) \cong M_{m \times n}(K)$.

Eigenwerte, Eigenvektoren Sei $f : V \to V$ ein Endomorphismus. Für $\lambda \in K$ ist $E(\lambda) = \ker(f - \lambda \,\mathrm{id})$ der Eigenraum von f zu λ. Ist $E(\lambda) \neq 0$, so nennt man λ einen Eigenwert von f. Die Elemente aus $E(\lambda)$ heißen Eigenvektoren zum Eigenwert λ. Ist f diagonalisierbar, so besitzt V eine Basis aus Eigenvktoren und umgekehrt. Die geometrische Vielfachheit von λ ist $\dim(E(\lambda)) = \dim V - \mathrm{rank}(f - \lambda \,\mathrm{id})$. Ähnliche Matrizen haben dieselben Eigenwerte.

charakteristisches Polynom Das charakteristische Polynom ist $\chi_f(X) = \det(f - X \,\mathrm{id})$. Ist $\chi_f(\lambda) = 0$, so ist $E(\lambda) \neq 0$, also ist λ ein Eigenwert von f. Nach dem Satz von Cayley–Hamilton ist jede Matrix (jeder Homomorphismus) Nullstelle ihres (seines) charakteristischen Polynoms.

Minimalpolynom Das Minimalpolynom $\mu_f(X)$ ist das normierte Polynom kleinsten Grades, so dass $\mu_f(f) = 0$, daher gilt $\mu_f \big| \chi_f$.

Jordan-Normalform Eine Matrix ist Trigonalisierbar, falls das charakteristische Polynom vollständig in Linearfaktoren zerfällt. Insbesondere ist dies der Fall, wenn der Grundkörper algebraisch abgeschlossen ist. In diesem Fall lässt sich eine Matrix in die sogenannte Jordan'sche Normalform bringen

$$\begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_r \end{pmatrix}$$

wobei die J_i Jordanblöcke genannt werden. Sie haben auf der Diagonalen einen Eigenwert und auf der Nebendiagonalen 1.

2 Gruppentheorie: kurze Wiederholung

2.1 Themen

Gruppen, Untergruppen
Gruppenordnung
Äquivalenzrelationen
Satz von Lagrange
Homomorphismen
Faktorgruppen
Isomorphiesätze
Chinesischer Restsatz
Zyklische Gruppen
Direkte und semidirekte Produkte
Symmetrische Gruppe
Sylowsätze

2.2 Einige wichtige Konzepte

2.2.1 Gruppenaxiome

Sei G eine Menge und $\cdot : G \times G \to G$; $(x, y) \mapsto x \cdot y = xy$ eine Abbildung. Wir betrachten folgende Axiome:

(a) Assoziativität: $\forall x, y, z \in G$: $(xy)z = x(yz)$.

(b) Neutrales Element: $\exists! e \in G \forall x \in M$: $ex = x = xe$.

(c) Inverses Element: $\forall x \in G \exists! x' \in G$: $xx' = e = x'x$. Wir setzen $x^{-1} := x'$.

(d) Kommutativität: $\forall x, y \in G$: $xy = yx$.

$(G, \cdot)$ heißt Gruppe, falls (a), (b), (c) gelten, abelsche Gruppe, falls zusätzlich (d) gilt.

2.2.2 Untergruppen

Eine Teilmenge H einer Gruppe $(G, \cdot)$ heißt Untergruppe, falls sie selbst wieder eine Gruppe ist.
Dies ist der Fall, wenn zusätzlich gilt

(a) $e \in H$

(b) $\forall x, y \in H$ ist $xy \in H$

(c) $\forall x \in H : x^{-1} \in H$.

Sie $X \subset G$.

$$\langle X \rangle = \{y \in G \mid \exists n \in \mathbb{N}_0, x_1, \ldots, x_n \in X \cup X^{-1} : y = x_1 \cdots x_n\}$$

ist die von X erzeugte Untergruppe von G.
Ist $X = \{x\}$, so ist

$$\langle x \rangle = \langle \{x\} \rangle = \{x^a \mid a \in \mathbb{Z}\}$$

abelsche Untergruppe (zyklische Gruppe).

2.2.3 Ordnung

Die Zahl $|G| \in \mathbb{N}_0 \cup \{\infty\}$ heißt Ordnung der Gruppe G.
Für $x \in G$ gilt $\text{ord}(x) = |\langle x \rangle| \in \mathbb{N}_0 \cup \infty$.
Sei p eine Primzahl. Eine endliche Gruppe heißt p-Gruppe, falls es $n \in \mathbb{N}$ gibt mit $|G| = p^n$.
Hat $x \in G$ endliche Ordnung, so sind äquivalent:

(a) $n = \text{ord}(x) = |\langle x \rangle|$,

(b) $\langle x \rangle = \{e, x, \ldots, x^{n-1}\}$ und $x_i \neq x_j$ für $i \neq j$,

(c) $\forall z \in \mathbb{Z} : x^z = e \Leftrightarrow n | z$,

(d) $n = \min\{k \in \mathbb{N} \,|\, x^k = e\}$.

2.2.4 Äquivalenzrelationen

Sei X eine Menge. Eine Relation $\sim$ auf X heißt Äquivalenzrelation falls

(a) $\forall x \in X$: $x \sim x$ (Reflexivität)

(b) $\forall x, y \in X$: $x \sim y \Leftrightarrow y \sim x$ (Symmetrie)

(c) $\forall x, y, z \in X$: $x \sim y, y \sim z \Rightarrow x \sim z$ (Transitivität)

Für $x \in X$ heißt $\overline{x} = \{y \in X \mid x \sim y\}$ die Äquivalenzklasse von x.

2.2.5 Satz von Lagrange

Sei G eine Gruppe, $H \subset G$ eine Untergruppe. Betrachte die Äquivalenzrelation auf G:

$$x \sim y \Leftrightarrow \exists h \in H : xh = y \Leftrightarrow x^{-1}y \in H \Leftrightarrow y^{-1}x \in H.$$

$\overline{x} = xH$ ist die Linksnebenklasse von H in G repräsentiert durch x. Die Menge aller Linksnebenklassen von H in G ist G/H. (Genauso für rechts statt links.)
Die Zahl $[G : H] = |G/H| = |H\backslash G| \in \mathbb{N} \cup \{\infty\}$ heißt Index von H in G.

Satz. *Sei G endliche Gruppe, $H \subset G$ Untergruppe. Dann gilt*

$$|G| = [G : H] \cdot |H|.$$

Insbesondere sind $[G : H]$ und $|H|$ Teiler von $|G|$.

2.2.6 Gruppenoperationen

Sei X eine Menge $\neq \emptyset$, G eine Gruppe. Eine Abbildung

$$G \times X \to X, (g, x) \mapsto g \cdot x = gx$$

heißt (Links)Operation von G auf X, falls

(a) für alle $x \in X$ gilt $ex = x$;

(b) für alle $x \in X$ und $g_1, g_2 \in G$ gilt $g_2(g_1x) = (g_1g_2)x$.

Die Operation heißt transitiv, falls es für alle $x, y \in X$ ein $g \in G$ gibt mit $y = gx$.
Die Bahn von $x \in X$ ist $\overline{x} = Gx = \{gx \mid g \in G\} \subset X$.
Der Stabilisator von $x \in X$ ist $G_x = \mathrm{Stab}_G(x) = \{g \in G \mid gx = x\} \subset G$, eine Untergruppe von G.
Die Fixpunkte von G sind $X^G = \{x \in X \mid gx = x \forall g \in G\} \subset X$.

2.2.7 Bahnengleichung

Sei X endliche Menge, G endliche Gruppe, $G \times X \to X$, $(g, x) \mapsto gx$ eine Operation.

(a) Für alle $x \in X$ gilt $|Gx| = [G : G_x]$.

(b) Ist $T \subset X$ eine Transversale der Bahnen dann ist die Vereinigung $X = \bigcup_{x \in T} Gx$ disjunkt.

(c) Es gilt

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

Ist X_0 die Menge der Fixpunkte, dann gilt

$$|X| = |X_0| + \sum_{x \in T \backslash X_0} [G : G_x].$$

2.2.8 Konjugation

Sei G eine Gruppe. $x, y \in G$ sind zueinander konjugiert $\Leftrightarrow \exists u \in G : uxu^{-1} = y$.
Die Konjugationsklasse (Äquivalenzklasse) von $x \in G$ ist

$$C_x = \{uxu^{-1} : u \in G\} \subseteq G.$$

Der Zentralisator (Stabilisatoruntergruppe) von $x \in G$ ist

$$C_G(x) = \{u \in G : uxu^{-1} = x\} = \{u \in G : ux = xu\} \subseteq G.$$

Das Zentum einer Gruppe ist

$$Z(G) = \{x \in G : ux = xu \forall u \in G\}.$$

Ist C_x die Konjugationsklasse von x, dann gilt

$$|C_x| = [G : C_G(x)].$$

Klassengleichung: Sei S eine Transversale der Konjugationsklassen in $G \backslash Z(G)$, dann gilt

$$|G| = |Z(G)| + \sum_{s \in S} [G : C_G(s)].$$

2.2.9 Homomorphismus

Seien G und G' Gruppen. Eine Abbildung $f : G \to G'$ heißt Homomorphismus, falls für alle $x, y \in G$: $f(xy) = f(x)f(y)$. Dann gilt $f(e) = e'$ und $f(x^{-1}) = f(x)^{-1}$.

- Isomorphismus: f ist bijektiv $\Leftrightarrow$ f hat ein inverses $f' = f^{-1} : G' \to G$
- Endomorphismus :$\Leftrightarrow$ $G = G'$
- Automorphismus :$\Leftrightarrow$ f ist bijektiv und $G = G'$
- f ist injektiv $\Leftrightarrow$ $\ker(f) = e$
- f ist surjektive $\Leftrightarrow$ $\mathrm{im}(f) = G'$
- Sind $H \subset G$ und $H' \subset G'$ Untergruppen, dann sind $f(H) \subset G'$ und $f^{-1}(H') \subset G$ Untergruppen. Insbesondere sind $\ker(f) \subset G$ und $\mathrm{im}(f) \subset G'$ Untergruppen.

2.2.10 Normalteiler

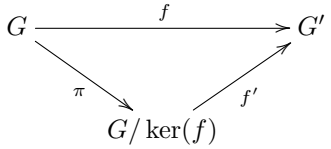
Sei G Gruppe. Eine Untergruppe $N \subset G$ heißt Normalteiler, wenn für alle $x \in G$ $xNx^{-1} = N$, geschrieben $N \triangleleft G$.

- Ist $f : G \to G'$ Homomorphismus, dann ist $\ker(f) \triangleleft G$.
- Ist $N' \triangleleft G'$, dann ist $f^{-1}(N') \triangleleft G$.
- Ist f surjektiv und $N \triangleleft G$, dann ist $f(N) \triangleleft G'$.
- Ist $N \triangleleft G$, so ist G/N eine Gruppe (Faktorgruppe von G modulo N. Kanonische Abbildung $\pi : G \to G/N$ mit $\ker(\pi) = N$.

2.2.11 Isomorphiesätze

Sei $f : G \to G'$ Gruppenhomomorphismus.

Homomorphiesatz: Es gibt genau einen injektiven Homomorphismus $f' : G/Ker(f) \to G'$ mit $f = f' \circ \pi$ wobei π der kanonische Homomorphismus ist, das heißt, das Diagramm



kommutiert. Insbesondere ist

$$f' : G/\ker(f) \to \mathrm{im}(f), x \ker(f) \mapsto f(x)$$

Isomorphismus.

1. Isomorphiesatz: Sei $H \subset G$ Untergruppe und $N \triangleleft G$ Normalteiler. Dann ist $HN = NH$ Untergruppe von G, $N \triangleleft HN$. $H \cap N \triangleleft H$, und die Abbildung

$$H/H \cap N \to HN/N, hH \cap N \mapsto hN$$

ist Isomorphismus.

2. Isomorphiesatz: Seien $M \triangleleft G$, $N \triangleleft G$ Normalteiler mit $M \subset N$. Dann sind $M \triangleleft N$, $N/M \triangleleft G/M$ Normalteiler, und die Abbildung

$$G/N \to (G/M)/(N/M), xN \mapsto (xM)(N/M)$$

ist Isomorphismus.

2.2.12 Zyklische und einfache Gruppen

Sei G Gruppe. G ist genau dann zyklisch, wenn es $n \in \mathbb{N}_0$ gibt, mit $G \cong \mathbb{Z}/\mathbb{Z}n$. Ist G zyklisch, dann sind auchdie Unter- und Faktorgruppen von G zyklisch.
G heißt einfach, wenn $G \neq \{e\}$ und G außer G und $\{e\}$ keine Normalteiler enthält.

2.2.13 Direktes Produkt

Seien $G_1, \ldots, G_r$ Gruppen. Das kartesische Produkt $G := \prod_{i=1}^r G_i$ mit komponentenweiser Multiplikation heißt auch direktes Produkt der G_i.
Sei G eine Gruppe und $H_1, \ldots, H_r$ Untergruppen. G ist direktes Produkt der H_i, wenn

$$f : \prod_{i=1}^{r} H_i \to G, (x_1, \ldots, x_r) \mapsto x_1 \cdots x_r$$

ein Isomorphismus ist.
Dann sind $H_1, \ldots, H_r$ sind Normalteiler mit

$$G = H_1 \cdots H_r \quad \text{und} \quad H_i \cap (H_{i+1} \ldots H_r) = \{e\}$$

für $1 \leqslant i \leqslant r$.
Man schreibt

$$G = H_1 \times \cdots \times H_r = \times_{i=1}^r H_i.$$

oder falls G abelsch ist

$$G = H_1 \oplus \cdots \oplus H_r = \bigoplus_{i=1}^{r} H_i.$$

2.2.14 Hauptsatz für endliche abelsche Gruppen

Sei A endliche abelsche Gruppe, $|A| = n = p_1^{\nu_1} \cdots p_r^{\nu_r}$, $r \in \mathbb{N}_0$, Primzahlen $p_1 < \cdots < p_r$, und $\nu_i \in \mathbb{N}$. Dann gibt es $b_{ij} \in A$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s_i$, und natürliche Zahlen $k_{i1} \geqslant \ldots \geqslant k_{is_i} \geqslant 1$ mit

$$A = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s_i} \mathbb{Z}\, b_{ij} \quad \text{und } \operatorname{ord}(b_{ij}) = p_i^{k_{ij}} \text{ für } 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s_i.$$

Diese Zerlegung ist eindeutig.

2.2.15 Semidirektes Produkt

Seien G_1, G_2 Gruppen und $\tau : G_2 \to \operatorname{Aut}(G_1)$ ein Homomorphismus. Die Menge $G_1 \times G_2$ ist Gruppe:
- Multiplikation: $(x, y)(x', y') = (x\tau(y)(x'), yy')$
- Neutrales Element: (e, e)
- Inverses: $(x, y)^{-1} = (\tau(y^{-1})(x^{-1}), y^{-1})$

Sie heißt äußeres Semidirektes Produkt $G_1 \times_\tau G_2$.
Sei G eine Gruppe, $N \triangleleft G$, $H \subset G$ Untergruppe mit $G = NH = HN$ und $N \cap H = \{e\}$, sei $H \to \operatorname{Aut}(N)$ definiert durch $\kappa(y)(x) = yxy^{-1}$ für $x \in N$, $y \in H$. Dann ist

$$f : N \times_\kappa H \to G, (x, y) \mapsto xy$$

ein Isomorphismus.
G heißt inneres semidirektes Produkt von N und H.

2.2.16 Symmetrische Gruppen

Zykel: $\sigma = (a_1 \dots a_k) \in \mathfrak{S}_n$ = Zykel der Länge k: $a_1, \dots, a_k \in \{1, \dots, n\}$ paarweise verschieden mit

$$\begin{aligned} \sigma(a_i) &= a_{i+1} \quad \text{für } 1 \leqslant i < k, \\ \sigma(a_k) &= a_1, \\ \sigma(x) &= x \quad \text{für } x \in \{1, \dots, n\} \backslash \{a_1, \dots, a_k\} \end{aligned}$$

Zweizykel heißen Transpositionen.
Jedes Element $\sigma \in \mathfrak{S}_n$ ist Produkt von endlich vielen disjunkten Zykeln $\sigma = \sigma_1 \cdots \sigma_r$.
Es gilt $\operatorname{ord}(\sigma) = \operatorname{kgV}(\operatorname{ord}(\sigma_i))$.
Typ einer Permutation: Sei $\sigma = \sigma_1 \cdots \sigma_r$ Zerlegung in paarweise disjunkte Zyklen, $k_i = \operatorname{ord}(\sigma_i)$, $k_1 \geqslant \cdots \geqslant k_r$. Dann heißt $(k_1, \dots, k_r)$ Typ von σ.
Zwei Permutationen sind genau dann konjugiert, wenn sie denselben Typ haben.
Signum einer Permutation:

$$\varepsilon : \mathfrak{S}_n \to \{-1, 1\}, \varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Ist $\sigma = \tau_1 \cdots \tau_n$ Produkt von Transpositionen, dann gilt

$$\varepsilon(\sigma) = (-1)^n.$$

Ist $\sigma = \sigma_1 \cdots \sigma_r$ Produkt von disjunkten Zyklen, $\operatorname{ord}(\sigma_i) = k_i$, dann gilt

$$\varepsilon(\sigma) = (-1)^{\sum (k_i - 1)}.$$

σ heißt gerade (bzw. ungerade) falls $\varepsilon(\sigma) = 1$ (bzw. $\varepsilon(\sigma) = -1$).
Alternierende Gruppe: Man setzt

$$A_n = \ker \varepsilon.$$

Dies ist die Menge der geraden Permutationen und der einzige Normalteiler vom Index 2 von $\mathfrak{S}_n$. Es gilt

$$\begin{aligned} \mathfrak{S}_n / A_n &\cong \{-1, 1\} \\ |A_n| &= \frac{n!}{2}. \end{aligned}$$

$\mathfrak{S}_n$ ist semidirektes Produkt von A_n und jeder von einer Transposition erzeugten Untergruppe.
Wir wissen $A_2 = \{\mathrm{id}\}$, $A_3 = \langle (123) \rangle$, A_4 ist nicht einfach, A_3 schon. Für $n \geqslant 5$ ist A_n einfach.

2.2.17 Sylow-Sätze

Normalisator: Sei $H \subset G$ Untergruppe einer endlichen Gruppe:

$$N_G(H) = \{x \in G \mid xHx^{-1} = H\}$$

heißt Normalisator von H in G. $N_G(H)$ ist die größte Untergruppe von G, in der H als Normalteiler enthalten ist.
p-Sylowuntergruppe: Seien G eine endliche Gruppe, p eine Primzahl, $|G| = p^a m$ mit $a \in \mathbb{N}_0$, $m \in \mathbb{N}$ und $p \nmid m$. Eine Untergruppe der Ordnung p^a von G heißt p-Sylowuntergruppe.

Satz 2.1 (Sylow)**.** *Sei G eine endliche Gruppe, p Primzahl, $|G| = p^a m = n$ mit $p \nmid m$.*

(a) G enthält mindestens eine p-Sylowuntergruppe, und jede p-Untergruppe ist in einer solchen enthalten.

(b) Je zwei p-Sylowuntergruppen sind zueinander konjugiert.

(c) Sei s_p die Anzahl der p-Sylowgruppen, sei P eine p-Sylowgruppe. Dann gilt

$$s_p = [G : N_G(P)] \quad , \quad s_p \mid m \quad \textit{und} \quad s_p \equiv 1 \mod p.$$

Sei G eine endliche Gruppe, p Primzahl; dann sind folgende Aussagen äquivalent:

(a) G ist p-Gruppe.

(b) Für alle $x \in G$ ist $\operatorname{ord}(x)$ p-Potenz.

Die Sylowsätze haben viele wichtige Anwendungen!

2.2.18 Nilpotente Gruppen

Kommutator: Für $x, y \in G$ heißt $[x, y] = xyx^{-1}y^{-1}$ Kommutator von x und y. Es gilt

$$[x, y] = e \quad \Leftrightarrow \quad xy = yx.$$

Für Untergruppen $H, K \subset G$ ist $[H, K]$ die Kommutatoruntergruppe. $[G, G]$ ist die Kommutatoruntergruppe von G.
Absteigende Zentralreihe:

$$\begin{aligned} C^1(G) &= G \\ C^{i+1}(G) &= [C^i(G), G] \end{aligned}$$

— $C^i(G) \triangleleft G$, $i \geqslant 1$,
— $G = C^1(G) \supset C^2(G) \supset \ldots$
— Da $C^i(G)/C^{i+1}(G) \subset Z(G/C^{i+1}(G))$ ist, ist $C^i(G)/C^{i+1}(G)$ abelsch.
— Die Folge $\left(C^i(G)\right)_{i \geqslant 1}$ heißt absteigende Zentralreihe von G.
Nilpotente Gruppen: Eine endliche Gruppe heißt nilpotent, falls folgende äquivalente Bedingungen erfüllt sind:

(a) Es gibt $n \in \mathbb{N}$ mit $C^n(G) = \{e\}$.
(b) Es gibt eine Folge von Untergruppen $G = H_1 \supset H_2 \supset \ldots \supset H_m = \{e\}$ mit $[H_i, G] \subset H_{i+1}$, $1 \leqslant i \leqslant m-1$. (Dann gilt $H_i \triangleleft G$.)

— p-Gruppen sind nilpotent.
— Untergruppen, Faktorgruppen und endliche direkte Produkte endlicher nilpotenter Gruppen sind nilpotent.
— Ist G endlich, $H \subset Z(G)$ eine Untergruppe und ist G/H nilpotent, dann ist G nilpotent.

2.2.19 Auflösbare Gruppen

Abgeleitete Reihe:

$$\begin{aligned} D^0(G) &= G \\ D^1(G) &= [G, G] \\ D^{n+1}(G) &= D^1(D^n(G)) = [D^n(G), D^n(G)] \quad \text{für } n \geqslant 1 \end{aligned}$$

— $D^n(G) \triangleleft G$, $n \geqslant 0$
— $G = D^0(G) \supset D^1(G) \supset D^2(G) \supset \ldots$
— Die Faktorgruppe $D^n(G)/D^{n+1}(G)$ ist abelsch aber im Allgemeinen nicht zentrale Untergruppe von $G/D^{n+1}(G)$, $n \geqslant 0$.
— Die Folge $\left(D^i(G)\right)_{i \geqslant 1}$ heißt abgeleitete Reihe von G.
Auflösbare Gruppen: Eine Gruppe G heißt auflösbar, wenn folgende äquivalente Bedingungen erfüllt sind:

(a) Es gibt $n \in \mathbb{N}_0$ mit $D^n(G) = \{e\}$.
(b) Es gibt eine Folge von Normalteilern $G = H_0 \supset H_1 \supset \ldots \supset H_m = \{e\}$, $m \geqslant 0$, so daß H_i/H_{i+1} abelsch ist für $0 \leqslant i < m$.
(c) Es gibt eine Folge von Untergruppen $G = H_0 \supset H_1 \supset \ldots \supset H_m = \{e\}$, $m \geqslant 0$, so daß $H_{i+1} \triangleleft H_i$ und H_i/H_{i+1} abelsch ist für $0 \leqslant i < m$. (Normalreihe mit abelschen Faktoren)

— Ist G auflösbar, so auch jede Untergruppe und jedes epimorphe Bild von G.
— Ist $N \triangleleft G$, so daß N und G/N auflösbar sind, dann ist G auflösbar.
— Endliche direkte Produkte auflösbarer Gruppen sind auflösbar.

2.3 Beispiele

2.3.1 Beispiele für Gruppen:

(a) Sei K ein Körper, dann ist $(K, +)$ abelsche Gruppe, $(K, \cdot)$ abelsches Monoid und $(K\backslash\{0\}, \cdot)$ abelsche Gruppe.

(b) $(\mathbb{Z},+)$ abelsche Gruppe, $(\mathbb{Z},\cdot)$ abelsches Monoid, $(\mathbb{Z}\setminus\{0\},\cdot)$ abelsches Monoid, $(\{1,-1\},\cdot)$ abelsche Gruppe.

(c) Sei $\mathcal{X}\neq\emptyset$ eine Menge. Die Menge $\mathfrak{S}_\mathcal{X}$ aller Bijektionen von $\mathcal{X}$ nach $\mathcal{X}$ ist bezüglich der Komposition eine Gruppe, die symmetrische Gruppe von $\mathcal{X}$. Ist $\mathcal{X}=\{1,\dots,n\}$, dann setzt man $\mathfrak{S}_n := \mathfrak{S}_\mathcal{X}$. Es gilt $|\mathfrak{S}_n| = n!$. $\mathfrak{S}_n$ ist nur für $n=1,2$ abelsch. Die Elemnte der $\mathfrak{S}_n$ werden in der Gestalt $\sigma = \binom{1\dots n}{\sigma(1)\dots\sigma(n)}$ geschrieben.

(d) Ist $(M,\cdot)$ Monoid, dann ist $M^\times = \{x\in M \mid \exists x'\in M : xx' = e =' x\}$ eine Gruppe; sie heißt Einheitengruppe von $(M,\cdot)$. Speziell $(\mathbb{Z},\cdot)^\times = \{1,-1\}$.

(e) Sind $G_1,\dots,G_n$ Gruppen (Monoide), dann ist das kartesische Produkt $G_1\times\cdots\times G_n$ mit komponentenweiser Multiplikation eine Gruppe (ein Monoid) $(x_1,\dots,x_n)\cdot(y_1,\dots,y_n) = (x_1y_1,\dots,x_ny_n)$.

(f) Weitere Beispiele: $\mathbf{GL}_n(K)$, $\mathbf{SL}_n(K)$, $\mathbf{O}_n$, $\mathbf{SO}_n$, $\mathbf{U}_n$, $\mathbf{SU}_n$,...

(g) Abelsche Gruppen bis auf Isomorphie:

$$\begin{array}{rl} n=4 & \mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}2 \quad , \quad \mathbb{Z}/\mathbb{Z}4 \\ n=6 & \mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}3\cong\mathbb{Z}/\mathbb{Z}6 \\ n=8 & \mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}2 \quad , \quad \mathbb{Z}/\mathbb{Z}4\times\mathbb{Z}/\mathbb{Z}2 \quad , \quad \mathbb{Z}/\mathbb{Z}8 \\ n=12 & \mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}3\cong\mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/\mathbb{Z}6 \quad , \quad \mathbb{Z}/\mathbb{Z}4\times\mathbb{Z}/\mathbb{Z}3\cong\mathbb{Z}/\mathbb{Z}12 \end{array}$$

2.3.2 Beispiele für endlich erzeugte Gruppen:

(a) Die symmetrische Gruppe

$$G=\mathfrak{S}_3=\left\{e, a=\begin{pmatrix}123\\231\end{pmatrix}, a^2=\begin{pmatrix}123\\312\end{pmatrix}, b=\begin{pmatrix}123\\132\end{pmatrix}, c=\begin{pmatrix}123\\321\end{pmatrix}, d=\begin{pmatrix}123\\213\end{pmatrix}\right\}$$

mit den Relationen $a^3=e$, $a^{-1}=a^2$, $b^2=c^2=d^2=e$, $b^{-1}=b$, $c^{-1}=c$, $d^{-1}=d$, $ab=d$, $a^2b=c$.

$$\begin{array}{rcl} \langle a\rangle & = & \langle a^2\rangle = \{e,a,a^2\} \\ \langle b\rangle & = & \{e,b\} \\ \langle c\rangle & = & \{e,c\} \\ \langle d\rangle & = & \{e,d\} \end{array}$$

ergibt

$$\begin{array}{rcl} \operatorname{ord}(e) & = & 1 \\ \operatorname{ord}(a) & = & 3 \\ \operatorname{ord}(b)=\operatorname{ord}(c)=\operatorname{ord}(d) & = & 2 \end{array}$$

Also: $G=\{e,a,a^2,b,ab,a^2b\}$. Kommutatorrelation: $ba=c=a^2b$.

(b) Sei $n\geqslant 2$, $a=\begin{pmatrix}\cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n}\\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n}\end{pmatrix}$, $b=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ in $\mathbf{O}_2$. Es gilt

$$\begin{array}{rcll} a^n & = & e & \\ a^i & = & a^j & \text{für } 0\leqslant i<jn \\ b^2 & = & e & \end{array}$$

Relation: $ba=a^{n-1}b$
Untergruppen:

$$\begin{array}{rcl} \langle a\rangle & = & \{e,a,\dots a^{n-1}\} \quad \text{also } \operatorname{ord}(a)=n \\ \langle b\rangle & = & \{e,b\} \quad \text{also } \operatorname{ord}(b)=2 \\ D_n & = & \{e,a,a^2\dots,a^{n-1},b,a^2b\dots,a^{n-1}b\} \quad \text{ist Gruppe der Ordnung } 2n \end{array}$$

Jede zu D_n isomorphe Gruppe heißt Diedergruppe der Ordnung $2n$.
Für $n = 2$:

$$D_2 = \{e, a, b, ab\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \cos\pi & -\sin\pi \\ \sin\pi & \cos\pi \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} \cos\pi & \sin\pi \\ \sin\pi & -\cos\pi \end{pmatrix} \right\}$$

ist abelsche Gruppe der Ordnung 4. Jede dazu isomorphe Gruppe heißt Kleinsche Vierergruppe.
Für $n = 3$:

$$D_3 \cong S_3.$$

(c) Sei $a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in $\mathbf{U}_2$. Dann

$$\begin{aligned} a^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ a^4 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e \\ a^3 &= \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = a^{-1} \\ b^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = a^2 \\ b^4 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e \\ b^3 &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = b^{-1} \end{aligned}$$

Relationen: $b^2 = a^2$, $ba = a^3b$

$$Q = \langle a, b \rangle = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

hat Ordnung 8 und heißt Quaternionengruppe.

(d) Jede Untergruppe von $(\mathbb{Z}, +)$ ist von der Gestalt $\mathbb{Z}\,n$ mit eindeutigem $n \in \mathbb{N}_0$.

2.3.3 Beispiele für Gruppenoperationen

(a) Sei $X \neq \emptyset$ eine Menge, $G \subset \mathfrak{S}_X$ eine Untergruppe. Dann ist

$$G \times X \to X, (\sigma, x) \mapsto \sigma(x)$$

eine Operation.
Speziell $X = \{1, 2, 3\}$, $G = S_3$. Dann ist $G.1 = G.2 = G.3 = X$, also ist die Operation transitiv. Sie ist fixpunktfrei.

$$\begin{aligned} G_1 &= \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\} \\ G_2 &= \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\} \\ G_3 &= \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \end{aligned}$$

(b) $X = \mathbb{R}^2$, $G = \mathbf{SO}_2 = \left\{ \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \mid 0 \leqslant \varphi < 2\pi \right\}$. Dann ist

$$\mathbf{SO}_2 \times \mathbb{R}^2 \to \mathbb{R}^2, (A, x) \mapsto Ax$$

eine Operation mit $G_0 = G$, $G_x = e$ für $x \neq 0$.

2.3.4 Beispiel Konjugation

$\mathfrak{S}_3 = \{e, a, a^2, b, ab, a^2b\}$ mit $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ und $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $ba = a^2b$.

Konjugationsklassen:

$$\begin{aligned} C_e &= \{e\} \\ C_a &= \{a, a^2\} \quad \text{denn } bab = a^2\text{; das sind die Elemente der Ordnung 3} \\ C_b &= \{b, ab, a^2b\} \quad \text{denn } a^{-1}ba = ab,\ a^{-2}ba^2 = ba = a^2n\text{, dies sind die Elemente der Ordnung 2} \end{aligned}$$

Zentralisatoren: Diese sind Untergruppen von $\mathfrak{S}_3$, haben also Ordnung $1, 2, 3$ oder 6.

$$\begin{aligned} C_{\mathfrak{S}_3}(e) &= \mathfrak{S}_3 \\ C_{\mathfrak{S}_3}(a) &= \{e, a, a^2\} \quad \text{nicht-triviale echte Untergruppe, denn } a \text{ vertauscht mit sich selbst, aber nicht mit } b \\ &= C_{\mathfrak{S}_3}(a^2) \\ C_{\mathfrak{S}_3}(b) &= \{e, b\} \quad \text{nicht-triviale echte Untergruppe, denn } b \text{ vertauscht mit sich selbst, aber nicht mit } a \\ C_{\mathfrak{S}_3}(ab) &= \{e, ab\} \quad \text{nicht-triviale echte Untergruppe, denn } ab \text{ vertauscht mit sich selbst, aber nicht mit } a \\ C_{\mathfrak{S}_3}(a^b) &= \{e, a, a^2\} \quad \text{nicht-triviale echte Untergruppe, denn } a^2b \text{ vertauscht mit sich selbst, aber nicht mit } a \end{aligned}$$

Zentrum: $Z(G) = \{e\}$.

2.3.5 Beispiele für Normalteilter

(a) Ist G abelsch, dann sind alle Untergruppen von G Normalteiler.

(b) Die Normalteiler von $\mathfrak{S}_3$ sind $\{e\}$, S_3, $\left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle$.

(c) Ist $H \subset G$ Untergruppe vom Index 2, dann ist $H \triangleleft G$: Für $x \in G \backslash H$ gilt $G = H \cup xH = H \cup Hx$ disjunkt, also $xH = Hx$, für $x \in H$ gilt $xH = H = Hx$.

(d) Die einfachen abelschen Gruppen sind bis auf Isomorphie genau die $\mathbb{Z}/\mathbb{Z}p$, p prim.

2.3.6 Konstruktion äußerer semidirekter Produkte

Sei $m, n \in \mathbb{N} \backslash \{1\}$, $r \in \mathbb{Z}$ mit $r^m \equiv 1 \mod n$, dh. $\operatorname{ord}_n(r) \big| m$. Dann ist

$$\rho : \mathbb{Z}/\mathbb{Z}n \to \mathbb{Z}/\mathbb{Z}n, \overline{z} \mapsto \overline{rz}$$

Homomorphismus mit $\rho^m = \mathrm{id}_{\mathbb{Z}/\mathbb{Z}n}$. Also ist $\rho \in \operatorname{Aut}(\mathbb{Z}/\mathbb{Z}n)$ und $\operatorname{ord}(\rho) \big| m$. Die Abbildung

$$\tau : \mathbb{Z}/\mathbb{Z}m \to \operatorname{Aut}(\mathbb{Z}/\mathbb{Z}n), \overline{y} \mapsto \rho^y$$

ist Gruppenhomomorphismus, explizit

$$\tau(\overline{y})(\overline{x}) = \rho^y(\overline{x}) = \overline{r}^y\overline{x}$$

für $\overline{y} \in \mathbb{Z}/\mathbb{Z}m$, $\overline{x} \in \mathbb{Z}/\mathbb{Z}n$. Sei

$$G = \mathbb{Z}/\mathbb{Z}n \times_\tau \mathbb{Z}/\mathbb{Z}m.$$

In G gilt

$$(\overline{x}, \overline{y})(\overline{x}', \overline{y}') = (\overline{x} + \overline{r}^y\overline{x}', \overline{y} + \overline{y}'),$$

neutrales Element ist $(0, 0)$, Inverses ist $(\overline{x}, \overline{y})^{-1} = (-\overline{r}^{-y}\overline{x}, -\overline{y})$. Seien $a = (\overline{1}, \overline{0})$, $b = (\overline{0}, \overline{1})$, dann ist $\operatorname{ord}(a) = n$ und $\operatorname{ord}(b) = m$, ferner $bab^{-1} = a^r$ (äquivalent dazu: $ba = a^rb$). Es folgt $G = \{a^ib^j \mid 0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant m-1\}$. Außerdem $\langle a \rangle \triangleleft G$, $G = \langle a \rangle\langle b \rangle = \langle b \rangle\langle a \rangle$, $\langle a \rangle \cap \langle b \rangle = \{e\}$. G ist genau dann abelsch, wenn $r \equiv 1 \mod n$, dh. wenn τ trivial ist. Spezialfall: $1 \neq n \in \mathbb{N}$, $m = 2$ und $r = -1$. Dann ist

$$\mathbb{Z}/\mathbb{Z}n \times_\tau \mathbb{Z}/\mathbb{Z}2 = \{e, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\} \text{ mit } \operatorname{ord}(a) = n, \operatorname{ord}(b) = 2, ba = a^{n-1}b$$

die bereits bekannte Diedergruppe der Ordnung $2n$.

2.3.7 Beispiele: Symmetrische Gruppe

(a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 1 & 6 \end{pmatrix} = (13425) \in \mathfrak{S}_6$

(b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 1 & 4 & 7 & 9 & 3 & 8 & 6 & 5 & 10 \end{pmatrix} = (12)(34786)(59)$

(c) Sei p prim, $\sigma = (a_1 \dots a_p)$ ein p-Zykel. Dann sind auch $\sigma^2, \dots, \sigma^{p-1}$ p-Zyklen, denn diese Elemente haben alle Ordnung p. Dagegen: für $\sigma = (1234)$ ist $\sigma^2 = (13)(24)$.

(d) Es gilt $|\mathfrak{S}_3| = 6$, $|A_3| = 3$. Man macht sich leicht klar, daß

$$\begin{aligned} \mathfrak{S}_3 &= \{\mathrm{id}, (123), (132), (12), (13), (23)\} \\ A_3 &= \{\mathrm{id}, (123), (132)\} \lhd \mathfrak{S}_3 \end{aligned}$$

Als nächstes betrechten wir die Gruppe $\mathfrak{S}_4$. Analog zu oben gilt $|\mathfrak{S}_4| = 24$, $|A_4| = 12$. Es ist nun bereits weit aufwendiger, die Gruppen auszurechenen:

$$\begin{aligned} \mathfrak{S}_4 &= \{\mathrm{id}, (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), \\ &\quad (143), (234), (243), (1234), (1243), (1324), (1342), (1423), (1432)\} \\ A_4 &= \{\mathrm{id}, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\} \lhd \mathfrak{S}_4 \\ V &= \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd \mathfrak{S}_4 \quad \text{die Klein'sche Vierergruppe} \end{aligned}$$

Also ist A_4 semidirektes Produkt aus V und den Untergruppen der Ordnung 3.

2.3.8 Beispiele: Sylow-Sätze

(a) $G = \mathfrak{S}_3$. 2-Sylowuntergruppen: $\langle(12)\rangle$, $\langle(13)\rangle$, $\langle(23)\rangle$. 3-Sylowuntergruppe: $\langle(123)\rangle$.

(b) Die Sylowuntergruppen einer endlichen abelschen Gruppe sind genau die p-Komponenten.

(c) Eine Gruppe der Ordnung 6 ist isomorph zu $\mathbb{Z}/6\mathbb{Z}$ oder zu $D_3 \cong \mathfrak{S}_3$.

(d) Die Sylowuntergruppen von $\mathfrak{S}_4$:

(i) $p = 2$: $\mathfrak{S}_4$ enthält eine Diedergruppe der Ordnung 8, diese ist 2-Sylowuntergruppe. Also sind die 2-Sylowuntergruppen von $\mathfrak{S}_4$ genau die Diedergruppen der Ordnung 8, die in $\mathfrak{S}_4$ enthalten sind. Für deren Anzahl s_2 gilt, $s_2 \mid 3$ und $s_2 \equiv 1 \mod 2$. Also $s_2 \in \{1, 3\}$. Da $\mathfrak{S}_4$ mehr als 8 Elemente enthält, deren Ordnung 2-Potenz ist, folgt $s_2 = 3$.
V ist in jeder 2-Sylowuntergruppe enthalten, offenbar ist dann $V = O_s(\mathfrak{S}_4)$.

(ii) $p = 3$: Die 3-Sylowuntergruppen von $\mathfrak{S}_4$ sind genau die Untergruppen der Ordnung 3. Für deren Anzahl gilt $s_3 = 4$.

(e) Die Sylowuntergruppen von A_4:

(i) $p = 2$: V.

(ii) $p = 3$: Wie in $\mathfrak{S}_4$.

2.3.9 Beispiele: nilpotente und auflösbare Gruppen

(a) Endliche abelsche Gruppen sind nilpotent.

(b) $\mathfrak{S}_3$ ist nicht nilpotent.

(c) Allgemein gilt: D_n ist genau dann nilpotent, wenn n Potenz von 2 ist.

(d) Abelsche Gruppen, endliche p-Gruppen und endliche nilpotente Gruppen sind auflösbar.

(e) $\mathfrak{S}_3$ und $\mathfrak{S}_4$ sind auflösbar mit den Normalreihen mit abelschen Faktoren

$$\mathfrak{S}_3 \supset A_3 \supset \{e\} \quad \text{und} \quad \mathfrak{S}_4 \supset A_4 \supset V \supset \{e\}$$

aber nicht nilpotent.

(f) D_n, $n \geqslant 2$, ist auflösbar, denn jede solche Gruppe hat einen zyklischen Normalteiler vom Index 2.

(g) Endliche, einfache nicht-abelsche Gruppen sind nicht auflösbar. Insbesondere sind die Gruppen A_n für $n \geqslant 5$ nicht auflösbar. Damit sind auch die $\mathfrak{S}_n$ für $n \geqslant 5$ nicht auflösbar.

(h) Sind $p \neq q$ Primzahlen, $a, b \in \mathbb{N}$. Dann ist jede Gruppe der Ordnung $p^a q^b$ auflösbar (Burnside).

(i) Jede Gruppe ungerader Ordnung ist auflösbar (Feit, Thompson).

3 Ringtheorie: kurze Wiederholung

3.1 Themen

Unterringe
Ideale: maximale Ideale, Primideale
Faktorringe
Homomorphiesatz
Isomorphiesätze
Polynomalgebren
Integritätsringe
Faktorielle Ringe
Euklidische Ringe
Division mit Rest
Quotientenringe
Quarakteristik
Teilbarkeit, Irreduzibilität
Chinesischer Restsatz

3.2 Einige wichtige Konzepte

3.2.1 Ringaxiome

Eine Menge R zusammen mit zwei Abbildungen $+ : R \times R \to R, (r, s) \mapsto r + s$ und $\cdot : R \times R \to R, (r, s) \mapsto rs$, heißt Ring mit Einselement, wenn gilt:

(a) Additive Gruppe: $(R, +)$ ist abelsche Gruppe; neutrales Element sei 0, Inverses von $r \in R$ sei $-r$.

(b) Multiplikatives Monoid: $(R, \cdot)$ ist Monoid (nicht notwendigerweise Inverses); neutrales Element sei 1.

(c) Distributivgesetz: Für alle $r, s, t \in R$ gilt: $(r + s)t = rt + st$ und $r(s + t) = rs + rt$.

— Einheitengruppe: $R^\times = \{$ invertierbare Elemente $\}$
— Kommutativer Ring: $(R, \cdot)$ kommutativ
— Schiefkörper: $1 \neq 0$ und $R^\times = (R \backslash \{0\})$
— Körper: R kommutativ, $1 \neq 0$ und $R^\times = (R \backslash \{0\})$

3.2.2 Unterringe

Sei R ein Ring. Eine Teilmenge $S \subset R$ heißt Unterring, wenn S Untergruppe von $(R, +)$ und Untermonoid von $(R, \cdot)$ ist. Dann ist S bezüglich $+$ und $\cdot$ ein Ring.
S ist genau dann Unterring von R, wenn gilt $1 \in S$ und für alle $s, t \in S$ ist $s - t \in S$ und $st \in S$.

3.2.3 Ideale

Eine Teilmenge $A \subset R$ heißt Linksideal von R, wenn A Untergruppe von $(R, +)$ ist, und für alle $a \in A$, $r \in R$ gilt $ra \in A$.
Genauso Rechtsideal/ beidseitiges Ideal.

— Beliebige Schnitte von Idealen: Ist $(A_i)_{i \in I}$ Familie von (Links-/Rechts-)Idealen, dann ist auch

$$\bigcap_{i \in I} A_i$$

(Links-/Rechts-)Ideal.

— Endliche Summen von Idealen: Sind $A_1, \ldots A_n$ (Links-/Rechts-)Ideale, dann ist

$$A_1 + \ldots + A_n = \left\{ x \in R \;\middle|\; \exists a_i \in A_i, 1 \leqslant i \leqslant n : x = a_1 + \ldots + a_n \right\}$$

(Links-/Rechts-)Ideal.

— Erzeugtes Ideal: Ist $X \subset R$ Teilmenge, dann ist

$$\begin{aligned} {}_R(X) &= \bigcap \{A \mid A \text{ Linksideal von } R \text{ mit } X \subset A\} \\ &= \left\{ r \in R \mid \exists n \in \mathbb{N}_0, x_1, \ldots, x_n \in X, r_1, \ldots, r_n \in R : r = \sum_{i=1}^{r} r_i x_i \right\} \end{aligned}$$

das kleinste Linksideal, das X enthält.
Sind $a_1, \ldots, a_r \in R$, dann

$$Ra_1 + \ldots + Ra_n = {}_R(a_1, \ldots, a_n) = {}_R(\{a_1, \ldots, a_n\}) = \left\{ r \in R \mid \exists r_1, \ldots, r_n \in R : r = \sum_{i=1}^{n} r_i a_i \right\}.$$

3.2.4 Ringhomomorphismen

Eine Abbildung $\varphi : R \to R'$ zwischen zwei Ringen heißt Ringhomomorphismus, falls $\varphi : (R, +) \to (R', +)$ Gruppenhomomorphismus ist, und $\varphi : (R, \cdot) \to (R', \cdot)$ Monoidhomomorphismus ist.
Bilder/Urbilder von Unterringen sind Unterringe.
Urbilder von Idealen sind Ideale. Ist ein Homomorphismus surjektive, so sind auch Bilder von Idealen Ideale.
Sei R ein kommutativer Ring. Ein Ring R' (mit Eins) heißt R-Algebra, wenn es einen Ringhomomorphismus $\varphi : R \to R'$ gibt mit $\mathrm{im}(\varphi) \subset Z(R')$. Man definiert dann eine Skalarmultiplikation von R auf R' durch

$$r.r' = \varphi(r)r' \quad \text{für } r \in R, r' \in R'.$$

Eine Algebra ist gleichzeitig ein Ring und ein Vektorraum.

3.2.5 Faktorringe

R ein Ring, $A \subset R$ ein zweiseitiges Ideal.
Der Faktorring von R modulo A ist die Menge R/A der Nebenklassen additiven Nebenklassen $r + A$ mit Addition

$$R/A \times R/A \to R/A, (r + A, s + A) \mapsto r + s + A$$

und Multiplikation

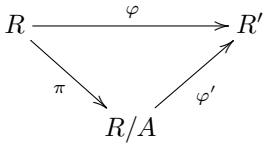
$$R/A \times R/A \to R/A, (r + A, s + A) \mapsto rs + A.$$

Die kanonische Projektion:

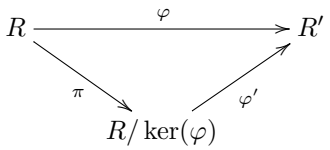
$$\pi : R \to R/A, r \mapsto r + A$$

ist ein surjektiver Ringhomomorphismus mit $\ker(\pi) = A$.
Sei $\varphi : R \to R'$ ein Ringhomomorphismus.

(a) Ist A Ideal von R mit $A \subset \ker(\varphi)$, dann gibt es genau einen Ringhomomorphismus $\varphi' : R/A \to R$ mit $\varphi = \varphi' \circ \pi$.



(b) **(Homomorphiesatz)** Es gibt genau einen injektiven Ringhomomorphismus $\varphi' : R/\ker(\varphi) \to R'$ mit $\varphi = \varphi' \circ \pi$.



Insbesondere ist die Abbildung

$$\varphi : R/\ker(\varphi) \to \mathrm{im}(\varphi), r + \ker(\varphi) \mapsto \varphi(r)$$

ein Ringisomorphismus.

(c) **(1. Isomorphiesatz)** Sei $S \subset R$ ein Unterring, $A \subset R$ ein Ideal. Dann ist $S \cap A \subset S$ ein Ideal, $S + A \subset R$ Unterring, $A \subset S + A$ ein Ideal, und die Abbildung

$$S/S \cap A \to S + A/A, s + S \cap A \mapsto s + A$$

ein Ringisomorphismus.

(d) **(2. Isomorphiesatz)** Seien A, B Ideale von R mit $A \subset B$. Dann ist $B/A \subset R/A$ ein Ideal, und die Abbildung

$$R/B \to (R/A)/(B/A), r + B \mapsto (r + A) + B/A$$

ein Ringisomorphismus.

3.2.6 Polynomalgebren

Sei R ein komutativer Ring. Ein Polynom über R in einer Variablen ist ein formale Summe

$$f = a_n X^n + \ldots + a_1 X + a_0 = \sum_{i=0}^{n} a_i X^i$$

Die Variable X ist unabhängig von den Elementen des Rings.

$$R[X] = \left\{ f = \sum_{i \geqslant 0} a_i X^i \;\middle|\; \text{fast alle } a_i = 0 \right\}$$

ist ein kommutativer Ring mit der "gewöhnlichen" Addition und Multipikation.

$$\begin{aligned} (\sum_{i \geqslant 0} a_i X^i) + (\sum_{i \geqslant 0} b_i X^i) &= \sum_{i \geqslant 0} (a_i + b_i) X^i \\ (\sum_{i \geqslant 0} a_i X^i) \cdot (\sum_{i \geqslant 0} b_i X^i) &= \sum_{i \geqslant 0} (\sum_{k+l=i} a_k b_l) X^i \end{aligned}$$

mit additivem beziehungsweise multiplikativem Inversen

$$\begin{aligned} 1_{R[X]} &= 1X^0 = 1 \\ 0_{R[X]} &= 0X^0 = 0 \end{aligned}$$

Grad eines Polynoms $f \in R[X]$:

$$\deg(f) := \begin{cases} \infty & \text{falls } f = 0 \\ \max\{n \in \mathbb{N}_0 : a_n \neq 0\} & \text{sonst} \end{cases}$$

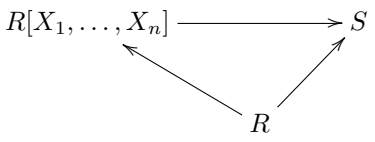
Es gilt $\deg(f \cdot g) \leqslant \deg(f) + \deg(g)$.
Rekursiv definiert man Polynomringe in mehreren Variablen:

$$R[X_1, \ldots, X_n] := R[X_1, \ldots, X_{n-1}][X_n].$$

Man betrachtet hier also Polynome in der Variablen X_n mit Koeffizienten in dem kommutativen Ring $R[X_1, \ldots, X_{n-1}]$.

3.2.7 Einsetzungshomomorphismus

Sei S eine kommutative R-Algebra, sei $n \in \mathbb{N}$ und $(s_1, \ldots, s_n) \in S^n$. Dann gibt es genau einen R-Algebren-Homomorphismus $\rho : R[X_1, \ldots, X_n] \to S$, mit $\rho(X_i) = s_i$, $1 \leqslant i \leqslant n$.



Man schreibt $\rho(f) = f(s_1, \ldots, s_n)$.
$(s_1, \ldots, s_n)$ heißt Nullstelle von f, falls $\rho(f) = f(s_1, \ldots, s_n) = 0$.

3.2.8 Division mit Rest in $R[X]$

Sei R ein kommutativer Ring, $0 \neq f \in R[X]$ ein Polynom, dessen höchster Koeffizient eine Einheit in R ist. Zu jedem $g \in R[X]$ gibt es dann eindeutig bestimmte Polynome $q, h \in R[X]$ mit $g = qf + h$ und $\deg(h) < \deg(f)$.
Seien $f \in R[X]$, $c \in R$.

(a) Es gibt $g \in R[X]$ mit $f = (X - c)g + f(c)$.

(b) c ist genau dann Nullstelle von f, wenn es $g \in R[X]$ gibt mit $f = (X - c)g$.

3.2.9 Integritätsringe

Ein kommutativer Ring heißt Integritätsring oder Integritätsbereich, wenn $1 \neq 0$ und $(R\backslash\{0\}, \cdot)$ Untermonoid von $(R, \cdot)$ ist, das heißt, wenn $1 \neq 0$ und für alle $r, s \in R\backslash\{0\}$ gilt $rs \neq 0$.

„Kürzungsregel“: Ein kommutativer Ring R ist genau dann Integritätsbereich, wenn $1 \neq 0$ und für alle $r, s, t \in R$ mit $rs = rt$ und $r \neq 0$ folgt $s = t$.

Für einen Integritätsbereich R gelten viele nützliche Eigenschaften.
- $R[X_1, \ldots, X_n]$ ist Integritätsring, für $f, g \in R[X_1, \ldots, X_n]$ gilt $\deg(fg) = \deg(f) + \deg(g)$.
- $R[X_1, \ldots, X_n]^\times = R^\times$.
- Jedes Polynom $0 \neq f \in R[X]$ hat höchstens $\deg(f)$ Nullstellen.

3.2.10 Euklidische Ringe

Ein Integritätsring R heißt euklidisch, wenn es eine Abbildung $\delta : R\backslash\{0\} \to \mathbb{N}_0$ gibt, so daß gilt: Für alle $a, b \in R$, $b \neq 0$, gibt es $q, r \in R$ mit $a = bq + r$ und wenn $r \neq 0$ ist, dann $\delta(r) < \delta(b)$. Eine solche Abbildung heißt euklidische Norm.

Ein Integritätsring R heißt Hauptidealring, wenn jedes Ideal von R Hauptideal ist.
In einem euklidischen Ring ist jedes Ideal ein Hauptideal, das heißt, von einem Element erzeugt.

Merkregel: Es gelten folgende Inklusionen für kommutative Ringe:

Körper $\subset$ Euklidische Ringe $\subset$ Hauptidealringe $\subset$ faktorielle Ringe $\subset$ Integritätsringe

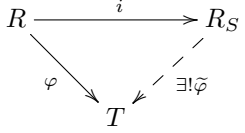
3.2.11 Quotientenringe

Idee: Man will eine multiplikativ abgeschlossene Teilmenge eines (kommutativen) Rings $S \subset R \setminus \{0\}$ invertieren.

Konstruktion: Definiere auf $R \times S$ eine Äquivalenzrelation:

$$(r, s) \sim (r', s') \text{ genau dann wenn es } t \in S \text{ gibt, so daß } (rs' - r's)t = 0.$$

Man setzt $R_S = R \times S/\sim$ und bezeichnet die Äquivalenzklasse von (r, s) mit $\frac{r}{s}$. Also gilt $\frac{r}{s} = \frac{r'}{s'}$ genau dann wenn es $t \in S$ gibt mit $(rs' - r's)t = 0$.
- Dies ist ein kommutativer Ring mit Null $\frac{0}{1}$ und Eins $\frac{1}{1}$.
- Kanonische Abbildung: $i : R \to R_S$, $r \mapsto \frac{r}{1}$ ist Ringhomomorphismus mit $\ker(i) = \{r \in R \mid \exists s \in S : rs = 0\}$.
- Für alle $s \in S$ ist $i(s) = \frac{s}{1}$ Einheit von R_S.
- Ist R ein Integritätsring, dann ist das t aus der Definition nicht notwendig, und i injektiv. Schreibe $r = \frac{r}{1}$.
- Universelle Eigenschaft: Ist T ein kommutativer Ring, $\varphi : R \to T$ Ringhomomorphismus mit $\varphi(S) \subset T^\times$, dann gibt es genau einen Ringhomomorphismus $\widetilde{\varphi} : R_S \to T$ mit $\widetilde{\varphi} \circ i = \varphi$, das heißt, das Diagramm



— Ideale: gegeben durch $(i(A)) = \left\{ \frac{a}{s} \; ; \; a \in A, s \in S \right\}$, $A \subset R$ Ideal.

3.2.12 Charakteristik

R Integritätsring.
Primring: $R_0 = \mathbb{Z} \cdot 1$ ist der kleinste Unterring von R.

Zwei Fälle sind möglich:

(a) $R_0 \cong \mathbb{Z}$; genau dann, wenn $z1 \neq 0$ für alle $z \in \mathbb{Z} \setminus \{0\}$.

(b) Es gibt eine Primzahl $p \in \mathbb{N}$ mit $R_0 \cong \mathbb{Z}/(p)$; p ist die kleinste natürliche Zahl $z \in \mathbb{N}$ mit $z.1 = 0$.

K Körper.
Primkörper: K_0 ist der kleinste Unterkörper von K.

Zwei Fälle sind möglich:

(a) $K_0 \cong \mathbb{Q}$; genau dann, wenn $z.1 \neq 0$ für alle $z \in \mathbb{Z} \setminus \{0\}$.

(b) Es gibt eine Primzahl $p \in \mathbb{N}$ mit $K_0 \cong \mathbb{Z}/(p)$; p ist die kleinste natürliche Zahl $z \in \mathbb{N}$ mit $z.1 = 0$.

Charakteristik von K:

$$\operatorname{char}(K) = \begin{cases} 0 & \text{falls für alle } 0 \neq z \in \mathbb{Z} : z.1 \neq 0 \\ p & \text{Primzahl, falls } p \text{ die kleinste natürliche Zahl ist mit } z.1 = 0 \end{cases}$$

3.2.13 Maximale Ideale

Sei R ein Ring. Ein (Links-/Rechts-/beidseitiges) Ideal $A \subset R$ heißt maximal, wenn $A \neq R$ ist und es kein (Links-/Rechts-/beidseitiges) Ideal $B \subset R$ gibt, mit $A \subsetneq B \subsetneq R$.

— Jedes (Links-/Rechts-/beidseitige) Ideal ist in einem maximalen enthalten.
— Jeder kommutative Ring $R \neq 0$ besitzt ein maximales Ideal.
— Sei R ein kommutativ, $A \subset R$ ein Ideal. A ist genau dann maximal, wenn R/A ein Körper ist.

3.2.14 Primideale

Sei R ein kommutativer Ring. Ein Ideal $P \subset R$ heißt Primideal, wenn $P \neq R$ und wenn für alle $r, s \in R$ gilt: ist $rs \in P$, dann ist $r \in P$ oder $s \in P$.
Äquivalent dazu:
— $R \setminus P$ ist multiplikativ abgeschlossen.
— R/P ist Integritätsbereich.
In einem kommutativen Ring ist jedes maximale Ideal auch Primideal.

3.2.15 Irreduzible Elemente, Primelemente

Sei R ein kommutativer Ring, $r, s \in R$.

Teiler: $r \big| s$, wenn $\exists t \in R$ mit $s = rt$, genau dann, wenn $(s) \subset (r)$.

Assoziiert: $r \sim s$, wenn $r \big| s$ und $s \big| r$, genau dann, wenn $(s) = (r)$.

Echter Teiler: $r \big| s$, $r \notin R^\times$ und r nicht zu s assoziiert ist, genau dann, wenn $(s) \subsetneq (r) \subsetneq R$.

Irreduzibel: r heißt irreduzibel oder unzerlegbar, wenn $r \notin R^\times \cup \{0\}$ und r keine echten Teiler hat,

Sei R Integritätsring. Ein Element $p \in R$ heißt Primelement, wenn $p \in R \setminus (R^\times \cup \{0\})$ und für alle $r, s \in R \setminus \{0\}$ gilt: falls $p \big| rs$, dann $p \big| r$ oder $p \big| s$, das heißt, wenn $p \neq 0$ und (p) Primideal ist.
Sei R Integritätsring.
— Ist $p \in R$ ein Primelement, $p \big| r_1 \cdots r_n$, dann gibt es $1 \leqslant i \leqslant n$ so daß $p \big| r_i$.
— Jedes Primelement ist irreduzibel.
— Ist R sogar Hauptidealring, dann ist ein Element genau dann Primelement, wenn es irreduzibel ist.
— Die Zerlegung eines Elements in Primelemente ist eindeutig (bis auf Ordnung und Einheiten), falls sie existiert.

Faktorieller Ring: Ein Integritätsring heißt faktoriell, wenn jedes Element $r \in R\backslash(R^\times \cup \{0\})$ Produkt von Primelementen ist.

Äquivalent dazu:
- Jedes Element $r \in R\backslash(R^\times \cup \{0\})$ ist Produkt von irreduziblen Elementen, und je zwei solche Zerlegungen sind äquivalent.
- Es gibt eine Teilmenge $P \subset R\backslash\{0\}$ mit der Eigenschaft, daß es zu jedem Element $r \in R\backslash\{0\}$ eine eindeutig bestimmte Einheit $u_r \in R^\times$ und eine eindeutig bestimmte Familie $(\nu_p(r))_{p\in P}$ von Zahlen in $\mathbb{N}_0$, fast alle Null, gibt, mit $r = u_r \prod_{p\in P} p^{\nu_p(r)}$.

3.2.16 kgV und ggT

Sei R Integritätsring und $r_1, \ldots, r_n, v, t \in R\backslash\{0\}$.

kgV v heißt kleinstes gemeinsames Vielfaches von $r_1, \ldots, r_n$, wenn:
(a) v ist Vielfaches der r_i, d.h. $r_i \big| v$ für alle $1 \leqslant i \leqslant n$
(b) v teilt alle anderen Vielfachen der r_i, d.h. für alle $s \in R\backslash\{0\}$ mit $r_i \big| s$ für alle $1 \leqslant i \leqslant n$ folgt $v \big| s$.

ggT t heißt größter gemeinsamer Teiler der $r_1, \ldots, r_n$, wenn:
(a) t ist Teiler der r_i, d.h. $t \big| r_i$ für alle $1 \leqslant i \leqslant n$,
(b) t wird von allen anderen Teilern der r_i geteilt, d.h. falls $s \big| r_i$ für alle $1 \leqslant i \leqslant n$, dann $s \big| t$.

Teilerfremd $r_1, \ldots, r_n$ heißen teilerfremd bzw. relativ prim, wenn 1 ein ggT von ihnen ist.

Sei R ein Integritätsring, $r_1, \ldots, r_n, v, t \in R\backslash\{0\}$.
(a) v ist genau dann ein kgV von $r_1, \ldots, r_n$, wenn $(v) = \bigcap_{i=1}^n (r_i)$.
(b) Gilt $(t) = \sum_{i=1}^n (r_i) = (r_1, \ldots, r_n)$, dann ist t ein ggT von $r_1, \ldots, r_n$.
Ist R Hauptidealring, gilt die Umkehrung: t ist genau dann ein ggT von $r_1, \ldots, r_n$, wenn $(t) = (r_1, \ldots, r_n)$.

Bekannte historische Resultate:

Lemma von Bezout Sei R Hauptidealring. $r_1, \ldots, r_n$ sind genau dann teilerfremd, wenn es $s_1, \ldots, s_n \in R$ gibt, mit $\sum_{i=1}^n s_i r_i = 1$.

Lemma von Euklid Sei R faktoriell, $r, s, t \in R\backslash\{0\}$. Gilt $r \big| st$ und sind r und s teilerfremd, dann gilt $r \big| t$.

euklidischer Algorithmus Seien $r, s \in R\backslash\{0\}$. Dann gibt es $n \in \mathbb{N}_0$, und Folgen

$$r_{-1} = r, r_0 = s, r_1, \ldots, r_n \in R\backslash\{0\} \quad \text{und} \quad q_1, \ldots q_{n+1} \in R$$

mit

$$\begin{aligned} r &= q_1 s + r_1, \quad \delta(r_1) < \delta(s) \\ s &= q_2 r_1 + r_2, \quad \delta(r_2) < \delta(r_1) \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, \quad \delta(r_n) < \delta(r_{n-1}) \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

Für $0 \neq c \in R$ gilt

$$c \big| r, s \Leftrightarrow c \big| s, r_1 \Leftrightarrow c \big| r_1, r_2 \Leftrightarrow \cdots \Leftrightarrow c \big| r_{n-2}, r_{n-1} \Leftrightarrow c \big| r_n.$$

Durch rekursives Einsetzen im Euklidischen Algorithmus erhält man $a, b \in R$ mit $r_n = ra + sb$.

3.2.17 Faktorielle Polynomringe

Sei R ein faktorieller Ring und $K = \mathrm{Frac}(R)$.
- $R[X]$ und $R[X_1, X_2, \ldots, X_n]$ sind faktoriell.
- Ist $A \subset R$ ein Ideal, so ist

$$R[X]/AR[X] \to (R/A)[X], f + AR[X] \mapsto \overline{f}$$

  ein R-Algebrenisomorphismus.
- $A \subset R$ ist Primideal $\Leftrightarrow$ $AR[X] \subset R[X]$ ist Primideal. $p \in R$ ist ein Primelement in R, genau dann, wenn es Primelement in $R[X]$ ist.
- $f \in R[X]$ heißt primitiv, wenn die Koeffizienten teilerfremd sind. Sind $f, g \in R[X]$ primitiv, so auch fg.
- Die Primelemente in $R[X]$ sind die Primelemente in R und die primitiven irreduziblen Polynome.
- In K: Für $0 \neq f \in K[X]$ gibt es x in K und $\widetilde{f} \in R[X]$ primitiv mit $f = x\widetilde{f}$ (eindeutig bis auf Einheiten in R). $\Rightarrow$ für Irreduziblität genügt es in $R[X]$ zu arbeiten.
  Sei $f \in R[X] \backslash R$.
  (a) Ist f nicht Produkt von nichtkonstanten Polynomen in $R[X]$, dann ist f in $K[X]$ irreduzibel.
  (b) Ist f in $R[X]$ irreduzibel, dann ist f auch in $K[X]$ irreduzibel.
  (c) Ist f primitiv und irreduzibel in $K[X]$, dann ist f irreduzibel in $R[X]$.
  (d) Sind $f, g \in R[X]$, sei f primitiv. Gilt $f \big| g$ in $K[X]$, dann gilt $f \big| g$ auch in $R[X]$.
  (e) Ist $f \in R[X]$ normiert, und und $g, h \in K[X]$ normiert mit $f = gh$, dann gilt $g, h \in R[X]$.

3.2.18 Irreduzibilitätskriterien

R Integritätsring.

Homomorphismus SeiR' ein weiterer Integritätsring, $f \in R[X] \backslash R$ primitiv, $\varphi : R[X] \to R'$, der nichtkonstante Faktoren von f auf Nichteinheiten abbildet. Ist $\varphi(f)$ irreduzibel, dann ist auch f irreduzibel. (Sehr allgemein, selten so verwendet.)

Automorphismus Sei $\varphi : R[X] \to R[X]$ ein Automorphismus, $f \in R[X] \backslash R$ primitiv. Ist $\varphi(f)$ irreduzibel, dann ist auch f irreduzibel. (Hilfreich, wenn man "den Trick sieht".)

Reduktionskriterium Seien $\mathfrak{P} \subset R$ ein Primideal, $\pi : R \to R/\mathfrak{P}$ der kanonische Homomorphismus, sei $f = \sum_{i=0}^{n} r_i X^i \in R[X] \backslash R$ primitiv mit $r_n \notin \mathfrak{P}$. Ist ${}^{\pi}f \in (R/\mathfrak{P})[X]$ irreduzibel, dann ist auch f irreduzibel. (Sehr nützlich.)

Eisensteinkriterium Sei $0 \neq f = \sum_{i=0}^{n} r_i X^i \in R[X]$ primitiv, $p \in R$ ein Primelement mit $p \nmid r_n$ aber $p \big| r_j$ für alle $0 \leqslant j \leqslant n-1$, und $p^2 \nmid r_0$. Dann ist f in $R[X]$ irreduzibel.

3.2.19 Chinesischer Restsatz

Allgemeine Version:
Seien $A_1, \ldots, A_n$ paarweise fremde Ideale von R.

(a) Die Abbildung

$$\begin{aligned} R/A_1 \cdots A_n &\to \prod_{i=1}^{n} R/A_i \\ r + A_1 \cdots A_n &\mapsto (r + A_1, \ldots, r + A_n) \end{aligned}$$

ist ein R-Algebrenisomorphismus.

(b) Die Abbildung

$$\begin{aligned} (R/A_1 \cdots A_n)^* &\to \prod_{i=1}^{n} (R/A_i)^* \\ r + A_1 \cdots A_n &\mapsto (r + A_1, \ldots, r + A_n) \end{aligned}$$

ist ein Gruppenisomorphismus.

Bekanntere Version: R Hauptidealring (z.B. $R = \mathbb{Z}$)
Seien $a_1, \ldots, a_n \in R \backslash \{0\}$ paarweise teilerfremd.

(a) Die Abbildung

$$\begin{aligned} R/(a_1 \cdots a_n) &\to \prod_{i=1}^{n} R/(a_i) \\ r + (a_1 \cdots a_n) &\mapsto (r + (a_1), \ldots, r + (a_n)) \end{aligned}$$

ist ein R-Algebrenisomorphismus.

(b) Die Abbildung

$$\begin{aligned} (R/(a_1 \cdots a_n))^* &\to \prod_{i=1}^{n} (R/(a_i))^* \\ r + (a_1 \cdots a_n) &\mapsto (r + (a_1), \ldots, r + (a_n)) \end{aligned}$$

ist ein Gruppenisomorphismus.

Zu $b_1, \ldots, b_n \in R$ gibt es also $r \in R$ mit $r \equiv b_i \mod a_i$ für $1 \leqslant i \leqslant n$, und r ist modulo $a_1 \cdots a_n$ eindeutig bestimmt.

3.3 Beispiele

3.3.1 Beispiele: Ringe

(a) $\mathbb{Z}$, $\mathbb{Z} / \mathbb{Z}\, a$ für $a \in \mathbb{Z}$ sind kommutative Ringe. $\mathbb{Z}$ ist Unterring von $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. $\mathbb{Q}$ ist Unterring von $\mathbb{R}$, $\mathbb{C}$.

(b) Sei $d \in \mathbb{Z} \setminus \{0, 1\}$.

$$R = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

ist Unterring von $\mathbb{C}$, sogar Körper.

$$S = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

ist Unterring von R.

(c) Sei R ein Ring, $n \in \mathbb{N}$. Die Menge $R^{n \times n}$ der (n, n)-Matrizen mit Koeffizienten in R ist Ring bezüglich der üblichen Addition und Multiplikation von Matrizen. $(R^{n,n})^\times = \mathbf{GL}_n(R)$ ist die Gruppe der invertierbaren Matrizen in $R^{n \times n}$.

(d) Sei R Ring. Dann ist das Zentrum

$$Z(R) = \{r \in R \mid \forall s \in R : rs = sr\}$$

ein kommutativer Unterring von R

(e) Sei R ein kommutativer Ring, $n \in \mathbb{N}$. Dann ist $R^{n,n}$ eine R-Algebra bezüglich

$$\varphi : R \to R^{n,n}, r \mapsto \begin{pmatrix} r & 0 & \cdots & 0 \\ 0 & r & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & r \end{pmatrix}.$$

Die Skalarmultiplikation dazu ist $r.(r_{ij}) = (rr_{ij})$.

(f) Sei R ein Ring. Dann ist

$$\varphi : \mathbb{Z} \to R, z \mapsto z.1$$

ein Ringhomomorphismus mit $\mathrm{im}(\varphi) \subset Z(R)$. Also ist R eine $\mathbb{Z}$-Algebra. Die Skalarmultiplikation dazu ist die von den abelschen Gruppen her bekannte.

3.3.2 Beispiele: Ideale

(a) In einem Ring R sind $\{0\}$ und R selbst stets Ideale.

(b) Sei R ein Ring, A (Links-/Rechts-)Ideal mit $R^\times \cap A \neq \emptyset$. Dann gilt $A = R$. Für Linksideal sieht man das wie folgt: Sei $a \in R^\times \cap A$. Dann gibt es $a' \in R$ so daß $a'a = 1$. Damit gilt für alle $r \in R$: $r = ra'a \in A$.

(c) Sei R kommutativer Ring. R ist genau dann Körper, wenn $1 \neq 0$ und $\{0\}$ und R die einzigen Ideale von R sind.

(d) Die Ideale von $\mathbb{Z}$ sind genau die Untergruppen $\mathbb{Z}\,a$, für $a \in \mathbb{Z}$.

3.3.3 Beispiele: Integritätsringe

(a) $\mathbb{Z}$ ist ein Integritätsbereich, Körper sind Integritätsbereiche.

(b) Unterringe von Integritätsringen sind Integritätsringe. Insbesondere sind Unterringe von Körpern Integritätsringe.

(c) Sei $n \in \mathbb{N}_0$. $\mathbb{Z}/n\,\mathbb{Z}$ ist genau dann Integritätsbereich, wenn $n = 0$ oder n Primzahl ist.

(d) Ist R ein Integritätsbereich, so ist auch $R[X_1, \dots X_n]$ ein Integritätsbereich.

3.3.4 Beispiele: Euklidische Ringe

(a) $\mathbb{Z}$ ist euklidisch bezüglich $\delta : \mathbb{Z} \to \mathbb{N}_0$, $z \mapsto |z|$.

(b) Sei K ein Körper. $K[X]$ ist euklidisch bezüglich $K[X]\backslash\{0\} \to \mathbb{N}_0$, $f \mapsto \deg(f)$.

(c) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} = \mathbb{Z} \oplus \mathbb{Z}\,i$ ist Unterring von $\mathbb{C}$, der $\mathbb{Z}$ enthält; er heißt Ring der ganzen Gaußschen Zahlen. $\delta : \mathbb{Z}[i] \to \mathbb{N}_0$, $x = a + bi \mapsto x\overline{x} = a^2 + b^2$ ist euklidische Norm.

3.3.5 Beispiele: Hauptidealringe

(a) $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[X]$ für einen Körper K sind Hauptidealringe, sogar euklidische Ringe.

(b) $\mathbb{Z}[X]$ und $K[X, Y]$ sind **keine** Hauptidealringe, also auch nicht euklidisch.

3.3.6 Beispiele: Quotientenringe

(a) Ist R Integritätsring, dann ist S=$R\backslash\{0\}$ multiplikativ abgeschlossen. Dann ist $\mathrm{Frac}(R) := R_S$ ein Körper (Quotientenkörper.
— $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$
— K ein Körper: $K(X_1, \dots, X_n) = \mathrm{Frac}(K[X_1, \dots, X_n])$, Körper der rationalen Funtionen
— $\mathrm{Frac}(\mathbb{Z}[i]) = \mathbb{Q}[i] = \left\{a + bi \in \mathbb{C} \;\middle|\; a, b \in \mathbb{Q}\right\}$, es genügt $S = \mathbb{Z}\backslash\{0\}$ zu invertieren.

(b) $s \in R$. $S = \{s^n \mid n \in \mathbb{N}_0\}$ ist genau dann multiplikativ abgschlossen, wenn $s^n \neq 0$ für alle $n \in \mathbb{N}$ ist, das heißt, wenn s nicht nilpotent ist. Dies ist in einem Integritätsring für alle $s \neq 0$ erfüllt.

$$R_S = \{\frac{r}{s^k} \mid r \in R\}.$$

(c) Sei $p \in \mathbb{N}$ Primzahl. Dann ist $\mathbb{Z}\backslash(p)$ multiplikativ abgeschlossene Teilmenge von $\mathbb{Z}$.

$$\mathbb{Z}_S =: \mathbb{Z}_{(p)} = \left\{\frac{r}{s} \;\middle|\; r \in R, s \in S\right\} = \left\{\frac{r}{s} \;\middle|\; r, s \in R, p \nmid s\right\}.$$

Ideale: $B = \mathbb{Z}_{(p)} \cdot A$, wobei $A \subset \mathbb{Z}$ Ideal mit $A \cap \{\mathbb{Z}\backslash(p)\} = \emptyset$, also $A \subset (p)$.
In $\mathbb{Z}_{(p)}$ ist (p) maximal bezüglich Inkusion (das einzige Ideal mit dieser Eigenschaft). Ein solcher Ring heißt lokal, $\mathbb{Z}_{(p)}$ heißt Lokalisierung von $\mathbb{Z}$ bei (p).

3.3.7 Beispiele: Maximale Ideale und Primideale

(a) Die maximalen Ideale von $\mathbb{Z}$ sind die Ideale (p), wobei p eine Primzahl ist. (Denn für $n \in \mathbb{N}_0$ gilt: (n) maximal genau dann, wenn $\mathbb{Z}/(n)$ Körper, genau dann, wenn n Primzahl.)

(b) Sei K Körper, dann ist $(X) = K[X]X$ maximales Ideal. (Denn $K[X]/X \to K, f + (X) \mapsto f(0) =$ konstanter Koeffizient von f ist Ringisomorphismus.)

(c) Die Primideal von $\mathbb{Z}$ sind (0) und die Ideale (p), p eine Primzahl. Das Ideal (0) ist nicht maximal.

(d) Sei R kommutativer Ring. Das Ideal (0) ist genau dann Primideal, bzw. maximales Ideal, wenn R Integritätsring, bzw. Körper, ist.

(e) Sei R Integritätsring. Dann ist $(X) = R[X]X$ Primideal in $R[X]$. (Denn $R[X]/X \to R, f + (X) \mapsto f(0)$ ist Ringisomorphismus.)

3.3.8 Beispiele: Irreduzible Elemente

(a) Sei K ein Körper, R der Unterring von $K[X]$ bestehend aus den Polynomen $f = \sum_{i=0}^{n} a_i X^i$, mit $a_1 = 0$. Es gilt $R = K[X^2, X^3]$. Außerdem gilt $R^\times = K^\times$. Die Elemente X^2 und X^3 sind in R irreduzibel: Sei $X^2 = fg$ mit $f, g \in R$, dann gilt $\deg(f), \deg(g) \in \{0, 2\}$, also $f \in R^\times$ oder $g \in R^\times$. Ebenso für X^3.
Die Elemente X^2 und X^3 sind in R nicht prim: Es gilt $X^6 = X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3$, und $X^2 \nmid X^3$ bzw. $X^3 \nmid X^2$. Also hat man zwei nicht-äquivalente Zerlegungen von X^6 in irreduzible Elemente gefunden.

3.3.9 Beispiele: Faktorielle Ringe

(a) Jeder Hauptidealring R ist faktoriell.

(b) $\mathbb{Z}$ ist faktoriell, mit $\mathbb{Z}^\times = \{-1, +1\}$, $P = \{p \in \mathbb{N} \mid p \text{ prim}\}$ ist Transversale der Primelemente von $\mathbb{Z}$ „modulo Einheiten“. P ist unendlich.

(c) Sei K Körper. Dann ist $K[X]$ faktoriell mit $K[X]^\times = K^\times$, $P = \{f \in K[X] \mid f \text{ normiert und irreduzibel }\}$ ist eine Transversale der Primelemente „modulo Einheiten“. P ist unendlich.

(d) Ist R faktoriell, so auch $R[X]$.

3.3.10 Beispiele: Irreduzibilität

(a) R faktoriell, $K = \operatorname{Frac} R$. Ein Polynom $f \in R[X]$, das reduzibel in $R[X]$ ist, aber irreduzibel in $K[X]$:
Sei $p \in R$ prim $r \in R$ beliebig, dann ist $f = pX - rp = p(X - r)$ nicht irreduzibel in $R[X]$ (insbesondere nicht primitiv), aber irreduzibel in $K[X]$, denn p ist invertierbar in K.

(b) Sei R ein Integritätsring. Ein normiertes Polynom $f \in R[X]$ vom Grad 2 oder 3 ist genau dann irreduzibel, wenn es in R keine Nullstellen hat (Denn f ist genau dann reduzibel, wenn es einen Faktor $X - a$ mit $a \in R$ hat.) Dies ist nur der Fall für **normierte** Polynome. Gegenbeispiel: $6X^2 + 11X + 3 = (2X + 3)(3X + 1)$ ist reduziebel in $\mathbb{Z}[X]$ hat aber keine Nullstelle in $\mathbb{Z}$, nur in $\mathbb{Q}$.

(c) Sei R faktoriell, $K = \operatorname{Frac}(R)$. Seien $a \in R$, $p \in R$ Primelement mit $p \mid a$, $p^2 \nmid a$, $n \in \mathbb{N}$. Dann ist $f = X^n - a$ irreduzibel in $R[X]$ nach Eisenstein, damit auch in $K[X]$.

(d) Sei K Körper, $n \in \mathbb{N}$. $f = X^n - Y \in K[X, Y] = K[X][Y]$ ist trivialerweise irreduzibel, oder $f \in K[Y][X]$ ist irreduzibel nach (c), denn Y ist Primelement in $K[Y]$.

(e) Sei K Körper, $\operatorname{char}(K) \neq 2$. $f = X^2 + Y^2$ ist irreduzibel, da f als Polynom in $K[Y]$ keine Nullstelle hat. $g = X^2 + Y^3 + Z^n \in K[X, Y, Z] = K[X, Y][Z]$ ist irreduzibel nach (c).

4 Körpertheorie: kurze Wiederholung

4.1 Themen

Algebraische Erweiterungen
Endliche Erweiterungen
Minimalpolynom
Algebraischer Abschluß
Zerfällungskörper
Normale Erweiterungen
Separable Erweiterungen
Primitives Element
Endliche Körper
Galoiserweiterungen
Galoistheorie
Endliche abelsche Erweiterungen
Symmetrische Polynome
Auflösbarkeit von Gleichungen durch Radikale
Zyklische Galoiserweiterungen
Konstruktionen mit Zirkel und Lineal

4.2 Einige wichtige Konzepte

4.2.1 Endliche Körpererweiterungen

K ein Körper (= kommutativer Ring mit Eins, so daß jedes Element $\neq 0$ invertierbar ist. Körpererweiterung: $K \subset L$, $A \subset L$ eine Teilmenge

$$\begin{aligned} K[A] &= \{x \in L; \exists n \in \mathbb{N}_0, f \in K[X_1, \ldots, X_n], a_1, \ldots, a_n : x = f(a_1, \ldots, a_n)\} \\ &= \text{„ kleinster Unterrring, der } K \cup A \text{ enthält“} \end{aligned}$$

$$\begin{aligned} K(A) &= \left\{x \in L; \exists y, z \in K[A], z \neq 0, : x = \frac{y}{z}\right\} \\ &= \text{„ kleinster Unterkörper, der } K \cup A \text{ enthält“} \end{aligned}$$

Ist $A = \{a_1, \ldots, a_n\}$, dann ist

$$\begin{aligned} K[A] = K[a_1, \ldots, a_n] &= \{f(a_1, \ldots, a_n) : f \in K[X_1, \ldots, X_n]\} \\ K(A) = K(a_1, \ldots, a_n) &= \left\{\frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} : f, g \in K[X_1, \ldots, X_n], g(a_1, \ldots, a_n) \neq 0\right\}. \end{aligned}$$

Endlich erzeugt: wenn es $a_1, \ldots, a_n \in L$ gibt mit $L = K(a_1, \ldots, a_n)$
Einfach: wenn es $a \in L$ gibt mit $L = K(a)$.

Grad von L über K: $[L : K] := \dim_K L \in \mathbb{N} \cup \{\infty\}$
Die Körpererweiterung L/K heißt endlich, wenn $[L : K]$ endlich ist, andernfalls unendlich. **Gradmultiplikationsformel**: $K \subset L \subset M$ Körpererweiterungen. Die Erweiterung M/K ist genau dann endlich, wenn L/K und M/L endlich sind. Dann ist

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

4.2.2 Algebraische Erweiterungen

$x \in L$ heißt algebraisch über K, wenn es $f \in K[X]$ gibt mit $f(x) = 0$. Ansonsten heißt es transzendent. L/K heißt algebraisch, wenn jedes Element $x \in L$ über K algebraisch ist, sie heißt transzendent, wenn sie nicht algebraisch ist.
Minimalpolynom: $x \in L$ algebraisch über K, sei

$$\varphi : K[X] \to L, g \mapsto g(x).$$

Es gibt genau ein normiertes, irreduzibles Polynom $f \in K[X]$ mit $\ker(\varphi) = (f)$. Die Abbildung

$$K[X]/(f) \to K[x], g + (f) \mapsto g(x)$$

ist K-Algebrenisomorphismus.
Der Ring $K[x]$ ist ein Unterkörper von L mit $[K[x] : K] = \deg(f)$. Ist $n = \deg(f)$, dann ist $1, x, \ldots, x^{n-1}$ K-Basis von $K[x]$ über K.
Für ein normiertes Polynom $f \in K[X]$ mit $f(x) = 0$ sind äquivalent:

(a) f ist das Minimalpolynom von x.

(b) Für alle $0 \neq g \in K[X]$ gilt: ist $g(x) = 0$, dann $f \big| g$.

(c) Für alle $0 \neq g \in K[X]$ gilt: ist $g(x) = 0$, dann ist $\deg(f) \leqslant \deg(g)$.

(d) f ist irreduzibel.

L/K ist endlich. $\Leftrightarrow$ L/K ist algebraisch und es gibt $x_1, \ldots, x_n \in L$ mit $L = K(x_1, \ldots, x_n)$. $\Leftrightarrow$ Es gibt über K algebraische Elemente $x_1, \ldots, x_n \in L$ mit $L = K(x_1, \ldots, x_n)$
$K \subset L \subset M$ Körpererweiterungen. M/K ist genau dann algebraisch, wenn L/K und M/L algebraisch sind.

4.2.3 Algebraischer Abschluss (in einem Oberkörper)

Die Menge $\overline{K}$ aller über K algebraischer Elemente von L sind ein Unterkörper von L, der K enthält. Es gilt $\overline{\overline{K}} = \overline{K}$. Der Körper $\overline{K}$ heißt algebraischer Abschluß von K in L. Der Körper K heißt algebraisch abgeschloßen in L, wenn $K = \overline{K}$.

4.2.4 Zerfällungskörper

Satz von Kronecker: K Körper, $f \in K[X]$ irreduzibel. Es gibt $L \supset K$ und $x \in L$ mit $f(x) = 0$ und $L = K(x)$.
Dies ist eindeutig bis auf Isomorphie: Sind $K(x_i) = L_i$ für $i = 1, 2$ Erweiterungen von K mit $f(x_i) = 0$, dann gibt es genau einen Ringisomorphismus $\sigma : L_1 \to L_2$ mit $\sigma(x_1) = x_2$ und $\sigma\big|_K = \mathrm{id}_K$, das heißt genau einen K-Algebrenisomorphismus $\sigma : L_1 \to L_2$ mit $\sigma(x_1) = x_2$.

Fortsetzungssatz: Sei $K \subset L$ endliche Körpererweiterung, $\varphi : K \to K'$ Ringhomomorphismus in einen Körper K'. Dann gibt es eine endliche Körpererweiterung $K' \subset L'$ und einen Ringhomomorphismus $\psi : L \to L'$ mit $\psi\big|_K = \varphi$.

$$\begin{array}{ccc} K & \hookrightarrow & L \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ K' & \to & L' \end{array}$$

Zerfällungskörper: Sei K ein Körper, $f \in K[X]$. Ein Oberkörper L von K heißt Zerfällungskörper von f, wenn:

(a) Es existieren $\alpha \in K$, $n \in \mathbb{N}_0$, $x_1, \ldots, x_n \in L$, so daß $f = \alpha \prod_{i=1}^{n} (X - x_i)$.

(b) Der Körper L ist gegeben durch $K(x_1, \ldots, x_n)$.

Dann ist L endlich über K.

Existenz: Es gibt einen Zerfällungskörper $L \supset K$ von f.

Eindeutigkeit: Sind $K \subset L_i$, $i = 1, 2$, Zerfällungskörper von f, dann gibt es einen Ringismorphismus $\sigma : L_1 \to L_2$ mit $\sigma\big|_K = \mathrm{id}_K$.

Grad: Ist $f \neq 0$, dann gilt

$$[L : K] \big| \deg(f)!.$$

Speziell: Sei f irreduzibel vom Grad n, dann gilt

$$n \big| [L : K] \big| n!.$$

4.2.5 Normale Erweiterungen

Normale Erweiterung: Eine Körpererweiterung $K \subset L$ heißt normal, wenn sie algebraisch ist und jedes irreduzible Polynom in $K[X]$, das in L eine Nullstelle hat, über L in Linearfaktoren zerfällt.

Äquivalent:

(a) L ist normale Erweiterung von K.

(b) L ist Zerfällungskörper eines Polynoms in $K[X]$.

(c) Für alle Oberkörper $L \subset L'$ und alle K-Algebrenhomomorphismen $\sigma : L \to L'$ gilt $\sigma(L) = L'$.

Ist $K \subset L$ endlich und normal, $K \subset E \subset L$ ein Zwischenkörper, dann ist auch L/E endlich und normal.
Aber: Dagegen ist im Allgemeinen E/K nicht normal!

4.2.6 Galoisgruppe

Ist $K \subset L$ Körpererweiterung, dann ist

$$\mathrm{Gal}(L/K) = \left\{\sigma \in \mathrm{Aut}(L) \;\middle|\; \sigma\big|_K = \mathrm{id}_K\right\} \subset \mathrm{Aut}(L)$$

die Galoisgruppe von L/K. Es gilt

$$\mathrm{Gal}(L/K) \subset \mathrm{Alg}_K(L, L).$$

Wenn L_0 der Primkörper von L ist, dann gilt $\mathrm{Aut}(L) = \mathrm{Gal}(L/L_0)$.

Sei $K \subset L$ endlich und normal, $G = \mathrm{Gal}(L/K)$, $f \in K[X]$ ein irreduzibles Polynom, das über L in Linearfaktoren zerfällt. Sei Z die Menge der Nullstellen von f in L. Dann ist

$$G \times Z \to Z, (\sigma, x) \mapsto \sigma(x)$$

eine transitive Operation (G permutiert die Nullstellen). Für $x \in Z$ gilt $G_x = \mathrm{Gal}(L/K(x))$ (Stabilisatoruntergruppe).

4.2.7 Separable Erweiterungen

Sei K ein Körper.

(a) Ein irreduzibles Polynom $f \in K[X]$ heißt separabel, wenn f in einem (und dann jedem) Zerfällungskörper nur einfache Nullstellen hat.

(b) Der Körper K heißt perfekt oder vollkommen, wenn jedes irreduzible Polynom $f \in K[X]$ separabel ist.

(c) Sei $K \subset L$ Körpererweiterung. Ein Element $x \in L$ heißt separabel, wenn x algebraisch über K ist, und das Minimalpolynom von x über K separabel ist.

(d) Ein Oberkörper L heißt separabel über K, wenn jedes Element in L über K separabel ist.

Äquivalent: Für eine endliche Körpererweiterung $K \subset L$ sind folgende Aussagen äquivalent:

(a) Die Erweiterung L/K ist separabel.

(b) Es gibt über K separabel Elemente $x_1, \ldots, x_n \in L$ mit $L = K(x_1, \ldots, x_n)$.

Sei L/K normal. L/K ist genau dann separabel, wenn $|\mathrm{Gal}(L/K)| = [L : K]$ ist.

Transitivität: Sei $K \subset L$ endliche Erweiterung, $K \subset E \subset L$ ein Zwischenkörper. L/K ist genau dann separabel, wenn E/K und L/E separabel sind.

Satz vom primitiven Element: Jede endliche separabel Erweiterung $K \subset L$ ist einfach, dh. es gibt $x \in L$ mit $L = K(x)$.

Kriterium für Separabilität von Polynomen: Sei $f \in K[X]$ irreduzibel. Das Polynom f ist genau dann separabel, wenn $f' \neq 0$ ist.

Charakteristik = 0: Für $f \in K[X]$ gilt $f' = 0$ genau dann, wenn $f \in K$. Das heißt jedes irreduzible Polynom in $K[X]$ ist separabel.
Insbesondere ist jeder Körper von Charkteristik 0 vollkommen.

Charakteristik = $p \neq 0$: Für $f \in K[X]$ gilt $f' = 0$ genau dann, wenn $f \in K[X^p]$. Das heißt ein irreduzibles Polynom $f \in K[X]$ ist genau dann separabel, wenn $f \notin K[X^p]$.
Insbesondere ist K genau dann vollkommen, wenn $K = K^p$, das heißt der Frobenius $\sigma : K \to K, a \mapsto a^p$ ist surjektiv.

4.2.8 Endliche Körper

$p > 0$, p prim. Setze $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
Frobenius: $\sigma : \mathbb{F}_p \to \mathbb{F}_p$ ist injektiv, also bijektiv. $\Rightarrow \mathbb{F}_p$ ist vollkommen.

Körper mit p^n Elementen: Man bezeichnet mit $\mathbb{F}_{p^n}$ den Zerfällungskörper des Polynoms $f = X^{p^n} - X \in \mathbb{F}_p[X]$. Er besteht genau aus den Nullstellen des Polynoms f und hat p^n Elemente.
Ist K ein endlicher Körper, so gibt es $n \in \mathbb{N}$ und eine Primzahl $p \in \mathbb{N}$ mit $K \cong \mathbb{F}_{p^n}$.

Jeder endliche Körper, $K \cong \mathbb{F}_{p^n}$ ist vollkommen (Frobenius σ ist ein Isomorphismus).
Es gilt $\mathrm{Aut}(K) = \mathrm{Gal}(K/K_0) = \langle\sigma\rangle$, und diese Gruppe hat Ordnung n. Dabei ist σ der Forbeniushomomorphismus von K.

Endliche Erweiterungen: Sei $K \cong \mathbb{F}_{p^n}$ endlicher Körper, $K \subset L$ endliche Körpererweiterung vom Grad m. Dann ist

$$\begin{aligned} L &\cong \mathbb{F}_{p^{mn}} \\ \mathrm{Gal}(L/K) &= \langle\sigma^n\rangle \\ |\mathrm{Gal}(L/K)| &= m \end{aligned}$$

Die Erweiterung L/K ist normal und separabel.

4.2.9 Galoiserweiterungen

Eine Körpererweiterung $K \subset L$ heißt Galois'sch oder Galoiserweiterung, wenn L/K normal und separabel ist.

Für eine Körpererweiterung $K \subset L$ sind äquivalent:

(a) Die Erweiterung L/K ist endlich und Galois'sch.
(b) Es gibt eine endliche Untergruppe G von $\mathrm{Aut}(L)$ mit $K = \mathrm{Fix}(G)$.
(c) Die Erweiterung L/K ist endlich und $K = \mathrm{Fix}(\mathrm{Gal}(L/K))$.
(d) Die Erweiterung L/K ist endlich und $|\mathrm{Gal}(L/K)| = [L : K]$.

Hauptsatz der Galoistheorie
Sei $K \subset L$ eine endliche Galoiserweiterung mit $G = \mathrm{Gal}(L/K)$, sei $\mathscr{K}$ die Menge aller Zwischenkörper zwischen K und L, $\mathscr{G}$ die Menge aller Untergruppen von G. Dann gilt:

(a) Die Abbildungen

$$\begin{aligned} \mathscr{K} \to \mathscr{G}, &\quad E \mapsto \mathrm{Gal}(L/E) \\ \mathscr{G} \to \mathscr{K} &\quad H \mapsto \mathrm{Fix}_L(H) \end{aligned}$$

sind zueinander invers und antiton. Das heißt, sie sind antiton (monoton und ordnungsumkehrend), und für alle $E \in \mathscr{K}$ gilt $E = \mathrm{Fix}_L(\mathrm{Gal}(L/E))$, und für alle $H \in \mathscr{G}$ gilt $H = \mathrm{Gal}(L/\mathrm{Fix}_L(H))$.

(b) Für $E \in \mathscr{K}$ ist L/E Galois'sch und es gilt

$$\begin{aligned} [L : E] &= |\mathrm{Gal}(L/E)| \\ [E : K] &= [G : \mathrm{Gal}(L/E)]\,. \end{aligned}$$

Für $E \in \mathscr{K}$, $H = \mathrm{Gal}(L/E)$ sind äquivalent:

(i) Die Erweiterung E/K ist Galois'sch.

(ii) Für alle $\sigma \in G$ ist $\sigma(E) = E$.

(iii) Die Gruppe H ist ein Normalteiler von G.

Gilt eine der Aussagen (i)-(iii), dann ist die Abbildung

$$G \to \mathrm{Gal}(E/K), \sigma \mapsto \sigma\big|_E$$

ein surjektiver Gruppenhomomorphismus mit Kern H. Dann ist

$$G/H \to \mathrm{Gal}(E/K), \sigma H \mapsto \sigma\big|_E,$$

Isomorphismus.

Konjugierte Galoisgruppen
Sei $K \subset L$ endliche Galoiserweiterung Für $K \subset E, E \subset L$ und $\sigma \in \mathrm{Gal}(L/K)$ sind äquivalent:

(a) $E' = \sigma(E)$,

(b) $\mathrm{Gal}(L/E') = \sigma\,\mathrm{Gal}(L/E)\sigma^{-1}$.

Minimalpolynome über Zwischenkörpern
Sei $K \subset L$ endliche Galoiserweiterung mit $G = \mathrm{Gal}(L/K)$.

(a) Sei $K \subset E \subset L$ und $x \in E$ ein primitives Element über K. Ist $H = \mathrm{Gal}(L/E)$ und $\sigma_1, \ldots, \sigma_m$ eine Linkstransversale von H in G. Dann ist $\prod_{i=1}^{m}(X - \sigma_i(x))$ das Minimalpolynom von x über K. Ist insbesondere x ein primitives Element von L über K, dann ist $\prod_{\sigma\in G}(X-\sigma(x))$ das Minimalpolynom von x über K.

(b) Sei $L = K(x)$, $H \in \mathscr{G}$, $E = \mathrm{Fix}_L(H)$ und $g = \prod_{\sigma\in H}(X - \sigma(x)) = \sum_{i=0}^{t}\alpha_i X^i$. Dann gilt $E = K(\alpha_0, \ldots, \alpha_{t-1})$.

4.2.10 Komposita als Galoiserweiterungen

Kompositum von E und F $= EF = E(F) = F(E) = K(E \cup F)$

Sei $K \subset L$ Körpererweiterung, seien E, E', F Körper zwischen K und L mit $E \subset E'$. Wenn E'/E eine endliche Galoiserweiterung ist, dann ist auch $E'F/EF$ eine endliche Galoiserweiterung und die Abbildung

$$\varphi : \mathrm{Gal}(E'F/EF) \to \mathrm{Gal}(E'/E), \sigma \mapsto \sigma\big|_{E'}$$

ist ein injektiver Gruppenhomomorphismus.

Sei $K \subset L$ Körpererweiterung, seien E, F Körper zwischen K und L, so daß E/K und F/K endliche Galoiserweiterungen sind.

(a) Die Erweiterung EF/K ist endliche Galoiserweiterung und die Abbildung

$$\varphi : \mathrm{Gal}(EF/E) \to \mathrm{Gal}(F/E \cap F), \sigma \mapsto \sigma\big|_F,$$

ist ein Gruppenisomorphismus.

(b) Die Abbildung

$$\psi : \mathrm{Gal}(EF/K) \to \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K), \sigma \mapsto (\sigma\big|_E, \sigma\big|_F),$$

ist injektiver Homomorphismus. Wenn $E \cap F = K$ ist, dann ist ψ auch surjektiv.

4.2.11 Kreistielungsteilungskörper

Einheitswurzeln: Sei K ein Körper, $n \in \mathbb{N}$. Das Element $\xi \in K$ heißt n-te Einheitswurzel, wenn $\xi^n = 1$. Menge der n-te Einheitswurzeln: $\mu_n(K)$.

(a) Die Menge der n-te Einheitswurzeln ist eine zyklische Untergruppe von K^*, deren Ordnung n teilt.

(b) Sei L Zerfällungskörper von $X^n - 1 \in K[X]$.

(i) Ist $\mu_n(L) = \langle\zeta\rangle$, dann ist $L = K(\zeta)$.

(ii) $\operatorname{char} K \nmid n$, dann hst $\mu_n(L)$ Ordnung n.

(iii) $\operatorname{char}(K) = p$ prim mit $p \mid n$, und ist $n = p^k m$ mit $k \in \mathbb{N}$ und $p \nmid m$, dann gilt $\mu_n(L) = \mu_m(L)$.

Primitive Einheitswurzel: Eine n-te Einheitswurzel $\zeta \in K$ heißt primitiv, wenn $\operatorname{ord}(\zeta) = n$ ist, das heißt, wenn $\mu_n(K) = \langle\zeta\rangle$ und $\mu_n(K)$ Ordnung n hat. Dann gibt es $\varphi(n)$ primitive n^{te} Einheitswurzeln.

Zerfällungskörper von $X^n - a$: Seien K ein Körper, $0 \neq a \in K$, $n \in \mathbb{N}$ mit $\operatorname{char}(K) \nmid n$ und L ein Zerfällungskörper von $X^n - a \in K[X]$. Dann gilt:

(a) Die Erweiterung L/K ist endlich und Galois'sch.

(b) Die Gruppe $\operatorname{Gal}(L/K)$ ist isomorph zu einer Untergruppe des semidirekten Produktes $\mathbb{Z}/n\mathbb{Z} \times_j (\mathbb{Z}/n\mathbb{Z})^*$, wobei $j : (\mathbb{Z}/n\mathbb{Z})^* \to \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$ der bekannte Isomorphismus $j(\overline{x})(\overline{y}) = \overline{xy}$ für $x \in (\mathbb{Z}/n\mathbb{Z})^*$, $y \in \mathbb{Z}/n\mathbb{Z}$ ist.

Zerfällungskörper von $X^n - 1$: Sei K Körper, $n \in \mathbb{N}$ mit $\operatorname{char}(K) \nmid n$ und $K^{(n)}$ ein Zerfällungskörper von $X^n - 1 \in K[X]$.

(a) Die Erweiterung $K^{(n)}/K$ ist Galois'sch.

(b) Die Gruppe $\operatorname{Gal}(K^{(n)}/K)$ ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$. Sie ist also abelsch und ihre Ordnung teilt $\varphi(n)$.

Der Körper $K^{(n)}$ heißt Körper der n^{ten} Einheitswurzeln oder n^{ter} Kreisteilungskörper über K.

Kreisteilungspolynome: Sei K ein Körper, $n \in \mathbb{N}$ mit $\operatorname{char}(K) \nmid n$ und $K^{(n)}$ ein Zerfällungskörper von $X^n - 1 \in K[X]$. Ferner sei P_n die Menge aller primitiven n^{ten} Einheitswurzeln in $K^{(n)}$ und $\phi_{K,n} = \phi_n = \prod_{\zeta \in P_n}(X - \zeta)$.

(a) Das Polynom ϕ_n ist in $K[X]$ enthalten, und $\deg(\phi_n) = \varphi(n)$.

(b) Das Polynom $X^n - 1$ zerfällt über K als $X^n - 1 = \prod_{\mathbb{N} \ni d \mid n} \phi_d$.

Das Polynom ϕ_n heißt n^{tes} Kreisteilungspolynom.

Über den rationalen Zahlen:

(a) Das n^{te} Kreisteilungspolynom ϕ_n über $\mathbb{Q}$ liegt in $\mathbb{Z}[X]$ und ist irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$.

(b) Der Körper $\mathbb{Q}^{(n)}$ der n^{ten} Einheitswurzeln ist Galoiserweiterung von $\mathbb{Q}$ vom Grad $\varphi(n)$. Ist $\varepsilon \in \mathbb{Q}^{(n)}$ eine primitive n^{te} Einheitswurzel, dann gilt $\mathbb{Q}^{(n)} = \mathbb{Q}(\varepsilon)$ und das Minimalpolynom von ε über $\mathbb{Q}$ ist ϕ_n.

(c) Die Abbildung $\rho : \operatorname{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ mit $\rho(\sigma) = \bar{l}$, wenn $\sigma(\varepsilon) = \varepsilon^l$, ist Gruppenisomorphismus.

Über endlichen Körpern: Sei p eine Primzahl, $k \in \mathbb{N}$, $q = p^k$, $K = \mathbb{F}_q$ der Körper mit q Elementen. Ferner sei $n \in \mathbb{N}$ mit $p \nmid n$, $K^{(n)}$ der Zerfällungskörper von $X^n - 1 \in K[X]$

(a) Ist $\varepsilon \in K^{(n)}$ eine primitive n^{te} Einheitswurzel, dann ist $K^{(n)} = K(\varepsilon)$.

(b) $\rho : \operatorname{Gal}(K^{(n)}/K) \to \mathbb{Z}/n\mathbb{Z}^*$ mit $\rho(\tau) = \bar{l}$, wenn $\tau(\varepsilon) = \varepsilon^l$, ist ein injektiver Homomorphismus ist. Es gilt $\operatorname{Gal}(K^{(n)}/K) = \langle\sigma^k\rangle$, wobei σ der Frobeniushomomorphismus ist, da $K^{(n)}$ ebenfalls endlich ist.
Genauer $\rho(\sigma^k) = \overline{q}$, und $\operatorname{im}(\rho) = \langle\overline{q}\rangle$. Damit folgt $[K^{(n)} : K] = \operatorname{ord}(\overline{q}) = \operatorname{ord}_n(q)$.

(c) Das Bild $\overline{\phi}_n \in \mathbb{F}_p[X]$ des n^{ten} Kreisteilungspolynoms $\phi_n \in \mathbb{Z}[X]$ ist genau dann irreduzibel über K, wenn $\mathbb{Z}/n\mathbb{Z}^* = \langle\overline{q}\rangle$, dh. wenn $\operatorname{ord}_n(q) = \varphi(n)$.

4.2.12 Galoisgruppe von Polynomen

Sei K ein Körper, $f = f_1 \cdots f_r \in K[X]$ mit paarweise nicht assoziierten, irreduziblen $f_1, \ldots, f_r$. Sei L ein Zerfällungskörper von f über K, $M = \{x \in L \mid f(x) = 0\}$, $M_i = \{x \in L \mid f_i(x) = 0\}$ für $i = 1, \ldots, r$.
Es gilt $M = \bigcup_{i=1}^{r} M_i$.
Galoisgruppe von f: $G(f) = \mathrm{Gal}(L/K)$
Operation: $G(f) \times M \to M, (\sigma, x) \mapsto \sigma(x)$

(a) Die Bahnen dieser Operationen sind $M_1, \ldots, M_r$.

(b) Die Abbildung $G(f) \to \mathfrak{S}_M, \sigma \mapsto (x \mapsto \sigma(x))$ ist injektiver Gruppenhomomorphismus.

f ist irreduzibel $\Leftrightarrow$ $G(f)$ operiert auf $M = \{x_1, \ldots, x_n\}$ transitiv
Sei f separabel: also Galois'sch und $|\mathrm{Gal}(L/K)| = |G(f)| = [L : K]$.

(a) Man hat die Einbettung $\varphi : G(f) \to \mathfrak{S}_n$ mit $\varphi(\sigma)(i) = j$ falls $\sigma(x_i) = x_j$. Die Ordnung von $G(f)$ teilt $n!$.

(b) Ist f irreduzibel, dann teilt n die Ordnung von $G(f)$.

Diskriminante: Sei $G(f)_+ = \varphi^{-1}(A_n)$.

$$G(f)_+ \triangleleft G(f)$$

$[G(f) : G(f)_+] \leqslant [S_n : A_n] = 2$.

$$\begin{aligned} \delta = \delta(f) &= \prod_{i<j}(x_i - x_j) \in L\backslash\{0\} \\ D = D(f) &= \delta^2 = \prod_{i<j}(x_i - x_j)^2. \end{aligned}$$

Für $\sigma \in G(f)$ gilt

$$\sigma(\delta) = \prod_{i<j}(\sigma(x_i) - \sigma(x_j)) = \prod_{i<j}(x_{\varphi(\sigma)(i)} - x_{\varphi(\sigma)(j)}) = (-1)^m \delta,$$

wobei m die Anzahl der Transversionen von $\varphi(\sigma)$ ist. Es folgt $\sigma(D) = D$ für alle $\sigma \in G(f)$. Also ist $D \in \mathrm{Fix}(G(f)) = K$. Man nennt D die Diskriminante von f.

Sei $\mathrm{char}(K) \neq 2$.

(a) Der Fixkörper von G_+ ist $\mathrm{Fix}(G_+) = K(\delta)$, die Erweiterung $K(\delta)/K$ ist Galois'sch mit Galoisgruppe $\mathrm{Gal}(K(\delta)/K) \cong G/G_+$ vom Grad $[K(\delta) : K] \leqslant 2$.

(b) Genau dann gilt $G = G_+$, wenn D Quadrat eines Elementes von K ist.

Polynome vom Grad 3 und 4: Sei $\mathrm{char}(K) \neq 2$, $f \in K[X]$ normiert irreduzibel, separabel vom Grad 3 und $G = G(f)$.

(a) Es gilt $G \cong A_3$ oder $G \cong \mathfrak{S}_3$.

(b) Genau dann gilt $G \cong A_3$, wenn D Quadrat in K ist.

Sei $f \in K[X]$ normiert, irreduzibel und separabel vom Grad 4,

$$\begin{aligned} M = \{x_1, \ldots, x_4\} &\quad \text{die Menge der Nullstellen im Zerfällungskörper } L \\ \text{definiere } \alpha = x_1x_2 + x_3x_4, \beta = x_1x_3 + x_2x_4, \gamma = x_1x_4 + x_2x_3 \in L &\quad \text{und } E = K(\alpha, \beta, \gamma) \\ G = G(f) & \\ G(f)_+ = \varphi^{-1}(A_4) & \\ N = \varphi^{-1}(V) \triangleleft G, &\quad \text{wobei } V \text{ die Klein'sche Vierergruppe ist,} \end{aligned}$$

Es gilt $\mathrm{Fix}(N) = E$, $\mathrm{Gal}(L/E) = N$, und E/K ist Galois'sch mit $\mathrm{Gal}(E/K) \cong G/N$.
Sei $m = [E : K] = [G : N]$. Dann gilt:

(a) Ist $m = 6$, dann ist $G \cong \mathfrak{S}_4$.

(b) Ist $m = 3$, dann ist $G \cong A_4$.

(c) Ist $m = 1$, dann ist $G \cong V$.

(d) Im Fall $m = 2$ ist entweder $G \cong D_4$ oder $G \cong \mathbb{Z}/(4)$. Der erste Fall tritt genau dann ein, wenn f über E irreduzibel bleibt.

Erweiterungen zu vorgegebenen Galoisgruppen:
Jede endliche Gruppe ist isomorph zur Galoisgruppe einer endlichen Galoiserweiterung. In der Regel ist der Basiskörper "riesig":
Sei $M = K(U_1, \ldots, U_n)$ der rationale Funktionenkörper in den Unbestimmten $U_1, \ldots, U_n$ über K, sei Y eine weitere Unbestimmte. Sei

$$F = Y^n + U_1 Y^{n-1} + \cdots + U_{n-1} Y + U_n \in M[Y].$$

das allgemeine Polynom n^{ten} Grades. Die Galoisgruppe des allgemeinen Polynoms $F = Y^n + U_1 Y^{n-1} + \cdots + U_{n-1} Y + U_n \in M[Y]$ ist isomorph zu $\mathfrak{S}_n$.

Jede endliche abelsche Gruppe G ist isomorph zur Galoisgruppe einer endlichen Galoiserweiterung $\mathbb{Q} \subset K$ mit $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

4.2.13 Auflösbare Erweiterungen

Eine endliche Galoiserweiterung L/K heißt
— zyklisch, wenn $\mathrm{Gal}(L/K)$ zyklisch ist.
— abelsch, wenn $\mathrm{Gal}(L/K)$ abelsch ist.
— auflösbar, wenn $\mathrm{Gal}(L/K)$ auflösbar ist.

Zyklische Erweiterungen: Hier unterscheidet man, ob die Charakteristik des Grundkorpers den Grad des Polynoms teilt oder nicht:

Sei K ein Körper und $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Wir nehmen an, daß K eine primitive n^{te} Einheitswurzel enthält.

(a) Ist $f = X^n - a \in K[X]$, L ein Zerfällungskörper von f und $x \in L \backslash K$ eine Nullstelle von f, dann gilt $L = K(x)$ und L/K ist eine zyklische Galoiserweiterung. Ferner ist $d = [L : K]$ Teiler von n, es gilt $x^d \in K$ und $X^d - x^d$ ist das Minimalpolynom von x über K. Ist f irreduzibel, dann ist L/K zyklische Galoiserweiterung vom Grad n.

(b) Wenn umgekehrt $K \subset L$ eine zyklische Galoiserweiterung vom Grad n ist, dann gibt es $x \in L$ mit $x^n \in K$ und $L = K(x)$. Also ist $X^n - x^n$ das Minimalpolynom von x und L ist sein Zerfällungskörper.

Sei K ein Körper mit Primzahlcharakteristik p.

(a) Ist $f = X^p - X - a \in K[X]$, L ein Zerfällungskörper von f und $x \in L$ eine Nullstelle von f, so ist $L = K(x)$ und L/K ist zyklische Galoiserweiterung vom Grad 1 oder p. Genau dann ist $[L : K] = p$, wenn f irreduzibel ist.

(b) Ist L/K zyklische Galoiserweiterung vom Grad p, so gibt es $a \in K$ und eine Nullstelle des irreduziblen Polynoms $f = X^p - X - a \in K[X]$ mit $L = K(x)$.

Durch Radikale auflösbare Erweiterungen: Eine endliche Erweiterung $K \subset L$ heiße vom
Typ I wenn L aus K durch Adjunktion einer Einheitswurzel entsteht.
Typ II wenn L aus K durch Adjunktion einer Nullstelle des Polynoms $X^n - a \in K[X]$ mit $\mathrm{char}(K) \nmid n$ entsteht.
Typ III wenn L aus K durch Adjunktion einer Nullstelle eines Polynoms $X^p - X - a \in K[X]$ mit $\mathrm{char}(K) = p > 0$ entsteht.
Die adjungierten Elemente heißen auch Radikale.

(a) Eine endliche Erweiterung $K \subset M$ heißt Radikalerweiterung, wenn es eine Folge von Zwischenkörpern $K = M_0 \subset M_1 \subset \ldots \subset M_r = M$ gibt, so daß die Erweiterungen $M_i \subset M_{i+1}$ von einem der Typen I,II oder III sind. Offenbar ist dann M/K separabel.

(b) Eine endliche Erweiterung $K \subset L$ heißt durch Radikale auflösbar, wenn es eine Radikalerweiterung $K \subset M$ gibt, mit $L \subset M$.

(c) Eine endliche Erweiterung $K \subset L$ heißt auflösbar, wenn es eine Erweiterung $L \subset M$ gibt, so daß M/K endliche auflösbare Galoiserweiterung ist.

Es gilt:

— Seien $K \subset E \subset L$ endliche Erweiterungen. Die Erweiterung L/K ist genau dann auflösbar, beziehungsweise durch Radikale auflösbar, wenn E/K und L/E die jeweiligen Eigenschaften haben

— Eine endliche Körpererweiterung $K \subset L$ ist genau dann durch Radikale auflösbar, wenn sie auflösbar ist.

4.2.14 Konstruktionen mit Zirkel und Lineal

Sei $M \subset \mathbb{R}^2 \cong \mathbb{C}$ eine Menge mit $0, 1 \in M$, $g(M)$ die Menge aller Geraden durch zwei verschiedenen Punkte in M, $k(M)$ die Menge aller Kreise, deren Mittelpunkte in M liegen und deren Radius jeweils die Abstände zweier Punkte in M sind. Mit folgenden Operationen werden aus Punkten in M Punkte in $\mathbb{R}^2$ konstruiert:

(S1) Schnitt zweier verschiedener Geraden in $g(M)$.

(S2) Schnitt einer Geraden in $g(M)$ mit einem Kreis in $k(M)$.

(S3) Schnitt zweier verschiedener Kreise.

Die Menge der aus M konstruierten Punkte sei M'. Offenbar gilt $M \subset M'$. Wir setzen induktiv

$$\begin{aligned} M_0 &= M \\ M_1 &= M' \\ &\vdots \\ M_{n+1} &= (M_n)' \\ \hat{M} &= \bigcup_{n \geqslant 0} M_n \end{aligned}$$

Die Punkte aus $\hat{M}$ heißen (mit Zirkel und Lineal) konstruiert. Jeder Punkt aus $\hat{M}$ kann durch endlich viele Operationen (S1), (S2), (S3) aus M erhalten werden. Es gilt $(\hat{M})' = \hat{M}$, denn ist $p \in (\hat{M})'$, so kann P aus endlich vielen Punkten in $\hat{M}$ konstituiert werden, diese liegen in M_n für $n \geqslant 0$ groß genug, also gilt $P \in M_n' = M_{n+1} \subset \hat{M}$.

Es gilt:

(a) Die Menge $\hat{M}$ ist der kleinste Unterkörper von $\mathbb{C}$ mit folgenden Eigenschaften:

$$M \subset \hat{M}, \qquad \overline{\hat{M}} = \hat{M}, \qquad \forall z \in \mathbb{C} : z^2 \in \hat{M} \Rightarrow z \in \hat{M}.$$

(b) Der Körper $K = \mathbb{Q}(M \cup \overline{M})$ ist Unterkörper von $\hat{M}$ und $K = \overline{K}$.

Konstruierbarkeit: Sei $M \subset \mathbb{C}$ mit $0, 1 \in M$ und $K = \mathbb{Q}(M, \overline{M})$. Für einen Punkt $z \in \mathbb{C}$ sind folgende Aussagen äquivalent:

(a) Es ist $z \in \hat{M}$, das heißt z ist aus M (mit Zirkel und Lineal) konstruierbar.

(b) Es gibt eine Folge von Erweiterungen $K = L_0 \subset L_1 \subset \ldots \subset L_r = L$, $r \in \mathbb{N}_0$, und $w_i \in L_i$ mit $w_i^2 \in L_{i-1}$ und $L_i = L_{i-1}(w_i)$ für $1 \leqslant i \leqslant r$, so daß $z \in L$ ist. (Spezielle Radikalerweiterungen)

(c) Das Element z ist algebraisch über K und die Galoisgruppe des Minimalpolynoms $f \in K[X]$ von z ist eine 2-Gruppe.

4.3 Beispiele

4.3.1 Beispiele: endliche Erweiterungen

(a) Ist L/K eine endliche Körpererweiterung, $n = [L : K]$ und $x \in L$, dann sind $1, x, \ldots, x^n$ linear abhängig über K, dh. es existieren $\alpha_0, \ldots, \alpha_n \in K$ nicht alle Null mit $\sum_{i=0}^n \alpha_i x^i = 0$, d.h. x ist Nullstelle des Polynoms $f = \sum_{i=0}^n \alpha_i X^i \in K[X] \backslash \{0\}$.

(b) Sei $d \in \mathbb{N}$ mit $\sqrt{d} \notin \mathbb{Q}$. $\mathbb{Q} \subset \mathbb{Q}[\sqrt{d}]$ ist quadratische Körpererweiterung.

(c) $\mathbb{R} \subset \mathbb{C} = \mathbb{R}[i]$ ist endliche Erweiterung, also algebraisch. Ein Element $x \in \mathbb{C}$ ist Nullstelle von $(X-x)(X-\overline{x}) = X^2 - (x+\overline{x})X + x\overline{x} \in \mathbb{R}[X]$. Für $x \in \mathbb{R}$ ist $X - x$ das Minimalpolynom, für $x \in \mathbb{C} \setminus \mathbb{R}$ ist $X^2-(x+\overline{x})X+x\overline{x}$ das minimalpolynom. Insbesondere ist X^2+1 das Minimalpolynom von i über $\mathbb{R}$ und es gilt

$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}\,.$$

(d) $\sqrt[3]{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$ mit Minimalpoynom $X^3 - 2$. Also gilt

$$\mathbb{Q}[X]/(X^3-2) \cong \mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2}).$$

(e) $K \subset K(X)$ ist transzendent, denn X/K ist transzendent, $\dim_K K[X] = \infty$, $K[X] \subsetneq K(X)$.

(f) $\mathbb{Q} \subset \mathbb{R}$ ist transzendent, denn zum Beispiel sind e, π transzendent über $\mathbb{Q}$ (Hermite: 187, Lindemann: 1882).

4.3.2 Beispiele: algebraischer Abschluß

(a) Der algebraische Abschluß $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ in $\mathbb{C}$ ist eine unendliche algebraische Erweiterung von $\mathbb{Q}$. Er heißt Körper der algebraischen Zahlen.

(b) Der Körper $\overline{\mathbb{Q}}$ ist abzählbar unendlich.

(c) Die Mengen $\mathbb{R} \setminus \overline{\mathbb{Q}}$, $\mathbb{C} \setminus \overline{\mathbb{Q}}$ sind überabzählbar.

4.3.3 Beispiele: Zerfällungskörper

(a) Die komplexen Zahlen $\mathbb{C}$ sind Zerfällungskörper von $X^2 + 1 \in \mathbb{R}[X]$.

(b) Der Körper $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist Zerfällungskörper von $(X^2-2)(X^2-3) \in \mathbb{Q}[X]$.

(c) Sei $K = \mathbb{Z}/(2)$, $f = X^2 + X + 1 \in K[X]$. Das Polynom f ist irreduzibel, also ist $L = K[X]/(f)$ Körpererweiterung von K. L ist Zerfällungskörper von f denn mit $x = X + (f)$ gilt $f = (X + x)(X + x + 1)$ und $L = K(x)$. Es gilt $[L : K] = 2$, also hat L 4 Elemente.

(d) Sei $f = X^3 - 2 \in \mathbb{Q}[X]$. Das Polynom f ist irreduzibel (Eisenstein). Sei

$$\omega = \frac{1}{2}(-1 + \sqrt{-3}) = e^{\frac{2\pi i}{3}} \in \mathbb{C}\,.$$

Es gilt $\omega^2 = \overline{\omega}$ und $\omega^3 = 1$. Die Nullstellen von f sind

$$\sqrt[3]{2}, \omega\sqrt[3]{2}, \overline{\omega}\sqrt[3]{2},$$

also ist

$$f = (X - \sqrt[3]{2})(X - \omega\sqrt[3]{2})(X - \overline{\omega}\sqrt[3]{2}) = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{2}^2).$$

Also ist $\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ Zerfällungskörper von f. Es gilt

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6 = 3!$$

4.3.4 Beispiele: Normale Erweiterungen

(a) Quadratische Erweiterungen sind normal.

(b) Beispiel eines Körperturms $K \subset L \subset M$ an, so daß $K \subset L$ und $L \subset M$ normal sind, aber $K \subset M$ nicht.
Lösung: Betrachte die Erweiterungen $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. Die Erweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ ist quadratisch, das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist $X^2 - 2$. Die Erweiterung $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ ist ebenso quadratisch, das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}(\sqrt{2})$ ist $X^2 - \sqrt{2}$. Aber $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ ist nicht normal, denn das Minimalpolynom $X^4 - 2$ von $\sqrt[4]{2}$ über $\mathbb{Q}$ zerfällt über $\mathbb{Q}(\sqrt[4]{2})$ nicht in Linearfaktoren, sondern nur in $(X - \sqrt[4]{2})(X + \sqrt[4]{2})(X^2 + \sqrt{2})$.

4.3.5 Beispiele: Separable Erweiterungen

(a) Das Polynom $f = X^3 - 2 \in \mathbb{Q}[X]$ ist separabel.

(b) Sei $K = \mathbb{Z}/(2)(X)$, $f = Y^2 + X \in K[Y]$. Dann ist f irreduzibel, denn f ist irreduzibel in $\mathbb{Z}/(2)[X][Y]$ nach Eisenstein. Es gibt eine Erweiterung $K \subset L = K(y)$ vom Grad 2 mit $0 = f(y) = y^2 + X$, also $y^2 = X$ über $\mathbb{Z}/(2)$ und es gilt

$$(Y + y)^2 = Y^2 + 2Yy + y^2 = Y^2 + y^2 = Y^2 + X = f.$$

Also ist f nicht separabel.

(c) Sei $K/\mathbb{Q}$ der Zerfällungskörper von $f = X^3 - 2 \in \mathbb{Q}[X]$. Wir wissen, daß

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2})(\omega),$$

wobei $\omega = \frac{1}{2}(-1 + \sqrt{-3}) = e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Das Minimalpolynom von ω über $\mathbb{Q}$ oder $\mathbb{Q}(\sqrt[3]{2})$ ist $\phi_3 = X^2 + X + 1$. $K/\mathbb{Q}$ ist normal und separabel, also gilt $|\operatorname{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 6$. Die Gruppe $\operatorname{Gal}(K/\mathbb{Q})$ besteht genau aus folgenden Elementen

$$\begin{aligned}
\mathrm{id}_K: &\quad \sqrt[3]{2} \mapsto \sqrt[3]{2}, &\quad \omega \mapsto \omega \\
\alpha: &\quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, &\quad \omega \mapsto \omega \\
\alpha^2: &\quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2, &\quad \omega \mapsto \omega \\
\beta: &\quad \sqrt[3]{2} \mapsto \sqrt[3]{2}; &\quad \omega \mapsto \omega^2, \\
\alpha\beta: &\quad \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}, &\quad \omega \mapsto \omega^2 \\
\alpha^2\beta: &\quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2, &\quad \omega \mapsto \omega^2
\end{aligned}$$

Damit sieht man $\operatorname{ord}(\alpha) = 3$, $\operatorname{ord}(\beta) = 2$, $\beta\alpha\beta = \alpha^2$, dh. $\operatorname{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_3$.

4.3.6 Beispiele: Galoisgruppe

(a) Ist die Erweiterung $K \subset L$ endlich, dann gilt $\operatorname{Gal}(L/K) = \operatorname{Alg}_K(L, L)$, denn jeder K-Algebrenhomomorphismus $\sigma : L \to L$ ist injektiv, also bijektiv.

(b) Wenn L_0 der Primkörper von L ist, dann gilt $\operatorname{Aut}(L) = \operatorname{Gal}(L/L_0)$.

4.3.7 Beispiele: Endliche Körper

(a) $L = \mathbb{Z}/(9)$ ist kein Körper, da 9 nicht prim ist. Insbesondere keine Erweiterung von $\mathbb{F}_3$.

(b) $L = \mathbb{Z}[\sqrt{2}]/(3)$ ist ein Körper: (3) ist ein Primdeal in $\mathbb{Z}[\sqrt{2}]$, also ist L ein endlicher Integritätsbereich, und damit ein Körper. Es gibt einen Isomorphismus

$$\mathbb{Z}[\sqrt{2}]/(3) \xrightarrow{\sim} \mathbb{F}_3[X]/(X^2 + 1) \cong \mathbb{F}_9, \sqrt{2} \mapsto \overline{X}.$$

4.3.8 Beispiele: Galoiserweiterungen

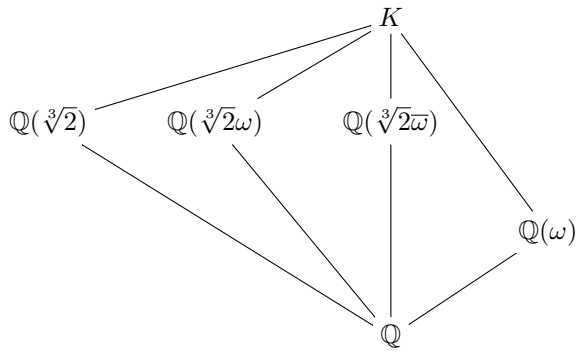
(a) Endliche Erweiterungen von endlichen Körpern sind Galois'sch.
Sei $K \cong \mathbb{F}_{p^n}$ und $K \subset L$ endliche Erweiterung vom Grad m. Die Erweiterung L/K ist Galois'sch mit Galoisgruppe $\operatorname{Gal}(L/K) = \langle \sigma^n \rangle$, wobei σ der Frobeniushomomorphismus von L ist. Die Körper zwischen K und L sind genau die Fixkörper $\operatorname{Fix}_L(\langle \sigma^{nd} \rangle)$ mit $d \in \mathbb{N}$, $d \big| m$. Ist $m = dd'$, $E = \operatorname{Fix}_L(\langle \sigma^{nd} \rangle)$, dann gilt

$$[E : K] = [\langle \sigma^n \rangle : \langle \sigma^{nd} \rangle] = \frac{m}{d'} = d.$$

Es folgt $E \cong \mathbb{F}_{p^{nd}}$.

(b) Jede quadratische Erweiterung $K \subset L$ ist normal. Denn für $x \in L \backslash K$ gilt $L = K(x)$. Ist $f = X^2 + \alpha X + \beta \in K[X]$ das Minimalpolynom von x, dann $f = X^2 + \alpha X + \beta - x^2 - \alpha x - \beta = (X - x)(X + x + \alpha)$. Also ist L/K Zerfällungskörper von f. Insbesondere ist jede separabel quadratische Erweiterung $K \subset L$ Galoiserweiterung.

(c) Das Polynom $f = X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel und separabel. Der Körper $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ mit $\omega = \frac{1}{2}(-1 + \sqrt{-3})$ ist Zerfällungskörper von f. Also ist $K/\mathbb{Q}$ Galois'sch. Wir wissen, daß $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_3$ ist. Die Körper zwischen $\mathbb{Q}$ und K sind



Die Unterkörper vom Grad 3 sind die Fixkörper der drei Untergruppen der Ordnung 2 von $\mathrm{Gal}(K/\mathbb{Q})$, der Unterkörper vom Grad 2 ist der Fixkörper von A_3. Die Körper vom Grad 3 sind zueinander konjugiert. Nur K und $\mathbb{Q}(\omega)$ sind Galois'sch über $\mathbb{Q}$.

4.3.9 Beispiele: EInheitswurzeln

(a) Die n^{ten} Einheitswurzeln in $\mathbb{C}$ sind $e^{\frac{2\pi ik}{n}}$, $1 \leqslant k \leqslant n$. Die primitiven sind dabei diejenigen, für die n und k teilerfremd sind.

(b) Sei p Primzahl, $n \in \mathbb{N}$. Alle Elemente in $\mathbb{F}_{p^n}^*$ sind $(p^n - 1)^{\text{te}}$ Einheitswurzeln.

4.3.10 Beispiele: Kreisteilungspolynome

Sei $\mathrm{char}(K) = 0$. Es ist $\phi_1 = X - 1$. Ist p Primzahl, so ist $X^p - 1 = \phi_1\phi_p$. Also ist

$$\phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Ist außerdem $k \in \mathbb{N}$, dann $X^{p^k} - 1 = \phi_1\phi_p \cdots \phi_{p^{k-1}}\phi_{p^k} = (X^{p^{k-1}} - 1)\phi_{p^k}$. Also

$$\phi_{p^k} = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = X^{p^{k-1}(p-1)} + \cdots + X^{p^k - 1} + 1 = \phi_p(X^{p^{k-1}}).$$

Die ersten zehn Kreisteilungspolynome sind:

$$\begin{aligned}
\phi_1 &= X - 1 \\
\phi_2 &= X + 1 \\
\phi_3 &= X^2 + X + 1 \\
\phi_4 &= X^2 + 1 \\
\phi_5 &= X^4 + X^3 + X^2 + X + 1 \\
\phi_6 &= X^2 - X + 1 \\
\phi_7 &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
\phi_8 &= X^4 + 1 \\
\phi_9 &= X^6 + X^3 + 1 \\
\phi_{10} &= X^4 + X^3 + X^2 - X + 1
\end{aligned}$$

4.3.11 Beispiele Diskriminante

(a) Ist $f = X^2 + bX + c \in K[X]$, $f = (X - x_1)(X - x_2) = X^2 - (x_1 + x_2)X + x_1x_2$, dann $D = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = b^2 - 4ac$.

(b) Sei $f = X^3 + bX^2 + cX + d \in K[X]$. Wir werden sehen: $D = b^2c^2 + 18bcd - 4b^3d - 4c^3 - 27d^2$.

4.3.12 Beispiele: Polynome vom Grad 3

(a) Sei K Unterkörper von $\mathbb{R}$, $f \in K[X]$ normiert und irreduzibel vom Grad 3, und sei $G = G(f)$. Dann gilt:

(i) Hat f nur eine reelle Nullstelle, dann ist $D < 0$ und $G \cong \mathfrak{S}_3$.

(ii) Hat f lauter reelle Nullstellen, dann ist $D > 0$. Genau dann ist $G \cong A_3$, wenn D Quadrat in K ist.

(b) Das Polynom $f = X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel, seine Diskriminante ist $D = -27(-2)^2 = -27 \cdot 4 < 0$. Also hat f genau eine reelle Nullstelle und es gilt $G(f) \cong \mathfrak{S}_3$.

(c) Das Polynom $f = X^3 - 3X - 1 \in \mathbb{Q}[X]$ ist irreduzibel, seine Diskriminante ist $D = -4(-3)^3 - 27(-1)^2 = 4 \cdot 27 - 27 = 9^2 > 0$. Also hat f drei reelle Nullstellen und es gilt $G(f) \cong A_3$.

(d) Das Polynom $f = X^3 - 4X - 1 \in \mathbb{Q}[X]$ ist irreduzibel, seine Diskriminante ist $D = -4(-4)^3 - 27(-1)^2 = 256 - 27 = 229 > 0$, kein Quadrat. Also hat f drei reelle Nullstellen, aber $G(f) \cong \mathfrak{S}_3$.

4.3.13 Beispiele: Auflösbare Erweiterungen

(a) Sei $K = \mathbb{Q}(\sqrt[3]{2})(\omega) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ der Zerfällungskörper von $X^3 - 2 \in \mathbb{Q}[X]$, wobei $\omega = e^{\frac{2\pi i}{3}}$. Dann ist $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ Erweiterung vom Typ II und $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$ vom Typ I. Also ist $K/\mathbb{Q}$ Galois'sche Radikalerweiterung.

(b) Jede separabel Erweiterung $K \subset L$ vom Grad $\leqslant 4$ ist durch Radikale auflösbar.

(c) Sei $K \subset L$ eine endliche und separabel Erweiterung, $L \subset L'$ ein normaler Abschluß von L/K. Wenn $\mathrm{Gal}(L'/K)$ eine einfache nicht-abelsche Untergruppe enthält, dann ist L/K nicht durch Radikale auflösbar.

4.3.14 Beispiele: Konstruktionen mit Zirkel und Lineal

Würfelverdopplung *Gegeben sei ein Würfel der Kantenlänge $a > 0$. Ist ein Würfel doppelten Inhalts, nämlich $2a^3$, aus a mit Zirkel und Lineal konstruierbar?*
Sei speziell $a = 1$, ist $\sqrt[3]{2}$ aus $M = \{0, 1\}$ konstruierbar? Es gilt $K = \mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$. Das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ ist $f = X^3 - 2$, es gilt $G(f) \cong \mathfrak{S}_3$. Da $\mathfrak{S}_3$ keine Zweigruppe ist, ist $\sqrt[3]{2}$ nicht aus M konstruierbar.

Winkeldreiteilung *Gegeben ist ein Winkel φ. Ist $\frac{\varphi}{3}$ mit Zirkel und Lineal konstruierbar? Genauer: Ist $z = e^{i\frac{\varphi}{3}}$ aus $\{0, 1, w = e^{i\varphi}\}$ konstruierbar?*
Wir betrachten speziell $\varphi = \frac{\pi}{3}$, das heißt $w = e^{i\frac{\pi}{3}} = e^{2\pi i \frac{1}{6}} = \frac{1}{2}(1 + i\sqrt{-3})$. Sei $z = e^{i\frac{\pi}{9}} = x + iy$ mit $x = \cos\frac{\pi}{9}$ und $y = \sin\frac{\pi}{9}$. Der Punkt z ist genau dann konstruierbar, wenn x, y kontruierbar sind. Es gilt

$$w = z^3 = x^3 - 3xy^2 + (3x^2y - y^3)i = x^3 - 3x(1 - x^2) + (3(1 - y^2)y - y^3)i = 4x^3 - 3x + (3y - 4y^3)i.$$

Es folgt $4x^3 - 3x - \frac{1}{2} = 0$, also $(2x)^3 - 3(2x) - 1 = 0$. Das Polynom $X^3 - 3X - 1 \in \mathbb{Q}[X]$ ist irreduzibel, also hat $2x$ den Grad 3 über $\mathbb{Q}$. Damit sind $2x$, x und z nicht konstruierbar.

Einheitswurzeln *Ist $\zeta_{2019} = e^{\frac{2\pi i}{2019}}$ mit Zirkel und Lineal konstruierbar?*
Die Einheitswurzel ζ_{2019} ist konstruierbar, wenn $\varphi(2019)$ Zweierpotenz ist. Aber da $2019 = 3 \cdot 673$ prim ist und $\varphi(2019) = \varphi(3) \cdot \varphi(673) = 2 \cdot 672 = 2 \cdot 2^5 \cdot 3 \cdot 7$, ist dies nicht der Fall.