Algebra 1

Gruppentheorie

- Index: $[G : H] := \#\{gH \mid g \in G\} = \#\{Hg \mid g \in G\}$
- Elementordnung: $o(g) = \#\langle g \rangle = \min\{n \in \mathbb{N} \mid g^n = 1\}$
- Normalteiler: $N \trianglelefteq G$ falls $gN = Ng$
  - einfache Gruppe: nur $\{e\}, G$ sind Normalteiler
- Nebenklassen: $G/H := \{gH \mid g \in G\}$ mit $H \leq G$
  - Falls $H \trianglelefteq G$, ist G/H eine Gruppe.
- Gruppenwirkung/-operation: $G \times M \to M$ mit $em = m$ und $g_1(g_2 m) = (g_1 g_2)m$
- Bahn/Orbit: Gm. M ist die disjunkte Vereinigung seiner Bahnen: $M = \bigcup_{v \in V} Gv$
- Stabilisator: $\operatorname{Stab}(m) := \{g \in G \mid gm = m\} \leq G$
  - $Gm \cong G/\operatorname{Stab}(m)$
  - $\#Gm = [G : \operatorname{Stab}(m)]$
  - $\operatorname{Stab}(am) = a \operatorname{Stab}(m) a^{-1}$
- Bahnengleichung: $M \cong \bigcup_{v \in V} G/\operatorname{Stab}(v)$; falls M endlich ist $\#M = \sum_{v \in V} \#Gv$
  - Satz von Lagrange: Sei $H \leq G$, dann $\#G = \#H \cdot \#(G/H)$
- Homomorphiesatz: Sei $f : G \to H$ Homomorphismus, dann ist $\ker(f) \trianglelefteq G$ und $G/\ker(f) \cong f(G)$
  - Korrespondenzsatz: Sei $\varphi : G \to H$ surjektiver Homomorphismus, dann gibt es eine Bijektion zwischen den Untergruppen von H und den Untergruppen von G die $\ker(\varphi)$ enthalten, mit $U \mapsto \varphi(U)$ und $V \mapsto \varphi^{-1}(V)$. Es gilt $U \trianglelefteq G \iff \varphi(U) \trianglelefteq H$ und $G/U \cong H/\varphi(U)$.
- Erster Isomorphiesatz: Sei $N \trianglelefteq G$ und $H \leq G$, dann ist $N \trianglelefteq HN \leq G$ und $H \cap N \trianglelefteq H$ und es ist $H/(H \cap N) \cong HN/N$.
- Zweiter Isomorphiesatz: Sei $N \trianglelefteq H \trianglelefteq G$ und $N \trianglelefteq G$, dann ist $G/H \cong (G/N)/(H/N)$.
- p-Gruppe: $\#G = p^k$
- p-Sylowgruppe: Sei $\#G = p^r m$, $p \nmid m$, dann heißt $H \leq G$ mit $\#H = p^r$ eine p-Sylowgruppe.
  - Ist G endlich, existiert für jedes $p \mid \#G$ eine p-Sylowgruppe.
  - Ist H eine p-(Sylow)-Gruppe, dann auch gHg^{-1}.
- konjugierte Elemente: Seien $g, x \in G$, dann heißt gxg^{-1} das zu x durch g konjugierte Element
- konjugierte Untergruppen: Seien $H, K \leq G$, dann heißen H, K zueinander konjugiert, wenn es $g \in G$ gibt mit $K = gHg^{-1}$.
- Konjugationsklassen von x: $\{axa^{-1} \mid a \in G\}$
  - Bahn von x in der Gruppenoperation $(a, x) \mapsto axa^{-1}$
- Frobenius: Sei $p^s \mid \#G$, dann existieren $1 + kp$ Untergruppen der Ordnung p^s, $k \in \mathbb{N}_0$.
- Cauchy: Ist $p \mid \#G$, existiert ein Element mit Ordnung p.
- Sylow-Sätze: Sei $\#G = p^r m$, $p \nmid m$.
  - Sylow 1: Für alle $0 \leq s \leq r$ hat G eine Untergruppe der Ordnung p^s.
  - Sylow 2: Ist P eine p-Sylowgruppe und H eine p-Untergruppe, existiert $a \in G$ mit $H \subseteq aPa^{-1}$.
  - Sylow 3: Sei n_p die Anzahl der p-Sylowgruppen, dann ist $n_p \mid m$ und $n_p \equiv 1 \bmod p$
  - Alle p-Sylowgruppen sind konjugiert/isomorph.
  - Eine p-Sylowgruppe P ist Normalteiler $\iff$ P ist die einzige p-Sylowgruppe.
  - Wenn alle Sylowgruppen $P_1, \ldots, P_r$ von G Normalteiler sind, ist $G = P_1 \otimes \ldots \otimes P_r$
- Normalisator: Sei $X \subseteq G$ (nicht notwendigerweise Untergruppe), dann ist $N(X) := \{g \in G \mid gX = Xg\} \leq G$.
  - Gruppenwirkung $G \times \mathcal{P}(G) \to \mathcal{P}(G), (g, X) \mapsto gXg^{-1}$. Dann ist $\operatorname{Stab}(X) = N(X)$.
  - Für die Bahn $\Xi := \{gXg^{-1} \mid g \in G\}$ gilt $\#\Xi = \frac{\#G}{\#N(X)}$. Ist Ξ unendlich, ist $\Xi \cong G/N(X)$.

- Ist $U \leq G$, dann ist $U \trianglelefteq N(U) \leq G$ die größte Untergruppe in der U noch Normalteiler ist.
- $N(X)$ ist ein Maß dafür, wie weit X weg ist, Normalteiler zu sein.

- Zentrum: $Z(G) \coloneqq \{x \in G \mid gx = xg \quad \forall g \in G\}$
  - $Z(G) \trianglelefteq G$
  - $Z(G)$ ist die größte abelsche Untergruppe von G.
  - Ist G eine p-Gruppe, gilt $p \mid \#Z(G)$.
  - G ist abelsch $\iff G/Z(G)$ ist zyklisch
  - $Z(G)$ ist ein Maß dafür, wie weit weg G ist, abelsch zu sein.
- Normalreihe: Kette von Untergruppen $G = U_r \supset U_{r-1} \supset ... \supset U_1 \supset U_0 = \{e\}$ mit $U_{j-1} \trianglelefteq U_j$
  - Ist $\#G = p^r$, dann gibt es eine Normalreihe mit $\#U_j = p^j, 0 \leq j \leq r$.
- Cayley: $G \cong H \leq S(G)$ mit $g \mapsto \varphi_g, \varphi_g(h) = gh$
- Struktursatz für endliche abelsche Gruppen: $G \cong \mathbb{Z}_{p_1^{l_1}} \otimes ... \otimes \mathbb{Z}_{p_r^{l_r}}$ (mit nicht notwendigerweise verschiedenen Primzahlen p_i)
- Ist $\#G = p$, ist $G \cong \mathbb{Z}_p$.
- Ist $\#G = p^2$, ist $G \cong \mathbb{Z}_{p^2}$ oder $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.
- Ist $\#G = pq, p < q$, hat G genau eine q-Sylowgruppe und eine oder q verschiedene p-Sylowgruppen.
  - Falls $p \nmid q - 1$ ist G zyklisch
  - Falls $p = 2$ ist $G \cong \mathbb{Z}_{2q}$ oder $G \cong D_q$.
- Chinesischer Restsatz: Zu paarweise teilerfremden $r_1, ..., r_n \in \mathbb{N}$ und beliebigen $a_1, ..., a_n \in \mathbb{Z}$ gibt es genau ein $k \in \mathbb{Z}_{r_1 \cdots r_n}$ mit $k \equiv a_i \bmod r_i$ für alle $1 \leq i \leq n$.
  - $\varphi : \mathbb{Z}_{r_1 \cdots r_n} \to \mathbb{Z}_{r_1} \times ... \times \mathbb{Z}_{r_n}, k + r_1 \cdots r_n \mathbb{Z} \mapsto (k + r_1\mathbb{Z}, ..., k + r_n\mathbb{Z})$ ist ein Isomorphismus.
- Zyklus: Permutation $\sigma \in S_n$ mit $\sigma(a_k) = a_{k+1 \bmod l}, \sigma(x) = x$ mit $a_1, ...a_l \in \{1, ..., n\}, x \notin \{a_1, ..., a_l\}$. Wir schreiben $\sigma = (a_1, ..., a_l)$
  - Transposition: Zyklus mit $l = 2$
  - Jeder Zyklus ist Produkt von Transpositionen.
  - Jede Permutation ist Produkt von disjunkten Zyklen.
  - Jede Permutation ist Produkt von höchstens $n - 1$ Transpositionen.
  - Für zwei elementfremde Zyklen $\sigma = (A), \tau = (B), A \cap B = \emptyset$ gilt $\sigma \circ \tau = \tau \circ \sigma$.
  - $o((a_1...a_l)) = l$
  - $(a_1...a_l)^{-1} = (a_l...a_1)$
  - $(a_1...a_l) = (a_1a_2)...(a_{l-1}a_l)$
  - $\sigma(a_1...a_l)\sigma^{-1} = (\sigma(a_1)...\sigma(a_l))$
- $\operatorname{sgn} : S_n \to \{\pm 1\}, \operatorname{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$ ist ein Homomorphismus
  - $\operatorname{sgn}(\tau) = -1$ für Transpositionen $\tau \in S_n$

Beispiele für Gruppen

- zyklische Gruppe: $G = \langle g \rangle$
  - Zyklische Gruppen sind abelsch.
  - Zyklische Gruppen sind isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$.
  - Jede Untergruppe einer zyklischen Gruppe ist zyklisch.
  - Für endliche zyklische Gruppen G mit $\#G = n$ gilt $\operatorname{Aut}\ G \cong Z_n^\times$.
  - Für unendliche zyklische Gruppen gilt $\operatorname{Aut}\ G \cong \mathbb{Z}_2$
- Diedergruppe: Symmetriegruppe eines regelmäßigen n-Ecks mit Drehungen g^i und Spiegelung s.
  - $D_n = \left\{g^i s^j \mid 0 \leq i \leq n - 1, 0 \leq j \leq 1\right\}$ mit $g^n = e, s^2 = e, sgs = g^{-1}$
  - $\#D_n = 2n$
  - $\langle g \rangle \cong \mathbb{Z}_n$
- symmetrische Gruppe/Permutationsgruppe: $S_X = (\{\sigma : X \to X \mid \sigma \text{ bijektiv}\}, \circ)$

- $\#S_n = n!$
- Automorphismengruppe: $\mathrm{Aut}(G) \coloneqq \{\varphi : G \to G \mid \varphi \text{ Automorphismus}\}$
  - innerer Automorphismus: $\varphi_g(h) = ghg^{-1}$
- Für $n \neq 6$ ist jedes $\varphi \in \mathrm{Aut}(S_n)$ ein innerer Automorphismus.

- alternierende Gruppe: $A_n = \ker(\mathrm{sgn}) = \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\} \trianglelefteq S_n$
  - $\#A_n = \frac{1}{2}n!$
  - Jedes $\sigma \in A_n$ ist Produkt einer geraden Anzahl Transpositionen, d.h. $A_n = \langle\{(ab)(cd) \mid 1 \leq a < b \leq n, 1 \leq c < d \leq n\}\rangle$
  - Für $n \geq 3$ ist $A_n = \langle\{(abc) \mid 1 \leq a < b < c \leq n\}\rangle$
  - Für $n \geq 5$ ist A_n einfach.
- $\mathrm{GL}_n = \{A \in \mathbb{R}^{n\times n} \mid \det A \neq 0\}$
- $O_n = \left\{A \in \mathbb{R}^{n\times n} \mid A^T A = E\right\}$
  - $O_2 = \left\{\begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix} \mid \theta \in (0, 2\pi]\right\}$
- $\mathrm{SO}_n = \{A \in O_n \mid \det A = 1\}$

Ringtheorie

- Einheitengruppe: $R^\times = \{r \in R \mid \exists\ r' \in R \text{ mit } rr' = r'r = 1\}$
- Die einzigen Ringhomomorphismen $\mathbb{Z} \to \mathbb{Z}$ sind 0 und id.
- Ideal: Unterring $\mathfrak{a} \subseteq R$ mit $R\mathfrak{a} \subseteq \mathfrak{a}, \mathfrak{a}R \subset \mathfrak{a}$
  - Einfacher Ring: nur $\{0\}, R$ sind Ideale
  - Jeder einfache kommutative Ring mit 1 ist ein Körper.
- Faktorring: Sei $\mathfrak{a} \subset R$ Ideal, dann ist $R/\mathfrak{a}$ (bzgl. $+$) ein Ring mit
  - $(r_1 + \mathfrak{a}) + (r_2 + \mathfrak{a}) = (r_1 + r_2) + \mathfrak{a}$
  - $(r_1 + \mathfrak{a})(r_2 + \mathfrak{a}) = (r_1 r_2) + \mathfrak{a}$
  - Hauptideal: $\mathfrak{a} = (a)$
- $(A) = \{\text{endliche Summe von Ausdrücken der Form } na, r_1 a, ar_2, r_1 a r_2 \mid a \in A, n \in \mathbb{Z}, r_1, r_2 \in R\}$
  - Ist R kommutativ: $(A) = \left\{\sum_{i=1}^{s}(k_i a_i + r_i a_i) \mid a_i \in A, k_i \in \mathbb{Z}, r_i \in R\right\}$
  - Ist R kommutativ mit 1: $(A) = \left\{\sum_{i=1}^{s} r_i a_i \mid a_i \in A, r_i \in R\right\}$, und $(a) = Ra$
- Produktideal: $(\mathfrak{ab})$ mit $\mathfrak{ab} = \{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$
- Maximales Ideal: $\mathfrak{m} \subsetneq R$ mit $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R \Longrightarrow \mathfrak{a} = R$ oder $\mathfrak{a} = \mathfrak{m}$
  - Ist $\mathfrak{m}$ maximales Ideal und $\mathfrak{a} \not\subset \mathfrak{m}$, dann ist $\mathfrak{a} + \mathfrak{m} = R$.
  - Ist R kommutativ mit 1, dann ist $\mathfrak{m}$ maximales Ideal genau dann, wenn $R/\mathfrak{m}$ ein Körper ist.
- Lemma von Zorn: Ist X halbgeordnet und jede total geordnete Teilmenge von X hat eine obere Schranke, dann hat X ein maximales Element.
  - Sei R Ring mit 1 und $\mathfrak{a} \subsetneq R$ Ideal, dann existiert ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subseteq \mathfrak{m}$.
- Homomorphiesatz: Sei $\varphi : R \to S$ Ringhomomorphismus, dann ist $\ker(\varphi)$ ein Ideal in R und $R/\ker(\varphi) \cong S$
  - Korrespondenzsatz: Sei $\varphi : R \to S$ surjektiver Ringhomomorphismus, dann gibt es eine Bijektion zwischen den Idealen von S und den Idealen von R die $\ker(\varphi)$ enthalten, mit $\mathfrak{a} \mapsto \varphi(\mathfrak{a})$ und $\mathfrak{b} \mapsto \varphi^{-1}(\mathfrak{b})$. Es gilt $R/\mathfrak{a} \cong S/\varphi(\mathfrak{a})$.
- Erster Isomorphiesatz: Sei R Ring, $\mathfrak{a}$ Ideal und S Unterring, dann ist $S/(S \cap \mathfrak{a}) \cong (S + \mathfrak{a})/\mathfrak{a}$.
- Zweiter Isomorphiesatz: Sei R Ring, $\mathfrak{b} \subseteq \mathfrak{a}$ beides Ideale, dann ist $R/\mathfrak{a} \cong (R/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b})$.
- Nullteiler: $a \in R$ mit $\exists b \in R \setminus \{0\}$ mit $ab = 0$ oder $ba = 0$
- Kürzungslemma: Sei $a \in R$ kein Nullteiler, dann $ab = ac$ oder $ba = ca$ impliziert $b = c$.
- Teiler: $d \mid a$ falls $a = dr$ oder $a = rd$ für ein $r \in R$.
  - gemeinsamer Teiler: $d \mid a_i$ für $1 \leq i \leq n$

  - größter gemeinsamer Teiler: $D = \gcd(a_1, ..., a_n)$ falls D gemeinsamer Teiler der a_i und $d \mid D$ für jeden gemeinsamen Teiler d der a_i gilt
  - teilerfremde Elemente: $\gcd(a_1, ..., a_n) = 1$
- assoziierte Elemente: $a \sim b$ falls $a = \varepsilon b$ für ein $\varepsilon \in R^\times$
- primes Element: $p \mid ab$ impliziert $p \mid a$ oder $p \mid b$
- irreduzibles Element: $q = bc$ impliziert $b \in R^\times$ oder $c \in R^\times$
  - prim $\implies$ irreduzibel
- Integritätsring: kommutativer Ring ohne Nullteiler
- Hauptidealring: Integritätsring mit 1, in dem jedes Ideal Hauptideal ist
- Faktorieller Ring: Integritätsring mit 1, in dem alle $r \in R \setminus (R^\times \cup \{0\})$ eine im wesentlichen eindeutige Zerlegung in irreduzible Elemente hat: $r = q_1 \cdot \cdots \cdot q_s$. Äquivalente Charakterisierungen:
  - Jedes $r \in R \setminus (R^\times \cup \{0\})$ ist Produkt irreduzibler Elemente und alle irreduziblen Elemente sind prim.
  - Jedes $r \in R \setminus (R^\times \cup \{0\})$ ist Produkt primer Elemente.
  - Es gilt die Teilerkettenbedingung und Primbedingung:
    - Jede aufsteigende Folge $(a_1) \subseteq (a_2) \subseteq ...$ von Hauptidealen wird stationär.
    - Jedes irreduzible Element ist prim.
- Euklidischer Ring: kommutativer Ring mit 1 und Funktion $E : R \setminus \{0\} \to \mathbb{N}_0$. Zu $a, b \in R, b \neq 0$ existieren $q, r \in R$ mit $a = qb + r$ und $r = 0$ oder $E(r) < E(b)$.
  - In euklischen Ringen terminiert der euklidische Algorithmus.
- Noetherscher Ring: kommutativer Ring mit 1, in dem jedes Ideal endlich erzeugt ist. Äquivalente Charakterisierungen:
  - Jede aufsteigende Folge von Idealen wird stationär.
  - Jede nichtleere Menge von Idealen hat ein maximales Element.
- Primideal: Sei R kommutativer Ring, dann heißt $\mathfrak{p}$ Primideal, wenn $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Äquivalente Charakterisierungen:
  - $a, b \notin \mathfrak{p} \implies ab \notin \mathfrak{p}$
  - $R/\mathfrak{p}$ ist unter Multiplikation abgeschlossen
  - $R/\mathfrak{p}$ ist Integritätsring
  - $\varphi : R \to R/\mathfrak{p}, r \mapsto r + \mathfrak{p}$ ist Ringhomomorphismus mit $\ker(\varphi) = \mathfrak{p}$
- Sei R Integritätsring mit 1, $p \in R \setminus (R^\times \cup \{0\})$
  - $1 \mid a, a \mid 0, a \mid a$
  - $R^\times = \{d \in R \mid d \mid 1\}$
  - $a \mid b \implies ac \mid bc$
  - $a \mid b_i$ für $1 \leq i \leq n$ impliziert $a \mid \sum_{i=1}^{n} b_i$
  - $a \mid b$ und $b \mid c$ impliziert $a \mid c$
  - $a \mid b \iff b \in (a) \iff (b) \subseteq (a)$
  - $a \mid b$ und $b \mid a$ impliziert $a \sim b$
  - p prim $\iff (p)$ ist Primideal
  - p irreduzibel $\iff (p)$ ist maximal in $\{\mathfrak{a} \subset R \mid \mathfrak{a} \neq R\}$
  - p prim: $p \mid a$ oder p und a sind teilerfremd
  - p, q prim: $p \sim q$ oder p und q teilerfremd
- Sei R Hauptidealring:
  - $d = \gcd(a_1, ..., a_n) \iff (d) = (a_1, ..., a_n)$
  - Bezout: Sei $d = \gcd(a_1, ..., a_n)$, dann existieren $r_1, ..., r_n \in R$ mit $d = \sum_{i=1}^{n} r_i a_i$
  - Euklidischer Hilfssatz: Seien a, b teilerfremd, dann gilt $a \mid bc \implies a \mid c$ und $a \mid c, b \mid c \implies ab \mid c$

- Sei $a \in R \setminus (R^\times \cup \{0\})$, dann existieren $p_1, ..., p_r$ prim mit $a = p_1 \cdot \cdots \cdot p_r$. Diese Zerlegung ist bis auf Reihenfolge und Assoziiertheit eindeutig.

Beispiele für Ringe

- Matrizenring: $R^{n\times n} = \left\{ \left(a_{ij}\right)_{1\le i,j\le n} \mid a_{ij} \in R \right\}$
- Potenzreihenring: $R[[X]] = \left\{ \sum_{i=0}^{\infty} a_i X^i \mid a_i \in R \right\}$
  - $\sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} b_i X^i = \sum_{i=0}^{\infty} (a_i + b_i) X^i$
  - $\left(\sum_{i=0}^{\infty} a_i X^i\right)\left(\sum_{i=0}^{\infty} b_i X^i\right) = \sum_{i=0}^{\infty} \sum_{j=0}^{i} a_j b_{i-j} X^i$
- Polynomring: $R[X] = \left\{ \sum_{i=0}^{n} a_i X^i \mid a_i \in R, n \in \mathbb{N}_0 \right\}$, Unterring von $R[[X]]$
- Polynomabbildungen: $\mathcal{P}(R) = \left\{ \tilde{f} : R \to R, x \mapsto f(x) \mid f \in R[X] \right\}$
- $\mathbb{Z}\left[\sqrt{-5}\right] = \left\{ a + \sqrt{5}bi \in \mathbb{C} \mid a, b \in \mathbb{Z} \right\}$
  - kein faktorieller Ring: $6 = 2 \cdot 3 = \left(1 + \sqrt{5}i\right)\left(1 - \sqrt{5}i\right)$
- $\mathbb{Z}[i]$ ist euklidischer Ring mit $E(z) = |z|^2$

Polynome in einer Unbestimmten

- Ist R kommutativer Ring mit 1, $f, g \in R[X]$, mit $f, g, fg \neq 0$, dann ist $\deg(fg) \le \deg(f) + \deg(g)$
  - Ist R zusätzlich Integritätsring, gilt $\deg(fg) = \deg(f) + \deg(g)$
- R Integritätsring mit $1 \iff R[X]$ Integritätsring mit 1
- Ist K Körper, dann ist $K[X]$ euklidischer Ring mit $E(f) = \deg(f)$
- Sei R Integritätsring mit 1, dann ist $R[X]$ Hauptidealring genau dann, wenn R Körper ist.
- Sei R Integritätsring mit 1 und $a \in R$ Nullstelle von $f \in R[X]$, dann ist $X - a \mid f$.
  - Seien $a_1, ..., a_n \in R$ alle Nullstellen von $f \in R[X]$, dann ist $(X - a_1)^{\nu_1} \cdot \cdots \cdot (X - a_n)^{\nu_n} \mid f$.
- Sei R Integritätsring mit 1 und $\#R = \infty$, dann ist $R[X] \cong \mathcal{P}(R)$
- Sei R Integritätsring mit 1 und $a_0, ..., a_n \in R$ paarweise verschieden und $f, g \in R[X]$ mit $\deg(f) \le n, \deg(g) \le n$ und $f(a_i) = g(a_i)$ für $0 \le i \le n$, dann ist $f = g$.
- Lagrange-Interpolation: Sei K Körper und $a_0, ..., a_n \in K$ paarweise verschieden, dann existiert für jedes $b_0, ..., b_n \in K$ genau ein Polynom $f \in K[X]$ mit $\deg(f) \le n$ und $f(a_i) = b_i$ für $0 \le i \le n$. Dann gilt $f = \sum_{i=0}^{n} b_i \prod_{j=0, j\neq i}^{n} \frac{X - a_j}{a_i - a_j}$
- Gauß: Ist R faktorieller Ring, dann ist auch $R[X]$ faktorieller Ring.
- Inhalt: Sei $f = \sum_{i=0}^{n} a_i X^i$, dann ist $I(f) = \gcd(a_0, ..., a_n)$
  - f heißt primitiv, falls $1 \in I(f)$.
- Lemma von Gauß: Sei R faktoriell, $f, g \in R[X]$, dann gilt $I(fg) \sim I(f)I(g)$
  - Ist $f, g \in R[X]$ primitiv, dann ist auch fg primitiv.
- Sei $f \in R[X]$ und $K = Q(R)$
  - Kleiner Gauß: Ist $f = gh$ mit $g, h \in K[X]$, dann existieren $a, b, c \in K^\times$ mit $f = cg_1h_1$ und $g_1 = ag, h_1 = bh$ primitiv in $R[X]$.
  - Ist f irreduzibel in $R[X]$, dann ist f irreduzibel in $K[X]$.
  - Ist $f = gh$ mit $g \in K[X]$ und $h \in R[X]$ primitiv, dann ist $g \in R[X]$.
  - Sei $g \in R[X]$, dann gilt: $f \mid g$ in $R[X]$ genau dann, wenn $I(f) \mid I(g)$ in R und $f \mid g$ in $K[X]$.
- Sei $f = \sum_{i=0}^{n} a_i X^i \in R[X], n \ge 2$.
  - Wenn f eine Nullstelle $\frac{c}{b} \in K$ hat, gilt $b \mid a_n$ und $c \mid a_0$.
  - Reduktionssatz: Sei $\varphi : R \to S$ Ringhomomorphismus mit $\varphi(1_R) = 1_S$. Ist $\varphi(f) \in S[X]$ irreduzibel, dann ist f irreduzibel.

- Eisenstein: Wenn es ein Primelement $p \in R$ gibt mit $p \mid a_i$ für $0 \leq i \leq n-1$, $p \nmid a_n$ und $p^2 \nmid a_0$, dann ist f irreduzibel in $R[X]$ und $K[X]$.
- Basissatz von Hilbert: Sei R noetherscher Ring, dann ist auch $R[X]$ noetherscher Ring.

Polynome in mehreren Unbestimmten

- Grad: Ein Monom: $aX_1^{k_1} \cdot \cdots \cdot X_n^{k_n}$ hat Grad $k_1 + ... + k_n$.
  - Ein Polynom $f = \sum_{i_1,...,i_n} a_{i_1,...,i_n} X_1^{i_1} \cdot \cdots \cdot X_n^{i_n}$ hat Grad $\max\{i_1 + ... + i_n \mid a_{i_1,...,i_n} \neq 0\}$
  - f heißt homogen vom Grad d, falls alle Monome von f Grad d haben.
- symmetrisches Polynom: S_n wirke auf $R[X_1, ..., X_n]$ durch $\sigma f = f\big(X_{\sigma(1)}, ..., X_{\sigma(n)}\big)$. f heißt symmetrisch, falls $\sigma f = f$ für alle $\sigma \in S_n$. Die symmetrischen Polynome bilden einen Unterring von $R[X_1, ..., X_n]$.
- elementarsymmetrische Polynome: $s_k = \sum_{i_1 < ... < i_k} X_{i_1} \cdot \cdots \cdot X_{i_k}$
  - $\prod_{j=1}^{n} (Y - X_j) = \sum_{k=0}^{n} (-1)^k s_k(X_1, ..., X_n) Y^{n-k} \in R[X_1, ..., X_n][Y]$
- Fundamentalsatz der symmetrischen Polynome: Sei R Integritätsring mit 1, dann ist jedes symmetrische Polynom in $R[X_1, ..., X_n]$ eindeutig darstellbar als Polynom in den elementarsymmetrischen Polynomen.
  - $\varphi : R[X_1, ..., X_n] \to R[X_1, ..., X_n], f \mapsto f(s_1, ..., s_n)$ ist ein Isomorphismus auf den symmetrischen Polynomen.
  - Ist $f(s_1, ..., s_n) = 0$, dann ist $f = 0$.

Körpertheorie

- Schiefkörper: Körper mit nichtkommutativer Multiplikation
- Seien $K \subset M \subset L$ Körper. Dann heißen, L/M, M/K, L/K Körpererweiterungen und M heißt Zwischenkörper.
- Primkörper: $\Pi(L) = \bigcap\{K \mid K \text{ Teilkörper von } L\}$
- Ist $\mathrm{char}(L) = 0$, dann ist $\Pi(L) \cong \mathbb{Q}$. Ist $\mathrm{char}(L) = p > 0$, dann ist $\Pi(L) \cong \mathbb{F}_p$.
- Adjunktion: Sei L/K Körpererweiterung und $A \subset L$, dann ist $K(A) = \bigcap\{M \mid M \text{ Zwischenkörper von } L/K, A \subset M\}$ der kleinste Teilkörper von L, der A enthält.
- Grad: Ist L/K Körpererweiterung, dann ist L ein K-Vektorraum. Der Grad $[L : K]$ von L/K ist die Dimension von L als K-Vektorraum.
  - Gradsatz: Sind L/M und M/K Körpererweiterungen, dann ist $[L : K] = [L : M] \cdot [M : K]$. Ist $(v_i)_{i \in I}$ eine Basis von L/M und $\big(w_j\big)_{j \in J}$ eine Basis von M/K, dann ist $\big(v_i w_j\big)_{i \in I, j \in J}$ eine Basis von L/K.
  - Ist $\#K < \infty$ und $\mathrm{char}(K) = p$, dann ist $\#K = p^{[K:\mathbb{F}_p]}$ und $K \cong \mathbb{F}_p^{[K:\mathbb{F}_p]}$
  - L/K heißt endlich, wenn $[L : K] < \infty$.
  - L/K heißt einfach, wenn $L = K(a)$ mit $a \in L$. a heißt primitives Element.
- Transzendente/Algebraische Elemente: $a \in L$ heißt algebraisch, wenn es ein $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$ gibt. Andernfalls heißt a transzendent.
- Minimalpolynom: Sei L/K Körpererweiterung, $a \in L$ algebraisch, und $\varepsilon_a : K[X] \to L$ der Einsetzungshomomorphismus. Dann ist $\ker(\varepsilon_a) = (m_a)$ da $K[X]$ Hauptidealring ist, und wenn m_a normiert ist, heißt m_a Minimalpolynom von a über K.
  - m_a ist irreduzibel in $K[X]$.
  - $K(a) \cong K[X]/(m_a)$
  - $1, a, ..., a^{\deg(m_a)-1}$ ist eine Basis von $K(a)/K$, insbesondere ist $[K(a) : K] = \deg(m_a)$.
  - $[K(a) : K] < \infty \iff a$ ist algebraisch über K
- Sei L/K Körpererweiterung und $a \in L$ transzendent über K. Dann ist $K(a) \cong K(X)$ mit $\frac{f}{g} \mapsto \frac{f(a)}{g(a)}$ und $1, a, a^2, ...$ sind linear unabhängig.

- Algebraische Körpererweiterung: L/K mit allen $a \in L$ algebraisch über K
  - $[L:K] < \infty \Longrightarrow L/K$ algebraisch
  - $[L:K] < \infty \Longleftrightarrow L = K(a_1, ..., a_n)$ mit a_i algebraisch über K
  - L/K ist genau dann einfach algebraisch,also $L = K(a)$, wenn L/K nur endlich viele Zwischenkörper hat.
  - Ist M Zwischenkörper von L/K, dann gilt: L/K algebraisch $\Longleftrightarrow L/M$ und M/K algebraisch.
- algebraischer Abschluss: $A(L/K) := \{a \in L \mid a \text{ algebraisch über } K\}$ ist ein Teilkörper von L.

Beispiele für (Schief-)Körper

- Hamilton'sche Quaternionen: $\mathbb{R}^4$ mit Basis $1, i, j, k$ mit $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$
- Quotientenkörper: Sei R Integritätsring, dann ist $Q(R) = \left\{\frac{a}{b} \mid a \in R, b \in R \setminus \{0\}\right\}/\sim$ mit $\frac{a}{b} \sim \frac{b}{c} \Longleftrightarrow ac = bd$.
  - $\mathbb{Q} := Q(\mathbb{Z})$
  - Körper der rationalen Funktionen: $R(X) = Q(R[X])$