Inhaltsangabe zur Vorlesung Algebra

JProf.-Dr. Christoph Wockel

16. Juli 2012

Elementare Gruppentheorie

1. Vorlesung (10. April)

Grundbegriffe der Gruppentheorie:

- Definition: Monoide, Gruppen, Ordnung
- Beispiele: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (additiv), $\mathbb{Q}^*$ (multiplikativ), $\mathrm{Sym}(X)$, $\mathrm{GL}(V)$, $\mathrm{GL}_n(k)$
- Definition: Homomorphismus, Endomorphismus, Isomorphismus, Automorphismus (+Beispiele)
- Schreibweisen $g_1 \circ ... \circ g_n$, gh, $g + h$, g^n
- Lemma: Kürzungsregeln $(h = g^{-1}k) \Leftrightarrow (gh = k) \Leftrightarrow (g = kh^{-1})$
- Definition: Untergruppe (+Kriterium $gh^{-1} \in H$)
- Beispiele: $\mathrm{SL}_n(k)$, $\mathrm{SL}_2(\mathbb{Z})$, Dreiecksmatrizen.

Literatur: [JS06], **I.1.5-I.1.10** (nicht **I.1.3**+**I.1.4**)

2. Vorlesung (13. April)

- Erzeugen von Untergruppen, Erzeugendensystem
- Satz:
  1. $\text{ord}(g) = n < \infty \Rightarrow n$ minimal mit $g^n = e$
  2. $\text{ord}(g) = \infty \Leftrightarrow g_n \neq g^m \ \forall\ n, m$
  3. $\text{ord}(g) = n < \infty \Rightarrow \text{ord}(g^s) = \frac{n}{\text{ggT}(n,s)}$
- Definition: Zyklische Gruppe.
- Satz: Untergruppen zyklischer Gruppen sind zyklisch.
- Definition: Links- und Rechtsnebenklassen von Untergruppen.
- Definition: Transversale einer Untergruppe (T ist H-Transversale, wenn jedes xH *genau* ein Element von T enthält)
- Definition/Satz: Index $[G : H]$ einer Untergruppe $H \leq G$ und
$$[G : H] = [G : N] \cdot [N : H].$$

Literatur: [JS06], **I.1.11-I.1.14**

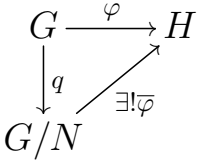
3. Vorlesung (20. April)

- Satz von Lagrange: $H \leq G \Rightarrow |H|$ teilt $|G|$.
- Kleiner Satz von Fermat: $g^{|G|} = 1$ für jedes $g \in G$.
- Definition: Eulersche φ-Funktion $\varphi(n) := |\{d < n \mid d \text{ teilerfremd zu } n\}|$.
- Satz von Euler: m, n teilerfremd $\Rightarrow m^{\varphi(n)} = 1 \bmod n$
- Definition: Normale Untergruppe ($N \trianglelefteq G \Leftrightarrow g^{-1}Ng \in N$ für $g \in G$)
- Beispiel: $\mathrm{SL}_n(k) \trianglelefteq \mathrm{GL}_n(k)$
- Definition: Faktorgruppe G/N und Quotientenhomom. $G \to G/N$
- Definition: Normale Hülle, erzeugte *normale* Untergruppe
- Def.: Kern $\ker(\varphi)$ und Bild $\mathrm{im}(\varphi)$ eines Homom. $\varphi\colon G \to H$.
- Satz: $\varphi(g^n) = \varphi(g)^n$ $\forall n \in \mathbb{Z}$, $\mathrm{im}(\varphi) \leq H$ und $\ker(\varphi) \trianglelefteq G$.
- Satz: normale Untergruppen sind Kerne von Homomorphismen

Literatur: [JS06] **I.1.15-I.1.16** [Sch], **1.6.3**+**1.6.6** [JS06], **§I.2**

4. Vorlesung (24. April)

- Beispiel (Konjugation): $G \xrightarrow{\alpha} \mathrm{Aut}(G)$, $g \mapsto c_g$ (hier: $\mathrm{im}(\alpha) \trianglelefteq \mathrm{Aut}(G)$).
- Universelle Eigenschaft der Faktorgruppe: falls $N \subseteq \ker(\varphi)$, so gilt



- Kanonische Faktorisierung: $\varphi\colon G \to H$ induziert Isomorphismus $\overline{\varphi}\colon G/\ker(\varphi) \to \mathrm{im}(\varphi)$
- Beispiel: Endliche zyklische Gruppen sind isomorph zu $\mathbb{Z}_n$
- 1. Isomorphiesatz: $H \leq G$, $N \trianglelefteq G \Rightarrow H/(N \cap H) \cong NH/N$
- 2. Isomorphiesatz: $M \trianglelefteq G$, $N \trianglelefteq G$, $N \leq M \Rightarrow (G/N)/(M/N) \cong G/M$.
- Def.: Direktes Produkt $\prod_{i \in I} G_i$ einer Familie $(G_i)_{i \in I}$ von Gruppen.
- Satz: Universelle Eigenschaft des direkten Produkts.

Literatur: [JS06], **§I.2.6**, **§I.4** und **§I.5.1** (universelle Eigenschaft: Übung)

5. Vorlesung (27. April)

- Beispiel: $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$
- Satz: Kriterium für $G \cong G_1 \times \ldots \times G_n$ mit $G_i \trianglelefteq G$
- Def.: Direkte Summe $\bigoplus_{i \in I} A_i$ einer Familie $(A_i)_{i \in I}$ *abelscher* Gpn.
- Universelle Eigenschaft der direkten Summe.
- Def.: Semi-direkte Produkte anhand des Bsp.: $\mathrm{SL}_n(k) \trianglelefteq \mathrm{GL}_n(k)$
  ($\mathrm{SL}_n(k)$ hat Komplement $\{\mathrm{diag}(1, ..., 1, a) \colon a \neq 0\}$)
- Satz/Def.: Homom. $\gamma \colon H \to \mathrm{Aut}(N) \rightsquigarrow N \times H$ wird mit

$$(n, h) \cdot (n', h') := (n\gamma(h)(n'), hh')$$

  zur Gruppe $N \rtimes H$ und $N \trianglelefteq (N \rtimes H)$, $H \leq (N \rtimes H)$, $N \cap H = \{e\}$

Literatur: [JS06], **I.5.2-§I.5.5** (ohne Gruppenerweiterungen)

6. Vorlesung (4. Mai)

- Definition: Symmetrische Gruppe $S_n := \mathrm{Sym}(\{1, ..., n\})$
- Definition: Zykel $\pi = (m_1 ... m_k)$
- Satz: S_n wird erzeugt von
  - sowohl allen Zyklen als auch (nur) den Transpositionen,
  - ebenso von $A = \{(12), (13), ..., (1n)\}$
  - und auch von $B = \{(12), (23), ..., (n-1\ n)\}$.
- Def.: Signum von $\pi \in S_n$: $\mathrm{sgn}(\pi) := \prod_{1 \le i < j \le n} \frac{\pi(i) - \pi(j)}{i - j}$
- Satz/Def.: $\mathrm{sgn}\colon S_n \to \{\pm 1\}$ ist Homomorphismus, $\mathrm{sgn}^{-1}(1)$:=gerade Permutationen, $\mathrm{sgn}^{-1}(-1)$:=ungerade Permutationen.

Literatur: [JS06], **§I.3**

7. Vorlesung (8. Mai)

- Def.: Alternierende Gruppe $A_n := \ker(\text{sgn}) \trianglelefteq S_n$
- Eigenschaften: $S_n = A_n \rtimes \{\pm 1\}$, $[S_n : A_n] = 2$, $|A_n| = \frac{n!}{2}$
- Beispiel: Dieder-Gruppe $N \rtimes \mathbb{Z}_2$, insbesondere $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$
- Def.: Gruppenwirkungen $(G \curvearrowright X)$: $G \times X \to X$, $(g, x) \mapsto g.x$ mit

$$(g \cdot h).x = g.(h.x) \quad \text{und} \quad e.x = x \quad \forall g, h \in G, x \in X$$

- Lemma: Gruppenwirkungen $\overset{1:1}{\longleftrightarrow}$ Homomorphismen $G \to \text{Sym(X)}$
- Def.: Bahn $G \cdot x$, transitive und treue Wirkung, G-Morphismus
- Beispiele für Gruppenwirkungen:
  - $S_n \curvearrowright \{1, ..., n\}$ (via $S_n \xrightarrow{\text{id}} \text{Sym}(\{1, ..., n\})$)
  - $G \curvearrowright G$ durch $g.h := c_g(h) := ghg^{-1}$ (Konjugationswirkung)
    Beachte: $c_g \in \text{Aut}(G)$ (und nicht nur $c_g \in \text{Sym}(G)$)!
  - $H \leq G \Rightarrow G \curvearrowright G/H$, $g.(xH) = (gx)H$ (wirkt transitiv)

- Def.: Isotropiegruppe (Stabilisator) G_x

Literatur: [JS06], **I.3.4 I.6.1-I.6.3**

8. Vorlesung (11. Mai)

- Beispiel: $\mathrm{SO}_2(\mathbb{R})$ wirkt auf $\mathbb{R}^2$ durch Rotation (daran anschaulich: Bahnen, Stabilisatoren)
- Lemma: $G_{g.x} = gG_xg^{-1}$
- Beispiel: Zentralisator, Normalisator
- Satz: $G \curvearrowright X \Rightarrow p\colon G/G_x \to G{\cdot}x$ ist Isomorphismus von G-Räumen (insbesondere gilt $|G \cdot x| = [G : G_x]$).
- Beispiel: $\mathrm{SO}_n(\mathbb{R})$ wirkt auf $\mathbb{R}^n \rightsquigarrow \mathbb{S}^{n-1} \cong \mathrm{SO}_n(\mathbb{R})/\mathrm{SO}_{n-1}(\mathbb{R})$
- Kor.: $(x_i)_{i\in I}$: Repräs.-syst. d. Bahnen $\Rightarrow |X| = |X^G| + \sum\limits_{x_i \notin X^G} [G : G_{x_i}]$
- Burnside-Lemma: $|G\backslash X| = |G|^{-1} \sum_{g\in G} |\operatorname{Fix}_g|$ ($\operatorname{Fix}_g = \{x : g.x = x\}$)
- Beispiel: Dieder-Gruppen D_n als Symmetriegruppe des reg. n-Ecks

Literatur: [JS06], **I.6.2-I.6.6** (Burnside-Lemma: Wikipedia)

Strukturtheorie von Gruppen

9. Vorlesung (15. Mai) Bis auf Widerruf: p Primzahl.

- Definition: G ist p-Gruppe $:\Leftrightarrow |G| = p^k$ für ein $k \in \mathbb{N}_0$.
- Satz (Cauchy): $p \mid |G| \Rightarrow \exists g \in G$ mit $\operatorname{ord}(g) = p$.
- Kor.: G ist p-Gruppe $\Leftrightarrow \forall\ g \in G$ gilt $\operatorname{ord}(g) = p^k$ für ein $k \in \mathbb{N}$.
- Lemma: G p-Gruppe, $G \curvearrowright X$, $|X| < \infty \Rightarrow |X| \equiv |X^G| \bmod p$.
- Satz: G p-Gruppe, $G \neq \{1\} \Rightarrow Z(G) \neq \{1\}$.
- Definition: $|G| = p^m q$ mit $\operatorname{ggT}(p, q) = 1$, $H \leq G$ mit $|H| = p^m \Leftrightarrow$:
  H ist p-Sylow-Untergruppe
- Satz (Sylow): $|G| = p^m q$ mit $\operatorname{ggT}(p, q) = 1$:
  a) $1 \leq k \leq m \Rightarrow \exists\ H \leq G$ mit $|H| = p^k$.
  b) $H \leq G$ p-Ugp., $S \leq G$ p-Sylow-Ugp. $\Rightarrow \exists\ g \in G$: $H \leq gSg^{-1}$
  c) Mit $\operatorname{Syl}_p G := \{H \leq G : H \text{ ist } p\text{-Sylow Ugp.}\}$ und $s := |\operatorname{Syl}_p G|$ gilt $s \mid q$ und $s \equiv 1 \bmod p$.

Literatur: [JS06], **II.1**

10. Vorlesung (18. Mai)

- Korollar: Alle p-Sylow-Untergruppen sind zueinander konjugiert.
- Beispiel: $|G| = 2 \cdot 3 \cdot 7 \Rightarrow \exists\ N \trianglelefteq G$ mit $N \cong \mathbb{Z}_7$ und $|G/N| = 6$.
- Satz: Sind p, q Primzahlen mit $p < q$ und $p \nmid (q-1)$, dann gilt

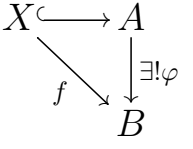
$$|G| = pq \Rightarrow g \cong \mathbb{Z}_{pq}$$

- Satz: $|G| = 2p \Rightarrow G \cong \mathbb{Z}_{2p}$ oder $G \cong D_p$.
- Beispiel: Klassifikation einiger Gruppen bis Ordnung 20.

[JS06], **II.5.1-II.5.3**

11. Vorlesung (22. Mai) Bis auf Widerruf: A abelsche Gruppe.

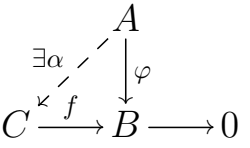
- Satz: Charakterisierung direkter Summen abelscher Gruppen.
- Def.: A heißt *frei abelsch*, falls $A \cong \bigoplus_{i \in I} \mathbb{Z}$.
- Lemma/Def.: A frei abelsch $\Leftrightarrow \exists\, X \subseteq A$ mit $\operatorname{ord}(x) = \infty$ für $x \in X$ und $A = \bigoplus_{x \in X} \langle x \rangle$. Dann heißt X *Basis* von A.
- Universelle Eigenschaft frei abelscher Gruppen: Ist X eine Basis von A, B abelsch, $f\colon X \to B$ eine *Funktion* so existiert ein eindeutiger Homomorphismus $\varphi\colon A \to B$ mit $\alpha|_X = f$:



- Kor.: Jede abelsche Gruppe ist Quotient einer frei abelschen Grp.
- Satz: Basen isomorpher Gruppen haben gleiche Mächtigkeit.

$\rightsquigarrow$ Def.: $\operatorname{Rang}(A) := |X|$.

- Def.: A heißt *projektiv* $:\Leftrightarrow$ Für jeden Hom. $\varphi\colon A \to B$ und surjektiven Hom. $f\colon C \to B$ existiert $\alpha\colon A \to C$ mit $f \circ \alpha = \varphi$:



- Satz: Eine frei abelsche Gruppe ist projektiv.
- Kor.: $B \leq A$ mit A/B frei $\Rightarrow A = Q \oplus B$ mit $Q \cong A/B$.

Literatur: [JS06], **II.5.1** bis **II.5.7**

12. Vorlesung (25. Mai)

- Satz: Untergruppen frei abelscher Gruppen sind frei abelsch von kleinerem Rang.
- Kor.: A ist projektiv $\Leftrightarrow$ A ist frei abelsch.
- Satz: Endlich erzeugbare abelsche Gruppen sind Quotienten frei abelscher Gruppen mit endlichem Rang. Untergruppen endlich erzeugbarer Gruppen sind endlich erzeugbar.
- Def.: Torsionsgruppen (jedes Elt. hat endliche Ordnung) und torsionsfreie Gruppen, $T(A) \leq A$ Torsionsuntergruppe.
- Lemma: $T(A) \leq A$ und $A/T(A)$ ist torsionsfrei.
- Def.: p-primäre Komponente $A_p := \{a \in A \mid \exists n \in \mathbb{N} : p^n a = 0\}$.
- Satz: A endlich erzeugbar, torsionsfrei $\Rightarrow$ A frei abelsch.
- Kor.: A endlich erzeugbar $\Rightarrow$ $A \cong F \oplus T(A)$ mit F frei, $T(A)$ endlich.

Literatur: [JS06], **II.5.8** bis **II.5.12**

13. Vorlesung (5. Juni)

- Satz: $|A| < \infty \Rightarrow A = \oplus_p A_p$ mit $A_p := \{a \in A \mid \exists n \in \mathbb{N} : p^n a = 0\}$.
- Satz: $|A| < \infty$, $a \in A$ habe maximale Ordnung

  $$\Rightarrow \text{existiert Ugp. } U \leq A \text{ mit } A = \langle a \rangle \oplus U.$$

- Satz: $|A| = p^n \Rightarrow$ ex. $\nu_1 \geq ... \geq \nu_k > 0$ mit $\sum_{i=1}^{k} \nu_i = n$ und $B_i \leq A$ mit $|B_i| = p^{\nu_i}$ und

  $$A = B_1 \oplus ... \oplus B_k.$$

  Die ν_i sind durch A eindeutig bestimmt.

- **Theorem** (Klassifikation endlich erzeugbarer abelscher Gruppen): Ist A endlich erzeugbar und abelsch, dann existieren Primzahlpotenzen $q_1, ..., q_k$ so dass

  $$A = \mathbb{Z}^{\text{Rang}(A)} \oplus \mathbb{Z}/q_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/q_k\mathbb{Z}$$

  Es sind die q_i und $\text{Rang}(A)$ durch A eindeutig festgelegt.

Literatur: [JS06], **II.5.13** bis **II.5.17**

Ringe

- Def.: Ring, kommutativer Ring, Ringhomomorphismus (-endomorphismus, -isomorphismus, -automorphismus).
- Bsp.: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, der Matrizenring $M_n(k)$, Produkte von Ringen, $\mathrm{End}(A)$ für A eine abelsche Gruppe.
- Def.: Unterring, Links- und Rechtsideal, Ideal (Notation: $\mathfrak{s} \trianglelefteq R$).

Literatur: [JS06], **III.1.1** bis **III.1.3**

14. Vorlesung (8. Juni)

- Summe, Schnitt und Produkt von Idealen, echte Ideale
- Ideale in $\mathbb{Z}$ sind von der Form $n\mathbb{Z}$ und $n\mathbb{Z} + m\mathbb{Z} = \mathrm{ggT}(n, m)\mathbb{Z}$
- Lemma: $\mathfrak{s} \trianglelefteq R \Rightarrow R/\mathfrak{s}$ ist ein Ring bzgl. $(x + \mathfrak{s}) \cdot (y + \mathfrak{s}) = (xy + \mathfrak{s})$
- $R/\mathfrak{s}$ heißt Faktorring, Beziehung zu Idealen in R, universelle Eigenschaft von $R/\mathfrak{s}$, $S \subseteq R$ Unterring $\Rightarrow S/S \cap \mathfrak{s} \to S + \mathfrak{s}/\mathfrak{s}$ ist Isom.
- Def.: Inverse, Einheiten (Notation: R^*), Divisionsring, Nullteiler, Integritätsbereich, Körper
- Satz: R Körper $\Leftrightarrow$ R und $\{0\}$ sind einzige Ideale $\Leftrightarrow$ jeder Ringhom. $\varphi\colon R \to S$ mit $S \neq 0$ ist injektiv.
- Def. (Charakteristik): $\varphi\colon \mathbb{Z} \to R$, $n \mapsto n \cdot 1_R$ hat Kern $\mathrm{char}(R) \cdot \mathbb{Z}$.
- Bsp.: $\mathrm{char}(\mathbb{Z}) = 0$; $\mathrm{char}(\mathbb{Z}_n) = n$; R Integritätsbereich $\Rightarrow \mathrm{char}(R) =$ Null oder Primzahl
- $\mathrm{char}(R) = p$ (Primzahl) $\rightsquigarrow$ Frobenius-Endomorphismus $x \mapsto x^p$.

Literatur: [JS06], **III.1.3** bis **III.2.6**

15. Vorlesung (12. Juni) Bis auf Widerruf: A, B kommutative Ringe.

- Def.: Hauptideal $(x) := xA$ für jedes $x \in A$, Hauptidealring
- Von $M \subseteq A$ erzeugtes Ideal, endlich erzeugbares Ideal
- Def.: $\mathfrak{p} \subsetneq A$ Primideal $:\Leftrightarrow p \cdot q \in \mathfrak{p}$ impliziert $p \in \mathfrak{p}$ oder $q \in \mathfrak{p}$
  $\mathfrak{a} \subsetneq A$ max. Ideal $:\Leftrightarrow \nexists \mathfrak{b} \trianglelefteq A$ mit $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq A$
- Lemma: $\mathfrak{p} \trianglelefteq A$ prim $\Leftrightarrow A/\mathfrak{p}$ ist Integritätsbereich
  $\mathfrak{a} \trianglelefteq A$ maximal $\Leftrightarrow A/\mathfrak{a}$ ist Körper.
- Bsp.: In $\mathbb{Z}$ sind Primzahlen = Primideale = max. Ideale
- Primideale verhalten sich schön unter Urbildern von Ringhomom.!
- Def.: A euklidisch $:\Leftrightarrow \exists$ Gradabbildung $\lambda\colon A\backslash\{0\} \to \mathbb{N}$
- Satz: A euklidisch $\Rightarrow$ jedes Ideal ist Hauptideal
- Bsp.: $\mathbb{Z}$ und $k[X]$ sind Hauptidealringe.
- Satz: Jedes Ideal ist in einem maximalen Ideal enthalten.
- Def.: Teilerfremdheit von Idealen.

Literatur: [JS06], **III.3.1** bis **III.3.8** (nicht **III.3.5 (2)**)

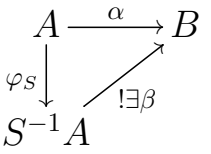
16. Vorlesung (15. Juni)

- Satz: $\mathfrak{a}_1, ..., \mathfrak{a}_n \trianglelefteq A$ paarweise teilerfremde Ideale $\Rightarrow$
  1. Jedes $\mathfrak{a}_i$ ist teilerfremd zu $\prod_{i \neq j} \mathfrak{a}_j$
  2. $\prod_{i=1}^n \mathfrak{a}_i = \cap_{i=1}^n \mathfrak{a}_i$.
  3. $A/\prod_{i=1}^n \mathfrak{a}_i \to \prod_{i=1}^n A/\mathfrak{a}_i$, $x \mapsto (x + \mathfrak{a}_1, ..., x + \mathfrak{a}_n)$ ist Isom.
- Bsp.: Simultane Kongruenzen, Chinesischer Restesatz (falls $A = \mathbb{Z}$).
- Kor.: $p, q \in \mathbb{Z}$ teilerfremd $\Rightarrow \varphi(pq) = \varphi(p)\varphi(q)$
- Anwendung: RSA-Verschlüsselung
- Def.: Ring der Brüche $S^{-1}A$ für $S \subseteq A$ multiplikativ abgeschlossen:

  $S^{-1}A := (A \times S)/\sim$ mit $(a, s) \sim (b, t) :\Leftrightarrow \exists u \in S : (at - bs)u = 0$

- Lemma: $\varphi_S \colon A \to S^{-1}A$, $a \mapsto (a, 1)$ ist Ringhom. und $\varphi_S(S) \subseteq (S^{-1}A)^*$

- Universelle Eigenschaft: $\alpha\colon A \to B$ mit $\alpha(S) \subseteq B^*$, dann gilt



- Bsp.: A nullteilerfrei $\Rightarrow S := A\backslash\{0\}$ mult. abgeschl., $S^{-1}A$ Körper (der *Quotientenkörper* $Q(A)$ von A).

- Bsp.: $\mathfrak{p} \trianglelefteq A$ prim $\Rightarrow S := A\backslash\mathfrak{p}$ mult. abgeschl., $A_{\mathfrak{p}} := S^{-1}A$ „Lokalisierung“ von A an $\mathfrak{p}$ (hat eindeutiges maximales Ideal).

Literatur: [JS06], **III.3.9** bis **III.4.3**, RSA-Verfahren: [Sch] **I.6.7**

17. Vorlesung (19. Juni) Bis auf Widerruf: A Integritätsbereich.

- Def.: Für $a, b, p, u \in A$ definieren wir:
  $a \mid b :\Leftrightarrow \exists c : ac = b \Leftrightarrow (b) \subseteq (a)$ („a teilt b“)
  $a \sim b :\Leftrightarrow a \mid b$ und $b \mid a \Leftrightarrow (a) = (b)$ („a und b assoziiert“)
  p prim $:\Leftrightarrow p \neq 0$ und (p) ist Primideal
  u irreduzibel $:\Leftrightarrow u \neq 0$, $u \notin A^*$ und
  $u = v \cdot w \Rightarrow u \in A^*$ oder $v \in A^*$

- Bem.: „assoziiert“ ist Äq.-rel. da $a \sim b \Leftrightarrow \exists u \in A^*$ mit $a = ub$.

- Bem.: $u \in A$ ist genau dann irreduzibel wenn $(u) \neq 0$, $(u) \neq A$ und (u) maximales *Haupt*ideal ist.

- Bsp.: In $A = \mathbb{Z}$ ist a unzerlegbar falls $a = \pm p$ für p Primzahl.

- Satz: $a \in A$ prim $\Rightarrow a$ irreduzibel. Ist Hauptidealring, so gilt die Umkehrung auch und Primideale sind maximale Ideale.

- Def.: $a, b \in A \rightsquigarrow \mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ (nicht eindeutig!)

- Satz: In Hauptidealringen existieren $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ immer.

- Def.: a, b *teilerfremd* $\Leftrightarrow$ 1 ist ein ggT(a, b).
- Kor.: a, b *teilerfremd* $\Leftrightarrow$ (a) und (b) teilerfremd $\Leftrightarrow$ $1 = ma + nb$.
- Bestimmung von ggT(a, b) mit dem Euklidischer Algorithmus.

Literatur: [JS06], **III.5.1** bis **III.5.6**

18. Vorlesung (22. Juni)

- Def.: A ist *faktoriell* $:\Leftrightarrow$ jedes $0 \neq a \in A \backslash A^*$ hat „eindeutige“ Produktdarstellung durch irreduzible.

- Satz: Es sind äquivalent

  1. A ist faktoriell.
  2. Jedes irreduzible Element ist prim und jedes $0 \neq a \in A \backslash A^*$ hat Produktdarstellung durch irreduzible.
  3. Jedes irreduzible Element ist prim und jede aufsteigende Kette $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq ... \subsetneq \mathfrak{a}_n \subsetneq ...$ von *Haupt*idealen wird stationär.

- Korollar: In einem faktoriellen Ring ist jedes Hauptideal in nur endlich vielen Hauptidealen echt enthalten.

- Primfaktorzerlegung und Bestimmung von ggT und kgV.

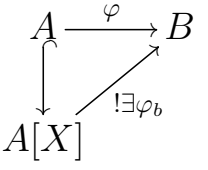
- Def.: R heißt *noethersch* falls jede aufsteigende Kette $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq ... \subsetneq \mathfrak{a}_n \subsetneq ...$ von (beliebigen) Idealen stationär wird.
- Satz: Es sind äquivalent:
  1. R ist noethersch.
  2. Jede nicht-leere Menge von Idealen hat ein maximales Element.
  3. Jedes Ideal von R ist endlich erzeugbar.
- Kor.:Hauptidealringe sind noethersch und faktoriell.
- Def.: Polynom (abbrechende Folge $f = (f_n)_{n \in \mathbb{N}_0}$), Polynomring $A[X]$
- Achtung: Polynome sind nicht das gleiche wie Polynomfunktionen!

Literatur: [JS06], **III.5.7** bis **III.5.11** und **IV.1.1**

Polynomringe

19. Vorlesung (26. Juni) A, B: (bis auf Widerruf) A, B kommutative Ringe

- Darstellung $f \in A[X]$ als $f = \sum f_n X^n$, $\mathrm{gr}(f)$ („Grad“), normiertes Polynom
- Universelle Eigenschaft von $A[X]$: ist $\varphi\colon A \to B$ Hom. $b \in B$



mit $\varphi_b(X) = b$. $\rightsquigarrow$ Auswertungshomomorphismus für $a \in A$:

$$\mathrm{ev}_a\colon A[X] \to A \text{ mit } \mathrm{ev}_a(X) = a \text{ und } f(a) := \mathrm{ev}_a(f)$$

- Satz: $\mathrm{gr}(f+g) \leq \max\{\mathrm{gr}(f), \mathrm{gr}(g)\}$, $\mathrm{gr}(fg) \leq \mathrm{gr}(f) + \mathrm{gr}(g)$, $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$ in Integritätsbereichen.
- Kor.: A Integritätsbereich $\Leftrightarrow$ $A[X]$ Integrtätsbereich. Außerdem gilt $A[X]^* = A^*$.

- Beispiele:
  1. $A \subseteq B$ Unterring, $b \in B$ heißt *algebraisch* über A falls $f \in A[X]$ ex. mit $f(b) = 0$ (andernfalls heißt a *transzendent*).
  2. $\varphi\colon A \to B \rightsquigarrow \varphi_*\colon A[X] \to B[X]$ mit $\varphi_*(\sum f_n X^n) = \sum \varphi(f_n) X^n$
  3. Reduktion der Koeffizienten für $\mathfrak{a} \trianglelefteq A$: $\pi_*\colon A[X] \to (A/\mathfrak{a})[X]$
- Satz: Eindeutige Division mit Rest in $A[X]$ ($\Rightarrow k[X]$ ist euklidisch).
- Kor.: $A[X]$ Hauptidealring $\Leftrightarrow$ A ist Körper.
- Def.: $a \in A$ ist *Nullstelle* (NS) von $f \in A[X]$ falls $f(a) = 0$.
- Satz: $f = (X - a_1)^{n_1} \cdots (X - a_m)^{n_m} \cdot g$ so dass die a_i paarweise verschieden sind und g keine NS mehr hat.
- Def.: f *zerfällt in Linearfaktoren* falls $g \in A$ in obiger Zerlegung.
- Satz.: A nullteilerfrei $\Rightarrow$ f hat höchstens $\mathrm{gr}(f)$ viele NS.

Literatur: [JS06], **IV.1.1** bis **IV.2.2**

20. Vorlesung (29. Juni)

- Kor.: k: Körper, $G \leq k^*$ endliche Ugp. $\Rightarrow G$ ist zyklisch.
- Kor.: A nullteilerfrei, $|A| = \infty \Rightarrow \mathrm{ev}\colon A[X] \to \mathrm{Map}(A, A)$ injektiv.
- k : endlicher Körper $\Rightarrow \ker(\mathrm{ev}) = (X^n - X) \cdot k[X]$ mit $n = |k|$.
- Definition: n-fache NS.
- Differentiation von Polynomen $f \mapsto f'$, Linearität und Leibnitzregel.
- Satz: Für $f \in k[X]$, $\mathrm{gr}(f) > 0$, $f(a) = 0$ ist die Vielfachheit von a genau dann 1 wenn $f'(a) \neq 0$.
- Satz: $f \in k[X]$, $\mathrm{gr}(f) > 0$:
  1. $\mathrm{char}(k) = 0 \Rightarrow \mathrm{gr}(f') = \mathrm{gr}(f) - 1$
  2. $\mathrm{char}(k) = p \Rightarrow \mathrm{gr}(f') \leq \mathrm{gr}(f) - 1$ und

$$f' = 0 \Leftrightarrow \exists g \in k[X] \text{ mit } f(X) = g(X^p)$$

Von nun an sei (bis auf Widerruf) A ein faktorieller Ring und $k = Q(A)$ der Quotientenkörper von A. Außerdem wählen wir ein festes Repräsentantensystem $\mathcal{P}$ der irreduziblen Elemente von A (dadurch werden z.B. ggT und kgV eindeutig).

- Def.: Inhalt $c(f)$ für $f \in A[X]$ und $f \in k[X]$.
  f ist *primitiv* $:\Leftrightarrow c(f) = 1$.

- Lemma:

  1. Zerlegung $f = \frac{a}{b} f_0$ mit $\mathrm{ggT}(a, b) = 1$, f_0 primitiv (ist eindeutig bis auf Einheiten).
  2. $f \in A[X] \Rightarrow b \sim 1$ und $a \sim c(f)$.

- Satz: Es gilt $c(f \cdot g) = c(f) \cdot c(g)$ für $f, g \in k[X] \backslash \{0\}$.

Literatur: [JS06], **IV.2.3** bis **IV.2.8** und **IV.4.1** bis **IV.4.3**

21. Vorlesung (3. Juli) Bis auf Widerruf: A faktoriell $k := Q(A)$.

- Kor.: Für $f \in A[X]$ gilt
  1. $f = gh$ in $k[X] \Rightarrow f = c(f)g_0h_0$ in $A[X]$ (g_0, h_0 primitiv, s.o.)
  2. f irred. in $A[X] \Leftrightarrow f$ irred. in $k[X]$ und $c(f) = 1$
  3. $f = gh$ in $k[X]$ und $g \in A[X]$ primitiv $\Rightarrow h \in A[X]$
- Satz (Eisenstein-Kriterium): Sei $f = \sum_{i=0}^{n} f_i X^i \in A[X]$ vom Grad n und $p \in A$ prim mit

  $$p \mid f_i \text{ für } i < n, \quad p \nmid f_n \quad \text{und} \quad p^2 \nmid f_0.$$

  Dann ist f in $A[X]$ (und somit auch in $k[X]$) irreduzibel.
- Beispiele:
  1. $X^3 - 2$ ist über $\mathbb{Z}$ irreduzibel
  2. für p Primzahl ist $X^{p-1} + ... + X + 1 = \frac{X^p - 1}{X - 1}$ über $\mathbb{Z}$ irreduzibel
  3. $Y^3 + X^2 - 1$ ist in $\mathbb{Q}[X, Y]$ irreduzibel.

- Satz (Reduktionskriterien):

  1. $\varphi\colon A \to B$, $f \in A[X]$ mit $\varphi(f_{\mathrm{gr}(f)}) \neq 0$:

     $$f = gh \text{ mit } g, h \notin A \Rightarrow \varphi_*(f) = \varphi_*(g)\varphi_*(h) \text{ mit } \varphi_*(g), \varphi_*(h) \notin B$$

  2. $\mathfrak{p} \trianglelefteq A$ prim, $\pi\colon A \to A/\mathfrak{p}$, $f \in A[X]$ mit $\pi(f_{\mathrm{gr}(f)}) \neq 0$:

     $$\pi_*(f) \in (A/\mathfrak{p})[X] \text{ irred.} \Rightarrow f \in Q(A)[X] \text{ irred.}$$

- Satz (ohne Beweis): A faktoriell $\Rightarrow A[X]$ faktoriell.
- Satz (ohne Beweis): A noethersch $\Rightarrow A[X]$ noethersch.
- Insbesondere ist $A[X_1, ..., X_n]$ immer faktoriell und noethersch wenn A dies ist, aber nur ein Hauptidealring falls $n = 1$ und A ein Körper.

Literatur: [JS06], **IV.4.5** bis **IV.4.9**

Körpererweiterungen

22. Vorlesung (6. Juli)

Von nun an seinen (bis auf Widerruf) E, F, k Körper. Es bezeichnet $k \subset E$ eine Körpererweiterung und $\mathbb{F}_p$ den Körper mit p Elementen.

- Def.: Primkörper $P_k := \bigcap\{U \mid U \text{ ist Teilkörper von } k\} \subset k$
- Lemma: $P_k \cong \mathbb{Q}$ falls $\text{char}(k) = 0$ und $P_k \cong \mathbb{F}_p$ falls $\text{char}(k) = p$.
- Def.: $k \subset E$ heißt *einfach* falls $E = k(a)$ für ein $a \in E$.
- Lem.: Der Ringhomomorphismus $\varphi_a \colon k[X] \to k(a)$ mit $\varphi_a|_k = \text{id}_k$ und $\varphi_a(X) = a$ ist injektiv oder surjektiv (aber nicht beides).
- φ_a injektiv ($\Leftrightarrow a$ transzendent) $\Rightarrow \varphi_a$ induziert $k(X) \xrightarrow{\cong} k(a)$
- φ_a surjektiv ($\Leftrightarrow a$ algebraisch) $\Rightarrow \varphi_a$ induziert $k[X]/I \xrightarrow{\cong} k(a)$
- Def.: a algebraisch $\Rightarrow I = (p)$ für $p \in k[X]$ irreduzibel, normiert mit $p(a) = 0$. Dieses p heißt *Minimalpolynom* von a (Bez.: $m_{a,k}$).
- Satz: 1. a transzendent $\Rightarrow [k(a) : k] = \infty$
  2. a algebraisch $\Rightarrow [k(a) : k] = \text{gr}(m_{a,k})$

- Bsp.: $\mathbb{C} = \mathbb{R}(i)$ und $[\mathbb{R}(i) : \mathbb{R}] = 2$, da $m_{i,\mathbb{R}} = X^2 + 1$;
  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, da $m_{\sqrt[3]{2},\mathbb{Q}} = X^3 - 2$; $[\mathbb{Q}(e^{\frac{2\pi i}{3}}) : \mathbb{Q}] = 2$
- Def.: $k \subset E$ heißt *endlich* falls $[E : k] < \infty$ und *algebraisch* falls jedes $a \in E$ über k algebraisch ist.
- Satz:
  1. $k \subset E$ endlich $\Rightarrow k \subset E$ algebraisch
  2. $k \subset E$ endlich $\Leftrightarrow E = k(a_1, ..., a_n)$ für $a_i \in E$ algebraisch
  3. $k \subset F$ und $F \subset E$ algebraisch $\Rightarrow k \subseteq E$ algebraisch
- Def.: k heißt *algebraisch abgeschlossen* falls jedes $f \in k[X] \backslash k$ eine Nullstelle in k hat.
- Satz: Es sind äquivalent
  1. k ist algebraisch abgeschlossen.
  2. Jedes $f \in k[X] \backslash k$ ist Produkt von Polynomen vom Grad 1.
  3. Die irreduziblen Polynome sind genau $X - a$ für $a \in k$.
  4. Ist $k \subset E$ algebraisch, so gilt $E = k$.
- Def.: Algebraischer Abschluss.

Literatur: [LL07], Kapitel **3** und [JS06], **VI.2.3** und **IV.3.3**

23. Vorlesung (10. Juli)

- Theorem: Jeder Körper hat einen algebraischen Abschluss
- Bsp.: $\mathbb{R} \subset \mathbb{C}$; $\mathbb{Q} \subset \mathbb{C}$ (ist kein alg. Abschluss); $[\overline{\mathbb{F}_q}, \mathbb{F}_q] = \infty$
- Def.: k-Homomorphismus $\varphi\colon k \subset E \to k \subset F$, $\mathrm{Hom}_k(E,F)$, $\mathrm{Aut}_k(E)$
- φ ist k-Isomorphismus $\Leftrightarrow [E:k] = [F:k]$
- φ ist k-Homom. $a \in E$ alg. $\Rightarrow \varphi(a) \in F$ alg. und $\varphi_*(m_a, k) = m_{\varphi(a),k}$
- Satz: Sei $\sigma\colon k_1 \to k_2$, $k_1 \subset E$, $k_2 \subset F$ und $a \in E$, $b \in F$ algebraisch.

  1. Gilt $\sigma_*(m_{a,k_1}) = m_{b,k_2}$, dann gibt es genau einen Homom. $\varphi_{a,b}\colon k_1(a) \to F$ mit $\varphi_{a,b}|_{k_1} = \sigma$ und $\varphi_{a,b}(a) = b$ und es gilt $\varphi_{a,b}(k_1(a)) = k_2(b)$.
  2. Die Abbildung

     $$\mathrm{NS}(\sigma_*(m_{a,k})) \to \{f \in \mathrm{Hom}(k_1(a), E)\colon\ f|_{k_1} = \sigma\}, \quad c \mapsto \varphi(a,c)$$

     ist bijektiv.

- Kor.: $k \subset k(a)$, $k \subset k(b)$, $m_{a,k} = m_{b,k} \Rightarrow \exists! \varphi \colon k \subset k(a) \to k \subset k(b)$ mit $\varphi(a) = b$
- Satz: Fortsetzung von Homomorphismen $\varphi \colon k \to M$ mit M algebraisch abgeschlossen zu $\widetilde{\varphi} \colon E \to M$ falls $k \subset E$ algebraisch.
- Kor.: Algebr. Abschluss ist eindeutig bis auf k-Isomorphismen!
- Def.: Zerfällungskörper eines Polynoms $f \in k[X]$.
- Satz: Existenz und Eindeutigkeit von Zerfällungskörpern.
- Bsp.: $\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$ ist Zerfällungskörper von $X^3 - 2$.

Literatur: [KM10], Kapitel **23** [JS06], **IV.3** und **IV.4**

24. Vorlesung (13. Juli)

- Def.: $k \subset E$ *normal* $:\Leftrightarrow E = k(\mathrm{NS}(M))$ mit $M \subseteq k[X]$.
- Satz: $k \subset E$ algebraisch, $E \subset \overline{E}$ alg. Abschluss. Es sind äquivalent:

  1. $k \subset E$ ist normal.
  2. $E = k(\mathrm{NS}(\{m_{a,k} \colon a \in E\}))$.
  3. Für jeden k-Hom. $\varphi \colon k \subset E \to k \subset \overline{E}$ gilt $\varphi(E) = E$.
  4. Jedes irred. $p \in k[X]$ mit einer NS in E zerfällt über E in Linearfaktoren.

- Satz: E: Körper, $G \leq \mathrm{Aut}(E)$,

$$k := E^G := \{a \in E \colon \sigma(a) = a \ \forall \sigma \in G\}.$$

  Ist $G \cdot a = \{a_1, ..., a_n\}$, so ist a alg. über k mit $m_{a,k} = \prod_{i=1}^{n}(X - a_i)$.
- Def.: Eine Erweiterung $k \subset E$ heißt *galoissch* falls $k = E^{\mathrm{Aut}_k(E)}$.
- Satz: Ist $\mathrm{char}(k) = 0$ und $k \subset E$ algebraisch, so sind äquivalent:

  1. $k \subset E$ ist galoissch.
  2. $k \subset E$ ist normal.

- Bsp.: Zerfällungskörper von Polynomen sind galoissch.
- Def.: $\mathcal{Z}(k \subset E) :=$ Menge der Zwischenkörper von $k \subset E$
  $\mathcal{U}(\mathrm{Aut}_k(E)) :=$ Menge der Untergruppen von $\mathrm{Aut}_k(E)$.
- Satz: $k \subset E$ galoissch, $\mathrm{char}(k) = 0$:
  1. Für $F \in \mathcal{Z}(k \subset E)$ ist $F \subset E$ galoissch.
  2. $\mathcal{Z}(k \subset E) \to \mathcal{U}(\mathrm{Aut}_k(E))$, $F \mapsto \mathrm{Aut}_F(E)$ ist injektiv.
- Theorem (Hauptsatz): $k \subset E$ endlich, galoissch:
  $$\mathcal{Z}(k \subset E) \to \mathcal{U}(\mathrm{Aut}_k(E)),\ F \mapsto \mathrm{Aut}_F(E)$$
  $$\mathcal{U}(\mathrm{Aut}_k(E)) \to \mathcal{Z}(k \subset E),\ U \mapsto E^U$$
  sind invers zueinander und es gilt:
  1. $[E : F] = |\mathrm{Aut}_F(E)|$ für alle $F \in \mathcal{Z}(k \subset E)$
  2. $F_1 \subset F_2 \Leftrightarrow \mathrm{Aut}_{F_2}(E) \subseteq \mathrm{Aut}_{F_1}(E)$
  3. $k \subset F$ galoissch $\Leftrightarrow \mathrm{Aut}_F(E) \trianglelefteq \mathrm{Aut}_k(E)$.
- Bsp.: $|k| = p^n$ endlich $\Rightarrow \mathbb{F}_p \subset k$ galoissch und $\mathrm{Aut}_{F_p}(k) \cong \mathbb{Z}_n$ wird vom Frobenius-Automorphismus erzeugt.

Literatur: [KM10] Kapitel **23.3** und **26**, [LL07] Kapitel **8**

Literatur

[JS06] Jantzen, J. C. and Schwermer, J. *Algebra* (Springer Verlag, 2006). URL http://www.springerlink.com/content/978-3-540-21380-2

[KM10] Karpfinger, C. and Meyberg, K. *Algebra* (Spektrum Akademischer Verlag, 2010)

[LL07] Lorenz, F. and Lemmermeyer, F. *Algebra 1. Körper und Galoistheorie. (4. Auflage)* (Heidelberg: Elsevier/Spektrum Akademischer Verlag, 2007)

[Sch] Schweigert, C. *Algebra*. http://www.math.uni-hamburg.de/home/schweigert/. URL http://www.math.uni-hamburg.de/home/schweigert/ss03/skript.pdf. Skript