Algebra I - Wintersemester 2005/2006
Prof. Dr. F. Herrlich

Timo Bingmann

28. Juli 2006

Inhaltsverzeichnis

Benannte Sätze

Einleitung

Algebra beschäftigt sich mit Lösen von Gleichungen:

- Polynomiale Gleichungen: $f(x) = 0$ für $f \in K[x]$.
  $$\begin{aligned} &f_1(x_1, \dots x_n) = 0 \\ \text{also} \quad &\vdots \\ &f_r(x_1, \dots x_n) = 0 \end{aligned}$$
- Quadratische Gleichungen: $x^2 + px + q = 0$
  $\Longrightarrow x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$
- Gleichungen 3. Grades: $f(x) = x^3 + ax + b = 0$
  $$\Longrightarrow x = \sqrt[3]{-\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{-\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}$$
- Gleichungen 4. Grades: lassen sich auf Gleichungen 3. Grades zurückführen.
- Lagrange ($\sim$1780) : Nutze Symmetrie.

  Beispiel: $f(x) = x^3 + ax + b$ habe die Lösungen x_1, x_2, x_3.

  Sei ξ dritte Einheitswurzel:
  $$(x_1 + \xi x_2 + \xi^2 x_3)^3$$
  ist invariant unter zyklischer Vertauschung von x_1, x_2, x_3. Es genügt also einer quadratischen Gleichung.
- Galois (1830): allgemeine Lösungstheorie

Kapitel 1

Gruppen

1.1 Grundlegende Definitionen

Definition 1.1

Sei M eine Menge.

a) Eine ***Verknüpfung*** auf M ist eine Abbildung $\cdot : M \times M \to M$

b) Eine Menge M zusammen mit einer Verknüpfung $\cdot$ heißt ***Magma***.

c) Eine Verknüpfung $\cdot : M \times M \to M$ heißt ***assoziativ***, wenn

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \qquad \forall x, y, z \in M$$

d) Eine ***Halbgruppe*** ist ein assoziatives Magma.

e) $e \in M$ heißt ***neutrales Element*** für die Verknüpfung $\cdot$, wenn für alle $x \in M$ gilt:

$$x \cdot e = e \cdot x = e$$

f) Eine Halbgruppe mit neutralem Element heißt ***Monoid***.

g) Eine ***Gruppe*** ist ein Monoid $(G, \cdot)$, in dem es zu jedem $x \in G$ ein $x' \in G$ gibt, so dass

$$x \cdot x' = x' \cdot x = e$$

x' heißt ***zu*** x ***inverses Element***.

Bemerkung 1.2

Sei $(M, \cdot)$ ein Magma.

a) In M gibt es höchstens ein neutrales Element

Beweis Sind e_1, e_2 neutrale Elemente, so ist

$$e_1 \overset{e_2 \text{ neutral}}{=\!=} e_1 \cdot e_2 \overset{e_1 \text{ neutral}}{=\!=} e_2$$

b) Ist M Monoid, so gibt es zu $x \in M$ höchstens ein inverses Element.

Beweis Sind x', x'' zu x invers, so ist

$$x' = (x'' \cdot x) \cdot x' = x' \cdot (x \cdot x') = x''$$

Definition und Bemerkung 1.3

Sei $(M, \cdot)$ ein(e) $\left\{ \begin{array}{c} \text{Magma} \\ \text{Halbgruppe} \\ \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$

a) $U \subseteq M$ heißt Unter-$\left\{ \begin{array}{c} \text{Magma} \\ \text{Halbgruppe} \\ \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$, wenn $U \cdot U \subseteq U$ (Verknüpfung bleibt auf U)

und $(U, \cdot)$ selbst $\left\{ \begin{array}{c} \text{Magma} \\ \text{Halbgruppe} \\ \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$ist.

b) $U \subseteq M$ Unterhalbgruppe $\iff U \cdot U \subseteq U$.

Beweis Klar.

c) $U \subseteq M$ Untermonoid $\iff U \cdot U \subseteq U$ und $e \in U$.

Beweis Klar.

d) (***Untergruppenkriterium***)
$G \subseteq M$ Untergruppe $\iff U \neq \emptyset$ und für alle $x, y \in U$ gilt $x \cdot y^{-1} \in G$

Beweis „$\Longrightarrow$“ Klar. „$\Longleftarrow$“:
Sei $x \in U \implies e = x \cdot x^{-1} \in U$
$\implies$ mit x ist auch x^{-1} in U.
$\implies$ mit x, y ist auch $x \cdot y = x \cdot (y^{-1})^{-1} \in U$.

Bemerkung 1.4

Sei $(M, \cdot)$ Monoid, dann ist

$$M^\times = \left\{ x \in M : \text{ es gibt inverses Element } x^{-1} \text{ zu } x \text{ in } M \right\}$$

eine Gruppe.

Beweis $e \in M^\times$, da $e \cdot e = e$, also $M^\times \neq \emptyset$.
Sind $x, y \in M^\times$, so ist $x \cdot y \in M$,
da $x \cdot y \cdot (y^{-1} \cdot x^{-1}) = e \implies \cdot$ ist Verknüpfung auf $M^\times$.
$\implies (M^\times, \cdot)$ ist Gruppe.

Definition und Bemerkung 1.5

Seien $(M, \cdot)$, $(M', *)$ $\left\{\begin{array}{c}\text{Magma}\\ \text{Halbgruppe}\\ \text{Monoid}\\ \text{Gruppe}\end{array}\right\}$

a) Eine Abbildung $f : M \to M$ heißt ***Homomorphismus***, wenn für alle $x, y \in M$ gilt:

$$f(x, y) = f(x) * f(y) \qquad \text{(i)}$$

Hat M ein neutrales Element, so muss außerdem gelten:

$$f(e) = e' \qquad \text{(ii)}$$

b) Ist $f : G \to G'$ Abbildung von Gruppen, die (i) erfüllt, so ist f Homomorphismus ((ii) ist bereits erfüllt)

Beweis $f(e) = f(e \cdot e) = f(e) * f(e) \implies$ (Multipliziere mit $f(e)^{-1}$ aus G') $\implies e' = f(e)$.

c) Ein Homomorphismus $f : M \to M'$ heißt ***Isomorphismus***, wenn es einen Homomorphismus $g : M' \to M$ gibt mit $f \cdot g = id_M$

d) Jeder bijektive Homomorphismus ist ein Isomorphismus.

Beweis Sei $f : M \to M'$ bijektiver Homomorphismus
und $g : M' \to M$ die Umkehrabbildung.

Zu zeigen: g ist Homomorphismus.

Seien $x, y \in M'$
Schreibe $x = f(\tilde{x}), y = f(\tilde{y})$ für passende $\tilde{x}, \tilde{y} \in M$.
$\implies g(x * y) = g(f(\tilde{x}) * f(\tilde{y})) = g(f(x \cdot y)) = x \cdot y$.

e) Die Komposition von Homomorphismen ist wieder ein Homomorphismus.

Definition und Bemerkung 1.6

Sei $f : M \to M'$ Homomorphismus von $\left\{\begin{array}{c}\text{Magma}\\ \text{Halbgruppe}\\ \text{Monoid}\\ \text{Gruppe}\end{array}\right\}$

a) $\text{Bild}(f) := \{f(x) : x \in M\} \subseteq M'$
ist ein Unter-$\left\{\begin{array}{c}\text{Magma}\\ \text{Halbgruppe}\\ \text{Monoid}\\ \text{Gruppe}\end{array}\right\}$.

Beweis Sind $x, x' \in M$, so ist $f(x) * f(x') \overset{\text{f Hom}}{=\!=} f(x \cdot x') \in \text{Bild}(f)$

Sind M, M' Monoide: $f(e) = e' \in \text{Bild}(f)$

Sind M, M' Gruppen: $f(x)^{-1} = f(x^{-1}) \in \text{Bild}(f)$, denn $f(x) * f(x^{-1}) = f(x \cdot x^{-1}) = f(e) = e'$.

b) Sind M, M' $\left\{ \begin{array}{c} \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$, so ist

$$\text{Kern}(f) := \{x \in M : f(x) = e'\}$$

Unter-$\left\{ \begin{array}{c} \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$von M.

Beweis Seien $x, y \in \text{Kern}(f) \Longrightarrow f(x \cdot y) = f(x) * f(y) = e' * e' = e' \Longrightarrow x \cdot y \in \text{Kern}(f)$
Sind M, M' Monoide: $e \in \text{Kern}(f)$.
Sind M, M' Gruppen: $f(x^{-1}) = f(x)^{-1} = (e')^{-1} = e' \Longrightarrow x^{-1} \in \text{Kern}(f)$.

c) Sind G, G' Gruppen, so ist f genau dann injektiv, wenn $\text{Kern}(f) = \{e\}$

1.2 Beispiele und Konstruktionen

(1) Sei M eine Menge, $M^M := \{f : M \to M \text{ Abbildung}\}$ ist mit der Verknüpfung $\cdot$ ein Monoid.

$$\left(M^M\right)^\times = \{f : M \to M \text{ bijektive Abbildung}\} =: \text{Perm}(M) = S_m$$

Insbesondere $M = \{1, \ldots n\} : S_{\{1,\ldots n\}} =: S_n$
Ist $(M, \cdot)$ ein $\left\{ \begin{array}{c} \text{Magma} \\ \text{Halbgruppe} \\ \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$, so ist $\text{End}(M) := \{f \in M^M : f \text{ Homomorphismus}\}$ ein Untermonoid von M^M und

$$\text{Aut}(M) := \text{Perm}(M) \cap \text{End}(M)$$

Untergruppe von $\text{Perm}(M)$.

(2a) Sei X Menge, $(M, \cdot)$ ein $\left\{ \begin{array}{c} \text{Magma} \\ \text{Halbgruppe} \\ \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$, dann ist $M^X = \{f : X \to M \text{ Abbildung}\}$ mit der Verknüpfung $(f \cdot g)(x) := f(x) \cdot g(x)$ ein $\left\{ \begin{array}{c} \text{Magma} \\ \text{Halbgruppe} \\ \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$.

Assoziativ: Nein!.

Neutrales Element: Gibt es $E : X \to M$ mit $(E \cdot f)(x) = f(x) \forall x \in X$?
Ja!: $E(x) = e \forall x \in X$

Inverse Abbildung zu $f : X \to G$: $f^{-1}(x) = (f(x))^{-1}$

(2b) Ist $(M, \cdot)$ Halbgruppe und $(H, +)$ kommutative Halbgruppe,
dann ist $\text{Hom}(M, H) = \{f \in H^M : f \text{ Homomorphismus}\}$ eine kommutative Unterhalbgruppe von H^M.

Denn sind $f, g : M \to H$ homomorph, so ist für alle $x, y \in M$:

$$(f + g)(x \cdot y) = f(x \cdot y) + g(x \cdot y) = f(x) + f(y) + g(x) + g(y) = (f + g)(x) + (f + g)(y)$$

(3) Sei I eine Indexmenge. Für jedes $i \in I$ sei $(M_i, \cdot)$ ein $\left\{ \begin{array}{c} \text{Magma} \\ \text{Halbgruppe} \\ \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$.

a) $\prod_{i \in I} M_i$ ist mit komponentenweiser Verknüpfung ein $\left\{ \begin{array}{c} \text{Magma} \\ \text{Halbgruppe} \\ \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$.

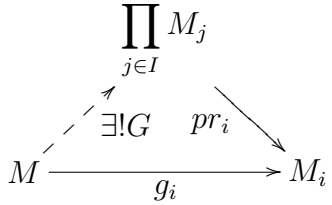
b) Sind M_i Monoide,
so ist $\bigoplus_{i \in I} M_i = \left\{ (x_i)_{i \in I} \in \prod_{i \in I} M_i : x_i = e_i \text{ für fast alle } i \right\}$ ein Monoid.

Definition und Bemerkung 1.7

a) $\prod M$ heißt ***direktes Produkt***.
$\bigoplus M$ heißt ***direkte Summe***.

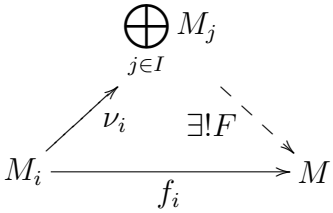
b) ist I endlich, so ist $\prod M \cong \bigoplus M$.

c) Sei M ein $\left\{ \begin{array}{c} \text{Magma} \\ \text{Halbgruppe} \\ \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$ und für jedes $i \in I$, $g_i : M \to M_i$ Homomorphismus, dann gibt es genau einen Homomorphismus $G : M \to \prod_{i \in I} M_i$, so dass $g_i = pr_i \circ G$, wobei $pr_i : \prod_{j \in I} M_j \to M_i$ Projektion.



Beweis Setze $G(m) := (m_j)_{j \in I}$ mit $m_j = g_j(m)$ für $m \in M$:
G ist Homomorphismus. $\surd$
G ist eindeutig, da $pr_i(G(m)) = g_i(m)$ sein muss.

d) Ist $(M, +)$ ein kommutativer Monoid, und für jedes $i \in I$, $f_i : M_i \to M$ ein Homomorphismus, so gibt es genau einen Homomorphismus $F : \bigoplus_{j \in I} M_j \to M$, so dass für jedes $i \in I$: $f_i = F \circ \nu_i$,
wobei $\nu_i : M_i \to \bigoplus_{j \in I} M_j$, $m \mapsto (m_j)_{j \in I}$, wobei $m_j = \begin{cases} m & j = i \\ e_j & j \neq i \end{cases}$



Beweis Setze $F((m_j)_{j\in I}) = \sum_{j\in I} f_j(m_j)$
(Betrachte $F((0,\dots 0, m_i, 0, \dots 0)) = f_i(m_i)$)

(4) Sei S eine Menge („Alphabet“).

$F^a(S) := \bigcup_{n=1}^{\infty} S^n$ ist Halbgruppe mit der Verknüpfung „Nebeneinanderschreiben“ = „Konkatenation“: $(x_1,\dots,x_n)\cdot(y_1,\dots,y_m) := (x_1,\dots,x_n,y_1,\dots,y_m)$

$F^a(S)$ heißt „Worthalbgruppe“ über S.

Variation: S^0 = „leeres Wort“.

Bemerkung 1.8

Ist $(H,\cdot)$ eine Halbgruppe, $f: S^1 \to H$ eine Abbildung, so gibt es genau einen Homomorphismus $F: F^a(S) \to H$ mit $F|_{S^1} = f$.

Beweis Setze $F((x_1,\dots,x_n)) = F((x_1)(x_2)\dots(x_n)) = F(x_1)\cdot F(x_2)\cdot\ldots\cdot F(x_n) = f(x_1)\cdot f(x_2)\cdot\ldots\cdot f(x_n)$

(5) Sei $(M,\cdot)$ ein Monoid. Für $x\in M$ ist $\varphi_x: \mathbb{N}\to M$, $n\mapsto x^n$ ein Homomorphismus.

Ist G Gruppe, $x\in G$, so ist $\varphi_x: \mathbb{Z}\to G$, $n\mapsto x^n$ ein Gruppenhomomorphismus.

Definition und Bemerkung 1.9

Sei G Gruppe.

a) $\langle x\rangle :=$ Bild(φ_x) heißt die von x erzeugt ***zyklische Untergruppe***.

b) $|\langle x\rangle|$ heißt die ***Ordnung*** von x.

c) $|G|$ heißt Ordnung von G. (falls $|G|$ endlich).

(6) Sei G Gruppe. Für $g\in G$ sei $\tau_g: G\to G$, $x\mapsto g\cdot x$ („***Linksmultiplikation***“)
$\tau_g(e) = g \Longrightarrow$ kein Gruppenhomomorphismus außer $\tau_e = id$

Bemerkung 1.10 (Satz von Cayley)

Für jede Gruppe G ist die Abbildung

$$\tau: G\to \mathrm{Perm}(G), g\mapsto \tau_g$$

ein injektiver Gruppenhomomorphismus (Einbettung)

Beweis (i) $\tau_g \in \mathrm{Perm}(G)$: τ_g ist bijektiv mit Umkehrabbildung $\tau_{g^{-1}}$

(ii) τ ist Gruppenhomomorphismus, denn $\tau(g_1\cdot g_2)(x) = (g_1\cdot g_2)x = g_1(g_2\cdot x) = \tau_{g_1}(\tau_{g_1}(x)) = (\tau_{g_1}\cdot\tau_{g_2})(x) \forall x\in G$

(iii) $\mathrm{Kern}(\tau) = \{e\}$, denn ist $\tau_g = id_G$, so ist $\tau_g(x) = g\cdot x = x \forall x\in G \Longrightarrow g = e$

Definition und Bemerkung 1.11

(7) Sei G Gruppe mit $g\in G$

a) Die Abbildung $c_g : G \to G$, $x \mapsto g \cdot x \cdot g^{-1}$ heißt ***Konjugation*** mit g.
c_g ist ein Automorphismus.

Beweis c_g ist Homomorphismus: $c_g(x_1 \cdot x_2) = g(x_1 \cdot x_2)g^{-1} = g(x_1(g^{-1}g)x_2)g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) = c_g(x_1) \cdot c_g(x_2)$
$\Longrightarrow$ c_g ist bijektiv. Die Umkehrabbildung ist $c_{g^{-1}}$

b) Die Abbildung $c : G \to \mathrm{Aut}(G)$, $g \mapsto c_g$ ist ein Gruppenhomomorphismus.

Beweis $c(g_1 \cdot g_2)(x) = (g_1g_2) \cdot x \cdot (g_1g_2)^{-1} = (g_1g_2) \cdot x \cdot (g_2^{-1}g_1^{-1}) = c_{g_1}(c_{g_2}(x)) = (c_{g_1} \cdot c_{g_2})(x) \forall x \in G$

c) $Z(G) := \mathrm{Kern}(c)$ heißt ***Zentrum*** von G.
auch ist $Z(G) = \{g \in G : gx = xg \forall x \in G\}$ „kommutative Elemente“.

d) Die Elemente von $\mathrm{Bild}(c) =: \mathrm{Aut}_i(G)$ heißen ***innere Automorphismen*** von G.

e) Eine Untergruppe $N \subseteq G$ heißt ***Normalteiler*** von G, wenn $c_g(N) \subseteq N \forall g \in G$
äquivalent: $gxg^{-1} \in N \forall g \in G \forall x \in N$

f) Ist $f : G \to G'$ ein Gruppenhomomorphismus, dann ist $\mathrm{Kern}(f)$ Normalteiler von G.

Beweis Sei $x \in \mathrm{Kern}(f)$, $g \in G$. Dann ist $f(gxg^{-1}) = f(g) \cdot f(x) \cdot f(g^{-1}) = f(g) \cdot f(g^{-1}) = e'$

g) $\mathrm{Aut}_i(G)$ ist Normalteiler in $\mathrm{Aut}(G)$.

Beweis Sei $\varphi \in \mathrm{Aut}(G), g \in G$
Zu zeigen: $\varphi c_g \varphi^{-1} \in \mathrm{Aut}_i(G)$
Es ist $(\varphi \cdot c_g \cdot \varphi^{-1})(x) = \varphi(c_g(\varphi^{-1}(x))) = \varphi(g \cdot \varphi^{-1}(x) \cdot g^{-1}) = \varphi(g) \cdot \varphi(\varphi^{-1}(x)) \cdot \varphi(g^{-1}) = \varphi(g) \cdot x \cdot \varphi(g)^{-1} = c_{\varphi(g)}(x) \forall x \in G$.
$\Longrightarrow$ $\varphi \circ c_g \circ \varphi^{-1} = c_{\varphi(g)} \in \mathrm{Aut}_i(G)$

Definition und Bemerkung 1.12

(8) Sei G Gruppe, $H \subseteq G$ Untergruppe.

a) Für jedes $g \in G$ heißt $g \cdot H = \{g \cdot h : h \in H\} = \tau_g(H)$ ***Linksnebenklassen*** von G bezüglich H.
und
$H \cdot g = \{g \cdot h : h \in H\}$ ***Rechtsnebenklassen***.

b) Für $g_1, g_2 \in G$ gilt:
$(g_1 \cdot H) \cap (g_2 \cdot H) \neq \emptyset \Longleftrightarrow g_1H = g_2H$

Beweis „$\subseteq$“ Sei $y = g_1h_1 = g_2h_2 \in g_1H \cap g_2H$ mit $h_1, h_2 \in H$.
$\Longrightarrow$ $g_1 = g_2h_2h_1^{-1} \in g_2H \Longrightarrow g_1H \subseteq g_2H$
genauso $g_2H \subseteq g_1H$

c) H ist genau dann Normalteiler, wenn $gH = Hg$ für alle $g \in G$.

Beweis $gH = Hg \Longleftrightarrow H = gHg^{-1}$

d) Alle Nebenklassen von G bzgl. H sind gleich mächtig. ($\exists$ Bijektion)

Beweis $\tau_g : H \to g \cdot H$, $h \mapsto g \cdot h$ ist bijektiv.

e) Die Anzahl der Linksnebenklassen bzgl H ist gleich der Anzahl der Rechtsnebenklassen. Sie heißt ***Index*** $[G : H]$ von H in G.

Beweis Die Zuordnung $\{\text{Linksnebenklassen}\} \to \{\text{Rechtsnebenklassen}\}$, $g \cdot H \mapsto H \cdot g^{-1}$ ist bijektiv und wohldefiniert:
wohldef: ist $g_1 H = g_2 H$, also $g_2 = g_1 h$ für ein $h \in H$,
$\implies Hg_2^{-1} = H(g_1 h)^{-1} = H \cdot h^{-1} \cdot g^{-1} = Hg_1^{-1}$

f) (Satz von Lagrange)
Ist G endlich, so ist $[G : H] = \dfrac{|G|}{|H|}$

Beweis G ist disjunkte Vereinigung der $[G : H]$ Linksnebenklassen bzgl H. Diese haben alle $|H|$ Elemente.

1.3 Quotientenbildung

Definition und Bemerkung 1.13

Sei $f : M \to M'$ eine Abbildung von Mengen.

a) Die Relation $\sim_f$ auf M, $x \sim_f y \Leftrightarrow f(x) = f(y)$ ist eine Äquivalenzrelation.

b) Für $x \in M$ sie $\bar{x} = \{y \in M : y \sim_f x\}$.
Es ist $\bar{x} = f^{-1}(\{f(x)\})$
$\overline{M} := {}^{M}\!/_{\sim_f} := \{\bar{x} : x \in M\}$

c) Ist $f : (M, \cdot) \to (M', *)$ ein Homomorphismus, so wird durch $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$ eine Verknüpfung auf $\overline{M}$ definiert.

Beweis Zu zeigen ist: $\cdot$ ist wohldefiniert.
Sei also $x' \in \bar{x}, y' \in \bar{y}$, zu zeigen: $\overline{x' \cdot y'} = \overline{x \cdot y}$
Also $f(x' \cdot y') = f(x \cdot y) \iff \overline{x'y'} = \overline{xy}$
Also $x' \in \bar{x}, y' \in \bar{y} \iff f(x') = f(x), f(y') = f(y)$
Es ist $f(x' \cdot y') = f(x') * f(y') = f(x) * f(y) = f(x \cdot y)$.

d) Ist $(M, \cdot)$ $\left\{ \begin{array}{c} \text{Magma} \\ \text{Halbgruppe} \\ \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$, so auch $(\overline{M}, \cdot)$.

Definition und Bemerkung 1.14

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

a) $\overline{G} = {}^{G}\!/_{\sim_f}$ ist die Menge der Linksnebenklassen bzgl Kern(f).

b) $\overline{G} =: {}^{G}\!/_{\mathrm{Kern}(f)}$ heißt ***Faktorgruppe*** von G bzgl. $\mathrm{Kern}(f)$.

Beweis Seien $x, y \in G$, dann gilt:
$\bar{x} = \bar{y} \iff f(x) = f(y) \iff f(x) \cdot f(y^{-1}) = e' \iff f(x \cdot y^{-1}) = e' \iff xy^{-1} \in \mathrm{Kern}(f)$
$\iff y = (xy^{-1})^{-1}x \in \mathrm{Kern}(f) \cdot x \iff x^{-1}y \in \mathrm{Kern}(f) \iff y = x \cdot (x^{-1}y) \in x\,\mathrm{Kern}(f)$
$\iff y \cdot \mathrm{Kern}(f) = x \cdot \mathrm{Kern}(f)$

Definition und Bemerkung 1.15

Sei G Gruppe, $N \subseteq G$ Normalteiler. Dann gibt es eine Gruppe $\overline{G}$ und einen surjektiven Gruppenhomomorphismus $f : G \to \overline{G}$ mit $N = \mathrm{Kern}(f)$.

Folgerung: Nach 1.14 ist dann $\overline{G} \cong {}^{G}\!/_{\mathrm{Kern}(f)} =: {}^{G}\!/_{N}$. Man kann also nach jedem Normalteiler eine Faktorgruppe bilden.

Beweis Sei $\overline{G} := \{x \cdot N : x \in G\} (\subset \mathcal{P}(G))$
Für $x, y \in G$ setze $(x \cdot N)(y \cdot N) = (x \cdot y \cdot N)$

Behauptung: $(\overline{G}, \cdot)$ ist Gruppe.
(i) Die Verknüpfung ist wohldefiniert. (Unabhängig des Repräsentanten der Nebenklasse):
Seien $x, x', y, y' \in G$ mit $xN = x'N$, $yN = y'N$.
Dann gibt es $n, m \in N$: $x' = xn$, $y' = ym$.
$\implies x'y' = xnym$, da N Normalteiler gibt es es $n' \in N$ mit $ny = yn'$, also
$\implies x'y' = xyn'm \implies x'y'N = xyN$

(ii) alle übrigen Eigenschaften „vererben“ sich schon von G auf $\overline{G}$.
$f : G \to \overline{G}$, $x \mapsto xN$ ist surjektiver Gruppenhomomorphismus mit $\mathrm{Kern}(f) = N$.

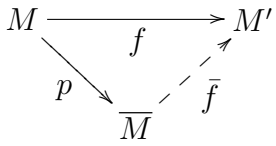
Satz 1 (Homomorphiesatz)

a) Sei $f : M \to M'$ Homomorphismus von $\left\{ \begin{array}{c} \text{Magma} \\ \text{Halbgruppe} \\ \text{Monoid} \\ \text{Gruppe} \end{array} \right\}$,
$\overline{M} := {}^{M}\!/_{\sim_f}$ heißt der Quotientenraum,
$p : M \to \overline{M}, x \mapsto \bar{x}$ die Restklassenabbildung.

(i) p ist surjektiver Homomorphismus.

(ii) Es gibt genau einen ($\exists!$) Homomorphismus $\bar{f} : \overline{M} \to M'$ mit $f = \bar{f} \circ p$

(iii) $\bar{f}$ ist injektiv. Ist f surjektiv $\implies$ $\bar{f}$ bijektiv.



b) (***Universelle Abbildungseigenschaft der Faktorgruppe***)
Sei G Gruppe, $N \subseteq G$ Normalteiler.
Dann gibt es zu jedem Gruppenhomomorphismus $f : G \to G'$ mit $N \subseteq \mathrm{Kern}(f)$
genau einen Gruppenhomomorphismus $\bar{f} : {}^{G}\!/_{N} \to G'$ mit $f = \bar{f} \circ p$

Beweis a) i) $\surd$

ii) Setze $\bar{f}(\bar{x}) := f(x)$. Dies ist die einzige Möglichkeit!
$\Longrightarrow$ $\bar{f}$ ist eindeutig (wenn es existiert)
$\bar{f}$ ist wohldefiniert: Ist $y \in \bar{x}$, also $y \sim_f x \Longrightarrow f(y) = f(x) \Longrightarrow \bar{f}(\bar{y}) = f(y) = f(x) = \bar{f}(\bar{x})$.
$\bar{f}$ ist Homomorphismus: $\bar{f}(\bar{x} \cdot \bar{y}) = f(x \cdot y) = f(x) \cdot f(y) = \bar{f}(\bar{x}) \cdot \bar{f}(\bar{y})$

iii) $\surd$ (aus nicht-injektiven wird eine Restklasse)

b) Setze $\bar{f}(xN) := f(x)$ Das ist eindeutig wie in a).
$\bar{f}$ wohldefiniert: Sei $y \in G$ mit $y \cdot N = x \cdot N$.
$\Longrightarrow$ $y = x \cdot n$ für ein $n \in N \subseteq \text{Kern}(f)$
$\Longrightarrow$ $f(y) = f(x \cdot n) = f(x) \cdot f(n) = f(x) \Longrightarrow$ $\bar{f}$ ist Homomorphismus.

1.4 Zyklische Gruppen

Definition und Bemerkung 1.16

Sei G Gruppe, $A \subseteq G$ Teilmenge.

a) $\langle A \rangle := \bigcap_{\substack{H \subseteq G \text{ Untergruppe} \\ A \subseteq H}} H$ heißt die von A erzeugte Untergruppe von G.

b) G heißt ***zyklisch***, wenn es ein $g \in G$ gibt mit $G = \langle g \rangle$

c) Für $g \in G$ ist $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$

d) Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z}/n\mathbb{Z}$ für genau ein $n \in \mathbb{N} \setminus \{0\}$

e) Jede Untergruppe einer zyklischen Untergruppe ist zyklisch.

f) Für $g \in G$ heißt $\text{ord}(g) := |\langle g \rangle|$ die ***Ordnung*** von g in G.
Es ist $\text{ord}(g) = \begin{cases} \min\{n \in \mathbb{N} \setminus \{0\} : g^n = e\} & \text{sonst} \\ \infty & g^n \neq e \forall n \in \mathbb{N} \setminus \{0\} \end{cases}$

g) Ist G endlich, so ist für alle $g \in G$: $\text{ord}(g)$ ein Teiler der Gruppenordnung

Beweis a) Zu zeigen: $\langle A \rangle := \bigcap_{\substack{H \subseteq G \text{ Untergruppe} \\ A \subseteq H}} H$ ist Untergruppe von G.

(i) $e \in H \forall H \subseteq G$, da H Untergruppe $\Longrightarrow$ $e \in \langle A \rangle \Longrightarrow$ $\langle A \rangle \neq \emptyset$.

(ii) Seien $x, y \in \langle A \rangle$, H Untergruppe von G mit $A \subseteq H$.
$\Longrightarrow$ $x, y \in H. \Longrightarrow$ $xy^{-1} \in H \Longrightarrow$ $xy^{-1} \in \langle A \rangle$

c) „$\supseteq$“ $\surd$
„$\subseteq$“: Nach 1.9 ist $\{g^n : n \in \mathbb{Z}\} = \text{Bild}(\varphi_g)$ Untergruppe von G (Eines der Untergruppen im Schnitt $\Longrightarrow$ Schnitt kann nicht größer als eines der Elemente sein).

d) Sei $G = \langle g \rangle$, $\varphi_g : \mathbb{Z} \to G, n \mapsto g^n$ (siehe 1.9)

φ_g ist surjektiver Gruppenhomomorphismus.
Nach Satz 1 ist $G \cong {}^{\mathbb{Z}}/_{\text{Kern}(\varphi_g)}$.

Da jede Untergruppe von $\mathbb{Z}$ von der Form $H = n \cdot \mathbb{Z}$ für $n \in \mathbb{N}_0 \Longrightarrow$ Behauptung.

e) Sei $G = \langle g \rangle$ zyklisch, $H \subseteq G$ Untergruppe,
$n := \min\{k \in \mathbb{N} \setminus \{0\} : g^k \in H\}$

Dann ist $\langle g^n \rangle \subseteq H$
Wäre $k \in H \setminus \langle g^n \rangle$, also $k = g^m$ mit $m \notin n\mathbb{Z}$
$\Longrightarrow d := \text{ggT}(m, n) < n$
Nach Euklid gibt es $a, b \in \mathbb{Z}$ mit $a \cdot m + b \cdot n = d$
$\Longrightarrow g^d = (g^m)^a \cdot (g^n)^b \in H$
Widerspruch zu n minimal mit $g^n \in H$

g) Folgt aus dem Satz von Lagrange (1.12 f)

Definition und Bemerkung 1.17

a) Die Abbildung $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N}, n \mapsto \varphi(n)$ mit
$\varphi(n) := |\{k \in \mathbb{N} : 1 \leq k \leq n : \text{ggT}(k, n) = 1\}|$
heißt ***Eulersche φ-Funktion***.

b) Ist G zyklische Gruppe der Ordnung n, so gilt für jeden Teiler d von n:
$|\{x \in G : \text{ord}(x) = d\}| = \varphi(d)$

c) Für jedes $n \in \mathbb{N} \setminus \{0\}$ gilt: $n = \sum_{d|n} \varphi(d)$

Beweis b) Sei $G = \langle g \rangle$. Für $x = g^k \in G$ ist $\text{ord}(x) = \dfrac{n}{\text{ggT}(k, n)}$.

Also ist $\text{ord}(x) = d \Longleftrightarrow ggT(k, n) = \dfrac{n}{d}$

Es ist $|\{k \in \mathbb{N} : 1 \leq k \leq n : \text{ggT}(k, n) = \dfrac{n}{d}\}|$
$= |\{l \in \mathbb{N} : 1 \leq l \leq d : \text{ggT}(l, d) = 1\}|$

denn: $k \mapsto \dfrac{k}{\frac{n}{d}}$

c) $n = |G| = \sum_{d|n} |\{x \in G : \text{ord}(x) = d\}| = \sum_{d|n} \varphi(d)$

Beispiele

1) $\left\{e^{\frac{2\pi ik}{n}} : n \in \mathbb{N} \setminus \{0\}, 0 \leq k \leq n\right\}$ ist zyklische Untergruppe von $(\mathbb{C}, \cdot)$ der Ordnung n.
(die n-te Einheitswurzeln)

2) Sei $V = \{id, \tau, \sigma_1, \sigma_2\}$ mit
$\tau =$ Drehung um 180 Grad im $\mathbb{R}^2 : \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$

σ_1 = Spiegelung an der x-Achse : $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$
σ_2 = Spiegelung an der y-Achse : $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$

V ist abelsche Gruppe, aber nicht zyklisch. V heißt ***Kleinsche Vierergruppe***.

$$V \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

3)

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$$

$$\{1, \sigma\} \oplus \{1, \tau, \tau^2\} \cong \{1, a, a^2, a^3, a^4, a^5\}$$

mit $a \mapsto (\sigma, \tau)$

1.5 Abelsche Gruppen

Definition und Bemerkung 1.18

Sei $(A, +)$ eine abelsche Gruppe, $X \subseteq A$.

a) A heißt ***freie abelsche Gruppe*** mit ***Basis*** X, wenn jedes $a \in A$ eine eindeutige Darstellung $a = \sum_{x \in X} n_x \cdot x$ hat mit $n_x \in \mathbb{Z}$ und $n_x \neq 0$ nur für endliche viele $x \in X$.

Ist in dieser Situation $|X| = n$, so heißt n der ***Rang*** von A. A ist isomorph zu $\mathbb{Z}^X := \bigoplus_{x \in X} \mathbb{Z}$

b) Universelle Abbildungseigenschaft der freien abelschen Gruppen.

Zu jeder abelschen Gruppe A und jeder Abbildung $f : X \to A$ gibt es genau einen Homomorphismus $\varphi : \mathbb{Z}^X \to A$ mit $\varphi(x) = f(x) \forall x \in X$.

Beweis a) $A \to \mathbb{Z}^X$, $\sum n_x x \mapsto (n_x)_{x \in X}$ ist Isomorphismus.

b) Setze $\varphi(\sum_{x \in X} n_x x) := \sum_{x \in X} n_x f(x)$. („bleibt nichts anderes übrig“).

Wichtigstes Beispiel X endliche Menge, $X = \{x_1, \dots x_n\}$.
Dann ist $\mathbb{Z}^X \cong \mathbb{Z}^n$

$\mathbb{Z}^n$ ist „so was ähnliches“ wie ein Vektorraum: heißt ***freier Modul***.
Insbesondere lassen sich die Gruppenhomomorphismen $\mathbb{Z}^n \to \mathbb{Z}^m$ durch eine n-m-Matrix mit Einträgen in $\mathbb{Z}$ beschreiben.

Satz 2 (Elementarteilersatz)

Sei H eine Untergruppe von $\mathbb{Z}^n$ $(n \in \mathbb{N} \setminus \{0\})$.
Dann gibt es eine Basis $\{x_1, \dots x_n\}$ von $\mathbb{Z}^n$, ein $r \in \mathbb{N}$ mit $0 \leq r \leq n$ und $a_1, \dots a_r \in \mathbb{N} \setminus \{0\}$ mit $a_i \mid a_{i+1}$ für $i = 1, \dots r-1$, so dass $a_1 x_1, \dots a_r x_r$ eine Basis von H ist.
Insbesondere ist H ebenfalls eine freie abelsche Gruppe.

Beweis 1. Schritt: Behauptung: H ist endlich erzeugt.

Induktion über n:

$n = 1$: $\surd$ ($\mathbb{Z}^1$ jede Untergruppe ist $n\mathbb{Z}$ für ein n).

$n > 1$: Sei $e_1, \dots e_x$ Basis von $\mathbb{Z}^n$, $\pi : \mathbb{Z}^n \to \mathbb{Z}$, $\sum_{i=1}^n a_i e_i \mapsto a_n$. („Projektion auf letzte Komponente“).

1. Fall: $\pi(H) = \{0\} \implies H \subseteq \mathbb{Z}^{n-1} \implies H$ endlich erzeugt.

2. Fall: $\pi(H) = l \cdot \mathbb{Z}$ für ein $l \in \mathbb{N} \setminus \{0\}$. (Bild von einem Gruppenhomomorphismus ist Gruppe)
Sei $y \in H$ mit $\pi(y) = l$

Behauptung: $H \cong \langle y \rangle \oplus (H \cap \mathrm{Kern}(\pi))$

Dann folgt die Behauptung von Schritt 1, da $\mathrm{Kern}(\pi) \cong \mathbb{Z}^{n-1}$, dann ist $H \cap \mathrm{Kern}(\pi)$ Untergruppe von $\mathbb{Z}^{n-1}$, also endlich erzeugt nach Induktionshypothese. $\implies H$ endlich erzeugt.

Beweis der Behauptung:
$\langle y \rangle \cap (H \cap \mathrm{Kern}(\pi)) = \{0\}$ nach Definition von y. $\implies$ Summe ist direkt.
Sei $z \in H$ mit $\pi(z) = k \cdot l$ für ein $k \in \mathbb{Z} \implies z - k \cdot y \in H \cap \mathrm{Kern}(\pi) \implies$ Behauptung.

2. Schritt: Sei $y_1, \dots y_r$ ein Erzeugendensystem von H. Nach Schritt 1 kann $r \leq n$ erreicht werden.

Schreibe $y_j = \sum_{i=1}^n a_{ij} e_i$. Dann ist $A := (a_{ij}) \in \mathbb{Z}^{n \times r}$ eine Darstellungsmatrix der Abbildung $H \hookrightarrow \mathbb{Z}^n$ bezüglich der Basen $\{y_1, \dots y_r\}$ von H und $\{e_1, \dots e_n\}$ von $\mathbb{Z}^n$.

Zeilen- und Spaltenumformungen entsprechen Basiswechseln in H bzw. $\mathbb{Z}^n$.
Vorsicht: dabei dürfen nur ***ganzzahlige*** Basiswechselmatrizen benutzt werden, deren inverse Matrix ebenfalls ganzzahlige Einträge hat!

Ziel: Bringe A durch elementare Zeilen- und Spaltenumformungen auf Diagonalgestalt:

$$\widetilde{A} := \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_r \end{pmatrix}$$

mit $a_i \in \mathbb{Z}$ und $a_i \mid a_{i+1} \forall i = 1 \dots r-1$

3. Schritt: Das geht! Ganzzahliger Gauß-Algorithmus:

i) Suche den betragsmäßig kleinsten Matrixeintrag $\neq 0$ und bringe den nach a_{11}. Dazu brauche ich höchstens eine Zeilen- und eine Spaltenvertauschung.

ii) Stelle fest ob alle a_{i1} $(i = 2 \dots n)$ durch a_{11} teilbar sind.

Falls nicht, teile a_{i1} mit Rest durch a_{11}:
$a_{i1} = q \cdot a_{11} + r$ mit $0 < r < |a_{11}|$
Dann ziehe von der i-ten Zeile das q-fache der ersten ab. Die neue i-te Zeile beginnt jetzt mit $\widetilde{a}_{i1} = r$. Zurück zu i).

iii) Sind schließlich alle a_{i1} durch a_{11} teilbar, so wird die erste Spalte zu $\begin{pmatrix} a_{11} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ gemacht,

indem man von der i-ten Zeile das $\dfrac{a_{i1}}{a_{11}}$-fache der ersten Zeile abzieht.

iv) Genauso wird die 1. Zeile zu $\begin{pmatrix} a_{11} & 0 & \cdots & 0 \end{pmatrix}$

v) Gibt es jetzt noch einen Matrixeintrag a_{ij} $(i,j \geq 2)$, der nicht durch a_{11} teilbar ist, schreibe $a_{ij} = q \cdot a_{11} + r$ mit $0 < r < |a_{11}|$. Ziehe von der i-ten Zeile das q-fache der ersten ab.

Die neue i-te Zeile lautet dann $\begin{pmatrix} -qa_{11} & a_{i2} & \cdots & a_{ij} & \cdots & a_{ir} \end{pmatrix}$ (da $a_{i1} = 0, a_{ik} = 0$ für $1 < k < r$).

Addiert man nun zur j-ten Spalte die erste, so ist das neue Element $\widetilde{a}_{ij} = a_{ij} - qa_{11} = r$.

Zurück zu (i)

vi) Nach endlich vielen Schritten, erhalte Matrix $\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}$, in der alle Einträge von A' durch a_{11} teilbar sind.

Wende nun (i)-(vi) auf A' an.

Ergänzung

1) In der Situation von Satz 2 heißen die a_{ii}, $i = 1, \ldots r$, ***Elementarteiler*** von H.

2) Ist $A = \begin{pmatrix} h_1 & \cdots & h_r \end{pmatrix} \in \mathbb{Z}^{n \times r}$, so erzeugen die Spalten $h_1, \ldots h_r$ eine Untergruppe von $\mathbb{Z}^n$. A ist die Darstellungsmatrix der Einbettung $H \hookrightarrow \mathbb{Z}^n$. Die Elementarteiler von H heißen auch Elementarteiler von A.

Satz 3 (Struktursatz für endlich erzeugte abelsche Gruppen)

Jede endlich erzeugbare abelsche Gruppe A ist isomorph zu einer direkten Summe von zyklischen Gruppen.
genauer: Es gibt $r, m \in \mathbb{N}$ und $a_1, \ldots a_m \in \mathbb{N}$, $a_i \geq 2 \forall i = 1 \ldots m$ und $a_i \mid a_{i+1}$ für $i = 1 \ldots m-1$, so dass gilt $A \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z}$, r, m und die a_i sind durch A eindeutig bestimmt.

Beweis Sei $x_1, \ldots x_n$ ein Erzeugendensystem von A. Nach 1.18 gibt es einen surjektiven Gruppenhomomorphismus $\varphi : \mathbb{Z}^n \to A$ mit $\varphi(x_i) = x_i$ $(i = 1 \ldots n)$. Nach dem Homomorphiesatz ist dann $A \cong \mathbb{Z}^n/\mathrm{Kern}(\varphi)$
Nach Satz 2 gibt es $m \in \mathbb{N}$, $m \leq n$, eine Basis $z_1, \ldots z_n$ von $\mathbb{Z}^n$ und Elementarteiler $a_1, \ldots a_n$ mit $a_i \mid a_{i+1}$, $i = 1 \ldots m-1$, so dass $a_1 z_1, \ldots a_m z_m$ Basis vom $\mathrm{Kern}(\varphi)$ ist.

Dann ist $A \cong \mathbb{Z}^n/\mathrm{Kern}(\varphi) \cong (\bigoplus_{i=1}^{n} z_i \cdot \mathbb{Z})/(\bigoplus_{i=1}^{m} z_i \cdot \mathbb{Z}) \cong (\bigoplus_{i=1}^{m} z_i \cdot \mathbb{Z})/a_i z_i \mathbb{Z} \oplus \bigoplus_{i=m+1}^{n} z_i\mathbb{Z}$

$\cong \bigoplus_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z} \oplus \mathbb{Z}^{n-m}$

Dabei sind r, m und die a_i eindeutig bestimmt. r ist die maximale Anzahl linear unabhängiger Elemente in A.

Sei also $T := \bigoplus_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z} \cong \bigoplus_{j=1}^{m'} \mathbb{Z}/b_j\mathbb{Z} =: T'$

Zu zeigen: $m' = m$ und $a_i = b_i$ $\forall i = 1 \ldots m$ mit $b_j \mid b_{j+1}$ für $j = 1 \ldots m-1$

Behauptung: Für jedes $x \in T$ ist ord(x) Teiler von a_m:
Genauso: Für jedes $y \in T'$ ist ord(y) Teiler von b_m.
T enthält ein Element von Ordnung a_m, nämlich $(\bar{0}, \dots \bar{0}, \bar{1}) \in T$.
$\Longrightarrow$ T' enthält auch ein Element von Ordnung $a_m \Longrightarrow a_m \mid b_{m'}$
Umgekehrt: $b_{m'}$ teilt $a_m \Longrightarrow a_m = b_{m'}$
Sei $\widetilde{T} := {}^{T}\!/_{(\mathbb{Z}/a_m\mathbb{Z})} \cong \bigoplus_{i=1}^{m-1} \mathbb{Z}/a_i\mathbb{Z}$, und da $\widetilde{T} = {}^{T}\!/_{(\mathbb{Z}/b_m\mathbb{Z})} \cong \bigoplus_{j=1}^{m-1} \mathbb{Z}/b_h\mathbb{Z}$
Induktion über m: Eindeutigkeit gilt für $\widetilde{T} \Longrightarrow$ Satz.
Beweis der Behauptung:
Sei $x = (x_1, x_2, \dots x_m) \in T$ mit $x_i \in \mathbb{Z}/a_i\mathbb{Z}$
$\Longrightarrow$ $a_m x = (a_m x_1, \dots a_m x_m) = (0, \dots 0)$ weil a_i Teiler von a_m ist.
$\Longrightarrow$ ord(x) ist Teiler von a_m.

Definition und Bemerkung 1.19

Verloren gegangen?

1.6 Freie Gruppen

Definition und Bemerkung 1.20

Sei F eine Gruppe und $X \subseteq F$

a) F heißt ***freie Gruppe mit Basis*** X, wenn jedes $y \in F$ eine eindeutige Darstellung $y = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ hat, in der

- $n \geq 0$ ($n = 0$ ist das „leere Wort“, es ist das neutrale Element in F).
- $x_i \in X$ für $i = 1 \dots n$
- $\varepsilon_i \in \{+1, -1\}$
- $x_{i+1}^{\varepsilon_{i+1}} \neq x_i^{-\varepsilon_i}$ für $i = 1 \dots n-1$

b) Ist F frei mit Basis X, so gilt für jedes $x \in X$: $x^{-1} \notin X$ und ord$(x) = \infty$.

c) $\mathbb{Z}$ ist frei mit Basis $\{1\}$ (oder $\{-1\}$)

d) Ist F frei mit Basis X und $|X| \geq 2$, so ist F nicht abelsch.

Beweis Seien $x_1, x_2 \in X, x_1 \neq x_2 \Longrightarrow x_1 x_2 x_1^{-1} x_2^{-1} \neq e$ „Kommutator“ $\Longrightarrow x_1 x_2 \neq x_2 x_1$

Satz 4

a) Zu jeder Menge X gibt es eine freie Gruppe $F(X)$ mit Basis X.

b) Zu jeder Gruppe G und jeder Abbildung $f : X \to G$ gibt es genau einen Gruppenhomomorphismus $\varphi : F(X) \to G$ mit $\varphi(x) = f(x)$ für alle $x \in X$.

c) Jede Gruppe ist Faktorgruppe einer freien Gruppe.

d) $F(X) \cong F(Y) \iff |X| = |Y|$ ($\iff X \cong Y$)

Beweis a) Sei $X^{\pm} = X \times \{\pm 1\}$ und $i : X^{\pm} \to X^{\pm}$ die Abbildung $i(x, \varepsilon) = (x, -\varepsilon)$. i ist bijektiv und $i^2 = id$.

Schreibweise: $(x, 1) =: x$ und $(x, -1) =: x^{-1}$. $\implies i(x) = x^{-1}$ und $i(x^{-1}) = x$

Ein Element $y = (x_1 \dots x_n) \in F^a(X^{\pm})$ (freie Worthalbgruppe) heißt reduziert, wenn $x_{\nu+1} \neq i(x_\nu)$ für $\nu = 1 \dots n-1$

Sei $F(X)$ die Menge der reduzierten Wörter in $F^a(X^{\pm})$

Definition: Zwei Wörter in $F^a(X^{\pm})$ heißen ***äquivalent***, wenn sie durch endliches Einfügen oder Streichen von Wörter der Form $(x, i(x))$, $x \in X^{\pm}$ auseinander hervorgehen.

Beispiel: $x_1 \sim x_1 x_2 x_2^{-1} \sim x_1 x_2 x_3^{-1} x_3 x_2^{-1}$.

Behauptung: In jeder Äquivalenzklasse gibt es genau ein reduziertes Wort.

Dann definiere Produkt auf $F(X)$:
$(x_1 \dots x_n) * (y_1 \dots y_n)$ sei *das* reduzierte Wort in der Äquivalenzklasse von $(x_1 \dots x_n y_1 \dots y_n)$.

Dieses Produkt ist assoziativ: Für $x, y, z \in F(X)$ ist $(x * y) * z$ das eindeutig bestimmte reduzierte Wort in der Klassen von $(x_1 \dots x_n y_1 \dots y_n z_1 \dots z_n)$. Das gleiche gilt für $x*(y*z)$.

Neutrales Element: $e = ()$.

Inverse Element zu $(x_1 \dots x_n)$ ist $(i(x_1) \dots i(x_n))$

$\implies F(X)$ ist Gruppe.

$F(X)$ ist freie Gruppe mit Basis X nach Konstruktion.

Beweis der Behauptung: In jeder Klasse gibt es ein reduziertes Wort.

Eindeutigkeit: Seien x, y reduziert und äquivalent. Dann gibt es ein Wort w, aus dem sowohl x als auch y durch Streichen hervorgeht.

Zu zeigen also: Jede Reihenfolge von Streichen in w führt zum selben reduzierten Wort.

Induktion über die Länge $l(w)$

I.A.: $l(w) = 0\surd$, $l(w) = 1\surd$.

I.S.: Sei $l(w) \geq 2$:

- Ist w reduziert, so ....
- Enthält w genau ein Paar $(x_\nu, i(x_\nu))$, so muss das als erstes gestrichen werden.
  Es entsteht w' mit $l(w') = l(w) - 2 \overset{\text{I. Vor}}{\implies}$ Behauptung.
- Enthält w Paare $(x_\nu, i(x_\nu))$ und $(x_\mu, i(x_\mu))$, so gibt es 2 Fälle:
  $(x_\nu, i(x_\nu), x_\nu)$ dann führen beide Streichungen zum selben Wort. Ohne Einschränkung sei $\mu > \nu$

  Fall $\mu = \nu + 1$: $(x_\nu, i(x_\nu), x_\nu)$
  dann führen beide Streichungen zum selben Wort.

  Fall $\mu \geq \nu+2$: Streiche beide Paare, erhalte w' mit $l(w'') = l(w)-4 \implies$ Behauptung.

b) $\varphi(x_1 \dots x_n) := \widetilde{f}(x_1) \cdot \widetilde{f}(x_2) \cdots \widetilde{f}(x_n)$

mit $\widetilde{f}(x_i) = \begin{cases} f(x_i) & x_i \in X \\ f(x_i^{-1})^{-1} & x_i \in X^- := \{(x, -1) \in X^{\pm}\} \end{cases}$

(Existenz und Eindeutigkeit gezeigt)

c) Sei $S \subseteq G$ ein Erzeugendensystem. (d.h. die einzige Untergruppe H von G mit $S \subseteq H$ ist G selbst)

Sei $F(S)$ die freie Gruppe mit Basis S, $f : S \to G$ die Identität und $\varphi : F(S) \to G$ der Homomorphismus aus b).

φ ist surjektiv, weil $\varphi(F(S))$ Untergruppe ist, die S enthält.

Also ist nach Homomorphiesatz $G \cong {}^{F(S)}\!/_{\mathrm{Kern}(\varphi)}$

d) „$\Leftarrow$“: Sei $f : X \to Y$ bijektive Abbildung.

Dazu gibt es Gruppenhomomorphismen $\varphi_f : F(X) \to F(Y)$ und $\varphi_{f^{-1}} : F(X) \to F(Y)$.

Wegen b):
$(\varphi_f \circ \varphi_{f^{-1}})|_Y = id_Y$ und $(\varphi_{f^{-1}} \circ \varphi_f)|_X = id_X$ und $id_{F(Y)}|_Y = id_Y$
$\xRightarrow{\text{Eindeutigkeit in b)}} \varphi_f \circ \varphi_{f^{-1}} = id_{F(Y)}$

genauso: $\varphi_{f^{-1}} \circ \varphi_f = id_{F(X)}$

(Erklärung: Es gibt hier 2 Abbildungen $F \to F$: $(\varphi_f \circ \varphi_{f^{-1}})$ und $id_{F(Y)}$. Diese werden beide durch f induziert, sind also gleich)

„$\Rightarrow$“: Sei $|X| \neq |Y|$

Die Anzahl der Gruppenhomomorphismen von $F(X)$ in ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ ist gleich der Anzahl der Abbildungen von X nach ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ (wegen b).

Diese ist $|({}^{\mathbb{Z}}\!/_{2\mathbb{Z}})^X| = 2^{|X|} \neq 2^{|Y|}$

1.7 Kategorien und Funktoren

Definition 1.21

Eine ***Kategorie*** $\mathcal{C}$ besteht aus einer Klasse $\mathrm{Ob}\,\mathcal{C}$ von ***Objekten*** und für je zwei $A, B \in \mathrm{Ob}\,\mathcal{C}$ aus einer Menge $\mathrm{Mor}_{\mathcal{C}}(A, B)$ von ***Morphismen*** von A nach B, für die folgende Eigenschaften erfüllt sind:

(i) Für jedes $A \in \mathrm{Ob}\,\mathcal{C}$ ein Element $id_A \in \mathrm{Mor}_{\mathcal{C}}(A, A)$

(ii) Für je 3 Objekte A, B, C gibt es eine Abbildung:

$$\begin{array}{rccccc} \circ : & \mathrm{Mor}(B,C) & \times & \mathrm{Mor}(A,B) & \to & \mathrm{Mor}(A,C) \\ & (g & , & h) & \mapsto & g \circ f \end{array}$$

$$\begin{array}{rcl} & g \circ id_A = g & \text{für alle } g \in \mathrm{Mor}(A,B) \\ \text{mit} & id_B \circ g = g & \text{für alle } g \in \mathrm{Mor}(A,B) \\ & (h \circ g) \circ f = h \circ (g \circ f) & \text{für alle } f, g, h... \end{array}$$

Beispiele

1. Mengen mit Abbildungen
2. Mengen mit bijektiven Abbildungen (gibt viele leere $\mathrm{Mor}(A, B)$)
3. K-Vektorraum mit K-linearen Abbildungen

4. Halbgruppen mit Homomorphismen
5. Monoide mit Homomorphismen
6. Magma mit Homomorphismen
7. Gruppen mit Homomorphismen
8. abelsche Gruppen mit Homomorphismen
9. topologische Räume mit stetigen Abbildungen

Definition 1.22

Seien $\mathcal{A}$ und $\mathcal{B}$ Kategorien.

a) Ein (***kovarianter***) ***Funktor*** $F : \mathcal{A} \to \mathcal{B}$
besteht aus einer Abbildung

$$F : \mathrm{Ob}(\mathcal{A}) \to \mathrm{Ob}(\mathcal{B})$$

sowie für je 2 Objekte $X, Y \in \mathrm{Ob}(\mathcal{A})$ aus einer Abbildung

$$F : \mathrm{Mor}_{\mathcal{A}}(X, Y) \to \mathrm{Mor}_{\mathcal{B}}(F(X), F(Y))$$

so dass gilt:

(i) $F(id_X) = id_{F(X)}$ für alle $X \in \mathrm{Ob}(\mathcal{A})$
(ii) $F(g \circ f) = F(g) \circ F(f)$ für alle $f \in \mathrm{Mor}_{\mathcal{A}}(X, Y)$, $g \in \mathrm{Mor}_{\mathcal{A}}(Y, Z)$

b) Ein ***kontravarianter Funktor*** $F : \mathcal{A} \to \mathcal{B}$

$$F : \mathrm{Mor}_{\mathcal{A}}(X, Y) \to \mathrm{Mor}_{\mathcal{B}}(F(Y), F(X))$$

und

$$F(g \circ f) = F(f) \circ F(g)$$

Verdeutlichung:

$$\begin{array}{ccccc} X & \xrightarrow{f} & Y & \xrightarrow{g} & Z \\ F(X) & \xleftarrow{F(f)} & F(Y) & \xleftarrow{F(g)} & F(Z) \end{array}$$

Beispiele

1. $\begin{array}{ccc} \text{Gruppen} & \to & \text{Mengen} \\ (G, \cdot) & \mapsto & G \end{array}$ genannt: „Vergiss-Funktor“

2. $\mathcal{P} : \text{Menge} \to \text{Menge}$, $X \mapsto \mathcal{P}(X)$ (Potenzmenge).
Für $f : X \to Y$ sei $\mathcal{P}(f) : \begin{array}{ccc} \mathcal{P}(X) & \to & \mathcal{P}(Y) \\ \mathcal{U} & \mapsto & f(\mathcal{U}) \end{array}$

3. Sei $\mathcal{C}$ Kategorie, X ein Objekt in $\mathcal{C}$

   Definiere Funktoren $\mathcal{C} \to$ Mengen durch

$$\begin{array}{lll} \mathrm{Hom}(X,\cdot): & Y \mapsto & \mathrm{Mor}_{\mathcal{C}}(X,Y) \quad \text{kovariant} \\ \mathrm{Hom}(\cdot,X): & Y \mapsto & \mathrm{Mor}_{\mathcal{C}}(Y,X) \quad \text{kontravariant} \end{array}$$

   Für $f: Y \to Z$ ist $\mathrm{Hom}(X,\cdot)(f): \mathrm{Mor}(X,Y) \to \mathrm{Mor}(X,Z)$ gegeben durch $g \mapsto f \circ g$ und $\mathrm{Hom}(\cdot,X)(f): \mathrm{Mor}(Z,X) \to \mathrm{Mor}(Y,X)$, $g \mapsto g \circ f$.

4. Sei X Menge.

$$\begin{array}{lllll} F_X: & \text{Gruppen} & \to & \text{Menge} \\ & G & \mapsto & \mathrm{Abb}(X,G) = \mathrm{Mor}_{\text{Mengen}}(X,G) \end{array}$$

   Für jedes $f: X \to G$ gibt es $\varphi: F(X) \to G$ (Satz 4)
   also Bijektion $\alpha_G: F_X(G) \to \mathrm{Hom}_{\text{Gruppen}}(F(X),G)$

   („Vertragen sich mit den jeweiligen Gruppenhomomorphismen“.)

   $\varphi: G \to G'$ Homomorphismus.

1.8 Gruppenaktionen und die Sätze von Sylow

Definition und Bemerkung 1.23

Sei G eine Gruppe, X eine Menge.

a) Eine ***Aktion*** (Wirkung) von G auf X ist ein Gruppenhomomorphismus $\rho: G \to \mathrm{Perm}(X)$.
   G ***operiert*** auf X.

b) Die Aktionen von G auf X entsprechen bijektiv den Abbildungen

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

   für die gilt:

$$\begin{array}{lll} \text{(i)} & e \cdot x = x & \forall x \in X \\ \text{(ii)} & (g_1 g_2)x = g_1(g_2 x) & \forall g_1, g_2 \in G, x \in X \end{array}$$

   Beweis $g \cdot x = \rho(g)(x)$ gibt die gewünschte Bijektion.

   Beispiele

   1) $G \times G \to G$, $(g_1, g_2) \mapsto g_1 \cdot g_2$ („Linksmultiplikation“)
   2) $G \times G \to G$, $(g,h) \mapsto g \cdot h \cdot g^{-1}$ („Konjugation“) $[\rho(g) = c_g]$
   3) S_n operiert auf X^n (X eine Menge) durch Vertauschen der Komponenten.
      $\sigma(x_1, \ldots x_n) = (x_{\sigma(1)}, \ldots x_{\sigma(n)})$

c) Eine Aktion $\rho: G \to \mathrm{Perm}(X)$ heißt ***effektiv*** (oder ***treu***), wenn $\mathrm{Kern}(\rho) = \{e\}$.
   Allgemein heißt $\mathrm{Kern}(\rho)$ ***Ineffektivitätskern*** der Aktion.

Beispiele

1) ist effektiv.
2) Der Ineffektivitätskern ist das Zentrum $Z(G)$
3) auch effektiv, wenn $|X| \geq 2$

d) Für $x \in X$ heißt $G \cdot x = \{gx : g \in G\}$ die ***Bahn*** von x unter G.

e) X ist disjunkte Vereinigung von G-Bahnen.

Beweis Ist $y \in G \cdot x$, so ist $G \cdot y = G \cdot x$,
denn $\begin{matrix} y = gx \\ g^{-1}y = x \end{matrix} \implies \begin{matrix} h \cdot x = h \cdot g \cdot x \\ hg^{-1}y = hx \end{matrix} \in G \cdot x \quad \forall h \in G$

f) Für $x \in X$ heißt $G_x = \{g \in G : g \cdot x = x\}$ die ***Fixgruppe*** von x unter G (oder ***Stabilisator*** oder ***Isotropiegruppe***)

g) Für $x \in X$ und $g \in G$ ist
$$G_{gx} = g \cdot G_x \cdot g^{-1}$$

Beweis Für $h \in G$ gilt:
$h \in G_{gx} \iff h \cdot (g \cdot x) = g \cdot x \iff g^{-1}hgx = x \iff g^{-1}hh \in G_x$

Proposition 1.24 (Bahnbilanz)

Sei X endliche Menge, G Gruppe, die auf X operiert.
Sei $x_1, \dots x_r$ ein Vertretersystem der G-Bahnen in X. (d.h. aus jeder G-Bahn genau ein Element.)
Dann gilt:
$$|X| = \sum_{i=1}^{r} [G : G_{x_i}]$$

Beweis Nach 1.23 e) ist $|X| = \sum_{i=1}^{r} |G \cdot x_i|$
Zu zeigen also: $|G \cdot x_i| = [G : G_{x_i}]$
Behauptung: $\alpha_i : \{\text{Nebenklassen bzgl. } G_{\nu_i}\} \to G_{x_i}$, $g \cdot G_{x_i} \mapsto g \cdot x_i$
ist bijektive Abbildung, denn α_i ist wohldefiniert:
Ist $h = g \cdot g_1 \in g \cdot G_{x_i}$, so ist $h \cdot x_i = (g \cdot g_1)x_i = g \cdot x_i$ offensichtlich injektiv und surjektiv.

Satz 5 (Sätze von Sylow)

Sei G eine endliche Gruppe, $|G| = n$, p eine Primzahl.
Sei $n = p^k \cdot m$ mit $k \geq 0$ und $\text{ggT}(m, p) = 1$
Dann gilt:

a) G enthält eine Untergruppe S der Ordnung p^k.

Jede solche Untergruppe heißt p-Sylowgruppe von G.

b) je zwei p-Sylowgruppen sind konjugiert.

c) Die Anzahl s_p der p-Sylowgruppen in G erfüllt: $s_p \mid m$ und $s_p \equiv 1 \mod p$

Beweis a) $k = 0 \surd$

Sei also $k \geq 1$:

a) Sei $\mathcal{M} = \{M \subseteq G : |M| = p^k\} \subset \mathcal{P}(G)$

Es ist $|M| = \binom{n}{p^k} = \binom{p^k \cdot m}{p^k}$

Behauptung 1: $p \nmid |\mathcal{M}|$

G operiert auf $\mathcal{M}$ durch Linksmultiplikation $g \cdot M = \{g \cdot x : x \in M\} \in \mathcal{M}$
$\Longrightarrow$ $|\mathcal{M}|$ ist Summe von Bahnlängen.

Wegen Behauptung 1 gibt es eine Bahn $G \cdot M_0$ mit $p \nmid |G \cdot M_0|$

$\overset{1.24}{\Longrightarrow} |G \cdot M_0| = [G \cdot G_{M_0}] = \dfrac{|G|}{|G_{M_0}|}$

$\Longrightarrow$ p^k teilt $|G_{M_0}|$

Andererseits ist $|G_{M_0}| \leq p^k = |M_0|$, denn für $x \in M_0$ ist $g \mapsto g \cdot x$ injektive Abbildung $G_{n_0} \to M_0$

$\Longrightarrow$ $|G_{M_0}| = p^k$, d.h. G_{M_0} ist p-Sylowgruppe.

Beweis von Behauptung 1:

$$\binom{p^k \cdot m}{p^k} = \prod_{i=0}^{p^k-1} \frac{p^k \cdot m - i}{p^k - i},$$

schreibe jedes i in der Form $p^{\nu_i} \cdot m_i$ und $p \nmid m_i$ $(0 \leq \nu_i < k)$

$\Longrightarrow$ $\dfrac{p^k \cdot m - i}{p^k - i} = \dfrac{m \cdot p^{k \cdot \nu_i} - m_i}{p^{k \cdot \nu_i} - m_i}$

$\Longrightarrow$ weder Zähler noch Nenner ist durch p teilbar.

$\Longrightarrow$ Behauptung

b) Sei $S \subset G$ p-Sylowgruppe

$$\mathcal{S} := \{S' \subset G : S' = gSg^{-1} \text{ für ein } g \in G\}$$

Behauptung 2: $p \nmid |\mathcal{S}|$

Beweis 2:

G operiert auch auf $\mathcal{S}$ durch Konjugation. Diese Aktion ist transitiv, d.h. es gibt nur eine Bahn.

Die Fixgruppe von S' unter dieser Aktion ist

$$N_{S'} := \{g \in G : gS'g^{-1} = S'\}$$

$N_{S'}$ heißt der ***Normalisator*** von S' in G. (S' ist Normalteiler in $N_{S'}$ und maximal mit dieser Eigenschaft.)

$\implies |\mathcal{S}| = [G : N_S] = \dfrac{|G|}{|N_S|} = \dfrac{p^k \cdot m}{|N_S|}$

S ist Untergruppe von $N_S \implies p^k \mid |N_S| \implies |\mathcal{S}|$ ist Teiler von m.

Sei $\widetilde{S}$ eine p-Sylowgruppe in G.

Zu zeigen: $\widetilde{S} \in \mathcal{S}$

$\widetilde{S}$ operiert auf $\mathcal{S}$ (da $\widetilde{S} \subset G$)

Sei $S_1, \dots S_r$ ein Vertretersystem der Bahnen.

$\implies |\mathcal{S}| = \sum_{i=1}^{r} [\widetilde{S} : \widetilde{S}_{S_i}] = \sum_{i=1}^{r} \dfrac{p^k}{|\widetilde{S}_{S_i}|}$

Aus Behauptung 2 folgt: es gibt ein i mit $|\widetilde{S}_{S_i}| = p^k \implies \widetilde{S} = \widetilde{S}_{S_i}$.

Dann ist $\widetilde{S} \subset N_{S_i}$

Behauptung 3: Dann ist $\widetilde{S} \subseteq S_i$ (also $\widetilde{S} = S_i$, da beide p^k Elemente haben.)

Beweis 3: S_i ist Normalteiler in N_{S_i}, $\widetilde{S}$ ist Untergruppe in N_{S_i}.

$\implies \widetilde{S} \cdot S_i$ ist Untergruppe von N_{S_i} (ü 4 A 1)

Wäre $\widetilde{S} \not\subseteq S_i$, dann wäre $\widetilde{S} \cdot S_i \supsetneq S_i$ also $|\widetilde{S} \cdot S_i| = p^k \cdot d$ mit $d > 1$ (und $p \nmid d$)

$\xrightarrow{\text{ü 4 A 1}} \widetilde{S}S_i/S_i \cong \widetilde{S}/(\widetilde{S} \cap S_i)$

$\implies (p^k \cdot d =) \ |\widetilde{S} \cdot S_i| = \dfrac{|S_i| \cdot |\widetilde{S}|}{|\widetilde{S} \cap S_i|} = \dfrac{p^2 k}{|\widetilde{S} \cap S_i|} = p^l$ für ein l. Widerspruch.

c) $s_p = |\mathcal{S}| \implies s_p \mid m$

und $|\mathcal{S}| = \sum_{i=1}^{r} [\widetilde{S} : \widetilde{S}_{S_i}]$

da $[\widetilde{S} : \widetilde{S}_{S_i}] = 1 \iff \widetilde{S} = \widetilde{S}_{S_i} \overset{\text{Beh 3}}{\iff} \widetilde{S} = S_i$, also genau <u>einmal</u>.

Alle anderen Summanden sind durch p teilbar.

Folgerung 1.25

Ist G eine endliche Gruppe und p Primzahl, die $|G|$ teilt, so enthält G ein Element von Ordnung p.

Beweis Sei $|G| = p^k \cdot m$ mit $p \nmid m$, $k \geq 1$.
$S \subseteq G$ eine p-Sylowgruppe und $x \in S$, $x \neq e$
$\xrightarrow{\text{Lagrange}}$ ord(x) ist Teiler von $|S| = p^k$
$\implies$ ord$(X) = p^d$ für ein d mit $1 \leq d \leq k$.
$\implies x^{p^{d-1}}$ hat Ordnung p.

Beispiel $G = A_5$ hat 60 Elemente, z.B. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ hat Ordnung 5.

konjugiert dazu $\begin{pmatrix} 1 & 3 & 2 & 4 & 5 \end{pmatrix}$. $\xrightarrow{\text{(c)}}$ 6 Gruppen mit 5 Elementen.

1.9 Kompositionsreihen

Vorüberlegungen G Gruppe, $N \trianglelefteq G$ Normalteiler, G/N die Faktorgruppe.
Frage: Lässt sich G aus N und G/N rekonstruieren?
Schreibweise: $1 \to N \to G \to G/N \to 1$ ist exakt

Definition 1.26

Sei

$$\ldots \to G_{i-1} \xrightarrow{\alpha_{i-1}} G_i \xrightarrow{\alpha_i} G_{i+1} \to \ldots$$

eine Sequenz von Gruppen und Gruppenhomomorphismen.
Sie heißt ***exakt*** an der Stelle i, wenn der $\mathrm{Kern}(\alpha_i) = \mathrm{Bild}(\alpha_{i-1})$ ist.

Beispiele

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

sind exakt.
Die Aufgabe, Gruppen zu klassifizieren, zerlegt sich damit in 2 Teilaufgaben:

1) Gegeben N und G/N, welche Möglichkeiten gibt es für G?
2) Welche „unzerlegbaren“ Gruppen gibt es?

Definition 1.27

Sei G eine Gruppe

a) G heißt ***einfach***, wenn G nur die trivialen Normalteiler G und $\{e\}$ besitzt.

b) Eine Reihe der Form $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{e\}$ (für ein $n \in \mathbb{N}$)
heißt ***Normalreihe***, wenn G_{i+1} Normalteiler in G_i ist (für $i = 0 \ldots n-1$) und $G_{i+1} \neq G_i$.

c) Eine Normalreihe heißt ***Kompositionsreihe***, wenn sie sich nicht verfeinern lässt, d.h. wenn G_i/G_{i+1} einfach ist für $i = 0 \ldots n-1$.

Bemerkung 1.28

a) $\mathbb{Z}/m\mathbb{Z}$ ist einfach $\iff$ m ist Primzahl.

b) $\mathbb{Z}$ besitzt keine Kompositionsreihe.

c) Eine abelsche Gruppe G ist einfach $\iff$ $G \cong \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p.

d) Jede endliche Gruppe besitzt eine Kompositionsreihe

e) G endlich mit einer Normalreihe wie in Def 1.27, so gilt

$$|G| = \prod_{i=0}^{n-1} \left| \frac{G_i}{G_{i-1}} \right|$$

Proposition 1.29

Für $n \neq 4$ ist A_n einfach.

$|A_4| = 12$. A_4 enthält 8 Dreizyklen und 3 Doppelzweier.

A_4 ist auch die Symmetriegruppe des Tetraeders!

Beweis Behauptung 1: Jedes $\sigma \in A_n$ ist als Produkt von 3-Zyklen darstellbar.

denn: $\begin{array}{lcl} (1\ 2)(2\ 3) & = & (1\ 2\ 3) \\ (1\ 2)(3\ 4) & = & (1\ 2\ 3)(2\ 3\ 4) \end{array}$

Behauptung 2: Je zwei 3-Zyklen in A_n sind konjugiert in A_n

denn: Zu zeigen: $(i\ j\ k)$ ist zu $(1\ 2\ 3)$ konjugiert. 1. Fall: $(i\ j\ k) = (1\ 3\ 2)$ Sei $\tilde{p} = (2\ 3) = \tilde{p}^{-1}$ $\Longrightarrow$ $\tilde{p}^{-1}(1\ 3\ 2)\tilde{p} = (1\ 2\ 3)$

aber $\tilde{p} \notin A_n$

Rettung: $p = (2\ 3)(4\ 5) \Longrightarrow p^{-1}(1\ 3\ 2)p = (1\ 2\ 3)$

Behauptung 3: Enthält N einen „Doppelzweier“, so ist $N = A_n$ (N Normalteiler in A_n)

denn: Sei $\sigma = (1\ 2)(3\ 4) \in N, \tau = (1\ 2)(3\ 5)$
Dann ist $\sigma(\tau\sigma\tau^{-1}) = (1)(2)(3\ 4\ 5) \in N$

Behauptung 4: N enthält einen 3-Zyklus oder einen Doppelzweier.

Beweis 4: Genügt zu zeigen: N enthält ein $\sigma \neq id$ mit $\sigma(i) \neq i$ für höchstens 4 verschiedene $i \in \{1, \dots n\}$.

Für jedes $\sigma \in A_n$ sei $k_\sigma := |\{i \in \{1, \dots n\} : \sigma(i) \neq i\}|$

Sei $\sigma \in N \setminus \{id\}$ mit minimal k_σ.

Annahme: $k_\sigma \geq 5$:

1. Fall: σ enthält einen Zyklus der Länge ≥ 3.

Ohne Einschränkung sei $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(4) \neq 4$, $\sigma(5) \neq 5$.

Sei $\alpha := \sigma^{-1}(3\ 4\ 5)\sigma(3\ 5\ 4)$

Für alle i mit $\sigma(i) = i$ ist $\alpha(i) = i \Longrightarrow k_\alpha \leq k_\sigma$

Außerdem ist $\alpha(1) = 1 \Longrightarrow k_\alpha < k_\sigma$. Widerspruch!

2. Fall: σ ist Produkt von disjunkten Transpositionen (mindestens 4).

Ohne Einschränkung sei $\sigma = (1\ 2)(3\ 4)(5\ 6)(7\ 8)\widetilde{\sigma}$
mit $\widetilde{\sigma} \in A_n$, $\widetilde{\sigma}(i) = i$ für $i = 1, \dots 8$.

$\alpha = \sigma^{-1}(3\ 4\ 5)\sigma(3\ 5\ 4)$ erfüllt $\alpha(i) = i$ falls $\sigma(i) = i$, und $\alpha(1) = 1$

$\Longrightarrow k_\alpha < k_\sigma \Longrightarrow$ Widerspruch.

Satz 6 (Satz von Jordan-Hölder)

Sei G eine Gruppe,

$$\begin{array}{rl} G = & G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_m = \{1\} \\ & H_0 \triangleright H_1 \triangleright H_2 \triangleright \cdots \triangleright H_l = \{1\} \end{array}$$

Kompositionsreihe für G.
Dann ist $m = l$ und es gibt eine Permutation $\sigma \in S_m$ mit

$$G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}$$

mit $i = 0, \dots m-1$

Beweis Induktion über m:

$m = 1$ Dann ist G einfach, also auch $l = 1$.

$m > 1$ Sei $\overline{G} = G/G_1$, $\pi : G \to \overline{G}$ die Restklassenabbildung. $\Longrightarrow$ $\overline{H_i} = \pi(H_i)$ ist Normalteiler in $\overline{H_{i-1}}$ (sei $\pi(h_i) = \overline{h_i} \in \overline{H_i}$, $\pi(g) = \overline{g} \in \overline{H_{i-1}} \Longrightarrow \overline{g}\overline{h_i}\overline{g}^{-1} = \pi(gh_ig^{-1}) \in \overline{H_i}$)
Nach Voraussetzung ist $\overline{G}$ einfach $\Longrightarrow$ $\exists j \in \{0, \dots l-1\}$ mit

$$\overline{H_0} = \dots = \overline{H_j} = \overline{G}, \overline{H_{j+1}} = \dots \overline{H_l} = \{1\}$$

Sei $C_i := H_i \cap G_1$
Behauptung 1: $G_1 = C_0 \triangleright C_1 \triangleright \dots \triangleright C_j \triangleright C_{j+2} \triangleright \dots \triangleright C_l = \{1\}$ ist Kompositionsreihe für G_1.
Dann: $G_1 \triangleright G_2 \triangleright \dots \triangleright G_m = \{1\}$ ist auch Kompositionsreihe.
$\overset{\text{Ind. Vor.}}{\Longrightarrow} m - 1 = l - 1$ und es gibt $\sigma : \{1, \dots m\} \to \{0, \dots j, j+2, \dots l\}$ bijektiv mit
$C_{i-1}/C_i \cong G_{\sigma(i)-1}/G_{\sigma(i)}$ für $i \neq j+1$ und $C_j/C_{j+2} \cong G_\sigma(j)/G_{\sigma(j)+1}$.
Behauptung 2:

a) $C_j = C_{j+1}$
b) $C_{i-1}/C_i \cong H_{i-1}/H_i$ für $i \neq j+1$
c) $H_j/H_{j+1} \cong G/G_1 = \overline{G}$

Behauptung 1 folgt aus Behauptung 2:
C_i ist Normalteiler in C_{i-1}: $x \in C_i = H_i \cap G_1$, $y \in H_{i-1} \cap G_1 \Longrightarrow yxy^{-1} \in H_i \cap G_1$ für $i = 1, \dots l$.
C_{j+2} ist Normalteiler in C_j wegen 2a).
C_{i-1}/C_i ist wegen 2b) einfach und $\neq \{1\}$ $(i \neq j+1)$

Beweis (Beweis von Behauptung 2) a) $\overline{H_{j+1}} = \{1\}$ d.h. $H_{j+1} \subseteq G_1 \Longrightarrow C_{j+1} = H_{j+1}$
$C_j = H_j \cap G_1$ ist Normalteiler in H_j (weil G_1 Normalteiler in H_j)
Da $\overline{H_j} \neq \{1\}$, ist $C_j \neq H_j$
$\Longrightarrow$ $H_{j+1} \trianglelefteq C_j \not\trianglelefteq J_{j+1}$
$H_i/H_k \overset{\text{einfach}}{\Longrightarrow} C_j = H_{j+1} = C_{j+1}$

b) Für $i > j+1$ ist $\overline{H_i} = \{1\}$, also $H_i \subset G_i$, und damit $C_i = H_i$
Für $i \leq j$ ist $\overline{H_i} = \overline{G} = G/G_1$
$\Longrightarrow$ $H_iH_1 = G_1H_i = G$
$C_{i-1}/C_i = C_{i-1}/H_i \cap C_{i-1} \cong C_{i-1}/H_i$

Zu zeigen also: $C_{i-1}H_i = H_{i-1}$
denn: „$\subseteq$“ $\surd$
„$\supseteq$“: Da $G_1H_i = G$ ist, gibt es zu $x \in H_{i-1}$ ein $h \in H_i$ und ein $g \in G_1$ mit $x = gh$
$\Longrightarrow\ g = x \cdot h^{-1} \in H_{i-1} \cap G_1 = C_{i-1}$

c) $H_{j+1} \leq G_1$ ($\leq$: ist Untergruppe)
$\Longrightarrow\ {}^{H_j}\!/_{H_{j+1}} = {}^{H_i}\!/_{C_{j+1}} \overset{\text{a)}}{=\!=} {}^{H_j}\!/_{C_j} \cong {}^{H_j}\!/_{H_j \cap G_1} = {}^{H_jG_1}\!/_{G_1} = {}^{G}\!/_{G_1}$

Definition und Bemerkung 1.30

a) Eine Gruppe G heißt ***auflösbar***, wenn sie eine Normalreihe mit abelschen Faktorgruppen besitzt.

b) Eine endliche Gruppe ist genau dann auflösbar, wenn die Faktoren in ihrer Kompositionsreihe zyklisch von Primzahlordnung ist.

c) Sei $1 \to G' \to G \to G'' \to 1$ kurze exakte Sequenz von Gruppen.
Dann gilt: G ist auflösbar $\Longleftrightarrow$ G' und G'' auflösbar sind.

Kapitel 2

Ringe

2.1 Grundlegende Definitionen und Eigenschaften

Definition und Bemerkung 2.1

a) Ein ***Ring*** ist eine Menge R mit Verknüpfungen $+$ und $\cdot$, so dass gilt:

(i) $(R, +)$ ist kommutative Gruppe.

(ii) $(R, \cdot)$ ist Halbgrupppe.

(iii) die Distributivgesetze gelten:

$$\begin{array}{rcl} x \cdot (y+z) & = & xy + xz \\ (x+y) \cdot z & = & xz + yz \end{array} \quad \text{für alle } x, y, z \in R$$

b) R heißt ***Ring mit Eins*** , wenn $(R, \cdot)$ Monoid ist.

c) R heißt ***kommutativer Ring***, wenn $(R, \cdot)$ kommutativ ist.

d) R heißt ***Schiefkörper***, wenn $R^\times = R \setminus \{0\}$, d.h. wenn jedes $x \in R \setminus \{0\}$ invertierbar ist bzgl $\cdot$.

e) Ein kommutativer Schiefkörper heißt ***Körper***.

Beispiele [Ring ohne Eins: $(\mathbb{Z}, +, \cdot')$ mit $\cdot'$ nur auf $\mathbb{Z}/7\mathbb{Z}$]

$H := \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$

mit komponentenweiser Addition und folgender Multiplikation : $i^2 = -1 = j^2 = k^2$, $ij = k = -ji$.

(z.B ist dann $ik = iij = -j$, $kj = ijj = -i$, etc.)

Es gilt: H ist Schiefkörper (Hamilton-Quaterionen):

$$\begin{aligned} &(a + bi + cj + dk) \cdot (a - bi - cj - dk) \\ &\qquad = a^2 - abi - acj - adk + bia + b^2 - bicj - bidk \\ &\qquad + cja - cjbi + c^2 - cjdk + dka - dkbi - bkcj + d^2 \\ &\qquad = a^2 + b^2 + c^2 + d^2 \end{aligned}$$

$\Longrightarrow \dfrac{1}{a+bi+cj+dh} = \frac{a}{a^2+b^2+c^2+d^2} - \frac{b}{a^2+b^2+c^2+d^2}i - \frac{c}{a^2+b^2+c^2+d^2}j - \frac{d}{a^2+b^2+c^2+d^2}k,$
falls nicht $a = b = c = d = 0$.

f) In jedem Ring gilt:

$$\begin{array}{ccccc} x\cdot 0 & = & 0 & = & 0\cdot x \\ x(-y) & = & -(x\cdot y) & = & (-x)y \quad \text{für alle } x,y\in R \\ (-x)\cdot(-y) & = & x\cdot y & & \end{array}$$

Beweis • $x\cdot 0 = x\cdot(0+0) = x\cdot 0 + x\cdot 0 \xRightarrow{-(x\cdot 0) \text{ auf beiden Seiten}} 0 = x\cdot 0$
genauso für $0\cdot x$

- $x\cdot(-y) + x\cdot y = x\cdot(-y+y) = x\cdot 0 = 0.$
- $(-x)(-y) = -((-x)\cdot y) = -(-(x\cdot y)) = x\cdot y$

g) Ist R ein Ring mit Eins und $R \neq \{0\}$, so ist $0 \neq 1$ in R.

Beweis Wäre $0 = 1$, so gilt für jedes $x \in R$: $x = x\cdot 1 = x\cdot 0 = 0$, also doch $R = \{0\}$.

Definition 2.2

Sei $(R, +, \cdot)$ Ring.

a) $R' \subseteq R$ heißt ***Unterring***, wenn $(R', +, \cdot)$ Ring ist. Umgekehrt heißt R dann ***Erweiterungsring*** von R'.

b) $I \subseteq R$ heißt (Zweiseitiges-)***Ideal***, wenn $(I, +)$ Untergruppe von $(R, +)$ ist und $r\cdot x \in I$ und $x\cdot r \in I$ für alle $x \in I$, $r \in R$.

c) $x \in R$ heißt Links- (bzw. Rechts-) ***Nullteiler***, wenn es $y \in R \setminus \{0\}$ gibt mit $x\cdot y = 0$ (bzw. $y\cdot x = 0$).

d) R heißt ***nullteilerfrei***, wenn 0 der einzige Nullteiler in R ist.
(d.h. wenn aus $x\cdot y = 0$ folgt $x = 0$ oder $y = 0$.)

e) R heißt ***Integritätsbereich*** (integral [domain]), wenn er nullteilerfrei, kommutativ ist und eine Eins besitzt.

Definition und Bemerkung 2.3

a) Eine Abbildung $\varphi : R \to R'$ (R, R' Ringe) heißt ***Ringhomomorphismus***,
wenn $\varphi : (R, +) \to (R', +)$ Gruppenhomomorphismus,
und $\varphi : (R, \cdot) \to (R', \cdot)$ Halbgruppenhomomorphismus ist.

b) Sind R, R' Ringe mit Eins, so heißt der Ringhomomorphismus $\varphi : R \to R'$ ein ***Homomorphismus von Ringen mit Eins*** , wenn

$$\varphi(1_R) = 1_{R'}$$

c) Die Ringe bilden mit Ringhomomorphismen eine Kategorie.

d) Die Ringe mit Eins bilden mit Homomorphismen von Ringen mit Eins ebenfalls eine Kategorie (eine echte Unterkategorie der Ringe).

e) $(R,+,\cdot) \mapsto (R,+)$ ist kovarianter Funktor Ringe $\to$ AbGruppen

oder

$(R,+,\cdot) \mapsto (R^\times,\cdot)$ ist kovarianter Funktor Ringe mit Eins $\to$ Gruppen.

Bemerkung 2.4

Sei $\varphi : R \to R'$ Ringhomomorphismus. Dann gilt:

a) Bild(φ) ist Unterring von R'.

b) Kern(φ) ist Ideal in R. (Kern(φ) $= \varphi^{-1}(0)$).

Beweis Sei $x \in \text{Kern}(\varphi), r \in R \Longrightarrow \varphi(r{\cdot}x) = \varphi(r)\varphi(x) = \varphi(r){\cdot}0 = 0 \Longrightarrow r{\cdot}x \in \text{Kern}(\varphi)$.

c) Ist R Schiefkörper und φ Homomorphismus von Ringen mit Eins, dann ist φ injektiv (oder $R' = \{0\}$).

Beweis Sei $x \in R \setminus \{0\} \Longrightarrow \varphi(x) \cdot \varphi(x^{-1}) = \varphi(1_R) = 1_{R'} \neq 0$ (wenn $R' \neq \{0\}$).
$\Longrightarrow \varphi(x) \neq 0 \Longrightarrow$ Kern(φ) $= \{0\} \Longrightarrow \varphi$ injektiv.

Definition und Bemerkung 2.5

Sei R Ring mit Eins.

a) $\varphi_R : \mathbb{Z} \to R$, $n \mapsto \begin{cases} n \cdot 1 = 1 + \cdots + 1 & n \geq 0 \\ -((-n) \cdot 1) & n < 0 \end{cases}$
ist Homomorphismus von Ringen mit Eins.

b) Ist Kern(φ_R) $= n \cdot \mathbb{Z}$ ($n \geq 0$), so heißt n die ***Charakteristik*** von R. $n = \text{char}(R)$.

c) Ist R nullteilerfrei, so ist char(R) $= 0$ oder char(R) $= p$ für eine Primzahl p.

d) Bild(φ_R) $\cong {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$

Ist K (Schief-)Körper der Charakteristik $p > 0$, so ist Bild(φ_K) $\cong {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} =: \mathbb{F}_p$ der kleinste Teilkörper von K.

Er heißt ***Primkörper***.

Ist char(K) $= 0$, so ist der kleinste Teilkörper K isomorph zu $\mathbb{Q}$.

Beispiel R Ring $R^{n\times n}$ = Ring der $(n \times n)$ Matrizen mit Einträgen in R.
Für $n \geq 2$ ist $R^{n\times n}$ nicht kommutativ und nicht nullteilerfrei.
Die Eins in $R^{n\times n}$ ist die Einheitsmatrix $\begin{pmatrix} 1_R & & 0 \\ & \ddots & \\ 0 & & 1_R \end{pmatrix}$, vorausgesetzt R hat eine Eins.
Die Einheiten in $R^{n\times n}$ sind die invertierbaren Matrizen:

$$\left(R^{n\times n}\right)^\times = GL_n(R) = \left\{A \in R^{n\times n} : \det A \in R^\times\right\}$$

Zur Definition von $\det A$ muss R kommutativ sein.
$SL_n(R) := \{A \in GL_n(R) : \det A = 1\}$ ist Untergruppe von $GL_n(R)$ und Normalteiler:
$\det(BAB^{-1}) = \det(B)\det(A)\det(B)^{-1} = \det(A)$
$GL_n(R)/SL_n(R) \cong R^\times$ (Isomorphismus: $A \cdot R_n(R) \mapsto \det(A)$)

Definition und Bemerkung 2.6

a) Sei R ein Ring, $a \in R$. Dann ist $(a) := a \cdot R = \{a \cdot r : r \in R\}$ ein Rechtsideal in R.
Es ist $a \in (a)$, falls R eine Eins hat.

b) Ein (Rechts-)Ideal I in R heißt ***Hauptideal***, wenn es ein $a \in R$ gibt mit $I = (a)$.

c) Ein kommutativer Ring mit Eins heißt ***Hauptidealring***, wenn jedes Ideal in R ein Hauptideal ist.

Beispiel Sei $I \subset \mathbb{Z}$ Ideal, $a \in I$ mit $|a| \leq |b| \forall b \in I \setminus \{0\}$.
Behauptung: $I = (a)$
Denn: „$\supseteq$“ $\surd$
und „$\subseteq$“ sei $b \in I$, teile b durch a: $b = qa + r$ mit $r < |a| \implies r = b - q \cdot a \in I \implies r = 0$.

d) Sei R kommutativer Ring mit Eins, $R \neq \{0\}$.
Dann gilt:

$$R \text{ ist Körper} \Leftrightarrow (0) \text{ und } R \text{ sind die einzigen Ideale in } R$$

Beweis „$\Rightarrow$“ Sei $I \subseteq R$ Ideal, $a \in I \setminus \{0\}$. $\implies$ es gibt $a^{-1} \in R \implies aa^{-1} \in I \implies I = R$
$(x \in R \implies x \cdot 1 = x)$
„$\Leftarrow$“ Sei $a \subset R \setminus \{0\} \implies (a) = R \implies \exists b \in R$ mit $a \cdot b = 1$

Definition und Bemerkung 2.7

Sei R Ring, I_1, I_2 Ideale in R.
Dann gilt:

a) $I_1 \cap I_2$ ist Ideal.
$I_1 + I_2 = \{a + b : a \in I_1, b \in I_2\}$ ist Ideal.
$I_1 \cdot I_2 = \left\{\sum_{i=1}^{<\infty} a_i \cdot b_i : a_i \in I_1, b_i \in I_2\right\}$ ist Ideal.

b) $I_1 \cdot I_2 \subseteq I_1 \cap I_2$ (aber i.A. $\neq$!)

c) Ein beliebiger Durchschnitt von Idealen ist Ideal.

c) Sei R kommutativ mit Eins, $X \subseteq R$

$$(X) = \bigcap_{\substack{I \subseteq R \text{ Ideal} \\ X \subseteq I}} I = \left\{ \sum_{\text{endlich}} r_i x_i : r_i \in R, x_i \in X \right\}$$

heißt das von X erzeugte Ideal.

e) $I_1 + I_2 = (I_1 \cup I_2)$
$I_1 \cdot I_2 = (\{a \cdot b : a \in I_1, b \in I_2\})$

2.2 Polynomringe

Definition und Bemerkung 2.8

Sei R ein kommutativer Ring mit Eins, $R \neq \{0\}$

a) Ein ***Polynom*** über R ist eine Folge

$$f = (a_0, a_1, \ldots) \text{ mit } a_i \in R \text{ und } a_i = 0 \text{ für fast alle } i$$

symbolische Schreibweise: $f = \sum_{n=0}^{n} a_i X^i$ (n so groß, dass $a_i = 0$ für $i > n$)

b) $R[X] = \{f = (a_0, a_1, \ldots) : f \text{ Polynom über } R\}$ ist kommutativer Ring mit Eins mit den Verknüpfungen

$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + a_2, \ldots)$

$(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (c_0, c_1, \ldots)$ mit $c_i = \sum_{k=0}^{i} a_k b_{i-k}$

c) $R \to R[X]$, $a \mapsto (a, 0, \ldots)$ ist injektiver Ringhomomorphismus.

d) Für $n \leq 2$ heißt $R[X_1, \ldots, X_n] = (R[X_1, \ldots, X_{n-1}])[X_n]$ ***Polynomring in*** n ***Variablen*** über R.

Proposition 2.9

Sei R kommutativer Ring mit Eins.

a) Zu jedem $x \in R$ gibt es genau einen Ringhomomorphismus
$\varphi_x : R[X] \to R$ mit $\varphi_x|_R = id_R$ und $\varphi_x(X) = x$.
Es ist $\varphi_x(a_0, a_1, \ldots) = \sum_{i \geq 0} a_x x^i$

Beweis Ist b) für $R' = R$ und $\alpha = id_R$

b) Zu jedem Homomorphismus von Ringen mit Eins: $\alpha : R \to R'$ und jedem $y \in R'$ gibt es genau einen Ringhomomorphismus $\varphi_y : R[X] \to R'$ mit $\varphi_y|_R = \alpha$ und $\varphi_y(X) = y$.

Beweis $\varphi_y(a_0, a_1, \ldots) := \sum_{i \geq 0} \alpha(a_i) y^i$

ist die einzig mögliche Definition eines Ringhomomorphismus, weil
$(a_0, a_1, \ldots) = \sum_{i=0}^{n} a_i X^i$
und da $\varphi_y(a_0, a_1, \ldots) = \varphi_y(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \varphi_y(a_i)\varphi_y(X)^i$ sein muss.

Folgerung 2.10

Die Zuordnung $R \mapsto R[X]$ ist ein kovarianter Funktor Ringe mit Eins $\to$ Ringe mit Eins.

Beweis Ist $\alpha : R \to R'$ Ringhomomorphismus, so sei $a : R[X] \to R'[X]$ der Homomorphismus, der durch $\alpha : R \to R' \overset{2.8.c)}{\hookrightarrow} R'[X]$ und $X \mapsto X$ bestimmt ist.

Definition und Bemerkung 2.11

a) Für $f = (a_0, a_1, \ldots) \in R[X]$. $f \neq 0$ sei $\mathrm{Grad}(f) := \max\{i : a_i \neq 0\} = \deg(f)$

b) Für f, g ist $\mathrm{Grad}(f + g) \leq \max(\mathrm{Grad}(f), \mathrm{Grad}(g))$

c) Für f, g ist $\mathrm{Grad}(f \cdot g) \leq \mathrm{Grad}(f) + \mathrm{Grad}(g)$ und $=$ falls R nullteilerfrei.

Folgerung 2.12

Ist R Integritätsbreich, so ist $R[X]$ auch Integritätsbereich und $R[X]^\times = R^\times$.

Definition und Bemerkung 2.13

Sei R kommutativer Ring mit Eins, $(H, \cdot)$ Halbgruppe.

a) $R[H] := \{(a_k)_{k \in H}, a_k \neq 0$ nur für endlich viele $h \in H\}$ ist mit den Verknüpfungen
$(a_k) + (b_k) = (a_k + b_k)$ und $(a_k) \cdot (b_k) = (c_k)$ mit $c_k = \sum_{h_1 \cdot h_2 = h} a_{h_1} b_{h_2}$ ein Ring.

$R[H]$ heißt ***Halbgruppenring*** zu H über R.

Schreibe auch $\sum_{h \in H} a_h \cdot h$ für (a_k).

b) $R\left[(\mathbb{N}, +)\right] \cong R[X]$
$R\left[(\mathbb{N}^n, +)\right] \cong R[X_1, \ldots, X_n]$

c) $R[H] \left\{ \begin{array}{c} \text{kommutativ} \\ \text{hat Eins} \end{array} \right\} \iff H \left\{ \begin{array}{c} \text{kommutativ} \\ \text{hat Eins} \end{array} \right\}$.

d) $(H, \cdot) \to (R[H], \cdot)$, $h \mapsto 1_R \cdot h$ ist injektiver Halbgrupppenhomomorphismus.

e) Ist $(H, \cdot)$ Monoid, so ist $R \to R[H]$, $r \mapsto r \cdot 1_H$ injektiver Ringhomomorphismus.

Satz 7 (Universelle Eigenschaft des Monoidrings)

Sei R kommutativer Ring mit Eins, $(H, \cdot)$ Monoid. Dann gibt es zu jedem $\varphi : R \to R'$ Homomorphismus von Ringen mit Eins und jeden Monoidhomomorphismus $\sigma : H \to (R', \cdot)$ genau einen Ringhomomorphismus $\Phi : R[H] \to R'$ mit $\Phi|_R = \varphi$ und $\Phi|_H = \sigma$.
Dabei werden R und H wie in 2.13 d) bzw. e) in $R[H]$ eingebettet.

Beweis Es muss gelten: $\Phi(\sum_{h\in H} a_h \cdot h) := \sum_{h\in H} \varphi(a_h) \cdot \sigma(h)$
Das zeigt die Eindeutigkeit, taugt aber auch als Definition von Φ, was die Existenz zeigt.

Definition und Bemerkung 2.14

a) $R[\![X]\!] := \{(a_i)_{i\in\mathbb{N}} : a_i \in R\}$
ist mit + und $\cdot$ wie bei Polynomring ein kommutativer Ring mit Eins.
$R[\![X]\!]$ heißt ***Ring der (formalen) Potenzreihen*** über R.
Schreibweise: $f = \sum_{i=0}^{\infty} a_i x^i$ für $f = (a_i)_{i\in N}$.

b) Sei $0 \neq f = \sum_{i=0}^{\infty} a_i x^i \in R[\![X]\!]$.
Dann heißt $o(f) := \min\{i \in \mathbb{N} : a_i \neq 0\}$ der ***Untergrad*** von f.
Es gilt für alle $f, g \in R[\![X]\!] \setminus \{0\}$:
$o(f + g) \leq \min(o(f) + o(g))$ und $o(f \cdot g) \leq o(f) + o(g)$

c) Ist R Integritätsbreich, so ist $o(f \cdot g) = o(f) + o(g)$ $\forall f, g \in R[\![X]\!] \setminus \{0\}$.
und es gilt: $R[\![X]\!]^\times = \left\{ f = \sum_{i=0}^{\infty} a_i x^i \in R[\![x]\!] : a_0 \in R^\times \right\}$

d) Ist $R = K$ Körper, so ist $m := K[\![X]\!] \setminus K[\![X]\!]^\times = \left\{ \sum_{i=0}^{\infty} a_i x^i : a_0 = 0 \right\}$ Ideal in $K[\![X]\!]$.

Beweis a), b), d) $\surd$

c) „$\subseteq$“ Sei $f = \sum a_i x^i \in R[\![X]\!]^\times$, dann gibt es $g = \sum b_i x^i \in R[\![X]\!]^\times$ mit
$1 = f \cdot g = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \cdots$.
$\Longrightarrow a_0 b_0 = 1 \Longrightarrow a_0 \in R^\times$.
„$\supseteq$“ Definiere $g = \sum b_i x^i$ rekursiv durch
$b_0 = a_0^{-1}$, $b_i := a_0^{-1} \cdot \sum_{k=0}^{i} a_k b_{i-k}(-1)^k$? für $i \geq 1$.
Dann ist $f \cdot g = 1$. Bsp ist $b_1 = -a_0^{-1}(a_1 \cdot b_0)$.

2.3 Quotienten

Sei R kommutativer Ring mit Eins.

Definition und Bemerkung 2.15

a) Sei I Ideal in R.

Durch die Verknüpfung $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$ wird die Faktorgruppe ${}^{(R,+)}\!/_{(I,+)}$ zu einem kommutativen Ring mit Eins.

${}^{R}\!/_{I}$ heißt ***Faktorring*** oder ***Quotientenring*** von R in I.

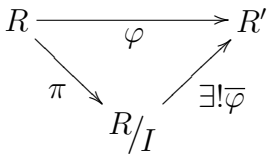
b) Die Restklassenabbildung $\pi : R \to {}^{R}\!/_{I}$, $x \mapsto \overline{x}$ ist surjektiver Ringhomomorphismus mit $\mathrm{Kern}(\pi) = I$.

c) (Universelle Abbildungseigenschaft des Faktorings)

Sei $\varphi : R \to R'$ ein Ringhomomorphismus. Dann gibt es zu jedem Ideal $I \subseteq R$ mit $I \subseteq \mathrm{Kern}(\varphi)$ einen eindeutig bestimmten Ringhomomorphismus

$$\overline{\varphi} : {}^{R}\!/_{I} \to R' \text{ mit } \varphi = \overline{\varphi} \circ \pi$$

so dass



kommutiert.

d) (Homomorphiesatz für Ringe)

Ist $\varphi : R \to R'$ surjektiver Ringhomomorphismus, dann ist $R' \cong {}^{R}\!/_{\mathrm{Kern}(\varphi)}$

Beweis a) Wohldefiniertheit des Produkts: Seien $x', y' \in R$ mit $\overline{x'} = \overline{x}$, $\overline{y'} = \overline{y}$. Dann gibt es $a, b \in I$ mit $x' = x + a$, $y' = y + b$.

$\Longrightarrow x' \cdot y' = (x + a) \cdot (y + b) = xy + \underbrace{ay}_{\in I} + \underbrace{xb}_{\in I} + \underbrace{ab}_{\in I}$

$\Longrightarrow \overline{x'} \cdot \overline{y'} = \overline{x} \cdot \overline{y}$

Restlichen Eigenschaften vererben sich dann von R.

b) π ist surjektiver Gruppenhomomorphismus mit $\mathrm{Kern}(\pi) = I$ nach Satz 1a).

$\pi(xy) = \pi(x) \cdot \pi(y)$ nach Definition der Verknüpfung.

c) Nach Satz 1b) gibt es eindeutigen bestimmten Gruppenhomomorphismus $\overline{\varphi} : {}^{R}\!/_{I} \to R'$ mit $\varphi = \overline{\varphi} \circ \pi$.

Zeige also: $\overline{\varphi}$ ist Ringhomomorphismus.

Für $x, y \in R$ ist $\overline{\varphi}(\overline{x} \cdot \overline{y}) = \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = \overline{\varphi}(\overline{x}) \cdot \overline{\varphi}(\overline{y})$.

d) Folgt aus c) und Satz 1a).

Definition und Bemerkung 2.16

a) Ein Ideal $I \subsetneq R$ heißt ***maximal***, wenn es kein Ideal I' in R gibt mit $I \subsetneq I' \subsetneq R$.

b) Ein Ideal $I \subsetneq R$ heißt ***Primideal***, wenn für $x, y \in R$ mit $x \cdot y \in I$ gilt: $x \in I$ oder $y \in I$.

Beispiele

1) p Primzahl $\iff p \cdot \mathbb{Z}$ ist Primideal in $\mathbb{Z}$, sogar maximal.
2) (x) ist Primideal in $R[\![X]\!] \iff R$ ist Körper.

c) R ist nullteilerfrei $\iff (0)$ ist Primideal.

d) Jedes maximale Ideal I ist Primideal.

Beweis c) R ist nicht nullteilerfrei $\iff \exists a, b \in R \setminus \{0\} : a \cdot b = 0 \iff (0)$ kein Primideal.

d) Seien $x, y \in R$ mit $x \cdot y \in I$ und $x \notin I$. Dann ist $(x) + I \supsetneq I$.
$\xrightarrow{I \text{ maximal}} (x) + I = R$
$\implies 1 \in (x) + I$, d.h. es gibt $r \in R$, $a \in I$ mit $1 = r \cdot x + a$.
$\implies y = \underbrace{rxy}_{\in I} + \underbrace{ay}_{\in I} \in I$
$\implies I$ ist Primideal.

Definition und Bemerkung 2.17

Sei $I \subsetneq R$ ein Ideal. Dann gilt:

a) I ist Primideal $\iff {}^{R}\!/_{I}$ ist nullteilerfrei.

b) I ist maximales Ideal $\iff {}^{R}\!/_{I}$ ist Körper.

Beweis a) ${}^{R}\!/_{I}$ ist nicht nullteilerfrei
$\iff \exists \overline{x} \neq 0 \neq \overline{y} \in {}^{R}\!/_{I}$ mit $\overline{x} \cdot \overline{y} = \overline{0} = \overline{x \cdot y}$.
$\iff x \cdot y \in I$, $x, y \notin I$.
$\implies I$ kein Primideal.

b) Nach 2.6 d) ist ${}^{R}\!/_{I}$ genau dann Körper, wenn (0) und ${}^{R}\!/_{I}$ die einzigen Ideale in ${}^{R}\!/_{I}$ sind. Nach Blatt 7, A 3 entsprechen die Ideale in ${}^{R}\!/_{I}$ bijektiv den Idealen in R, die I enthalten.

Beispiel Sei $C = \{(a_n)_{n\in\mathbb{N}} : (a_n)_n \text{ Cauchy-Folge}, a_n \in \mathbb{Q}\}$
(d.h. für $k \in \mathbb{N}\exists n \in \mathbb{N} : |a_i - a_j| < \frac{1}{k}$ für $i, j \geq n$.)
C ist Ring mit komponentenweiser $+$ und $\cdot$ (vornehm $C \subset \prod_{n\in\mathbb{N}} \mathbb{Q}$)
$N := \{(a_n) \in C : (a_n) \text{ Nullfolge}\}$ (d.h. für $k \in \mathbb{N}\exists n \in \mathbb{N} : |a_i| < \frac{1}{k}\forall i \geq n$)
N ist Ideal in C. $\surd$ (NF + NF $\in C$, NF $\cdot$ CF $\in N$)
Behauptung: ${}^{C}\!/_{N}$ ist Körper (bzw. N ist maximal)
Beweis: Sei $a = (a_n)_{n\in\mathbb{N}} \in C \setminus N$. Zu zeigen: $1 \in N + (a) = \langle N \cup \{a\}\rangle$ (ist 1 im Ideal, spannt es ganz C auf).
$(a_n) \notin N \implies a_n = 0$ nur für endlich viele n, d.h. $a \neq 0$ für $i > n$.

$$b_n := \begin{cases} 0 & i < n_0 \\ \frac{1}{a_i} & i \geq n_0 \end{cases} \text{ und } b := (b_n) \in C.$$

$$a \cdot b =: (c_n),\ c_n = \begin{cases} 0 & n < n_0 \\ 1 & n \geq n_0 \end{cases}$$

$$\implies 1 - ab = (d_n),\ d_n = \begin{cases} 1 & n < n_0 \\ 0 & n \geq n_0 \end{cases} \implies d_n \in N.$$

$\implies 1 = (d_n) + ba \in N + (a) \implies N$ ist maximal.
${}^{C}\!/_{N} = \mathbb{R}$!

Satz 8 (Chinesischer Restesatz)

Sei R kommutativer Ring mit Eins, $I_1, \ldots, I_n$ Ideale in R mit $I_\nu + I_\mu = R$ für alle $\nu \neq \mu$ (dann heißen I_ν und I_μ relativ prim oder koprim). Für $\nu = 1, \ldots, n$ sei $p_\nu : R \to {}^{R}\!/_{I_\nu}$ die Restklassenabbildung. Dann gilt:

a) $\varphi : R \to {}^{R}\!/_{I_1} \times \cdots \times {}^{R}\!/_{I_n}$ ist surjektiv. $x \mapsto (p_1(x), \ldots, p_n(x))$

b) ${}^{R}\!/_{I_1} \times \cdots \times {}^{R}\!/_{I_n} \cong {}^{R}\!/_{\bigcap_{\nu=1}^{n} I_\nu}$ (klar nach Homomorphiesatz Kern$(\varphi) = \bigcap_{\nu=1}^{n} I_\nu$)

c) (Simultane Kongruenzen)

Für paarweise teilerfremde ganze Zahlen $m_1, \ldots, m_n$ und beliebige $r_1, \ldots, r_n \in \mathbb{Z}$ gibt es $x \in \mathbb{Z}$ mit $x \equiv r_\nu \mod m_\nu$ für $\nu = 1, \ldots, n$ (Spezialfall für $R = \mathbb{Z}$ von a)).

Beweis Genügt zu zeigen: $(0, \ldots, 0, 1, 0, \ldots, 0) \in \text{Bild}(\varphi)$ für jedes ν, d.h. es gibt $e_\nu \in R$, $(v = 1, \ldots n)$ mit $e_\nu \in I_\nu$ für $\mu \neq \nu$ und $1 - e_\nu =: a_\nu \in I_\nu$ (denn für $x = (\overline{r_1}, \ldots, \overline{r_n}) \in {}^{R}\!/_{I_1} \times \cdots \times {}^{R}\!/_{I_n}$ sei $e := \sum_{\nu=1}^{n} r_\nu e_\nu$ mit $r_\nu \in p_\nu^{-1}(r_\nu) \implies \varphi(e) = \sum_{\nu=1}^{n} p_\nu(r_\nu e_\nu) = x$)
Nach Voraussetzung gibt es für jedes $\mu \neq \nu$ $a_\mu \in I_\nu$, $b_\mu \in I_\nu$ mit $a_\mu + b_\mu = 1$

$$\implies 1 = \prod_{\substack{\mu=1 \\ \mu\neq\nu}}^{n} (a_\mu + b_\mu) = \underbrace{\prod_{\substack{\mu=1 \\ \mu\neq\nu}}^{n} b_\mu}_{\in \bigcap_{\substack{\mu=1 \\ \mu\neq\nu}} I_\mu} + \underbrace{a_\nu}_{\in I_\nu}$$

$\implies 1 = e_\nu - a_\nu$ wie gewünscht.

2.4 Teilbarkeit

Sei R kommutativer Ring mit Eins.

Definition und Bemerkung 2.18

Seien $a, b \in R$, $a \neq 0$.

a) a ***teilt*** b (Schreibweise $a \mid b$) $:\Longleftrightarrow b \in (a)$ $(\Longleftrightarrow \exists x \in R : b = a \cdot x)$

b) $d \in R$ heißt ***größter gemeinsamer Teiler*** von a und b (ggT(a, b)), wenn gilt:

(i) $d \mid a$ und $d \mid b$ (bzw. $a \in (d)$ und $b \in (d)$)

(ii) ist $d' \in R$ auch Teiler von a und b, so gilt $d' \mid d$, $d \in (d')$.

c) Ist $d \in R$ ein ggT von a und b und $e \in R^\times$, so ist auch $e \cdot d$ ein ggT. Ist R nullteilerfrei und sind d, d' beide ggT und a und b, so gibt es $e \in R^\times$ mit $d' = e \cdot d$.

Beweis Nach Definition gibt es $x, y \in R$ mit $d' = x \cdot d$ und $d = y \cdot d' \implies d' = xyd' \implies d'(1 - xy) = 0 \overset{\substack{R \text{ nullteilerfrei} \\ d \neq 0}}{\Longrightarrow} 1 = xy$, d.h. $x, y \in R^\times$.

Definition und Bemerkung 2.19

a) Ein Integritätsbereich R heißt ***euklidisch***, wenn es eine Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}$ mit folgender Eigenschaft gibt:

zu $f, g \in R$, $g \neq 0$ gibt es $q, r \in R$ mit $f = q \cdot g + r$ mit $r = 0$ oder $\delta(r) < \delta(g)$.

b) Sei R euklidisch, $a, b \in R \setminus \{0\}$. Dann gilt:

(i) in R gibt es einen ggT von a und b.

(ii) $d \in (a, b)$ (d.h. $\exists x, y \in R$ mit $d = x \cdot a + y \cdot b$)

(iii) $(d) = (a, b)$

c) Jeder euklidische Ring ist ein Hauptidealring.

Beispiel $\mathbb{Z}$ mit $\delta(a) = |a|$

$K[X]$ mit $\delta(f) = \text{Grad}(f)$

Beweis b) Ohne Einschränkung sei $\delta(a) \geq \delta(b)$. Nach Voraussetzung gibt es $q_1, r_1 \in R$ mit $a = q_1 \cdot b + r$, $\delta(r_1) < \delta(b)$ oder $r_1 = 0$.

Ist $r_1 = 0$, so ist $a \in (b) = (a, b)$ und ggT$(a, b) = b$.

Sonst gibt es $q_2, r_2 \in R$ mit $b = q_2 r_1 + r_2$ und $r_2 = 0$ oder $\delta(r_2) < \delta(r_1)$.

usw... $\implies$ $r_i = q_{i+2} r_{i+1} + r_{i+2}$

$r_{n-2} = q_n r_{n-1}$ (da $\delta(r_{i+2}) < \delta(r_{i+1})$)

Behauptung: $d := r_{n-1}$ ist ggT von a und b.

denn: $d \mid r_{n-2}$, vorletzte Zeile $r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$. $\implies d \mid r_{n-3}$.

Induktion: $d \mid r_i$ für alle $i \implies d \mid b \implies d \mid a$.

Umgekehrt: Sei d' Teiler von a und $b \implies d' \mid r_1 \overset{\text{I.V.}}{\implies} d' \mid r_i$ für alle $i \implies d' \mid d$.

Noch zu zeigen: (ii) $d \in (a,b)$
Nach Konstruktion ist $r_{i+2} \in (r_i, r_{i+1}) \subset \cdots \subset (a,b)\ \forall i$.

(iii) $(d) = (a,b)$
„$\subseteq$“: ist (ii)
„$\supseteq$“: $a \in (d)$, $b \in (d)$ nach Definition.

c) Sei $I \subset R$ Ideal, $I \neq \{0\}$.

Wähle $a \in I$ mit $\delta(a)$ minimal. Dann gilt für jedes $b \in I$:

$b = qa + r$ mit $r \in I$ und $\delta(r) < \delta(a)$. Widerspruch!

$\implies r = 0 \implies I = (a)$.

Definition und Bemerkung 2.20

Sei R kommutativer Ring mit Eins.

a) $x, y \in R$ heißen assoziiert, wenn es $e \in R^\times$ gibt mit $y = x \cdot e$.

„assoziiert“ ist eine Äquivalenzrelation.

b) $x \in R \setminus R^\times$ heißt ***irreduzibel***, wenn aus $x = y_1 y_2$ mit $y_1, y_2 \in R$ folgt $y_1 \in R^\times$ oder $y_2 \in R^\times$.

c) $x \in R \setminus R^\times$ heißt ***prim*** (oder ***Primelement***), wenn (x) ein Primideal ist.

d.h. aus $x \mid y_1 y_2$ folgt $x \mid y_1$ oder $x \mid y_2$.

d) Sind $x, y \in R \setminus R^\times$ assoziiert, so ist x genau dann irreduzibel (bzw. prim), wenn y irreduzibel (prim) ist.

e) Ist R nullteilerfrei, so ist jedes Primelement $\neq 0$ irreduzibel.

Beweis Sei (x) Primideal und $x = y_1 \cdot y_2$, $y_1, y_2 \in R$

$\implies$ Ohne Einschränkung sei $y_1 \in (x)$, d.h. $y_1 = x \cdot a$ für ein $a \in R$.

$\implies x = x \cdot a \cdot y_2$

$\implies x(1 - ay_2) = 0 \overset{R \text{ nullteilerfrei}, x \neq 0}{\implies} ay_2 = 1$.

Beispiel $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

Kleinster Ring in dem wir rechnen:
$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$
$(a + b\sqrt{-5})(c + d\sqrt{-5}) = ac - 5bd + (ad + bc)\sqrt{-5}$.

In R ist 2 kein Primelement: weder $1 + \sqrt{-5}$ noch $1 - \sqrt{-5}$ ist durch 2 teilbar.

Aber: 2 ist irreduzibel!
denn: Sei $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$

$\implies 4 = |2|^2 = (a + b\sqrt{-5})(a - b\sqrt{-5})(c + d\sqrt{-5})(c - d\sqrt{-5})$
$= (a^2 + 5b^2)(c^2 + 5d^2) = a^2c^2 + 5P$ mit $P > 0$

$\implies P = 0. \implies b = d = 0 \implies a^2 = 1,\ c^2 = 4.$

Definition und Bemerkung 2.21

Sei R ein Integritätsbereich.

a) Folgende Eigenschaften sind äquivalent:

(i) jedes $x \in R \setminus \{0\}$ lässt sich eindeutig als Produkt von Primelementen schreiben.

(ii) jedes $x \in R \setminus \{0\}$ lässt sich irgendwie als Produkt von Primelementen schreiben.

(iii) jedes $x \in R \setminus \{0\}$ lässt sich eindeutig als Produkt von irreduzibelen Elementen schreiben.

b) Sind die 3 Eigenschaften aus a) für R erfüllt, so heißt R ***faktorieller Ring*** (oder ZPE-Ring, engl. UFD).

Dabei ist in a): „eindeutig“ gemeint bis auf Reihenfolge und Multiplikation mit Einheiten.
Präziser: Sei $\mathcal{P}$ ein Vertretersystem der Primelemente ($\neq 0$) bzgl. „assoziiert“.
Dann heißt (i) $\forall x \in R \setminus \{0\} \exists! e \in R^\times$ und für jedes $p \in \mathcal{P}$ ein $\nu_p(x) \geq 0$: $x = e \cdot \prod_{p \in \mathcal{P}} p^{\nu_p(x)}$

(beachte $\nu_p(x) \neq 0$ nur für endlich viele p).

Beweis (i) $\Longrightarrow$ (ii) $\surd$. (ii) $\Longrightarrow$ (iii):
Sei $x \neq 0$, $x = e \cdot p_1 \cdot \ldots \cdot p_r$, $p_i \in \mathcal{P}$, $e \in R^\times$
Sei weiter $x = q_1 \cdot \ldots \cdot q_s$ mit irreduzibelen Elementen q_j.
Es ist $x \in (p_1) \Longrightarrow \exists j$ mit $q_j \in (p_1)$.
Ohne Einschränkung sei $j = 1$. d.h. $q_1 = \varepsilon_1 p_1$ mit $\varepsilon_1 \in R^\times$ (da q_1 irreduzibel).
$\Longrightarrow \varepsilon_1 \cdot q_2 \cdot \ldots \cdot q_s = e \cdot p_2 \cdot \ldots \cdot p_r$.
Mit Induktion über r folgt die Behauptung.
(iii) $\Longrightarrow$ (i): Noch zu zeigen: Jedes irreduzibles Element in R ist prim.
Sei $p \in R \setminus R^\times$ irreduzibel, $x, y \in R$ mit $x \cdot y \in (p)$, also $x \cdot y = p \cdot a$ für ein $a \in R$.
Schreibe $x = q_1 \cdot \ldots \cdot q_m$, $y = s_1 \cdot \ldots \cdot s_n$, $a = p_1 \cdot \ldots \cdot p_l$ mit irreduzibelen Elementen q_i, s_j, p_k.
$\Longrightarrow x \cdot y = q_1 \cdot \ldots \cdot q_m s_1 \cdot \ldots \cdot s_n = p \cdot a = p \cdot p_1 \cdot \ldots \cdot p_l$
$\overset{\text{Eindeutigkeit}}{\Longrightarrow} p \in \{q_1, \ldots q_m, s_1, \ldots s_n\}$ (bis auf Einheiten).
$\Longrightarrow x \in (p)$ oder $y \in (p)$.

Bemerkung 2.22

Ist R faktorieller Ring, so gibt es zu allen $a, b \in R \setminus \{0\}$ einen $\mathrm{ggT}(a, b)$

Beweis Sei $\mathcal{P}$ wie in 2.21 Vertretersystem der Primelemente.
$a = e_i \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$, $b = e_i \prod_{p \in \mathcal{P}} p^{\nu_p(b)} \Longrightarrow d := \prod_{p \in \mathcal{P}} p^{\nu_p(d)}$ mit $\nu_p(d) = \min(\nu_p(a), \nu_p(b))$
ist $\mathrm{ggT}(a, b)$.

Satz 9

Jeder nullteilerfreie Hauptidealring ist faktoriell.

Beweis 1. Schritt: Jedes $x \in R \setminus \{0\}$ lässt sich als Produkt von irreduzibelen Elementen schreiben.

2. Schritt: Jedes irreduzible $x \in R \setminus \{0\}$ erzeugt ein maximales Ideal.

Mit 2.21a (ii) folgt dann die Behauptung.

Beweis 2:

Sei $p \in R \setminus \{0\}$ irreduzibel, I Ideal in R mit $(p) \subseteq I \subsetneq R$.

Nach Voraussetzung gibt es $a \in R$ mit $I = (a)$, $a \notin R^\times$, da $I \neq P$.

Da $p \in (p) \subseteq I = (a)$, gibt es $\varepsilon \in R$ mit $p = a \cdot \varepsilon$

$\xRightarrow{p \text{ irreduzibel}} \varepsilon \in R^\times \implies (p) = (a) = I$.

Beweis 1:

$x \in R \setminus \{0\}$ heiße Störenfried, wenn x nicht als Produkt von irreduzibelen Elementen darstellbar ist.

Sei x Störenfried. Dann ist $x \notin R^\times$ und x nicht irreduzibel, also $x = x_1 \cdot y_2$ mit $x_1 y_1 \notin R^\times$.

Ohne Einschränkung ist x_1 Störenfried (sonst ist x doch Produkt von irreduzibelen)

Also $x_1 = x_2 \cdot y_2$, $x_2 y_2 \notin R^\times$. Ohne Einschränkung x_2 Störenfried.

Induktiv erhalten wir $x, x_1, x_2, \ldots$ alles Störenfriede, mit $(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots \subsetneq (x_i) \subsetneq (x_{i+1})$

Sei nun $I = \bigcup_{i \geq 1} (x_i)$. I ist Ideal. $\surd$.

$\implies$ es gibt $a \in R$ mit $I = (a) \implies \exists i$ mit $a \in (x_i) \implies x_j \in (x_i)$ für alles $j \geq i$. Widerspruch.

2.5 Brüche

Ziel: Verallgemeinerung der Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$:

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\} /_\sim$$

wobei $\frac{m}{n} \sim \frac{m'}{m'} :\Leftrightarrow mn' = m'n$.

Definition und Bemerkung 2.23

Sei R kommutativer Ring mit Eins.

$S \subset (R, \cdot)$ ein Untermonoid.

a) $S^{-1}R = R_S := (R \times S) /_\sim$ mit der Äquivalenzrelation

$$(a_1, s_1) \sim (a_2, s_2) :\Leftrightarrow \exists t \in S : t(a_2 s_1 - a_1 s_2) = 0$$

heißt ***Ring der Brüche*** von R mit Nennern in S (oder ***Lokalisierung*** von R nach S).

Schreibweise: $\frac{a}{s}$ sei die Äquivalenzklasse von (a, s).

Beweis $\sim$ ist Äquivalenzrelation.

reflexiv: $\surd$. symmetrisch: $\surd$.

transitiv:
(1) $a_2 s_1 = a_1 s_2$
(2) $a_3 s_2 = a_2 s_3$

$\Longrightarrow a_3 s_2 s_1 \overset{(2)}{=\!=} a_2 s_3 s_1 \overset{(1)}{=\!=} a_1 s_3 s_2 \Longrightarrow s_2(a_3 s_1 - a_1 s_3) = 0$

$\overset{\underline{\text{falls}}\ R\ \text{nullteilerfrei}\ \text{und}\ 0 \notin S}{\dashrightarrow} a_3 s_1 = a_1 s_3.$

(mit der neuen Definition mit $\exists t ...$)

Sei (1) $t(a_2 s_1 - a_1 s_2) = 0$
(2) $t'(a_2 s_3 - a_3 s_2) = 0$ mit $t, t' \in S$:

$$\begin{aligned} \Rightarrow \quad & t \cdot t' s_2 (a_3 s_1 - a_1 s_3) \\ = \quad & t(t' a_3 s_2 s_1 - t' a_1 s_3 s_2) \\ \overset{(2)}{=\!=} \quad & t(t' a_2 s_3 s_1 - t' a_1 s_3 s_2) \\ = \quad & t' s_3 t(s_2 s_1 - a_1 s_2) \qquad \overset{(1)}{=\!=} 0 \end{aligned}$$

b) Mit $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} := \frac{a_1 \cdot a_2}{s_1 \cdot s_2}$ und $\frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}$
ist R_S ein kommutativer Ring mit Eins.

Beweis $\cdot$ wohldefiniert: Sei $\frac{a_1'}{s_1'} = \frac{a_1}{s_1}$

$\Longrightarrow \exists t \in S : t(a_1' s_1 - a_1 s_1') = 0$

$\Longrightarrow t \cdot (a_1' a_2 s_1 s_2 - a_1 a_2 s_2 s_1') =$
$(t a_1 s_1' a_2 s_2 - t a_1 a_2 s_2 s_1') = 0.$

$+$ wohldefiniert: Sei $\frac{a_1'}{s_1'} = \frac{a_1}{s_1}$

$\Longrightarrow t(s_1' s_2 (a_1 s_2 + a_2 s_1) - s_1 s_2 (a_1' s_2 + a_2 s_1'))$
$= t s_2 (a_1 s_2 s_1' + \cancel{a_2 s_1 s_1'} - a_1' s_1 s_2 - \cancel{a_2 s_1 s_1'})$
$= 0$

Rest wie in $\mathbb{Q}$.

Beispiele 2.24

a) Sei R nullteilerfrei, $S = R \setminus \{0\}$
Dann ist $\text{Quot}(R) = R_S$ ein Körper, er heißt der ***Quotientenkörper*** von R.
denn: $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$ für $(a \neq 0)$
z.B. $R = K[X_1, \ldots, X_n]$, K ein Körper.
$\Longrightarrow \text{Quot}(R) = K(X_1, \ldots, X_n)$ Körper der rationalen Funktionen in n Variablen.
$R = \mathbb{Z}[X] \Longrightarrow \text{Quot}(R) = ...?$

b) $x \in R \setminus \{0\}$, $S = \{x^n : n \geq 0\}$
$R_S =: R_X = \{\frac{a}{x^n} : x \in R, n \geq 0\}$
z.B. $R = \mathbb{Z}$, $x = 2$, $\Longrightarrow R_S = \mathbb{Z}[\frac{1}{2}] = \left\{\frac{m}{2^n} : m \in \mathbb{Z}, n \in \mathbb{N}\right\}$

c) Sei $\mathfrak{p} \subset R$ Primideal, $S = R - \mathfrak{p}$ ist Monoid.

$R_S =: R_\mathfrak{p}$ heißt Lokalisierung von R nach $\mathfrak{p}$

z.B. $R = \mathbb{Z}$, $\mathfrak{p} = (2)$.

$\Longrightarrow \mathbb{Z}_{(2)} = \{\frac{m}{n} : m \in \mathbb{Z}, n \text{ ungerade}\}$

a) ist Spezialfall $\mathfrak{p} = (0)$

$\mathfrak{p}R_\mathfrak{p} = \{\frac{x}{y} : x \in \mathfrak{p}, y \in R \setminus \mathfrak{p}\}$ ist maximales Ideal in $R_\mathfrak{p}$ und zwar das einzige.

denn: Sei $\frac{z}{y} \in R_\mathfrak{p} \setminus \mathfrak{p}R_\mathfrak{p}$, d.h. $z \in R \setminus \mathfrak{p}$, $y \in R \setminus \mathfrak{p}$.

$\Longrightarrow \frac{z}{y} \in R_\mathfrak{p} \Longrightarrow \frac{y}{z} \in (R_\mathfrak{p})^\times$

typisches Beispiel: $R = \mathbb{R}[X]$ (oder $R = \mathcal{C}^0([-1,1])$)

$\mathfrak{p} = \{f \in R : f(0) = 0\}$ ist Primideal in R.

$R_\mathfrak{p} = \{\frac{f}{g} : f, g \in R, g(0) \neq 0\}$

d) Ist $0 \in S$, so ist $R_S = \{0\}$.

Bemerkung 2.25

Sei R kommutativer Ring mit Eins. $S \subset (R, \cdot)$ Monoid.

a) Die Abbildung $i_S : R \to R_S$, $a \mapsto \frac{a}{1}$ ist ein Ringhomomorphismus.

b) i_S ist injektiv, falls S keinen Nullteiler von R enthält und $0 \notin S$.

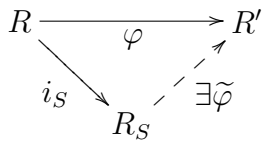
Beweis $\frac{a}{1} = 0 (= \frac{0}{1})$ in $R_S \Longrightarrow \exists s \in S$ mit $s(a \cdot 1 - 0 \cdot 1) = 0$

c) $i_S(S) \subset (R_S)^\times$

Beweis $(\frac{s}{1})^{-1} = \frac{1}{s}$

d) Universelle Abbildungseigenschaft:

Zu jedem Homomorphismus $\varphi : R \to R'$ von Ringen mit Eins mit $\varphi(S) \subset (R')^\times$ gibt es genau einen Homomorphismus $\widetilde{\varphi} : R_S \to S'$ mit $\varphi = \widetilde{\varphi} \circ i_S$ so dass



kommutiert.

Beweis $\widetilde{\varphi}(\frac{a}{s}) = \widetilde{\varphi}(a \cdot \frac{1}{s}) = \widetilde{\varphi}(\frac{a}{1} \cdot (\frac{s}{1})^{-1}) = \varphi(a) \cdot \varphi(s)^{-1}$

2.6 Teilbarkeit im Polynomring

Sei R faktorieller Ring. $\mathcal{P}$ Vertretersystem der Primelemente in R.
Jedes a besitzt eine eindeutige Darstellung $a = e \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$ mit $e \in R^\times$, $\nu_p(a) \in \mathbb{N}$.

Definition 2.26
Für $f \in R[X]$, $f = \sum_{i=0}^{n} a_i X^i$ und $p \in \mathcal{P}$ sei $\nu_p(f) = \min\{\nu_p(a_i) : i = 0, \ldots, n\}$
f heißt ***primitiv***, wenn $\nu_p(f) = 0$ für alle $p \in \mathcal{P}$.

Satz 10 (Irreduzibilitätskriterium von Eisenstein)
Sei R faktoriell, $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ primitiv mit $a_n \neq 0$.
Sei $p \in \mathcal{P}$ mit $p \nmid a_n$, $p \mid a_i$ für $i = 0, \ldots, n-1$ und $p^2 \nmid a_0$
Damit ist f irreduzibel.

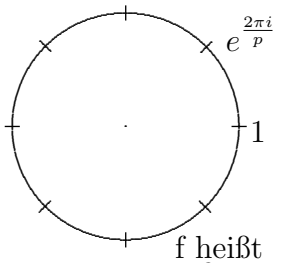
Beweis Sei $f = g \cdot h$ mit $g = \sum_{i=0}^{r} b_i X^i$, $h = \sum_{i=0}^{s} c_i X^i$ mit $b_r \neq 0 \neq c_s$.
$\Longrightarrow n = r + s$, $a_n = b_r c_s$, $a_0 = b_0 c_0 \Longrightarrow p \nmid b_r$, $p \nmid c_s$ und $p \mid b_0$, $p \mid c_0$.
Sei t maximal mit $p \mid b_i$ für $i = 0, \ldots, t$.

Dann ist $0 \leq t \leq r-1$ und $\underbrace{a_{t+1}}_{\notin (p)} = \underbrace{b_{t+1}}_{\notin (p)} \cdot c_0 + \underbrace{\sum_{i=0}^{t} b_i c_{t+1-i}}_{\in (p)}$

$\Longrightarrow t + 1 = n \Longrightarrow r = n \Longrightarrow s = 0$.

Beispiele 2.27

$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ mit $p \in \mathbb{Z}[x]$ Primzahl.
Behauptung: f ist irreduzibel.
Beobachtung: $f(x) = \dfrac{x^p - 1}{x - 1}$
Trick: $g(x) := f(x+1)$ ist genau dann irreduzibel, wenn $f(x)$ irreduzibel ist.
$g(x) = \dfrac{(x+1)^p - 1}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}$
wobei $\binom{p}{p} = 1 = a_{p-1}$, $a_0 = \binom{p}{1} = p$.
noch zu überlegen: $\binom{p}{k}$ ist durch p teilbar für $p = 2, \ldots, p-1$.
Bekannt ist $\binom{p}{k} = \dfrac{p!}{k!(p-k)!} \Longrightarrow$ durch p teilbar.
Mit Eisenstein folgt die Behauptung.
Beispiel: $f = x^2 - 4 \in \mathbb{Z}[x]$
mit $p = 2$: $\bar{f} = x^2 - 1 = (x-1)^2$
$p = 5$: $\bar{f} = x^2$
$p = 3$: $\bar{f} = x^2 + 1 \in \mathbb{F}_3[X]$ ist irreduzibel.
[macht das Sinn?]



f heißt „großer Kreis“

Proposition 2.28

Sei R faktorieller Ring, $p \in R$ Primelement.

a) $\overline{R}[X] = {}^{R[X]}\!/_{pR[X]}$ wobei $\overline{R} = {}^{R}\!/_{(p)}$

b) Sei $f \in R[X]$ primitiv, $p \nmid a_n$, $(f = \sum_{i=0}^{n} a_i X^i, a_n \neq 0)$
Ist $\overline{f} \in \overline{R}[X]$ irreduzibel, so ist f irreduzibel in $R[X]$.

Beweis a) $R \to \overline{R}$ induziert den Homomorphismus $\varphi : R[X] \to \overline{R}[X]$.
$\text{Kern}(\varphi) = \{f \in \sum_{i=0}^{n} a_i X^i : p \mid a_i \text{ für } i = 0, \ldots, n\} = pR[X]$
Mit dem Homomorphiesatz folgt die Behauptung.

b) Sei $f = g \cdot h \implies \overline{f} = \overline{g} \cdot \overline{h}$, schreibe $h = \sum_{i=0}^{s} c_i X^i$.
Also ohne Einschränkung $\overline{h} \in \left(\overline{R}[X]\right)^{\times} = \overline{R}^{\times}$
$\implies p \mid c_i$ für $i = 1, \ldots, s$
Wäre $s \geq 1$, so wäre c_s durch p teilbar, also auch $b_r c_s = a_n$. Widerspruch.

Satz 11 (Satz von Gauß)

Ist R faktorieller Ring, so ist $R[X]$ faktoriell.

Beweis Sei $K := \text{Quot}(R)$.
Dann ist $K[X]$ faktoriell (weil Hauptidealring), $R[X] \subseteq K[X]$ Unterring.
Sei $0 \neq f \in R[X]$ lässt sich als Produkt von Primelemente in $K[X]$ schreiben.
Zu zeigen also: die Faktoren liegen in $R[X]$ und sind dort prim.
Vorarbeit:

Bemerkung 2.29

Für jedes Primideal $p \in R$ und alle $f, g \in K[X]$ gilt: $\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$.
Dabei wähle System $\mathcal{P}$ von Vertretern der Primelemente,
zerlege $x \in R$ als $x = e \prod_{p \in \mathcal{P}} p^{\nu_p(x)}$,
und betrachte $\nu_p(x \cdot y) = \nu_p(x) \cdot \nu_p(y)$.
für $f = \sum_{i=0}^{n} a_i X^i$ ist $\nu_p(f) = \min_{i=0}^{n} \nu_p(a_i)$
für $x = \frac{a}{b} \in K$ sei $\nu_p(x) = \nu_p(a) - \nu_p(b) \in \mathbb{Z}$.

Beweis 1. Schritt: $\text{Grad}(f) = 0$, d.h. $f = a_o \in K$, $g = \sum_{i=0}^{n} b_i X^i$
$\implies f \cdot g = \sum_{i=0}^{n} a_0 b_i X^i$.
$\nu_p(f \cdot g) = \min_{i=0}^{n} \nu_p(a_0 b_i) = \min_{i=0}^{n} (\nu_p(a_0) + \nu_p(b_i)) = \nu_p(a_0) + \min_{i=0}^{n} \nu_p(b_i) = \nu_p(f) + \nu_p(g)$
2. Schritt: Wir dürfen annehmen: $f, g \in R[X]$ primitiv.
denn: Wähle $a \in R$ mit $a \cdot f \in R[X]$ („Hauptnenner“).

Sei d in ggT der Koeffizienten von $a \cdot f = \frac{a}{d} \cdot f \in R[X]$ ist primitiv.
Seien also $a \cdot f$ und $b \cdot g$ primitiv. ($a, b \in R \setminus \{0\}$ geeignet).
Es gilt dann $\nu_p(af \cdot bg) = \nu_p(a \cdot b) + \nu_p(f \cdot g) = \nu_p(a) + \nu_p(f) + \nu_p(b) + \nu_p(g) = \nu_p(af) + \nu_p(bg)$
und daraus folgt: $\nu_p(f \cdot g) = \nu_p(g) + \nu_p(g)$.
3. Schritt: Für primitive $f, g \in R[X]$ gilt: $\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$
Sei $p \in \mathcal{P}$, ${}^{\overline{R}}\!/_{(p)} \implies \bar{f} \neq 0 \neq g$ in $\overline{R}[X] \implies \bar{f} \cdot \bar{g} \neq 0$, da $R[X]$ nullteilerfrei, also $\nu_p(f \cdot g) = 0$.
f, g primitiv $\implies \nu_p(f) = \nu_p(g) = 0$.

Weiter mit dem Beweis des Satzes von Gauß:
Stand der Dinge:
$\mathcal{P}$ Vertretersystem der Primelemente in R.
$a \in R \setminus \{0\} \implies a = e \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$
$x = \frac{a}{b} \in K = \mathrm{Quot}(R) \implies \nu_p(x) = \nu_p(a) - \nu_p(b)$.
$f = \sum_{i=0}^{n} a_i X^i \in K[X] \implies \nu_p(f) = \min\{\nu_p(a_i), i = 0, \ldots n\}$.
$f \in R[X]$ primitiv $\iff \nu_p(f) = 0$ für alle $p \in \mathcal{P}$.
Es gilt: $\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$ für alle $f, g \in K[X]$.
Sei $\widetilde{\mathcal{P}}$ Vertretersystem der Primelemente in $K[X]$.
Alle $f_i \in \widetilde{\mathcal{P}}$ seien in $P[X]$ und primitiv.
Sei nun $f \in R[X]$, $f \neq 0$.
Schreibe $f = c \cdot f_1 \cdots f_n$, $f_i \in \widetilde{\mathcal{P}}$ (mit $c \in K^\times$)
Beobachte: $c \in R$, denn für $p \in \widetilde{\mathcal{P}}$ ist $0 \leq \nu_p(f) = \nu_p(c) + \sum_{i=0}^{n} \nu_p(f_i) = \nu_p(c) \implies c \in R$.
Schreibe als $c = e \cdot p_1 \cdots p_m$ mit $e \in R^\times$ und $p_i \in \mathcal{P}$.
Noch zu zeigen:
1) $p_i \in R[X]$ ist prim.
2) f_i ist prim in $R[X]$.
Beweis 1)
Zeige ${}^{R[X]}\!/_{(p_i)}$ ist nullteilerfrei.
Da ${}^{R[X]}\!/_{(p_i)} = {}^{R[X]}\!/_{p_i R[X]} \cong \underbrace{{}^{R}\!/_{p_i R}}_{\text{nullteilerfrei}}[X]$
$\implies$ Behauptung.
Beweis 2)
Seien $g, h \in R[X]$ mit $g \cdot h \in f_i R[X] = (f_i)$
Da f_i Primelement in $K[X]$ ist, muss (z.B.) g in $f_i K[X]$ liegen.
d.h. $g = f_i \tilde{g}$ für ein $\tilde{g} \in K[X]$.
Für jedes $p \in \mathcal{P}$ ist dann
$0 \leq \nu_p(g) = \underbrace{\nu_p(f_i)}_{=0} + \nu_p(\tilde{g}) = \nu_p(\tilde{g})$
$\implies \tilde{g} \in R[X] \implies f_i$ ist prim in $R[X]$.

2.7 Moduln

Sei R kommutativer Ring mit Eins.

Definition und Bemerkung 2.30

a) Eine abelsche Gruppe $(M,+)$ zusammen mit einer Abbildung $\cdot : R \times M \to M$ heißt R-***Modul***, wenn gilt:

(i) $a(x+y) = ax + ay$

(ii) $(a+b)x = ax + bx$

(iii) $(a \cdot b)x = a \cdot (bx)$

(iv) $1 \cdot x = x$

für alle $x, y \in M$, $a, b \in R$.

Beispiele

1) R ist R-Modul (mit $\cdot$ als Ringmultiplikation)
2) Ist R ein Körper, so ist R-Modul = R-Vektorraum.
3) $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$ ist $\mathbb{Z}$-Modul durch $n \cdot \bar{0} = \bar{0}$, $n \cdot \bar{1} = n$.
   jede abelsche Gruppe A ist $\mathbb{Z}$-Modul durch $n \cdot x = \underbrace{x + \cdots + x}_{n\text{-mal}}$ für $n \in \mathbb{N}$, $x \in A$.
4) Jedes Ideal in R ist R-Modul.

b) Eine Abbildung $\varphi : M \to M'$ von R-Moduln heißt R-***Modulhomomorphismus*** (oder R-linear),

wenn φ Gruppenhomomorphismus ist und für alle $x \in M$, $a \in R$ gilt: $\varphi(ax) = a \cdot \varphi(x)$.

c) $\mathrm{Hom}_R(M, M') := \{\varphi : M \to M' : \varphi \ R\text{-linear}\}$

ist R-Modul durch $(\varphi_1 + \varphi_2)(x) = \varphi_1(x) + \varphi_2(x)$ und $(a\varphi)(x) = a\varphi(x)$ für alle $\varphi_1, \varphi_2 \in \mathrm{Hom}_R(M, M')$, $a \in R$.

d) Die R-Moduln bilden mit den R-linearen Abbildungen eine Kategorie: $\underline{R\text{-Mod}}$.

e) Die Kategorien $\underline{\mathbb{Z}\text{-Mod}}$ und $\underline{\text{AbGruppen}}$ sind isomorph.

Beweis $\varphi(n \cdot x) = \varphi(x + \cdots + x) = \varphi(x) + \cdots + \varphi(x) = n \cdot \varphi(x)$ für $\varphi : A \to A'$ Gruppenhomomorphismus, $x \in A$, $n \in \mathbb{N}$.

$\Longrightarrow$ Jeder Gruppenhomomorphismus von abelschen Gruppen ist $\mathbb{Z}$-linear.

Definition und Bemerkung 2.31

Sei M ein R-Modul.

a) Eine Untergruppe U von $(M,+)$ heißt R-Untermodul von M, wenn $R \cdot U \subseteq U$ ist. (d.h. U ist selbst R-Modul)

b) Ist $\varphi : M \to M'$ R-linear, so sind Kern(φ) und Bild(φ) Untermoduln von M bzw. M'.
(denn: $\varphi(x) = 0 \implies \varphi(ax) = 0 \ \forall a \in R, x \in M$ und $a \cdot \varphi(x) = \varphi(a \cdot x) \ \forall a \in R, x \in M$.)

c) Sei $U \subseteq M$ Untermonoid. Dann wird ${}^{M}\!/_{U}$ zu R-Modul durch $a \cdot \overline{x} = \overline{a \cdot x}$.
(denn: ist $x' \in \overline{x}$, also $x - x' \in U$, so ist $a \cdot x' = a \cdot x = a(x' - x) \in U$.)
Die Restklassenabbildung $p : M \to {}^{M}\!/_{U}$, $x \mapsto \overline{x}$ ist R-linear.
(denn: $p(a \cdot x) = \overline{a \cdot x} = a\overline{x} = a \cdot p(x)$.)

Definition und Bemerkung 2.32

Sei M ein R-Modul.

a) Für $X \subseteq M$ heißt $\langle X \rangle = \bigcap_{\substack{U \text{ Untermodul von } M \\ X \subseteq U}} U$ der von X erzeugt Untermodul.

b) $\langle X \rangle = \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in R, x \in X, n \in \mathbb{N} \right\}$

c) $B \subseteq M$ heißt ***linear unabhängig***, wenn

$$0 = \sum_{i=0}^{n} a_i b_i \text{ mit } a_i \in R, b_i \in B, n \in \mathbb{N}$$

nur möglich ist mit $a_i = 0$ für alle i.

d) $B \subseteq M$ heißt ***Basis***, wenn jedes $x \in M$ eindeutig als Linearkombination

$$x = \sum_{i=0}^{n} a_i b_i (a_i \in R, a_i \in B, n \in \mathbb{N})$$

darstellbar ist.
äquivalent: B linear unabhängig und $\langle B \rangle = M$.

e) M heißt ***freier*** R-Modul, wenn M eine Basis besitzt.

Beispiel

1) R ist freier R-Modul mit Basis 1. (oder eine andere Einheit)

2) Für jedes $n \in \mathbb{N}$ ist $R^n = R \oplus R \oplus \cdots \oplus R$ freier R-Modul mit Basis $e_1, \ldots e_n$ mit $e_i = (0, \ldots \underbrace{1}_{i\text{-te Stelle}}, \ldots 0)$.

3) Ist $I \subseteq R$ Ideal, so ist $M := {}^{R}\!/_{I} = \langle \{\bar{1}\} \rangle$.
Für $I \neq \{0\}$ ist ${}^{R}\!/_{I}$ nicht frei!
denn: sei $\bar{x} \in M$, $a \in I \setminus \{0\}$
$\implies a \cdot \bar{x} = \overline{a \cdot x} = \bar{0}$
$\implies$ in M gibt es kein linear unabhängiges Element.

Kapitel 3

Algebraische Körpererweiterungen

3.1 Grundbegriffe

Definition 3.1

Sei L ein Körper, $K \subseteq L$ Teilkörper.

a) Dann heißt L ***Körpererweiterung*** von K.
Schreibweise: L/K Körpererweiterung.

b) $[L : K] := dim_K L$ heißt ***Grad*** von L über K.

c) L/K heißt ***endlich***, wenn $[L : K] < \infty$.

d) $\alpha \in L$ heißt ***algebraisch*** über K, wenn es ein $0 \neq f \in K[X]$ gibt mit $f(\alpha) = 0$.

e) $\alpha \in L$ heißt ***transzendent*** über K, wenn α nicht algebraisch ist.

f) L/K heißt ***algebraische Körpererweiterung***, wenn jedes $\alpha \in L$ algebraisch über K ist.

Beispiele

1) Für $a \in \mathbb{Q}$ und $n \geq 2$ ist $\sqrt[n]{a}$ algebraisch über $\mathbb{Q}$,
da Nullstelle von $x^n - a$.

Summe und Produkt von solchen Wurzeln sind auch algebraisch über $\mathbb{Q}$.

z.B. $\sqrt{2} + \sqrt{3}$ ist Nullstelle von $(x^2 - 5)^2 - 24 = x^4 - 10x^2 + 1$.

2) Sei $L = K(X) = \text{Quot}(K[X])$.

Dann ist X transzendent über K.

Das gleiche gilt für jedes $f \in K(X) \setminus K$.

3) In $\mathbb{R}$ gibt es sehr viele über $\mathbb{Q}$ transzendente Elemente. $\mathbb{Q}$ ist abzählbar, also auch $\mathbb{Q}[X]$, jedes $f \in \mathbb{Q}[X]$ hat endlich viele Nullstellen $\Longrightarrow$ es gibt nur abzählbar viele Elemente in $\mathbb{R}$, die algebraisch über $\mathbb{Q}$ sind.
$\Longrightarrow$ $\mathbb{R}$ ist nicht abzählbar.

Definition und Bemerkung 3.2

Sei L/K Körpererweiterung, $\alpha \in L$.
$\varphi_\alpha : K[X] \to L$, $f \mapsto f(\alpha)$ Einsetzungshomomorphismus.

a) $\mathrm{Kern}(\varphi_\alpha)$ ist Primideal in $K[X]$.

Beweis $\mathrm{Kern}(\varphi_\alpha)$ ist Ideal, da φ_α Homomorphismus.

Seien $f, g \in K[X]$ mit $f, g \in \mathrm{Kern}(\varphi_\alpha) \Longrightarrow (f \cdot g)(\alpha) = 0 = f(\alpha) \cdot g(\alpha) \Longrightarrow f(\alpha) = 0$ oder $g(\alpha) = 0$.

b) α algebraisch $\Longleftrightarrow \mathrm{Kern}(\varphi_\alpha) \neq \{0\}$.

c) Ist α algebraisch über K, so gibt es ein eindeutig bestimmtes irreduzibeles Polynom $f_\alpha \in K[X]$ mit $f_\alpha(\alpha) = 0$ und $\mathrm{Kern}(\varphi_\alpha) = (f_\alpha)$.

f_α heißt ***Minimalpolynom*** von α.

Beweis $K[X]$ ist Hauptidealring $\Longrightarrow \widetilde{f_\alpha}$ mit $\mathrm{Kern}(\varphi_\alpha) = (\widetilde{f_\alpha})$ wegen a) ist $\widetilde{f_\alpha}$ irreduzibel, eindeutig bis auf eine Einheit in $K[X]$, also ein Element aus $K^\times$.
$\Longrightarrow \exists! \lambda \in K^\times$, so dass $\lambda \widetilde{f_\alpha} = f_\alpha$ normiert ist.

d) $K[\alpha] := \mathrm{Bild}(\varphi_\alpha) = \{f(\alpha) : f \in K[X]\} \subset L$ ist der kleinste Unterring von L, der K und α enthält.

e) α ist transzendent $\Longleftrightarrow K[\alpha] \cong K[X]$.

Beweis Folgt aus b)

f) Ist α algebraisch über K, so ist $K[\alpha]$ ein Körper und $[K[\alpha] : K] = \deg(f_\alpha)$.

Beweis Nach Homomorphiesatz ist $K[\alpha] \cong {}^{K[X]}\!/_{\mathrm{Kern}(\varphi_x)}$.

$\mathrm{Kern}(\varphi_x)$ ist maximales Ideal, da Primideal $\neq (0)$ in $K[X]$ (siehe Beweis Satz 9, Behauptung 2),
$\Longrightarrow K[\alpha]$ ist Körper.

$f_\alpha(\alpha) = 0$, also $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$
mit $c_i \in K$, $c_0 \neq 0$ (f_α irreduzibel.)
$\Longrightarrow \alpha(\alpha^{n-1} + \cdots + c_1) = -c_0$.

Genauso: $1, \alpha, \alpha^2, \alpha^{n-1}$ ist K-Basis von $K[\alpha]$.

Definition 3.3

Sei L/K Körpererweiterung.

a) Für $A \subset L$ sei $K(A)$ der kleinste Teilkörper von L, der A und K umfasst.
$K(A)$ heißt der ***von*** A ***erzeugte Teilkörper*** von L.

Es ist $K(A) = \left\{ \dfrac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} : n \geq 1, \alpha_i \in A, f, g \in K[X_1, \ldots X_n], g \neq 0 \right\}$.

b) L/K heißt ***einfach***, wenn es $\alpha \in L$ gibt mit $L = K(\alpha)$.

c) L/K heißt ***endlich erzeugt***, wenn es eine endliche Menge $\{\alpha_1, \dots \alpha_n\} \subset L$ gibt mit $L = K(\alpha_1, \dots \alpha_n)$.

Definition und Bemerkung 3.4

Für eine Körpererweiterung L/K sind äquivalent:

(i) L/K ist endlich.

(ii) L/K ist endlich erzeugt und algebraisch.

(iii) L wird von endlich vielen über K algebraischen Elementen erzeugt.

Beweis (i) $\Longrightarrow$ (ii)
Sei $[L : K] = n$, $\alpha \in L \Longrightarrow 1, \alpha, \alpha^2, \dots, \alpha^n$ sind K-linear abhängig
$\Longrightarrow \exists c_i \in K$ nicht alle 0 mit $\sum_{i=0}^{n} c_i \alpha^i = 0$.
$\Longrightarrow f(\alpha) = 0$ für $f = \sum_{i=0}^{n} c_i X^i \in K[X]$.
(ii) $\Longrightarrow$ (iii) $\surd$
(iii) $\Longrightarrow$ (i): Induktion über die Anzahl n der Erzeuger:
$n = 1$: DefBem 3.2 f).
$n > 1$: auch DefBem 3.2 f).

Bemerkung 3.5

Seien $K \subset L \subset M$ Körper.

a) Seien M/L und L/K algebraisch, so auch M/K.

b) Seien M/L und L/K endlich, so auch M/K und es gilt: $[M : K] = [M : L] \cdot [L : K]$.

Beweis a) Sei $\alpha \in M$, $f_\alpha = \sum_{i=0}^{n} c_i X^i \in L[X]$ mit $f_\alpha(\alpha) = 0$.
Dann ist α algebraisch über $K(c_0, \dots, c_n) =: L' \subset L$
L' endlich erzeugt über $K \overset{3.4}{\Longrightarrow} L'/K$ endlich.
Außerdem ist $L'(\alpha)/L'$ endlich $\overset{(a)}{\Longrightarrow} K'(\alpha)/K$ endlich
$\Longrightarrow \alpha$ algebraisch über K'.

b) Sei $b_1, \dots b_m$ K-Basis von L und $e_1, \dots e_n$ L-Basis von M.
$\Longrightarrow B = \{e_i b_j : i = 1, \dots n, j = 1, \dots m\}$ ist K-Basis von M.
denn: B erzeugt M: Sei $\alpha \in M$, $\alpha = \sum_{i=1}^{n} \lambda_i e_i$ mit $\lambda_i \in L$.
$\lambda_i = \sum_{j=1}^{n} \mu_{ij} b_j$. einsetzen $\Longrightarrow$ Behauptung.
B linear unabhängig:
Ist $\sum \mu_{ij} e_i b_j = 0$, so ist für jedes feste i: $\sum_{j=1}^{n} \mu_{ij} b_j = 0$, da die e_i über L linear unabhängig sind.
Da die b_j linear unabhängig sind, sind die $\mu_{ij} = 0$.

Beispiele $\cos(\frac{2\pi}{n})$ ist für jedes $n \in \mathbb{Z} \setminus \{0\}$ algebraisch über $\mathbb{Q}$.

denn: $\cos(\frac{2\pi}{n}) = \Re(e^{\frac{2\pi i}{n}}) = \frac{1}{2}(e^{\frac{2\pi i}{n}} + \overline{e^{\frac{2\pi i}{n}}}) = \frac{1}{2}(e^{\frac{2\pi i}{n}} + e^{-\frac{2\pi i}{n}})$

$e^{\frac{2\pi i}{n}}$ ist Nullstelle von $(x^n - 1)$, also algebraisch über $\mathbb{Q}$.

$\Longrightarrow K = \mathbb{Q}(e^{\frac{2\pi i}{n}})$ ist endliche Körpererweiterung von $\mathbb{Q}$.

$\cos(\frac{2\pi}{n}) \in K \xrightarrow{3.4\text{ (i)} \Longrightarrow \text{(ii)}} \cos(\frac{2\pi}{n})$ algebraisch.

$\mathbb{Q} \subset \mathbb{Q}(\cos(\frac{2\pi}{n})) \subsetneqq K$ $(n \geq 3)$

Notation: L/K Körpererweiterung, $\alpha \in L$

$K[\alpha] = \text{Bild}(\varphi_\alpha) = \cdots$

$K(\alpha) = \text{Quot}(K[\alpha]) = K[\alpha]$ falls α algebraisch.

3.2 Algebraischer Abschluss

Proposition und Definition 3.6 (Kronecker)

Sei K ein Körper, $f \in K[X]$.

a) Es gibt eine endliche Körpererweiterung L/K, so dass f in L eine Nullstelle hat.

Beweis Ohne Einschränkung sei f irreduzibel.

Setze $L := {}^{K[X]}\!/_{(f)}$

L ist Körper, da (f) maximales Ideal.

$\alpha = \overline{X}$ = Klasse von X in L ist Nullstelle von f.

b) Es gibt eine endliche Körpererweiterung L/K, so dass f über L in Linearfaktoren zerfällt.

Beweis Induktion über $n = \deg(f)$: $n = 1$ $\surd$.

$n > 1$: L_1 wie in a). Dann ist $f(X) = (X - \alpha) \cdot f_1(X)$ in $L_1[X]$.

$\deg(f_1) = n - 1 < n$. Also gibt es L_2/L_1, so dass $f_1(X) = \prod_{i=0}^{n-1}(X - \alpha_i)$ mit $\alpha_i \in L_2$.

Dabei ist L_2/L_1 endlich, L_1/K endlich, also L_2/K endlich.

c) L/K heißt ***Zerfällungskörper*** von f, wenn f über L in Linearfaktoren zerfällt und L über K von den Nullstellen von f erzeugt wird.

d) Für jedes $f \in K[X]$ gibt es einen Zerfällungskörper $Z(f)$.

e) Ist f irreduzibel, $n = \deg(f)$, so ist $[Z(f) : L] \leq n!$.

Beweis In a) ist $[L : K] = n = \deg(f)$ und $f = (X - \alpha)f_1$ mit $\deg(f_1) = n - 1$. Mit Induktion folgt die Behauptung.

Beispiele

1) $f \in K[X]$ irreduzibel von Grad 2.
   Dann ist $L = {}^{K[X]}\!/_{(f)}$ der Zerfällungskörper von f.
   $f(X) = (X-\alpha)(X-\beta)$ $\alpha, \beta \in L$.
   Ist $f(X) = X^2 + pX + q$, so ist $\alpha + \beta = -p$.

2) $f(X) = X^3 - 2 \in \mathbb{Q}[X]$.
   Sei $\alpha = \sqrt[3]{2} \in \mathbb{R}$ Nullstelle von f.
   In $\mathbb{Q}(\alpha)$ liegt keine weitere Nullstelle von f, da $\mathbb{Q}(\alpha) \subset \mathbb{R}$.
   $X^3 - 2 = (X-\alpha)\underbrace{(X^2 + \alpha X + \alpha^2)}_{\text{irreduzibel über } \mathbb{Q}(\alpha)}$
   $\Longrightarrow [Z(f) : \mathbb{Q}] = 6$.

3) $K = \mathbb{Q}$, p Primzahl.
   $f(X) = X^p - 1 = (X-1)\underbrace{(X^{p-1} + X^{p-2} + \cdots + X + 1)}_{f_1}$
   f_1 ist irreduzibel (Eisenstein!).
   $L = {}^{Q[X]}\!/_{(f_1)} =: \mathbb{Q}(\zeta_p)$
   $\Longrightarrow \mathbb{Q}(\zeta_p) = Z(f)$.

Definition und Bemerkung 3.7

Sei K ein Körper.

a) K heißt ***algebraisch abgeschlossen***, wenn jedes nicht-konstante $f \in K[X]$ in K eine Nullstelle hat.

b) Die folgenden Aussagen sind äquivalent:

   (i) K algebraisch abgeschlossen.

   (ii) jedes $f \in K[X]$ zerfällt über K in Linearfaktoren.

   (iii) K besitzt keine echte algebraische Körpererweiterung.

   Beweis (i) $\Longrightarrow$ (iii):

   Angenommen, L/K algebraisch, $\alpha \in L/K$, dann sei $f_\alpha \in K[X]$ das Minimalpolynom von α: f_α ist irreduzibel und hat nach Voraussetzung eine Nullstelle in K.

   $\Longrightarrow \deg(f) = 1$ Widerspruch!

   (iii) $\Longrightarrow$ (ii): $Z(f) = K$.

Satz 12

Zu jedem Körper K gibt es eine algebraische Körpererweiterung $\overline{K}/K$, so dass $\overline{K}$ algebraisch abgeschlossen ist.
$\overline{K}$ heißt ***algebraischer Abschluss*** von K.

Beweis Hauptschritt:

Es gibt algebraische Körpererweiterung K'/K, so dass jedes nicht-konstante $f \in K[X]$ in K' eine Nullstelle hat.

Dann sei $K'' = (K')'$ und weiter $K^i = (K^{i-1})'$ für $i \geq 3$.

$L := \bigcup_{i \geq 1} K^i$

Es gilt:

i) L ist Körper:

$a + b \in L$ für $a \in K^i$, $b \in K^j$, ist OE $i \leq j$. Also auch $a \in K^j$.

ii) L ist algebraisch über K.

jedes $\alpha \in L$ liegt in einem K',

K' ist algebraisch über K.

iii) L ist algebraisch abgeschlossen.

denn:

Sei $f \in L[X]$, $f = \sum_{i=0}^{n} c_i X^i$ $c_i \in L$

Also gibt es j mit $c_i \in K^j$ für $i = 0, \ldots n$.

$\Longrightarrow$ f hat Nullstelle in $(K^j)' = K^{j+1} \subset L$.

Neue Vorlesung, darum gibt's hier Überschneidungen.

Hauptschritt im Beweis

Es gibt algebraische Körpererweiterung K'/K, so dass jedes $f \in K[X]$ eine Nullstelle in K' hat.

Beweis

Für jedes $f \in K[X] \setminus K$ Sei x_f ein Symbol.

$\mathfrak{X} := \{x_f : f \in K[X] \setminus K\}$

$R := K[\mathfrak{X}]$

I sei das von allen $f(x_f)$ in R erzeugte Ideal.

Sei $m \subset R$ ein maximales Ideal mit $I \subseteq m$.

$K' := {}^{R}\!/_{m}$

K' ist Körper, K'/K ist algebraisch.
denn: K' wird über K erzeugt von den $x_f \in \mathfrak{X}$ und $f(x_f) = 0$ in K', weil $f(x_f) \in I \subseteq m$.

f hat in K' die Nullstellen (Klassen von) x_f.

Noch zu zeigen:

1. $I \neq R$
2. Es gibt maximales Ideal m mit $I \subseteq m$.

Beweis 1:
Angenommen $I = R$, also $1 \in I$.

Dann gibt es $n \geq 1$, $f_1, \dots f_n \in K[X] - f$ und $g_1, \dots g_n \in R$ mit $1 = \sum_{i=1}^{n} g_i f_i(x_{f_i})$

Sei L/K Körpererweiterung, in der jedes f_i, $i = 1, \dots n$ Nullstelle α_i hat (z.B. der Zerfällungskörper von $f_1, \dots f_n$).

Zu Beweis von 2.:

Proposition Sei R kommuntativer Ring mit 1, $I \subset R$ echtes Ideal.

Dann gibt es ein maximales Ideal m in R mit $I \subseteq m$.

Lemma von Zorn Sei $M \neq \emptyset$ geordnet.

Hat jede total geordnete Teilmenge von M eine obere Schranke, so hat M ein maximales Element.

d.h. ein $x \in M$, so dass aus $y \in M, x \leq y$ folgt $x = y$.

Zurück zum Beweis von 2.

Sei M die Menge der echten Ideale in R, die I enthalten.

$I \subseteq M$, also $M \neq \emptyset$.

Sei $N \subseteq M$ total geordnete Teilmenge.

Behauptung: $\widetilde{J} := \bigcup_{J \in N} J$ ist Element von M (und *dann* auch die Schranke für N).

denn: $I \subseteq \widetilde{J}$ $\surd$.

$\widetilde{J}$ Ideal: $x_1, x_2 \in \widetilde{J} \implies x_1 \in J_1, x_2 \in J_2$: Ohne Einschränkung $J_2 \subseteq J_1 \implies x_2 \in J_1 \implies x_1 + x_2 \in J_1 \subset J$.

genauso: $r \cdot x_1 \in J_1$ für $r \in R$.

$1 \notin \widetilde{J}$, da sonst $1 \in J$ für ein $J \in N$.

3.3 Fortsetzung von Körperhomomorphismen

Proposition 3.8

Sei $L = K(\alpha)$, K Körper (also einfache Körpererweiterung)
Sei α algebraisch über K, $f = f_\alpha \in K[X]$ das Minimalpolynom.
Sei K' Körper und $\sigma : K \to K'$ ein Körperhomomorphismus.
Sei f^σ das Bild von f in $K'[X]$ unter dem Homomorphismus
$K[X] \to K'[X]$, $\sum a_i X^i \mapsto \sum \sigma(a_i) X^i$

Dann gilt:

a) Zu jeder Nullstelle β von f^σ in K' gibt es genau einen Körperhomomorphismus $\widetilde{\sigma} : L \to K'$ mit $\widetilde{\sigma}(\alpha) = \beta$ und $\widetilde{\sigma}|_K = \sigma$.

b) Ist $\widetilde{\sigma} : L \to K'$ Fortsetzung von σ (d.h. $\widetilde{\sigma}|_K = \sigma$), so ist $\widetilde{\sigma}(\alpha)$ Nullstelle von f^σ.

Beweis b) $f^\sigma(\widetilde{\sigma}(\alpha)) = f^{\widetilde{\sigma}}(\widetilde{\sigma}(\alpha)) = \widetilde{\sigma}(f(\alpha)) = 0$

a) Eindeutigkeit: $\widetilde{\sigma}$ ist auf den Erzeugern von L festgelegt.
Existenz: $\varphi : K[X] \to K'$, $X \mapsto \beta$.
$\Longrightarrow \varphi(f) = f^\sigma(\beta) = 0$, $g = \sum a_i X^i \mapsto \sum \sigma(a_i)\beta^i = g^\sigma(\beta)$
$\overset{\text{HomSatz}}{\Longrightarrow} \varphi$ induziert $\widetilde{\sigma} : {}^{K[X]}\!/_{(f)} \to K'$ mit $L = {}^{K[X]}\!/_{(f)}$.

Folgerung 3.9

Sei $f \in K[X] \setminus K$. Dann ist der Zerfällungskörper $Z(f)$ bis auf Isomorphie eindeutig.

Beweis Seien L, L' Zerfällungskörper, $L = K(\alpha_1, \ldots, \alpha_n)$, α_i Nullstelle von f.
Sei weiter $\beta_1 \in L'$ Nullstelle von f.
Nach 3.8 gibt es ein $\sigma : K(\alpha_1) \to L'$ mit $\sigma|_K = id_K$ und $\sigma(\alpha_1) = \beta_1$ und $\tau : K(\beta_1) \to L$ mit $\tau(\beta_1) = \alpha_1$, $\tau(K) = id_K$.
So ist $\tau \circ \sigma = id_{K(\alpha_1)}$, $\sigma \circ \tau = id_{K(\beta_1)} \Longrightarrow K(\alpha_1) \cong K(\beta_1)$.
Mit Induktion über n folgt die Behauptung.

Bemerkung 3.10

Sei L/K algebraische Körpererweiterung, $\overline{K}$ ein algebraische abgeschlossener Körper, $\sigma : K \to K'$ ein Homomorphismus. Dann gibt es eine Fortsetzung $\widetilde{\sigma} : L \to \overline{K}$.

Beweis Ist L/K' endlich, so folgt die Aussage aus 3.8.
Für den allgemeinen Fall sei:
$M := \{(L', \tau) : L'/K$ Körpererweiterung, $L' \subseteq L, \tau : L' \to \overline{K}$ Fortsetzung von $\sigma\}$.
$M \neq \emptyset$: $(K, \sigma) \in M$.
M ist geordnet durch: $(L_1, \tau_1) \leq (L_2, \tau_2) :\Longleftrightarrow L_1 \subseteq L_2$ und τ_2 Fortsetzung von τ_1.
Sei $N \subset M$ total geordnet: $L^\sim := \bigcup_{(L', \tau) \in N} L'$.
$L^\sim$ ist Körper, $L^\sim \subseteq L$, $\widetilde{\tau} : L^\sim \to \overline{K}$, $\widetilde{\tau}(x) = \tau(x)$, falls $x \in L'$ und $(L', \tau) \in N$.
wohldefiniert: ist $x \in L''$, so ist ohne Einschränkung $(L', \tau) \leq (L'', \tau'')$ und damit $\tau''(x) = \tau(x)$.
$\Longrightarrow (L^\sim, \widetilde{\tau})$ ist obere Schranke.
$\overset{\text{Zorn}}{\Longrightarrow} M$ hat maximales Element $(L^\sim, \widetilde{\tau})$.
Zu zeigen: $L^\sim = L$.
Sonst sei $\alpha \in L \setminus L^\sim$ und σ' Fortsetzung von $\widetilde{\sigma}$ auf $L^\sim(\alpha)$ (nach 3.8)
$\Longrightarrow (L^\sim(\alpha), \sigma') \in M$ und $(L^\sim, \sigma) \lneqq (L^\sim, \widetilde{\sigma})$. Widerspruch!

Folgerung 3.11

Für jeden Körper k ist der algebraische Abschluss $\overline{k}$ bis auf Isomorphie eindeutig bestimmt.

Beweis Seien $\overline{k}$ und c algebraische Abschlüsse von k. Also $k \subset \overline{k}$, $k \subset c$.
Nach Prop 3.10 gibt es einen Körperhomomorphismus $\sigma : \overline{k} \to c$, der id_K fortsetzt. Dann ist $\sigma(\overline{k})$ auch algebraisch abgeschlossen:
ist $f \in \sigma(\overline{k})[X]$
$\implies f^{\sigma^{-1}} \in \overline{k}[X]$.
Sei $f = \sum a_i X^i$,
$f^{\sigma^{-1}} = \sum \sigma^{-1}(a_i)X^i$ hat Nullstelle $\alpha \in \overline{k} \implies \sigma(\alpha)$ ist Nullstelle von f.
$\sum \sigma^{-1}(a_i)\alpha^i = 0$.
$\implies 0 = \sigma(\sum \sigma^{-1}(a_i)\alpha^i) = \sum a_i \sigma(\alpha)^i$
c ist algebraisch abgeschlossen über K, also erst recht über $\sigma(\overline{k}) \overset{3.7}{\implies} \sigma(\overline{k}) = c$.

Definition und Bemerkung 3.12

Seien L/K, L'/K Körpererweiterungen von K.

a)
$$\mathrm{Hom}_K(L, L') = \{\sigma : L \to L' \text{ Körperhomomorphismus}, \sigma|_K = id_K\}$$
$$\mathrm{Aut}_K(L) = \mathrm{Aut}(L/K) = \mathrm{Hom}_K(L, L)$$

b) Ist L/K endlich, $\overline{K}$ algebraischer Abschluss von K, so ist
$$|\mathrm{Hom}_K(L, \overline{K})| \leq [L : K]$$

Beweis Sei $L = K(\alpha_1, \ldots, \alpha_n)$, α_i algebraisch über K.
Induktion über n:
$n = 1$: Sei $f \in K[X]$ das Minimalpolynom von α_1
Für jedes $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ ist $\sigma(\alpha)$ Nullstelle von $f^\sigma \in \overline{K}[X]$.
Durch $\sigma|_K = id_K$ und $\sigma(\alpha)$ ist σ eindeutig bestimmt.
$\implies |\mathrm{Hom}_K(L, \overline{K})| = |\text{Nullstellen von } f^\sigma| \leq \deg(f^\sigma) = [L : K]$

$n > 1$: Sei $L_1 = K(\alpha_1, \ldots \alpha_{n-1})$, $f \in L_1[X]$ das Minimalpolynom von α_n über L_1:
Für $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ ist $\sigma(\alpha)$ Nullstelle von $f^\sigma \in \overline{K}[X]$ mit $\sigma_1 = \sigma|_{L_1}$.
$\implies |\mathrm{Hom}_K(L, \overline{K})| \leq |\mathrm{Hom}_K(L_1, \overline{K})| \cdot \deg(f) \leq [L_1 : K] \cdot [L : L_1] \overset{3.5\text{ b)}}{=\!=} [L : K]$

3.4 Separable Körpererweiterungen

Definition und Bemerkung 3.13

Sei L/K algebraische Körpererweiterung, $\overline{K}$ algebraischer Abschluss von K.

a) $f \in K[X] \setminus K$ heißt ***separabel***, wenn f in $\overline{K}$ keine vielfache Nullstellen hat.
(also $\deg(f)$ verschiedene Nullstellen)

b) $\alpha \in L$ heißt ***separabel***, wenn das Minimalpolynom von α über K separabel ist.

c) L/K heißt ***separabel***, wenn jedes $\alpha \in L$ separabel ist.

d) $f \in K[X] \setminus K$ ist genau dann separable, wenn $\mathrm{ggT}(f, f') = 1$.
Dabei ist für $f = \sum_{i=0}^{n} a_i X^i$, $f' = \sum_{i=0}^{n} i a_i X^{i-1}$

e) Ist $f \in K[X]$ irreduzibel, so ist f separabel genau dann, wenn $f' \neq 0$ ist.

Beweis d) Sei $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$, $\alpha_i \in \overline{K}$.

$\Longrightarrow f'(X) = \sum_{i=1}^{n} \prod_{i \neq j}(X - \alpha_i)$

Nach Definition ist f separabel $\Longleftrightarrow \alpha_i \neq \alpha_j$ für $i \neq j$.

Behauptung: $\alpha_1 = \alpha_i$ für ein $i \geq 2 \Longleftrightarrow (X - \alpha_1) \mid f'$ (teilt)

Aus der Behauptung folgt: f separabel $\Longleftrightarrow f$ und f' teilerfremd in $\overline{K}[X]$.

Ist das so, dann ist $\mathrm{ggT}(f, f') = 1$ (teilerfremd in $K[X]$).

Ist umgekehrt $\mathrm{ggT}(f, f') = 1$, so gibt es $g, h \in K[X]$ mit $1 = g \cdot f + h \cdot f'$

Das stimmt dann auch in $\overline{K}[X]$, also sind f und f' auch in $\overline{K}[X]$ teilerfremd.

Beweis der Behauptung: $(X - \alpha_i)$ teilt $\prod_{j \neq i}(X - \alpha_j)$ falls $i \neq 1$.

Also gilt: $X - \alpha_i$ teilt $f' \Longleftrightarrow X - \alpha_1$ Teiler von $\prod_{j \neq 1}(X - \alpha_j) \Longleftrightarrow \alpha_1 = \alpha_j$, für ein $j \neq 1$.

e) Ist $f' = 0$, so ist $\mathrm{ggT}(f, f') = f \neq 1$.

Ist $f' \neq 0$, so ist $\deg(f') < \deg(f)$

Ist f irreduzibel und $\alpha \in \overline{K}$ Nullstelle von f, so ist f das Minimalpolynom von $\alpha \overset{f' \neq 0}{\Longrightarrow} \alpha$ nicht Nullstelle von f'.

$\Longrightarrow \mathrm{ggT}(f, f') = 1$.

Folgerung 3.14

Ist $\mathrm{char}(K) = 0$, so ist jede algebraische Körpererweiterung von K separabel.

Beispiele 3.15

Sei p Primzahl, $K = \mathbb{F}_p(t) = \mathrm{Quot}(\mathbb{F}_p[t])$
Sei $f(X) = X^p - t \in K[X]$.
$f'(X) = pX^{p-1} = 0$, $t \in \mathbb{F}_p[t]$ ist Primelement.
$\overset{\text{Eisenstein}}{\Longrightarrow} f$ irreduzibel in $(\mathbb{F}_p[t])[X]$.
$\overset{\text{Folg 2.28}}{\Longrightarrow} f$ irreduzibel in $K[X]$.
$f(X) = X^p - a \in \mathbb{F}_p[X] \Longrightarrow f' = 0$
Frage: Ist f irreduzibel? Nein!
Denn f hat Nullstelle in $\mathbb{F}_p$, d.h. es gibt ein $b \in \mathbb{F}_p$ mit $b^p = a$,
denn $\varphi : \mathbb{F}_p \to \mathbb{F}_p, b \mapsto b^p$ ist Körperhomomorphismus!!!
denn: $(a + b)^p = a^p + b^p$! (siehe $\sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$)
Definition: φ heißt ***Frobenius***-Automorphismus.

Bemerkung 3.16

Sei $\text{char}(K) = p > 0$, $f \in K[X]$ irreduzibel.

a) Es gibt ein separabeles irreduzibeles Polynom $g \in K[X]$, so dass

$$f(X) = g(X^{p^r})$$

für ein $r \geq 0$.

b) Jede Nullstelle von f in $\overline{K}$ hat Vielfachheit p^r.

Beweis Sei f nicht separabel.
$f = \sum a_i X^i$, $f' = i a_i X^{i-1} = 0$
$\Longrightarrow$ $ia_i = 0$ für $i = 1, \ldots n$.
$\Longrightarrow$ $a_i = 0$ falls i nicht durch p teilbar.
$\Longrightarrow$ f ist Polynom in X^p, d.h. $f = g_1(X^p)$
Mit Induktion folgt die Behauptung.

Satz 13

Sei L/K endliche Körpererweiterung, $\overline{K}$ algebraischer Abschluss von L.

a) $[L : K]_S := |\,\text{Hom}_K(L, \overline{K})|$ heißt ***Separabilitätsgrad*** von L über K.

b) Ist L' Zwischenkörper von L/K, so ist

$$[L : K]_S = [L : L']_S \cdot [L' : K]_S$$

c) L/K ist separabel $\Longleftrightarrow$ $[L : K] = [L : K]_S$.

d) Ist $\text{char}(K) = p > 0$, so gibt es ein $r \in \mathbb{N}$ mit

$$[L : K] = p^r \cdot [L : K]_S$$

Beweis b) Sei $\text{Hom}_K(L', \overline{K}) = \{\sigma_1, \ldots \sigma_n\}$, $\text{Hom}_{L'}(L, \overline{K}) = \{\tau_1, \ldots \tau_m\}$.
Sei $\overline{\sigma}_i : \overline{K} \to \overline{K}$ Fortsetzung von σ_i, $i = 1, \ldots n$.
Dann ist $\overline{\sigma}_i \in \text{Aut}_K(\overline{K})$
Behauptung
1) $Hom_K(L, \overline{K}) = \{\overline{\sigma}_i \circ \tau_j : i = 1, \ldots n, j = 1, \ldots m\}$
2) $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_{i'} \circ \tau_{j'} \Longleftrightarrow i = i'$ und $j = j'$.
Aus 1) und 2) folgt b).

Beweis 1)
„$\supseteq$“ $\surd$.
„$\subseteq$“: Sei $\sigma \in \text{Hom}_K(L, \overline{K})$
Dann gibt es ein i mit $\sigma|_{L'} = \sigma_i$.
$\Longrightarrow$ $\overline{\sigma}_i^{-1} \circ \sigma = id_{L'} \Longrightarrow \exists j$ mit $\overline{\sigma}_i^{-1} \circ \sigma = \tau_j \Longrightarrow \sigma = \overline{\sigma}_i \circ \tau_j$.

Beweis 2)

Sei $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_{i'} \circ \tau_{j'}$

$\Longrightarrow \underbrace{\overline{\sigma}_i|_{L'}}_{=\sigma_i} = \underbrace{\overline{\sigma}_{i'}|_{L'}}_{=\sigma_{i'}} \Longrightarrow i = i' \Longrightarrow \tau_j = \tau_{j'} \Longrightarrow j = j'.$

c) „$\Longrightarrow$“ Sei $L = K(\alpha_1, \dots \alpha_n)$ separabel, endlich und α_i algebraisch.

Induktion über n:

$n = 1$: $L = K(\alpha)$, $f = f_\alpha \in K[X]$ das Minimalpolynom von α über K.

$\Longrightarrow [L : K]_S \overset{3.12}{=\!=} |\{\text{Nullstellen von } f \text{ in } \overline{K}\}| = \deg(f) = [L : K]$

$n > 1$: $L_1 := K(\alpha_1, \dots \alpha_{n-1})$, $f \in L_1[X]$ das Minimalpolynom von α_n.

Zu jedem $\sigma_1 \in \mathrm{Hom}_K(L_1, \overline{K})$ und jeder Nullstelle von f in $\overline{K}$ gibt es genau eine Fortsetzung $\overline{\sigma}_1 : L \to \overline{K}$.

$\overset{f \text{ separabel}}{=\!=\!=\!\Longrightarrow} [L : K]_S = |\operatorname{Hom}_K(L, \overline{K})| = (\deg f) \cdot |\operatorname{Hom}_K(L_1, \overline{K})|$

$= [L : L_1] \cdot [L_1 : K]_S \overset{\text{I.V.}}{=\!=} [L : L_1] \cdot [L_1 : K] = [L : K]$

„$\Longleftarrow$“ Ist $\mathrm{char}(K) = 0$, so ist L/K separabel.

Sei also $\mathrm{char}(K) = p > 0$ und $\alpha \in L$, $f \in K[X]$ das Minimalpolynom von α.

Nach 3.16 gibt es $r \geq 0$ und separabeles irreduzibeles $g \in K[X]$ mit $f(X) = f(X^{p^r})$

$\Longrightarrow [K(\alpha) : K]_S = |\{\text{Nullstellen von } f \text{ in } \overline{K}\}|$

$= |\{\text{Nullstelle von } g \text{ in } \overline{K}\}| \overset{g \text{ separabel}}{=\!=\!=} \deg(g)$

$\Longrightarrow [K(\alpha) : K] = \deg(f) = p^r \deg(g) = p^r [K(\alpha) : K]_S$

$\Longrightarrow [L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] \geq [L : K(\alpha)]_S \cdot p^r [K(\alpha) : K]_S = [L : K]_S \cdot p^r.$

$\Longrightarrow p^r = 1 \Longrightarrow g = f \Longrightarrow \alpha$ separabel.

d) Folgt aus der Gleichung ein paar Zeilen hierdrüber.

Satz 14 (Satz vom primitiven Element)

Jede endliche separable Körpererweiterung L/K ist einfach.

Beweis Ist K endlich, so folgt aus Paragraph 5, dass $L^\times$ zyklische Gruppe ist.
Ist $L^\times = \langle \alpha \rangle$, so ist $L = K[\alpha]$.
Sei also K unendlich, $L = K(\alpha_1, \dots \alpha_r)$. Ohne Einschränkung $r = 2$, also $L = K(\alpha, \beta)$.
Sei $\overline{K}$ algebraischer Abschluss von L, $[L : K] = n$
Sei $\mathrm{Hom}_L(L, \overline{K}) = \{\sigma_1, \dots \sigma_n\}$ (Satz 13 c)
Sei $g(X) = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha) - (\sigma_i(\beta) - \sigma_j(\beta)) \cdot X) \in K[X]$.
$g \neq 0$, denn aus $\sigma_i(\alpha) = \sigma_j(\alpha)$ und $\sigma_i(\beta) = \sigma_j(\beta)$ folgt $\sigma_i = \sigma_j$.
Da K unendlich ist, gibt es $\lambda \in K$ mit $g(\lambda) \neq 0$.
Behauptung $\gamma := \alpha + \lambda\beta \in L$ erzeugt L über K.
denn: Sei $f \in K[X]$ das Minimalpolynom von γ über K.
Für jedes i ist $f(\sigma_i(\gamma)) \overset{\sigma_i|_K = id_K}{=\!=\!=} \sigma_i(f(\gamma)) = 0.$

Angenommen $\sigma_i(\gamma) = \sigma_j(\gamma)$ für ein $i \neq j$.
Dann wäre $\sigma_i(\alpha) + \sigma_i(\beta)\lambda - (\sigma_j(\alpha) + \sigma_j(\beta)\lambda) = 0$.
$\Longrightarrow$ $g(\lambda) = 0$ Widerspruch! $\Longrightarrow$ f hat mindestens n Nullstellen.
$\Longrightarrow$ $\deg(f) = [K(\gamma) : K] \geq n = [L : K]$
Da $\gamma \in L$ folgt $K(\gamma) = L$.

3.5 Endliche Körper

Proposition 3.17

Ist K ein Körper, so ist jede endliche Untergruppe von $(K^\times, \cdot)$ zyklisch.

Beweis Sei $K \subseteq K^\times$ endliche Untergruppe, $a \in G$ ein Element maximaler Ordnung.
Sei $n = \text{ord}(a)$, $G_n := \{b \in G : \text{ord}(b) \mid n\}$
Behauptung: $G_n = \langle a \rangle$
denn: jedes $b \in G_n$ ist Nullstelle von $X^n - 1$.
Diese sind $1, a, a^2, \ldots a^{n-1}$ $\Longrightarrow$ $|G_n| = |\langle a \rangle| = n$.
Nach Satz 3 ist $G \cong \bigoplus_{i=1}^{r} \mathbb{Z}/a_i\mathbb{Z}$ mit $a_i \mid a_{i+1}$.
$\Longrightarrow$ Für jedes $b \in G$ ist $\text{ord}(b)$ Teiler von a_r.

Satz 15

Sei p Primzahl, $n \geq 1$, $q = p^n$
Sei $\mathbb{F}_q$ der Zerfällungskörper von $X^q - X \in \mathbb{F}_p[X]$.
Dann gilt:

a) $\mathbb{F}_q$ hat q Elemente.

b) Zu jedem endlichen Körper K gibt es ein $q = p^n$ mit $K \cong \mathbb{F}_q$.

Beweis a) $f(X) = X^q - X$ ist separabel, da $f'(X) = -1$ $\Longrightarrow$ $\text{ggT}(f, f') = 1$.
$\Longrightarrow$ f hat q verschiedene Nullstellen in $\mathbb{F}_q$
$\Longrightarrow$ $|\mathbb{F}_q| \geq q$.
Umgekehrt: jedes $a \in \mathbb{F}_q$ ist Nullstelle von f,
denn: $\mathbb{F}_q$ wird erzeugt von den Nullstellen von f. Sind a,b Nullstellen von f, so ist $a^q = a$, $b^q = b$, also auch $(ab)^q = ab$, $(a + b)^q = a^q + b^q = a + b$.

b) $K^\times$ ist Gruppe (mit $\cdot$) der Ordnung $q - 1$.
$\Longrightarrow$ Für jedes $a \in K$ gilt $a^q = a$.
$\Longrightarrow$ Jedes $a \in K$ ist Nullstelle von $X^q - X$.
$\Longrightarrow$ K enthält den Zerfällungskörper von $X^q - X$.
$\Longrightarrow$ K enthält $\mathbb{F}_q$ (bis auf Isomorphie)
$\Longrightarrow$ $K \cong \mathbb{F}_q$ (da $|K| = |\mathbb{F}_q| = q$)

Folgerung 3.18

Jede algebraische Erweiterung eines endlichen Körpers ist separabel.

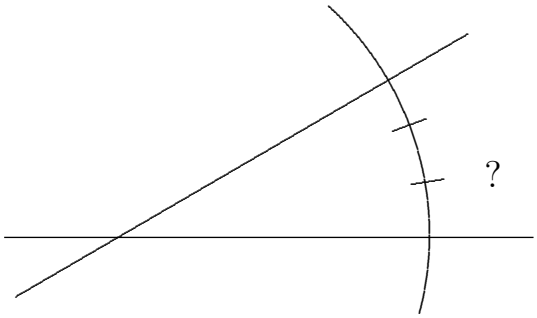
Beweis $\mathbb{F}_q/\mathbb{F}_p$ ist separabel, da $X^q - X$ separabeles Polynom ist. Ist K endlich, also $K = \mathbb{F}_q$, L/K algebraisch, $\alpha \in L$, so ist $K(\alpha)/K$ endlich, also separabel (da $K(\alpha) = \mathbb{F}_{q^r}$ für ein $q \geq 1$).

Definition Ein Körper K heißt ***vollkommen*** (perfekt), wenn jede algebraische Körpererweiterung L/K separabel ist.

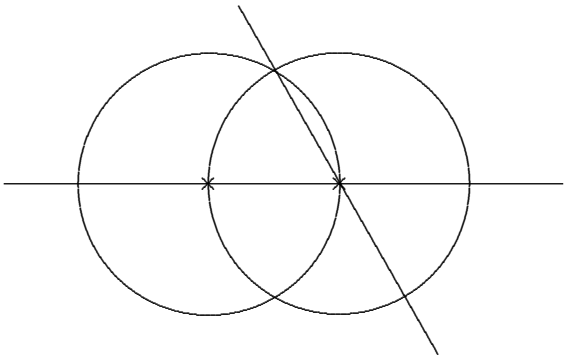
3.6 Konstruktion mit Zirkel und Lineal

Anregungen:

Dreiteilung eines Winkels?



Was lässt sich mit zwei Startpunkten konstruieren?



Aufgabe der Konstruktion mit Zirkel und Linear

Sei $M \subset \mathbb{C} = \mathbb{R}^2$, z.B. $M = \{0, 1\}$ Startpunkte.

Was können wir in einem Schritt konstruieren?

$\mathcal{L}(M) := \{L \subset \mathbb{R}^2 \text{ Gerade} : |L \cap M| \geq 2\} \cup \{K_{|z_1 - z_2|}(z_3) : z_1, z_2, z_3 \in M\}$

wobei $K_r(z) = \{y \in \mathbb{C} : |z - y| = r\}$

Also ergibt das die neue Menge

$K_1(M) := \{z \in \mathbb{C} : z \text{ liegt auf 2 verschiedenen Linien in } \mathcal{L}(M)\}$

$K_n(M) = K_1(K_{n-1}(M))$ für $n \geq 2$.

Beobachtung: $K \subseteq K_1(M)$, falls $|M| \geq 2$

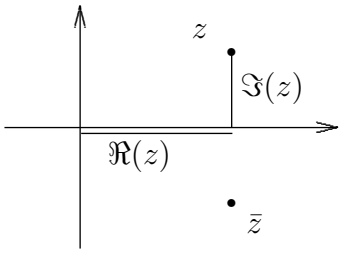
also: $K(M) = \bigcup_{n=1}^{\infty} K_n(M)$

Ab jetzt: $0, 1 \in M$, M symmetrisch zur x-Achse. (d.h. für $z \in M$ ist auf $\bar{z} \in M$)

Bemerkung 3.19

Für jedes $z \in K_1(M)$ ist $[\mathbb{Q}(M)(z) : \mathbb{Q}(M)] \leq 2$.

Beweis Vorüberlegung: Für $z \in M$ ist $\Re(z) = \frac{1}{2}(z + \bar{z}) \in \mathbb{Q}(M)$ und $\Im(z) = \frac{1}{2}(z - \bar{z})$.



(i) z ist Schnittpunkt zweier Geraden in $\mathcal{L}(M)$

$\Longrightarrow$ z ist Lösung zweier linearer Gleichungen: $z_1 + \lambda z_2 = z_1' + \mu z_2'$ mit $\lambda, \mu \in \mathbb{R}$.

(ii) z ist Schnittpunkt einer Gerade und eines Kreises: $\rightsquigarrow$ quadratische Gleichung mit Koeffizienten in $\mathbb{Q}(M)$.

(iii) z ist Schnittpunkt der Kreise $K_{r_1}(m_1)$ und $K_{r_2}(m_2)$ mit Mittelpunkten $m_1, m_2 \in M$.

Radius: $r_1 = |z_1 - z_1'|$, $r_2 = |z_2 - z_2'|$ also $r_1^2 = (z_1 - z_1')\overline{(z_1 - z_1')} \in \mathbb{Q}(M)$.

Dann ist $|z - m_1|^2 = r_1^2$
$\Longrightarrow$ $z\overline{z} - (z\overline{m_1} + \overline{z}m_1) = r_1^2 - m_1\overline{m_1}$ (1)
und $z\overline{z} - (z\overline{m_2} + \overline{z}m_2) = r_2^2 - m_2\overline{m_2}$
$\Longrightarrow$ $2\Re[z(\overline{m_1} - \overline{m_2})] = r_1^2 - r_2^2 - (m_1\overline{m_1} - m_2\overline{m_2})$

Das ist eine lineare Gleichung, die $\Re(z)$ und $\Im(z)$ enthält. Einsetzen in (1) gibt eine quadratische Gleichung für $\Re(z)$ mit Koeffizienten in $\mathbb{Q}(M)$.

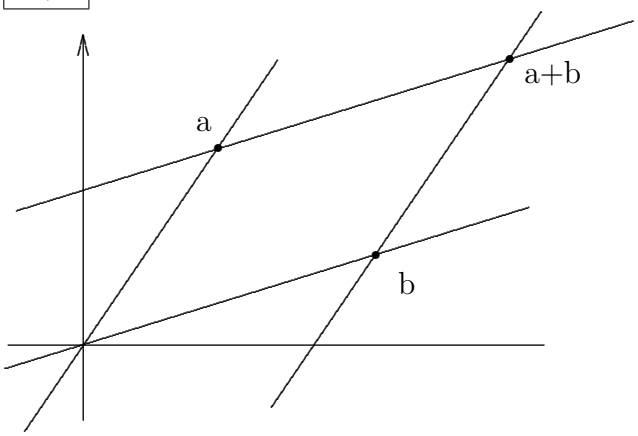
Satz 16

a) $K(M)$ ist algebraische Körpererweiterung von $\mathbb{Q}(M)$.

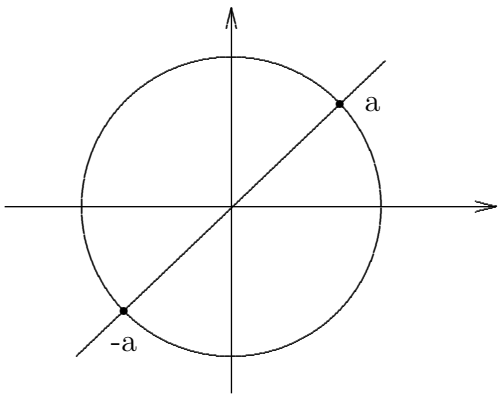
b) Sei $L/\mathbb{Q}(M)$ endliche Körpererweiterung. Gibt es $n \geq 0$
und Körper $\mathbb{Q}(M) = L_0 \subset L_1 \subset \cdots \subset L_n = L$ mit $[L_i : L_{i-1}] = 2$ für $i = 1, \ldots n$,
dann ist $L \subseteq K(M)$.

Beweis a) Seien $a, b \in K(M)$. Zu zeigen ist $a + b, -a, a \cdot b, \frac{1}{a}$ in $K(M)$.

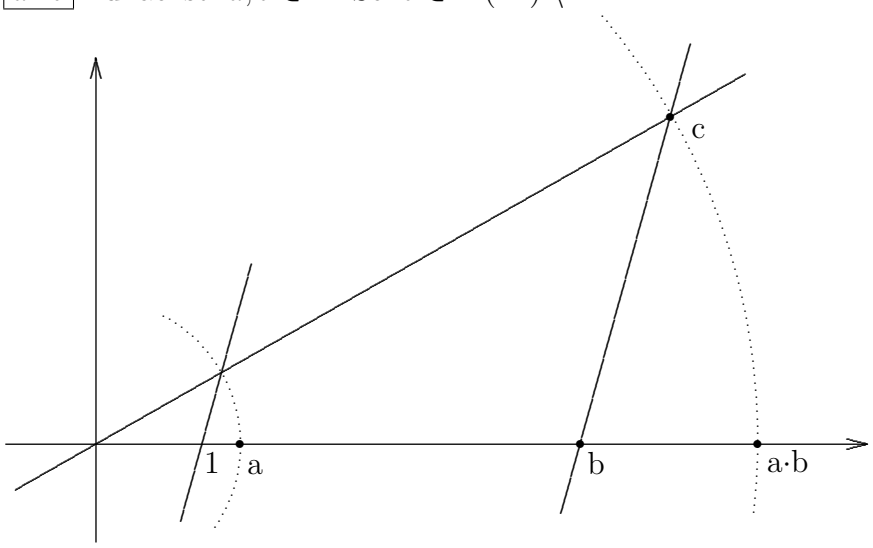
$\boxed{a+b}$



$\boxed{-a}$



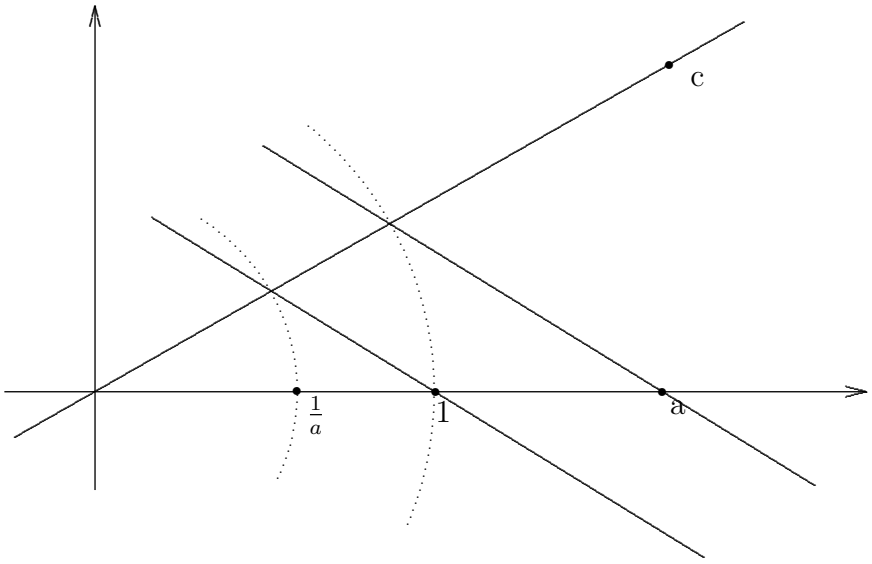
$\boxed{a \cdot b}$ Zunächst: $a, b \in \mathbb{R}$. Sei $b \in K(M) \setminus \mathbb{R}$:



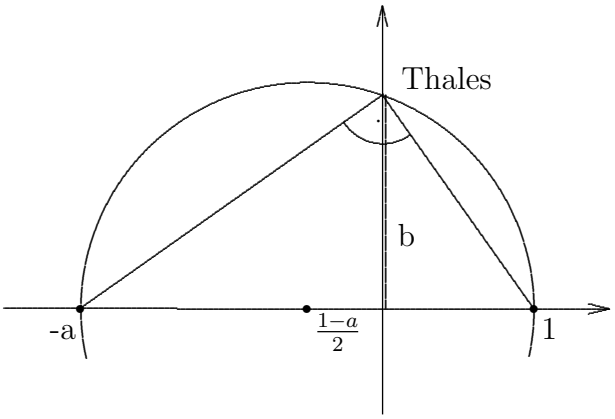
Der Strahlensatz:$\frac{1}{a} = \frac{b}{x}$. Also $x = a \cdot b$.

Winkel addieren. $\surd$. $\Longrightarrow$ $a \cdot b$ allgemein. $\surd$.

$\boxed{\frac{1}{a}}$ Ohne Einschränkung $a \in \mathbb{R}$:



b) Wurzelziehen: Sei $a \in \mathbb{R}$:



Nach dem Höhensatz ist dann: $b^2 = |-a| \cdot 1 = a$

Kapitel 4

Galois-Theorie

4.1 Der Hauptsatz

Definition und Proposition 4.1

Sei L/K algebraische Körpererweiterung.

a) L/K heißt ***normal***, wenn es eine Familie $\mathcal{F} \subset K[X]$ gibt, so dass L Zerfällungskörper von $\mathcal{F}$ ist.

b) Ist L/K normal, so ist $\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Aut}_K(L)$.
(wobei $\overline{K}$ algebraischer Abschluss von L sei.)

Beweis „$\supseteq$“ gilt immer.

„$\subseteq$“ Sei $L = Z(\mathcal{F})$, $f \in \mathcal{F}$, $\alpha \in L$ Nullstelle von f.
$\Longrightarrow$ Für jedes $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ ist $\sigma(\alpha)$ auch Nullstelle von f:

Sei $f(X) = \sum_{i=0}^{n} a_i X^i \Longrightarrow 0 = \sigma(f(\alpha))$

$$= \sum_{i=0}^{n} \underbrace{\sigma(a_i)}_{=a_i,\ \text{da } a_i \in K} \sigma(\alpha)^i = f(\sigma(\alpha)).$$

$\Longrightarrow \sigma(\alpha) \in L$.

L wird von den Nullstellen der $f \in \mathcal{F}$ erzeugt.
$\Longrightarrow \sigma(L) \subseteq L$.

c) L/K heißt ***galoissch*** (Galois-Erweiterung), wenn L/K normal und separabel ist.

d) Ist L/K galoissch, so heißt $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ die ***Galoisgruppe*** von L/K.

e) Eine endliche Erweiterung L/K ist genau dann galoissch, wenn

$$|\mathrm{Aut}_K(L)| = [L : K]$$

Beweis „$\Rightarrow$“ Aus b) folgt
$|\mathrm{Aut}_K(L)| = |\mathrm{Hom}_K(L, \overline{K})| \overset{\text{Def.}}{=\!=} [L : K]_S \overset{\text{sep. und Satz 13}}{=\!=\!=\!=\!=} [L : K]$. $(*)$
„$\Leftarrow$“ Es gilt stets: $|\mathrm{Aut}_K(L)| \leq [L : K]_S \leq [L : K]$

Aus $|\operatorname{Aut}_K(L)| = [L:K]$ folgt also $[L:K]_S = [L:K] \Longrightarrow L/K$ separabel.

$\overset{\text{Satz 14}}{\Longrightarrow} L = K(\alpha)$ für ein $\alpha \in L$, sei $f \in K[X]$ das Minimalpolynom von α.

Sei $\beta \in \overline{K}$ Nullstelle von f.

Nach 3.8 gibt es $\sigma \in \operatorname{Hom}_K(L, \overline{K})$ mit $\sigma(\alpha) = \beta$.

Wegen $(*)$ ist $\sigma \in \operatorname{Aut}_K(L) \Longrightarrow \beta \in L$.

$\Longrightarrow L$ ist Zerfällungskörper von f.

f) Ist L/K galoissch und E ein Zwischenkörper, so ist L/E galoissch und $\operatorname{Gal}(L/E) \subseteq \operatorname{Gal}(L/K)$.

Beweis L/E normal, da Zerfällungskörper von $\mathcal{F} \subset K[X] \subset E[X]$
L/E separabel, da L/K separabel.

g) Ist in f) zusätzlich auch E/K galoissch, so ist

$$\begin{array}{ccccccccc} 1 & \to & \operatorname{Gal}(L/E) & \to & \operatorname{Gal}(L/K) & \overset{\beta}{\to} & \operatorname{Gal}(E/K) & \to & 1 \\ & & & & \sigma & \mapsto & \sigma|_E & & \end{array}$$

exakt.

[also $\operatorname{Gal}(E/K) = {}^{\operatorname{Gal}(L/K)}\!/_{\operatorname{Gal}(L/E)}$]

Beweis Für $\sigma \in \operatorname{Gal}(L/K) = \operatorname{Aut}_K(L)$ ist $\sigma|_E : E \to L$,
also $\sigma \in \operatorname{Hom}_K(E, L) \subseteq \operatorname{Hom}_K(E, \overline{K}) = \operatorname{Aut}_K(E)$, da E/K galoissch.

$\Longrightarrow \beta$ ist wohldefiniert.

β *surjektiv*: Sei $\sigma \in \operatorname{Gal}(E/K)$

Nach 3.10 lässt sich σ fortsetzen zu $\widetilde{\sigma} : L \to \overline{K}$, $\widetilde{\sigma} \in \operatorname{Hom}_K(L, \overline{K}) = \operatorname{Aut}_K(L) = \operatorname{Gal}(L/K)$ und $\beta(\widetilde{\sigma}) = \widetilde{\sigma}|_E = \sigma$.

$\operatorname{Kern}(\beta) = \{\sigma \in \operatorname{Gal}(L/K) : \sigma|_E = id_E\} = \operatorname{Aut}_E(L) = \operatorname{Gal}(L/E)$

Satz 17 (Hauptsatz der Galoistheorie)

Sei L/K endliche Galois-Erweiterung.

a) Die Zuordnung

$$\begin{array}{ccc} \{\text{Zwischenkörper von } L/K\} & \overset{\Psi}{\underset{\Phi}{\longleftrightarrow}} & \{\text{Untergruppen von } \operatorname{Gal}(L/K)\ \} \\ E & \mapsto & \operatorname{Gal}(L/E) \\ L^H := \{\alpha \in L : \sigma(\alpha) = \alpha \forall \sigma \in H\} & \hookleftarrow & H \end{array}$$

sind bijektiv und zueinander invers.

b) Ein Zwischenkörper E von L/K ist genau dann galoissch über K, wenn $\operatorname{Gal}(L/E)$ Normalteiler in $\operatorname{Gal}(L/K)$ ist.

Beweis a) L^H ist Zwischenkörper (liegt daran, dass $\sigma \in$ Aut Körperhomomorphismus ist). $\surd$.

„$\underline{\Psi \circ \Phi = id}$“: Sei $H \subseteq \mathrm{Gal}(L/K)$ Untergruppe.

Zu zeigen: $\mathrm{Gal}(L/L^H) = H$.

„$\supseteq$“ Nach Definition von L^H.

„$\subseteq$“ Nach 4.1 e) ist $|\mathrm{Gal}(L, L^H)| = [L : L^H]$

Genügt also zu zeigen: $[L : L^H] \leq |H|$.

Sei $\alpha \in L$ primitives Element von L/L^H also $L = L^H(\alpha)$.

Sei $f := \prod_{\sigma \in H}(X - \sigma(\alpha)) \in L[X]$

dann ist $\deg(f) = |H|$.

Für jedes $\tau \in H$ ist $f^\tau = f$ (mit σ durchläuft auch $\tau \cdot \sigma$ alle Elemente von H)

$\Longrightarrow f \in L^J[X] \Longrightarrow$ Das Minimalpolynom g von α über L^H ist Teiler von f.

$\Longrightarrow [L : L^H] = \deg(g) \leq \deg(f) = |H|$.

„$\underline{\Phi \circ \Psi = id}$“: Sei E Zwischenkörper, $H := \mathrm{Gal}(L/E)$.

Zu zeigen: $E = L^H$.

„$\subseteq$“ Folgt aus der Definition der Symbole.

„$\supseteq$“ Da L^H/E separabel ist, genügt es zu zeigen: $[L^H : E]_S = 1$.

Sei $\sigma \in \mathrm{Hom}_E(L^H, \overline{K})$, Fortsetzung $\widetilde{\sigma} \in \mathrm{Hom}_E(L, \overline{K}) = \mathrm{Aut}_E(L) = \mathrm{Gal}(L, E) = H$.

$\Longrightarrow \sigma = \widetilde{\sigma}_{L^H} = id_{L^H}$

b) „$\Rightarrow$“ siehe 4.1 g)

„$\Leftarrow$“ Sei $H := \mathrm{Gal}(L/E)$ Normalteiler in $\mathrm{Gal}(L/K)$

Wegen 4.1 e) genügt es zu zeigen:

Für jedes $\sigma \in \mathrm{Hom}_K(E, \overline{K})$ ist $\sigma(E) \subseteq E$.

Sei also $\sigma \in \mathrm{Hom}_K(E, \overline{K})$, Fortsetzung $\widetilde{\sigma} \in \mathrm{Hom}_K(L, \overline{K}) = \mathrm{Gal}(L, K)$.

Sei nun $\alpha \in E, \tau \in H$.

Dann ist $\tau(\sigma(\alpha)) = (\tau \circ \widetilde{\sigma})(\alpha) = (\widetilde{\sigma} \circ \tau')(\alpha)$ mit $\widetilde{\sigma}^{-1} \circ \tau \circ \widetilde{\sigma} =: \tau^{-1} \in H$ nach Voraussetzung.

$= \widetilde{\sigma}(\alpha) = \sigma(\alpha)$

$\Longrightarrow \sigma(\alpha) \in L^H \overset{\text{a)}}{=\!=} E$.

Folgerung 4.2

Sei L/K endliche Galoiserweiterung

Dann gilt für Zwischenkörper E, E' bzw. Untergruppen H, H' von $\mathrm{Gal}(L/K)$

a) $E \subseteq E' \Longleftrightarrow \mathrm{Gal}(L/E) \supseteq \mathrm{Gal}(L/E')$

b) $\mathrm{Gal}(L/(E \cap E')) = \langle \mathrm{Gal}(L/E), \mathrm{Gal}(L/E') \rangle$

Beweis Im Tutorium?

Folgerung 4.3

Zu jeder endlichen separabelen Körpererweiterung gibt es nur endlich viele Zwischenkörper.

Beweis Ist L/K endliche Galoiserweiterung, so entsprechen die Zwischenkörper bijektiv den Untergruppen der endlichen Gruppen $\mathrm{Gal}(L/K)$.
Im Allgemeinen ist $L = K(\alpha)$ (Satz 14), sei also f das Minimalpolynom von α über K.
f ist separabel, da L/K separabel ist.
Sei $\widetilde{L}$ der Zerfällungskörper von f über K
$\Longrightarrow$ $\widetilde{L}/K$ ist galoissch, $K \subseteq L \subseteq \widetilde{L} \Longrightarrow$ L/K hat nur endlich viele Zwischenkörper.
[$\widetilde{L}$ sogar minimale galoissche Erweiterung]

Proposition 4.4

Sei L ein Körper, $G \subset \mathrm{Aut}(L)$ eine endliche Untergruppe.
$K := L^G = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ für alle } \sigma \in G\}$
Dann ist L/K Galoiserweiterung und $\mathrm{Gal}(L/K) = G$.

Beweis K ist Körper: $\surd$
L/K ist algebraisch und separabel.
Sei $\alpha \in L$: $\{\sigma(\alpha) : \sigma \in G\} = G \cdot \alpha$ ist endlich.
Sei $G \cdot \alpha = \{\sigma_1(\alpha), \ldots, \sigma_r(\alpha)\}$ mit $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ für $i \neq j$ und $\sigma_1 = id_L$
Dabei ist r ein Teiler von $n = |G|$
Sei $f_\alpha(X) = \prod_{i=1}^{r}(X - \sigma_i(\alpha)) \in L[X]$
Zu zeigen: $f_\alpha \in K[X]$
denn: Für $\sigma \in G$ ist $f_\alpha^\sigma(X) = \prod_{i=1}^{r}(X - \sigma\sigma_i(\alpha))$
$\Longrightarrow$ $f_\alpha = f_\alpha^\sigma \Longrightarrow$ $f_\alpha \in K[X]$
$\Longrightarrow$ α algebraisch, α separabel (da f_α separabeles Polynom),
$(*)$ $[K(\alpha) : K] \leq n$.

- L/K normal: Der Zerfällungskörper von f_α ist in L enthalten.
  $\Longrightarrow$ L ist Zerfällungskörper der Familie $\{f_\alpha : \alpha \in L\}$
- L/K ist endlich. Sei $(\alpha_i)_{i \in I}$ Erzeugendensystem von L/K
  Für jede endliche Teilmenge $I_0 \subseteq I$ ist $K(\{\alpha_i : i \in I_0\})$ endlich über K,
  also $K(\{\alpha_i : i \in I_0\}) = K(\alpha_0)$ für ein $\alpha_0 \in L$.
  $\overset{(*)}{\Longrightarrow}$ $[K(\{\alpha_i : i \in I_0\}) : K] \leq n$.
  Sei $I_1 \subseteq I$ endlich, so dass $K(\{\alpha_i : i \in I_1\})$ maximal unter den $K(\{\alpha_j : j \in J\})$ für $J \subseteq I$ endlich.
  Annahme: $K_1 \neq L$
  Dann gibt es $i \in I$ und $\alpha_i \notin K_1$
  $\Longrightarrow$ $K_1(\alpha_i) \supsetneq K_1$, trotzdem endlich.
  im Widerspruch zur Wahl von K_1.
  $\Longrightarrow$ L/K endlich, genauer: $[L : K] \leq n$ wegen $(*)$
- $\mathrm{Gal}(L/K) = G$ „$\supseteq$“ nach Definition.
  Nach 4.1 e) ist $n = |G| \leq |\mathrm{Gal}(L/K)| = [L : K] \leq n$.

4.2 Die Galoisgruppe einer Gleichung

Definition und Bemerkung 4.5

Sei K ein Körper, $f \in K[X]$ ein separabeles Polynom.

a) Sei $L = K(f)$ Zerfällungskörper von f über K.
Dann heißt $\mathrm{Gal}(f) := \mathrm{Gal}(L/K)$ ***Galoisgruppe von*** f.

b) Ist $n = \deg(f)$, so gibt es injektiven Gruppenhomomorphismus $\mathrm{Gal}(f) \hookrightarrow S_n$
(durch Permutation der Nullstellen von f)

c) Ist L/K separable Körpererweiterung vom Grad n, so ist $\mathrm{Aut}_K(L)$ isomorph zu einer Untergruppe von S_n.

Beweis Sei $L = K(\alpha)$, $f \in K[X]$ Minimalpolynom von α, $\alpha = \alpha_1, \ldots, \alpha_d$ die Nullstellen von f in L.
$\Longrightarrow$ jedes $\sigma \in \mathrm{Aut}_K(L)$ permutiert $\alpha_1, \ldots, \alpha_d$.

Beispiele 4.6

Die Galoisgruppe von $f(x) = x^5 - 4x - 2 \in \mathbb{Q}[x]$ ist S_5.

Beweis
- f ist irreduzibel: Eisenstein für $p = 2$.
- f hat 3 reelle und 2 zueinander konjugierte komplexe Nullstellen:
  $f(-\infty) = -\infty$, $f(0) = 2$, $f(1) = -1$, $f(\infty) = \infty$
  $\Longrightarrow$ f hat mindestens 3 reelle Nullstellen
  $f'(x) = 5x^4 - 4 = 5(x^2 - \frac{2}{\sqrt{5}})(x^2 + \frac{2}{\sqrt{5}})$ hat 2 reelle Nullstellen
  $\Longrightarrow$ f hat genau 3 reelle Nullstellen.
  Ist $\alpha \in \mathbb{C}$ Nullstelle von f, so ist $f(\overline{\alpha}) = \overline{f(\alpha)} = 0$.
- $G = \mathrm{Gal}(f)$ enthält die komplexe Konjugation τ.
  τ operiert als Transposition: 2 Nullstellen werden vertauscht, 3 bleiben fix.
- G enthält ein Element der Ordnung 5. Ist α Nullstelle von f, so ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ und $\mathbb{Q}(\alpha) \subseteq L(f)$
  $\overset{\text{Satz 17}}{\Longrightarrow}$ 5 teilt $|G|$
  $\overset{\text{Sylow}}{\Longrightarrow}$ Behauptung.
- G enthält also einen 5-Zyklus und eine Transposition $\overset{(!)}{\Rightarrow} G = S_5$.

Bemerkung 4.7 (Allgemeine Gleichungen n-ten Grades)

Sei k ein Körper, $L = k(T_1, \ldots, T_n) = \mathrm{Quot}(k[T_1, \ldots T_n])$

a) S_n operiert auf L durch $\sigma(T_i) = T_{\sigma(i)}$

b) Sei $K := L^{S_n}$. L/K ist Galoiserweiterung (nach Prop 4.4) von Grad n.

c) L ist (über K) Zerfällungskörper von

$$f(X) = \prod_{i=1}^{n}(X - T_i) \in K[X]$$

d) $\mathrm{Gal}(f) = S_n$

e) $f(X) = \sum_{\nu=0}^{n}(-1)^\nu s_\nu(T_1, \dots T_n)X^{n-\nu}$

mit $s_\nu(T_1, \dots T_n) = \sum_{1 \dots i_1 < \dots < i_\nu \le n} T_{i_1} \cdots T_{i_\nu}$

z.B: $s_1(T_1, \dots T_n) = T_1 + \dots + T_n$, $s_2 = T_1T_2 + T_1T_3 + \dots$, $s_n = T_1 \cdot \dots \cdot T_n$

f) $K = K(s_1, \dots s_n)$

4.3 Einheitswurzeln

Definition und Bemerkung 4.8

Sei K ein Körper, $\overline{K}$ algebraischer Abschluss. $n \in \mathbb{N}$ teilerfremd zu $\mathrm{char}(K)$.

a) Die Nullstellen von $X^n - 1$ in $\overline{K}$ heißen ***n-te Einheitswurzeln***.

b) $\mu_n(\overline{K}) = \{\zeta \in \overline{K} : \zeta^n = 1\}$ ist zyklische Untergruppe von $\overline{K}^\times$ von Ordnung n.

Beweis $\mu_n(\overline{K})$ Untergruppe $\sqrt{}$, also zyklisch nach 3.17
$f(X) = X^n - 1$ ist separabel, da $f'(X) = nX^{n-1}$ (Prop 3.13)

c) Eine n-te Einheitswurzel ζ heißt ***primitiv***, wenn $\langle\zeta\rangle = \mu_n(\overline{K})$.

Satz 18 (Einheitswurzeln)

Voraussetzungen wie in 4.8. ($n \ge 2$)

a) Die Anzahl der primitiven n-ten Einheitswurzeln in $\overline{K}$ ist
$\varphi(n) = \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right| = |\{m \in \{1 \dots n\} : \mathrm{ggT}(m, n) = 1\}|$
($n \mapsto \varphi(n)$ ist die ***Eulersche φ-Funktion***)

Beweis Ist ζ primitive n-te Einheitswurzel, so ist $\mu_n(\overline{K}) = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$
ζ^k erzeugt $\mu_n(\overline{K}) \iff \mathrm{ggT}(n, k) = 1$

b) Ist $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ (Primfaktorzerlegung),
so ist $\varphi(n) = \prod_{i=1}^{r} p_i^{\nu_i - 1}(p_1 - 1)$

Beweis $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_r^{\nu_r}\mathbb{Z}$ (Satz 8)

$\Longrightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^\times = \left(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}\right)^\times \oplus \cdots \oplus \left(\mathbb{Z}/p_r^{\nu_r}\mathbb{Z}\right)^\times$

$\left|\left(\mathbb{Z}/p_\nu\mathbb{Z}\right)^\times\right| = p^\nu - p^{\nu-1} = p^{\nu-1}(p-1)$

c) Sind $\zeta_1, \ldots, \zeta_{\varphi(n)}$ die primitiven Einheitswurzeln, so heißt

$$\Phi_n(X) = \prod_{i=1}^{\varphi(n)} (X - \zeta_i) \in \overline{K}[X]$$

das n-te ***Kreisteilungspolynom***.

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

Beweis $X^n - 1 = \prod_{\zeta \in \nu_n} (X - \zeta) = \prod_{d|n} \prod_{\substack{\zeta \in \mu_n \\ \mathrm{ord}(\zeta)=d}} (X - \zeta) = \prod_{d|n} \Phi_d(X)$

e) Sei ζ primitive n-te Einheitswurzel. Dann ist $K(\zeta)/K$ Galoiserweiterung.

Beweis $K(\zeta)$ ist Zerfällungskörper von $X^n - 1$ über K, also normal.

$X^n - 1$ ist separabel, siehe Beweis 4.8 b)

f) $\chi_n : \mathrm{Gal}(K(\zeta)/K) \to \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$, $\sigma \mapsto \chi_x(\sigma)$

ist injektiver Gruppenhomomorphismus, wobei $\sigma(\zeta) = \zeta^{\chi_n(\sigma)}$.

(χ_n heißt ***zyklotonischer Charakter***)

Beweis $\chi_n(\sigma) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$, da $\sigma(\zeta)$ primitive Einheitswurzel sein muss.

χ_n ist Gruppenhomomorphismus. $\sigma_1, \sigma_2 \in \mathrm{Gal}(K(\zeta)/K)$
$\Longrightarrow \sigma_1(\sigma_2(\zeta)) = \sigma_1(\zeta^{\chi_n(\sigma_1)}) = (\sigma_1(\zeta))^{\chi_n(\sigma_1)} = \zeta^{\chi_n(\sigma_1)\chi_n(\sigma_2)}$

χ_n ist injektiv.
$\chi_n(\sigma) = 1 \Longrightarrow \sigma(\zeta) = \zeta \Longrightarrow \sigma = id.$

g) $\Phi_n \in K[X]$, genauer: $\Phi_n(X) \in \begin{cases} \mathbb{Z}[X] \text{ primitiv} & \mathrm{char}(K) = 0 \\ \mathbb{F}_p[X] & \mathrm{char}(K) = p \end{cases}$

Beweis Induktion über n:

$n = 1$: $\surd$, $n = 2$: $\surd$.

$n > 2$:

$$\underbrace{X^n - 1}_{} \overset{\text{d)}}{=} \Phi_n(X) \cdot \underbrace{\prod_{\substack{d|n \\ d<n}} \Phi_d(X)}_{}$$

$\mathrm{char}(K) = p$: $\in \mathbb{F}_p[x]$ $\qquad \in \mathbb{F}_p[x]$ nach I.V.
$\Longrightarrow \Phi_n(X) \in \mathbb{F}_p[x]$ mit Euklidischem Algorithmus.

$\mathrm{char}(K) = 0$: $\in \mathbb{Z}[x]$ $\qquad \in \mathbb{Z}[x]$ primitiv.
$\overset{\text{Satz von Gauß}}{\Longrightarrow} \Phi_n(X) \in \mathbb{Z}[X]$ primitiv

h) Ist $K = \mathbb{Q}$, so ist Φ_n irreduzibel und χ_n ein Isomorphismus.

$\mathbb{Q}(\zeta)$ heißt n-te ***Kreisteilungskörper***.

Beweis Genügt zu zeigen: Φ_n irreduzibel (dann folgt χ_n isomorph aus e) und f))

Sei $f \in \mathbb{Q}[x]$ das Minimalpolynom von ζ. $f \in \mathbb{Z}[x]$ wegen g).

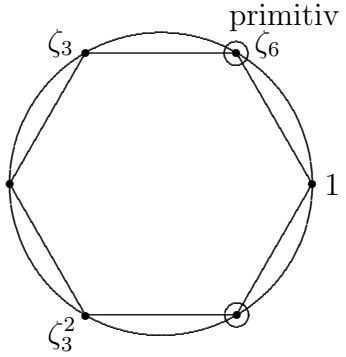
Behauptung: $f(\zeta^p) = 0$ für jede Primzahl p mit $p \nmid n$.

Dann ist auch $f(\zeta^m) = 0$ für jedes m mit $\mathrm{ggT}(m, n) = 1$
$\Longrightarrow$ $f(\zeta_i) = 0$ für jede primitive Einheitswurzel ζ_i
$\Longrightarrow$ $\Phi_n \mid f \Longrightarrow \Phi_n = f$.

Beweis der Behauptung: Sei $X^n - 1 = f \cdot h$.

Wäre $f(\zeta^p) \neq 0 \Longrightarrow h(\zeta^p) = 0$
d.h. ζ ist Nullstelle von $h(X^p) \Longrightarrow h(X^p)$ ist Vielfaches von f
$\Longrightarrow \exists g \in \mathbb{Z}[X]$ mit $h(X^p) = f \cdot g \overset{\text{mod } p}{\Longrightarrow} \overline{f} \cdot \overline{g} = \overline{h}^p$ in $\mathbb{F}_p[X]$.
$\Longrightarrow$ $\overline{f}$ und $\overline{h}$ haben gemeinsame Nullstellen in $\overline{\mathbb{F}_p}$
$\Longrightarrow$ $X^n - \overline{1} = \overline{f} \cdot \overline{h}$ hat doppelte Nullstelle. Widerspruch zu $X^n - 1$ separabel.

Beispiele $\Phi_2(x) = x + 1$
$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$
$\Phi_4(x) = \dfrac{x^4 - 1}{\Phi_2 \cdot \Phi_1} = \dfrac{x^4 - 1}{x^2 - 1} = x^2 + 1$
$\Phi_6(x) = \dfrac{x^6 - 1}{\Phi_3 \cdot \Phi_2 \cdot \Phi_1} = \cdots = x^2 - x + 1$
$\Phi_8(x) = x^4 - 1$
Für $n < 105$ sind alle Koeffizienten von Φ_n 0, 1 oder -1.



Folgerung 4.9

Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist.

Beweis Zu zeigen: ζ_n (primitive Einheitswurzel) $\in K(\{0,1\}) \Longleftrightarrow \varphi(n) = 2^l$ für ein $l > 1$.
$\Longleftrightarrow \underbrace{[\mathbb{Q}(\zeta_n) : \mathbb{Q}]}_{=\varphi(n)} = 2^l$ und es gibt Kette $\mathbb{Q} \subset L_1 \subset \cdots \subset L_l = \mathbb{Q}(\zeta_n)$ mit $[L_i : L_{i-1}] = 2$

„$\Longleftarrow$“ Woher kommt die Kette?
$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ ist abelsch von Ordnung 2^l
Dazu gehört eine Kompositionsreihe mit Faktoren $\mathbb{Z}/2\mathbb{Z}$.

4.4 Norm, Spur und Charaktere

Definition und Bemerkung 4.10

Sei G ein Gruppe, K ein Körper.

a) Ein ***Charakter*** von G (mit Werten in K) ist ein Gruppenhomomorphismus $\chi : G \to K^\times$.

b) $X_K(G) = \{\chi : G \to K^\times : \chi \text{ Charakter } \} = \mathrm{Hom}(G, K^\times)$ heißt ***Charaktergruppe*** von G (mit Werten in K).

c) (Lineare Unabhängigkeit der Charaktere, E. Artin)

$X_K(G)$ ist linear unabhängige Teilmenge des K-Vektorraums $\mathrm{Abb}(G, K)$.

Beweis Angenommen $X_K(G)$ ist linear abhängig, dann sei $n > 0$ minimal, so dass es in $X_K(G)$ n paarweise verschiedene linear unabhängige Elemente gibt: es gebe also $\chi_1, \dots \chi_n \in X_K(G)$, $\lambda_1, \dots \lambda_n \in K^\times$ mit $\sum_{i=1}^n \lambda_i \chi_i = 0$.

Dazu muss $n \geq 2$ sein.

Sei $g \in G$ mit $\chi_1(g) \neq \chi_2(g)$. Dann gilt für alle $h \in G$.

$$0 = \sum_{i=1}^n \lambda_i \chi_i(gh) = \sum_{i=1}^n \underbrace{\lambda_i \chi_i(g)}_{=\mu_i \in K^\times} \chi_i(h) = \sum_{i=1}^n \mu_i \chi_i(h) \Longrightarrow \sum_{i=1}^n \mu_i \chi_i = 0$$

Sei $\nu_i = \mu_i - \lambda_i \chi_1(g)$, $i = 1, \dots n$.

Dann ist $\sum_{i=1}^n \nu_i \chi_i = 0$,
$\nu_1 = \lambda_1 \chi_1(g) - \lambda_1 \chi_1(g) = 0$,
$\nu_2 = \lambda_2 \chi_2(g) - \lambda_2 \chi_1(g) = \lambda_2(\chi_2(g) - \chi_1(g)) \neq 0$.

Widerspruch zur Minimalität von n.

Definition und Bemerkung 4.11

Sei L/K endliche Körpererweiterung.
$q := \dfrac{[L:K]}{[L:K]_S} (= p^r, p = \mathrm{char}(K))$, $n := [L:K]_S$
$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots \sigma_n\}$

a) Für $\alpha \in L$ heißt $\mathrm{tr}_{L/K}(\alpha) := q \cdot \sum_{i=1}^n \sigma_i(\alpha) \in \overline{K}$ die ***Spur*** von α (über K).

b) $\mathrm{tr}_{L/K}(\alpha) \in K$ für alle $\alpha \in K$.

Beweis Ohne Einschränkung sei L/K separabel.

Ist L/K normal, also galoissch, so ist
$\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Gal}(L/K) =: G$
und $\mathrm{tr}_{L/K}(\alpha) \in L^G = K$ [Die Spur ist invariant unter $\sigma \in \mathrm{Gal}(L/K)$, dann Hauptsatz]

Andernfalls sei $\widetilde{L}$ normale Erweiterung von L mit $L \subset \widetilde{L}$.

Für $\tau \in \mathrm{Hom}_K(\widetilde{L}, \overline{K}) = \mathrm{Gal}(\widetilde{L}/K)$ und jedes $i = 1, \dots n$ ist $\tau \circ \sigma_i \in \mathrm{Hom}_K(L, \overline{K})$ (da $\sigma_i(L) \subseteq \widetilde{K}$)

$\Longrightarrow \mathrm{tr}_{L/K}(\alpha) \in \widetilde{L}^{\mathrm{Gal}(\widetilde{L}/K)} = K$.

c) $\mathrm{tr}_{L/K}$ ist K-linear.

d) Für $\alpha \in L$ heißt $N_{L/K}(\alpha) := \left(\prod_{i=1}^n \sigma_i(\alpha) \right)^q$ die ***Norm*** von α (über K).

e) $N_{L/K}(\alpha) \in K$

Beweis Ist L/K separabel, so argumentiere wie in b), sonst siehe Bosch.

f) $N_{L/K} : L^\times \to K^\times$ ist Gruppenhomomorphismus.

Bemerkung 4.12

Sei L/K endliche Körpererweiterung.
Für $\alpha \in L$ sei $m_\alpha : L \to L$, $x \mapsto \alpha x$.
m_α ist K-linear und es gilt: $\mathrm{tr}_{L/K}(\alpha) = \mathrm{Spur}(m_\alpha)$, $N_{L/K}(\alpha) = \det(m_\alpha)$.

Beweis Ist L/K separabel, so sei $L = K(\alpha)$
Dann ist $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ eine K-Basis von L, $[L : K] = n$.
Weiter sei $f(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0 \in K[X]$ das Minimalpolynom von α über K.
Dann ist die Abbildungsmatrix von m_α bzgl. der Basis $1, \ldots, \alpha^{n-1}$:

$$\begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & -c_0 \\ 1 & 0 & & & \vdots & -c_1 \\ \vdots & 1 & 0 & & \vdots & \vdots \\ \vdots & \vdots & 1 & \ddots & & \\ \vdots & \vdots & \vdots & \ddots & 0 & \\ 0 & 0 & 0 & \cdots & 1 & -c_{n-1} \end{pmatrix}$$

$\Longrightarrow \mathrm{Spur}(m_\alpha) = -c_{n-1}$, $\det(m_\alpha) = (-1)^n c_0$
In $\overline{K}[X]$ zerfällt f in Linearfaktoren: $f = \prod_{i=1}^{n}(X - \sigma_i(\alpha))$

$\Longrightarrow c_{n-1} = \sum_{i=1}^{n} \sigma_i(\alpha), c_0 = (-1)^n \prod_{i=1}^{n} \sigma_i(\alpha)$
Ist $L \neq K(\alpha)$, so sei $b_1, \ldots b_m$ eine $K(\alpha)$-Basis von L.
Dann ist $B = \{b_i\alpha^j : i = 1, \ldots m, j = 0, \ldots n-1\}$ eine K-Basis von L.
Dann ist die Darstellungsmatrix von m_α bzgl B:

$$\begin{pmatrix} D & 0 & \cdots & 0 \\ 0 & D & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & 0 & & D \end{pmatrix}$$

$\Longrightarrow \mathrm{Spur}(m_\alpha) = m \cdot (-c_{n-1})$, $det(m_\alpha) = ((-1)^n c_0)^m$
Für jedes $\sigma_i \in \mathrm{Hom}_K(L, \overline{K})$ ist $\sigma_i(\alpha)$ Nullstelle von f.
Jede Nullstelle von f wird dabei gleich oft angenommen, nämlich $m = [L : K(\alpha)]$-mal.
$\Longrightarrow \mathrm{tr}_{L/K}(\alpha) = m \cdot \mathrm{tr}_{K(\alpha)/K}(\alpha) = m \cdot (-c_{n-1})$
und $N_{L/K}(\alpha) = (N_{K(\alpha)/K}(\alpha))^m = ((-1)^n c_0)^m$.

Satz 19 (Hilbert 90)

Sei L/K zyklische Galois-Erweiterung (d.h. $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ für ein σ)

a) Ist $\beta \in L$ mit $N_{L/K}(\beta) = 1$, so gibt es ein $\alpha \in L^\times$ mit

$$\beta = \frac{\alpha}{\sigma(\alpha)}$$

Beweis $n := [L/K]$

Nach 4.10 c) sind die Charaktere $id, \sigma, \ldots, \sigma^{n-1} : L^\times \to L^\times$ linear unabhängig über L.

Also ist $f = id + \beta \cdot \sigma + \beta \cdot \sigma(\beta)\sigma^2 + \cdots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}$

$\Longrightarrow \exists \gamma \in L$ mit $\alpha := f(\gamma) \neq 0$. Dies eingesetzt:

$\beta\sigma(\alpha) = \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \cdots + \underbrace{\beta\sigma(\beta)\cdots\sigma^{n-1}(\beta)}_{N_{L/K}(\beta)=1}\underbrace{\sigma^n(\gamma)}_{\gamma}$

b) Sei L/K zyklische Galoiserweiterung, $\sigma \in \mathrm{Gal}(L/K)$ ein Erzeuger. $n := [L : K]$

Zu $\beta \in L$ mit $\mathrm{tr}_{L/K}(\beta) = 0$ gibt es $\alpha \in L$ mit

$$\beta = \alpha - \sigma(\alpha)$$

Beweis Sei $\gamma \in L$ mit $\mathrm{tr}_{L/K}(\gamma) \neq 0$ und

$\alpha := \frac{1}{\mathrm{tr}_{L/K}(\alpha)} \cdot [\beta\sigma(\gamma) + (\beta + \sigma(\beta))\sigma^2(\gamma) + \cdots + (\beta + \sigma(\beta) + \cdots + \sigma^{n-2}(\beta))\sigma^{n-1}(\gamma)]$

$\Longrightarrow \sigma(\alpha) = \frac{1}{\mathrm{tr}_{L/K}(\gamma)} \cdot [\sigma(\beta)\sigma^2(\gamma) + (\sigma(\beta) + \sigma^2(\beta))\sigma^3(\gamma) + \cdots + (\sigma(\beta) + \cdots + \sigma^{n-1}(\beta))\sigma^n(\gamma)]$

$\Longrightarrow (\alpha - \sigma(\alpha)) \cdot \mathrm{tr}_{L/K}(\gamma) = \beta\sigma(\gamma) + \beta\sigma^2(\gamma) + \cdots + \beta\sigma^{n-1}(\gamma) - \underbrace{(\sigma(\beta) + \cdots + \sigma^{n-1}(\beta))}_{-\beta}\gamma$

$= \beta\,\mathrm{tr}_{L/K}(\gamma)$

Folgerung 4.13

Voraussetzungen wie in Satz 19

a) Ist $\mathrm{char}(K)$ kein Teiler von $n := [L : K]$ und enthält K eine primitive n-te Einheitswurzel ζ, so gibt es ein primitives Element $\alpha \in L$, so dass das Minimalpolynom von α über K:

$$X^n - \gamma$$

ist für ein $\gamma \in K$. („***Kummer-Erweiterung***“)

b) Ist $\mathrm{char}(K) = [L : K] = p$, so gibt es ein primitives Element $\alpha \in L$ mit Minimalpolynom

$$X^p - X - \gamma$$

für ein $\gamma \in K$. („***Artin-Schreier-Erweiterung***“)

Beweis a) Es ist $N_{L/K}(\zeta) = \zeta^n - 1 = N_{L/K}(\zeta^{-1})$

$\xrightarrow{\text{Satz 19a}}$ es gibt $\alpha \in L$ mit $\sigma(\alpha) = \zeta\alpha$

$\Longrightarrow \sigma^i(\alpha) = \zeta^i\alpha$, $i = 0, \dots n-1$

$\Longrightarrow$ Das Minimalpolynom von α über K hat n verschiedene Nullstellen.

$\Longrightarrow L = K(\alpha)$

Außerdem ist $\sigma(\alpha^n) = \sigma(\alpha)^n = \alpha^n$

$\Longrightarrow \gamma := \alpha^n \in K$

$\Longrightarrow$ Das Minimalpolynom von α ist $X^n - \gamma$.

b) $\mathrm{tr}_{L/K}(1) = 1 + \dots + 1 = p = 0$

$\xrightarrow{\text{Satz 19b}}$ es gibt $\alpha \in L$ mit $\sigma(\alpha) = \alpha + 1$

$\Longrightarrow \sigma^i(\alpha) = \alpha + i$, $i = 0, \dots n-1$

$\Longrightarrow K(\alpha) = L$

$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = \alpha^p + 1 - (\alpha + 1) = \alpha^p + \alpha.$

$\Longrightarrow \alpha^p - \alpha =: \gamma \in K$ und $X^p - X - \gamma$ ist Minimalpolynom von α.

Proposition 4.14

Sei L/K einfache Körpererweiterung $L = K(\alpha)$

a) Ist α Nullstelle eines Polynoms $X^n - \gamma$ für ein $\gamma \in K$ und enthält K eine primitive n-te Einheitswurzel ζ, so ist L/K galoissch, $\mathrm{Gal}(L/K)$ zyklisch, $d := [L : K]$ ist Teiler von n, $\alpha^d \in K$, $X^d - \alpha^d$ ist Minimalpolynom von α.

b) Ist $\mathrm{char}(K) = p > 0$ und $\alpha \in L/K$ Nullstelle eines Polynoms $X^p - X - \gamma$ für ein $\gamma \in K$, so ist L/K galoissch und $\mathrm{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$.

Beweis a) Die Nullstellen von $X^n - \gamma$ sind $\alpha, \zeta\alpha, \dots, \zeta^{n-1}\alpha$.

$\Longrightarrow L$ ist Zerfällungskörper von $X^n - \gamma$, also normal und separabel, also galoissch.

Für $\sigma \in \mathrm{Gal}(L/K)$ ist $\sigma(\alpha) = \zeta^{\nu(\sigma)}\alpha$ für ein $\nu(\sigma) \in \mathbb{Z}/n\mathbb{Z}$

$\sigma \mapsto \nu(\sigma)$ ist injektiver Gruppenhomomorphismus $\mathrm{Gal}(L/K) \to \mathbb{Z}/n\mathbb{Z}$

$\Longrightarrow \mathrm{Gal}(L/K)$ ist zyklisch, da Untergruppe von $\mathbb{Z}/n\mathbb{Z}$

$\Longrightarrow d = [L : K]$ teilt n.

Für $\sigma \in \mathrm{Gal}(L/K)$ ist $\sigma(\alpha^d) = (\zeta^{\nu(\sigma)})^d \cdot \alpha^d = \alpha^d$

$X^d - \alpha^d$ ist Minimalpolynom, da $L = K(\alpha)$ und $[K(\alpha) : K] = d$

b) Für $i \in \mathbb{F}_p$ ist $(\alpha + i)^p - (\alpha + i) - \gamma = \alpha^p + \underbrace{i^p}_{=i} - \alpha - i - \gamma = 0.$

$\Longrightarrow X^p - X - \gamma$ hat p verschiedene Nullstellen in L.

$\Longrightarrow L$ ist Zerfällungskörper von $X^p - X - \gamma$ und L/K ist separabel.

Außerdem folgt: $\mathrm{Gal}(L/K) = \mathbb{Z}/p\mathbb{Z}$

4.5 Auflösung von Gleichungen durch Radikale

Definition 4.15

Sei K ein Körper

a) Eine einfache Körpererweiterung $L = K(\alpha)$ heißt ***elementare*** (oder ***einfache***) ***Radikalerweiterung***, wenn entweder

(i) α ist eine Einheitswurzel.

(ii) α ist Nullstelle von $X^n - \gamma$ für ein $\gamma \in K$ und $\mathrm{char}(K) \nmid n$.

(iii) α ist Nullstelle von $X^p - X - \gamma$ für ein $\gamma \in K$ und $\mathrm{char}(K) = p$.

b) Eine endliche Körpererweiterung L/K heißt ***Radikalerweiterung***, wenn es eine Körpererweiterung L'/L gibt und eine Kette $K = L_0 \subset L_1 \subset \cdots \subset L_n = L'$ von Zwischenkörpern, so dass L_{i+1}/L_i elementare Radikalerweiterung ist für $i = 0, \ldots, n-1$.

c) Ist $f \in K[X]$ separabel, nicht konstant, so heißt die Gleichung $f(X) = 0$ ***durch Radikale auflösbar***, wenn der Zerfällungskörper von f eine Radikalerweiterung ist.

Beispiel $K = \mathbb{Q}$, $f(X) = X^3 - 3X + 1$

Behauptung: Ist α Nullstelle von f, so ist $\mathbb{Q}(\alpha)$ Zerfällungskörper von f, hat also Grad 3 über $\mathbb{Q}$. $\mathbb{Q}(\alpha)/\mathbb{Q}$ ist keine Radikalerweiterung!

Die Nullstellen von f sind $\alpha_1 = e^{\frac{2\pi i}{9}} + e^{\frac{16\pi i}{9}}$, $\alpha_2 = e^{\frac{8\pi i}{9}} + e^{\frac{10\pi i}{9}}$, $\alpha_3 = e^{\frac{14\pi i}{9}} + e^{\frac{4\pi i}{9}}$.

Es ist $\alpha_i^2 = e^{\frac{4\pi i}{9}} + e^{\frac{14\pi i}{9}} + 2 = \alpha_3 + 2 \Longrightarrow \alpha_3 \in \mathbb{Q}(\alpha_1)$

$\Longrightarrow \alpha_2 = -\alpha_1 - \alpha_3 \in \mathbb{Q}(\alpha_1)$.

Satz 20

Sei K ein Körper, $f \in K[X]$ separabel, nicht konstant.

a) Die Gleichung $f(X) = 0$ ist genau dann durch Radikale auflösbar, wenn ihre Galoisgruppe G auflösbar ist.

(d.h. G hat Normalreihe, $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$ mit G_i/G_{i+1} abelsch.)

Beispiel $X^5 - 4X + 2$ hat Galoisgruppe S_5
und ist deshalb nicht durch Radikale auflösbar,
denn $S_5 \subset A_5 \subset \{e\}$ ist Kompositionsreihe.

Nach Jordan-Hölder tritt A_5 in jeder Kompositionsreihe für S_5 als Faktorgruppe auf.

b) Eine endliche Körpererweiterung L/K ist genau dann Radikalerweiterung, wenn es eine endliche Galoiserweiterung L'/K gibt mit $L \subseteq L'$, so dass $\mathrm{Gal}(L'/K)$ auflösbare Gruppe ist.

Beweis „$\Longrightarrow$“ Sei $K = L_0 \subset L_1 \subset \cdots \subset L_m$ Kette wie in der Definition mit $L \subset L_m$.

Induktion über m

$m = 1$: Ist L_1/K vom Typ (i), so ist $L_1 = K(\zeta)$ für eine primitive n-te Einheitswurzel ζ und $\mathrm{Gal}(K(\zeta)/K) \subseteq \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$, also auflösbar.

Ist L_1/K vom Typ (iii), so ist L_1/K galoissch und $\mathrm{Gal}(L_1/K) = \mathbb{Z}/p\mathbb{Z}$.

Sei L_1/K vom Typ (ii):

Enthält K eine primitive n-te Einheitswurzel, so ist $K(\alpha)/K$ galoissch und $\mathrm{Gal}(K(\alpha)/K) \cong \mathbb{Z}/n\mathbb{Z}$.

Andernfalls sei $F = K(\zeta)$ der Zerfällungskörper von $X^n - 1$ über K und $L_1' = F(\alpha) = L_1(\zeta) = FL_1$ das „Kompositum“ von F und L_1.

L_1' ist galoissch über K (Zerfällungskörper von $X^n - \gamma$ über K) und es gibt exakte Sequenz:

$$1 \to \underbrace{\mathrm{Gal}(L_1'/F)}_{\text{zyklisch}} \to \mathrm{Gal}(L_1'/K) \to \underbrace{\mathrm{Gal}(F/K)}_{\text{abelsch}} \to 1$$

$\Longrightarrow$ $\mathrm{Gal}(L_1'/K)$ auflösbar.

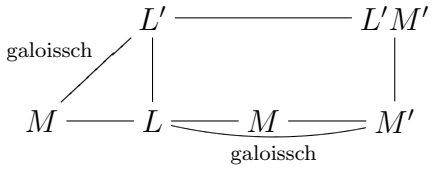
$n > 1$: Eine endliche Körpererweiterung L/K heiße ***auflösbar***, wenn es eine endliche Erweiterung L'/L gibt, so dass L'/K galoissch ist und $\mathrm{Gal}(L'/K)$ auflösbar.

Nach I.V. ist L_{m-1}/K auflösbar.

Außerdem ist L_m/L_{m-1} auflösbar

Zu zeigen also: Sind $K \subset L \subset M$ Körpererweiterungen (Umbenannt: L war L_{m-1}, M war L_m) und L/K auflösbar, M/L auflösbar, so ist M/K auflösbar.

Seien dazu L'/L und M'/M Erweiterungen wie in der Definition:



Behauptung: L'M'/L' ist galoissch und $\mathrm{Gal}(L'M'/L')$ ist auflösbar.

denn: Nach Voraussetzung ist M'/L galoissch, also Zerfällungskörper eines Polynoms $f \in L[X]$.
$\Longrightarrow$ $M'L'$ ist Zerfällungskörper von $f \in L'[X]$ über L'.

Außerdem: $\mathrm{Gal}(L'M'/L') \to \mathrm{Gal}(M'/L)$, $\sigma \mapsto \sigma|_{M'}$!$\in \mathrm{Gal}(M'/L)$

ist wohldefiniert und injektiv: ist $\sigma|_{M'} = id_{M'}$, so ist $\sigma = id_{L'M}$, da $\sigma_{L'} = id_{L'}$ nach Voraussetzung.

Also ohne Einschränkung $L = L'$, $L'M' = M$.

Ist M/K galoissch, so ist $\mathrm{Gal}(M/K)$ auflösbar, da dann

$$1 \to \underbrace{\mathrm{Gal}(M/L)}_{\text{auflösbar}} \to \mathrm{Gal}(M/K) \to \underbrace{\mathrm{Gal}(L/K)}_{\text{auflösbar}} \to 1$$

exakt ist.

Andernfalls sei $\widetilde{M}/M$ minimale Erweiterung, so dass $\widetilde{M}/K$ galoissch ist.

$\widetilde{M}$ wird über K erzeugt von den $\sigma(M)$, $\sigma \in \mathrm{Hom}_K(M, \overline{K})$ ($\overline{K}$ fest gewählter algebraischer Abschluss von K)

Für jedes $\sigma \in \mathrm{Hom}_K(M, \overline{K})$ ist $\sigma(M)$ Galoiserweiterung von $\sigma(L) = L$.

Dann ist $\mathrm{Gal}(\widetilde{M}/L) \to \prod_{\sigma \in \mathrm{Hom}_K(M,\overline{K})} \mathrm{Gal}(\sigma(M), L)$, $\tau \mapsto (\tau|_{\sigma(M)})_\sigma$ injektiver Gruppenhomomorphismus.

Für jedes $\sigma \in \mathrm{Hom}_K(M, \overline{K})$ ist $\mathrm{Gal}(\sigma(M)/L) \cong \mathrm{Gal}(M, L)$ also auflösbar. $\Longrightarrow \prod_\sigma \mathrm{Gal}(\sigma(M)/L)$ ist auflösbar (!)

$\Longrightarrow$ $\mathrm{Gal}(\widetilde{M}/L)$ auflösbar (als Untergruppe einer auflösbaren Gruppe)

$\Longrightarrow$ $\mathrm{Gal}(\widetilde{M}/K)$ ist auflösbar wegen

$$1 \to \mathrm{Gal}(\widetilde{M}/L) \to \mathrm{Gal}(\widetilde{M}/K) \to \mathrm{Gal}(L/K) \to 1$$

exakt.

Beweis: „$\Longleftarrow$“

$G := \mathrm{Gal}(L'/K)$ sei auflösbar, $G = G_0 \supset G_1 \supset \cdots \supset G_m = \{1\}$ Normalreihe so dass G_{i+1} Normalteiler in G_i und ${}^{G_i}\!/_{G_{i+1}} \cong {}^{\mathbb{Z}}\!/_{p_i\mathbb{Z}}$ mit Primzahlen p_i, $i = 0 \ldots m-1$

Dazu gehört eine Kette von Zwischenkörpern $K = K_0 \subset K_1 \subset \cdots \subset K_m = L$, in der ${}^{K_i}\!/_{K_{i-1}}$ Galoiserweiterung ist mit $\mathrm{Gal}(K_i/K_{i-1}) \cong {}^{\mathbb{Z}}\!/_{p_i\mathbb{Z}}$

Ist $p_i = \mathrm{char}(K)$, so ist K_i/K_{i-1} Artin-Schreier-Erweiterung (d.h. Typ (iii))

Ist $p_1 \neq \mathrm{char}(K)$, so ist K_i/K_{i-1} vom Typ (ii), (Folgerung zu Satz 19) falls K_{i-1} eine primitive n-te Einheitswurzel ζ enthält.

Sei also $d := \prod_{\substack{p \text{ prim} \\ p \mid\mid G|}} p$ und F der Zerfällungskörper von $X^d - 1$ über K.

$\Longrightarrow$ F/K ist Erweiterung vom Typ (i).

Sei $\widetilde{L} := FL' \Longrightarrow \widetilde{L}/F$ ist Galoiserweiterung (wie bei dem Diagramm zu $L'M'$)
und $\mathrm{Gal}(\widetilde{L}/F) \subset \mathrm{Gal}(L'/K)$, also auflösbar.

Beginne von vorne mit $\widetilde{L}$ und F statt L' und K.

Erhalte Kette $K \subset F \subset F_1 \subset \cdots \subset F_r = \widetilde{L}$ von Zwischenkörpern mit ${}^{F_i}\!/_{F_{i-1}}$ Galoiserweiterung, $\mathrm{Gal}(F_i/F_{i-1}) \cong {}^{\mathbb{Z}}\!/_{p_i\mathbb{Z}}$ und F_i/F_{i-1} ist ***elementare Radikalerweiterung***.

Vokabeln