

Algebra I

Prof. Dr. F. Herrlich

28. September 2017

Die Mitarbeiter von <http://mitschriebwiki.nomeata.de/>

Inhaltsverzeichnis

Inhaltsverzeichnis	2
1 Gruppen	5
1.1 Grundlegende Definitionen	5
1.2 Beispiele und Konstruktionen	7
1.3 Quotientenbildung	12
1.4 Abelsche Gruppen	14
1.5 Freie Gruppen	19
1.6 Kategorien und Funktoren	22
1.7 Gruppenaktionen und die Sätze von Sylow	25
1.8 Symmetrische und alternierende Gruppen	29
1.9 Kompositionsreihen	31
2 Ringe	37
2.1 Grundlegende Definitionen und Eigenschaften	37
2.2 Polynomringe	41
2.3 Faktoringe	43
2.4 Teilbarkeit	46
2.5 Brüche	51
2.6 Der Satz von Gauß	53
2.7 Maximale Ideale	56
2.8 Moduln	57
3 Algebraische Körpererweiterungen	61
3.1 Algebraische und transzendente Elemente	61
3.2 Algebraischer Abschluss	64
3.3 Fortsetzung von Körperhomomorphismen	67
3.4 Separable Körpererweiterungen	70
3.5 Endliche Körper	73
3.6 Konstruktion mit Zirkel und Lineal	74
4 Galois-Theorie	79
4.1 Der Hauptsatz	79
4.2 Die Galoisgruppe einer Gleichung	82
4.3 Einheitswurzeln	84
4.4 Norm, Spur und Charaktere	87

Inhaltsverzeichnis

4.5 Auflösung von Gleichungen durch Radikale 91

1 Gruppen

1.1 Grundlegende Definitionen

Definition 1.1.1

Sei M eine Menge.

- (a) Eine **Verknüpfung** auf M ist eine Abbildung $\cdot : M \times M \rightarrow M$
- (b) Eine Menge M zusammen mit einer Verknüpfung \cdot heißt **Magma**.
- (c) Eine Verknüpfung $\cdot : M \times M \rightarrow M$ heißt **assoziativ**, wenn

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

- (d) Eine **Halbgruppe** ist ein assoziatives Magma.
- (e) $e \in M$ heißt **neutrales Element** für die Verknüpfung \cdot , wenn

$$\forall x \in M : x \cdot e = e \cdot x = x$$

- (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 mit

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

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

Bemerkung 1.1.2

Sei (M, \cdot) ein Magma.

- (a) In M gibt es höchstens ein neutrales Element.

Beweis: Sind e, e' neutrale Elemente, so ist $e = e \cdot e' = e'$ ■

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

Beweis: Seien x', x'' zu x invers, so ist $x' = (x'' \cdot x) \cdot x' = x'' \cdot (x \cdot x') = x''$ ■

1 Gruppen

Definition + Bemerkung 1.1.3

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

- (a) $U \subseteq M$ heißt Unter- $\left\{ \begin{array}{l} \cdot \\ \cdot \\ \cdot \end{array} \right\}$, wenn $U \cdot U \subseteq U$ und (U, \cdot) selbst ein(e) $\left\{ \begin{array}{l} \cdot \\ \cdot \\ \cdot \end{array} \right\}$ ist.
- (b) $U \subseteq M$ Unterhalbgruppe $\Leftrightarrow U \cdot U \subseteq U$
- (c) $U \subseteq M$ Untermonoid $\Leftrightarrow U \cdot U \subseteq U$ und $e \in U$
- (d) $U \subseteq M$ Untergruppe $\Leftrightarrow U \neq \emptyset$ und $\forall x, y \in U : x \cdot y^{-1} \in U$

Beweis: " \Leftarrow ":

Sei $x \in U \Rightarrow e = x \cdot x^{-1} \in U \Rightarrow$ mit x ist auch x^{-1} in $U \Rightarrow$ mit x, y ist auch $xy = x(y^{-1})^{-1} \in U$ ■

Bemerkung 1.1.4

Sei (M, \cdot) Monoid. Dann ist $M^\times := \{x \in M : \text{es gibt inverses } x^{-1} \text{ zu } x \in M\}$ 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 $x \cdot y \in M^\times$, da $xy \cdot (y^{-1}x^{-1}) = e \Rightarrow \cdot$ ist Verknüpfung auf $M^\times \Rightarrow (M^\times, \cdot)$ ist Gruppe. ■

Definition + Bemerkung 1.1.5

Seien $(M, \cdot), (M', *) \left\{ \begin{array}{l} \cdot \\ \cdot \\ \cdot \end{array} \right\}$

- (a) Eine Abbildung $f : M \rightarrow M'$ heißt **Homomorphismus**, wenn $\forall x, y \in M :$

$$f(x \cdot y) = f(x) * f(y) \quad (\text{i})$$

Hat M ein neutrales Element, so muß außerdem gelten:

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

- (b) Ist $f : G \rightarrow G'$ Abbildung von Gruppen, die (i) erfüllt, so ist f Homomorphismus.

Beweis: $f(e) = f(e \cdot e) = f(e) * f(e) \stackrel{\cdot f(e)^{-1}}{\Rightarrow} e' = f(e)$ ■

- (c) Ein Homomorphismus $f : M \rightarrow M'$ heißt **Isomorphismus**, wenn es einen Homomorphismus $g : M' \rightarrow M$ gibt, mit $f \circ g = id_{M'}$ und $g \circ f = id_M$
- (d) Jeder bijektive Homomorphismus ist Isomorphismus.

Beweis: Sei $f : M \rightarrow M'$ bijektiver Homomorphismus und $g : M' \rightarrow M$ die Umkehrabbildung. z.z.: g ist Homomorphismus.

Seien $x, y \in M'$. Schreibe $x = f(\hat{x}), y = f(\hat{y})$ für passende $\hat{x}, \hat{y} \in M \Rightarrow g(x \cdot y) = g(f(\hat{x}) \cdot f(\hat{y})) = g(f(\hat{x} \cdot \hat{y})) = \hat{x} \cdot \hat{y} = g(f(\hat{x})) \cdot g(f(\hat{y})) = g(x) \cdot g(y)$ ■

(e) Die Komposition von Homomorphismen ist wieder ein Homomorphismus.

Definition 1.1.6

Sei $f : M \rightarrow M'$ Hom von $\left\{ \begin{array}{c} \cdot \\ \cdot \\ \cdot \end{array} \right\}$.

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

Beweis: Sind $x, x' \in M$, so ist $f(x) * f(x') = f(x \cdot x') \in \text{Bild}(f)$. Sind M, M' Monoide, so gilt: $f(e) = e' \in \text{Bild}(f)$. Sind M, M' Gruppen, so gilt: $f(x)^{-1} = f(x^{-1}) \in \text{Bild}(f)$, da $f(x \cdot x^{-1}) = f(e) = e' = f(x) * f(x^{-1})$ ■

(b) Sind M, M' Monoide/Gruppen, so ist $\text{Kern}(f) := \{x \in M : f(x) = e'\}$ Untermonoid/-gruppe von M .

Beweis: $x, y \in \text{Kern}(f) \Rightarrow f(xy) = f(x) * f(y) = e' * e' = e' \Rightarrow xy \in \text{Kern}(f), e \in \text{Kern}(f) \checkmark$
 $x \in \text{Kern}(f) \Rightarrow f(x^{-1}) = f(x)^{-1} = (e')^{-1} = e' \Rightarrow x^{-1} \in \text{Kern}(f)$ ■

(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.

$M^M := \{f : M \rightarrow M \text{ Abbildung}\}$ ist mit der Verknüpfung \cdot ein Monoid. $(M^M)^X = \{f : M \rightarrow M \text{ bijektiv}\} =: \text{Perm}(M) = S_M$.

insbesondere: $M = \{1, \dots, n\} : S_{\{1, \dots, n\}} = S_n$ Ist (M, \cdot) ein $\left\{ \begin{array}{c} \cdot \\ \cdot \\ \cdot \end{array} \right\}$, so ist $\text{End}(M) :=$

$\{f \in M^M : f \text{ Hom.}\}$ 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 ein(e) $\left\{ \begin{array}{c} \cdot \\ \cdot \\ \cdot \end{array} \right\}$. Dann ist $M^X = \{f : X \rightarrow M \text{ Abbildung}\}$ mit der

Verknüpfung $(f \cdot g)(x) = f(x) \cdot g(x)$ ein(e) $\left\{ \begin{array}{c} \cdot \\ \cdot \\ \cdot \end{array} \right\}$

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

denn: Sind $f, g : M \rightarrow H$ Homomorphismen, so ist $\forall x, y \in M$:

1 Gruppen

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

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

a) $\prod_{i \in I} M_i$ ist mit komponentenweiser Verknüpfung ein(e) $\left\{ \begin{array}{c} \cdot \\ \cdot \\ \cdot \end{array} \right\}$.

b) Sind M_i Monoide, so ist

$$\bigoplus_{i \in I} M_i := \{(x_i)_{i \in I} \in \prod_{i \in I} M_i, x_i = e_i \text{ ffa. } i\}$$

ein Monoid.

Definition + Bemerkung 1.2.1

(a) \prod heißt **direktes Produkt**

\bigoplus heißt **direkte Summe**

(b) Ist I endlich, so ist $\prod M_i \cong \bigoplus M_i$

(c) Sei M ein(e) $\left\{ \begin{array}{c} \cdot \\ \cdot \\ \cdot \end{array} \right\}$ und für jedes $i \in I : g_i : M \rightarrow M_i$ ein Homomorphismus. Dann gibt es genau einen Homomorphismus $G : M \rightarrow \prod_{i \in I} M_i$, so dass $g_i = pr_i \circ G$, wobei

$$pr_i : \prod_{j \in I} M_j \rightarrow M_i \text{ Projektion.}$$

Beweis: Setze $G(m) := (m_j)_{j \in I}$ mit $m_j = g_j(m)$ für $m \in M$. G ist Homomorphismus. ✓

G ist eindeutig, da $pr_i(G(m)) = g_i(m)$ sein muss. ■

(d) Ist $(M, +)$ ein kommutatives Monoid, und für jedes $i \in I : f_i : M_i \rightarrow M$ ein Homomorphismus, so gibt es genau einen Homomorphismus

$$F : \bigoplus_{j \in I} M_j \rightarrow M, \text{ so dass für jedes } i \in I : f_i = F \circ \nu_i, \text{ wobei } \nu_i : M_i \rightarrow \bigoplus_{j \in I} M_j$$

$$m \mapsto (m_j)_{j \in I}, \text{ wobei } m_j = \begin{cases} m & i = j \\ e_j & \text{sonst} \end{cases}$$

Beweis: Setze $F((m_j)_{j \in I}) = \sum_{j \in I} f_j(m_j)$

Brauche: $F((e, \dots, e, m_i, e, \dots, e)) = F(\nu_i(m_i)) \stackrel{!}{=} f_i(m_i)$

$$\Rightarrow F((e, \dots, e, m_i, e, \dots, e, m_j, e, \dots, e)) = f_i(m_i) + f_j(m_j) = F((e, \dots, e, m_i, e, \dots, e)) + F((e, \dots, e, m_j, e, \dots, e)) \quad \blacksquare$$

- (4) Sei S eine Menge ("Alphabet") $F^a(S) := \bigcup_{n=1}^{\infty} S^n$ ist Halbgruppe mit Verknüpfung "Nebeneinanderschreiben" $(x_1, \dots, x_n) \cdot (y_1, \dots, y_m) := (x_1, \dots, x_n, y_1, \dots, y_m)$
 $F^a(S)$ heißt freie Halbgruppe oder "Worthalbgruppe" über S .
 Definiert man $S^0 := \{\varepsilon\}$, dann ist $F_0^a(S) := \bigcup_{n=0}^{\infty} S^n$ ein Monoid mit neutralem Element ε , dem „leeren Wort“. Für $S = \{1\}$ ist $F_0^a(S) = (\mathbb{N}_0, +)$.

Bemerkung 1.2.2

Ist (H, \cdot) Halbgruppe, $f : S \rightarrow H$ eine Abbildung, so gibt es genau einen Homomorphismus $\varphi : F^a(S) \rightarrow H$ mit $\varphi(s) = f(s)$ für alle $s \in S$, wobei man S als $S^1 \subset F^a(S)$ auffasst.

Beweis: Für $(x_1, \dots, x_n) \in S^n$ muss gelten: $\varphi(x_1, \dots, x_n) = \varphi(x_1) \cdot \dots \cdot \varphi(x_n) = f(x_1) \cdot \dots \cdot f(x_n)$. Also ist φ eindeutig und existiert, da es so definiert werden kann. ■

Bemerkung + Definition 1.2.3

Sei (M, \cdot) ein Monoid und (G, \cdot) eine Gruppe

- (a) Für $x \in M$ ist $\varphi_x : \mathbb{N}_0 \rightarrow M, n \mapsto x^n$ ein Homomorphismus.
- (b) Für $g \in G$, so ist $\varphi_g : \mathbb{Z} \rightarrow G, n \mapsto g^n$ ein Gruppenhomomorphismus.
- (c) $\langle g \rangle := \text{Bild}(\varphi_g)$ heißt die von g erzeugte **zyklische Untergruppe** von G .
- (d) G heißt **zyklisch**, wenn es ein $g \in G$ gibt mit $\langle g \rangle = G$.
- (e) $|\langle g \rangle| \in \mathbb{N} \cup \{\infty\}$ heißt **Ordnung** von g
- (f) Ist G endlich, so heißt $|G|$ die **Ordnung** von G .

Definition + Bemerkung 1.2.4 (Satz von Cayley)

- (a) Für $g \in G$ heißt die Abbildung $\tau_g : G \rightarrow G, h \mapsto gh$ die *Linksmultiplikation* mit g .
- (b) Für jedes $g \in G$ ist τ_g bijektiv, da $\tau_{g^{-1}}$ die Umkehrabbildung ist.
- (c) Die Abbildung:

$$\begin{aligned} \tau & : G \rightarrow \text{Perm}(G) \\ g & \mapsto \tau_g \end{aligned}$$

ist ein injektiver Gruppenhomomorphismus.

Beweis:

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

1 Gruppen

- (2) τ ist Homomorphismus: $\tau(g_1 g_2) = \tau(g_1) \circ \tau(g_2)$, denn: $\forall x \in G : \tau(g_1 \circ g_2)(x) = (g_1 g_2)x = g_1(g_2 x) = \tau_{g_1}(\tau_{g_2}(x)) = (\tau_{g_1} \circ \tau_{g_2})(x)$
- (3) $\text{Kern}(\tau) = \{e\}$, denn ist $\tau(g) = id_g$, so ist $\forall x \in G : \tau_g(x) = gx = x$, also $g = e$ ■

Definition + Bemerkung 1.2.5

Sei G Gruppe, $g \in G$

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

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

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

Beweis: $\forall x \in G : c(g_1 g_2)(x) = (g_1 g_2)x(g_1 g_2)^{-1} = g_1(g_2 x g_2^{-1})g_1^{-1} = (c(g_1) \circ c(g_2))(x)$ ■

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

- (d) $Z(G) := \text{Kern}(c)$ heißt **Zentrum** von G . Es ist $Z(G) = \{g \in G : \forall x \in G : gx = xg\}$

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

- (f) Ist $f : G \rightarrow G'$ Gruppenhomomorphismus, so ist $\text{Kern}(f)$ Normalteiler in G .

Beweis: Sei $x \in \text{Kern}(f), g \in G$. Dann ist $f(gxg^{-1}) = f(g)\underbrace{f(x)}_{e'}f(g)^{-1} = e'$.
 ■

- (g) $\text{Aut}_i(G)$ ist Normalteiler in $\text{Aut}(G)$

Beweis: Sei $\varphi \in \text{Aut}(G), g \in G$: z.z.: $\varphi \cdot c_g \cdot \varphi^{-1} \in \text{Aut}_i(G)$.
 Es ist $(\varphi \cdot c_g \cdot \varphi^{-1})(x) = \varphi(c_g(\varphi^{-1}(x))) = \varphi(g \cdot \varphi^{-1}(x) \cdot g^{-1}) = \varphi(g) \cdot \varphi(\varphi^{-1}(x)) \cdot \varphi(g^{-1}) = \varphi(g) \cdot x \cdot \varphi(g)^{-1} = c_{\varphi(g)}(x) \Rightarrow \varphi \circ c_g \circ \varphi^{-1} = c_{\varphi(g)} \in \text{Aut}_i(G)$ ■

Definition + Bemerkung 1.2.6

Sei G Gruppe, $H \subseteq G$ Untergruppe.

- (a) Für $g \in G$ heißt $g \cdot H = \{g \cdot h : h \in H\} = \tau_g(H)$ **Linksnebenklasse** von G bzgl. H und $H \cdot g = \{h \cdot g : h \in H\}$ **Rechtsnebenklasse**
- (b) Für $g_1, g_2 \in G$ gilt: $g_1H \cap g_2H \neq \emptyset \Leftrightarrow g_1H = g_2H$

Beweis: Sei $y = g_1h_1 = g_2h_2 \in g_1H \cap g_2H$ und $h_1, h_2, h \in H \Rightarrow g_1 = g_2h_2h_1^{-1} \Rightarrow g_1h = g_2h_2h_1^{-1}h \in g_2H \Rightarrow g_1H \subseteq g_2H$, die Umkehrung folgt analog. ■

- (c) H ist genau dann Normalteiler, wenn $\forall g \in G : g \cdot H = H \cdot g$

Beweis: $gH = Hg \Leftrightarrow H = gHg^{-1}$ ■

- (d) Alle Nebenklassen von G bzgl. H sind gleichmächtig.

Beweis: $\tau_g : \underbrace{H}_{e \cdot H} \rightarrow g \cdot H, h \mapsto g \cdot h$ 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

$$\begin{array}{ccc} \{\text{Linksnebenklasse}\} & \rightarrow & \{\text{Rechtsnebenklasse}\} \\ g \cdot H & \mapsto & H \cdot g^{-1} \end{array}$$

ist **wohldefiniert** und bijektiv.

Wohldefiniertheit: ist $g_1H = g_2H$, also $g_2 = g_1h$ für ein $h \in H \Rightarrow Hg_2^{-1} = H(g_1h)^{-1} = H \cdot h^{-1}g_1^{-1} = Hg_1^{-1}$ ■

- (f) **Satz von Lagrange:** Ist G endlich, so ist

$$[G : H] = \frac{|G|}{|H|}$$

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

1.3 Quotientenbildung

Definition + Bemerkung 1.3.1

Sei $f : M \rightarrow M'$ 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 $x \in M$ sei $\bar{x} := [x]_f := \{y \in M : y \sim_f x\} = \{y \in M : f(y) = f(x)\}$. Es ist $\bar{x} = f^{-1}(f(x))$
Weiter sei $\bar{M} := M / \sim_f := \{\bar{x} : x \in M\}$
- (c) $\bar{f} : \bar{M} \rightarrow \text{Bild}(f)$, $\bar{x} \mapsto f(x)$ ist eine bijektive Abbildung.

Definition 1.3.2

Ist (M, \cdot) und $(M', *)$ ein $\left\{ \begin{array}{l} \cdot \\ \cdot \end{array} \right\}$, und $(M, \cdot) \rightarrow (M', *)$ ein Homomorphismus, so wird durch $\bar{x} \cdot \bar{y} := \overline{x \cdot y}$ eine Verknüpfung auf \bar{M} definiert. So wird (\bar{M}, \cdot) auch zu einem $\left\{ \begin{array}{l} \cdot \\ \cdot \end{array} \right\}$.

Beweis: z.z.: \cdot ist wohldefiniert. Seien also $x' \in \bar{x}, y' \in \bar{y}$ zu zeigen: $\overline{x' \cdot y'} = \overline{x \cdot y}$ dh. $f(x' \cdot y') = f(x \cdot y)$ dh. $f(x') = f(x), f(y') = f(y)$ Es ist $f(x' \cdot y') = f(x') * f(y') = f(x) * f(y) = f(x \cdot y)$ ■

Definition + Bemerkung 1.3.3

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

- (a) $\bar{G} = G / \sim_f$ ist die Menge der Linksnebenklassen bzgl. $\text{Kern}(f)$ also ist für jedes $g \in G$: $[g]_f = g \cdot \text{Kern}(f) = \text{Kern}(f) \cdot g$.
- (b) $\bar{G} = G / \text{Kern}(f)$ heißt **Faktorgruppe** von G bzgl. $\text{Kern}(f)$.

Beweis: Seien $x, y \in G$. Dann gilt: $\bar{x} = \bar{y} \Leftrightarrow f(x) = f(y) \Leftrightarrow f(x) \cdot f(y^{-1}) = e' \Leftrightarrow xy^{-1} \in \text{Kern}(f) \Leftrightarrow y = (xy^{-1})^{-1}x \in \text{Kern}(f) \cdot x \Leftrightarrow x^{-1}y \in \text{Kern}(f) \Leftrightarrow y = x(x^{-1}y) \in x \cdot \text{Kern}(f) \Leftrightarrow y \cdot \text{Kern}(f) = x \cdot \text{Kern}(f)$ ■

Beispiel: $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{C}^\times, \cdot)$, $t \mapsto e^{2\pi it}$ ist ein Gruppenhomomorphismus. Es ist $\exp(t_1) = \exp(t_2) \iff 1 = e^{2\pi i(t_2 - t_1)} \iff t_2 - t_1 \in \mathbb{Z}$, also ist $\text{Kern}(\exp) = \mathbb{Z}$.

Die Abbildung $[0, 1) \rightarrow \mathbb{R}/\mathbb{Z}$, $t \mapsto [t]_f$ ist bijektiv, spiegelt aber die Eigenschaften dieser Gruppe nicht wieder. Besser geeignet ist die Bijektion \mathbb{R}/\mathbb{Z} , $\bar{t} \mapsto e^{2\pi it}$.

Bemerkung 1.3.4

Sei G Gruppe. Es ist $N \subseteq G$ Normalteiler, genau dann, wenn es eine Gruppe G' mit einem surjektiven Gruppenhomomorphismus $f : G \rightarrow G'$ und $N = \text{Kern}(f)$ gibt.

Beweis: Die Richtung \Leftarrow folgt aus 1.2.5 f). Sei $G' := \{x \cdot N, x \in G\} (\subseteq \mathcal{P}(G))$
 Für $x, y \in G$ setze $(x \cdot N)(y \cdot N) = (xy \cdot N)$
Behauptung: (G', \cdot) ist Gruppe, **denn:**

- (i) Die Verknüpfung ist wohldefiniert: Seien $x, x', y, y' \in G$ mit $x \cdot N = x' \cdot N, y \cdot N = y' \cdot N$. Dann gibt es $n, m \in N$ mit $x' = xn, y' = ym \Rightarrow x', y' = x(ny)m$. Da N Normalteiler ist, gibt es $n' \in N$ mit $ny = yn' \Rightarrow x'y' = xyn'm \Rightarrow x'y' \cdot N = xy \cdot N$
- (ii) alle übrigen Eigenschaften "vererben" sich von G auf G'
 $f : G \rightarrow G', x \mapsto x \cdot N$ ist surjektiver Gruppenhomomorphismus mit $\text{Kern}(f) = N$
 ■

Definition + Bemerkung 1.3.5

Sei G Gruppe, $N \subseteq G$ Normalteiler. Die Gruppe G' aus dem vorherigen Beweis heißt Faktorgruppe von G nach N , und wir schreiben $G' = G/N$ („ G modulo N “). Sie ist gleich der Faktorgruppe $G/\text{Kern}(f)$ für das f aus der vorherigen Bemerkung (ii).

Satz 1

- (a) Sei $f : M \rightarrow M'$ eine Abbildung. $\bar{M} := M/\sim_f$ und $p : M \rightarrow \bar{M}, x \mapsto \bar{x}$ die Restklassenabbildung. Dann existiert genau eine Abbildung $\bar{f} : \bar{M} \rightarrow M'$ mit $f = \bar{f} \circ p$. Es ist p surjektiv und \bar{f} injektiv.
- (b) Ist $f : M \rightarrow M'$ ein Homomorphismus von $\left\{ \begin{smallmatrix} \cdot \\ \cdot \\ \cdot \end{smallmatrix} \right\}$, so ist \bar{M} auch ein $\left\{ \begin{smallmatrix} \cdot \\ \cdot \\ \cdot \end{smallmatrix} \right\}$ und p, \bar{f} sind Homomorphismen.
- (c) **Homomorphiesatz**
 Ist $f : G \rightarrow G'$ ein Gruppenhomomorphismus, so ist $G/\text{Kern}(f) \cong \text{Bild}(f)$
- (d) **Universelle Abbildungseigenschaft (UAE) der Faktorgruppe**
 Sei G Gruppe, $N \subseteq G$ Normalteiler. Dann gibt es zu jedem Gruppenhomomorphismus $f : G \rightarrow G'$ mit $N \subseteq \text{Kern}(f)$ genau einen Gruppenhomomorphismus $f_N : G/N \rightarrow G'$ mit $f = f_N \circ p_N$, wobei p_N die Restklassenabbildung ist.

Beweis:

- (a) $\bar{f}(\bar{x}) = f(x)$, wie in 1.3.1 c)
- (c) $\bar{f} : G/\text{Kern}(f) \rightarrow \text{Bild}(f)$ ist injektiv, ein Gruppenhomomorphismus nach a), b) und 1.3.3. Also ist \bar{f} ein bijektiver Homomorphismus, also eine Isomorphie.

(d) Setze $f_N(x \cdot N) := f(x)$
 f_N ist wohldefiniert: Ist $gN = g'N$, so ist $(g')^{-1}g \in N \subseteq \text{Kern}(f)$, also $f((g')^{-1}g) = e' \implies f(g') = f(g)$. Die Eindeutigkeit von \bar{f} , sowie dass \bar{f} ein Homomorphismus ist, ist klar. ■

1.4 Abelsche Gruppen

Bemerkung 1.4.1 (a) Jede zyklische Gruppe ist isomorph zu \mathbb{Z} oder zu $\mathbb{Z}/n\mathbb{Z}$ für genau ein $n \in \mathbb{N} \setminus \{0\}$.

Beweis: Sei $G = \langle g \rangle$, $\varphi_g : \mathbb{Z} \rightarrow G$, $n \mapsto g^n$ (siehe 1.2.3)
 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 $H = n\mathbb{Z}$ für ein $n \in \mathbb{N}$ ist, folgt die Behauptung. ■

(b) Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

Beweis: Sei $G = \langle g \rangle$ zyklisch, $H \subseteq G$ Untergruppe. Ist $H = \{e\}$, so ist $H = \langle e \rangle$ zyklisch. Anderenfalls sei $n := \min\{k \in \mathbb{N} \setminus \{0\} : g^k \in H\}$.

Behauptung: $\langle g^n \rangle = H$, denn sonst gibt es ein $m > 0$ mit $g^m \in H \setminus \langle g^n \rangle$.
 Sei m minimal mit dieser Eigenschaft. Dann ist $0 < m - n < m$. Aber:
 $g^{m-n} = g^m g^{-n} \in H \implies g^{m-n} \in \langle g^n \rangle \implies g^m = g^{m-n} g^n \in \langle g^n \rangle$ Wid! ■

Definition + Bemerkung 1.4.2

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

(b) $\varphi(1) = 1 = \varphi(2)$, $\varphi(p) = p - 1$ für p Primzahl, $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, falls m, n teilerfremd, $\varphi(p^k) = p^{k-1}(p - 1)$, für p Primzahl.

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

Beweis: $n = |G| = \sum_{d|n} |\{x \in G, \text{ord}(x) = d\}| \stackrel{(d)}{=} \sum_{d|n} \varphi(d)$ ■

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

Beweis: Sei $G = \langle g \rangle$. Für $x = g^k \in G$ ist $\text{ord}(x) = \frac{n}{\text{ggT}(k, n)}$. Also ist $\text{ord}(x) = d \Leftrightarrow \text{ggT}(k, n) = \frac{n}{d} \implies |\{g \in G \mid \text{ord}(g) = d\}| = |\{l \in \{1, \dots, n\} \mid \text{ggT}(l, d) = 1\}| = \varphi(d)$. ■

Beispiel:

(1)

$$\{e^{\frac{2\pi i k}{n}} : n \in \mathbb{N} \setminus \{0\}, 0 \leq k < n\}$$

ist zyklische Untergruppe von \mathbb{C}^* der Ordnung n . (n -te Einheitswurzel)

(2) Sei $V = \{id, \tau, \sigma_1, \sigma_2\}$ mit $\tau =$ Drehung im $\mathbb{R}^2 \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$,

$\sigma_1 =$ Spiegelung an der x -Achse $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$,

$\sigma_2 =$ Spiegelung an der y -Achse $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. V ist abelsche Gruppe, aber **nicht** zyklisch. V heißt **Kleinsche Vierergruppe** $V \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$$(3) \begin{array}{ccc} \mathbb{Z}/6\mathbb{Z} & \cong & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \\ \{1, a, a^2, a^3, a^4, a^5\} & & \{1, \sigma\} \quad \{1, \tau, \tau^2\} \\ a & \mapsto & (\sigma, \tau) \end{array}$$

Definition + Bemerkung 1.4.3

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

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

Beweis: z.z.: $\langle A \rangle = \bigcap_{\substack{H \subseteq G \text{ Ugr.} \\ A \subseteq H}} H$ ist Untergruppe in G .

(i) $\forall H \subseteq G, H$ Untergruppe: $e \in H \Rightarrow e \in \langle A \rangle \Rightarrow \langle A \rangle \neq \emptyset$

(ii) Seien $x, y \in \langle A \rangle, H$ Untergruppe von G mit $A \subseteq H \Rightarrow x, y \in H \stackrel{H \text{ Ugr.}}{\implies} xy^{-1} \in H \Rightarrow xy^{-1} \in \langle A \rangle. \Rightarrow \langle A \rangle$ Untergruppe von G . ■

1 Gruppen

$$(b) \langle A \rangle = \{g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n}, n \in \mathbb{N}, g_i \in A, \varepsilon_i \in \{\pm 1\}\}$$

Definition + Proposition 1.4.4

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

- (a) A heißt **freie abelsche Gruppe** mit Basis X , wenn gilt: $A = \langle X \rangle$ und für alle paarweisen verschiedenen Elemente $x_1, \dots, x_n \in X$ ist $\sum_{i=1}^n n_i x_i = 0$, $n_i \in \mathbb{Z}$, nur dann möglich ist, wenn alle $n_i = 0$ sind.

Jedes $a \in A$ hat dann eine eindeutige Darstellung $a = \sum_{x \in X} n_x x$ mit $n_x \in \mathbb{Z}$, $n_x \neq 0$ nur für endlich viele $x \in X$.

Beweis: $A \rightarrow \mathbb{Z}^X : \sum n_x x \mapsto (n_x)_{x \in X}$ ist Isomorphismus. ■

- (b) \mathbb{Z} ist frei mit Basis $\{1\}$.

- (c) A ist frei mit Basis X genau dann, wenn $A \cong \bigoplus_{x \in X} \mathbb{Z}$.

- (d) Ist A frei mit Basis X , und X endlich, so heißt $|X|$ der Rang von A .

- (e) (UAE der freien abelschen Gruppe)

Ist A frei mit Basis X , dann gibt es zu jeder abelschen Gruppe A' und jeder Abbildung $f : X \rightarrow A'$ genau einen Homomorphismus $\varphi : A \rightarrow A'$ mit $\forall x \in X : \varphi(x) = f(x)$

Beweis: Setze $\varphi(\sum_{x \in X} n_x x) := \sum_{x \in X} n_x f(x)$ ■

Beispiel: (wichtig!) X endlich, $X = \{x_1, \dots, x_n\}$. Dann ist $\mathbb{Z}^X \cong \mathbb{Z}^n$

\mathbb{Z}^n ist "so etwas ähnliches" wie ein Vektorraum ("freier Modul"). Insbesondere lassen sich die Gruppenhomomorphismen $\mathbb{Z}^n \rightarrow \mathbb{Z}^m$ durch eine $m \times n$ -Matrix mit Einträgen in \mathbb{Z} beschreiben.

Beispiel: Ist $(\mathbb{Q}, +)$ frei? $(\mathbb{Q}, +)$ ist nicht frei von Rang 1, sonst wäre $\mathbb{Q} = r\mathbb{Z}$ für ein $r \in \mathbb{Q}$.

Sei also $(\mathbb{Q}, +)$ frei mit Basis X und $x_1 \neq x_2 \in X$. Es gilt $x_i = \frac{n_i}{m_i}$, $n_i, m_i \in \mathbb{Z}$. Dann ist $n_2 m_1 x_1 - n_1 m_2 x_2 = 0$, also sind x_1, x_2 linear abhängig.

Satz 2 (Elementarteilersatz)

Jede Untergruppe einer freien abelschen Gruppe von endlichem Rang n ist frei mit Rang $r \leq n$. Genauer:

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 teilt 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. Die a_i sind eindeutig bestimmt.

Beweis: 1. Schritt: H ist endlich erzeugt: Induktion über n :

$n = 1$: ✓

$n > 1$: Sei e_1, \dots, e_n Basis von \mathbb{Z}^n , $\pi : \mathbb{Z}^n \rightarrow \mathbb{Z}$, $\sum_{i=1}^n a_i e_i \mapsto a_n$

(Projektion auf letzte Komponente).

1. Fall: $\pi(H) = \{0\} \Rightarrow H \subseteq \mathbb{Z}^{n-1}$, also endlich erzeugt nach **IV**.

2. Fall: $\pi(H) = l\mathbb{Z}$ für ein $l \in \mathbb{N} \setminus \{0\}$ Sei $y \in H$ mit $\pi(y) = l$

Beh.: $H \cong \langle y \rangle \oplus (H \cap \text{Kern}(\pi))$ Dann folgt die Behauptung von Schritt 1, da $\text{Kern}(\pi) \cong \mathbb{Z}^{n-1}$, $H \cap \text{Kern}(\pi)$ Untergruppe von \mathbb{Z}^{n-1} , existiert also nach **IV** \Rightarrow

Bew. der Beh.: $\langle y \rangle \cap (H \cap \text{Kern}(\pi)) = \{0\}$ nach Definition von $y \Rightarrow$ Summe direkt.

Sei $z \in H$ mit $\pi(z) = k \cdot l$ für ein $k \in \mathbb{Z} \Rightarrow z - ky \in H \cap \text{Kern}(\pi) \Rightarrow$ Beh.

2. Schritt: Sei y_1, \dots, y_r 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

Einbettung $H \hookrightarrow \mathbb{Z}^n$ bzgl. 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:

$$\tilde{A} = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_r \end{pmatrix} \text{ mit } a_i \in \mathbb{Z} \text{ und } a_i \text{ teilt } a_{i+1} \forall i = 1, \dots, r-1$$

3. Schritt: Das geht! Ganzzahliger Gauß-Algorithmus, „Elementarteileralgorithmus“.

- (i) Suche den betragsmäßig kleinsten Matrixeintrag $\neq 0$ und bringe diesen nach a_{11} . Dazu braucht man höchstens eine Zeilen- und eine Spaltenumformung.
- (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} : $a_{i1} = qa_{11} + r$ mit $0 < r < |a_{11}|$. Ziehe dann von der i -ten Zeile das q -fache der ersten ab. Die neue i -te Zeile beginnt nun mit $\tilde{a}_{i1} = r \Rightarrow$ 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 $\frac{a_{i1}}{a_{11}}$ -fache der ersten Zeile abzieht.

1 Gruppen

Gegebenenfalls zurück zu (i).

(iv) Genauso wird die erste Zeile zu $(a_{11}, 0, \dots, 0)$

(v) Gibt es jetzt noch einen Matrixeintrag, der nicht durch a_{11} teilbar ist, schreibe $a_{ij} = qa_{11} + r$ mit $0 < r < |a_{11}|$ Ziehe von der i -ten Zeile das q -fache der ersten ab. Die neue i -te Zeile lautet dann:

$$(-qa_{11}, a_{i2}, \dots, a_{ij}, \dots, a_{ir})$$

(da $a_{i1} = 0, a_{1k} = 0$ für $1 < k \leq r$)

Addiert man zur j -ten Spalte die erste, so ist das neue Element $\tilde{a}_{ij} = a_{ij} - qa_{11} = r \Rightarrow$ Zurück zu (i)

(vi) Nach endlich vielen Schritten erhalte Matrix

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix},$$

in der alle Einträge von A' durch a_{11} teilbar sind. Wende nun den Algorithmus auf A' an.

Noch zu zeigen: Die Eindeutigkeit der a_i :

r ist eindeutig, da r der Rang von H ist.

Ist x_1, \dots, x_n Basis von \mathbb{Z}^n , und a_1x_1, \dots, a_rx_r eine Basis von H wie im Satz, so ist $H \subseteq \mathbb{Z}^r$ und $\mathbb{Z}^r/H \cong \bigoplus_{i=1}^r \mathbb{Z}/a_i\mathbb{Z}$, denn $\varphi: \mathbb{Z}^r \rightarrow \bigoplus_{i=1}^r \mathbb{Z}/a_i\mathbb{Z}, x_i \mapsto e_i := (0, \dots, s_i, \dots, 0)$, (s_i Erzeuger von $\mathbb{Z}/a_i\mathbb{Z}$) ist ein surjektiver Homomorphismus.

$\text{Kern}(\varphi) \supseteq \langle \{a_1x_1, \dots, a_rx_r\} \rangle = H$, sowie $\text{Kern}(\varphi) \subseteq H$, denn für $y \in \text{Kern}(\varphi)$, $y = \sum_{i=1}^r b_ix_i$ gilt: $\varphi(y) = \sum_{i=1}^r b_ie_i = (b_1s_1, \dots, b_rs_r) = (0, \dots, 0)$, also gilt $a_i \mid b_i, i = 1, \dots, r$, also $y \in H$. Nach dem Homomorphiesatz gilt also: $\mathbb{Z}^r/H \cong \bigoplus_{i=1}^r \mathbb{Z}/a_i\mathbb{Z}$.

Zu zeigen ist nun: Für $T := \bigoplus_{i=1}^r \mathbb{Z}/a_i\mathbb{Z} \cong \bigoplus_{i=1}^s \mathbb{Z}/b_i\mathbb{Z} =: \tilde{T}$ mit $a_i \mid a_{i+1}, i = 1, \dots, r-1$ und $b_i \mid b_{i+1}, i = 1, \dots, s-1$ gilt: $r = s$ und $a_i = b_i, i = 1, \dots, r$.

Für $z \in T$ gilt: $\text{ord}(z) \mid a_r$, denn mit $z = (z_1, \dots, z_n), z_i \in \mathbb{Z}/a_i\mathbb{Z}$ gilt $a_r \cdot z = (a_raz_1, \dots, a_rz_r) = (0, \dots, 0)$. Genauso: $\text{ord}(z) \mid b_s$. T enthält das Element $(0, \dots, 0, s_r) = e_r$ und $\text{ord}(e_r) = a_r$, also gilt $a_r \mid b_s$ und $b_s \mid a_r$, also $a_r = b_s$. Die Behauptung folgt dann per Induktion über r ■

Ergänzung:

- (1) In der Situation von Satz 2 heißen die a_{ij} $i = 1, \dots, r$ die **Elementarteiler** von H .
- (2) Ist $A = (h_1, \dots, h_r) \in \mathbb{Z}^{n \times r}$, so erzeugen die Spalten h_1, \dots, h_r eine Untergruppe von \mathbb{Z}^n . A ist Darstellungsmatrix der Einbettung $H \hookrightarrow \mathbb{Z}^n$. Die Elementarteiler von H heißen auch Elementarteiler von A .

Folgerung 1.4.5 (Struktursatz für endlich erzeugte abelsche Gruppen)
 Jede endlich erzeugte abelsche Gruppe A ist die direkte Summe von zyklischen Gruppen:

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

mit $r, m, a_1, \dots, a_m \in \mathbb{N}$, $\forall i: a_i \geq 2$, a_i teilt a_{i+1} für $i = 1, \dots, m-1$. Dabei sind r, m und die a_i eindeutig bestimmt.

Beweis: Sei x_1, \dots, x_n ein Erzeugendensystem von A .
 Nach 1.4.4 gibt es einen surjektiven Gruppenhomomorphismus $\varphi: \mathbb{Z}^n \rightarrow A$ mit $\varphi(e_i) = x_i$, für $i = 1, \dots, n$.
 Nach Homomorphiesatz (Satz 1) ist dann $A \cong \mathbb{Z}^n / \text{Kern}(\varphi)$.
 Nach Satz 2 gibt es $m \in \mathbb{N}$, $m \leq n$, eine Basis $\{z_1, \dots, z_n\}$ von \mathbb{Z}^n und Elementarteiler a_1, \dots, a_m mit a_i teilt a_{i+1} für $i = 1, \dots, m-1$, so dass $\{a_1 z_1, \dots, a_m z_m\}$ Basis von $\text{Kern}(\varphi)$ ist. Dann ist $A \cong \mathbb{Z}^n / \text{Kern}(\varphi) \cong \left(\bigoplus_{i=1}^n \mathbb{Z} z_i \right) / \left(\bigoplus_{i=1}^m a_i \mathbb{Z} z_i \right) \cong \bigoplus_{i=1}^m (\mathbb{Z} z_i / a_i \mathbb{Z} z_i) \oplus \bigoplus_{i=m+1}^n \mathbb{Z} z_i \cong \bigoplus_{i=1}^m \mathbb{Z}/a_i\mathbb{Z} \oplus \mathbb{Z}^{n-m}$

Ist $a_1 = 1$, so lassen wir die $\mathbb{Z}/1\mathbb{Z} = \{e\}$ weg. ■

1.5 Freie Gruppen

Definition + Bemerkung 1.5.1

Sei F eine Gruppe und $X \subseteq F$

- (a) F heißt **freie Gruppe mit Basis X** , wenn jedes $y \in F$ eine eindeutige Darstellung $y = x_1^{\varepsilon_1} \cdot \dots \cdot x_n^{\varepsilon_n}$ hat, in der
- $n \geq 0$ (für $n = 0$ ist y das "leere Wort", es ist das neutrale Element in F)
 - $x_i \in X$ für $i = 1, \dots, n$
 - $\varepsilon_i \in \{+1, -1\}$ für $i = 1, \dots, n$
 - $x_{i+1}^{\varepsilon_{i+1}} \neq x_i^{-\varepsilon_i}$ für $i = 1, \dots, n-1$

1 Gruppen

- (b) Ist F frei mit Basis X , so gilt für jedes $x \in X$: $x^{-1} \notin X$.
- (c) Ist F frei mit Basis X , so ist F torsionsfrei, das heißt: $\text{ord}(x) = \infty$ für jedes $x \in F$, $x \neq e$.
- (d) $(\mathbb{Z}, +)$ ist frei mit Basis $\{1\}$ oder Basis $\{-1\}$
- (e) Ist F frei mit Basis X und $|X| \geq 2$, so ist F nicht abelsch.

Beweis: Seien $x_1, x_2 \in X$: $x_1 \neq x_2 \Rightarrow x_1 x_2 x_1^{-1} x_2^{-1} \neq e \Rightarrow x_1 x_2 \neq x_2 x_1$ ■

Satz 3

- (a) Zu jeder Menge X gibt es eine freie Gruppe $F(X)$ mit Basis X .
- (b) Zu jeder Gruppe G und jeder Abbildung $f : X \rightarrow G$ gibt es genau einen Gruppenhomomorphismus $\phi : F(X) \rightarrow G$ mit $\phi(x) = f(x)$ für alle $x \in X$.
- (c) Jede Gruppe "ist" (d.h. ist isomorph zu einer) Faktorgruppe einer freien Gruppe.
- (d) $F(X) \cong F(Y) \Leftrightarrow |X| = |Y|$

Beweis:

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

Schreibweise: $(x, 1) =: x$, $(x, -1) =: x^{-1} \Rightarrow i(x) = x^{-1}$, $i(x^{-1}) = x$

Ein Element $g = (x_1, \dots, x_n) \in F_0^a(X^\pm)$ (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 $F_0^a(X^\pm)$

Def.: Zwei Wörter in $F_0^a(X^\pm)$ heißen **äquivalent**, wenn sie durch endliches Einfügen oder Streichen von Paaren der Form $(x, i(x))$, $x \in X^\pm$ auseinander hervorgehen.

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

Beh.: In jeder Äquivalenzklasse gibt es genau ein reduziertes Wort. Dann definiere Verknüpfung auf $F(X) : (x_1, \dots, x_n) \star (y_1, \dots, y_m)$ sei **das** reduzierte Wort in der Äquivalenzklasse von $(x_1, \dots, x_n, y_1, \dots, y_m)$. Dieses Produkt ist **assoziativ**: Für $x, y, z \in F(X)$ ist $(xy)z$ das eindeutig bestimmte reduzierte Wort in der Klasse von $(x_1, \dots, x_n, y_1, \dots, y_m, z_1, \dots, z_l)$, und das gleiche gilt für $x(yz)$.

neutrales Element: $e = ()$

inverses Element zu (x_1, \dots, x_n) ist $(i(x_n), i(x_{n-1}), \dots, i(x_1)) \Rightarrow F(X)$ ist Gruppe. $F(X)$ ist frei mit Basis X nach Konstruktion.

Bew. der Beh.: In jeder Klasse gibt es ein reduziertes Wort: **ja!**

Eindeutigkeit: Seien x, y reduziert und äquivalent. Dann gibt es ein Wort w , aus

dem sowohl x als auch y durch Streichen hervorgehen. Zu zeigen also: Jede Reihenfolge von Streichen führt zum selben reduzierten Wort.

Induktion über die Länge $l(w)$:

$$l(w) = 0 \quad \checkmark$$

$$l(w) = 1 \quad \checkmark$$

Sei $l(w) \geq 2$; Ist w reduziert, so ...

Enthält w genau ein Paar $(x_\nu, i(x_\nu))$, so muß dies als erstes gestrichen werden.

Es entsteht w' mit $l(w') = l(w) - 2 \stackrel{IV}{\Rightarrow}$ Beh. Enthält w Paare $(x_\nu, i(x_\nu))$ und $(x_\mu, i(x_\mu))$, so gibt es zwei Fälle: (Sei oBdA $\mu > \nu$)

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

$\mu \geq \nu + 2$: Streichen beider Paare, erhalte w'' mit $l(w'') = l(w) - 4 \stackrel{IV}{\Rightarrow}$ Beh.

- (b) Sei $f : X \rightarrow G$ eine Abbildung. Für $w = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ setze

$$\phi(w) = f(x_1)^{\epsilon_1} \cdots f(x_n)^{\epsilon_n}.$$

Dies muss eindeutig so sein, und so wird ein Homomorphismus definiert.

- (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 , $f : S \rightarrow G$ die Inklusion und $\phi : F(S) \rightarrow G$ der Homomorphismus aus (b). ϕ ist surjektiv, weil $\phi(F(S))$ Untergruppe ist, die S enthält. Also ist nach Homomorphiesatz $G \cong F(S)/\text{Kern}(\phi)$

Beispiele:

- a) G zyklisch von Ordnung $n \in \mathbb{N}$, dann ist $G \cong \mathbb{Z}/n\mathbb{Z}$.

- b) $\mathbb{Z}^2 := \mathbb{Z} \times \mathbb{Z}$, $S = \{(0, 1) =: x, (1, 0) =: y\}$. Der Homomorphismus $\varphi : F(S) \rightarrow \mathbb{Z}^2$, $x \mapsto (0, 1)$, $y \mapsto (1, 0)$ bildet $w = x^{n_1} y^{m_1} \cdots x^{n_d} y^{m_d} \in F(S)$ auf $\varphi(w) = (\sum_{i=1}^d n_i, \sum_{i=1}^d m_i)$ ab, also ist $\text{Kern } \varphi = \{w = x^{n_1} y^{m_1} \cdots x^{n_d} y^{m_d} \in F(S) \mid \sum_{i=1}^d n_i = \sum_{i=1}^d m_i = 0\} = \langle \{w_1 w_2 w_1^{-1} w_2^{-1}, w_1, w_2 \in F(S)\} \rangle = G^{\text{ab}}$. Kern φ ist kleinster Normalteiler von $F(\{x, y\})$, der $xyx^{-1}y^{-1}$ enthält, daher ist $\mathbb{Z}^2 \cong F(\{x, y\}) / \langle xyx^{-1}y^{-1} \rangle_{\text{NT}}$.

- (d) Erstmal ist klar, dass für jede Abbildung $g : X \rightarrow Y$ ein eindeutiger Gruppenhomomorphismus $\varphi_g : F(X) \rightarrow F(Y)$ mit $\varphi_g(x) = g(x)$ für alle $x \in X$ existiert. (Dies folgt aus (b), wenn die Abbildung $X \rightarrow F(Y)$, $x \mapsto g(x)$ als f eingesetzt wird.)

" \Leftarrow " Sei $f : X \rightarrow Y$ bijektive Abbildung. Dazu gibt es Gruppenhomomorphismen $\varphi_f : F(X) \rightarrow F(Y)$ sowie $\varphi_{f^{-1}} : F(Y) \rightarrow F(X)$. Es ist sowohl $\varphi_{f^{-1}} \circ \varphi_f|_X = id_X$ als auch $id_{F(X)}|_X = id_X$, also folgt aus der Eindeutigkeit (b), dass $\varphi_{f^{-1}} \circ \varphi_f = id_{F(X)}$. Analog; $\varphi_f \circ \varphi_{f^{-1}} = id_{F(Y)}$. Also ist φ_f ein Isomorphismus.

" \Rightarrow " Die Anzahl der Gruppenhomomorphismen von $F(X)$ in $\mathbb{Z}/2\mathbb{Z}$ ist gleich der Anzahl der Abbildungen von X nach $\{0, 1\}$ (wegen (b)), und diese ist $|2^X| = |\mathcal{P}(X)|$. Sei $|X| \neq |Y|$, dann ist $|\mathcal{P}(X)| \neq |\mathcal{P}(Y)|$. ■

1.6 Kategorien und Funktoren

Definition 1.6.1

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

- (i) Für jedes $A \in Ob \mathcal{C}$ gibt es ein Element $id_A \in Mor_{\mathcal{C}}(A, A)$
- (ii) Für je drei Objekte $A, B, C \in Ob \mathcal{C}$ gibt es eine Abbildung \circ :

$$\begin{array}{ccc} Mor(B, C) & \times & Mor(A, B) & \rightarrow & Mor(A, C) \\ (g & , & f) & \mapsto & g \circ f \end{array}$$

mit

$$\begin{array}{ll} g \circ id_A & = g & \text{für alle } g \in Mor(A, B) \\ id_B \circ f & = f & \text{für alle } f \in Mor(A, B) \\ (h \circ g) \circ f & = h \circ (g \circ f) & \text{für alle } f \in Mor(A, B), g \in Mor(B, C), h \in Mor(C, D) \end{array}$$

Beispiel:

- (1) Mengen mit Abbildungen
- (2) Mengen mit bijektiven Abbildungen
- (3) K -Vektorräume mit k -linearen Abbildungen
- (4) Halbgruppen mit Homomorphismen
- (5) Monoide mit Homomorphismen
- (6) Magmen mit Homomorphismen
- (7) Gruppen mit Homomorphismen
- (8) abelsche Gruppen mit Homomorphismen
- (9) topologische Räume mit stetigen Abbildungen

Definition 1.6.2

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

- (a) Ein **kovarianter Funktor** $F : \mathcal{A} \rightarrow \mathcal{B}$ besteht aus einer Abbildung $F : Ob \mathcal{A} \rightarrow Ob \mathcal{B}$, sowie für je zwei Objekte $X, Y \in Ob \mathcal{A}$ aus einer Abbildung $F : Mor_{\mathcal{A}}(X, Y) \rightarrow Mor_{\mathcal{B}}(F(X), F(Y))$, so dass gilt:

- (i) $F(id_X) = id_{F(X)}$ für alle $X \in Ob \mathcal{A}$
 - (ii) $F(g \circ f) = F(g) \circ F(f)$ für alle $f \in Mor_{\mathcal{A}}(A, B), g \in Mor_{\mathcal{A}}(B, C)$
- (b) Ein **kontravarianter** Funktor $F : \mathcal{A} \rightarrow \mathcal{B}$ ist ebenso wie in (a) definiert. Ausnahme: $F : Mor_{\mathcal{A}}(X, Y) \rightarrow Mor_{\mathcal{B}}(F(Y), F(X)), \dots$ und $F(g \circ f) = F(f) \circ F(g)$

Beispiel:

- (1) $V : \text{Gruppen} \rightarrow \text{Mengen}, (G, \cdot) \mapsto G, V(f) = f$ ist der „Vergissfunktoren“
- (2) a) $Im : \text{Mengen} \rightarrow \text{Mengen}, Im(X) = \mathcal{P}(X)$, für $f : X \rightarrow Y$ ist $Im(f) : \mathcal{P}(X) \rightarrow \mathcal{P}(Y), Im(f)(U) = f(U), U \in \mathcal{P}(X)$ ist kovariant.
- b) $Urb : \text{Mengen} \rightarrow \text{Mengen}, Urb(X) = \mathcal{P}(X)$, für $f : X \rightarrow Y$ ist $Urb(f) : \mathcal{P}(Y) \rightarrow \mathcal{P}(X), Urb(f)(V) = f^{-1}(V), V \in \mathcal{P}(Y)$ ist kontravariant.
- (3) Sei \mathcal{C} Kategorie, X ein Objekt in \mathcal{C} . Definiere Funktoren $\mathcal{C} \rightarrow \text{Mengen}$ durch
 $Hom(X, \cdot) : Y \mapsto Mor_{\mathcal{C}}(X, Y)$ (kovariant)
 $Hom(\cdot, X) : Y \mapsto Mor_{\mathcal{C}}(Y, X)$ (kontravariant)
 Für $f \in Mor(Y, Z)$ ist $Hom(X, \cdot)(f) : Mor(X, Y) \rightarrow Mor(X, Z)$ gegeben durch $g \mapsto f \circ g$ und $Hom(\cdot, X)(f) : Mor(Z, X) \rightarrow Mor(Y, X), g \mapsto g \circ f$
- (4) Sei X Menge, $F_X : \text{Gruppen} \rightarrow \text{Mengen}. G \mapsto Abb(X, G) = Mor_{\text{Mengen}}(X, G)$ ist kovarianter Funktor (also Komposition des Vergissfunktors und des Homomorphismen-Funktors $Hom(X, \cdot)$).

Definition 1.6.3

Sei \mathcal{C} eine Kategorie, X, Y Objekte in \mathcal{C} . $f \in Mor_{\mathcal{C}}(X, Y)$ heißt **Isomorphismus**, wenn es $g \in Mor_{\mathcal{C}}(Y, X)$ gibt, so dass $g \circ f = id_X$ und $f \circ g = id_Y$.

Definition 1.6.4

Seien \mathcal{A}, \mathcal{B} Kategorien und $F, G : \mathcal{A} \rightarrow \mathcal{B}$ kovariante Funktoren. F und G heißen **isomorph**, wenn es zu jedem Objekt $A \in Ob \mathcal{A}$ einen Isomorphismus $\alpha_A : F(A) \rightarrow G(A)$, also $\alpha_A \in Mor_{\mathcal{B}}(F(A), G(A))$ gibt, so dass für alle Morphismen $f : A \rightarrow A'$ in \mathcal{A} das folgende Diagramm kommutiert:

$$\begin{array}{ccc}
 F(A) & \xrightarrow{\alpha_A} & G(A) \\
 F(f) \downarrow & & \downarrow G(f) \\
 F(A') & \xrightarrow{\alpha_{A'}} & G(A')
 \end{array}$$

Also: $G(f) \circ \alpha_A = \alpha_{A'} \circ F(f)$.

Sind die α_A nur Morphismen (also nicht notwendigerweise Isomorphismen), so heißt $\alpha : F \rightarrow G$ eine **natürliche Transformation** von Funktoren.

1 Gruppen

Proposition 1.6.5

Sei X eine Menge, $F(X)$ die freie Gruppe mit Basis X . Dann sind die Funktoren F_X und $Hom(F(X), \cdot) : \underline{\text{Gruppen}} \rightarrow \underline{\text{Mengen}}$ isomorph.

Beweis: Nach Satz 3 gibt es für jede Gruppe G eine bijektive Abbildung $\alpha_G : F_X(G) = Abb(X, G) \rightarrow Hom(F(X), G)$, $f \mapsto \varphi = \hat{f}$. Sei $\rho : G \rightarrow G'$ ein Gruppenhomomorphismus. Dann kommutiert:

$$\begin{array}{ccc} F_X(G) & \xrightarrow{\alpha_G} & Hom(F(X), G) \\ F_X(\rho) \downarrow & & \downarrow Hom(F(X), \cdot)(\rho) \\ F_X(G') & \xrightarrow{\alpha_{G'}} & Hom(F(X), G') \end{array}$$

Denn für $f \in F_X(G)$ ist $\alpha_G(f) = \hat{f}$ und $((Hom(F(X), \cdot)(\rho))(\hat{f}) = \rho \circ \hat{f}$ sowie $F_X(\rho)(\hat{f}) = \rho \circ f$ und $\alpha_{G'}(\rho \circ f) = \widehat{\rho \circ f}$. Beides ist **der** eindeutig bestimmte Gruppenhomomorphismus $F(X) \rightarrow G'$, der auf X die Abbildung $g \circ f$ ist. ■

Definition + Bemerkung 1.6.6

1. Sei \mathcal{C} eine Kategorie und $F : \mathcal{C} \rightarrow \text{Mengen}$ ein kovarianter Funktor. Ein Objekt $U \in \mathcal{C}$ heißt **darstellendes Objekt** für F , wenn F isomorph zu $Hom(U, \cdot)$ ist.
Analog gilt das für kontravariante Funktoren, wenn F isomorph zu $Hom(\cdot, U)$ ist.
2. F heißt **darstellbar**, wenn es ein darstellendes Objekt für F gibt.
3. Ist F darstellbar, so sind je zwei darstellende Objekte für F isomorph.

Beweis: Seien U, W darstellende Objekte für F . Dann gibt es einen Isomorphismus von Funktoren $\alpha := h_U := Hom(U, \cdot) \rightarrow Hom(W, \cdot)$, insbesondere also bijektive Abbildungen $\alpha_U : Mor(U, U) \rightarrow Mor(W, U)$ und $\alpha_W : Mor(U, W) \rightarrow Mor(W, W)$. Sei $\varphi := \alpha_U(id_U)$, $\psi := \alpha_W^{-1}(id_W)$. Zu zeigen: $\varphi \circ \psi = id_U$, $\psi \circ \varphi = id_W$.

Das kommutative Diagramm aus Definition 1.6.4 für den Morphismus ψ ist:

$$\begin{array}{ccc} Mor(U, U) & \xrightarrow{\alpha_U} & Mor(W, U) \\ h_U(\psi) \downarrow & & \downarrow h_W(\psi) \\ Mor(U, W) & \xrightarrow{\alpha_W} & Mor(W, W) \end{array}$$

Also gilt

$$\begin{aligned}
 id_W &= \alpha_W(\psi) \\
 &= \alpha_W(\psi \circ id_U) \\
 &= (\alpha_W \circ h_U(\psi))(id_U) \\
 &= (h_W(\psi) \circ \alpha_U)(id_U) \\
 &= h_W(\psi)(\varphi) \\
 &= \psi \circ \varphi
 \end{aligned}$$

und analog folgt $\varphi \circ \psi = id_U$. ■

1.7 Gruppenaktionen und die Sätze von Sylow

Definition + Bemerkung 1.7.1

Sei G eine Gruppe, X eine Menge.

- (a) Eine **Aktion** (Wirkung) von G auf X ist ein Gruppenhomomorphismus $\rho : G \rightarrow \text{Perm}(X)$. G **operiert** dann auf X .
- (b) Die Aktionen von G auf X entsprechen bijektiv den Abbildungen: $G \times X \rightarrow X$, $(g, x) \mapsto gx$, für die gilt
- (i) $ex = x$ für alle $x \in X$
 - (ii) $(g_1g_2)x = g_1(g_2x)$ für alle $g_1, g_2 \in G$, $x \in X$

Beweis: Sei $\rho : G \rightarrow \text{Perm}(X)$ ein Homomorphismus. Dann erfüllt $G \times X \rightarrow X$, $(g, x) \mapsto \rho(g)(x)$ die Eigenschaften (i) und (ii), denn $\rho(e) = id_X$ und $\rho(g_1g_2)(x) = \rho(g_1)(\rho(g_2)(x))$.

Ist umgekehrt $\mu : G \times X \rightarrow X$ mit (i), (ii) gegeben, so sei für $g \in G$ die Abbildung $\rho(g) : X \rightarrow X$ definiert durch $\rho(g)(x) = \mu(g, x)$. $\rho(g)$ ist bijektiv, da $\rho(g^{-1})$ die Umkehrabbildung ist:

$$\begin{aligned}
 \rho(g^{-1})(\rho(g)(x)) &= \mu(g^{-1}, \mu(g, x)) \\
 &= g^{-1} \cdot (g \cdot x) \\
 &= (g^{-1} \cdot g) \cdot x \\
 &= e \cdot x \\
 &= x
 \end{aligned}$$

Dann ist $\rho : G \rightarrow \text{Perm}(X)$, $g \mapsto \rho(g)$ wegen (ii) ein Homomorphismus. ■

1 Gruppen

Beispiel:

- a) $G \times G \rightarrow G, (g_1, g_2) \mapsto g_1 g_2$ ("Linksmultiplikation") ist eine Gruppenaktion.
- b) $(g, h) \mapsto h \cdot g$ ist im Allgemeinen keine Gruppenaktion, aber $(g, h) \mapsto hg^{-1}$ ist eine.
- c) $G \times G \rightarrow G, (g, h) \mapsto ghg^{-1}$ ("Konjugation") ist eine Gruppenaktion.
- d) Ist X eine beliebige Menge, so operiert S_n auf X^n durch Vertauschen der Komponenten: $\sigma(x_1, \dots, x_n) = (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})$.

- (c) Eine Aktion ρ heißt **effektiv** (oder **treu**), wenn $\text{Kern}(\rho) = \{e\}$.
Allgemein heißt $\text{Kern}(\rho)$ **Ineffektivitätskern** ("Nichtsnutz") der Aktion.

Beispiel:

- a) ist effektiv
- c) Der Ineffektivitätskern ist das Zentrum $Z(G)$
- d) ist effektiv für $|X| \geq 2$

- (d) Für $x \in X$ heißt $Gx := \{gx : g \in G\}$ die **Bahn** von x unter G .
- (e) X ist disjunkte Vereinigung von G -Bahnen.

Beweis: Durch $x \sim y \iff \exists g \in G : y = gx$ wird eine Äquivalenzrelation definiert, deren Äquivalenzklassen gerade die G -Bahnen sind. ■

- (f) Für $x \in X$ heißt $G_x := \{g \in G : gx = x\}$ die **Fixgruppe** von x unter G (auch **Stabilisator** oder **Isotropiegruppe** von x genannt). Dies ist eine Untergruppe von G .
- (g) Für $x \in X, g \in G$ ist $G_{gx} = gG_x g^{-1}$

Proposition 1.7.2 (Bahnbilanz)

Sei X endliche Menge, G Gruppe, die auf X operiert. Sei x_1, \dots, x_n ein Vertretersystem der G -Bahnen in X . (dh. aus jeder G -Bahn genau ein Element). Dann gilt:

$$|X| = \sum_{i=1}^r [G : G_{x_i}]$$

Beweis: Nach 1.7.1 ist $|X| = \sum_{i=1}^r |Gx_i|$. Zu zeigen bleibt also: $|Gx_i| = [G : G_{x_i}]$.

Beh.:

$$\alpha_i = \begin{cases} Gx_i & \rightarrow G/G_{x_i} \\ gx_i & \mapsto gG_{x_i} \end{cases}$$

ist bijektive Abbildung, denn:

- α_i ist wohldefiniert: Ist $g \cdot x_i = h \cdot x_i$, so ist $(h^{-1}g)x_i = x_i$, also $h^{-1}g \in G_{x_i} \implies g \in hG_{x_i} \implies gG_{x_i} \cap hG_{x_i} \neq \emptyset \implies gG_{x_i} = hG_{x_i}$
- α_i ist injektiv. Ist $gG_{x_i} = hG_{x_i}$, so ist $g \in hG_{x_i} \implies h^{-1}g \in G_{x_i} \implies (h^{-1}g)x_i = x_i \implies g \cdot x_i = h \cdot x_i$
- α_i ist offensichtlich surjektiv.

Satz 4 (Sylow)

Sei G endliche Gruppe, $|G| = n$, p eine Primzahl. Sei $n = p^k m$ mit $k \geq 0$ und $p \nmid m$. Dann gilt:

- G enthält eine Untergruppe S der Ordnung p^k . Jede solche Untergruppe heißt **p-Sylowgruppe** von G .
- Je zwei p -Sylowgruppen sind konjugiert.
- Die Anzahl s_p der p -Sylowgruppen in G erfüllt: $s_p \mid m$ und $s_p \equiv 1 \pmod{p}$.

Beweis: $k = 0$: ✓ Sei also $k \geq 1$.

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

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

Beh.1: $p \nmid |\mathcal{M}|$

G operiert auf \mathcal{M} durch die Linksmultiplikation $gM = \{gx : x \in M\} \in \mathcal{M} \Rightarrow |\mathcal{M}|$ ist Summe der Bahnlängen. Wegen Beh.1 gibt es eine Bahn GM_0 mit $p \nmid |GM_0|$.

$$\stackrel{1.7.2}{\Rightarrow} |GM_0| = [G : G_{M_0}] = \frac{|G|}{|G_{M_0}|} = \frac{p^k m}{|G_{M_0}|} \Rightarrow p^k \mid |GM_0|.$$

Andererseits ist $|G_{M_0}| \leq p^k = |M_0|$, denn für $x \in M_0$ ist $g \mapsto gx$ injektive Abbildung $G_{M_0} \rightarrow M_0 \Rightarrow |G_{M_0}| = p^k$, dh. G_{M_0} ist p -Sylowgruppe.

Bew. von Beh.1:

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

1 Gruppen

Schreibe jedes dieser i in der Form $p^{\nu_i} m_i$, mit $p \nmid m_i (0 \leq \nu_i < k) \Rightarrow \frac{p^k m - i}{p^k - i} = \frac{mp^{k-\nu_i} - m_i}{p^{k-\nu_i} - m_i} \Rightarrow$ weder Zähler noch Nenner sind durch p teilbar. \Rightarrow Beh.

(b) Sei $S \subseteq G$ p -Sylowgruppe.

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

Beh.2: $p \nmid |\mathcal{S}|$.

Bew.2: G operiert 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.)

$$\Rightarrow |\mathcal{S}| = [G : N_S] = \frac{|G|}{|N_S|} = \frac{p^k m}{|N_S|}$$

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

Sei \tilde{S} eine p -Sylowgruppe in G . zu zeigen: $\tilde{S} \in \mathcal{S}$.

\tilde{S} operiert auf \mathcal{S} (da $\tilde{S} \subset G$). Sei nun s_1, \dots, s_r ein Vertretersystem der Bahnen.

$$\Rightarrow |\mathcal{S}| = \sum_{i=1}^r [\tilde{S} : \tilde{S}_{s_i}] = \sum_{i=1}^r \frac{p^k}{|\tilde{S}_{s_i}|} \stackrel{\text{Beh.2}}{\Rightarrow} \text{Es gibt ein } i \text{ mit } \tilde{S} = \tilde{S}_{s_i}$$

Dann ist $\tilde{S} \subseteq N_{S_i}$.

Beh.3: Dann ist $\tilde{S} \subseteq S_i$, also $\tilde{S} = S_i$, da beide p^k Elemente haben.

Bew.3: S_i ist Normalteiler in N_{S_i} , \tilde{S} ist Untergruppe in $N_{S_i} \Rightarrow \tilde{S}S_i$ ist Untergruppe von N_{S_i} (Übung)

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

Übung $\tilde{S}S_i/S_i \cong \tilde{S}/\tilde{S} \cap S_i \Rightarrow |\tilde{S}S_i| = \frac{|S_i| |\tilde{S}|}{|\tilde{S} \cap S_i|} = \frac{p^k}{|\tilde{S} \cap S_i|} = p^l$ für ein $l \in \mathbb{N}$. $p^l = p^k d$, $d \neq 1 \Rightarrow \zeta!$

(c) $s_p = |\mathcal{S}| \Rightarrow s_p \mid m$ und $\mathcal{S} = \sum_{i=1}^r [\tilde{S} : \tilde{S}_{s_i}]$

$[\tilde{S} : \tilde{S}_{s_i}] = 1 \Leftrightarrow \tilde{S} = \tilde{S}_{s_i} \stackrel{\text{Beh.3}}{\Leftrightarrow} \tilde{S} = S_i$, also genau **einmal**. Alle anderen Summanden sind durch p teilbar. ■

Folgerung 1.7.3

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

Beweis: Sei $|G| = p^k m$ mit $p \nmid m$, $k \geq 1$. $S \subseteq G$ eine p -Sylowgruppe und $x \in S$, $x \neq e$.
 $\stackrel{1,2,6}{\Rightarrow}$ $\text{ord}(x)$ ist Teiler von $|S| = p^k \Rightarrow \text{ord}(x) = p^d$ für ein d , $1 \leq d \leq k \Rightarrow x^{p^{d-1}}$ hat dann Ordnung p . ■

Beispiel: Wieviele Gruppen G gibt es mit $|G| = 15$? Mindestens eine: $G = \mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Nach Sylow gibt es nicht 5 3-elementigen Untergruppen, da $5 \equiv 1 \pmod{3}$ nicht gilt, und nicht 3, da $3 \nmid s_3$. also gibt es nur eine S_3 und ebenso nur eine S_5 .

Daher gibt es genau zwei Elemente der Ordnung 3 und vier Elemente der Ordnung 5. Übrig bleiben 8 Elemente, die Ordnung 15 haben müssen, also ist $G \cong \mathbb{Z}/15\mathbb{Z}$.

1.8 Symmetrische und alternierende Gruppen

Definition + Bemerkung 1.8.1

Sei $n \geq 0$.

- (a) $S_n = \text{Perm}(\{1, \dots, n\})$ heißt *symmetrische Gruppe*.
- (b) $|S_n| = n!$
- (c) $\xi \in S_n$ heißt **Zyklus** wenn es ein k gibt (mit $1 \leq k \leq n$) und paarweise verschiedene Elemente i_1, \dots, i_k von $\{1, \dots, n\}$ mit $\xi(i_\nu) = i_{\nu+1}$ für $\nu = 1, \dots, k-1$, $\xi(i_k) = i_1$ und $\xi(j) = j$ für $j \notin \{i_1, \dots, i_k\}$. In diesem Fall heißt ξ ein **k -Zyklus**, und k wird die **Länge** dieses Zyklus ξ genannt.
- (d) Jedes $\sigma \in S_n$ lässt sich als Produkt von paarweise disjunkten Zykeln schreiben (wobei zwei Zykeln als disjunkt gelten, wenn jedes Element von $\{1, \dots, n\}$ von mindestens einem der beiden unverändert gelassen wird). Diese Darstellung ist eindeutig bis auf die Reihenfolge.
- (e) 2-Zykel heißen auch Transpositionen.
- (f) Jeder k -Zyklus ist Produkt von $k-1$ Transpositionen:

$$(1\ 2 \cdots k) = (1\ 2) \circ (2\ 3) \circ \cdots \circ (k-1\ k)$$

- (g) $\sigma \in S_n$ heißt *gerade*, wenn es als Produkt einer geraden Anzahl von Transpositionen geschrieben werden kann, anderenfalls *ungerade*.
- (h) $\text{sign} : S_n \rightarrow \{+1, -1\}$,

$$\text{sign}(\sigma) = \begin{cases} +1, & \sigma \text{ gerade} \\ -1, & \sigma \text{ ungerade} \end{cases}$$

1 Gruppen

ist ein Homomorphismus.

$A_n := \text{Kern}(\text{sign}) = \{\sigma \in S_n \mid \sigma \text{ gerade}\}$ heißt *alternierende Gruppe*.

Bemerkung 1.8.2 (a) Je zwei k -Zykel in S_n sind konjugiert.

Beweis: Für $\sigma \in S_n$ ist $\sigma(1\ 2\ \dots\ k)\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \dots\ \sigma(k))$, also kann man jedes k -Zykel so darstellen. ■

(b) Daraus folgt: Zwei Permutationen in S_n sind genau dann konjugiert, wenn sie die gleiche „Zykelstruktur“ haben (d. h. derart jeweils als Produkte disjunkter Zykel dargestellt werden können, dass die Längen der Zykel in der Darstellung der ersten Permutation gleich den Längen der entsprechenden Zykel in der Darstellung der zweiten Permutation sind).

Bemerkung 1.8.3 (a) In A_4 kann die vorangehende Bemerkung nicht stimmen: $(1\ 2\ 3)$ und $(3\ 2\ 1)$ sind nicht konjugiert.

(b) Für $n \geq 5$ sind je zwei 3-Zykel in A_n konjugiert.

Beweis:

(a) Ausprobieren

(b) $(1\ 3\ 2) = \sigma(1\ 2\ 3)\sigma^{-1}$ mit $\sigma = (1\ 2)(4\ 5)$
 $(i\ j\ k) = \sigma(1\ 2\ 3)\sigma^{-1}$ mit $\sigma = (1\ i\ 2\ j)(3\ k)$ für $i, j, k > 3$. Weitere Fälle: Übung. ■

Bemerkung 1.8.4

Jede gerade Permutation ist als Produkt von 3-Zykeln darstellbar

Beweis: $(1\ 2)(3\ 4) = (1\ 2\ 3)(2\ 3\ 4)$, $(1\ 2)(2\ 3) = (1\ 2\ 3)$ ■

Satz 5

Für $n \neq 4$ enthält A_n nur die Normalteiler $\{1\}$ und A_n

Beweis: In A_4 ist $\{\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (2\ 3)(1\ 4)\}$ Normalteiler, $A_1 = A_2 = \{\text{id}\}$ und $A_3 = \mathbb{Z}/3\mathbb{Z}$.

Sei also $n \geq 5$ und $N \neq \{\text{id}\}$ ein Normalteiler von A_n .

Es genügt zu zeigen: N enthält einen 3-Zyklus, denn nach 1.8.3 sind dann alle 3-Zykel in N und nach 1.8.4 ist damit $N = A_n$.

Es genügt auch zu zeigen, dass N das Produkt von zwei Transpositionen enthält, denn ist $\sigma = (1\ 2)(3\ 4) \in N$, so ist auch $(3\ 4\ 5) = \sigma(\tau\sigma^{-1}\tau) \in N$, mit $\tau = (1\ 2)(3\ 5)$.

Das Ziel ist also zu zeigen, dass N ein Element σ enthält mit $\sigma(i) \neq i$ für höchstens vier i , denn dann ist $\sigma \in A_4$, also 3-Zykel oder Produkt von zwei Transpositionen.

Für $\sigma \in A_n$ sei $k_\sigma := |\{i : \sigma(i) \neq i\}|$. Wähle $\sigma \in N \setminus \{\text{id}\}$ so dass $k_\sigma \leq k_\alpha$ für alle $\alpha \in N \setminus \{\text{id}\}$.

Annahme: $k_\sigma \geq 5$. 1. Fall: σ enthält einen Zyklus der Länge ≥ 3 , also $\sigma(1) = 2, \sigma(2) = 3, \sigma(4) \neq 4, \sigma(5) \neq 5$. Sei $\alpha := \sigma^{-1}(3\ 4\ 5)\sigma(3\ 5\ 4) \in N$. Ist $\sigma(i) = i$, so ist $\alpha(i) = i$ für $i \geq 6$. Außerdem ist $\alpha(1) = 1$ und $\alpha(2) = \sigma^{-1}(4) \neq 2$, also ist $\alpha \neq \text{id}$ und $k_\alpha < k_\sigma$.

2. Fall: σ ist Produkt von disjunkten Transpositionen (mind. 4). Ohne Einschränkung der Allgemeinheit ist $\sigma = (12)(34)(56)(78)\tilde{\sigma}$ mit $\tilde{\sigma} \in A_n, \tilde{\sigma}(i) = i$ für $i = 1, \dots, 8$. $\alpha = \sigma^{-1}(345)\sigma(354)$ erfüllt $\alpha(i) = i$, falls $\sigma(i) = i$, und $\alpha(1) = 1 \Rightarrow k_\alpha < k_\sigma$

Also enthält N ein σ , das höchstens vier i nicht gleich lässt. Damit ist $N = A_n$ gezeigt. ■

1.9 Kompositionsreihen

Vorüberlegung: G Gruppe, $N \trianglelefteq G$ Normalteiler und G/N die Faktorgruppe. Lässt sich nun G aus N und G/N rekonstruieren? Nicht unbedingt, wie das Beispiel D_n zeigt. D_n hat als Normalteiler $\mathbb{Z}/n\mathbb{Z}$, und $D_n/(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, aber $D_n \not\cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Definition 1.9.1

Sei $(*) \dots \rightarrow G_{i-1} \xrightarrow{\alpha_{i-1}} G_i \xrightarrow{\alpha_i} \dots$ eine Sequenz (Folge) von Gruppen und Gruppenhomomorphismen.

$(*)$ heißt **exakt** an der Stelle i , wenn $\text{Kern}(\alpha_i) = \text{Bild}(\alpha_{i-1})$.

Die Sequenz $(*)$ heißt **exakt**, wenn sie an jeder Stelle exakt ist.

Beispiel:

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

und

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

sind exakt. Allgemein ist die Sequenz

$$1 \rightarrow N \rightarrow G \rightarrow G/N \rightarrow 1 \quad (*)$$

exakt, wann immer G eine Gruppe und N ein Normalteiler von G sind.

Die Aufgabe, Gruppen zu klassifizieren zerfällt in zwei Teilaufgaben:

1 Gruppen

- (1) Geg.: N und G/N . Welche Möglichkeiten gibt es für G ?
- (2) Welche "unzerlegbaren" Gruppen gibt es?

Definition 1.9.2

Sei G eine Gruppe.

- (a) Eine Reihe der Form

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{e\} \quad (**)$$

(mit $n \in \mathbb{N}$) heißt **Normalreihe**, wenn G_{i+1} Normalteiler in G_i ist ($i = 0, \dots, n-1$) und $G_{i+1} \neq G_i$.

- (b) Die Faktorgruppen G_i/G_{i+1} in einer Kompositionsreihe $G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n$ heißen die **Faktoren** (oder **Faktorgruppen**) dieser Kompositionsreihe.
- (c) G heißt **einfach**, wenn $G \triangleright \{e\}$ die einzige Normalreihe ist, das heißt: G besitzt nur die trivialen Normalteiler G und $\{e\}$ und $G \neq \{e\}$.
- (d) Eine Normalreihe heißt **Kompositionsreihe**, wenn sie sich nicht verfeinern läßt, dh. wenn G_i/G_{i+1} einfach ist für $i = 0, \dots, n-1$

Bemerkung 1.9.3

- (a) $\mathbb{Z}/n\mathbb{Z}$ ist einfach $\Leftrightarrow n$ ist Primzahl.
- (b) Eine abelsche Gruppe G ist einfach $\Leftrightarrow G \cong \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p .
- (c) \mathbb{Z} besitzt keine Kompositionsreihe.
- (d) Jede endliche Gruppe besitzt eine Kompositionsreihe.
- (e) Ist G endlich, $(**)$ eine Normalreihe, so gilt:

$$|G| = \prod_{i=0}^{n-1} [G_i : G_{i+1}] = \prod_{i=0}^{n-1} \frac{|G_i|}{|G_{i+1}|}$$

- (f) Es ist eine Kompositionsreihe:

$$S_4 \triangleright A_4 \triangleright D_2 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \triangleright \mathbb{Z}/2\mathbb{Z} \triangleright \{1\}$$

- (g) Für $n \geq 5$ ist eine Kompositionsreihe:

$$S_n \triangleright A_n \triangleright \{1\}$$

Satz 6 (Jordan-Hölder)

Sei G eine Gruppe, und seien

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{1\}$$

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_l = \{1\}$$

Kompositionsreihen für G .

Dann ist $m = l$ und es gibt eine Permutation $\sigma \in \text{Perm}(\{0, \dots, m-1\})$ mit $G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}$ für $i = 0, \dots, m-1$.

Beweis: Induktion über m :

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

m > 1: Sei $\bar{G} := G/G_1$, $\pi : G \rightarrow \bar{G}$ die Restklassenabbildung.

$\Rightarrow \bar{H}_i = \pi(H_i)$ ist Normalteiler in \bar{H}_{i-1} für $i = 1, \dots, l$, denn für $\bar{h}_i \in \bar{H}_i$, $\bar{g} \in \bar{H}_{i-1}$ ist $\bar{g}\bar{h}_i\bar{g}^{-1} = \pi(gh_i g^{-1}) \in \bar{H}_i$ (da $gh_i g^{-1} \in H_i$).

Nach Voraussetzung ist \bar{G} einfach, also $\bar{H}_0 = \bar{G}$, $\bar{H}_1 = \bar{G}$ oder $\bar{H}_1 = \{1\}$, usw.

$\Rightarrow \exists j \in \{0, \dots, l-1\}$ mit $\bar{H}_0 = \cdots = \bar{H}_j = \bar{G}$, $\{1\} = \bar{H}_{j+1} = \cdots = \bar{H}_l$.

Sei $C_i := H_i \cap G_1$, $i = 0, \dots, l$.

Beh.1:

$$G_1 = C_0 \triangleright C_1 \triangleright \cdots \triangleright C_j \triangleright C_{j+2} \triangleright \cdots \triangleright C_l = \{1\}$$

ist Kompositionsreihe für G_1 wenn $j \leq l-2$, bzw.

$$G_1 = C_0 \triangleright C_1 \triangleright \cdots \triangleright C_j = \{1\}$$

ist Kompositionsreihe für G_1 wenn $j = l-1$.

Aber

$$G_1 \triangleright G_2 \triangleright G_3 \triangleright \cdots \triangleright G_m = \{1\}$$

ist ebenfalls Kompositionsreihe. $\stackrel{IV}{\Rightarrow} m-1 = l-1$, also $m = l$ und es gibt $\sigma : \{0, \dots, j, j+2, \dots, l-1\} \rightarrow \{1, \dots, l-1\}$ bijektiv mit

$$C_i/C_{i+1} \cong G_{\sigma(i)}/G_{\sigma(i)+1} \text{ für } i \in \{0, \dots, j, j+2, \dots, l-1\}.$$

Beh.2

(a) $C_j = C_{j+1}$

(b) $C_i/C_{i+1} \cong H_i/H_{i+1}$ für $i \neq j$

(c) $H_j/H_{j+1} \cong \bar{G} = G/G_1$

Beh.1 folgt aus Beh.2:

C_{i+1} ist Normalteiler in C_i ($i = 0, \dots, l-1$), denn für $x \in C_{i+1} = H_{i+1} \cap G_1$ und $y \in C_i = H_i \cap G_1$ ist $xyx^{-1} \in H_i \cap G_1 = C_i$.

C_{j+2} ist Normalteiler in C_j wegen Beh.2(a).

C_{i-1}/C_i sind wegen Beh.2(b) einfach und $\neq \{1\}$ ($i \neq j+1$)

Bew. von Beh.2:

(a) $\bar{H}_{j+1} = \{1\}$, dh. $H_{j+1} \subseteq \text{Kern } \pi = G_1 \Rightarrow C_{j+1} = H_{j+1}$. $C_j = H_j \cap G_1$ ist Normalteiler in H_j . (weil G_1 Normalteiler in G ist)

Da $\bar{H}_j = \bar{G} \neq \{1\}$, ist $C_j \neq H_j \Rightarrow H_{j+1} = C_{j+1} \trianglelefteq C_j \triangleleft H_j$, und weil H_j/H_{j+1} einfach ist, folgt $C_j = H_{j+1} = C_{j+1}$

(b) Für $i \geq j+1$ ist $\bar{H}_i = \{1\}$, also $H_i \subseteq G_1$ und damit $C_i = H_i$.

Für $i < j$ ist $\bar{H}_{i+1} = \bar{G} = G/G_1 \Rightarrow H_{i+1} \cdot G_1 = G_1 \cdot H_{i+1} = G$

$$C_i/C_{i+1} = C_i/(H_{i+1} \cap C_i) \stackrel{\text{Übung}}{\cong} C_i \cdot H_{i+1}/H_{i+1}$$

zu zeigen also: $C_i \cdot H_{i+1} = H_i$

denn: „ \subseteq “: ✓

„ \supseteq “: Da $G_1 H_{i+1} = G$ ist, gibt es zu $x \in H_i$ ein $h \in H_{i+1}$ und $g \in G_1$ mit $x = gh \Rightarrow g = xh^{-1} \in H_i \cdot H_{i+1} \subseteq H_i$, also $g \in H_i \cap G_1 = C_i$ und folglich $x = gh \in C_i H_{i+1}$.

(c) $H_{j+1} \subseteq G_1 \Rightarrow H_j/H_{j+1} = H_j/C_{j+1} \stackrel{(a)}{=} H_j/C_j = H_j/H_j \cap G_1 \cong H_j G_1/G_1 = G/G_1$



Definition + Bemerkung 1.9.4

- (a) Eine Gruppe 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 sind.

Beweis: „ \Leftarrow “: Klar

„ \Rightarrow “: Sei

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_m = \{1\}$$

eine Normalreihe mit G_i/G_{i+1} abelsch für $i = 0, \dots, m-1$. Verfeinere sie zur

Kompositionsreihe

$$G = G_0 = H_{0,0} \triangleright H_{0,1} \triangleright \dots \triangleright H_{0,d_0} = G_1 = H_{1,0} \triangleright \dots \triangleright H_{1,d_1} = G_2 \triangleright \dots \triangleright G_m = \{1\}$$

Dabei ist

$$H_{i,j}/H_{i,j+1} \cong H_{i,j}/G_{i+1}/H_{i,j+1}/G_{i+1} \subseteq G_i/G_{i+1}/H_{i,j+1}/G_{i+1}$$

also ist $H_{i,j}/H_{i,j+1}$ isomorph zu einer Untergruppe einer Faktorgruppe einer abelschen Gruppe, also selbst auch abelsch. ■

Beispiel:

- $D_n = \{1, \tau, \dots, \tau^{n-1}, \sigma, \sigma\tau, \dots, \sigma\tau^{n-1}\} \triangleright \{1, \tau, \dots, \tau^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z} \triangleright \{1\}$, also ist D_n auflösbar.
- Für $n \geq 5$ ist $S_n \triangleright A_n \triangleright \{1\}$ Kompositionsreihe, also ist S_n nicht auflösbar.

Proposition 1.9.5

Sei $1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1$ kurze exakte Sequenz von Gruppen, das heißt: G' ist Normalteiler zu G und $G'' = G/G'$. Dann ist G auflösbar genau dann, wenn G' und G'' auflösbar sind.

Beweis: „ \implies “: Sei

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_m = \{1\}$$

eine Normalreihe mit G_i/G_{i+1} abelsch für $i = 0, \dots, m - 1$. Dann ist

$$G' = G_0 \cap G' \triangleright G_1 \cap G' \triangleright \dots \triangleright G_m \cap G' = \{1\}$$

nach Weglassen von Wiederholungen eine Normalreihe für G' . Die Faktorgruppen

$$G_i \cap G' / G_{i+1} \cap G' \cong G_{i+1} \cdot (G_i \cap G') / G_{i+1} \subseteq G_i / G_{i+1}$$

sind abelsch.

$$G'' = G_0 / (G_0 \cap G') \triangleright G_1 / (G_1 \cap G') \triangleright \dots \triangleright G_m / (G_m \cap G') = \{1\}$$

ist ebenso nach Weglassen von Wiederholungen eine Normalreihe für G'' mit abelschen Faktorgruppen.

„ \impliedby “: Ist

$$G' = G_0 \triangleright G_1 \triangleright \dots \triangleright G_m = \{1\}$$

eine Normalreihe für G' mit abelschen Faktoren,

$$G'' = H_0 \triangleright H_1 \triangleright \dots \triangleright H_n = \{1\}$$

1 Gruppen

eine solche für G'' und $\pi : G \rightarrow G/G' = G''$ die Restklassenabbildung, dann ist

$$G = \pi^{-1}(H_0) \triangleright \pi^{-1}(H_1) \triangleright \cdots \triangleright \pi^{-1}(H_n) = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{1\}$$

eine Normalreihe für G , da $\pi^{-1}(H_{i+1})$ Normalteiler in $\pi^{-1}(H_i)$ ist und $\pi^{-1}(H_i)/\pi^{-1}(H_{i+1}) \cong H_i/H_{i+1}$ abelsch ist. ■

2 Ringe

2.1 Grundlegende Definitionen und Eigenschaften

Definition + Bemerkung 2.1.1 (a) Ein **Ring** ist eine Menge R mit Verknüpfungen $+$ und \cdot , so dass gilt:

- (i) $(R, +)$ ist abelsche Gruppe
- (ii) (R, \cdot) ist Halbgruppe
- (iii) Die Distributivgesetze gelten:

$$\left. \begin{aligned} x \cdot (y + z) &= xy + xz \\ (x + y) \cdot z &= xz + yz \end{aligned} \right\} \text{für alle } x, y, z \in R$$

- (b) R heißt **Ring mit Eins**, wenn (R, \cdot) Monoid ist.
- (c) R heißt **kommutativer Ring**, wenn (R, \cdot) kommutativ ist.
- (d) Ein Ring R mit Eins heißt **Schiefkörper**, wenn $R^\times = (R, \cdot)^\times = R \setminus \{0\}$, dh. wenn jedes $x \in R \setminus \{0\}$ invertierbar bzgl. \cdot ist.

Beispiel:

$$\mathbb{H} := \left\{ \begin{pmatrix} w & z \\ -\bar{z} & \bar{w} \end{pmatrix}, w, z \in \mathbb{C} \right\}$$

ist ein Schiefkörper, genannt die **Hamilton-Quaternionen**.

- (e) Ein kommutativer Schiefkörper heißt **Körper**.
- (f) In jedem Ring gilt:

$$\left. \begin{aligned} x \cdot 0 &= 0 = 0 \cdot x \\ x(-y) &= -(xy) = (-x)y \\ (-x)(-y) &= xy \end{aligned} \right\} \text{für alle } x, y \in R$$

Beweis: $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$ (genauso für $0 \cdot x$)
 $x(-y) + xy = x(-y + y) = x \cdot 0 = 0$
 $(-x)(-y) = -((-x)y) = -(-(xy)) = xy$ ■

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

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

Definition 2.1.2

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

- (a) $R' \subseteq R$ heißt **Unterring**, wenn $(R', +, \cdot)$ Ring ist. Umgekehrt heißt R dann **Ring-erweiterung** von R' .
- (b) $I \subseteq R$ heißt (zweiseitiges) **Ideal**, wenn $(I, +)$ Untergruppe von $(R, +)$ ist und $rx \in I, xr \in I$ für alle $x \in I, r \in R$.

Beispiel: In $R = \mathbb{Z}$ sind $n\mathbb{Z}$ für jedes $n \in \mathbb{Z}$ Ideale. In $R = \mathbb{Q}$ dagegen sind diese für $n \neq 0$ keine Ideale.

Definition + Bemerkung 2.1.3

Sei R ein kommutativer Ring.

- (a) Für a ist $(a) := a \cdot R = \{a \cdot r, r \in R\}$ ein Ideal in R .
- (b) Ein Ideal I in R heißt **Hauptideal**, wenn es ein $a \in R$ gibt mit $I = (a)$.
- (c) R heißt **Hauptidealring**, wenn jedes Ideal in R ein Hauptideal ist.
- (d) \mathbb{Z} ist ein Hauptidealring.
- (e) Sei R ein kommutativer Ring mit Eins, $R \neq \{0\}$. Dann ist R ein Körper genau dann, wenn (0) und R die einzigen Ideale in R sind.

Beweis: " \Rightarrow " Sei $I \subset R$ Ideal, $a \in I \setminus \{0\} \Rightarrow$ es gibt $a^{-1} \in R \Rightarrow 1 = aa^{-1} \in I \Rightarrow I = R$ ($x \in R \Rightarrow x = 1x$)
 " \Leftarrow " Sei $a \in R \setminus \{0\} \Rightarrow (a) = R \Rightarrow \exists b \in R : ab = 1$ ■

Beispiel: $\mathbb{Z}/n\mathbb{Z}$ ist ein kommutativer Ring mit Eins für jedes $n \in \mathbb{N}$. Ist $n = p$ für eine Primzahl p , so ist $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ein Körper, und $(\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z})^\times = \{\bar{a}, a \in \mathbb{Z}, \text{ggT}(a, n) = 1\}$. In $\mathbb{Z}/6\mathbb{Z}$ dagegen gilt $\bar{2} \cdot \bar{3} = \bar{0}$.

Definition 2.1.4

Sei R ein kommutativer Ring.

- (a) $x \in R$ heißt **Nullteiler**, wenn es ein $y \in R \setminus \{0\}$ gibt mit $xy = 0$.
- (b) $R \neq \{0\}$ heißt **nullteilerfrei**, wenn 0 der einzige Nullteiler in R ist. (Das heißt: Aus $xy = 0$ folgt, dass $x = 0$ oder $y = 0$.)

- (c) R heißt **Integritätsbereich** (engl. **integral domain**), wenn er nullteilerfrei und kommutativ ist sowie eine Eins besitzt.

Definition + Bemerkung 2.1.5 (a) Eine Abbildung $\varphi : R \rightarrow R'$ (R, R' Ringe) heißt **Homomorphismus von Ringen**, wenn $\varphi : (R, +) \rightarrow (R', +)$ ein Homomorphismus von Gruppen und $\varphi : (R, \cdot) \rightarrow (R', \cdot)$ ein Homomorphismus von Halbgruppen ist.

- (b) Sind R, R' Ringe mit Eins, so heißt ein Homomorphismus von Ringen $\varphi : R \rightarrow R'$ ein **Homomorphismus von Ringen mit Eins**, wenn $\varphi(1_R) = 1_{R'}$.
- (c) Die Ringe bilden mit Ringhomomorphismus eine Kategorie
- (d) Die Ringe mit Eins bilden mit Homomorphismen von Ringen mit Eins eine Kategorie (echte Unterkategorie der Ringe)
- (e) $(R, +, \cdot) \hookrightarrow (R, +)$ ist kovarianter Funktor: Ringe \rightarrow abelsche Gruppen.
 $(R, +, \cdot) \mapsto (R^\times, \cdot)$ ist kovarianter Funktor: Ringe mit Eins \rightarrow Gruppen.

Beispiel: Sei R ein kommutativer Ring mit Eins und $R^{n \times n}$ der 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:

$$E_n := \begin{pmatrix} 1_R & & 0 \\ & \ddots & \\ 0 & & 1_R \end{pmatrix}$$

Die Einheiten in $R^{n \times n}$ sind die invertierbaren Matrizen: $(R^{n \times n})^\times = GL_n(R) = \{A \in R^{n \times n} : \exists B \in R^{n \times n} : A \cdot B = B \cdot A = E_n\} = \{A \in R^{n \times n} : \det A \in R^\times\}$, denn für die Adjungierte $A^\#$ von A gilt: $A \cdot A^\# = \det(A) \cdot E_n$.

($A^\# = (b_{ij})$ mit $b_{ij} = (-1)^{i+j} \det A_{ji}$, wobei A_{ji} die Matrix A ohne die j -te Zeile und i -te Spalte ist.)

Bemerkung 2.1.6

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

- (a) $\text{Bild}(\varphi)$ ist Unterring von R'
- (b) $\text{Kern}(\varphi) := \varphi^{-1}(0)$ ist Ideal in R

Beweis: Sei $x \in \text{Kern}(\varphi)$, $r \in R \Rightarrow \varphi(rx) = \varphi(r)\varphi(x) = \varphi(r)0 = 0 \Rightarrow rx \in \text{Kern}(\varphi)$ ■

2 Ringe

- (c) Ist R Schiefkörper, R' Ring mit Eins, φ Homomorphismus von Ringen mit Eins, so ist φ injektiv oder die Nullabbildung.

Beweis: Sei $x \in R \setminus \{0\} \Rightarrow \varphi(x)\varphi(x^{-1}) = \varphi(1) \neq 0$, sofern φ nicht die Nullabbildung $\Rightarrow \varphi(x) \neq 0 \Rightarrow \text{Kern}(\varphi) = \{0\} \Rightarrow \varphi$ injektiv. ■

Definition + Bemerkung 2.1.7

Sei R Ring mit Eins.

(a)

$$\varphi_R : \mathbb{Z} \rightarrow R, n \mapsto \begin{cases} n \cdot 1_R = \underbrace{1_R + \dots + 1_R}_n & n \geq 0 \\ -((-n) \cdot 1_R) & n \leq 0 \end{cases}$$

ist Homomorphismus von Ringen mit Eins.

- (b) Ist $\text{Kern}(\varphi_R) = n\mathbb{Z}$ ($n \geq 0$), so heißt n die **Charakteristik** von R : $n = \text{char}(R)$
- (c) Ist R nullteilerfrei, so ist $\text{char}(R) = 0$, oder $\text{char}(R) = p$ für eine Primzahl p .
- (d) $\text{Bild}(\varphi_R) \cong \mathbb{Z}/n\mathbb{Z}$, $n = \text{char}(R)$
- (e) Ist K (Schief-)Körper der Charakteristik $p > 0$, so ist $\text{Bild}(\varphi_K) \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ der kleinste Teilkörper von K . Er heißt **Primkörper**. Ist $\text{char}(K) = 0$, so lässt sich φ_K eindeutig fortsetzen zu einem injektiven Homomorphismus $\tilde{\varphi}_K : \mathbb{Q} \rightarrow K$ mit $\tilde{\varphi}_K\left(\frac{n}{m}\right) = \varphi_K(n) \cdot \varphi_K(m)^{-1}$.

Definition + Bemerkung 2.1.8

Sei R Ring. Dann gilt:

- (a) Ist J eine Indexmenge und sind $I_j, j \in J$ Ideale in R , so ist $\bigcap_{j \in J} I_j$ ein Ideal in R .
- (b) Sind I_1, I_2 Ideale in R , dann ist $I_1 + I_2 = \{a + b : a \in I_1, b \in I_2\}$ ein Ideal.
- (c) Sind I_1, I_2 Ideale in R , dann ist $I_1 \cdot I_2 = \left\{ \sum_{i=1}^{<\infty} a_i b_i : a_i \in I_1, b_i \in I_2 \right\}$ ein Ideal.
- (d) Sind I_1, I_2 Ideale in R , dann ist $I_1 \cdot I_2 \subseteq I_1 \cap I_2$ (aber im allgemeinen \neq !)
- (e) Sei R kommutativ mit Eins, $X \subseteq R$. Die Menge

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

heißt das von X erzeugte Ideal.

- (f) Sind I_1, I_2 Ideale in einem kommutativen Ring R mit Eins, so ist $I_1 + I_2 = (I_1 \cup I_2)$ und $I_1 \cdot I_2 = (\{ab : a \in I_1, b \in I_2\})$.

2.2 Polynomringe

Definition + Bemerkung 2.2.1

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

- (a) Ein **Polynom** über R ist eine Folge $f = (a_i)_{i \in \mathbb{N}}$ mit einem $n_0 \in \mathbb{N}$ so, dass $\forall i > n_0 : a_i = 0$.

$$\text{Symbolische Schreibweise: } f = \sum_{i=0}^n a_i X^i$$

- (b) Die Menge $R[X]$ der Polynome über R ist kommutativer Ring mit Eins mit den Verknüpfungen

$$\begin{aligned} (a_i)_{i \in \mathbb{N}} + (b_i)_{i \in \mathbb{N}} &= (a_i + b_i)_{i \in \mathbb{N}} \\ (a_i)_{i \in \mathbb{N}} \cdot (b_i)_{i \in \mathbb{N}} &= (c_i)_{i \in \mathbb{N}} \text{ mit } c_i = \sum_{k=0}^i a_k b_{i-k} \end{aligned}$$

- (c) $R \rightarrow R[X]$, $a \mapsto (a, 0, \dots)$ ist injektiver Ringhomomorphismus
- (d) Für $f = \sum a_i X^i \in R[X]$, $f \neq 0$, heißt $\text{Grad}(f) := \max\{i \in \mathbb{N}, a_i \neq 0\}$ der Grad von f .
- (e) Für f, g ist $\text{Grad}(f + g) \leq \max(\text{Grad}(f), \text{Grad}(g))$, falls $f, g, f + g \neq 0$
- (f) Für f, g ist $\text{Grad}(f \cdot g) \leq \text{Grad}(f) + \text{Grad}(g)$ für $f, g, f \cdot g \neq 0$.
 = , falls R nullteilerfrei

Folgerung 2.2.2

Ist R Integritätsbereich, so ist $R[X]$ ebenfalls Integritätsbereich und $R[X]^\times = R^\times$

Proposition 2.2.3

Sei R kommutativer Ring mit Eins.

- (a) Zu jedem $x \in R$ gibt es genau einen Ringhomomorphismus $\varphi_x : R[X] \rightarrow R$ mit $\varphi_x|_R = \text{id}_R$ und $\varphi_x(X) = x$. Es ist $\varphi_x(a_0, a_1, \dots) = \sum_{i \geq 0} a_i x^i$
- (b) Zu jedem Homomorphismus $\alpha : R \rightarrow R'$ von Ringen mit Eins und jedem $y \in R'$ gibt es genau einen Ringhomomorphismus $\varphi_y : R[X] \rightarrow R'$, $\varphi_y|_R = \alpha$ und $\varphi_y(X) = y$.
 Explizit: $\varphi_y(\sum a_i X^i) = \sum \alpha(a_i) y^i$.

Beweis:

- (a) ist (b) für $R' = R$ und $\alpha = \text{id}_R$
- (b) Die angegebene Formel ist die einzig mögliche Definition dieses Ringhomomorphismus, weil $\varphi_y(a_0, a_1, \dots) = \varphi_y(\sum_{i=0}^n a_i X^i) = \sum_{i=0}^n \varphi_y(a_i) \varphi_y(X)^i$ sein muß. ■

Bemerkung 2.2.4

Die vorangehende Folgerung bleibt richtig, wenn R' nicht kommutativ ist, solange $\alpha(R) \subseteq Z(R')$ ist, also $\alpha(a) \cdot b = b \cdot \alpha(a)$ für alle $a \in R, b \in R'$ gilt.

Bemerkung 2.2.5

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

Beweis: Ist $\alpha : R \rightarrow R'$ Ringhomomorphismus, so sei $\Psi : R[X] \rightarrow R'[X]$ der Homomorphismus, der durch $\alpha : R \rightarrow R' \xrightarrow[2.8(c)]{} R'[X]$ und $X \mapsto X$ bestimmt ist. ■

Definition + Bemerkung 2.2.6 (a) $R[[X]] = \{(a_i)_{i \in \mathbb{N}} : a_i \in R\}$ ist mit $+$ und \cdot wie im Polynomring ein kommutativer Ring mit Eins. $R[[X]]$ heißt **Ring der (formalen) Potenzreihen** über R .

Schreibweise (auch):

$$f = \sum_{i=0}^{\infty} a_i X^i$$

für $f = (a_i)_{i \in \mathbb{N}}$

(b) $R[X]$ ist Unterring von $R[[X]]$.

(c) 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 $f, g \in R[[X]] \setminus \{0\}$:

$$o(f + g) \geq \min\{o(f), o(g)\} \text{ und } o(f \cdot g) \geq o(f) + o(g)$$

wobei in der Ungleichung für die Multiplikation Gleichheit gilt, wenn R nullteilerfrei ist.

Proposition 2.2.7 (a) Ist R Integritätsbereich, so ist $o(f \cdot g) = o(f) + o(g) \forall f, g \in R[[X]] \setminus \{0\}$ und es gilt: $R[[X]]^\times = \{f = \sum_{i=0}^{\infty} a_i X^i \in R[[X]] : a_0 \in R^\times\}$

(b) Ist $R = K$ Körper, so ist $m := K[[X]] \setminus K[[X]]^\times = \{\sum a_i X^i : a_0 = 0\}$ Ideal in $K[[X]]$, und das einzige maximale.

Beweis: (a), (b), (d) ✓

(c) " \subseteq ": Sei $f = \sum a_i X^i \in R[[X]]^\times$. Dann gibt es $g = \sum b_i X^i \in R[[X]]$ mit $1 = fg = a_0 b_0 + (a_1 b_0 + a_0 b_1)X + \dots \Rightarrow a_0 \in R^\times$

" \supseteq ": Definiere $g = \sum b_i X^i$ rekursiv durch $b_0 = a_0^{-1}, b_i := a_0^{-1} \cdot \sum_{k=1}^i (-1)^k a_k b_{i-k}, i \geq 1$. Dann ist $fg = 1$ ■

Beispiel: $i = 1 : b_i = a_0^{-1}(a_1 b_0)$

2.3 Faktorringe

Sei R ein kommutativer Ring mit Eins.

Definition + Bemerkung 2.3.1 (a) Sei I Ideal in R . Durch die Verknüpfung $\bar{x} \cdot \bar{y} := \overline{xy}$ wird die Faktorgruppe $(R, +)/(I, +)$ ein kommutativer Ring mit Eins. Dieser Ring R/I heißt **Faktoring** oder **Quotientenring** von R und I . (Man verwechsle diesen Begriff des Quotientenrings nicht mit dem Quotientenkörper eines Integritätsbereiches, siehe weiter unten!)

- (b) Die Restklassenabbildung $\pi : R \rightarrow R/I, x \mapsto \bar{x}$ ist surjektiver Ringhomomorphismus mit $\text{Kern}(\pi) = I$.
- (c) (UAE des Faktorrings:) Sei $\varphi : R \rightarrow R'$ ein Ringhomomorphismus. Dann gibt es zu jedem Ideal $I \subseteq R$ mit $I \subseteq \text{Kern}(\varphi)$ einen eindeutig bestimmten Ringhomomorphismus $\bar{\varphi} : R/I \rightarrow R'$ mit $\varphi = \bar{\varphi} \circ \pi$
- (d) (Homomorphiesatz für Ringe:) Ist $\varphi : R \rightarrow R'$ surjektiver Ringhomomorphismus, dann ist $R' \cong R/\text{Kern}(\varphi)$.

Beweis:

- (a) **Wohldef. des Produkts:** Seien $x', y' \in R$ mit $\bar{x}' = \bar{x}, \bar{y}' = \bar{y}$. Dann gibt es $a, b \in I$ mit $x' = x + a, y' = y + b$. $\Rightarrow x'y' = (x + a)(y + b) = xy + \underbrace{ay + bx + ab}_{\in I} \Rightarrow \bar{x}'\bar{y}' = \bar{xy}$.
Die restlichen Eigenschaften vererben sich dann von R .
- (b) π ist surjektiver Gruppenhomomorphismus mit $\text{Kern}(\varphi) = I$ nach Satz 1(a). $\pi(xy) = \pi(x) \cdot \pi(y)$ nach Definition der Verknüpfung.
- (c) Nach Satz 1(d) gibt es einen eindeutig bestimmten Gruppenhomomorphismus $\bar{\varphi} : R/I \rightarrow R'$ mit $\varphi = \bar{\varphi} \circ \pi$.
Zeige also: $\bar{\varphi}$ ist Ringhomomorphismus: Für $x, y \in R$ ist $\bar{\varphi}(\bar{xy}) = \varphi(xy) = \varphi(x)\varphi(y) = \bar{\varphi}(\bar{x})\bar{\varphi}(\bar{y})$
- (d) Folgt aus (c) und Satz 1(a) ■

Definition 2.3.2 (a) Ein Ideal $I \subsetneq R$ heißt **maximal**, wenn es kein Ideal I' in R gibt mit $I \subsetneq I' \subsetneq R$.

Beispiel: In $R = K[X]$, K Körper, ist $(X) = \{f = \sum_{i=0}^n a_i X^i, a_0 = 0\}$ maximal.

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

2 Ringe

Beispiel:

- (1) Für $p \in \mathbb{Z}$, $p > 0$ gilt: p prim $\Leftrightarrow p\mathbb{Z}$ ist Primideal in \mathbb{Z} (sogar maximal)
- (2) (X) ist Primideal in $R[[X]] \Leftrightarrow R$ ist Körper.

(3) $\{0\}$ ist Primideal in \mathbb{Z} .

Bemerkung 2.3.3 (a) R ist nullteilerfrei $\Leftrightarrow (0)$ ist Primideal.

(b) $I \subsetneq R$ ist Primideal genau dann, wenn R/I nullteilerfrei ist.

Beweis:

(a) R ist nicht nullteilerfrei $\Leftrightarrow \exists a, b \in R \setminus \{0\}: ab = 0 \Leftrightarrow (0)$ kein Primideal.

(b) Seien $x, y \in R$ mit $x \cdot y = 0$, also $\bar{x} \cdot \bar{y} = 0$ in R/I . I Primideal $\Leftrightarrow x \in I$ oder $y \in I \Leftrightarrow \bar{x} = 0$ oder $\bar{y} = 0 \Leftrightarrow R/I$ ist nullteilerfrei. ■

Bemerkung 2.3.4

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

- (a) Jedes maximale Ideal ist Primideal.
- (b) I ist maximales Ideal $\Leftrightarrow R/I$ ist Körper.

Beweis:

(a) folgt aus (b) und Bemerkung 2.3.5.

(b) Nach 2.1.3 (e) ist R/I genau dann Körper, wenn (0) und R/I die einzigen Ideale in R/I sind. Die Behauptung folgt dann aus: $I \subsetneq J \subsetneq R$ in $R \Leftrightarrow 0 \neq \bar{J} \neq R/I$ in R/I wobei \bar{J} das Bild von J in R/I ist. ■

Bemerkung 2.3.5

Sei I ein Ideal in R . Dann entsprechen die Ideale in R/I bijektiv den Idealen in R , die I enthalten.

Beweis: Sei $\pi : R \rightarrow R/I$ die Restklassenabbildung. Für jedes Ideal \bar{J} in R/I ist $\pi^{-1}(\bar{J})$ ein Ideal in R . Es gilt $\pi^{-1}(\bar{J}) \supseteq \pi^{-1}(0) = \text{Kern } \pi = I$.

Sei umgekehrt $J \subsetneq R$ ein Ideal mit $I \subseteq J$. Dann ist $\bar{J} := \pi(J)$ ein Ideal in R/I , da π surjektiv ist.

Weiter ist $\pi^{-1}(\pi(J)) = J$, da Kern $\pi \subseteq J$, und $\pi(\pi^{-1}(\bar{J})) = \bar{J}$, da π surjektiv ist. ■

Beispiel 2.3.6 (Algebraische Konstruktion der reellen Zahlen)

Sei $C = \{(a_n)_{n \in \mathbb{N}} : (a_n) \text{ Cauchy-Folge, } a_n \in \mathbb{Q}\}$ (dh. 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: $C \subset \prod_{n \in \mathbb{N}} \mathbb{Q}$).

$N = \{(a_n) \in C : (a_n) \text{ Nullfolge}\}$ (dh. für $k \in \mathbb{N} \exists n \in \mathbb{N} : |a_i| < \frac{1}{k} \forall i > n$)

N ist Ideal in C : ✓

Beh.: C/N ist Körper (bzw. N ist maximal)

Beweis: Sei $a = (a_n)_{n \in \mathbb{N}} \in C \setminus N$. zu zeigen: $1 \in (N + (a))$.

$(a_n) \notin N \Rightarrow a_n = 0$ nur für endlich viele n , dh. $a_i \neq 0$ für $i > n_0$.

$$b_n := \begin{cases} 0 & , a_i = 0 | i \leq n_0 \\ \frac{1}{a_i} & , a_i \neq 0 | i > n_0 \end{cases}$$

$b = (b_n) \in C$.

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

$$\Rightarrow 1 - ab = (d_n), d_n = \begin{cases} 1 & : n < n_0 \\ 0 & : n \geq n_0 \end{cases}$$

$\Rightarrow (d_n) \in N \Rightarrow 1 = (d_n) + ba \in N + (a) \Rightarrow N$ maximal.

$\Rightarrow C/N = \mathbb{R}$!

Satz 7 (Chinesischer Restsatz)

Sei R kommutativer Ring mit Eins, I_1, \dots, I_n Ideale in R mit $I_\nu + I_\mu = R$ für alle $\nu \neq \mu$ (dann heißen I_ν, I_μ **relativ prim** oder **koprim**) Für $\nu = 1, \dots, n$ sei $\pi_\nu : R \rightarrow R/I_\nu$ die Restklassenabbildung. Dann gilt:

(a) $\varphi : R \rightarrow R/I_1 \times \dots \times R/I_n$ ist surjektiv.
 $x \mapsto (\pi_1(x), \dots, \pi_n(x))$

(b) Wegen dem Homomorphiesatz und $\text{Kern}(\varphi) = \bigcap_{\nu=1}^n I_\nu$ gilt:

$$R/I_1 \times \dots \times R/I_n \cong R / \bigcap_{\nu=1}^n I_\nu$$

(c) (Simultane Kongruenzen:)

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

Beweis: Es genügt z.z.: $\bar{e}_\nu = (0, \dots, 0, \underbrace{1}_{\nu\text{-te Stelle}}, 0, \dots, 0) \in \text{Bild}(\varphi)$ für jedes ν ,
 dh. es gibt $e_\nu \in R$ ($\nu = 1, \dots, n$) mit $e_\nu \in I_\mu$ für $\nu \neq \mu$ und $1 - e_\nu =: a_\nu \in I_\nu$ (Denn
 für $x = (\bar{x}_1, \dots, \bar{x}_n) \in R/I_1 \times \dots \times R/I_n$ sei $e := \sum_{\nu=1}^n r_\nu e_\nu$ mit $r_\nu \in p_\nu^{-1}(\bar{x}_\nu) \Rightarrow \varphi(e) = \sum p_\nu(r_\nu e_\nu) = x$.)
 Nach Voraussetzung gibt es für jedes $\mu \neq \nu$ $a_\mu \in I_\nu, b_\mu \in I_\mu$ mit

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

$\Rightarrow 1 - e_\nu = a_\nu$ wie gewünscht. ■

2.4 Teilbarkeit

Sei R ein Integritätsbereich.

Definition + Bemerkung 2.4.1

Seien $a, b \in R \setminus \{0\}$.

- (a) a **teilt** b (Schreibweise $a \mid b$) $:\Leftrightarrow b \in (a)$ ($\Leftrightarrow \exists x \in R : b = ax$)
- (b) $d \in R$ heißt **größter gemeinsamer Teiler** von a und b , (Schreibweise $\text{ggT}(a,b)$)
wenn gilt:
 - (i) $d \mid a$ und $d \mid b$ bzw. $a \in (d), b \in (d)$
 - (ii) ist $d' \in R$ auch Teiler von a und b , so gilt $d' \mid d$ bzw. $d \in (d')$
- (c) Ist $d \in R$ ein ggT von a und b und $e \in R^\times$, so ist auch $e \cdot d$ ein ggT. Sind d, d' beide ggT von a und b , so gibt es $e \in R^\times$ mit $d' = ed$.

Beweis: Nach Definition gibt es $x, y \in R$ mit $d' = xd$ und $d = yd' \Rightarrow d' = xyd' \Rightarrow d'(1 - xy) = 0 \xrightarrow{d' \neq 0} 1 = xy \Leftrightarrow x, y \in R^\times$ ■
 R nullteilerfrei

- (d) In analoger Weise wird das kleinste gemeinsame Vielfache definiert.

Beispiel:

- (a) In \mathbb{Z} gibt es einen größten gemeinsamen Teiler.

(b) In jedem nullteilerfreiem Hauptidealring R gibt es zu je zwei Elementen a, b einen größten gemeinsamen Teiler: Denn $(a, b) = (a) + (b)$ ist ein Hauptideal, das heißt, es gibt ein $d \in R$ mit $(a, b) = (d)$. Also gilt $d \mid a$ und $d \mid b$ und für jedes $d' \in R$, für das $d' \mid a$ und $d' \mid b$ gilt, gilt auch: $(a) \subseteq (d')$, $(b) \subseteq (d')$, also $(a, b) \subseteq (d')$ und somit $(d) \subseteq (d')$, also $d' \mid d$.

(c) In $\mathbb{Z}[\sqrt{-5}]$ gibt es zu 6 und $4 + 2\sqrt{-5}$ keinen größten gemeinsamen Teiler.

Definition 2.4.2

Ein Integritätsbereich R heißt **euklidisch**, wenn es eine Abbildung: $\delta : R \setminus \{0\} \rightarrow \mathbb{N}$ mit folgender Eigenschaft gibt: zu $f, g \in R, g \neq 0$ gibt es $q, r \in R$ mit $f = qg + r$ mit $r = 0$ oder $\delta(r) < \delta(g)$.

Beispiel: \mathbb{Z} mit $\delta(a) = |a|$, $K[X]$ mit $\delta(f) = \text{Grad}(f)$

Bemerkung 2.4.3

Sei R euklidisch.

- (a) Für $a, b \in R \setminus \{0\}$ gilt:
- (i) in R gibt es einen ggT von a und b , er heiße d .
 - (ii) $(d) = (a, b) = (a) + (b)$
- (b) Jeder euklidische Ring ist ein Hauptidealring.

Beweis:

- (a) \exists sei $\delta(a) \geq \delta(b)$. Nach Voraussetzung gibt es $q_1, r_1 \in R$ mit $a = q_1 b + r_1$, $\delta(r_1) < \delta(b)$ oder $r_1 = 0$.
Ist $r_1 = 0$, so ist $a \in (b) = (a, b)$ und $\text{ggT}(a, b) = b$. 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...

$$\begin{aligned} r_i &= q_{i+2} r_{i+1} + r_{i+2} \\ \Rightarrow \quad &\vdots \quad \quad \quad \vdots \\ r_{n-2} &= q_n r_{n-1} \end{aligned}$$

(da $\delta(r_{i+2}) < \delta(r_{i+1})$)

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

denn: $d \mid r_{n-2}$ (vorletzte Zeile: $r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \Rightarrow d \mid r_{n-3}$)

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

umgekehrt: Sei d' Teiler von a und $b \Rightarrow d' \mid r_1 \xrightarrow{\text{Induktion}} d' \mid r_i \forall i \Rightarrow d' \mid d$.

noch zu zeigen ist $(d) = (a, b)$:

" \subseteq ": $d \in (a, b)$ Nach Konstruktion ist $r_{i+2} \in (r_i, r_{i+1}) \subset \dots \subset (a, b) \forall i$

" \supseteq ": $a \in (d), b \in (d)$ nach Definition.

- (b) Sei $I \subseteq R$ 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 $\delta(r) < \delta(a) \not\leq$ also $r = 0 \Rightarrow I = (a)$ ■

Definition + Bemerkung 2.4.4

Sei R kommutativer Ring mit Eins.

- (a) $x, y \in R$ heißen **assoziert**, wenn es $e \in R^\times$ mit $y = xe$ gibt. "assoziert" ist eine Äquivalenzrelation.
- (b) $x \in R \setminus R^\times$, $x \neq 0$ heißt **irreduzibel** (unzerlegbar), wenn aus $x = y_1 \cdot y_2$ 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, dh. 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 (bzw. prim) ist.
- (e) Ist R nullteilerfrei, so ist jedes von Null verschiedene Primelement irreduzibel.

Beweis: Sei (x) Primideal und $x = y_1 y_2$, $y_1, y_2 \in R \Rightarrow \exists e: y_1 \in (x)$, dh. $y_1 = xa$ für ein $a \in R$ (R nullteilerfrei, $x \neq 0$) $\Rightarrow x = x a y_2 \Rightarrow x(1 - a y_2) = 0 \xrightarrow{x \neq 0} a y_2 = 1 \Rightarrow y_2 \in R^\times$ ■

Beispiel 2.4.5 (a) In $\mathbb{Z}/6\mathbb{Z}$ ist 2 nicht irreduzibel: $2 \cdot (-2) = 2$.

- (b) In $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ ist $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$. In R ist 2 kein Primelement, weder $1 + \sqrt{-5}$ noch $1 - \sqrt{-5}$ sind durch 2 teilbar, **aber** 2 ist irreduzibel!

denn: Sei $2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) \Rightarrow 4 = |2|^2 = (a + b\sqrt{-5})(a - b\sqrt{-5})(\dots) = (a^2 + 5b^2)(c^2 + 5d^2) = a^2 c^2 + \underbrace{5P}_{P \geq 0} \Rightarrow P = 0 \Rightarrow b = d = 0 \Rightarrow a^2 = 1, c^2 = 4$

Proposition + Definition 2.4.6

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 irreduziblen Elementen schreiben.

(b) Sind diese drei Eigenschaften 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 ($\neq 0$) bezüglich "assoziert".

Dann heißt (i) $\forall x \in R \setminus \{0\} \exists! e \in R^\times$ und für jedes $p \in \mathcal{P}$ ein $\nu_p(x) \geq 0 : x = e \prod_{p \in \mathcal{P}} p^{\nu_p}$. (beachte $\nu_p \neq 0$ nur für endlich viele p).

Beweis:

(i) \Rightarrow (ii) \checkmark

(ii) \Rightarrow (iii) Sei $x \neq 0, x = ep_1 \cdot \dots \cdot p_r, p_i \in \mathcal{P}, e \in R^\times$.

Sei weiter $x = q_1 \cdot \dots \cdot q_s$ mit irreduziblem Element q_j .

Es ist $x \in (p_1) \Rightarrow \exists j$ mit $q_j \in (p_1)$. $\text{Cf. } j = 1$ dh. $q_1 = \varepsilon_1 p_1$ mit $\varepsilon_1 \in R^\times$ (da q_1 irreduzibel) $\Rightarrow \varepsilon_1 q_2 \cdot \dots \cdot q_s = ep_2 \cdot \dots \cdot p_r$. Mit Induktion über r folgt die Behauptung.

(iii) \Rightarrow (i) Noch zu zeigen: Jedes irreduzible Element in R ist prim.

Sei $p \in R \setminus R^\times$ irreduzibel, $x, y \in R$ mit $xy \in (p)$, also $xy = pa$ für ein $a \in R$.

Schreibe $x = q_1 \cdot \dots \cdot q_m, y = s_1 \cdot \dots \cdot s_n, a = p_1 \cdot \dots \cdot p_l$ mit irreduziblen Elementen q_i, s_j, p_k .

$$\Rightarrow xy = q_1 \dots q_m s_1 \dots s_n = pa = p \cdot p_1 \cdot \dots \cdot p_l \xrightarrow{\text{Eindeutigkeit}} p \in \{q_1, \dots, q_m, s_1, \dots, s_n\} \text{ (bis auf Einheiten)}$$



Bemerkung 2.4.7

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

Beweis: Sei \mathcal{P} wie in 2.4.6 Vertretersystem der Primelemente.

$$a = e_1 \prod_{p \in \mathcal{P}} p^{\nu_p(a)}, b = e_2 \prod_{p \in \mathcal{P}} p^{\nu_p(b)} \implies d := \prod_{p \in \mathcal{P}} p^{\nu_p(d)}$$

mit $\nu_p(d) = \min(\nu_p(a), \nu_p(b))$ ist ggT von a und b .



Satz 8

Jeder nullteilerfreie Hauptidealring ist faktoriell.

Beweis:

- (1) Jedes $x \in R \setminus \{0\}$ lässt sich als Produkt von irreduziblen Elementen schreiben.
- (2) Jedes irreduzible $p \in R \setminus \{0\}$ erzeugt ein maximales Ideal. Mit 2.4.6 folgt dann die Behauptung.

B(2) Sei $p \in R \setminus \{0\}$ irreduzibel, I Ideal in R mit $(p) \subseteq I \subset R$.
 Nach Voraussetzung gibt es $a \in R$ mit $I = (a)$, $a \notin R^\times$, da $I \neq R$.
 Da $p \in (p) \subseteq I = (a)$, gibt es $\varepsilon \in R$ mit $p = a\varepsilon \xrightarrow{p \text{ irreduzibel}} \varepsilon \in R^\times \Rightarrow (p) = (a) = I$

B(1) $x \in R \setminus \{0\}$ heie Strenfried, wenn x nicht als Produkt von irreduziblen Elementen darstellbar ist.

Sei x Strenfried. Dann ist $x \notin R^\times$ und x nicht irreduzibel, also $x = x_1 y_1$ mit $x_1, y_1 \notin R^\times$.

Sei x_1 Strenfried (sonst ist x doch Produkt von irreduziblen Elementen). Also $x_1 = x_2 y_2$, $x_2, y_2 \notin R^\times$.

Sei x_2 Strenfried. Induktiv erhalten wir x, x_1, x_2, \dots alles Strenfriede mit $(x) \subset (x_1) \subset (x_2) \subset \dots$

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

Es gibt $a \in R$ mit $I = (a) \Rightarrow \exists i$ mit $a \in (x_i) \Rightarrow x_j \in (x_i)$ fr alle $j > i$ ■

Bemerkung 2.4.8

Sei R ein faktorieller Ring, \mathcal{P} ein Vertretersystem der Primelemente $\neq 0$. Fr $x \in R \setminus \{0\}$ sei $x = e \prod_{p \in \mathcal{P}} p^{\nu_p(x)}$ die eindeutige Darstellung, also $e \in R^\times$, $\nu_p(x) \in \mathbb{N}$, $\nu_p(x) \neq 0$ nur fr endlich viele $p \in \mathcal{P}$. Dann gilt fr jedes $p \in \mathcal{P}$:

- (a) $\nu_p(x) = n \iff p^n \mid x$ und $p^{n+1} \nmid x$
- (b) Die Abbildung $\nu_p \rightarrow \mathbb{N}$ erfllt
 - (i) $\nu_p(x \cdot y) = \nu_p(x) + \nu_p(y)$
 - (ii) $\nu_p(x + y) \geq \min(\nu_p(x), \nu_p(y))$, falls $x + y \neq 0$
- (c) Sei $\rho \in \mathbb{R}$, $0 < \rho < 1$. Dann ist die Abbildung $|\cdot|_\rho : R \rightarrow \mathbb{R}$,

$$|x|_\rho = \begin{cases} \rho^{\nu_p(x)}, & x \neq 0 \\ 0 & x = 0 \end{cases}$$

ein „nichtarchimedischer Betrag“ auf R , d.h. $|x \cdot y|_\rho = |x|_\rho \cdot |y|_\rho$ und $|x + y|_\rho \leq \max(|x|_\rho, |y|_\rho)$.

- (d) $d_\rho(x, y) = |x - y|_\rho$ ist eine Metrik auf R .

Beispiel: $R = \mathbb{Z}$, $\mathcal{P} = \{p \in \mathbb{N}_{>0}, p \text{ Primzahl}\}$. ν_p ist die p -adische Bewertung und $|\cdot|_{\frac{1}{p}}$ ist der p -adische Betrag auf \mathbb{Z} (und \mathbb{Q}).

Satz 9 (Irreduzibilitätskriterium für Polynome)

Sei R ein faktorieller Ring, $p \in \mathcal{P}$, $f = \sum_{i=0}^n a_i X^i \in R[X]$ mit $a_n \neq 0$, $\text{ggT}(a_0, \dots, a_n) = 1$, $p \nmid a_n$.

- (a) (Eisenstein) Ist $n > 0$, $p \mid a_i$ oder $a_i = 0$ für $i = 0, \dots, n - 1$, $p^2 \nmid a_0 \neq 0$, so ist f irreduzibel.

Beweis: Sei $f = gh$ mit $g = \sum_{i=0}^r b_i X^i$, $h = \sum_{i=0}^s c_i X^i$ $b_r \neq 0 \neq c_s \Rightarrow n = r + s$, $a_n = b_r c_s$, $a_0 = b_0 c_0 \Rightarrow p \nmid b_r, p \nmid c_s$

- (a) $\exists p \mid b_0, p \nmid c_0$.
Sei t maximal mit $p \mid b_i$ für $i = 0, \dots, t$
Dann ist $0 \leq t \leq r - 1$ und

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

$\Rightarrow t + 1 = n \Rightarrow r = n \Rightarrow s = 0 \Rightarrow f = c_0 \cdot g$, nach Voraussetzung ist dann $c_0 \in R^\times$. ■

2.5 Brüche

Ziel: Verallgemeinere die Konstruktion von \mathbb{Q} aus \mathbb{Z} .

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

mit $\frac{m}{n} \sim \frac{m'}{n'} \Leftrightarrow mn' = m'n$

Definition + Bemerkung 2.5.1

Sei R kommutativer Ring mit Eins, $S \subseteq (R, \cdot)$ 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 eine Äquivalenzklasse von (a, s)

2 Ringe

Beweis: z.z.: \sim ist Äquivalenzrelation:

reflexiv ✓

symmetrisch ✓

transitiv: $\left. \begin{array}{l} (1) \quad a_2 s_1 = a_1 s_2 \\ (2) \quad a_3 s_2 = a_2 s_3 \end{array} \right\} \xrightarrow{?} a_3 s_1 = a_1 s_3$

$$a_3 s_2 s_1 \stackrel{(2)}{=} a_2 s_3 s_1 \stackrel{(1)}{=} a_1 s_3 s_2 \Rightarrow s_2(a_3 s_1 - a_1 s_3) = 0$$

(falls R nullteilerfrei und $0 \notin S \Rightarrow a_3 s_1 = a_1 s_3$)

Andernfalls sei nun mit $t, t' \in S$ $\left. \begin{array}{l} t(a_2 s_1 - a_1 s_2) = 0 \\ t'(a_2 s_3 - a_3 s_2) = 0 \end{array} \right\} \Rightarrow t t' s_2 (a_3 s_1 - a_1 s_3) = t(t' a_3 s_2 s_1 - t' a_1 s_3 s_2) \stackrel{(2)}{=} t(t' a_2 s_3 s_1 - t' a_1 s_3 s_2) = t s_3 t'(a_2 s_1 - a_1 s_2) \stackrel{(1)}{=} 0$ ■

(b) Mit $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$ 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 $\frac{a'_1}{s'_1} = \frac{a_1}{s_1} \Rightarrow \exists t \in S : t(a'_1 s_1 - a_1 s'_1) = 0(*) \Rightarrow$

$$t(a'_1 a_2 s_1 s_2 - a_1 a_2 s_2 s'_1) \stackrel{(*)}{=} (t a_1 s'_1 a_2 s_2 - t a_1 a_2 s_2 s'_1) = 0$$

+ wohldefiniert: Seien die $\frac{a'_1}{s'_1}, \frac{a_1}{s_1}$ wie oben. $\Rightarrow t(s'_1 s_2 (a_1 s_2 + a_2 s_1) - s_1 s_2 (a'_1 s_2 + a_2 s'_1)) = t s_2 (a_1 s_2 s'_1 + a_2 s_1 s'_1 - a'_1 s_1 s_2 - a_2 s_1 s'_1) \stackrel{(\dots)}{=} 0$. Die restlichen Eigenschaften vererben sich von R ■

Definition + Bemerkung 2.5.2

Sei R Integritätsbereich, $S = R \setminus \{0\}$. Dann ist $\text{Quot}(R) := R_S$ ein Körper, denn das Inverse zu $\frac{b}{a}$ mit $a \neq 0$ ist $\frac{a}{b}$. Er heißt der **Quotientenkörper** von R . (Dieser Begriff hat mit dem Quotientenring R/I von R modulo einem Ideal I nichts zu tun.)

Beispiel:

(a) $R = \mathbb{Z}[X] \Rightarrow \text{Quot}(R) = \mathbb{Q}(X)$

(b) $R = K[X_1, \dots, X_n]$, K Körper $\Rightarrow \text{Quot}(R) = K(X_1, \dots, X_n)$ Körper der rationalen Funktionen in n Variablen.

Beispiele 2.5.3 (a) Ist $0 \in S$, so ist $R_S = 0$.

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

(c) Sei $\mathfrak{p} \subset R$ Primideal, dann ist $S = R \setminus \mathfrak{p}$ ist Monoid.
 $R_S =: R_{\mathfrak{p}}$ heißt Lokalisierung von R nach \mathfrak{p} .

Beispiel:

- a) $R = \mathbb{Z}$, $\mathfrak{p} = (2) \Rightarrow \mathbb{Z}_{(2)} = \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \text{ ungerade} \right\}$
- b) $\mathfrak{p} = (0)$, R nullteilerfrei, dann ist $R_{\mathfrak{p}} = \text{Quot}(R)$.
- c) $R = K[X]$, $\mathfrak{p} = (X)$, dann ist $R_{\mathfrak{p}} = \left\{ \frac{f}{g}, f, g \in K[X], g(0) \neq 0 \right\}$.

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

denn: Sei $\frac{z}{y} \in R_{\mathfrak{p}} \setminus \mathfrak{p}R_{\mathfrak{p}}$, dh. $z \in R \setminus \mathfrak{p}, y \in R \setminus \mathfrak{p} \Rightarrow \frac{z}{y} \in R_{\mathfrak{p}} \Rightarrow \frac{z}{y} \in (R_{\mathfrak{p}})^{\times}$,
 typisches Beispiel: $R = \mathbb{R}[X]$ (oder $R = C^0([-1, 1])$) $\mathfrak{p} = \{f \in R : f(0) = 0\}$ ist
 Primideal in R . $R_{\mathfrak{p}} = \left\{ \frac{f}{g} : f, g \in R, g(0) \neq 0 \right\}$

Bemerkung 2.5.4

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

- (a) Die Abbildung $i_S : R \rightarrow R_S, a \mapsto \frac{a}{1}$ ist Ringhomomorphismus
- (b) i_S ist injektiv genau dann, wenn S keinen Nullteiler von R enthält. ($0 \notin S$)

Beweis: $\frac{a}{1} = 0 = \frac{0}{1}$ in $R_S \Rightarrow \exists s \in S$ mit $s(a1 - 01) = 0$ ■

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

Beweis: $\left(\frac{s}{1}\right)^{-1} = \frac{1}{s}$ ■

(d) (UAE) Zu jedem Homomorphismus $\varphi : R \rightarrow R'$ von Ringen mit Eins mit $\varphi(S) \subset (R')^{\times}$ gibt es genau einen Homomorphismus $\tilde{\varphi} : R_S \rightarrow R'$ mit $\varphi = \tilde{\varphi} \circ i_S$

Beweis: $\tilde{\varphi}\left(\frac{a}{s}\right) = \tilde{\varphi}\left(a \frac{1}{s}\right) = \tilde{\varphi}\left(\frac{a}{1} \left(\frac{s}{1}\right)^{-1}\right) = \varphi(a)\varphi(s)^{-1}$ ■

2.6 Der Satz von Gauß

Sei R faktorieller Ring, \mathcal{P} Vertretersystem der von Null verschiedenen Primelemente in R .

Bemerkung 2.6.1

Für jedes $p \in \mathcal{P}$ lässt sich ν_p fortsetzen zu einer Abbildung $\nu_p : \text{Quot}(R) \setminus \{0\} \rightarrow \mathbb{Z}$, die die Eigenschaften von 2.4.8 b) erfüllt. Dabei gilt für $a, b \in R \setminus \{0\} : \nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b)$.

Beispiel:

2 Ringe

- (a) $R = \mathbb{Z}$, $\mathcal{P} = \{p \in \mathbb{N}, p \text{ Primzahl}\}$. ν_p ist die **p -adische Bewertung** auf \mathbb{Q} . Die Vervollständigung von \mathbb{Q} wie in Beispiel 2.3.6 ergibt den Körper \mathbb{Q}_p der p -adischen Zahlen.
- (b) $R = \mathbb{C}[X]$, $\mathcal{P} = \{X - a, a \in \mathbb{C}\}$. Für $p = X - a \in \mathcal{P}$, $f \in \mathbb{C}[X]$ ist $\nu_p(f) = \text{ord}_a(f)$ die Nullstellenordnung der Nullstelle a .

Definition + Proposition 2.6.2

Sei R faktorieller Ring, \mathcal{P} Vertretersystem der von Null verschiedenen Primelemente in R , $p \in \mathcal{P}$ und $K = \text{Quot}(R)$.

- (a) Für $f = \sum_{i=0}^n a_i X^i \in K[X] \setminus \{0\}$ sei $\nu_p(f) := \min\{\nu_p(a_i), i = 0, \dots, n\}$.
- (b) $f \in K[X] \setminus \{0\}$ heißt **primitiv**, wenn $\nu_p(f) = 0$ für alle $p \in \mathcal{P}$ ist.
- (c) (Gauß) Für $f, g \in K[X] \setminus \{0\}$ gilt: $\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$ für alle $p \in \mathcal{P}$.

Beweis: Sei $f = \sum_{i=0}^n a_i X^i$, $g = \sum_{j=0}^m b_j X^j$, $f \cdot g = \sum_{k=0}^{m+n} c_k X^k$, also $c_k = \sum_{i+j=k} a_i b_j$.

1. Fall: Sei $m = 0$. Dann ist $c_k = a_k b_0$ für $k = 0, \dots, n$ und

$$\begin{aligned} \nu_p(f \cdot g) &= \min_{i=0}^n (\nu_p(a_i b_0)) \\ &= \min_{i=0}^n (\nu_p(a_i) + \nu_p(b_0)) \\ &= \min_{i=0}^n (\nu_p(a_i)) + \nu_p(b_0) = \nu_p(f) + \nu_p(g) \end{aligned}$$

2. Fall: Sei $f, g \in R[X]$ und primitiv, also $\nu_p(f) = \nu_p(g) = 0$. Sei $i_0 := \min_{i=0}^n \{i : p \nmid a_i\}$ und $j_0 := \min_{j=0}^m \{j : p \nmid b_j\}$. Es ist:

$$c_{i_0+j_0} = \underbrace{a_{i_0} b_{j_0}}_{p \nmid} + \sum_{i=0}^{i_0-1} \underbrace{a_i}_{p \mid} b_{i_0+j_0-i} + \sum_{j=0}^{j_0-1} a_{i_0+j_0-j} \underbrace{b_j}_{p \mid}$$

also gilt $p \nmid c_{i_0+j_0}$ und damit $\nu_p(f \cdot g) = 0$.

3. Fall: f, g sind beliebig. Es gibt $c, d \in K \setminus \{0\}$, so dass $\tilde{f} = c \cdot f$, $\tilde{g} = d \cdot g$ primitiv sind. Dann folgt aus Fall 1 und Fall 2, dass:

$$\begin{aligned} \nu_p(f \cdot g) &= \nu_p\left(\frac{1}{c} \tilde{f} \cdot \frac{1}{d} \tilde{g}\right) \\ &= \nu_p\left(\frac{1}{c}\right) + \nu_p\left(\frac{1}{d}\right) + \nu_p(\tilde{f} \cdot \tilde{g}) \\ &= \nu_p\left(\frac{1}{c}\right) + \nu_p(\tilde{f}) + \nu_p\left(\frac{1}{d}\right) + \nu_p(\tilde{g}) \\ &= \nu_p(f) + \nu_p(g) \end{aligned}$$

Satz 10 (Gauß)

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

Beweis: Sei $K = \text{Quot}(R)$. Dann ist $K[X]$ faktoriell (sogar euklidisch), und $R[X] \subseteq K[X]$ ist ein Unterring. Sei \mathcal{P} Vertretersystem der von Null verschiedenen Primelemente in $K[X]$. O.B.d.A. ist jedes Primpolynom in \mathcal{P} ein primitives Polynom in $R[X]$. Sei weiter $\tilde{\mathcal{P}}$ ein Vertretersystem der von Null verschiedenen Primelemente in R . Sei nun $f \in R[X] \setminus \{0\}$. Schreibe $f = c \cdot f_1 \cdots f_n$ mit $f_i \in \mathcal{P}$ und $c \in (K[X])^\times = K \setminus \{0\}$.

Es ist $c \in R$, denn: für $p \in \tilde{\mathcal{P}}$ ist nach 2.6.2

$$\underbrace{\nu_p(f)}_{\geq 0} = \nu_p(c) + \sum_{i=1}^n \underbrace{\nu_p(f_i)}_{=0},$$

also ist $\nu_p(c) \geq 0$.

Schreibe also $c = e \cdot p_1 \cdots p_m$ mit $e \in R^\times$ und $p_i \in \tilde{\mathcal{P}}$.

Behauptung 1: Jedes $p_i \in \tilde{\mathcal{P}}$ ist auch prim in $R[X]$:

Sei $(p) := p \cdot R[X]$ das von p in $R[X]$ erzeugte Ideal. Es genügt zu zeigen: $R[X]/(p)$ ist nullteilerfrei (nach 2.3.3 b)). Sei $\bar{R} := R/(p \cdot R)$. \bar{R} ist nullteilerfrei, da $p \in \tilde{\mathcal{P}}$ ist, also ist auch $\bar{R}[X]$ nullteilerfrei.

Die Restklassenabbildung $\pi : R \rightarrow \bar{R}$ ist surjektiv und induziert einen surjektiven Ringhomomorphismus $\tilde{\pi} : R[X] \rightarrow \bar{R}[X]$. Es ist Kern $\pi = \{f = \sum_{i=0}^n a_i X^i \in R[X], p \mid a_i, i = 0, \dots, n\} = p \cdot R[X]$, also ist $\bar{R}[X] \cong R[X]/(p)$.

Behauptung 2: Jedes $f_i \in \mathcal{P}$ ist auch prim in $R[X]$:

Seien $g, h \in R[X]$ mit $g \cdot h \in (f_i) := f_i \cdot R[X]$. Da f_i prim in $K[X]$ ist, ist o.B.d.A: $g \in f_i \cdot K[X]$, also $g = f_i \cdot \tilde{g}$ für ein $\tilde{g} \in K[X]$. Für jedes $p \in \tilde{\mathcal{P}}$ ist $0 \leq \nu_p(g) = \nu_p(f_i) + \nu_p(\tilde{g}) = \nu_p(\tilde{g})$, also ist $\tilde{g} \in R[X]$ und damit (f_i) ein Primideal in $R[X]$. ■

Beispiel 2.6.3

$f(X) = X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbb{Q}[X]$, p Primzahl. Beh.: f ist irreduzibel.

Beobachte:

$$f(X) = \frac{X^p - 1}{X - 1}$$

(f heißt "p-tes Kreisteilungspolynom" (Zeichnung fehlt))

Trick: $g(X) = f(X + 1)$ ist genau dann irreduzibel, wenn $f(X)$ irreduzibel ist.

$$g(X) = \frac{(X + 1)^p - 1}{X} = \sum_{k=1}^p \binom{p}{k} X^{k-1}, \quad (n = p-1), \quad \binom{p}{p} = 1 = a_{p-1}, \quad \binom{p}{1} = p = a_0$$

Noch zu überlegen: $\binom{p}{k}$ ist durch p teilbar für $k = 1, \dots, p-1$, bekannt: $\binom{p}{k} = \frac{p!}{k!(p-k)!} \Rightarrow \binom{p}{k}$ ist durch p teilbar. Mit Eisenstein folgt die Behauptung.

2.7 Maximale Ideale

Proposition 2.7.1

Sei R ein kommutativer Ring mit Eins. Dann gibt es zu jedem echten Ideal $I \subsetneq R$ ein maximales Ideal \mathfrak{m} mit $I \subseteq \mathfrak{m}$.

Lemma von Zorn

Sei M eine nicht leere, geordnete Menge. Hat jede total geordnete Teilmenge von M eine obere Schranke in M , so besitzt M ein maximales Element.

Zur Erinnerung:

- \leq heißt **Ordnung** wenn \leq reflexiv, transitiv und antisymmetrisch ist.
- $N \subset M$ ist **total geordnet**, falls für $x, y \in N$ gilt: $x \leq y$ oder $y \leq x$.
- $x \in M$ ist eine **oberere Schranke** für N wenn für alle $y \in N$ gilt: $y \leq x$.
- $m \in M$ heißt **maximal**, wenn für alle $x \in M$ aus $m \leq x$ folgt, dass $x = m$ ist.

Beweis: (der Proposition) Sei M die Menge aller echten Ideale in R , die I enthalten. $I \in M$, also $M \neq \emptyset$. M ist durch \subseteq geordnet.

Behauptung: $n = \bigcup_{J \in M} J$ ist obere Schranke für $N \subseteq M$. Nach Zorn enthält M dann ein maximales Element \mathfrak{m} . \mathfrak{m} ist ein maximales Ideal in R . ■

Beweis: (der Behauptung)

- n ist ein Ideal: Seien $x, y \in n$, also $x \in J_1, y \in J_2$. O.B.d.A.A. $J_1 \subseteq J_2$, also $x \in J_2$ und damit auch $x + y \in J_2 \subseteq n$. Auch gilt für alle $a \in R$: $a \cdot x \in J \subseteq n$.
- $I \subseteq n$ ✓
- n ist eine obere Schranke von N . ✓
- $n \neq R$, denn sonst wäre $1 \in n$, also $1 \in J$ für ein $J \in N$, im Widerspruch zu $J \in M$.

2.8 Moduln

Sei R kommutativ mit Eins.

Definition + Bemerkung 2.8.1 (a) Eine abelsche Gruppe $(M, +)$ zusammen mit einer Abbildung $\bullet : R \times M \rightarrow M$ heißt **R-Modul**, wenn für alle $a, b \in R, x, y \in M$ gilt:

- (i) $a(x + y) = ax + ay$
- (ii) $(a + b)x = ax + bx$
- (iii) $(ab)x = a(bx)$
- (iv) $1x = x$

Beispiel:

- (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 $n \cdot \bar{0} = \bar{0}, n \cdot \bar{1} = \bar{n}$. Jede abelsche Gruppe A ist \mathbb{Z} -Modul durch $nx = \underbrace{x + \dots + x}_{n\text{-mal}}$ und $(-n)x = n(-x)$ für $n \in \mathbb{N}_1, x \in A$
- (4) Jedes Ideal in R ist R -Modul.

(b) Eine Abbildung $\varphi : M \rightarrow M'$ von R -Moduln heißt **R-Modulhomomorphismus** (oder **R-linear**), wenn φ Gruppenhomomorphismus ist und für alle $x \in M, a \in R$ gilt: $\varphi(ax) = a\varphi(x)$

2 Ringe

$$(c) \text{ Hom}_R(M, M') := \{ \varphi : M \rightarrow M' : \varphi \text{ R-linear} \} \text{ ist R-Modul durch}$$

$$\left. \begin{aligned} (\varphi_1 + \varphi_2)(x) &:= \varphi_1(x) + \varphi_2(x) \\ (a\varphi)(x) &:= a\varphi(x) \end{aligned} \right\} \forall \varphi_1, \varphi_2 \in \text{Hom}_R(M, M'), a \in R, x \in M$$

(d) Die R -Moduln bilden mit den R -linearen Abbildungen eine Kategorie

(e) Die Kategorien \mathbb{Z} -**Mod.** und **Abelsche Gruppen** sind isomorph. denn:

$$\dots \varphi(nx) = \varphi(x + \dots + x) = \varphi(x) + \dots + \varphi(x) = n\varphi(x)$$

($\varphi : A \rightarrow A'$ Gruppenhomomorphismus, $x \in A, n \in \mathbb{N}$) \Rightarrow Jeder Gruppenhomomorphismus von abelschen Gruppen ist \mathbb{Z} -linear.

Definition + Bemerkung 2.8.2

Sei M ein R -Modul.

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

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

(c) Sei $U \subseteq M$ Untermodul.

Dann wird M/U zu einem R -Modul durch $a\bar{x} := \overline{ax}$ (denn: Ist $x' \in \bar{x}$, also $x - x' \in U$, so ist $ax' - ax = a(x' - x) \in U$)

Die Restklassenabbildung $p : M \rightarrow M/U, x \mapsto \bar{x}$ ist dann R -linear ($p(ax) = \overline{ax} = a\bar{x} = ap(x)$)

Definition + Bemerkung 2.8.3 (a) Für $X \subseteq M$ heißt

$$\langle X \rangle := \bigcap_{\substack{U \text{ Untermodul von } M \\ X \subseteq U}} U$$

der von X erzeugte Untermodul.

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

(c) Eine Teilmenge $B \subseteq M$ heißt **linear unabhängig**, wenn $0 = \sum_{b \in B} a_b b$ mit $a_b \in R$

(wobei $a_b = 0$ für alle bis auf endlich viele $b \in B$ gelten soll, damit die Summe $\sum_{b \in B} a_b b$ wohldefiniert ist) nur möglich ist mit $a_i = 0 \forall i$.

(d) Eine Teilmenge $B \subseteq M$ heißt **Basis**, wenn jedes $x \in M$ eindeutig als Linearkombination $0 = \sum_{b \in B} a_b b$ mit $a_b \in R$ (wobei $a_b = 0$ für alle bis auf endlich viele $b \in B$ gelten soll) darstellbar ist.

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

(e) M heißt **frei**(er R -Modul), wenn M eine Basis besitzt.

Beispiel:

- (1) R ist freier R -Modul mit Basis 1 (oder einer anderen Einheit)
- (2) Für jedes $n \in \mathbb{N}$ ist $R^n = R \oplus \cdots \oplus R$ freier R -Modul mit Basis e_1, \dots, e_n , $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ (hier steht die 1 an der i -ten Stelle).
- (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 $\bar{x} \in M$, $a \in I \setminus \{0\} \Rightarrow a\bar{x} = \overline{ax} = \bar{0} \Rightarrow$ in M gibt es kein linear unabhängiges Element (oder, um formal zu sein, keine linear unabhängige einelementige Teilmenge).

3 Algebraische Körpererweiterungen

3.1 Algebraische und transzendente Elemente

Definition 3.1.1

Sei L ein Körper, $K \subset L$ 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 über K ist.
- (f) L/K heißt **algebraische Körpererweiterung**, wenn jedes $\alpha \in L$ algebraisch über K ist.

Beispiel:

- (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 $X^4 - 10X^2 + 1$, i ist Nullstelle von $X^2 + 1$.

Klassische Frage: Hat jedes $f \in \mathbb{Q}[X]$ eine Nullstelle, die ein „Wurzelausdruck“ ist?.
- (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. Da \mathbb{Q} abzählbar ist, ist auch $\mathbb{Q}[X]$ abzählbar, da jedes $f \in \mathbb{Q}[X]$ endlich viele Nullstellen hat. Das heißt, es gibt nur abzählbar viele Elemente in \mathbb{R} , die algebraisch über \mathbb{Q} sind. \mathbb{R} ist aber nicht abzählbar.

Definition + Bemerkung 3.1.2

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

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

3 Algebraische Körpererweiterungen

Beweis: $\text{Kern}(\varphi_\alpha)$ ist Ideal, da φ_α Homomorphismus ist. Seien nun $f, g \in K[X]$ mit $f, g \in \text{Kern}(\varphi_\alpha) \Rightarrow (fg)(\alpha) = f(\alpha)g(\alpha) = 0 \stackrel{L \text{ Körper}}{\Rightarrow} f(\alpha) = 0$ oder $g(\alpha) = 0$ ■

- (b) α algebraisch genau dann, wenn φ_α nicht injektiv ist.
- (c) Ist α algebraisch über K , so gibt es ein eindeutig bestimmtes, irreduzibles und normiertes Polynom $f_\alpha \in K[X]$ mit $f_\alpha(\alpha) = 0$ und $\text{Kern}(\varphi_\alpha) = (f_\alpha)$. f_α heißt **Minimalpolynom** von α .

Beweis: $K[X]$ ist Hauptidealring $\Rightarrow \exists \tilde{f}_\alpha$ mit $\text{Kern}(\varphi_\alpha) = (\tilde{f}_\alpha)$. Wegen (a) ist \tilde{f}_α irreduzibel, eindeutig bis auf Einheit in $K[X]$, also ein Element aus $K^\times \Rightarrow \exists! \lambda \in K^\times$, so dass $\lambda \tilde{f}_\alpha = f_\alpha$ normiert ist. ■

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

Beweis: α ist transzendent $\Rightarrow \text{Kern}(\varphi_\alpha) = \{0\} \Rightarrow \varphi_\alpha$ injektiv ■

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

Beweis: Nach Homomorphiesatz ist $K[\alpha] \cong K[X]/\text{Kern}(\varphi_\alpha)$. $\text{Kern}(\varphi_\alpha)$ ist maximales Ideal, da Primideal $\neq (0)$ in $K[X]$ (siehe Bew. Satz 8, Beh. 2) $\Rightarrow K[\alpha]$ ist Körper.
 $f_\alpha(\alpha) = 0$, also $\alpha^n + c_{n-1}\alpha^{n-1} + \dots + c_1\alpha + c_0 = 0$ mit $c_i \in K$, $c_0 \neq 0$ (da f_α irreduzibel), $\alpha(\alpha^{n-1} + \dots + c_1) = -c_0$. Ebenso: $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ ist K -Basis von $K[\alpha]$, denn ist $\sum_{i=0}^{n-1} c_i \alpha^i = 0$ mit $c_i \in K$, so ist $\sum_{i=0}^n c_i X^i \in \text{Kern} \varphi_\alpha$, also sind alle $c_i = 0$, also sind $1, \alpha, \dots, \alpha^{n-1}$ linear unabhängig. Sei $g(\alpha) \in K[\alpha]$ für ein $g \in K[X]$, und schreibe $g = q \cdot f_\alpha + r$ mit $\text{Grad}(r) < n$. Also ist $g(\alpha) = r(\alpha)$ und $r = \sum_{i=0}^{n-1} c_i X^i$, also erzeugen $1, \alpha, \dots, \alpha^{n-1}$ ganz $R[\alpha]$. ■

Definition 3.1.3

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

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

(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 $L = K(\alpha_1, \dots, \alpha_n)$

Bemerkung 3.1.4

Sind M/L und L/K endlich, so auch M/K und es gilt $[M : K] = [M : L] \cdot [L : K]$

Beweis: Sei b_1, \dots, b_m K -Basis von L und e_1, \dots, e_n L -Basis von $M \Rightarrow B = \{e_i b_j : i = 1, \dots, n; j = 1, \dots, m\}$ ist K -Basis von M .

denn: B erzeugt M : Sei $\alpha \in M$, $\alpha = \sum_{i=1}^n \lambda_i e_i$ mit $\lambda_i \in L$, $\lambda_i = \sum_{j=1}^m \mu_{ij} b_j$ einsetzen \Rightarrow

Behauptung.

B linear unabhängig:

Ist $\sum \mu_{ij} e_i b_j = 0$, so ist für jedes feste $i : \sum_{j=1}^m \mu_{ij} b_j = 0$, da e_i über L linear unabhängig sind. Da die b_j linear unabhängig sind, sind die $\mu_{ij} = 0$ ■

Notation: L/K Körpererweiterung, $\alpha \in L$, $K[\alpha] = \text{Bild}(\varphi_\alpha) = \dots$
 $K(\alpha) = \text{Quot}(K[\alpha]) = K[\alpha]$, falls α algebraisch.

Bemerkung 3.1.5

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) \Rightarrow (ii) Jede K -Basis in L ist auch Erzeugendensystem von L/K . Ist $\alpha \in L$ transzendent über K , so ist $K[\alpha] \cong K[X]$ ein unendlichdimensionaler K -Vektorraum in L , Widerspruch. Also sind alle Elemente in L algebraisch.

(ii) \Rightarrow (iii) ✓

(iii) \Rightarrow (i) Induktion über die Anzahl n der Erzeuger:

$n = 1$: $[K(\alpha) : K] = \text{Grad}(f_\alpha)$ nach 3.1.2 (f).

$n > 1$: $K(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$, $K' := K(\alpha_1, \dots, \alpha_{n-1})/K$ ist endlich nach Induktionsvoraussetzung und L/K' ist endlich nach Fall 1, also folgt aus 3.1.4 L/K ist endlich.

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

denn:

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

$e^{\frac{2\pi i}{n}}$ ist Nullstelle von $X^n - 1$, also algebraisch (über \mathbb{Q}) $\Rightarrow K = \mathbb{Q} \left(e^{\frac{2\pi i}{n}} \right)$ ist endliche Körpererweiterung von \mathbb{Q} , $\cos \frac{2\pi}{n} \in K \stackrel{3.5(i) \Rightarrow (ii)}{\Rightarrow} \cos \frac{2\pi}{n}$ ist algebraisch.

$$\mathbb{Q} \subset \mathbb{Q} \left(\cos \frac{2\pi}{n} \right) \subsetneq K \quad (n \geq 3)$$

Bemerkung 3.1.6

Seien $K \subset L \subset M$ Körper. Sind M/L und L/K algebraisch, so auch M/K

Beweis: 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' ist endlich erzeugt über $K \stackrel{3.1.5}{\Rightarrow} L'/K$ endlich. Außerdem ist $L'(\alpha)/L'$ endlich. $\stackrel{(b)}{\Rightarrow} L'(\alpha)/K$ endlich $\Rightarrow \alpha$ algebraisch über K . ■

3.2 Algebraischer Abschluss

Proposition 3.2.1 (Kronecker)

Sei K Körper, $f \in K[X]$, f nicht konstant.

Es gibt eine endliche Körpererweiterung L/K , so dass f in L eine Nullstelle hat. Genauer: $[L : K] \leq \text{Grad } f$.

Beweis: $\mathbb{C}f$ irreduzibel. Setze $L := K[X]/(f)$. L ist Körper, da (f) maximales Ideal ist. $\alpha = \bar{X} =$ Klasse von X in L ist Nullstelle von f . Genauer: f ist das Minimalpolynom von α . ■

Bemerkung 3.2.2

Ist $f \in K[X] \setminus \{0\}$ und $\alpha \in K$ mit $f(\alpha) = 0$, dann ist $X - \alpha$ ein Teiler von f .

Beweis: $\{f \in K[X] : f(\alpha) = 0\}$ ist ein Ideal im Hauptidealring $K[X]$ und $X - \alpha$ sein Erzeuger. ■

Bemerkung + Definition 3.2.3

Sei K Körper, $f \in K[X] \setminus K$

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

Beweis: Induktion über $n = \deg(f)$:

$$n = 1 \quad \checkmark$$

$n \geq 1$ L_1 wie in Proposition 3.2.1. Dann ist $f(X) = (X - \alpha) \cdot f_1(X)$ in $L_1[X]$, $\deg(f_1) = n - 1$. Also gibt es L_2/L_1 , so dass $f_1(X) = \prod_{i=1}^{n-1} (X - \alpha_i)$ mit $\alpha_i \in L_2$. Dabei ist L_2/L_1 endlich, L_1/K endlich, also L_2/K endlich. ■

- (b) L/K heißt **Zerfällungskörper** von f , wenn f über L in Linearfaktoren zerfällt, und L über K von den Nullstellen von f erzeugt wird.
- (c) Es gibt einen Zerfällungskörper $Z(f)$.

Beweis: Induktion über den Grad und die Anzahl über die irreduziblen Faktoren:

⊆ Sei f irreduzibel. Sei $L_1 := K[X]/(f)$ und $\alpha := \bar{X} \in L$. Dann ist $L_1 = K(\alpha)$ und $f = (X - \alpha) \cdot g$ in $L_1[X]$. Nach Induktionsvoraussetzung gibt es einen Zerfällungskörper $Z(g)$ von g über L_1 , also wird $Z(g)$ über K von α und den Nullstellen von g erzeugt. ■

- (d) Ist f irreduzibel und $n = \deg(f)$, so ist $[Z(f) : K] \leq n!$

Beweis: In Proposition 3.2.1 ist $[L : K] = n = \deg(f)$ und $f = (X - \alpha) \cdot f_1$ mit $\deg(f_1) = n - 1$. Mit Induktion folgt die Behauptung. ■

Beispiel:

- (1) $f \in K[X]$ irreduzibel vom 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 $\mathbb{Q}(\alpha) \subset \mathbb{R}$

$$X^3 - 2 = (X - \alpha) \underbrace{(X^2 + \alpha X + \alpha^2)}_{\text{irreduzibel über } \mathbb{Q}(\alpha)} \Rightarrow [Z(f) : \mathbb{Q}] = 6$$

$$(3) \quad K = \mathbb{Q}, \quad p \text{ Primzahl}, \quad f(X) = X^p - 1 = (X - 1) \underbrace{(X^{p-1} + X^{p-2} + \dots + X + 1)}_{f_1}$$

f_1 irreduzibel (siehe 2.6.3).

$$L := \mathbb{Q}[X]/(f_1) =: \mathbb{Q}(\zeta_p); \quad (\zeta_p^k)^p = \zeta_p^{pk} = 1; \quad k = 1, \dots, p-1$$

$$\Rightarrow \mathbb{Q}(\zeta_p) = Z(f)$$

Definition + Bemerkung 3.2.4

Sei K ein Körper.

- (a) K heißt **algebraisch abgeschlossen**, wenn jedes nichtkonstante Polynom $f \in K[X]$ in K eine Nullstelle hat.
- (b) Die folgenden Aussagen sind äquivalent:
 - (i) K ist algebraisch abgeschlossen
 - (ii) Jedes $f \in K[X] \setminus K$ zerfällt über K in Linearfaktoren
 - (iii) K besitzt keine echte algebraische Körpererweiterung.

Beweis:

(i) \Rightarrow (ii) Induktion über den Grad von f .

(ii) \Rightarrow (iii) Angenommen L/K algebraisch, $\alpha \in L \setminus K$. Dann sei $f_\alpha \in K[X]$ das Minimalpolynom von α ; f_α ist irreduzibel und zerfällt in Linearfaktoren $\Rightarrow \deg(f) = 1 \nmid$

(iii) \Rightarrow (ii) Sei $f \in K[X]$ irreduzibel, $L := K[X]/(f)$, dann folgt aus der Voraussetzung $L = K$ und damit $\text{Grad } f = 1$. ■

Satz 11

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

Beweis:

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

Dann: sei $K'' := (K')'$ und weiter $K^i := (K^{i-1})'$, $i \geq 3$; Es ist $K^i \subset K^{i+1}$.

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

3.3 Fortsetzung von Körperhomomorphismen

- (i) L ist Körper: $a + b \in L$ für $a \in K^i, b \in K^j$, da $\mathbb{C}: i \leq j \Rightarrow a$ auch in K^j
- (ii) L ist algebraisch über K : jedes $\alpha \in L$ liegt in einem K^i , K^i 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 $i = 0, \dots, n \Rightarrow f$ hat Nullstelle in $(K^j)' = K^{j+1} \subset L \Rightarrow$ Behauptung

Bew. (Hauptschritt): Für jedes $f \in K[X] \setminus K$ sei X_f ein Symbol. $\mathcal{X} := \{X_f : f \in K[X] \setminus K\}$, $R := K[\mathcal{X}]$, I sei das von allen $f(X_f)$ in R erzeugte Ideal.

Behauptung: $I \neq R$.

Dann gibt es ein maximales Ideal $\mathfrak{m} \subset R$ mit $I \subset \mathfrak{m}$, $K' := R/\mathfrak{m}$, K' ist Körper, K'/K ist algebraisch,

denn: K' wird über K erzeugt von den $\bar{X}_f \in \mathcal{X}$ und $f(\bar{X}_f) = 0$ in K' , weil $f(\bar{X}_f) \in I \subset \mathfrak{m}$. f hat in K' die Nullstellen (Klasse von) \bar{X}_f .

Beweis der Behauptung Angenommen $I = R$, also $1 \in I$. Dann gibt es $n \geq 1, f_1, \dots, f_n \in K[X] \setminus K$ 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 $f_1 \cdot \dots \cdot f_n$).

Setze nun α_i für X_{f_i} ein ($i = 1, \dots, n$) (und 42 für alle anderen X_f). Dann ist $1 = \sum_{i=1}^n g_i(\alpha_1, \dots, \alpha_n, 42, \dots) \cdot \underbrace{f_i(\alpha_i)}_{=0} = 0 \neq 1$ ■

3.3 Fortsetzung von Körperhomomorphismen

Sei $f(x) = x^2 - 2$, $K = \mathbb{Q}$, $L = \mathbb{Q}[X]/(f)$ und $\alpha = \bar{X}$, also $f(\alpha) = 0$. Es gibt zwei Einbettungen von L in \mathbb{R} : Schreibe $x \in L$ als $x = a + b\alpha$ mit $a, b \in \mathbb{Q}$ (dies ist eindeutig), dann sind $\varphi_1(x) := a + b\sqrt{2}$ und $\varphi_2(x) := a - b\sqrt{2}$ Homomorphismen $L \rightarrow \mathbb{R}$.

Proposition 3.3.1

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 $\sigma : K \rightarrow K'$ ein Körperhomomorphismus. Sei f^σ das Bild von f in $K'[X]$ unter dem Homomorphismus $K[X] \rightarrow K'[X]$, $\sum a_i X^i \mapsto \sum \sigma(a_i) X^i$. Dann gilt:

- (a) Ein Homomorphismus $\tilde{\sigma} : L \rightarrow K'$ heißt **Fortsetzung** von σ , wenn $\tilde{\sigma}(a) = \sigma(a)$ für alle $a \in K$ gilt.

3 Algebraische Körpererweiterungen

- (b) Ist $\tilde{\sigma} : L \rightarrow K'$ Fortsetzung von σ , so ist $\tilde{\sigma}(\alpha)$ Nullstelle von f^σ .
- (c) Zu jeder Nullstelle β von f^σ in K' gibt es genau eine Fortsetzung $\tilde{\sigma} : L \rightarrow K'$ von σ mit $\tilde{\sigma}(\alpha) = \beta$.

Beweis:

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

(c) Eindeutigkeit: \checkmark $\tilde{\sigma}$ ist auf den Erzeugern von L festgelegt.

Existenz:

$$\varphi : K[X] \rightarrow K', \quad X \mapsto \beta$$

$$\sum_{=g} a_i X^i \mapsto \sum \sigma(a_i) \beta^i = g^\sigma(\beta)$$

$$\Rightarrow \varphi(f) = f^\sigma(\beta) \stackrel{\text{Hom.satz}}{\Rightarrow} \varphi \text{ induziert } \tilde{\sigma} : \underset{=L}{K[X]/(f)} \rightarrow K' \quad \blacksquare$$

Folgerung 3.3.2

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

Beweis: Seien L, L' Zerfällungskörper, $L = K(\alpha_1, \dots, \alpha_n)$, α_i die Nullstelle von f . Sei weiter $\beta_1 \in L'$ Nullstelle von f . Nach 3.3.1 gibt es $\sigma : K(\alpha_1) \rightarrow L'$ mit $\sigma|_K = \text{id}_K$ und $\sigma(\alpha_1) = \beta_1$ und $\tau : K(\beta_1) \rightarrow L$ mit $\tau(\beta_1) = \alpha_1$ und $\tau|_K = \text{id}_K$.

$$\tau \circ \sigma = \text{id}_{K(\alpha_1)}, \quad \sigma \circ \tau = \text{id}_{K(\beta_1)} \Rightarrow K(\alpha_1) \cong K(\beta_1)$$

Mit Induktion über n folgt die Behauptung. \blacksquare

Bemerkung 3.3.3

Sei L/K algebraische Körpererweiterung, \bar{K} ein algebraisch abgeschlossener Körper. $\sigma : K \rightarrow \bar{K}$ ein Homomorphismus. Dann gibt es eine Fortsetzung $\tilde{\sigma} : L \rightarrow \bar{K}$.

Beweis: Ist L/K endlich, so folgt die Aussage aus 3.3.1. Für den allgemeinen Fall sei $\mathcal{M} := \{(L', \tau) : L'/K \text{ Körpererw.}, L' \subseteq L, \tau : L' \rightarrow \bar{K} \text{ Fortsetzung von } \sigma\}$, $\mathcal{M} \neq \emptyset$: $(K, \sigma) \in \mathcal{M}$

\mathcal{M} ist geordnet durch $(L_1, \tau_1) \subseteq (L_2, \tau_2) :\Leftrightarrow L_1 \subseteq L_2$ und τ_2 Fortsetzung von τ_1 . Sei $\mathcal{N} \subset \mathcal{M}$ totalgeordnet $\tilde{L} := \bigcup_{(L', \tau) \in \mathcal{N}} L'$.

\tilde{L} ist Körper, $\tilde{L} \subseteq L$, $\tilde{\tau} : \tilde{L} \rightarrow \bar{K}$, $\tilde{\tau}(x) = \tau(x)$, falls $x \in L'$ und $(L', \tau) \in \mathcal{N}$.

Wohldefiniert: ist $x \in L''$, so ist $\mathbb{C}(L', \tau) \subseteq (L'', \tau'')$ und damit $\tau''(x) = \tau(x)$.
 $\Rightarrow (\tilde{L}, \tilde{\tau})$ ist obere Schranke $\xrightarrow{\text{Zorn}} \mathcal{M}$ hat maximales Element $(\tilde{L}, \tilde{\sigma})$

Zu zeigen: $\tilde{L} = L$. Sonst sei $\alpha \in L \setminus \tilde{L}$ und σ' Fortsetzung von $\tilde{\sigma}$ auf $\tilde{L}(\alpha)$ (nach 3.3.1)
 $\Rightarrow (\tilde{L}(\alpha), \sigma') \in \mathcal{M}$ und $(\tilde{L}, \tilde{\sigma}) \subsetneq (\tilde{L}(\alpha), \sigma') \nmid$ ■

Folgerung 3.3.4

Für jeden Körper K ist der algebraische Abschluss \bar{K} bis auf Isomorphie eindeutig bestimmt.

Beweis: Seien \bar{K} und C algebraische Abschlüsse von K . Nach Proposition 3.3.3 gibt es $\xrightarrow{\bar{K}} \xrightarrow{\text{id}_K} \xrightarrow{C}$

Körperhomomorphismus $\sigma : \bar{K} \rightarrow C$, der id_K fortsetzt. Dann ist $\sigma(\bar{K})$ auch algebraisch abgeschlossen: ist $f = \sum_{i=0}^n a_i X^i \in \sigma(\bar{K})[X] \Rightarrow f^{\sigma^{-1}} = \sum_{i=0}^n \sigma^{-1}(a_i) X^i \in \bar{K}[X]$ hat Nullstelle $\alpha \in \bar{K}$.
 $\Rightarrow \sigma(\alpha)$ ist Nullstelle von f :

$$\sum \sigma^{-1}(a_i) \alpha^i = 0 \Rightarrow 0 = \sigma(\sum \sigma^{-1}(a_i) \alpha^i) = \sum a_i \sigma(\alpha^i) = \sum a_i \sigma(\alpha)^i$$

C ist algebraisch über K , also erst recht über $\sigma(\bar{K}) \xrightarrow{3.2.4} \sigma(\bar{K}) = C$ ■

Definition + Bemerkung 3.3.5

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

(a)

$$\text{Hom}_K(L, L') := \{ \sigma : L \rightarrow L' \text{ Körperhomomorphismus, } \sigma|_K = \text{id}_K \}$$

$$\text{Aut}_K(L) := \{ \sigma : L \rightarrow L \text{ Körperautomorphismus, } \sigma|_K = \text{id}_K \}$$

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

Beweis: Sei $L = K(\alpha_1, \dots, \alpha_n)$, α_i algebraisch über K . Induktion über n :

$n = 1$ Sei $f \in K[X]$ das Minimalpolynom von α_1 . Für jedes $\sigma \in \text{Hom}_K(L, \bar{K})$ ist $\sigma(\alpha_1)$ Nullstelle von $f^\sigma \in \bar{K}[X]$. Durch $\sigma|_K = \text{id}_K$ und $\sigma(\alpha_1)$ ist σ eindeutig bestimmt. $\Rightarrow |\text{Hom}_K(L, \bar{K})| = |\text{Nullstellen von } f^\sigma| \leq \deg(f^\sigma) = [L : K]$

$n > 1$ Sei $L_1 = K(\alpha_1, \dots, \alpha_{n-1})$, $f \in L_1[X]$ das Minimalpolynom von α_n über L_1 . Für $\sigma \in \text{Hom}_K(L, \bar{K})$ ist $\sigma(\alpha_n)$ Nullstelle von $f^{\sigma|_{L_1}} \in \bar{K}[X]$ mit $\sigma|_{L_1} = \sigma|_{L_1} \Rightarrow |\text{Hom}_K(L, \bar{K})| \leq |\text{Hom}_K(L_1, \bar{K})| \cdot \deg(f) \stackrel{\text{IV}}{\leq} [L_1 : K] \cdot [L : L_1] \stackrel{3.1.6(b)}{=} [L : K]$ ■

3.4 Separable Körpererweiterungen

Definition + Bemerkung 3.4.1

Sei L/K algebraische Körpererweiterung und \bar{K} algebraischer Abschluss von K .

- (a) $f \in K[X]$ heißt **separabel**, wenn f in \bar{K} keine mehrfache Nullstelle hat (also $\text{deg}(f)$ 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 separabel, wenn $\text{ggT}(f, f') = 1$. Dabei ist für $f = \sum_{i=0}^n a_i X^i$ die **Ableitung** definiert durch $f' := \sum_{i=1}^n i a_i X^{i-1}$

Beweis: Sei $f(X) = \prod_{i=1}^n (X - \alpha_i)$, $\alpha_i \in \bar{K} \Rightarrow f'(X) = \sum_{i=1}^n \prod_{j \neq i} (X - \alpha_j)$ nach Definition ist f separabel $\Leftrightarrow \alpha_i \neq \alpha_j$ für $i \neq j$.

Beh.: $\alpha_1 = \alpha_i$ für ein $i \geq 2 \Leftrightarrow (X - \alpha_1) \mid f'$

Aus der Behauptung folgt: f separabel $\Leftrightarrow f$ und f' teilerfremd in $\bar{K}[X]$. Ist das so, dann ist $\text{ggT}(f, f') = 1$ (teilerfremd in $K[X]$). Ist umgekehrt $\text{ggT}(f, f') = 1$, so gibt es $g, h \in K[X]$ mit $1 = gf + hf'$.

Das stimmt dann auch in $\bar{K}[X]$, also sind f und f' in $\bar{K}[X]$ teilerfremd.

Bew. der Beh.: $(X - \alpha_1)$ teilt $\prod_{j \neq 1} (X - \alpha_j)$, falls $i \neq 1$. Also gilt $X - \alpha_1$ teilt $f' \Leftrightarrow X - \alpha_1$ Teiler von $\prod_{j \neq 1} (X - \alpha_j) \Leftrightarrow \alpha_1 = \alpha_j$ für ein $j \neq 1$. ■

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

Beweis: Ist $f' = 0$, so ist $\text{ggT}(f, f') = f \neq 1$

Ist $f' \neq 0$, so ist $\text{deg } f' < \text{deg } f$; ist f irreduzibel und $\alpha \in \bar{K}$ Nullstelle von f , so ist f das Minimalpolynom von $\alpha \stackrel{f' \neq 0}{\Rightarrow} \alpha$ nicht Nullstelle von $f' \Rightarrow \text{ggT}(f, f') = 1$ ■

Folgerung 3.4.2

Ist $\text{char}(K) = 0$, so ist jede algebraische Körpererweiterung separabel.

Beispiele 3.4.3

Sei p Primzahl, $K = \mathbb{F}_p(t) = \text{Quot}(\mathbb{F}_p[t])$. Sei $f(X) = X^p - t \in K[X]$.

$f'(X) = pX^{p-1} = 0$, $t \in \mathbb{F}_p[t]$ ist Primelement $\xrightarrow{\text{Eisenstein}} f$ irreduzibel in $(\mathbb{F}_p[t])[X] \xrightarrow{??} f$ irreduzibel in $K[X]$

$f(X) = X^p - a \in \mathbb{F}_p \Rightarrow f' = 0$, f ist nicht irreduzibel, da f Nullstelle in \mathbb{F}_p hat, dh. es gibt ein $b \in \mathbb{F}_p$ mit $b^p = a$.

Denn: $\varphi : \mathbb{F}_p \rightarrow \mathbb{F}_p, b \mapsto b^p$ ist Körperhomomorphismus! (denn $(a + b)^p = a^p + b^p$)

Proposition 3.4.4

Sei $\text{char}(K) = p > 0$, $f \in K[X]$ irreduzibel, \bar{K} ein algebraischer Abschluss von K .

- (a) Es gibt ein separables irreduzibles Polynom $g \in K[X]$, so dass $f(X) = g(X^{p^r})$ für ein $r \geq 0$.
- (b) Jede Nullstelle von f in \bar{K} hat Vielfachheit p^r .

Beweis: Sei f nicht separabel, $f = \sum_{i=0}^n a_i X^i$, $f' = \sum_{i=1}^n i a_i X^{i-1} = 0 \Rightarrow i a_i = 0$ für $i = 1, \dots, n \Rightarrow a_i = 0$, falls i nicht durch p teilbar $\Rightarrow f$ ist Polynom in X^p , dh. $f = g_1(X^p)$. Mit Induktion folgt die Behauptung. ■

Proposition + Definition 3.4.5

Sei L/K endliche Körpererweiterung, \bar{K} algebraischer Abschluss von L .

- (a) $[L : K]_s := |\text{Hom}_K(L, \bar{K})|$ 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 $\Leftrightarrow [L : K] = [L : K]_s$
- (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 $\text{Hom}_K(L', \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$, $\text{Hom}_{L'}(L, \bar{K}) = \{\tau_1, \dots, \tau_m\}$. Sei $\tilde{\sigma}_i : \bar{K} \rightarrow \bar{K}$ Fortsetzung von σ_i , $i = 1, \dots, n$. Dann ist $\tilde{\sigma}_i \in \text{Aut}_K(\bar{K})$.

Beh.:

(1) $\text{Hom}_K(L, \bar{K}) = \{\tilde{\sigma}_i \circ \tau_j : i = 1, \dots, n, j = 1, \dots, m\}$

(2) $\tilde{\sigma}_i \circ \tau_j = \tilde{\sigma}_{i'} \circ \tau_{j'} \Leftrightarrow i = i'$ und $j = j'$.

Aus (1) und (2) folgt (b).

Bew.(1): " \supseteq " ✓ " \subseteq ": Sei $\sigma \in \text{Hom}_K(L, \bar{K})$. Dann gibt es ein i mit $\sigma|_{L'} = \sigma_i \Rightarrow \tilde{\sigma}_i^{-1} \circ \sigma|_{L'} = \text{id}_{L'} \Rightarrow \exists j$ mit $\tilde{\sigma}_i^{-1} \circ \sigma = \tau_j \Rightarrow \sigma = \tilde{\sigma}_i \circ \tau_j$.

Bew.(2): Sei $\tilde{\sigma}_i \circ \tau_j = \tilde{\sigma}_{i'} \circ \tau_{j'} \Rightarrow \underbrace{\tilde{\sigma}_i|_{L'}}_{=\sigma_i} = \underbrace{\tilde{\sigma}_{i'}|_{L'}}_{=\sigma_{i'}} \Rightarrow i = i' \Rightarrow \tau_j = \tau_{j'} \Rightarrow j = j'$.

(c) " \Rightarrow ": Sei $L = K(\alpha_1, \dots, \alpha_n)$. Induktion über n :

n=1 $L = K(\alpha)$, $f = f_\alpha \in K[X]$ das Minimalpolynom von α über $K \Rightarrow [L : K]_s \stackrel{3.3.5}{=} |\{\text{Nullstellen von } f \text{ in } \bar{K}\}| = \deg f = [L : K]$.

n>1 $L_1 := K(\alpha_1, \dots, \alpha_{n-1})$, $f \in L_1[X]$ das Minimalpolynom von α_n . Zu jedem $\sigma_1 \in \text{Hom}_K(L_1, \bar{K})$ und jeder Nullstelle von f in \bar{K} gibt es genau eine Fortsetzung $\tilde{\sigma}_1 : L \rightarrow \bar{K}$.

$$\begin{aligned} f \text{ separabel} &\Rightarrow [L : K]_s = |\text{Hom}_K(L, \bar{K})| = \deg(f) \cdot |\text{Hom}_K(L_1, \bar{K})| = [L : L_1] \cdot \\ & [L_1 : K]_s \stackrel{IV}{=} [L : L_1] \cdot [L_1 : K] = [L : K]. \end{aligned}$$

" \Leftarrow ": Ist $\text{char}(K) = 0$, so ist L/K separabel. Sei also $\text{char}(K) = p > 0$ und $\alpha \in L$; $f \in K[X]$ das Minimalpolynom von α . Nach 3.4.4 gibt es $r \geq 0$ und ein separables, irreduzibles Polynom $g \in K[X]$ mit $f(X) = g(X^{p^r}) \Rightarrow [K(\alpha) : K]_s = |\{\text{Nullstellen von } g \text{ in } \bar{K}\}| \stackrel{g \text{ separabel}}{=} \deg(g) \cdot (*) \Rightarrow [K(\alpha) : K] = \deg(f) = p^r \cdot \deg(g) = p^r \cdot [K(\alpha) : K]_s \Rightarrow [L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] \geq [L : K(\alpha)]_s \cdot p^r [K(\alpha) : K]_s \stackrel{(b)}{=} [L : K]_s \stackrel{\text{Voraussetzung}}{\Rightarrow} p^r = 1 \Rightarrow g = f \Rightarrow \alpha \text{ separabel.}$

(d) folgt aus (*) ■

Satz 12 (Satz vom primitiven Element)

Jede endliche separable Körpererweiterung L/K ist einfach, also gibt es $\alpha \in L$ mit $L = K(\alpha)$. α heißt **primitives Element**.

Beweis: Ist K endlich, so folgt aus 3.5.1, dass L^\times zyklische Gruppe ist. Ist $L^\times = \langle \alpha \rangle$, so ist $L = K[\alpha]$.

Sei also K unendlich, $L = K(\alpha_1, \dots, \alpha_r)$. $\exists \epsilon: r = 2$, also $L = K(\alpha, \beta)$. Sei \bar{K} algebraischer Abschluss von L , $[L : K] = n$. Sei $\text{Hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$ (3.4.5(c)).

Sei $g(X) := \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha) + (\sigma_i(\beta) - \sigma_j(\beta))X) \in \bar{K}[X]$, $g \neq 0$, 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 $g(\lambda) \neq 0$.

Beh.: $\gamma := \alpha + \lambda\beta \in L$ erzeugt L über K .

denn: Sei $f \in K[X]$ das Minimalpolynom von γ über K . Für jedes i ist $f(\sigma_i(\gamma)) \stackrel{\sigma_i|_K = \text{id}_K}{=} \sigma_i(f(\gamma))$. Angenommen, $\sigma_i(\gamma) = \sigma_j(\gamma)$ für ein $i \neq j$. Dann wäre $(\sigma_i(\alpha) + \sigma_i(\beta)\lambda) - (\sigma_j(\alpha) + \sigma_j(\beta)\lambda) = 0 \Rightarrow g(\lambda) = 0 \stackrel{!}{\neq} \Rightarrow f$ hat mindestens n Nullstellen $\Rightarrow \deg(f) = [K(\gamma) : K] \geq n = [L : K]$, da $\gamma \in L$, folgt $K(\gamma) = L$. ■

3.5 Endliche Körper

Proposition 3.5.1

Ist K ein Körper, so ist jede endliche Untergruppe von (K^\times, \cdot) zyklisch.

Beweis: Sei $G \subseteq K^\times$ endliche Untergruppe, $a \in G$ ein Element maximaler Ordnung. Sei $n = \text{ord}(a)$, $G_n := \{b \in G : \text{ord}(b) \mid n\}$.

Beh.: $G_n = \langle a \rangle$

denn: jedes $b \in G_n$ ist Nullstelle von $X^n - 1$. Diese sind $1, a, a^2, \dots, a^{n-1} \Rightarrow |G_n| = |\langle a \rangle| = n$.

Nach Folgerung 1.4.5 ist $G \cong \bigoplus_{i=1}^r \mathbb{Z}/a_i\mathbb{Z}$ mit $a_i \mid a_{i+1} \Rightarrow$ Für jedes $b \in G$ ist $\text{ord}(b)$ Teiler von $a_r = n$. ■

Definition + Bemerkung 3.5.2

Sei K Körper mit Charakteristik $p > 0$.

- (a) Dann ist die Abbildung $\varphi : K \rightarrow K, x \mapsto x^p$ ein Homomorphismus. Er heißt **Frobenius**-Homomorphismus.
- (b) Es ist $\varphi(x) = x \iff x \in \mathbb{F}_p$ (als Primkörper in K).

Satz 13

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 $f'(X) = -1 \Rightarrow \text{ggT}(f, f') = 1 \Rightarrow f$ hat q verschiedene Nullstellen in $\mathbb{F}_q \Rightarrow |\mathbb{F}_q| \geq q$.

Umgekehrt: Jedes $a \in \mathbb{F}_q$ ist Nullstelle von f .

denn: \mathbb{F}_q wird erzeugt von den Nullstellen von f . Sind also 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, \cdot) ist Gruppe der Ordnung $q - 1 \Rightarrow$ Für jedes $a \in K$ gilt $a^q = a \Rightarrow$ Jedes $a \in K$ ist Nullstelle von $X^q - X \Rightarrow K$ liegt im Zerfällungskörper von $X^q - X \Rightarrow K$ enthält \mathbb{F}_q (bis auf Isomorphie).

$$\begin{aligned} |K| = |\mathbb{F}_q| = q \\ \Rightarrow K \cong \mathbb{F}_q \end{aligned}$$

Folgerung 3.5.3

Jede algebraische Erweiterung eines endlichen Körpers ist separabel.

Beweis: $\mathbb{F}_q/\mathbb{F}_p$ separabel, da $X^q - X$ separables 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 $r \geq 1$)

Definition: Ein Körper K heißt **vollkommen** (oder perfekt), wenn jede algebraische Körpererweiterung L/K separabel ist.

3.6 Konstruktion mit Zirkel und Lineal

Aufgabe: Sei $M \subset \mathbb{C} = \mathbb{R}^2$, z.B.: $M = \{0, 1\}$.

Linien: $\mathcal{L}(M) := \{L \subset \mathbb{R}^2 \text{ Gerade: } |L \cap M| \geq 2\} \cup \{K_{z_1-z_2}(z_3) : z_1, z_2, z_3 \in M\}$

$(K_r(z) = \{y \in \mathbb{R}^2 : |z - y| = r\})$

$K_1(M) := \{z \in \mathbb{C} : z \text{ liegt auf zwei verschiedenen Linien in } \mathcal{L}(M)\}$

$K_n(M) := K_1(K_{n-1}(M))$ für $n \geq 2$

$K(M) := \bigcup_{n=1}^{\infty} K_n(M)$

Satz 14

Sei $M \subseteq \mathbb{R}^2$ mit $0, 1 \in M$ und $K(M)$ die Menge der mit Zirkel und Lineal konstruierbaren Punkte.

- (a) $K(M)$ ist ein Teilkörper von \mathbb{C} .
- (b) $K(M)/\mathbb{Q}(M)$ ist eine algebraische Körpererweiterung, dabei sei $\mathbb{Q}(M)$ der kleinste Teilkörper von \mathbb{C} , der \mathbb{Q} und M umfasst und mit a auch \bar{a} enthält.
- (c) Eine komplexe Zahl $a \in \mathbb{C}$ liegt genau dann in $K(M)$, wenn es eine Kette

$$\mathbb{Q}(M) = L_0 \subset L_1 \subset \cdots \subset L_n$$

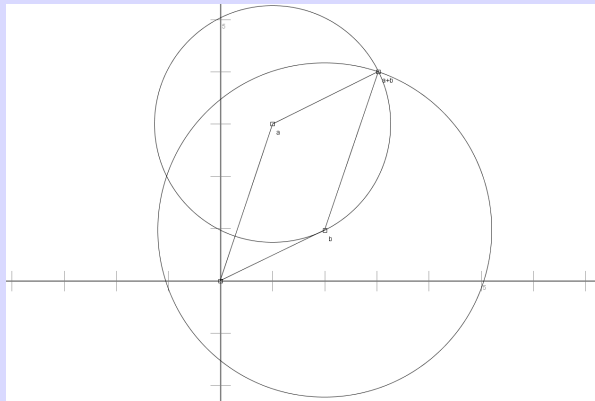
gibt mit $a \in L_n$ und $[L_i : L_{i-1}] = 2$ für $i = 1, \dots, n$.

Beweis:

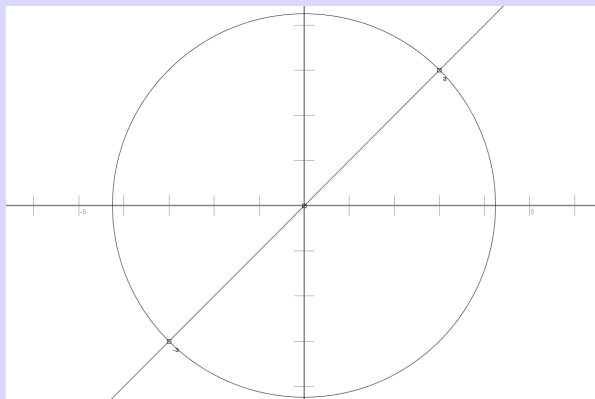
- (a) Seien $a, b \in K(M)$. Zu zeigen: $a + b, -a, a \cdot b, \frac{1}{a} \in K(M)$.

$a + b \in K(M)$:

3.6 Konstruktion mit Zirkel und Lineal



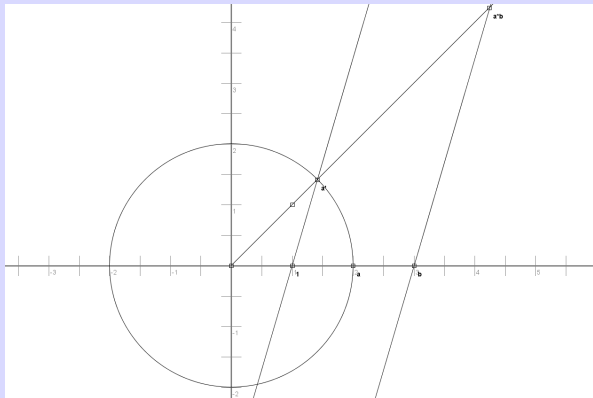
$-a \in K(M)$:



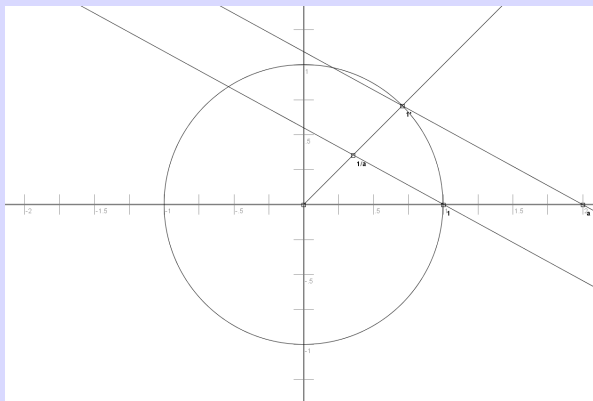
$a \cdot b \in K(M)$:

Strahlensatz: $\frac{1}{a} = \frac{b}{x}$, also $x = a \cdot b$. Winkel addieren $\checkmark \Rightarrow a \cdot b$ allgemein \checkmark

3 Algebraische Körpererweiterungen



$$\frac{1}{a} \in K(M) : \exists a \in \mathbb{R}$$



(b) folgt aus (a)

(c) Zeige mit Induktion über n : Jedes $a \in K_n(M)$ ist algebraisch über $\mathbb{Q}(M)$. Wegen $K_n(M) = K_1(\mathcal{L}_n(M))$ genügt es, die Behauptung für $n = 1$ zu zeigen. Sei also $z \in K_1(M)$.

Vorüberlegung: Für $z \in M$ ist $\Re(z) = \frac{1}{2}(z + \bar{z}) \in \mathbb{Q}(M)$ und $\Im(z) = \frac{1}{2}(z - \bar{z}) \in \mathbb{Q}(M)$.

- a) z ist Schnittpunkt zweier Geraden in $\mathcal{L}(M) \Rightarrow z$ ist Lösung zweier linearer Gleichungen $z_1 + \lambda z_2 = z'_1 + \mu z'_2$
- b) z ist Schnittpunkt einer Geraden und eines Kreises: \Rightarrow quadratische Gleichung mit Koeffizienten in $\mathbb{Q}(M)$

3.6 Konstruktion mit Zirkel und Lineal

c) z ist Schnittpunkt zweier Kreise $K_{r_1}(m_1)$ und $K_{r_2}(m_2)$ mit Mittelpunkten $m_1, m_2 \in M$. Radien: $r_1 = |z_1 - z_1'|$, $r_2 = \dots$ also $r_1^2 = (z_1 - z_1')(\overline{z_1 - z_1'}) \in \mathbb{Q}(M)$.

Dann ist $|z - m_1|^2 = r_1^2$.

$$\Rightarrow z\bar{z} - (z\bar{m}_1 + \bar{z}m_1) = r_1^2 - m_1\bar{m}_1 \text{ und } z\bar{z} - (z\bar{m}_2 + \bar{z}m_2) = r_2^2 - m_2\bar{m}_2 \Rightarrow 2\Re[z(\bar{m}_1 - \bar{m}_2)] = r_1^2 - r_2^2 - (m_1\bar{m}_1 - m_2\bar{m}_2)$$

Das ist eine lineare Gleichung, die $\Re(z)$ und $\Im(z)$ enthält. Einsetzen in (1) ergibt quadratische Gleichung für $\Re(z)$ (mit Koeffizienten in $\mathbb{Q}(M)$).

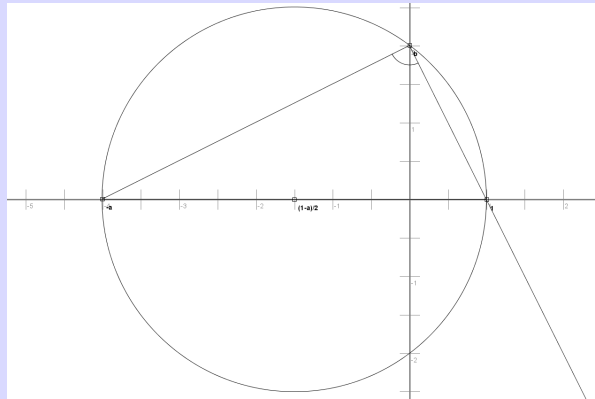
Noch zu zeigen: Ist $a \in \mathbb{C}$ und gibt es eine Kette

$$\mathbb{Q}(M) = L_0 \subset L_1 \subset \dots \subset L_n$$

von Körpererweiterungen mit $[L_i : L_{i-1}] = 2$ und $a \in L_n$, so ist $a \in K(M)$.

Sei also L/K quadratische Erweiterung von Körpern (mit Charakteristik ungleich 2). Dann gibt es $\alpha \in L$ und $a \in K$, so dass $L = K(\alpha)$ und $\alpha^2 = a$, das heißt $L = K(\sqrt{a})$. Zu zeigen ist also: Ist $K \subset K(M)$, so ist $\sqrt{a} \in K(M)$:

Wurzelziehen: $a \in \mathbb{R}$



$\xRightarrow{\text{Thales}}$ Winkel ist rechtwinklig $\xRightarrow{\text{Höhensatz}} b^2 = |-a| \cdot 1 = a$ ■

Beispiel: Das regelmäßige Fünfeck ist aus 0 und 1 konstruierbar. Ziel: Konstruiere Nullstellen von $X^5 - 1 = (X - 1) \cdot f$, $f := X^4 + X^3 + X^2 + X + 1$. Trick von Lagrange: $f(X) = X^2(X^2 + \frac{1}{X^2} + X + \frac{1}{X} + 1)$. Mit $Y := X + \frac{1}{X}$ ist dann $\frac{1}{X^2} \cdot f(X) = Y^2 + Y - 1 =: g(Y)$. Ist y Nullstelle von g und ξ Nullstelle von f , so ist $\mathbb{Q} \subset \mathbb{Q}(y) \subset \mathbb{Q}(\xi)$ eine Kette wie im Satz.

4 Galois-Theorie

4.1 Der Hauptsatz

Definition + Proposition 4.1.1

Sei L/K algebraische Körpererweiterung, \bar{K} ein algebraischer Abschluss von L .

- (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 $\text{Hom}_K(L, \bar{K}) = \text{Aut}_K(L)$

Beweis: " \supseteq " gilt immer. " \subseteq ": Sei $L = Z(\mathcal{F})$, $f \in \mathcal{F}$, $\alpha \in L$ Nullstelle von $f \Rightarrow$
 Für $\sigma \in \text{Hom}_K(L, \bar{K})$ ist $\sigma(\alpha)$ auch Nullstelle von f . Sei $f(X) = \sum_{i=0}^n a_i X^i \Rightarrow$

$$0 = \sigma(f(\alpha)) = \sum_{i=0}^n \underbrace{\sigma(a_i)}_{=a_i} \sigma(\alpha^i) = f(\sigma(\alpha)) \Rightarrow \sigma(\alpha) \in L \Rightarrow \sigma(L) \subseteq L. \sigma$$
 ist surjektiv, da L von den Nullstellen der $f \in \mathcal{F}$ erzeugt wird und jedes $f \in \mathcal{F}$ endlich viele Nullstellen hat, die durch σ permutiert werden. ■

- (c) L/K heißt **galoissch**, wenn L/K normal und separabel ist.
- (d) Ist L/K galoissch, so heißt $\text{Gal}(L/K) := \text{Aut}_K(L)$ die **Galoisgruppe** von L/K .
- (e) Eine endliche Erweiterung L/K ist genau dann galoissch, wenn $|\text{Aut}_K(L)| = [L : K]$

Beweis: " \Rightarrow " Aus (b) folgt

$$|\text{Aut}_K(L)| = |\text{Hom}_K(L, \bar{K})| = [L : K]_s \stackrel{3,4,5}{=} [L : K](*)$$

" \Leftarrow " In (*) gilt stets $|\text{Aut}_K(L)| \leq |\text{Hom}_K(L, \bar{K})| = [L : K]_s \leq [L : K]$.
 Aus $|\text{Aut}_K(L)| = [L : K]$ folgt also $[L : K]_s = [L : K] \Rightarrow L/K$ separabel.
 $\stackrel{1,2}{\Rightarrow} L = K(\alpha)$ für ein $\alpha \in L$; Sei $f \in K[X]$ das Minimalpolynom von α . Sei $\beta \in \bar{K}$ Nullstelle von f . Nach 3.3.1 gibt es $\sigma \in \text{Hom}_K(L, \bar{K})$ mit $\sigma(\alpha) = \beta$.
 Wegen (*) ist $\sigma \in \text{Aut}_K(L) \Rightarrow \beta \in L \Rightarrow L = Z(f)$. ■

Beispiel: Sei K Körper mit Charakteristik nicht 2, $d \in K^\times \setminus (K^\times)^2$. Dann ist $K(\sqrt{d})/K$ eine Galois-Erweiterung, denn $X^2 - d$ ist irreduzibel und separabel und zerfällt in $K(\sqrt{d})[X]$ in $(X - \sqrt{d})(X + \sqrt{d})$.

Bemerkung 4.1.2 (a) Ist L/K galoissch und E ein Zwischenkörper, so ist L/E galoissch und $\text{Gal}(L/E) \subseteq \text{Gal}(L/K)$.

Beweis: L/E normal, da Zerfällungskörper von $\mathcal{F} \subset K[X] \subseteq E[X]$. L/E separabel, da L/K separabel und das Minimalpolynom von $\alpha \in L$ über E in $E[X]$ Teiler des Minimalpolynoms über K ist. ■

(b) Ist in (a) zusätzlich auch E/K galoissch, so ist

$$1 \rightarrow \text{Gal}(L/E) \rightarrow \text{Gal}(L/K) \xrightarrow[\sigma \mapsto \sigma|_E]{\beta} \text{Gal}(E/K) \rightarrow 1$$

exakt.

Beweis: Für $\sigma \in \text{Gal}(L/K) = \text{Aut}_K(L)$ ist $\sigma|_E : E \rightarrow L$, also $\sigma|_E \in \text{Hom}_K(E, L) \subseteq \text{Hom}_K(E, \bar{K}) = \text{Aut}_K(E)$, da E/K galoissch ist. $\Rightarrow \beta$ ist wohldefiniert.

β **surjektiv:** Sei $\sigma \in \text{Gal}(E/K)$. Nach 3.3.3 läßt sich σ fortsetzen zu $\tilde{\sigma} : L \rightarrow \bar{K}$, $\tilde{\sigma} \in \text{Hom}_K(L, \bar{K}) = \text{Aut}_K(L) = \text{Gal}(L/K)$ und $\beta(\tilde{\sigma}) = \tilde{\sigma}|_E = \sigma$

Kern $\beta = \{\sigma \in \text{Gal}(L/K) : \sigma|_E = id_E\} = \text{Aut}_E(L) = \text{Gal}(L/E)$ ■

Satz 15 (Hauptsatz der Galoistheorie)

Sei L/K endliche Galois-Erweiterung.

(a) Die Zuordnungen

$$\begin{array}{ccc} \{\text{Zwischenkörper von } L/K\} & \begin{array}{c} \xrightarrow{\Psi} \\ \xleftarrow{\Phi} \end{array} & \{\text{Untergruppen von } \text{Gal}(L/K)\} \\ E & \begin{array}{c} \xrightarrow{\Phi} \\ \xleftarrow{\Psi} \end{array} & \text{Gal}(L/E) \\ L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \forall \sigma \in H\} & & H \end{array}$$

sind bijektiv und zueinander invers.

(b) Ein Zwischenkörper E von L/K ist genau dann galoissch über K , wenn $\text{Gal}(L/E)$ Normalteiler in $\text{Gal}(L/K)$ ist.

Beweis:(a) L^H ist Zwischenkörper: ✓"Ψ ◦ Φ = id": Sei $H \subseteq \text{Gal}(L/K)$ Untergruppe. z.z.: $\text{Gal}(L/L^H) = H$ "⊇": Nach Def. von L^H "⊆": Nach 4.1.1 ist $|\text{Gal}(L/L^H)| = [L : L^H]$. Es genügt also z.z.: $[L : L^H] \leq |H|$. 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 $\sigma \circ \tau$ alle Elemente von H) $\Rightarrow f \in L^H[X] \Rightarrow$ Das Minimalpolynom g von α über L^H ist Teiler von f . $\Rightarrow [L : L^H] = \deg(g) \leq \deg(f) = |H|$ "Φ ◦ Ψ = id": Sei E Zwischenkörper, $H := \text{Gal}(L/E)$. zu zeigen: $E = L^H$."⊆": Definition. "⊇": Da L^H/E separabel ist, genügt es zu zeigen $[L^H : E]_s = 1$. Sei also $\sigma \in \text{Hom}_E(L^H, \bar{K})$, $\tilde{\sigma} \in \text{Hom}_E(L, \bar{K}) = \text{Aut}_E(L) = \text{Gal}(L/E) = H$ Fortsetzung $\Rightarrow \tilde{\sigma}|_{L^H} = id_{L^H}$
 $=_{\sigma}$ (b) "⇒": 4.1.2 b), da $\text{Gal}(L/E) = \text{Kern } \beta$. "⇐": Sei $H := \text{Gal}(L/E)$ Normalteiler in $\text{Gal}(L/K)$. Wegen 4.1.1 c) genügt es zu zeigen: Für jedes $\sigma \in \text{Hom}_K(E, \bar{K})$ ist $\sigma(E) \subseteq E$. Sei also $\sigma \in \text{Hom}_K(E, \bar{K})$, $\tilde{\sigma} \in \text{Hom}_K(L, \bar{K})$ Fortsetzung.
 $=_{\text{Gal}(L/K)}$ Sei nun $\alpha \in E$, $\tau \in H$. Dann ist $\tau(\sigma(\alpha)) = (\tau \circ \tilde{\sigma})(\alpha) = (\tilde{\sigma} \circ \tau)(\alpha) = \tilde{\sigma}(\alpha) = \sigma(\alpha)$ mit $\tilde{\sigma}$ wie oben und $\tau' := \tilde{\sigma}^{-1} \circ \tau \circ \tilde{\sigma} \in H$ (nach Voraussetzung) $\Rightarrow \sigma(\alpha) \in L^H = E$ ✓**Folgerung 4.1.3**Sei L/K endliche Galoisweiterung. Dann gilt für Zwischenkörper E, E' bzw. Untergruppen H, H' von $\text{Gal}(L/K)$:(a) $E \subseteq E' \iff \text{Gal}(L/E) \supseteq \text{Gal}(L/E')$ $H \subseteq H' \iff L^H \supseteq L^{H'}$ (b) $\text{Gal}(L/E \cap E') = \langle \text{Gal}(L/E), \text{Gal}(L/E') \rangle$ $E \cap E' = L^{\langle \text{Gal}(L/E), \text{Gal}(L/E') \rangle}$ $L^{H \cap H'} = L^H \cdot L^{H'} := K(L^H \cup L^{H'})$ (das **Kompositum** von L^H und $L^{H'}$)**Folgerung 4.1.4**

Zu jeder endlichen separablen Körpererweiterung gibt es nur endlich viele Zwischenkörper.

Beweis: Ist L/K endliche Galoisweiterung, so entsprechen die Zwischenkörper (nach 15) bijektiv den Untergruppen der endlichen Gruppe $\text{Gal}(L/K)$. Im allgemeinen ist $L = K(\alpha)$

(12). Sei f das Minimalpolynom von α über K . f ist separabel, da L/K separabel. Sei \tilde{L} der Zerfällungskörper von f über K . $\Rightarrow \tilde{L}/K$ ist galoissch, $K \subseteq L \subseteq \tilde{L} \Rightarrow L/K$ hat nur endlich viele Zwischenkörper. ■

Proposition 4.1.5

Sei L ein Körper, $G \subseteq \text{Aut}(L)$ eine endliche Untergruppe. $K := L^G = \{\alpha \in L : \sigma(\alpha) = \alpha \forall \sigma \in G\}$

Dann ist L/K Galoiserweiterung und $\text{Gal}(L/K) = G$

Beweis:

- L/K ist algebraisch und separabel. Sei dazu $\alpha \in L$. $\{\sigma(\alpha) : \sigma \in G\} = G\alpha$ ist endlich. Sei $G\alpha = \{\sigma_1(\alpha), \dots, \sigma_r(\alpha)\}$ 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 $f_\alpha^\sigma(X) = \prod_{i=1}^r (X - \sigma(\sigma_i(\alpha)))$ (selbe Faktoren wie $f_\alpha(X)$) $\Rightarrow f_\alpha = f_\alpha^\sigma \Rightarrow f_\alpha \in K[X]$

$\Rightarrow \alpha$ algebraisch, α separabel (da f_α separabel), $[K(\alpha) : K] \leq n$ (*)

- L/K normal: Der Zerfällungskörper von f_α ist in L enthalten. $\Rightarrow L$ ist der Zerfällungskörper der Familie $\{f_\alpha : \alpha \in L\}$

- L/K 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 $\alpha_0 \in L \stackrel{(*)}{\Rightarrow} [K(\{\alpha_i : i \in I_0\}) : K] \leq n$. Sei $I_1 \subseteq I$ endlich, so dass $K_1 := K(\{\alpha_i : i \in I_1\})$ maximal unter den $K(\{\alpha_j : j \in J\})$ für $J \subseteq I$ endlich.

Ann.: $K_1 \neq L$. Dann gibt es $i \in I$ mit $\alpha_i \notin K_1 \Rightarrow K_1(\alpha_i) \supsetneq K_1$, trotzdem endlich im Widerspruch zu Wahl von $K_1 \Rightarrow L/K$ endlich, genauer $[L : K] \leq n$ wegen (*).

- $\text{Gal}(L/K) = G$: " \supseteq ": nach Definition. Nach 4.1.1 ist $n = |G| \leq |\text{Gal}(L/K)| = [L : K] \leq n$

4.2 Die Galoisgruppe einer Gleichung

Definition + Bemerkung 4.2.1

Sei K ein Körper, $f \in K[X]$ ein separables Polynom.

4.2 Die Galoisgruppe einer Gleichung

- (a) Sei $L = L(f)$ Zerfällungskörper von f über K . Dann heißt $\text{Gal}(f) := \text{Gal}(L/K)$ **Galoisgruppe von f** .
- (b) Ist $n = \deg(f)$, so gibt es injektiven Gruppenhomomorphismus $\text{Gal}(f) \hookrightarrow S_n$ (durch Permutation der Nullstellen von f)
- (c) Ist L/K separable Körpererweiterung vom Grad n , so ist $\text{Aut}_K(L)$ isomorph zu einer Untergruppe von S_n .

Beweis: Sei $L = K(\alpha)$, $f \in K[X]$ Minimalpolynom von α , $\alpha = \alpha_1, \dots, \alpha_d$ die Nullstellen von f in $L \Rightarrow$ jedes $\sigma \in \text{Aut}_K(L)$ permutiert $\alpha_1, \dots, \alpha_d$. ■

Beispiele 4.2.2

Die Galoisgruppe von $f(X) = X^5 - 4X + 2 \in \mathbb{Q}[X]$ ist S_5 .

Bew.:

- f ist irreduzibel: Eisenstein für $p = 2$
- f hat 3 reelle und 2 zueinander konjugiert komplexe Nullstellen $f(-\infty) = -\infty$, $f(0) = 2$, $f(1) = -1$, $f(\infty) = \infty \Rightarrow f$ 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 $\Rightarrow f$ hat genau 3 reelle Nullstellen. Ist $\alpha \in \mathbb{C}$ Nullstelle von f , so ist $f(\bar{\alpha}) = \overline{f(\alpha)} = 0$.
- $G = \text{Gal}(f)$ enthält die komplexe Konjugation τ . τ operiert als Transposition: 2 Nullstellen werden vertauscht, 3 bleiben fix.
- G enthält ein Element von Ordnung 5: Ist α Nullstelle von f , so ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ und $\mathbb{Q}(\alpha) \subseteq L(f) \stackrel{15}{\Rightarrow} 5$ teilt $|G| \stackrel{\text{Sylow}}{\Rightarrow}$ Beh.
- G enthält also einen 5-Zyklus und eine Transposition $\stackrel{(!)}{\Rightarrow} G = S_5$.

Bemerkung 4.2.3

Allgemeine Gleichung n -ten Grades: Sei k ein Körper, $L = k(T_1, \dots, T_n) = \text{Quot}(k[T_1, \dots, T_n])$

- S_n operiert auf L durch $\sigma(T_i) = T_{\sigma(i)}$
- Sei $K := L^{S_n}$. L/K ist Galois-Erweiterung (nach Proposition 4.1.5) vom Grad $n!$
- L ist (über K) Zerfällungskörper von $f(X) = \prod_{i=1}^n (X - T_i) \in K[X]$
- $\text{Gal}(f) = S_n$
- $f(X) = \sum_{\nu=0}^n (-1)^\nu s_\nu(T_1, \dots, T_n) X^{n-\nu}$ mit $s_\nu(T_1, \dots, T_n) = \sum_{1 \leq i_1 < \dots < i_\nu \leq n} T_{i_1} \cdot \dots \cdot T_{i_\nu}$
z.B.: $s_1(T_1, \dots, T_n) = T_1 + \dots + T_n$, $s_2 = T_1 T_2 + T_1 T_3 + \dots + T_{n-1} T_n$, $s_n = T_1 \cdot \dots \cdot T_n$

- $K = k(s_1, \dots, s_n)$

4.3 Einheitswurzeln

Bemerkung + Definition 4.3.1

Sei K ein Körper, \bar{K} algebraischer Abschluss von K . Sei n eine positive ganze Zahl. Angenommen, $\text{char}(K)$ ist entweder 0 oder teilerfremd zu n .

- (a) Die Nullstellen von $X^n - 1$ in \bar{K} heißen **n -te Einheitswurzeln**.
 (b) $\mu_n(\bar{K}) := \{\zeta \in \bar{K} : \zeta^n = 1\}$ ist zyklische Untergruppe von \bar{K}^\times der Ordnung n .

Beweis: $\mu_n(\bar{K})$ Untergruppe \checkmark , also zyklisch nach 3.5.1. $f(X) = X^n - 1$ ist separabel, da $f'(X) = nX^{n-1}$ (Bem 3.4.1) ■

- (c) Eine n -te Einheitswurzel ζ heißt **primitiv**, wenn $\langle \zeta \rangle = \mu_n(\bar{K})$

Satz 16

(Voraussetzungen wie eben.)

- (a) Die Anzahl der primitiven Einheitswurzeln in \bar{K} ist $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = \{m \in \{1, \dots, n\} : \text{ggT}(m, n) = 1\}$ ($n \mapsto \varphi(n)$ ist Eulersche φ -Funktion)

Beweis: Ist ζ primitive n -te Einheitswurzel, so ist $\mu_n(\bar{K}) = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$, ζ^k erzeugt $\{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\} \Leftrightarrow \text{ggT}(n, k) = 1$. ■

- (b) Ist $n = p_1^{\nu_1} \dots p_r^{\nu_r}$, (Primfaktorzerlegung) so ist $\varphi(n) = \prod_{i=1}^r p_i^{\nu_i-1} (p_i - 1)$

Beweis: Nach Satz 7 ist $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_r^{\nu_r}\mathbb{Z}$ (als Ringe) $\Rightarrow (\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/p_1^{\nu_1}\mathbb{Z})^\times \oplus \dots \oplus (\mathbb{Z}/p_r^{\nu_r}\mathbb{Z})^\times$ (als Gruppen). Doch für jede Primzahl p und jedes positive ν ist

$$|(\mathbb{Z}/p^\nu\mathbb{Z})^\times| = p^\nu - p^{\nu-1} = p^{\nu-1}(p - 1). \quad \blacksquare$$

- (c) Sind $\zeta_1, \dots, \zeta_{\varphi(n)}$ die primitiven Einheitswurzeln, so heißt $\Phi_n(X) := \prod_{i=1}^{\varphi(n)} (X - \zeta_i) \in \bar{K}[X]$ das **n -te Kreisteilungspolynom**

- (d) $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Beweis: $X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{d|n} \prod_{\substack{\zeta \in \mu_n \\ \text{ord}(\zeta)=d}} (X - \zeta) = \prod_{d|n} \Phi_d(X)$ ■

(e) Sei ζ primitive n -te Einheitswurzel. Dann ist $K(\zeta)/K$ Galois-Erweiterung.

Beweis: $K(\zeta)$ ist Zerfällungskörper von $X^n - 1$ über K , also normal. $X^n - 1$ ist separabel (4.3.1) ■

(f)

$$\chi_n : \begin{array}{ccc} \text{Gal}(K(\zeta)/K) & \rightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma & \mapsto & \chi_n(\sigma) \end{array}$$

ist injektiver Gruppenhomomorphismus, wobei $\sigma(\zeta) = \zeta^{\chi_n(\sigma)}$. (χ_n heißt **zyklotomischer Charakter**)

Beweis: $\chi_n(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$, da $\sigma(\zeta)$ primitive Einheitswurzel sein muß.

χ_n ist Gruppenhomomorphismus: $\sigma_1, \sigma_2 \in \text{Gal}(K(\zeta)/K) \Rightarrow \sigma_1(\sigma_2(\zeta)) = \sigma_1(\zeta^{\chi_n(\sigma_2)}) = (\sigma_1(\zeta))^{\chi_n(\sigma_2)} = \zeta^{\chi_n(\sigma_1)\chi_n(\sigma_2)}$

χ_n injektiv: $\chi_n(\sigma) = 1 \Rightarrow \sigma(\zeta) = \zeta \Rightarrow \sigma = id$ ■

(g) $\Phi_n(X) \in K[X]$, genauer $\Phi_n(X) \in \begin{cases} \mathbb{Z}[X] \text{ (primitiv)} & : \text{char}(K) = 0 \\ \mathbb{F}_p[X] & : \text{char}(K) = p \end{cases}$

Beweis: Induktion über n : $n = 1 \checkmark$

$$n > 1: \underbrace{X^n - 1}_{(*)} \stackrel{(d)}{=} \Phi_n(X) \underbrace{\prod_{\substack{d|n \\ d < n}} \Phi_d(X)}_{(**)}$$

$\text{char}(K) = p$: $(*) \in \mathbb{F}_p[X]$, $(**) \in \mathbb{F}_p[X]$ nach IV $\Rightarrow \Phi_n(X) \in \mathbb{F}_p[X]$: (weil Polynomdivision zweier Polynome in $\mathbb{F}_p[X]$ nie die Koeffizienten aus dem Körper \mathbb{F}_p herausführt).

$\text{char}(K) = 0$: $(*) \in \mathbb{Z}[X]$ (primitiv), $(**) \in \mathbb{Z}[X]$ primitiv nach IV

Lemma von Gauß $\Rightarrow \Phi_n(X) \in \mathbb{Z}[X]$ primitiv. ■

(h) Ist $K = \mathbb{Q}$, so ist Φ_n irreduzibel und χ_n ein Isomorphismus. $\mathbb{Q}(\zeta)$ heißt n -ter **Kreisteilungskörper**.

Beweis: Es genügt zu zeigen: Φ_n irreduzibel (dann folgt χ_n Isomorphismus aus (e) und (f))

Sei $f \in \mathbb{Q}[X]$ Minimalpolynom von ζ , $f \in \mathbb{Z}[X]$ wegen (g)

Beh.: $f(\zeta^p) = 0$ für jede Primzahl p mit $p \nmid n$.

Dann ist auch $f(\zeta^m) = 0$ für jedes m mit $\text{ggT}(m, n) = 1 \Rightarrow f(\zeta_i) = 0$ für jede primitive Einheitswurzel $\zeta_i \Rightarrow \Phi_n | f \Rightarrow \Phi_n = f$

Bew.: Sei $X^n - 1 = f \cdot h$. Wäre $f(\zeta^p) \neq 0 \Rightarrow h(\zeta^p) = 0$ dh. ζ Nullstelle von $h(X^p) \Rightarrow h(X^p)$ ist Vielfaches von $f \Rightarrow \exists g \in \mathbb{Z}[X]$ mit $h(X^p) = f \cdot g$
 $\xrightarrow{\text{mod } p} \bar{f}\bar{g} = \bar{h}^p$ in $\mathbb{F}_p[X] \Rightarrow \bar{f}$ und \bar{h} haben gemeinsame Nullstellen in $\mathbb{F}_p \Rightarrow X^n - 1 = \bar{f}\bar{h}$ hat doppelte Nullstelle ζ zu $X^n - 1$ separabel. ■

Beispiele: $\Phi_1(X) = 1$, $\Phi_2(X) = X + 1$, $\Phi_p(X) = X^{p-1} + X^{p-2} + \dots + X + 1$ für p prim.

$$\Phi_4(X) = \frac{X^4 - 1}{\Phi_2 \cdot \Phi_1} = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1$$

$$\Phi_6(X) = \frac{X^6 - 1}{\Phi_3 \Phi_2 \Phi_1} = \dots = X^2 - X + 1$$

$$\Phi_8(X) = X^4 + 1$$

Für $n < 105$ sind alle Koeffizienten 0, 1 oder -1 .

Folgerung 4.3.2

Das regelmäßige n -Eck ist genau dann mit Zirkel und Lineal (aus $\{0, 1\}$) konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist.

Beweis: z.z.: ζ_n (primitive n -te Einheitswurzel) $\in K(\{0, 1\}) \Leftrightarrow \varphi(n) = 2^l$ für ein $l \geq 1 \Leftrightarrow [\underbrace{\mathbb{Q}(\zeta_n) : \mathbb{Q}}_{\varphi(n)}] = 2^l$ und es gibt Kette $\mathbb{Q}(M) = L_0 \subset L_1 \subset \dots \subset L_n = \mathbb{Q}(\zeta_n)$ und $[L_i : L_{i-1}] = 2$.

" \Leftarrow ": $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ ist abelsch von Ordnung 2^l . Dazu gehört Kompositionsreihe mit Faktoren $\mathbb{Z}/2\mathbb{Z}$ Hauptsatz d. Galoistheorie \Rightarrow ■

4.4 Norm, Spur und Charaktere

Definition + Proposition 4.4.1

Sei G eine Gruppe, K ein Körper.

- (a) Ein **Charakter** von G (mit Werten in K) ist ein Gruppenhomomorphismus $\chi : G \rightarrow K^\times$
- (b) $X_K(G) := \{\chi : G \rightarrow K^\times, \chi \text{ Charakter}\} = \text{Hom}(G, K^\times)$ 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 $\text{Abb}(G, K)$

Beweis: Angenommen $X_K(G)$ ist linear abhängig. Dann sei $n > 0$ minimal, so dass es in $X_K(G)$ n paarweise verschieden linear abhängige Elemente gibt. Es gebe also paarweise verschiedene Charaktere $\chi_1, \dots, \chi_n \in X_K(G)$ und Körperelemente $\lambda_1, \dots, \lambda_n \in K$ mit $\sum_{i=1}^n \lambda_i \chi_i = 0$. Dazu muß $n \geq 2$ sein. Ferner sind die Körperelemente $\lambda_1, \dots, \lambda_n \in K$ von 0 verschieden, da sonst n nicht minimal wäre.

Sei $g \in G$ mit $\chi_1(g) \neq \chi_2(g)$. Dann gilt für alle $h \in G$:

$$0 = \sum_{i=1}^n \lambda_i \underbrace{\chi_i(gh)}_{=\chi_i(g)\chi_i(h)} = \sum_{i=1}^n \lambda_i \chi_i(g) \underbrace{\chi_i(h)}_{=\mu_i \in K^\times} = \sum_{i=1}^n \mu_i \chi_i(h) \Rightarrow \sum_{i=1}^n \mu_i \chi_i = 0$$

Sei $\nu_i := \mu_i - \lambda_i \chi_1(g)$, $i = 1, \dots, n$. Dann ist $\sum_{i=1}^n \nu_i \chi_i = 0$ (da $\sum_{i=1}^n \mu_i \chi_i = 0$

und $\sum_{i=1}^n \lambda_i \chi_i = 0$ ist). Da $\nu_1 = \lambda_1 \chi_1(g) - \lambda_1 \chi_1(g) = 0$ ist, bedeutet dies:

$$\sum_{i=2}^n \nu_i \chi_i = 0. \text{ Wegen } \nu_2 = \lambda_2 \chi_2(g) - \lambda_2 \chi_1(g) = \underbrace{\lambda_2}_{\neq 0} \underbrace{(\chi_2(g) - \chi_1(g))}_{\neq 0} \neq 0$$

sind also χ_2, \dots, χ_n linear abhängig. Dies steht im Widerspruch zur Minimalität von n . ■

Es sei angemerkt, daß der Begriff eines "Charakters" in der Mathematik in sehr vielen, teilweise stark unterschiedlichen Bedeutungen anzutreffen ist. So bedeutet "Charakter" in der Darstellungstheorie von Gruppen etwas anderes als in der obigen Definition 4.4.1.

Definition + Bemerkung 4.4.2

Sei L/K endliche Körpererweiterung, $q := \frac{[L:K]}{[L:K]_s}$ ($= p^r$, $p = \text{char}(K)$), $n := [L : K]_s$, $\text{Hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$

4 Galois-Theorie

- (a) Für $\alpha \in L$ heißt $\text{tr}_{L/K}(\alpha) := q \cdot \sum_{i=1}^n \sigma_i(\alpha) \in \bar{K}$ die **Spur** von α (über K)
- (b) $\forall \alpha \in L : \text{tr}_{L/K}(\alpha) \in K$

Beweis: $\exists L/K$ separabel. Ist L/K normal, also galoissch, so ist $\text{Hom}_K(L, \bar{K}) = \text{Gal}(L/K) =: G$ und $\text{tr}_{L/K}(\alpha) \in L^G = K$ (da invariant unter allen σ_i). Andernfalls sei \tilde{L} normale Erweiterung von K mit $L \subset \tilde{L}$. Für $\tau \in \text{Hom}_K(\tilde{L}, \bar{K}) = \text{Gal}(\tilde{L}/K)$ und jedes $i = 1, \dots, n$ ist $\tau \circ \sigma_i \in \text{Hom}_K(L, \bar{K})$ (da $\sigma_i(L) \subseteq \tilde{L}$) $\Rightarrow \text{tr}_{L/K}(\alpha) \in \tilde{L}^{\text{Gal}(\tilde{L}/K)} = K$ ■

(c) $\text{tr}_{L/K}$ 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) $N_{L/K}(\alpha) \in K$

(f) $N_{L/K} : L^\times \rightarrow K^\times$ ist Gruppenhomomorphismus

Beweis:

(e) Ist L/K separabel, so argumentiere wie in (b). Sonst siehe Bosch. ■

Bemerkung 4.4.3

Sei L/K endliche Körpererweiterung. Für $\alpha \in L$ sei $m_\alpha : L \rightarrow L, x \mapsto \alpha x$. m_α ist K -linear und es gilt:

$$\text{tr}_{L/K}(\alpha) = \text{Spur}(m_\alpha), N_{L/K}(\alpha) = \det(m_\alpha)$$

Beweis: Ist L/K separabel, so sei $L = K(\alpha)$. Dann ist $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ eine K -Basis von L , $[L : K] = n$. Weiter sei $f(X) = X^n + c_{n-1}X^{n-1} + \dots + c_1X + c_0 \in K[X]$ das Minimalpolynom von α über K . Dann ist die Abbildungsmatrix von m_α bezüglich der Basis $1, \dots, \alpha^{n-1}$

$$D = \begin{pmatrix} 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & & \vdots & -c_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 0 & 1 & -c_{n-1} \end{pmatrix}$$

$$\Rightarrow \text{Spur}(m_\alpha) = -c_{n-1}, \det(m_\alpha) = (-1)^n c_0.$$

In $\bar{K}[X]$ zerfällt f in Linearfaktoren:

$$f = \prod_{i=1}^n (X - \sigma_i(\alpha)) \Rightarrow c_{n-1} = -\sum_{i=1}^n \sigma_i(\alpha), c_0 = (-1)^n \prod_{i=1}^n \sigma_i(\alpha)$$

Ist $L \neq K(\alpha)$, so sei b_1, \dots, b_m eine $K(\alpha)$ -Basis von L . Dann ist $B = \{b_i \alpha^j, i = 1, \dots, m, j = 0, \dots, n-1\}$ eine K -Basis von L . Dann ist die Darstellungsmatrix von m_α bezüglich B :

$$\tilde{D} = \begin{pmatrix} D & 0 & \dots & 0 \\ 0 & D & & \\ & & \ddots & \\ 0 & 0 & & D \end{pmatrix}$$

$$\Rightarrow \text{Spur}(m_\alpha) = m(-c_{n-1}), \det(m_\alpha) = ((-1)^n c_0)^m$$

Für jedes $\sigma_i \in \text{Hom}_K(L, \bar{K})$ ist $\sigma_i(\alpha)$ Nullstelle von f . Jede Nullstelle von f wird dabei gleichoft angenommen, nämlich $m = [L : K(\alpha)]$ -mal $\Rightarrow \text{tr}_{L/K}(\alpha) = m \cdot \text{tr}_{K(\alpha)/K}(\alpha) = m(-c_{n-1})$ und $N_{L/K}(\alpha) = (N_{K(\alpha)/K})^m = ((-1)^n c_0)^m$ ■

Satz 17 ("Hilbert(s) Satz) 90")

Sei L/K zyklische Galois-Erweiterung. (dh. $\text{Gal}(L/K) = \langle \sigma \rangle$ 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 4.4.1 sind die Charaktere $id, \sigma, \dots, \sigma^{n-1} : L^\times \rightarrow L^\times$ linear unabhängig über L .

Nun ist $f = id + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \dots + \beta\sigma(\beta) \dots \sigma^{n-2}(\beta)\sigma^{n-1}$ nicht die Nullabbildung $\Rightarrow \exists \gamma \in L$ mit $\alpha := f(\gamma) \neq 0$

$$\beta\sigma(\alpha) = \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \dots + \underbrace{\beta\sigma(\beta) \dots \sigma^{n-1}(\beta)}_{N_{L/K}(\beta)=1} \underbrace{\sigma^n(\gamma)}_{=\gamma} = \alpha \quad \blacksquare$$

(b) Sei L/K zyklische Galois-Erweiterung, $n = [L : K]$, $\sigma \in \text{Gal}(L/K)$ ein Erzeuger. Zu $\beta \in L$ mit $\text{tr}_{L/K}(\beta) = 0$ gibt es $\alpha \in L$ mit $\beta = \alpha - \sigma(\alpha)$

Beweis: Sei $\gamma \in L$ mit $\text{tr}_{L/K}(\gamma) \neq 0$ und

$$\begin{aligned} \alpha &:= \frac{1}{\text{tr}_{L/K}(\gamma)} \cdot [\beta\sigma(\gamma) + (\beta + \sigma(\beta))\sigma^2(\gamma) + \dots + (\beta + \sigma(\beta) + \dots + \\ &\sigma^{n-2}(\beta))\sigma^{n-1}(\gamma)] \\ \Rightarrow \sigma(\alpha) &= \frac{1}{\text{tr}_{L/K}(\gamma)} [\sigma(\beta)\sigma^2(\gamma) + (\sigma(\beta) + \sigma^2(\beta))\sigma^3(\gamma) + \dots + (\sigma(\beta) + \dots + \end{aligned}$$

$$\begin{aligned} & \sigma^{n-1}(\beta)\sigma^n(\gamma) \\ \Rightarrow & (\alpha - \sigma(\alpha))\text{tr}_{L/K}(\gamma) = \beta\sigma(\gamma) + \beta\sigma^2(\gamma) + \dots + \beta\sigma^{n-1}(\gamma) - \\ & \underbrace{(\sigma(\beta) + \dots + \sigma^{n-1}(\beta))\gamma}_{-\beta} = \beta \cdot \text{tr}_{L/K}(\gamma) \quad \blacksquare \end{aligned}$$

Folgerung 4.4.4

Voraussetzungen wie in Satz 17.

- (a) Ist $\text{char}(K)$ 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 von der Form

$$X^n - \gamma$$

ist für ein $\gamma \in K$. ("Kummer-Erweiterung")

- (b) Ist $\text{char}(K) = [L : K] = p$, so gibt es ein primitives Element $\alpha \in L$, so dass das Minimalpolynom von α über K die Form

$$X^p - X - \gamma$$

hat für ein $\gamma \in K$. ("Artin-Schreier-Erweiterung")

Beweis:

- (a) Es ist $N_{L/K}(\zeta) = \zeta^n = 1 = N_{L/K}(\zeta^{-1}) \stackrel{\text{Satz 17}}{\Rightarrow}$ es gibt $\alpha \in L^\times$ mit $\sigma(\alpha) = \zeta\alpha \Rightarrow \sigma^i(\alpha) = \zeta^i\alpha$, $i = 1, \dots, n-1 \Rightarrow$ Das Minimalpolynom von α über K hat n verschiedene Nullstellen $\Rightarrow L = K(\alpha)$.

Außerdem ist $\sigma(\alpha^n) = \sigma(\alpha)^n = \alpha^n \Rightarrow \gamma := \alpha^n \in K \Rightarrow$ Das Minimalpolynom von α ist $X^n - \gamma$

- (b) $\text{tr}_{L/K}(1) = 1 + \dots + 1 = p = 0 \stackrel{\text{Satz 17}}{\Rightarrow}$ es gibt $\alpha \in L$ mit $\sigma(\alpha) = \alpha + 1 \Rightarrow \sigma^i(\alpha) = \alpha + i$, $i = 0, \dots, n-1 \Rightarrow K(\alpha) = L$

$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = \alpha^p + 1 - (\alpha + 1) = \alpha^p - \alpha \Rightarrow \alpha^p - \alpha =: \gamma \in K$ und $X^p - X - \gamma$ ist Minimalpolynom von α . \blacksquare

Proposition 4.4.5

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, $\text{Gal}(L/K)$ zyklisch, $d := [L : K]$ ist Teiler von n , $\alpha^d \in K$, $X^d - \alpha^d$ ist Minimalpolynom von α
- (b) Ist $\text{char}(K) = p > 0$ und $\alpha \in L \setminus K$ Nullstelle eines Polynoms $X^p - X - \gamma$ für ein $\gamma \in K$, so ist L/K galoissch und $\text{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$

Beweis:

- (a) Die Nullstellen von $X^n - \gamma$ sind $\alpha, \zeta\alpha, \dots, \zeta^{n-1}\alpha \Rightarrow L$ ist Zerfällungskörper von $X^n - \gamma$, also normal und separabel, also galoissch.
 Für $\sigma \in \text{Gal}(L/K)$ ist $\sigma(\alpha) = \zeta^{\nu(\sigma)}\alpha$ für ein $\nu(\sigma) \in \mathbb{Z}/n\mathbb{Z}$.
 $\sigma \mapsto \nu(\sigma)$ ist injektiver Gruppenhomomorphismus $\text{Gal}(L/K) \rightarrow \mathbb{Z}/n\mathbb{Z} \Rightarrow \text{Gal}(L/K)$ ist zyklisch, da Untergruppe von $\mathbb{Z}/n\mathbb{Z} \Rightarrow d = [L : K]$ teilt n .
 Für $\sigma \in \text{Gal}(L/K)$ ist $\sigma(\alpha^d) = (\zeta^{\nu(\sigma)})^d \alpha^d = \alpha^d \Rightarrow \alpha^d \in K$; $X^d - \alpha^d$ ist Minimalpolynom, da $L = K(\alpha)$ und $[K(\alpha) : K] = d$.
- (b) Für $i \in \mathbb{F}_p$ ist $(\alpha + i)^p - (\alpha + i) - \gamma = \alpha^p + \underbrace{i^p}_{=i} - \alpha - i - \gamma = 0 \Rightarrow X^p - X - \gamma$ hat p verschieden Nullstellen $\Rightarrow L$ ist Zerfällungskörper von $X^p - X - \gamma$ und L/K ist separabel. Außerdem folgt: $\text{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$ ■

4.5 Auflösung von Gleichungen durch Radikale

Definition 4.5.1

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 $\text{char}(K) \nmid n$
 - (iii) α ist Nullstelle von $X^p - X - \gamma$ für $\gamma \in K$, $\text{char}(K) = p$
- (b) Eine endliche Körpererweiterung L/K heißt **Radikalerweiterung**, wenn es eine Körpererweiterung L'/L gibt und eine Kette $K = L_0 \subset L_1 \subset \dots \subset L_n = L'$ von Zwischenkörpern, so dass L_{i+1}/L_i elementare Radikalerweiterung ist für $i = 0, \dots, n-1$
- (c) Ist $f \in K[X]$ separabel, nicht konstant, so heißt die Gleichung $f(X) = 0$ **durch Radikale auflösbar**, wenn der Zerfällungskörper von f Radikalerweiterung ist.

Beispiel: $K = \mathbb{Q}$, $f(X) = X^3 - 3X + 1$

Beh.: 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** einfache Radikalerweiterung.

Die Nullstellen von f sind:

$$\begin{aligned} \alpha_1 &= e^{2\pi i/9} + e^{16\pi i/9} \\ \alpha_2 &= e^{8\pi i/9} + e^{10\pi i/9} \\ \alpha_3 &= e^{14\pi i/9} + e^{4\pi i/9} \end{aligned}$$

Es ist $\alpha_1^2 = e^{4\pi i/9} + e^{14\pi i/9} + 2 = \alpha_3 + 2 \Rightarrow \alpha_3 \in \mathbb{Q}(\alpha_1) \Rightarrow \alpha_2 = -\alpha_1 - \alpha_3 \in \mathbb{Q}(\alpha_1)$

Satz 18

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 auflösbar ist (dh. G hat Normalreihe $G = G_0 \triangleright \dots \triangleright G_n = \{e\}$ mit G_i/G_{i+1} abelsch).
- (b) Eine endliche Körpererweiterung L/K ist genau dann Radikalerweiterung, wenn es eine endliche Galoiserweiterung L'/K gibt mit $L \subseteq L'$, so dass $\text{Gal}(L'/K)$ auflösbare Gruppe ist.

Beispiel: $X^5 - 4X + 2$ hat Galoisgruppe S_5 und ist deshalb nicht durch Radikale auflösbar, denn $S_5 \supset A_5 \supset \{e\}$ ist Kompositionsreihe. Nach Jordan-Hölder tritt A_5 in jeder Kompositionsreihe für S_5 als Faktorgruppe auf.

Beweis: " \Rightarrow ": Sei $K = L_0 \subset L_1 \subset \dots \subset L_m$ Kette wie in Def. 4.5.1 (b) mit $L \subseteq L_m$.

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 $\text{Gal}(K(\zeta)/K) \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$, also auflösbar.

Ist L_1/K vom Typ (iii), so ist L_1/K galoissch und $\text{Gal}(L_1/K) = \mathbb{Z}/p\mathbb{Z}$.

Sei L_1/K vom Typ (ii). Enthält K eine primitive n -te Einheitswurzel, so ist $K(\alpha)/K$ galoissch und $\text{Gal}(K(\alpha)/K) \cong \mathbb{Z}/n\mathbb{Z}$

Andernfalls sei $F = K(\zeta)$ der Zerfällungskörper von $X^n - 1$ über K und $L'_1 = L_1(\zeta) = F(\alpha) = F \cdot L_1$ 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

$$1 \rightarrow \underbrace{\text{Gal}(L'_1/F)}_{\text{zyklisch}} \rightarrow \text{Gal}(L'_1/K) \rightarrow \underbrace{\text{Gal}(F/K)}_{\text{abelsch}} \rightarrow 1$$

$\Rightarrow \text{Gal}(L'_1/K)$ auflösbar.

$m>1$: Eine endliche Körpererweiterung heißt **auflösbar**, wenn es eine endliche Erweiterung L'/L gibt, so dass L'/K galoissch und $\text{Gal}(L'/K)$ auflösbar ist.

Nach Induktionsvoraussetzung ist L_{m-1}/K auflösbar. Außerdem ist L_m/L_{m-1} auflösbar. ($m=1$)

4.5 Auflösung von Gleichungen durch Radikale

zu zeigen also: Sind $K \subset \underbrace{L}_{=L_{m-1}} \subset \underbrace{M}_{=L_m}$ Körpererweiterungen und ist L/K auflösbar und M/L auflösbar, so ist M/K auflösbar.

Seien dazu L'/L und M'/M Erweiterungen wie in Def.:

Beh.: $L'M'/L'$ ist galoissch und $\text{Gal}(L'M'/L)$ ist auflösbar.

denn: Nach Voraussetzung ist M'/L galoissch, also Zerfällungskörper eines Polynoms $f \in L[X] \Rightarrow M'L'$ ist Zerfällungskörper von $f \in L'[X]$ über L' .

Außerdem: $\text{Gal}(L'M'/L') \rightarrow \text{Gal}(M'/L)$, $\sigma \mapsto \sigma|_{M'} \stackrel{(!)}{\in} \text{Gal}(M'/L)$ ist wohldefiniert und injektiv: Ist $\sigma|_{M'} = id_{M'}$, so ist $\sigma = id_{L'M}$, da $\sigma|_{L'} = id_{L'}$ nach Voraussetzung.

Also $\mathcal{C}EL = L'$, $L'M' = M$.

m>1 (Forts.) Ist M/K galoissch, so ist $\text{Gal}(M/K)$ auflösbar, da dann

$$1 \rightarrow \underbrace{\text{Gal}(M/L)}_{\text{auflösbar}} \rightarrow \text{Gal}(M/K) \rightarrow \underbrace{\text{Gal}(L/K)}_{\text{auflösbar}} \rightarrow 1$$

exakt ist.

Andernfalls sei \tilde{M}/M (minimale) Erweiterung, so dass \tilde{M}/K galoissch ist. \tilde{M} wird (über K) erzeugt von den $\sigma(M)$, $\sigma \in \text{Hom}_K(M, \bar{K})$. (\bar{K} fest gewählter algebraischer Abschluss von K) Für jedes $\sigma \in \text{Hom}_K(M, \bar{K})$ ist $\sigma(M)$ Galoiserweiterung von $\sigma(L) = L$.

Dann ist

$$\begin{array}{ccc} \text{Gal}(\tilde{M}/L) & \rightarrow & \prod_{\sigma \in \text{Hom}_K(M, \bar{K})} \text{Gal}(\sigma(M)/L) \\ \tau & \mapsto & (\tau|_{\sigma(M)})_{\sigma} \end{array}$$

injektiver Gruppenhomomorphismus.

Für jedes $\sigma \in \text{Hom}_K(M, \bar{K})$ ist $\text{Gal}(\sigma(M)/L) \cong \text{Gal}(M/L)$, also auflösbar $\Rightarrow \prod_{\sigma} \text{Gal}(\sigma(M)/L)$ ist auflösbar. (!) $\Rightarrow \text{Gal}(\tilde{M}/L)$ auflösbar (als Untergruppe einer auflösbaren Gruppe) $\Rightarrow \text{Gal}(\tilde{M}/K)$ ist auflösbar wegen $1 \rightarrow \text{Gal}(\tilde{M}/L) \rightarrow \text{Gal}(\tilde{M}/K) \rightarrow \text{Gal}(L/K) \rightarrow 1$ exakt.

" \Leftarrow ":

$G := \text{Gal}(L'/K)$ sei auflösbar, $G = G_0 \supset G_1 \supset \dots \supset G_m = \{1\}$ 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 , $i = 0, \dots, m-1$ ist.

Dazu gehört eine Kette von Zwischenkörpern $K = K_0 \subset K_1 \subset \dots \subset K_m = L'$, in der K_i/K_{i-1} Galoiserweiterung ist und $\text{Gal}(K_i/K_{i-1}) \cong \mathbb{Z}/p_i\mathbb{Z}$.

4 Galois-Theorie

Fall 1: Ist $p_i = \text{char}(K)$, so ist K_i/K_{i-1} elementare Radikalerweiterung vom Typ (iii), also Minimalpolynom der Form $X^{p_i} - X - \gamma$.

Fall 2: Ist $p_i \neq \text{char}(K)$, so ist K_i/K_{i-1} vom Typ (ii), **falls** K_{i-1} eine primitive n -te Einheitswurzel ζ enthält.

Fall 3: $p_i \neq \text{char}(K)$, K_{i-1} enthält keine primitive Einheitswurzel. Sei also

$$d := \prod_{\substack{p \text{ prim} \\ p \mid |G|}} p$$

und F der Zerfällungskörper von $X^d - 1$ über K . $\Rightarrow F/K$ ist Erweiterungskörper vom Typ (i).

Sei $\tilde{L} = FL' \Rightarrow \tilde{L}/F$ ist Galoiserweiterung (siehe hier ausgelassenes Diagramm). Die Abbildung $\text{Gal}(\tilde{L}/F) \rightarrow \text{Gal}(L'/K)$, $\sigma \mapsto \sigma|_{L'}$, ist injektiver Gruppenhomomorphismus, also ist $\text{Gal}(\tilde{L}/F)$ auflösbar und $|\text{Gal}(\tilde{L}, F)|$ teilt $|G|$. Erhalte Kette $K \subset F \subset F_1 \subset \dots \subset F_r = \tilde{L}$ von Zwischenkörpern, F_i/F_{i-1} Galoiserweiterung, $\text{Gal}(F_i/F_{i-1}) \cong \mathbb{Z}/p_i\mathbb{Z}$ elementare Radikalerweiterung vom Typ (ii). ■