

Algebra 1 Vorlesungsmitschrieb  
nach Vorlesung von Prof. Gebhard Böckle

Yousef Khell

March 5, 2024

# Inhaltsverzeichnis

<b>1</b>	<b>Gruppentheorie</b>	<b>3</b>
1.1	Gruppen und Monoide . . . . .	3
	Monoid . . . . .	3
	Gruppe . . . . .	3
	Ring . . . . .	5
	Ordnung . . . . .	5
	Untermoid/Untergruppe . . . . .	5
	Erzeuger . . . . .	7
	Zyklische Gruppe . . . . .	7
	Satz von Lagrange . . . . .	9
	Exponent einer Gruppe . . . . .	11
1.2	Gruppenhomomorphismen . . . . .	12
	Homomorphismus . . . . .	12
	Isomorphismus . . . . .	13
1.3	Normalteiler . . . . .	14
	Kommutator/Kommutatoruntergruppe . . . . .	15
	Faktor-/Quotientengruppe . . . . .	17
1.4	Homomorphiesatz für Gruppen . . . . .	17
1.5	Einschub: Faktoringe . . . . .	19
1.6	Die Isomorphiesätze . . . . .	19
	Erster Isomorphiesatz . . . . .	19
	Zweiter Isomorphiesatz . . . . .	20
1.7	(Semi-)direkte Produkte . . . . .	22
	Direktes Produkt . . . . .	22
	Semi-direktes Produkt . . . . .	23
<b>2</b>	<b>Gruppen Strukturtheorie</b>	<b>25</b>
2.1	Strukturtheorie zu Gruppen (“Einige Aussagen”) . . . . .	25
	Wirkungen . . . . .	25
	Eigenschaften von Wirkungen . . . . .	26
	Bahn . . . . .	26
	Satz von Cayley . . . . .	28
	Stabilisator . . . . .	28
	Bahngleichung . . . . .	29
	Freie Operation . . . . .	29
	Fixpunkte . . . . .	29
	Konjugationsklasse . . . . .	30
	Klassengleichung . . . . .	30

	p-Gruppe . . . . .	30
	Satz von Cauchy . . . . .	31
2.2	Permutationsgruppen . . . . .	31
	Träger . . . . .	31
	disjunkte Permutationen . . . . .	31
	Zykel/Transposition . . . . .	32
	Zykeldarstellung von Permutationen . . . . .	33
	Young-Diagramm/Partition . . . . .	34
	Signum-Funktion/Alternierende Gruppe . . . . .	35
	Einfache Gruppe . . . . .	36
2.3	Sylow Theoreme . . . . .	38
	Sylow I . . . . .	38
	Satz von Cauchy . . . . .	40
	$p$ -Sylow Gruppe . . . . .	40
	Normalisator . . . . .	40
	Sylow II . . . . .	41
2.4	Auflösbare Gruppen . . . . .	44
	Satz von Jordan-Hölder . . . . .	45
	Abgeleitete Reihe . . . . .	47
	Auflösbarkeitskriterium . . . . .	47
	Perfekte Gruppe . . . . .	48
<b>3</b>	<b>Ringe</b>	<b>49</b>
	Ring/Einheitengruppe . . . . .	49
	Ringhomomorphismus . . . . .	49
	Unterring . . . . .	49
	Produkt von Ringen . . . . .	49
	Monoidring . . . . .	50
	Ringhomomorphismus . . . . .	50
3.1	Polynomringe . . . . .	51
	Polynomring . . . . .	52
	Primitives Monom . . . . .	53
	Grad, Liewkoeffizient, normiertes Polynom . . . . .	54
3.2	Symmetrische Polynome . . . . .	54
3.3	Elementar symmetrische Polynome . . . . .	56
3.4	Ringe von Brüchen/Lokalisierung . . . . .	61
3.5	Spezielle Ideale . . . . .	64
3.6	Teilbarkeit in Integritätsbereichen . . . . .	65
<b>4</b>	<b>Körper</b>	<b>72</b>
4.1	Grundlagen . . . . .	72
4.2	Algebraische und transzendente Elemente . . . . .	75
4.3	Normale Erweiterungen und Zerfällungskörper . . . . .	82
4.4	Seperabilität . . . . .	84
<b>5</b>	<b>Galoistheorie und Anwendungen</b>	<b>87</b>
5.1	Galoistheorie und Anwendungen . . . . .	87
5.2	Beispielklassen von Galoiserweiterungen . . . . .	92
	5.2.1 Endliche Körper . . . . .	92
	5.2.2 Einheitswurzelkörper (Kreisteilungskörper) . . . . .	92

5.2.3	Galoiserweiterungen von Grad $p$ (eine Primzahl) . . . . .	93
5.3	Auflösbarkeit durch Radikale . . . . .	95
5.4	Konstruierbarkeit mit Zirkel und Lineal . . . . .	96
5.5	Anwendungen . . . . .	98

# Kapitel 1

## Gruppentheorie

### 1.1 Gruppen und Monoide

**Notation.**

- $\mathbb{N} = \{1, 2, \dots\}$
- $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$
- $\#X$  = die Kardinalität/Mächtigkeit einer Menge  $X$

**Definition 1.1 (Monoid).** Ein Tripel  $(M, e, \circ)$  mit

- $M$  einer Menge.
- $e$  einem Element aus  $M$ ,
- $\circ : M \times M \rightarrow M$  einer zweistelligen Verknüpfung

heißt **Monoid** falls gilt

(M1) Assoziativität:

$$\forall a, b, c \in M : (a \circ b) \circ c = a \circ (b \circ c)$$

(M2) Neutrales Element:

$$\forall a \in M : a \circ e = a = e \circ a$$

Wir nennen ein  $a \in M$  **invertierbar**, falls

$$\exists b, b' \in M : b \circ a = e = a \circ b'$$

( $b$  bzw.  $b'$  heißen dann Links- bzw. Rechtsinverse)

**Bemerkung.**  $b = b'$ , denn

$$b' = e \circ b' = (b \circ a) \circ b' = b \circ (a \circ b') = b \circ e = b$$

**Definition 1.2 (Gruppe).** Eine **Gruppe** ist ein Monoid, in dem alle Elemente invertierbar sind.

**Bemerkung 1.3** (zur Assoziativität). Seien  $a_1, \dots, a_n \in M$ , und setzt man in

$$a_1 \circ \dots \circ a_n$$

Klammern, sodass  $\circ$  jeweils 2 Elemente verknüpft, so ist wegen (M1) das Ergebnis unabhängig von der Wahl der Klammerung, and also lässt man i.a. die Klammern weg. (Die Reihenfolge ist aber schon wichtig!)

**Definition 1.4 (Abelsche Gruppe/Monoid).** Ein Monoid bzw. eine Gruppe  $M$  heißt **abelsch** (oder kommutativ) :  $\iff \forall a, b \in M :$

$$a \circ b = b \circ a$$

**Proposition 1.5** (Eindeutigkeit des neutralen Elements bzw. der neutralen Elementen). *Sei  $M$  ein Monoid, dann*

(a) *Erfüllt  $e' \in M$  die Bedingung  $e' \circ a = a \forall a \in M$ , so gilt  $e' = e$ .*

(b) *Ist  $a \in M$  invertierbar, so ist sein Inverses eindeutig.*

*Beweis.*

(a) Nach Konstruktion  $e = e' \circ e = e'$ .

(b) Gelte  $a \circ b' = e$  und  $b$  sei ein Inverses von  $a$ , dann:

$$b' = e \circ b' = (b \circ a) \circ b' = b \circ (a \circ b') = b \circ e = b.$$

□

**Satz 1.6** (ohne Beweis (Jantzen-Schwermer 1.4)). *Sei  $(G, e, \circ)$  ein Tripel mit  $G$  eine Menge,  $e \in G$ ,  $\circ : G \times G \rightarrow G$  eine assoziative Verknüpfung sodass:*

- *$e$  ist Linkseins, d.h.*

$$\forall g \in G : e \circ g = g$$

- *jedes  $g$  hat ein Linksinverses*

$$\forall g \in G \exists h \in G : h \circ g = e$$

*So ist  $(G, e, \circ)$  eine Gruppe.*

**Hinweis** (Nutzen von Satz 6). Es müssen weniger Axiome geprüft werden.

**Notation.**

(i)  $ab := a \circ b$

(ii)  $a^0 = e, a^1 = a, a^{n+1} = a^n a, n \in \mathbb{N}$

(iii)  $a^n = (a^{-n})^{-1}, n < 0$

(iv) Ist  $\circ$  kommutativ, so schreibt man oft  $+$

**Übung** (Rechenregeln).

- (i)  $a^n a^m = a^{n+m}, (a^n)^m = a^{nm}, \forall m, n \in \mathbb{N}_0$
- (ii) Ist  $a$  invertierbar, so gelten die Regeln  $\forall n, m \in \mathbb{Z}$

**Proposition 1.7** (Übung). Sei  $G$  eine Gruppe, seien  $g, h \in G$ , dann:

- (a) Die Gleichung  $xg = h$  besitzt genau eine Lösung (in  $G$ ), nämlich  $x = hg^{-1}$ .
- (b) Es gilt  $(gh)^{-1} = h^{-1}g^{-1}$
- (c) Die Rechtstranslation (um  $g$ )  $r_g : G \rightarrow G, x \mapsto xg$  und die Linkstranslationen (um  $g$ )  $\ell_g : G \rightarrow G, x \mapsto gx$  sind bijektiv.

**Beispiel.** 1)  $(\mathbb{N}_0, 0, +), (\mathbb{N}_0, 1, \cdot)$  sind kommutative Monoide.

2) Jede Gruppe ist ein Monoid.

3) Ist  $X$  eine Menge,  $\text{Abb}(X, X)$  bzw.  $\text{Bij}(X, X)$  die Menge aller Abbildungen bzw. Bijektionen von  $X$  in sich, so gilt:

- (a)  $(\text{Abb}(X, X), \text{id}_X, \circ)$  ist ein Monoid.
- (b)  $(\text{Bij}(X, X), \text{id}_X, \circ)$  ist eine Gruppe.

Schreibe  $S_n := \text{Bij}(\{1, \dots, n\}, \{1, \dots, n\})$  für die Gruppe der Permutationen von  $\{1, \dots, n\}$ .

4) Ist  $(V, \langle \cdot, \cdot \rangle)$  ein Euklidischer Raum, so sind

- (i)  $O(V) := \{\varphi \in \text{End}_{\mathbb{R}}(V) \mid \varphi \text{ orthogonal}\}$  und  $SO(V) := \{\varphi \in O(V) \mid \det(\varphi) = 1\}$  Gruppen.
- (ii) Ist  $V = \mathbb{R}^2$  und  $P_n := \{\cos \frac{2\pi j}{n}, \sin \frac{2\pi j}{n} \mid j = 0, \dots, n-1\}$ , dann ist
  - (a)  $C_n := \{\varphi \in SO(V) \mid \varphi(P_n) = P\}$  die Gruppe der Drehungen um 0 von Winkel  $\frac{2\pi j}{n}, (j = 0, \dots, n-1)$  und
  - (b)  $D_n := \{\varphi \in O(V) \mid \varphi(P_n) = P\}$  die Diedergruppe der Ordnung  $2n$
 (Übung)  $\#C_n = n, \#D_n = 2n$ .

Gruppen beschreiben oft Symmetrien eines geometrischen Objekts.

5) Ist  $M$  ein Monoid, so ist  $M^\times := \{a \in M \mid a \text{ invertierbar}\}$  eine Gruppe, also  $(M^\times, e, \circ)$ .

**Definition 1.8 (Ring).** Ein Ring ist ein Tupel  $(R, 0, 1, +, \cdot)$ , sodass

- (R1)  $(R, 0, +)$  eine abelsche Gruppe,
- (R2)  $(R, 1, \cdot)$  ein Monoid,
- (R3) Es gelten die Distributivgesetze

**Definition 1.9 (Ordnung einer Gruppe).** Ist  $M$  ein Monoid oder eine Gruppe, so heißt

$$\text{ord}(M) := \#M$$

die Ordnung von  $M$ .

**Definition 1.10 (Untermonoid/Untergruppe).** Seien  $M$  ein Monoid,  $G$  eine Gruppe, dann

(a)  $N \subseteq M$  heißt Untermonoid (UM) wenn:

- $e \in N$
- $\forall n, n' \in N : n \circ n' \in N$

(b)  $H \subseteq G$  heißt Untergruppe (UG) wenn:

- $e \in H$
- $\forall h, h' \in H : h \circ h' \in H$

So schreiben wir  $N \leq M, H \leq G$ .

**Übung 1.11.** (i)  $N \leq M \implies (N, e, \cdot|_{N \times N} : N \times N \rightarrow N)$  ist Monoid

(ii)  $H \leq G \implies (H, e, \cdot|_{H \times H} : H \times H \rightarrow H)$  ist Monoid

**Beispiel.** Sei  $K$  ein Körper, dann ist

- (i)  $SL_n(K) \leq GL_n(K)$
- (ii)  $SO(V) \leq O(V) \leq \text{Aut}_{\mathbb{R}}(V)$

**Proposition 1.12 (Übung).** Sind  $(H_i)_{i \in I}$  Untergruppen von  $G$ , so ist

$$\bigcap_{i \in I} H_i \leq G.$$

**Beispiel.** Sei  $G$  eine Gruppe,  $g \in G, S \leq G$ , dann:

(i)  $C_G(g)$  **Zentralisator** von  $g \in G$ , also

$$C_G(g) = \{h \in G \mid hg = gh\} \leq G$$

(ii)  $C_G(S)$  **Zentralisator** von  $S$ , also

$$C_G(S) = \{h \in G \mid hs = sh \forall s \in S\} = \bigcap_{s \in S} C_G(s) \leq G$$

(iii)  $Z(G)$  **Zentrum** von  $G$ , also

$$Z(G) = C_G(G) \underset{\text{komm.}}{\leq} G$$

(iv) (Übung)  $Z(GL_n(K)) = K^\times \mathbf{1}_n$

**Lemma 1.13.** Sei  $G$  eine Gruppe und  $S \subseteq G$  eine Teilmenge, dann  $\exists$  kleinste Untergruppe  $\langle S \rangle \leq G$ , die  $S$  umfasst.

*Beweis.* Definiere

$$\langle S \rangle := \bigcap \{H \leq G \mid S \subseteq H\}.$$

□



**Übung 1.14.** Sei  $M$  ein Monoid,  $S \subseteq M$  eine Teilmenge, ein Wort aus  $S$  ist ein Ausdruck

$$s_1 \cdot \dots \cdot s_n, s_i \in S, n \in \mathbb{N}$$

Dann gilt:  $\{\text{Worte in } S \cup \{e\}\} = \langle S \rangle \leq M$  ist das kleinste Untermonoid von  $M$ , das  $S$  umfasst. Und ist  $G$  eine Gruppe, so gilt  $\{\text{Worte in } S \cup S^{-1} \cup \{e\}\} = \langle S \rangle \leq G$  ist die kleinste Untergruppe von  $G$ , die  $S$  umfasst.

**Definition 1.15 (Erzeugendensystem).** Sei  $G$  eine Gruppe und  $S \subseteq G$  eine Teilmenge.  $S$  heißt Erzeugendensystem von  $G \iff \langle S \rangle = G$ .

**Beispiel (Übung).** Seien  $E_{ij} \in M_{n \times n}(K)$  die Elementarmatrizen mit 1 an der Stelle  $(i, j)$  und 0 sonst. Dann ist

$$\{1_n + aE_{ij} \mid a \in K, i, j \in \{1, \dots, n\}, i \neq j\}$$

ein Erzeugendensystem von  $SL_n(K)$  (Gauß-Algorithmus)

**Lemma 1.16.** Sei  $G$  eine Gruppe,  $g \in G$ , dann gilt

$$\langle g \rangle = \langle \{g\} \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

*Beweis.* (Nach Übung 14)

$$\begin{aligned} \langle \{g\} \rangle &= \{\text{Worte in } \{g, g^{-1}, e\}\} \\ &= \{g^{i_1}, \dots, g^{i_n} \mid n \in \mathbb{N}, i_1, \dots, i_n \in \{0, \pm 1\}\} \\ &= \{g^{i_1 + \dots + i_n} \mid n \in \mathbb{N}, i_1, \dots, i_n \in \{0, \pm 1\}\} \\ &= \{g^n \mid n \in \mathbb{Z}\} \end{aligned}$$

□

**Bemerkung.**  $\langle g \rangle$  ist abelsch.

**Definition 1.17 (Ordnung eines Gruppenelements, Zyklische Gruppe).** Sei  $G$  eine Gruppe,  $g \in G$

(a) Die Ordnung von  $g$  ist

$$\text{ord}(g) = \#\langle g \rangle = \#\{g^n \mid n \in \mathbb{Z}\} \in \mathbb{N} \cup \{\infty\}$$

(b)  $g$  hat endliche Ordnung  $\iff \text{ord}(g) \in \mathbb{N}$

(c)  $G$  ist zyklisch  $\iff \exists g \in G : G = \langle g \rangle$

**Proposition 1.18.** Zyklische Gruppen sind abelsch.

*Beweis.*  $G$  zyklisch  $\implies \exists g \in G : G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ . Dann:

$$g^n g^m = g^{n+m} \stackrel{+ \text{ komm. in } \mathbb{Z}}{=} g^{m+n} = g^m g^n.$$

□

**Proposition 1.19.** Sei  $G$  eine Gruppe,  $g \in G, n := \text{ord}(g)$  und

$$n' = \sup\{m \in \mathbb{N} \mid e, g, g^2, \dots, g^{m-1} \text{ paarw. versch.}\}$$

Dann gelten:

(a)  $n' = \infty = \sup \mathbb{N}$  oder  $g^{n'} = e$  und  $\langle g \rangle = \{e, g, g^2, \dots, g^{n'-1}\}$ . Insbesondere ist  $n' = n$

(b) Falls  $n = \text{ord}(g) < \infty$ , so gilt für  $m, m' \in \mathbb{Z}$ :

$$g^m = g^{m'} \iff m \equiv m' \pmod{n}$$

Insbesondere ist  $g^m = e \iff n \mid m$

(c) Für  $s \in \mathbb{Z}$  gilt

$$\text{ord}(g^s) = \frac{n}{\text{ggT}(n, s)}$$

*Beweis.*

(a) Gelte  $n' < \infty$ :

Definition von  $n' \implies g^{n'} \in \{e, g, \dots, g^{n'-1}\}$  Annahme:  $g^{n'} = g^i$  für ein  $i \in \{1, \dots, n'-1\}$  Multipliziere mit  $g^{-i} \implies g^{n'-i} = g^0 = e$  und  $0 < n'-i < n'$ , d.h.  $g^{n'-i} \in \{e, \dots, g^{n'-1}\} \implies \{g^0, \dots, g^{n'-1}\}$  nicht paarweise verschieden (Widerspruch) Sei schließlich  $m \in \mathbb{Z}$  beliebig, Division mit Rest:

$$m = qn' + r : q, r \in \mathbb{Z}, 0 \leq r \leq n' - 1$$

$$\implies g^m = g^{qn'+r} = (g^{n'})^q g^r = g^r \in \{g^0, \dots, g^{n'-1}\}$$

Also:  $\langle g \rangle = \{e, \dots, g^{n'-1}\}$  sind paarweise verschieden.  $\implies \text{ord}(g) = \#\langle g \rangle = n'$

(b) Seien  $m, m' \in \mathbb{Z}$ , schreibe  $m' - m = qn' + r, (q, r \in \mathbb{Z}, 0 \leq r \leq n' - 1)$ , dann:

$$g^{m'} = g^m \iff g^{m'-m} = g^0 = e \iff g^{qn'+r} = e$$

$$\iff g = e \xrightarrow[e, \dots, g^{n'-1} \text{ paarw. versch.}]{1, \overset{n=n'}{\iff}} r = 0$$

$$\iff m' - m \text{ ist Vielfaches von } n = n' \iff m \equiv m' \pmod{n}$$

(c) Bestime die  $m \in \mathbb{Z}$  mit  $(g^s)^m = e$

$$(g^s)^m = e \iff g^{sm} = e \iff n \mid sm$$

$$\iff \frac{n}{\text{ggT}(n, s)} \mid \frac{s}{\text{ggT}(n, s)} m \iff \frac{n}{\text{ggT}(n, s)} \mid m$$

Da  $\frac{n}{\text{ggT}(n, s)}, \frac{s}{\text{ggT}(n, s)}$  teilerfremd sind

$$\xrightarrow{2.} \text{ord}(g^s) = \frac{n}{\text{ggT}(n, s)} \quad \square.$$

□

**Beispiel.**

$$\text{ord}(g) = 6 \implies \text{ord}(g^2) = 3 = 6/\text{ggT}(6, 2) = 6/2$$

**Korollar 1.20.** Sei  $G$  eine Gruppe, dann

(a) Für  $g \in G$  gilt:

$$\text{ord}(g) = \infty \iff g^n, n \in \mathbb{Z} \text{ sind paarw. verschieden}$$

(b) Ist  $G$  zyklisch und  $G \leq G$  eine Untergruppe, so ist  $H$  zyklisch.

*Beweis.*

(a)  $\Leftarrow$  vgl. 19(a)  $\implies$  wissen nach 19(a), dass  $e, g, \dots, g^n, \dots$  paarw. versch. sind. Multipliziere mit  $g^{-m}, (m \in \mathbb{N}) \implies g^{-m}, g^{-m+1}, \dots, g^0, g^1, \dots$  sind paarw. versch.

(b) Sei  $g \in G$  ein Erzeuger von  $G, H \leq G$  eine UG von  $G$  und ohne Einschränkung  $H \supsetneq \{e\}$

$$\implies \exists m \in \mathbb{Z} \setminus \{0\} : g^m \in H \setminus \{e\}$$

$$H \text{ ist Gruppe} \implies g^m, (g^m)^{-1} = g^{-m} \in H$$

Sei  $t \in \min\{m \in \mathbb{N} \mid g^m \in H\}$ . Behauptung:  $\langle g^t \rangle = H$ .

- " $\subseteq$ ": Klar, da  $g^t \in H$  also auch  $\langle g^t \rangle \subseteq H$  ( $H$  ist UG die  $t$  enthält)
- " $\supseteq$ ": Sei  $g^m \in H$ , Division mit Rest:  $m = tq + r : q, r \in \mathbb{Z}, 0 \leq r \leq t-1$

$$\implies H \ni g^m = g^{tq+r} = \underbrace{(g^t)^q}_{\in H} g^r \implies g^r = (g^m)((g^t)^q)^{-1} \in H$$

Nach Def von  $t$  muss gelten:  $r = 0$ , da  $r = 1, \dots, t-1$  verboten. Also ist  $g^m = (g^t)^q \in \langle g^t \rangle$ .

□

**Korollar 1.21** (Übung). Untergruppen von  $\mathbb{Z}$  sind die Mengen  $\mathbb{Z}n = \{an \mid a \in \mathbb{Z}\}, (n \in \mathbb{N}_0)$

**Wiederholung** (Vorbereitung).

- Äquivalenzrelationen
- Äquivalenzklassen
- Repräsentantensysteme

**Bemerkung.**

- $X = \bigsqcup_{r \in \mathcal{R}} [r]_{\sim}$
- Falls  $\#X < \infty : \# = \sum_{r \in \mathcal{R}} \#[r]_{\sim}$

**Satz 1.22** (Satz von Lagrange). Sei  $G$  eine endliche Gruppe und  $H \leq G$  eine Untergruppe, dann gilt  $\#H \mid \#G$ .

*Beweis.*

- 1) Definiere  $\sim$  auf  $G$  durch  $g \sim g' : \iff \exists h \in H : g' = gh \sim$  ist eine Äquivalenzrelation:

- reflexiv:  $g \sim g$  denn  $g = ge, e \in H$
- symmetrisch: gelte  $g' = gh$  für ein  $h \in H$

$$\xRightarrow{h^{-1}} g'h^{-1} = g \xRightarrow{H \text{ Gruppe}} h^{-1} \in H \implies g' \sim g$$

- transitiv: gelte  $g \sim g', g' \sim g'',$  d.h.  $\exists h \in H : g' = gh, \exists h' \in H'' g'' = g'h$

$$\implies g'' = g'h' = (gh)h' = g(hh') \implies g \sim g''$$

- 2) Äquivalenzklassen: Für  $g \in G$  ist

$$[g]_{\sim} = \{g' \in G \mid \exists h \in H : g' = gh\} = \{gh \mid h \in H\} =: gH$$

- 3) Beachte  $G$  endlich  $\implies H \subseteq G$  endlich (und ebenso jede Teilmenge von  $G$ )  
Behauptung:  $\#gH = \#H \forall g \in G$  Grund: Die Abbildungen

$$\ell_g : H \rightarrow gH, h \mapsto gh, \ell_{g^{-1}} : gH \rightarrow H, x \mapsto g^{-1}x$$

sind zueinander invers (Übung) und also bijektiv.  $\implies \#H = \#gH$ .

- 4) Sei  $\mathcal{R} \subseteq G$  ein Repräsentantensystem zu  $\sim$

$$\begin{aligned} \implies \#G &= \sum_{g \in \mathcal{R}} \#[g]_{\sim} = \sum_{g \in \mathcal{R}} \#gH = \sum_{g \in \mathcal{R}} \#H \stackrel{3)}{=} \#\mathcal{R} \#H \\ \implies \#H &\text{ teilt } \#G. \end{aligned}$$

□

**Notation.** Seien  $G$  eine Gruppe,  $H \leq G$  eine Untergruppe und  $\sim$  wie im Beweis vom Satz 22.

- Schreibe  $G/H$  für die Menge aller Äquivalenzklassen also für  $\{gH \mid g \in G\}$
- Schreibe  $[G : H] := \#G/H = \#\mathcal{R}$  (Index von  $H$  in  $G$ )

Lagrange sagt:  $\#G = \#G/H \cdot \#H = [G : H] \cdot \#H$

**Übung 1.23.** Seien  $H' \leq H \leq G$  Untergruppen, dann ist  $H' \leq G$  und

$$[G : H'] = [G : H] \cdot [H : H']$$

**Korollar 1.24.** Sei  $G$  eine endliche Gruppe, dann gelten:

- (a)  $\forall g \in G : \text{ord}(g) \mid \text{ord}(G) = \#G$   
(b) Ist  $\text{ord}(G)$  eine Primzahl, so ist  $G$  zyklisch

*Beweis.*

- (a)  $\langle g \rangle \leq G$  ist eine Untergruppe  $\xRightarrow{\text{Lagrange}} \text{ord}(g) = \#\langle g \rangle \mid \#G = \text{ord}(G)$

- (b) Sei  $p = \text{ord}(G) \in \mathbb{P}$  eine Primzahl, sei  $g \in G \setminus \{e\}$  ( $\#G \geq 2$ ) Nach 1. gilt  
 $\underbrace{\text{ord}(g)}_{\neq 1 \text{ da } g \neq e} \mid \text{ord}(G) = p$

Folglich:  $p = \text{ord}(g) = \text{ord}(G)$ , d.h.  $\langle g \rangle \leq G$  ist Inklusion gleichmächtiger endlicher Mengen, also  $\langle g \rangle = G$ .  $\square$

**Definition 1.25 (Gruppenexponent).** Sei  $G$  eine Gruppe, der Exponent von  $G$  ist  $\exp(G) = \min\{n \in \mathbb{N} \mid \forall g \in G : g^n = e\}$  (wobei  $\min \emptyset = \infty$ ).

**Beispiel (Übung).**

- (i)  $\exp(C_n) = n$
- (ii)  $\exp D_n = \text{kgV}(2, n)$
- (iii)  $\exp(S_3) = 6$
- (iv)  $\exp(S_4) = 12$
- (v)  $\exp(G) = 2 \implies G$  abelsch
- (vi)  $\mathbb{F}_p$  Körper mit  $p$  Elementen und  $0 \neq V$  ein  $\mathbb{F}_p$ -Vektorraum, so gilt  $\exp(V, 0, +) = p$

**Satz 1.26.** Sei  $G$  eine endliche Gruppe, es gelten

- (a)  $\exp(G) \mid \text{card}(G)$
- (b)  $\exp(G) = \text{kgV}(\{\text{ord}(g) \mid g \in G\})$

*Beweis.*

- (a) Folgt aus (b) und  $\text{ord}(g) \mid \text{ord}(G) \forall g \in G$  nach Korollar 24.
- (b)  $\text{ord}(g) \mid \exp(G), \forall g \in G$ , denn nach Definition gilt:

$$g^{\exp(G)} = e \xRightarrow{19} \text{ord}(g) \mid \exp(G)$$

folglich:  $N := \text{kgV}(\{\text{ord}(g) \mid g \in G\})$  teilt  $\exp G$ .

Behauptung:  $\exp G \leq N$ , (dann fertig)

Wir zeigen:  $g^N = e \implies \exp G \leq N$ . Dies folgt aus  $g^{\text{ord}(g)} = e$  und  $\text{ord}(g) \mid N = \text{kgV}(\dots)$ .  $\square$

**Übung 1.27.** Sei  $G$  eine endliche Gruppe, dann gelten:

- (a) Sind  $g, h \in G : gh = hg$  und gilt  $\text{ggT}(\text{ord}(g), \text{ord}(h)) = 1$ , so gilt

$$\text{ord}(gh) = \text{ord}(g)\text{ord}(h)$$

- (b) Gelte  $p^f \mid \exp G$  für  $p$  eine Primzahl und  $f \in \mathbb{N}$ , dann  $\exists g \in G : \text{ord}(g) = p^f$
- (c) Ist  $G$  abelsch, so  $\exists g \in G : \exp(G) = \text{ord}(g)$

**Satz 1.28.** Sei  $G$  eine endliche abelsche Gruppe, dann ist  $G$  genau dann zyklisch, wenn  $\text{ord}(G) = \exp(G)$

*Beweis.*

- “ $\implies$ ”: Sei  $g \in G$  Erzeuger  $\xRightarrow{19} \text{ord}(G) = \text{ord}(g)$

$$\text{ord}(g) \mid \exp G, \exp G \mid \text{ord}(G) \implies \exp G = \text{ord}(G)$$

- “ $\Leftarrow$ ”: Wähle nach 27.3 ein  $g \in G$  mit  $\text{ord}(g) = \exp(G)$ , nach Voraussetzung ist  $\exp(G) = \text{ord}(g) \implies \text{ord}(g) = \text{ord}(G) \implies \langle g \rangle \subseteq G$  ist Gleichheit, d.h.  $\langle g \rangle = G$ .

□

## 1.2 Gruppenhomomorphismen

Seien im Weiteren  $M, M'$  Monoide und  $G, G'$  Gruppen.

**Definition 1.29 (Monoid-/Gruppenhomomorphismus).**

(a) Eine Abbildung  $\varphi : M \rightarrow M'$  heißt **Monoidhomomorphismus**, falls

- (i)  $\varphi(e) = e'$  und
- (ii)  $\forall m, \tilde{m} \in M : \varphi(m \circ \tilde{m}) = \varphi(m) \circ' \varphi(\tilde{m})$

(b) Sind  $M, M'$  Gruppen, so heißt ein Gruppenhomomorphismus  $\iff$  (ii) gilt.

**Bemerkung 1.30.**

- (a) Ist  $\varphi : M \rightarrow M'$  ein Gruppenhomomorphismus, so gilt  $\varphi(e) = e'$  und  $\varphi(m^{-1}) = \varphi(m)^{-1}, \forall m \in M$ .
- (b) (Übung) Die Verkettung von Monoid- bzw. Gruppenhomomorphismen ist wieder ein solcher.

*Beweis.* Zu (a):

$$e' \circ' \varphi(e) = \varphi(e) = \varphi(e \circ e) = \varphi(e) \circ' \varphi(e)$$

Kürzen  $\implies e' = \varphi(e)$ . Und

$$\varphi(m^{-1}) \circ' \varphi(m) = \varphi(m^{-1} \circ m) = \varphi(e) = e'$$

Eindeutigkeit des Inverses  $\implies \varphi(m^{-1}) = \varphi(m)^{-1}$ . □

**Beispiel 1.31.** (a) Für  $g \in G$  ist die Abbildung

$$\varphi : \mathbb{Z} \rightarrow G, n \mapsto g^n$$

ein Gruppenhomomorphismus mit  $\text{Bild}(\varphi) = \langle g \rangle$ .

- (b) Sei  $K$  ein Körper,  $V, W$   $K$ -Vektorräume,  $\varphi : V \rightarrow W$  ein Vektorraumhomomorphismus, dann ist

$$\varphi : (V, 0_V, +_V) \rightarrow (W, 0_W, +_W)$$

ein Gruppenhomomorphismus.

(c) Die Vorzeichenfunktion (Aus der linearen Algebra)

$$\text{sgn} : S_n \rightarrow \{\pm 1\}, \sigma \mapsto \text{sgn}(\sigma)$$

ist ein Gruppenhomomorphismus.

**Definition 1.32 (Kern/Bild).** Sei  $\varphi : G \rightarrow G'$  ein Gruppenhomomorphismus.

(a) Der Kern von  $\varphi$  ist  $\text{Kern}(\varphi) := \{g \in G \mid \varphi(g) = e'\}$

(b) Das Bild von  $\varphi$  ist  $\text{Bild}(\varphi) := \{\varphi(g) \in G' \mid g \in G\}$

**Proposition 1.33 (Übung).** Sei  $\varphi : G \rightarrow G'$  ein Gruppenhomomorphismus, dann

(a) Für  $H \leq G$  eine Untergruppe ist  $\varphi(H) \leq G'$  eine Untergruppe.

(b) Für  $H' \leq G'$  eine Untergruppe ist  $\varphi^{-1}(H') \leq G$  eine Untergruppe.

Insbesondere sind  $\text{Bild}(\varphi) \leq G'$ ,  $\text{Kern}(\varphi) \leq G$  Untergruppen.

(c)  $\varphi$  ist injektiv (ein Gruppenmonomorphismus)  $\iff \text{Kern}(\varphi) = \{e\}$ .

(d)  $\varphi$  ist surjektiv (ein Gruppenepimorphismus)  $\iff \text{Bild}(\varphi) = G'$

**Bemerkung.** (a), (b) und (d) gelten auch für Monoide.

**Definition 1.34 (Gruppenisomorphismus).** Ein Gruppenhomomorphismus  $\varphi$  ist ein Gruppenisomorphismus, wenn  $\varphi$  bijektiv ist. ( $\iff \text{Kern}(\varphi) = \{e\}$  und  $\text{Bild}(\varphi) = G'$ ).

**Bemerkung (Übung).** Definiere ein Monoidhomomorphismus analog zu Definition 24.

**Notation.** Wir schreiben  $G \cong G'$  ( $G$  ist isomorph zu  $G'$ ) wenn  $\exists$  Gruppenisomorphismus  $\varphi : G \rightarrow G'$ .

**Definition 1.35 (Gruppenautomorphismus).** (a) Ein Gruppenisomorphismus  $\varphi : G \rightarrow G$  heißt Gruppenautomorphismus.

(b)  $\text{Aut}(G) := \{\varphi : G \rightarrow G \mid \varphi \text{ ist ein Gruppenautomorphismus}\}$ .

**Bemerkung 1.36 (Übung).** (a)  $\text{id}_G : G \rightarrow G \in \text{Aut}(G)$

(b) Verkettung von Gruppenisomorphismen (oder Automorphismen) ist wieder ein solcher.

(c) Ist  $\varphi : G \rightarrow G'$  ein Gruppenisomorphismus, so gelten

(i)  $\#G = \#G'$ .

(ii)  $G$  abelsch  $\iff G'$  abelsch.

(iii)  $S \subseteq G$  ein Erzeugendensystem  $\iff \varphi(S) \subseteq G'$  ein Erzeugendensystem.

**Proposition 1.37.**  $(\text{Aut}(G), \text{id}_G, \circ)$  und  $(\text{Aut}(M), \text{id}_M, \circ)$  sind Gruppen.

*Beweis.* (Übung) Zeige:

$$\text{Aut}(G) \leq \text{Bij}(G), \text{Aut}(M) \leq \text{Bij}(M)$$

sind Untergruppen. □

**Beispiel 1.38** (Übung).

(a)  $\text{Aut}((\mathbb{Z}, 0, +)) = \{\text{id}_{\mathbb{Z}}, -\text{id}_{\mathbb{Z}}\} \cong C_2$

(b) Für  $\mathbb{Z}_n := \mathbb{Z}/(n)$  der Ring der Restklassen modulo  $n$  gilt

$$(\mathbb{Z}_n, \bar{0}, +) \cong C_n \text{ und } \text{Aut}(\mathbb{Z}_n, \bar{0}, +) \cong \mathbb{Z}_n^\times$$

z.B. Erzeuger von  $\mathbb{Z}_n$  sind Reste  $\bar{a}$ , sodass  $\text{ggT}(a, n) = 1$

(c) Sei  $G$  beliebig, zu  $g \in G$  definiere den **Konjugationsautomorphismus** (**Konjugation** mit  $g$ )

$$c_g : G \rightarrow G, h \mapsto g \circ h \circ g^{-1}$$

(i)  $c_g \circ c_{g'} = c_{g \circ g'}, \forall g, g' \in G$

(ii)  $c_e = \text{id}_G$  und  $c_g \in \text{Aut}(G), \forall g \in G$

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

(iv)  $\text{Kern}(c) = Z(G)$  (Zentrum von  $G$ ).

**Bemerkung.**  $\text{Bild}(c) =: \text{Inn}(G)$  die Gruppe der **inneren Automorphismen** von  $G$

**Lemma 1.39.** Seien  $\varphi, \varphi' : G \rightarrow G'$  Gruppenhomomorphismen. Sei  $S \subseteq G$  ein Erzeugendensystem. Dann gilt

$$\varphi(s) = \varphi'(s) \forall s \in S \iff \varphi = \varphi' \quad (*)$$

Analoge Aussage gilt für Monoide

*Beweisskizze.* (Übung)

• “ $\Leftarrow$ ”: Klar.

• “ $\Rightarrow$ ”:

1) Zeige  $H := \{g \in G \mid \varphi(g) = \varphi'(g)\} \leq G$  ist eine Untergruppe.

2) Da  $S \subseteq H$  nach Definition von  $H$  und Voraussetzung von “ $\Rightarrow$ ”, folgt  $G = \langle S \rangle \subseteq H \leq G$ . □

## 1.3 Normalteiler

**Notation.** Für  $X \subseteq G$  und  $g \in G$  setze

$$\ell_g(X) = \{gx \mid x \in X\} = gX \text{ und } r_g(X) = \{xg \mid x \in X\} = Xg$$

Gruppenverknüpfung assoziativ  $\implies$



$$(i) \quad c_g(X) = \{gxg^{-1} \mid x \in X\} = (gX)g^{-1} = g(Xg^{-1}).$$

$$(ii) \quad g(hX) = (gh)X \text{ und } (Xg)h = X(gh).$$

**Bemerkung.** Ist  $H \leq G$  eine Untergruppe, dann heißt  $gH$  **Linksnebenklasse** und  $Hg$  **Rechtsnebenklasse**.

**Definition 1.40 (Normalteiler).** Eine Untergruppe  $N \leq G$  heißt Normalteiler (N.T.)  $\iff \forall g \in G : Ng = gN$ . (Diese Definition ist auch für Monoide sinnvoll)

**Lemma 1.41.** Für eine Untergruppe  $N \leq G$  sind äquivalent:

$$(i) \quad \forall g \in G : gN = Ng$$

$$(ii) \quad \forall g \in G : gNg^{-1} = N$$

$$(iii) \quad \forall g \in G : gNg^{-1} \subseteq N$$

*Beweis.* • “(ii)  $\implies$  (iii)”: Klar.

- “(iii)  $\implies$  (i)”: Rechtsmultiplikation mit  $g$  liefert aus (iii):

$$(gNg^{-1})g = gN(g^{-1}g) = gNe = gN \subseteq Ng$$

Für die andere Inklusion betrachte (iii) für  $g^{-1}$ :

$$g^{-1}Ng \subseteq N \xRightarrow{\text{Linksmult. mit } g} Ng \subseteq gN$$

- “(i)  $\implies$  (ii)”: Wende auf (i) Rechtsmultiplikation mit  $g^{-1}$  an. ( $r_{g^{-1}} : G \rightarrow G$  ist eine bijektive Abbildung.)

□

**Notation.**

$H \leq G$  bedeutet  $H \subseteq G$  ist eine Untergruppe.

$H \trianglelefteq G$  bedeutet  $H \subseteq G$  ist ein Normalteiler.

**Satz 1.42.** Ist  $\varphi : G \rightarrow G'$  ein Gruppenhomomorphismus, so ist  $\text{Kern}(\varphi) \trianglelefteq G$  ein Normalteiler.

*Beweis.* Sei  $g \in G$  beliebig, zu zeigen ist  $g \circ \text{Kern}(\varphi) \circ g^{-1} \subseteq \text{Kern}(\varphi)$

Sei  $h \in \text{Kern}(\varphi)$ , zu zeigen ist  $ghg^{-1} \in \text{Kern}(\varphi)$ . Damit:

$$\begin{aligned} \varphi(ghg^{-1}) &= \varphi(g)\varphi(h)\varphi(g^{-1}) \stackrel{h \in \text{Kern}(\varphi)}{=} \varphi(g) \circ e' \circ \varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) \\ &= \varphi(gg^{-1}) = \varphi(e) = e'. \end{aligned}$$

$$\implies \text{Kern}(\varphi) \trianglelefteq G.$$

□

**Übung 1.43.**

- (a) Ist  $N' \trianglelefteq G'$  und  $\varphi : G \rightarrow G'$  Gruppenhomomorphismus, so gilt  $\varphi^{-1}(N') \trianglelefteq G$ .

- (b) Ist  $h \leq G$  eine Untergruppe mit  $[G : H] = \#G/H = 2$ , so folgt  $H \trianglelefteq G$ .
- (c) Ist  $G$  abelsch, so ist jede Untergruppe  $H \leq G$  ein Normalteiler.
- (d) Der **Kommutator** zu  $g, h \in G$  ist  $ghg^{-1}h^{-1}$ , die **Kommutatoruntergruppe** von  $G$  ist

$$[G, G] := \langle ghg^{-1}h^{-1} \mid g, h \in G \rangle$$

Es gilt  $[G, G] \trianglelefteq G$ .

**Beispiel.** Es gibt Beispiele für folgende Aussagen:

- (i)  $\exists H \leq G : H \not\trianglelefteq G$
- (ii)  $\varphi : G \rightarrow G'$  ein Gruppenhomomorphismus und  $N \trianglelefteq G$  mit  $\varphi(G) \not\trianglelefteq G'$
- (iii)  $\exists N \trianglelefteq G$  und  $H \trianglelefteq N$ , so dass  $H \not\trianglelefteq G$ .

*Beweis.*

- (i)  $G = S_3 = \text{Bij}(\{1, 2, 3\}) \supseteq H = \{\text{id}, \sigma\}$  mit  $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ . Dann  $H \leq G$  Klar, aber  $H \not\trianglelefteq G$ , denn für  $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$  gilt  $\tau\sigma\tau^{-1}$  (Übung)  $\implies \tau H \tau^{-1} \not\subseteq H$
- (ii) Betrachte  $\varphi : H \rightarrow G$  Inklusion mit  $G, H$  aus (i), dann gilt  $H \trianglelefteq H$  aber  $\varphi(H) = H$  kein Normalteiler von  $G = S_3$ .
- (iii) Später.

□

**Satz 1.44.** Sei  $N \trianglelefteq G$  ein Normalteiler, dann gelten:

- (a) Aus  $gN = g'N$  und  $hN = h'N$  für  $g, g', h, h' \in G$  folgt  $ghN = g'h'N$  und insbesondere ist die Verknüpfung

$$\circ : \underbrace{G/N}_{\{gN \mid g \in G\}} \times G/N \longrightarrow G/N, (gN, hN) \longmapsto gN \circ hN = ghN$$

wohl-definiert.

- (b)  $G/N, \underbrace{N}_{=eN}, \circ$  ist eine Gruppe.

- (c)  $gN = g'N \iff g^{-1}g' \in N$ .

- (d)  $\pi : G \rightarrow G/N, g \mapsto gN$  ist ein Gruppenhomomorphismus mit  $\text{Kern}(\pi) = N$ .

*Beweis.* (a) Es gelten (Formeln von Definition 40)

$$\begin{aligned} (gh)N &= g(hN) \stackrel{N \trianglelefteq G}{=} g(Nh) = (gN)h \\ &= (g'N)h = g'(Nh) = g'(hN) = g'(h'N) = (g'h')N \implies (a) \end{aligned}$$

(b) Überlege Gruppenaxiome.

- Assoziativität (Übung)
- Linkseins ist  $N = eN$ , denn

$$N \circ (gN) = eN \circ gN \stackrel{\text{wohl-def.}}{=} (e \circ g)N = gN$$

- Linksinverses zu  $gN$  ist  $g^{-1}N$ , denn

$$(g^{-1}N) \circ gN \stackrel{\text{nach Def.}}{=} (g^{-1}g)N \stackrel{\text{Gruppe}}{=} eN = N$$

$$(c) \quad gN = g'N \stackrel{g^{-1} \circ_-}{=} N = g^{-1}g'N \stackrel{e \in N}{\implies} N \ni g^{-1}g'e, \text{ d.h. } g^{-1}g' \in G.$$

$$g^{-1}g' \in N \stackrel{\ell_{g^{-1}g'}: N \rightarrow N}{\implies} N = g^{-1}N \stackrel{g^{-1} \circ_-}{\implies} gN = g'N$$

$\ell_{g^{-1}g'}: N \rightarrow N$  ist bijektiv.

(d)  $\pi: G \rightarrow G/N, g \mapsto gN$  ist Gruppenhomomorphismus, denn

$$\pi(gg') = gg'N \stackrel{\text{Def. von } \circ}{=} gN \circ g'N = \pi(g) \circ \pi(g')$$

$$g \in \text{Kern}(\pi) \iff gN = eN \stackrel{(c)}{\iff} e^{-1}g = g \in N$$

□

**Bemerkung** (Bezeichnung).  $G/N$  (bzw.  $(G/N, eN, \circ)$ ) heißt **Faktorgruppe** von  $G$  modulo  $N$ .

**Bemerkung** (Übung).  $G$  abelsch  $\implies G/N$  abelsch.

## 1.4 Homomorphiesatz für Gruppen

**Satz 1.45** (Homomorphiesatz für Gruppen). Sei  $\varphi: G \rightarrow G'$  ein Gruppenhomomorphismus mit  $N = \text{Kern}(\varphi)$ , dann existiert genau ein Gruppenhomomorphismus  $\bar{\varphi}: G/N \rightarrow G'$ , sodass

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi \downarrow & \nearrow \bar{\varphi} & \\ G/N & & \end{array}$$

kommutiert, d.h.  $\bar{\varphi} \circ \pi = \varphi$ . (wobei  $\pi: G \rightarrow G/N, g \mapsto gN$  aus Satz 44). Die Abbildung  $\bar{\varphi}$  ist injektiv und  $\bar{\varphi}$  bijektiv  $\iff \varphi$  surjektiv.

*Beweis.* • Existenz von  $\bar{\varphi}$ : Definiere  $\bar{\varphi}(gN) = \varphi(g), \forall g \in G$ .

- $\bar{\varphi}$  wohl-definiert: Es gilt:  $gN = g'N \iff N = g^{-1}g'N \stackrel{44c}{\iff} g^{-1}g' \in N$ .  
Damit

$$\implies \varphi(g') = \varphi(gg^{-1}g') = \varphi(g)\varphi(\underbrace{g^{-1} \circ g'}_{\in N = \text{Kern}(\varphi)}) = \varphi(g)e = \varphi(g).$$

- $\bar{\varphi}$  Gruppenhomomorphismus:

$$\begin{aligned} \bar{\varphi}(gN \circ g'N) &\stackrel{\text{Def. von } \circ}{=} \bar{\varphi}(gg'N) \stackrel{\text{Def. von } \bar{\varphi}}{=} \varphi(gg') \stackrel{\varphi \text{ Hom.}}{=} \varphi(g)\varphi(g') \\ &\stackrel{\text{Def. von } \bar{\varphi}}{=} \bar{\varphi}(gN)\bar{\varphi}(g'N). \end{aligned}$$

- $\bar{\varphi} \circ \pi = \varphi$ : (Aus der Definition von  $\bar{\varphi}$ ):

$$\underbrace{\bar{\varphi}(gN)}_{\bar{\varphi}(\pi(g))} = \varphi(g)$$

- $\bar{\varphi}$  injektiv:  $\bar{\varphi}(gN) = e \iff \varphi(g) = e \iff g \in N = \text{Kern}(\varphi) \xrightarrow[44c]{\iff} gN = eN = N$ .
- $\bar{\varphi}$  eindeutig: Folgt aus der Surjektivität von  $\pi$ .
- Zusatz  $\varphi$  surjektiv  $\iff \bar{\varphi}$  Isomorphismus (Übung): Verwende  $\text{Bild}(\varphi) = \text{Bild}(\bar{\varphi})$  und  $\bar{\varphi}$  injektiv.

□

**Satz 45'** (Homomorphiesatz'). (Übung) Ist  $\varphi : G \rightarrow G'$  ein Gruppenhomomorphismus und  $N \trianglelefteq G$ , so dass  $N \subseteq \text{Kern}(\varphi)$ , dann existiert genau ein Gruppenhomomorphismus

$$\bar{\varphi} : G/N \longrightarrow G' \text{ mit } \bar{\varphi} \circ \pi = \varphi.$$

wobei  $\pi : G \rightarrow G/N, g \mapsto gN$

**Notation.** Für  $n \in \mathbb{N}$  sei  $\mathbb{Z}_n = \mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$  der Restklassenring. ( $n\mathbb{Z} \subseteq \mathbb{Z}$  eine Untergruppe)

**Korollar 1.46.** Sei  $G$  eine zyklische Gruppe,

(a) Falls  $m := \text{ord}(G) \in \mathbb{N} \implies G \cong \mathbb{Z}_m = \mathbb{Z}/(m)$ .

(b) Falls  $\text{ord}(G) = \infty \implies G \cong \mathbb{Z}$ .

*Beweis.* Sei  $g \in G$  ein Erzeuger und betrachte

$$\varphi : \mathbb{Z} \rightarrow G, n \mapsto g^n$$

$\varphi$  ist surjektiv, da  $\text{Bild}(\varphi) = \langle g^n \mid n \in \mathbb{Z} \rangle = G$ .

$$\xrightarrow[\text{Satz 45}]{\implies} \bar{\varphi} : \mathbb{Z}/\mathbb{Z}m \xrightarrow{\cong} G$$

für  $m \in \mathbb{N}_0$ , so dass  $\text{Kern}(\varphi) = \mathbb{Z}m$ .

- Fall (b):  $\text{ord}(G) = \infty \implies \text{Kern}(\varphi) = \{0\} \implies \varphi : \mathbb{Z} \rightarrow G$  ist ein Isomorphismus.
- Fall (a):  $\text{ord}(G) = m \in \mathbb{N}$  dann ist  $\bar{\varphi}$  der gewünschte Isomorphismus. □

**Korollar 1.47.** Für zyklische Gruppen  $G, H$  gilt  $G = H \iff \#G = \#H$

**Übung.** (a)  $G/[G, G]$  ist eine abelsche Gruppe.

(b) Für  $N \trianglelefteq G$  gilt:

$$G/N \text{ abelsch} \iff [G, G] \leq N$$

## 1.5 Einschub: Faktorringer

**Definition 1.48 (Ideal).** Sei  $R$  ein kommutativer Ring.  $I \subseteq R$  heißt Ideal wenn

- (i)  $I$  ist Untergruppe von  $(R, 0, +)$
- (ii)  $RI := \{ri \mid r \in R, i \in I\} \subseteq I$

**Beispiel.** 1)  $\mathbb{Z}n \subseteq \mathbb{Z}$  ist ein Ideal  $\forall n \in \mathbb{Z}$ .

2)  $Ra \subseteq R$  für  $a \in R$  ist ein Ideal von  $R$ .

**Satz 1.49.** Sei  $R$  ein kommutativer Ring,  $I \subseteq R$  ein Ideal, und  $R/I = \{r + I \mid r \in R\}$  die Nebenklassenmenge von  $R$  modulo  $I$  (für die Gruppe  $(R, 0, +)$ ). Dann:

(a) Die Verknüpfungen

$$+ : R/I \times R/I \longrightarrow R/I, (r + I, s + I) \longmapsto (r + s) + I$$

$$\cdot : R/I \times R/I \longrightarrow R/I, (r + I, s + I) \longmapsto rs + I$$

sind wohl-definiert auf  $R/I$

(b)  $(R/I, \bar{0}, \bar{1}, +, \cdot)$  ist ein kommutativer Ring ( $\bar{r} := r + I$  Notation für die Klasse von  $r$ ) der Restklassenring von  $R$  modulo  $I$ .

(c)  $\pi : R \longrightarrow R/I, r \longmapsto r + I$  ist ein surjektiver Ringhomomorphismus.

*Beweis.* (a) “+” wohl-definiert folgt aus Satz 44. ( $I \subseteq (R, 0, +)$  Ideal!)

“ $\cdot$ ” wohl-definiert: Gelte  $a + I = a' + I$  und  $b + I = b' + I$ .

$$\implies a'b' + I = ab + aj + bi + ij + I = ab + I$$

(b) (Übung)

(c) Wie in 45 (d). □

## 1.6 Die Isomorphiesätze

**Satz 1.50 (Erster Isomorphiesatz).** Sei  $G$  eine Gruppe,  $N \trianglelefteq G$  ein Normalteiler und  $H \leq G$  eine Untergruppe, dann gelten:

(a)  $HN = \{hn \mid h \in H, n \in N\} \subseteq G$  ist eine Untergruppe.

(b)  $H \cap N \subseteq H$  ist ein Normalteiler (und (Übung)  $N \trianglelefteq HN$ )

(c) Die folgende Abbildung ist wohl-definiert und ein Gruppenisomorphismus

$$H/H \cap N \longrightarrow HN/N, h(H \cap N) \longmapsto hN$$

*Beweis.* (a) Seien  $hn, h'n' \in HN$ , dann:

$$(h'n')(hn)^{-1} = h' \underbrace{n'n^{-1}h^{-1}}_{\substack{\in Nh^{-1} \\ N \trianglelefteq G} = h^{-1}N} = h'h^{-1}\tilde{n} \stackrel{H \text{ U.G.}}{=} (h'h^{-1})\tilde{n} \in HN$$

und  $e = ee = HN$

(b) Zu zeigen: für  $h \in H$  gilt  $h(H \cap N)h^{-1} \subseteq H \cap N$

Dazu:

$$\begin{aligned} h(H \cap N)h^{-1} &\subseteq hHh^{-1} = H \\ h(H \cap N)h^{-1} &\subseteq hNh^{-1} \stackrel{N \trianglelefteq G}{=} N \implies h(H \cap N)h^{-1} \subseteq H \cap N. \end{aligned}$$

(c) Betrachte die Verkettung von Gruppenhomomorphismen

$$\varphi : H \xrightarrow[h \mapsto h]{\text{Inklusion}} HN \xrightarrow[x \mapsto xN]{} HN/N$$

dann ist  $\varphi$  ein Gruppenautomorphismus.

$\varphi$  ist surjektiv: Jede Klasse in  $HN/N$  ist von der Form

$$hnN = \underbrace{hN}_{=\varphi(h)}$$

für ein  $h \in H$ . Nach Homomorphiesatz: nur noch zu zeigen  $\text{Kern}(\varphi) = H \cap N$ : für  $h \in H$ :

$$h \in \text{Kern}(\varphi) \iff \varphi(h) = eN \iff hN = eN \stackrel{44(c)}{\implies} h \in N \stackrel{h \in H}{\implies} h \in N \cap H$$

Umgekehrt:  $h \in N \cap H \implies h \in N \implies hN = eN = N$ .

□

**Satz 1.51 (Zweiter Isomorphiesatz).** Sei  $G$  eine Gruppe und  $N \trianglelefteq G$  ein Normalteiler, und sei  $\pi : G \longrightarrow G/N, g \longmapsto \bar{g} = gN$  die Faktorabbildung.

(a) Sei  $X := \{H \leq G \mid N \subseteq H\}$ , und sei  $\bar{X} := \{\bar{H} \leq G/N\}$ , dann ist die Abbildung

$$\psi : X \longrightarrow \bar{X}, H \longmapsto \pi(H) = H/N =: \bar{H}$$

eine Bijektion mit inverser Abbildung

$$\nu : \bar{X} \longrightarrow X, \bar{H} \longmapsto \pi^{-1}(\bar{H}).$$

Dabei gilt:

$$X \ni H \trianglelefteq G \iff \bar{X} \ni \pi(H) \trianglelefteq G/N$$

(b) Ist  $H \in X$  ein Normalteiler von  $G$ , so ist

$$G/H \longrightarrow \left( \left( G/N \right) / \left( H/N \right) \right), g \longmapsto \underbrace{\bar{g}}_{gN} \underbrace{\bar{H}}_{\pi(H)}$$

wohl-definiert und ein Gruppenisomorphismus.

*Beweis.* (a) Nach Proposition 33 sind  $\psi$  und  $\nu$  wohl-definiert.

- $\nu \circ \psi = \text{id}_X$ : Sei  $H \leq G$  mit  $N \subseteq H$ , zu zeigen ist  $\pi^{-1}(\pi(H)) = H$ .  
Es gilt:

$$g \in \pi^{-1}(\pi(H)) \iff \pi(g) \in \pi(H) \iff gN \in \bigcup_{h \in H} hN$$

$$\iff \exists h \in H : gNd = hN \xRightarrow{44(c)} h^{-1}g \in N \subseteq H \implies g \in hH = H.$$

(“ $\Leftarrow$ ” klar:  $g \in H \implies g \in \pi^{-1}(\pi(H))$ ).

- $\psi \circ \nu = \text{id}_{\bar{X}}$ : Für  $\bar{H} \in \bar{X}$  (d.h.  $\bar{H} \leq G/N$ ) ist zu zeigen  $\pi(\pi^{-1}(\bar{H})) = \bar{H}$ .  
Dies gilt, denn  $\pi$  ist surjektiv.
- Schließlich: Sei  $H \in X$ , zu zeigen ist  $H \trianglelefteq G \iff \pi(H) \trianglelefteq G/N$

$$H \trianglelefteq G \iff \forall g \in G : gHg^{-1} \subseteq H$$

$$\xRightarrow{\pi: G \rightarrow G/N \text{ surj.}} \forall \bar{g} \in G/N : \bar{g}\pi(H)\bar{g} \subseteq \pi(H) \implies \pi(H) \trianglelefteq \bar{G}$$

Umgekehrt: Falls  $\pi(H) \trianglelefteq \bar{G}$  und  $g \in G$ :

$$\pi(gHg^{-1}) = \bar{g}\pi(H)\bar{g}^{-1} \subseteq \pi(H)$$

$$\implies gHg^{-1} \subseteq \pi^{-1}(\pi(gHg^{-1})) \subseteq \pi^{-1}(\pi(H)) \stackrel{\nu \circ \psi = \text{id}_X}{=} H$$

(b) Sei  $H \trianglelefteq G$  ein Normalteiler mit  $N \subseteq H$ , so dass nach (a)

$$\bar{H} = \underbrace{H/N}_{\pi(H)} \trianglelefteq \underbrace{G/N}_{\pi(G)}$$

ein Normalteiler ist. Betrachte den verketteten Gruppenautomorphismus

$$\varphi : G \xrightarrow[g \mapsto gN]{\pi} G/N \xrightarrow[\bar{g} \mapsto \bar{g}\bar{H}]{\pi'} (G/N)/(H/N)$$

$\pi, \pi'$  sind surjektive Gruppenhomomorphismen nach Satz 44(d)  $\implies$  die Verkettung  $\varphi$  ist ein surjektiver Gruppenhomomorphismus.

Nach Homomorphiesatz für Gruppen bleibt zu zeigen:  $\text{Kern}(\varphi) = H$ :

$$g \in \text{Kern}(\varphi) \iff_{\pi'(\pi(g))=e} \pi(g) \in \text{Kern}(\pi') \iff gN \in H/N$$

$$\iff gN \subseteq H \iff_{N \leq H} g \in H.$$

□

## 1.7 (Semi-)direkte Produkte

**Lemma 1.52** (Übung). Seien  $(G_1, e_1, \circ_1)$  und  $(G_2, e_2, \circ_2)$  Gruppen, dann ist  $G = (G_1 \times G_2, (e_1, e_2), \circ)$  eine Gruppe mit

$$(g_1, g_2) \circ (h_1, h_2) = (g_1 \circ h_1, g_2 \circ h_2)$$

Analog für  $k \geq 2$  Faktoren. Dabei sind  $G_1 \times \{e_2\} \trianglelefteq G$  und  $\{e_1\} \times G_2 \trianglelefteq G$  Normalteiler von  $G$ .

**Definition 1.53 (Direktes Produkt).** Die Gruppe  $G$  aus Lemma 52 heißt das direkte Produkt von  $G_1$  und  $G_2$ , Notation  $G_1 \times G_2$ .

**Beispiel.**

$$(\mathbb{R}^n, \underline{0}, +) = (\mathbb{R}, 0, +) \times \cdots \times (\mathbb{R}, 0, +) = \bigtimes_{i=1}^n (\mathbb{R}, 0, +)$$

**Proposition 1.54.** Sei  $G$  eine Gruppe, seien  $N_1, N_2 \trianglelefteq G$  Normalteiler mit  $N_1 \cap N_2 = \{e\}$ , dann gelten:

- (a)  $\forall n_1 \in N_1, n_2 \in N_2 : n_1 n_2 = n_2 n_1$
- (b)  $N_1 N_2 \trianglelefteq G$  ist ein Normalteiler in  $G$
- (c)  $\psi : N_1 \times N_2 \rightarrow N_1 N_2, (n_1, n_2) \mapsto n_1 n_2$  ist ein Gruppenisomorphismus.  
(Insbesondere gilt  $\#N_1 N_2 = \#N_1 \#N_2$ )

*Zusatz:* Gilt  $G = N_1 N_2$ , so folgt  $G \cong N_1 \times N_2$  via  $\psi$ .

*Beweis.* (a) Seien  $n_1 \in N_1, n_2 \in N_2$ , setze  $x = n_1 n_2 n_1^{-1} n_2^{-1}$ . Nun:

$$x = (n_1 n_2 n_1^{-1}) n_2^{-1} \in (n_1 N_2 n_1^{-1}) N_2 \subseteq N_2 N_2 = N_2$$

analog

$$x = n_1 (n_2 n_1^{-1} n_2^{-1}) \in N_1 (n_2 N_1 n_2^{-1}) \stackrel{N_2 \trianglelefteq G}{\subseteq} N_1 N_1 = N_1$$

damit ist  $x \in N_1 \cap N_2 = \{e\} \implies x = e \implies n_1 n_2 = n_2 n_1$ .

(b) Für  $g \in G$ :

$$g N_1 N_2 g^{-1} = g N_1 g^{-1} g N_2 g^{-1} \subseteq N_1 N_2$$

(c)  $\psi$  ist wohl-definiert: klar.  $\psi$  ein Gruppenhomomorphismus folgt aus (a)

$$\begin{aligned} \psi((n_1, n_2) \circ (n'_1, n'_2)) &= \psi((n_1 \circ n'_1, n_2 \circ n'_2)) = n_1 n'_1 n_2 n'_2 \\ &\stackrel{(a)}{=} n_1 n_2 n'_1 n'_2 = \psi(n_1, n_2) \circ \psi(n'_1, n'_2) \end{aligned}$$

$\{(e, e)\} = \text{Kern}(\psi)$ :

$$\psi(n_1, n_2) = e \iff n_1 n_2 = e \iff n_1 = n_2^{-1} \in N_1 \cap N_2 = \{e\}$$

$$\iff n_1 = n_2 = e$$

$\text{Bild}(\psi) = N_1 N_2$ . □



**Korollar 1.55** (Übung). Sei  $G$  eine endliche Gruppe. Seien  $N_1, \dots, N_k \trianglelefteq G$  Normalteiler von  $G$  und gelte:

$$(i) \quad \forall i \neq j : \text{ggT}(\#N_i, \#N_j) = 1$$

$$(ii) \quad \prod_{j=1}^k \#N_j = \#G$$

Dann ist

$$\psi : \bigtimes_{j=1}^k N_j \longrightarrow G, (n_1, \dots, n_k) \longmapsto n_1 \cdot \dots \cdot n_k = \prod_{j=1}^k n_j$$

ein Gruppenisomorphismus.

**Übung.** Spezialfall:  $n = \prod_{i=1}^k p_i^{f_i}$  für  $p_1, \dots, p_k$  paarweise verschiedene Primzahlen, dann gilt:

$$\bigtimes_i^k \mathbb{Z}/(p_i^{f_i}) \cong \mathbb{Z}/(n)$$

ist Folge von Korollar 55.

**Lemma 1.56.** Seien  $H = (H, e_H, \circ_H), N = (N, e_N, \circ_N)$  Gruppen und sei  $\varphi : H \rightarrow \text{Aut}(N)$  ein Gruppenhomomorphismus. Definiere

$$G := N \rtimes H := N \rtimes_{\varphi} H = (N \times H, \underbrace{(e_N, e_H)}_{=: e}, \circ)$$

mit  $\circ$  der Verknüpfung auf  $G$  definiert durch

$$(n_1, h_1) \circ (n_2, h_2) = (n_1 \circ_N \varphi(h_1)(n_2), h_1 \circ_H h_2)$$

Dann ist  $G$  eine Gruppe und es gelten:

- $N' := \{(n, e_H) \mid n \in N\} \cong N$  ist ein Normalteiler in  $G$ ,
- $H' := \{(e_N, h) \mid h \in H\} \cong H$  ist eine Untergruppe von  $G$ ,
- $N'H' = G$  und  $N' \cap H' = \{e\}$ ,
- $G \rightarrow H, (n, h) \mapsto h$  ist ein Gruppenepimorphismus (surj.) mit Kern  $N'$ .

**Definition 1.57 (Semi-direktes Produkt).** Die Gruppe  $G = N \rtimes H$  heißt das semi-direkte Produkt von  $N$  mit  $H$  (bezüglich  $\varphi$ ).

**Satz 1.58.** Sei  $G$  eine Gruppe,  $N \trianglelefteq G$  ein Normalteiler,  $H \leq G$  eine Untergruppe, dann gelten:

(a)  $\varphi : H \rightarrow \text{Aut}(N), h \mapsto \underbrace{(c_h|_N : N \rightarrow N, n \mapsto hnh^{-1})}_{\text{Konjugation mit } h}$  ist wohl-definiert und ein Gruppenhomomorphismus.

(b) Gelten zusätzlich (i)  $NH = G$ , (ii)  $N \cap H = \{e\}$ , so ist

$$\psi : N \rtimes_{\varphi} H \rightarrow G, (n, h) \mapsto n \circ_G h$$

ein Gruppenisomorphismus.

*Beweis.* Siehe Jantzen, Schwermer - Algebra. □

**Beispiele.**

1. Seien  $A_n = \text{Kern}(\text{sign} : S_n \rightarrow \{\pm 1\})$  die Untergruppe der geraden Permutationen und  $\tau$  eine beliebige Transposition, dann gilt:

$$S_n \cong A_n \rtimes \{\text{id}, \tau\}$$

2.  $V$  Sei ein endlich dimensionaler euklidischer Vektorraum und  $\sigma \in O(V)$  eine Spiegelung, dann gilt

$$O(V) \cong SO(V) \rtimes \{\text{id}, \sigma\}$$

3. Sei  $K$  ein Körper, dann gilt

$$\text{GL}_n(K) \cong \text{SL}_n(K) \rtimes H \cong \text{SL}_n(K) \rtimes K^\times$$

wobei

$$H = \left\{ \left( \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \mid a \in K^\times \right) \right\} \cong K^\times$$

4. Sei  $\sigma \in A_4$  ein 3-Zykel, z.B.  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ , und  $V$  ist die kleinsche Vierergruppe

$$V = \{\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \trianglelefteq A_4,$$

dann gilt

$$A_4 \cong V \rtimes \{\text{id}, \sigma, \sigma^2\}$$

*Beweis.* (Übung) eventuell noch 12 Tage warten. □

## Kapitel 2

# Gruppen Strukturtheorie

### 2.1 Strukturtheorie zu Gruppen (“Einige Aussagen”)

Sei im Weiteren  $M$  ein Monoid,  $G$  eine Gruppe und  $X$  eine Menge.

**Definition 2.1 (Wirkung).** Eine Abbildung

$$\lambda : M \times X \rightarrow X, (m, x) \mapsto m \cdot x := \lambda(m, x)$$

heißt Linkswirkung (left action, Linksoperation) von  $M$  auf  $X$ , wenn es gelten  $\forall x \in X, m, m' \in M$ :

- (i) Neutrales Element:  $e \cdot x = x$
- (ii) Assoziativität:  $m \cdot (m' \cdot x) = (m \cdot m') \cdot x$

**Bezeichnung.** Ist  $M$  eine Gruppe, so heißt  $\lambda$  auch Gruppenwirkung und  $X$  heißt Links- $M$ -Menge.

**Bemerkung.** Analog kann man auch Rechtswirkungen

$$\rho : X \times M \rightarrow X, (x, m) \mapsto x \cdot m$$

definieren. (Axiome:  $x \cdot e = x$  und  $(x \cdot m) \cdot m' = x \cdot (m \cdot m')$ )

**Bemerkung (Übung).** Jede Links- $G$ -Wirkung kann man in eine Rechts- $G$ -Wirkung überführen: zu  $\lambda : G \times X \rightarrow X$  definiere  $\rho : X \times G \rightarrow X$  durch

$$\rho(x, g) := \lambda(g^{-1}, x) \iff x \cdot g := g^{-1} \cdot x$$

**Proposition 2.2** (Alternative Beschreibung von Wirkungen).

(a) Sei  $\lambda : G \times X \rightarrow X$  eine Linkswirkung, dann ist

$$\varphi : G \rightarrow \text{Bij}(X), g \mapsto (\varphi_g : X \rightarrow X, x \mapsto gx)$$

ein wohl-definierter Gruppenhomomorphismus.

(b) Sei  $\varphi : G \rightarrow \text{Bij}(X)$  ein Gruppenhomomorphismus, dann ist

$$\lambda : G \times X \rightarrow X, (g, x) \mapsto \varphi(g)(x)$$

eine Linkswirkung von  $G$  auf  $X$ .

*Beweis.* (a) Für  $g \in G$  sei  $\varphi_g : X \rightarrow X, x \mapsto gx$ , dann gelten:  $\varphi_e : X \rightarrow X, x \mapsto ex = x$  ist  $\text{id}_X$  (Axiom (i)), und

$$(*) \quad \varphi_g \circ \varphi_{g'} = \varphi_{gg'}$$

denn  $\forall x \in X$  :

$$(\varphi_g \circ \varphi_{g'})(x) = \varphi_g(\varphi_{g'}(x)) = g(g'x) \stackrel{(ii)}{=} (gg')x = \varphi_{gg'}(x)$$

Damit folgen:

1.  $\varphi_g \circ \varphi_{g^{-1}} = \underbrace{\varphi_e}_{\text{id}_X} = \varphi_{g^{-1}} \circ \varphi_g \implies \varphi_g$  ist eine bijektive Abbildung mit Inverse  $\varphi_{g^{-1}}$ , d.h.

$$\varphi : G \rightarrow \text{Bij}(X), g \mapsto \varphi_g$$

ist wohl-definiert.

2.  $\varphi$  ist ein Gruppenhomomorphismus: folgt aus  $(*)$  (Verknüpfung in  $\text{Bij}(X)$  ist die Verkettung von Abbildungen.)

(b) Übung.

□

**Bemerkung.** (a) Das Analogon von Proposition 2 gilt auch für Monoide. Die Linkswirkungen eines Monoids  $M$  auf  $X$  entsprechen Monoidhomomorphismen  $M \rightarrow (\text{Abb}(X, X), \text{id}_X, \circ)$

(b) Eine Gruppe kann auch auf “Objekten” mit mehr Struktur als eine Menge wirken, z.B. auf eine Gruppe!

**Beispiel.**  $G$  wirkt auf eine Gruppe  $N$  heißt, man hat einen Gruppenhomomorphismus  $G \rightarrow \text{Aut}(N)$  (vgl. Lemma 1.56)

**Definition 2.3** (Eigenschaften von Wirkungen). Sei  $\lambda : G \times X \rightarrow X$  eine Linkswirkung von  $G$  auf  $X$ .

(a) Die **Bahn** zu  $x \in X$  ist  $Gx = \{gx \mid g \in G\}$ . Die Länge der Bahn zu  $x$  ist  $\#Gx$

(b)  $\lambda$  ist transitiv  $\iff \forall y, z \in X \exists g \in G : gy = z \stackrel{\text{Übung}}{\iff} \forall y \in X : Gy = X \stackrel{\text{Übung}}{\iff} \exists x \in X : Gx = X$

(c)  $\lambda$  ist  $n$ -fach transitiv ( $n \in \mathbb{N}$ ), wenn für alle Paare von  $n$ -Tupeln  $(x_1, \dots, x_n), (y_1, \dots, y_n) \in X^n$  mit  $\#\{x_1, \dots, x_n\} = \#\{y_1, \dots, y_n\}$  gilt  $\exists g \in G : gx_i = y_i, \forall i$ .

- (d) Die Wirkung heißt **treu**, wenn der induzierte Gruppenhomomorphismus  $\varphi : G \rightarrow \text{Bij}(X)$  (aus Proposition 2) injektiv ist

$$\stackrel{\text{Übung}}{\Longleftrightarrow} \forall g \in G \setminus \{e\} : \exists x \in X : \underbrace{gX \neq X}_{\varphi_g(x) \neq \text{id}_X(x)}$$

**Beispiel 2.4.**

1. Ist  $V$  ein  $K$ -Vektorraum, so wirkt das Monoid  $(K, 1, \cdot)$  auf  $V$  durch Skalarmultiplikation  $(\lambda, v) \mapsto \lambda v$
2. Die folgenden 3 Beispiele sind Linkswirkungen von  $\text{GL}_n(K)$ :
  - (i)  $\text{GL}_n(K) \times K^n \rightarrow K^n, (g, v) \mapsto gv$ . (Übung: Es gibt die Bahnen  $\{0\}, K^n \setminus \{0\}$ )
  - (ii) Sei  $\mathcal{B} = \{\text{geordnete Basen von } K^n\}$  und

$$\text{GL}_n(K) \times \mathcal{B} \rightarrow \mathcal{B}, (g, (b_1, \dots, b_n)) \mapsto (gb_1, \dots, gb_n)$$

die Wirkung ist treu und transitiv.

- (iii)  $\text{GL}_n(K) \times \text{End}_K(K^n) \rightarrow \text{End}_K(K^n), (A, B) \mapsto ABA^{-1}$  die Wirkung ist nicht treu  $Z(\text{GL}_n(K))$  wirkt trivial. (Übung: Bahnen stehen in Bijektion zu den Frobeniusnormalformen von Matrizen.)
3.  $S_n \times \{1, \dots, n\} \rightarrow \{1, \dots, n\}, (\sigma, i) \mapsto \sigma(i)$  Wirkung ist treu und  $n$ -fach transitiv.
4. Abstrakte Beispiele: Sei  $H \leq G$  eine Untergruppe.

- (i)  $\lambda : H \times G \rightarrow G, (h, g) \mapsto hg$ . Die Bahnen sind die Mengen  $Hg$ , also die Rechtsnebenklassen zu  $H$  (treu?) Menge der Rechtsnebenklassen

$$H \backslash^G := \{Hg \mid g \in G\}$$

- (ii)  $\rho : G \times H \rightarrow G, (g, h) \mapsto gh$  Bahnen = Linksnebenklassen zu  $H$  und

$$G/H = \{gH \mid g \in G\}$$

- (iii)  $c : G \times G \rightarrow G, (g, g') \mapsto gg'g^{-1}$  ist eine Linkswirkung, denn der nach Proposition 2 zugehörige Gruppenhomomorphismus ist  $c : G \rightarrow \text{Aut}(G), g \mapsto c_g$ .
- (iv)  $G \times G/H \rightarrow G/H, (g, g'H) \mapsto gg'H$  Die Klassen  $gH$  heißen Linksnebenklassen wegen der Links- $G$ -Wirkung auf ihnen.

**Proposition 2.5.** Sei  $X$  eine Links- $G$ -Menge (zu der Wirkung  $\lambda : G \times X \rightarrow X, (g, x) \mapsto gx$ ) definiere Relation  $\sim$  auf  $X$  durch

$$x \sim y \iff \exists g \in G : gx = y$$

dann gelten:

- (a)  $\sim$  ist eine Äquivalenzrelation.

(b) Die Äquivalenzklasse zu  $x \in X$  bezüglich  $\sim$  ist die Bahn  $Gx$ . Insbesondere ist  $X$  die disjunkte Vereinigung seiner Bahnen. (Ist  $(x_i)_{i \in I}$  ein Repräsentantensystem der  $G$ -Bahnen, so gilt also  $\#X = \sum_{i \in I} \#Gx_i$ )

*Beweis.* (a)  $\sim$  ist eine Äquivalenzrelation: Prüfe

- $\sim$  reflexiv:  $ex = x \implies x \sim x$ .
- $\sim$  symmetrisch: Gelte  $x \sim y$ , d.h.  $\exists g \in G : gx = y$ , dann gilt  $x = ex = g^{-1}(gx) = g^{-1}y \implies y \sim x$ .
- $\sim$  transitiv: Gelte  $x \sim y$  und  $y \sim z$ , d.h.  $\exists g, h' \in G : gx = y, g'y = z$   
 $\implies (g'g)x = g'(gx) = g'y = z \implies x \sim z$

(b) Sei  $x \in X$ , dann ist

$$\{y \in X \mid x \sim y\} = \{y \in X \mid \exists g \in G : y = gx\} = \{gx \mid g \in G\} = Gx.$$

□

**Satz 2.6 (Satz von Cayley).** Jede Gruppe  $G$  (jedes Monoid  $M$ ) ist isomorph zu einer Untergruppe (einem Untermonoid) von  $(\text{Bij}(G), \text{id}_G, \circ)$  (bzw.  $(\text{Abb}(G, G), \text{id}_G, \circ)$ ).

*Beweis.* (Für Gruppen, Rest ist eine Übung) Definiere die Wirkung  $\lambda G \times G \rightarrow G, (g, h) \mapsto gh$ , dann erhalten wir den induzierten Gruppenhomomorphismus  $\varphi : G \rightarrow \text{Bij}(G)$ , wir zeigen  $\varphi$  ist injektiv: Sei  $g \in G \setminus \{e\}$ , dann gilt  $ge = g \neq e \implies$  Wirkung treu, also  $\varphi$  ist ein Gruppenmonomorphismus. D.h.  $G$  "ist" Untergruppe von  $\text{Bij}(G)$ . □

**Definition 2.7 (Stabilisator).** Sei  $X$  eine Links- $G$ -Menge und  $x \in X$ , dann heißt

$$G_x := \text{Stab}_G(x) := \{g \in G \mid gx = x\}$$

**Stabilisator** von  $x$  (unter  $G$ ). Warnung:  $G_x \neq G \cdot x$ .

**Beispiel.**  $\text{Stab}_{S_n}(\{n\}) = \{\sigma \in S_n \mid \sigma(n) = n\} \cong S_{n-1}$  mit der üblichen  $S_n$ -Wirkung auf  $\{1, \dots, n\}$ .

**Übung.**  $G$ -Wirkung auf einer Menge  $X$  ist treu

$$\iff \bigcap_{x \in X} \text{Stab}_G(x) = \{e\}$$

**Proposition 2.8.** Sei  $X$  eine links- $G$ -Menge,  $x \in X, g \in G$ , dann gilt

(a)  $\text{Stab}_G(x) \leq G$  ist eine Untergruppe.

(b)  $\text{Stab}_G(gx) = g \text{Stab}_G(x) g^{-1}$

*Beweis.*

(a)  $e \in \text{Stab}_G(x)$ , denn  $ex = x$ . Seien  $\underbrace{g_1, g_2 \in \text{Stab}_G(x)}_{\text{bedeutet } g_1x=x, g_2x=x}$ , zu zeigen ist  $g_1^{-1}g_2 \in$

$\text{Stab}_G(x)$

$$\xrightarrow{g_1^{-1} \cdot} x = ex = g_1^{-1}g_1x = g^{-1}x$$

Damit gilt  $(g_1^{-1} \cdot g_2^{-1})x = g_1^{-1}(g_2x) = g_1^{-1}x = x$

(b) Sei  $h \in G$ , dann:

$$\begin{aligned} h \in \text{Stab}_G(gx) &\iff hgx = gx \xrightarrow{g^{-1} \cdot} g^{-1}hgx = x \\ &\iff g^{-1}hg \in \text{Stab}_G(x) \xleftrightarrow[\text{Konj. mit } g]{} h \in g \text{Stab}_G(x)g^{-1}. \quad \square \end{aligned}$$

**Proposition 2.9** (Bahngleichung). *Sei  $X$  eine links- $G$ -Menge,  $x \in X$ , dann gilt:*

- $\psi : G/G_x \rightarrow Gx, hG_x \mapsto hx$  ist wohl-definiert und eine Bijektion.
- Ist  $G$  endlich, so folgt  $\#G \cdot x = [G : G_x]$ .

*Beweis.*

- $\psi$  injektiv und wohl definiert: Seien  $g, h \in G$ , dann

$$\begin{aligned} hx = gx &\iff g^{-1}hx = x \iff g^{-1}h \in G_x \leq G \\ &\iff g^{-1}hG_x = G_x \iff hG_x = gG_x \end{aligned}$$

- $\psi$  surjektiv nach Definition von  $G \cdot x$ .
- Aussage über Mächtigkeiten:  $\psi$  bijektiv  $\implies \#G/G_x = \#G \cdot x$ .  $\square$

**Bemerkung.** Die Abbildung  $\psi$  ist ein Homomorphismus von links- $G$ -Mengen (ein Isomorphismus!),  $G/G_x$  und  $G \times x \subseteq X$  sind links- $G$ -Mengen und  $\psi$  erfüllt:

$$\psi(g \cdot hG_x) = g \cdot \psi(hG_x)$$

(beides ist  $= gx \cdot x$ )

**Definition 2.10.** Sei  $X$  eine links- $G$ -Menge,

- (a) Man sagt  $G$  operiert **frei** auf  $X \iff \forall x \in X : G_x = \{e\}$
- (b) Die Menge der **Fixpunkte** der  $G$ -Wirkung ist

$$X^G := \{x \in X \mid G_x = G\}$$

**Beispiel.**  $\text{GL}_n(K)$  operiert frei auf der Menge der geordneten Basen von  $K^n$ .

**Korollar 2.11.** *Sei  $X$  eine links- $G$ -Menge. Sei  $x_1, \dots, x_n$  ein Repräsentantensystem der Bahnen der Länge  $\geq 2$ . Dann:*

- (a)  $X = X^G \sqcup \bigsqcup_{i \in \{1, \dots, n\}} G \cdot x_i$

$$(b) \#X = \#X^G + \sum_{i \in \{1, \dots, n\}} \underbrace{[G : G_{x_i}]}_{=\#G \cdot x}$$

*Beweis.* Aus Proposition 5 folgt (a), Lemma 9 gibt (b).  $\square$

**Anwendung.** Sei  $X := G$ . Sei die  $G$ -Wirkung durch Konjugation gegeben, d.h.

$$\underbrace{g \circ h}_{\text{Wirk.}} = ghg^{-1}$$

Die Bahnen unter dieser  $G$ -Wirkung heißen **Konjugationsklassen**. Die Konjugationsklasse zu  $h \in G = X$  ist

$$Gh := \{ghg^{-1} \mid g \in G\}$$

Bahnen der Länge 1 sind Fixpunkte unter Konjugation mit allen  $g \in G$

$$= \{h \in G \mid \forall g \in G : \underbrace{ghg^{-1}}_{gh=hg} = h\} =: Z(G) \text{ das Zentrum von } G$$

Stabilisator zu  $h \in G$  (unter Konjugationswirkung)

$$= \{g \in G \mid ghg^{-1} = h\} = C_G(h) \text{ Zentralisator von } h$$

Aus Korollar 11 ergibt sich nun:

**Satz 2.12** (Klassengleichung). *Sei  $G$  endlich. Ist  $g_1, \dots, g_n$  ein Repräsentantensystem der Konjugationsklassen der Länge  $\geq 2$ , so gilt:*

$$\# \underbrace{G}_X = \# \underbrace{Z(G)}_{X^G} + \sum_{i=1}^n [G : \underbrace{C_G(g_i)}_{C_g}]$$

**Definition 2.13** ( $p$ -Gruppe). Sei  $p$  eine Primzahl, eine Gruppe  $G$  heißt  $p$ -Gruppe  $\iff \#G = p^m$  für ein  $m \in \mathbb{N}$

**Beispiel.**

$$\mathbb{Z}/(p^m) \text{ oder } U_3(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_p \right\}$$

**Korollar 2.14.** *Ist  $G$  eine  $p$ -Gruppe, so gilt  $p \mid \#Z(G)$ , (d.h.  $Z(G)$  ist nicht-trivial und also eine  $p$ -Gruppe)*

*Beweis.* Seien  $g_1, \dots, g_n$  wie im Satz 12. Dann gilt:  $C_G(g_i) < G$  ist eine echte Untergruppe. (sonst  $g_i = Z(G)$ , ist ausgeschlossen)

$$\stackrel{\text{Lagrange}}{\implies} [G : C_G(g_i)] \text{ teilt } \#G = p^m$$

ist ungleich 1!

$$\implies p \mid [G : C_G(g_i)], \forall i \in \{1, \dots, n\}$$

Klassengleichung modulo  $p$ :

$$\underbrace{0}_{\#G} \cong \#Z(G) + \sum_{i=1}^n \underbrace{0}_{[G:C_G(g_i)]} \pmod{p} \implies p \mid \#Z(G). \quad \square$$



**Übung 2.15** (Satz von Cauchy). (?) Sei  $p$  eine Primzahl und  $G$  endlich, dann gilt:

$$p \mid \#G \implies \exists g \in G : \text{ord}(g) = p.$$

( $\implies \#G$  und  $\#\exp(G)$  haben dieselben Primteiler)

Idee: Verwende Induktion über  $\#G$  und die Klassengleichung. In Induktionsschritt 2 Fälle:

1.  $\exists H < G$  echte Untergruppe mit  $p \mid \#H$
2.  $\neg \exists H < G$  echte Untergruppe mit  $p \mid \#H$

Im 2. Fall wende Klassengleichung mod  $p$  an!

## 2.2 Permutationsgruppen

Sei  $n \in \mathbb{N}$ ,  $S_n = \text{Bij}(\{1, \dots, n\})$ , Notation für  $\sigma \in S_n$ , d.h.  $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  bijektiv ist

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Dabei gilt:  $(\sigma(1), \dots, \sigma(n))$  ist eine Permutation von  $\{1, \dots, n\}$ , d.h.

$$\#\{\sigma(1), \dots, \sigma(n)\} = n$$

**Korollar 2.16.**  $\#S_n = n!$

*Beweis.* (Übung) Betrachte die möglichen “Wertetabellen” für Permutationen. □

**Definition 2.17.** Für  $\sigma, \tau \in S_n$  definiere

- (a)  $\text{supp}(\sigma) = \text{Träger von } \sigma, \text{supp}(\sigma) := \{i \in \{1, \dots, n\} \mid \sigma(i) \neq i\}$
- (b)  $\sigma$  und  $\tau$  sind **disjunkt**  $\iff \text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$

**Bemerkung.**  $\text{supp}(\sigma) = \emptyset \iff \sigma = \text{id}$

**Lemma 2.18** (Andere Interpretation des Trägers). Sei  $\sigma \in S_n$ , dann gilt für die Wirkung von  $\langle \sigma \rangle : \text{supp}(\sigma) = \text{Vereinigung der Bahnen von } \langle \sigma \rangle \text{ auf } \{1, \dots, n\} \text{ der Länge } \geq 2$ .

*Beweis.*

- “ $\subseteq$ ”: Sei  $i \in \text{supp}(\sigma) \implies \sigma(i) \neq i \implies \{i, \sigma(i), \sigma^2(i), \dots, \sigma^m(i), \dots\}$  ist Bahn von  $\langle \sigma \rangle = \{\sigma^j \mid j \in \mathbb{N}_0\} = \{\text{id}, \sigma, \dots, \sigma^{r-1}\}$  der Länge  $\geq 2$ . für  $r = \text{ord}(\sigma)$ .
- “ $\supseteq$ ”: Sei  $i \notin \text{supp}(\sigma) \implies \sigma(i) = i \implies \sigma^j(i) = i, \forall j \in \mathbb{N} \implies$  Bahn von  $i$  unter  $\langle \sigma \rangle$  ist 1-elementig.

□

**Korollar 2.19.** Für  $\sigma \in S_n$  gelten:

- (a)  $i \in \text{supp}(\sigma) \iff \sigma(i) \in \text{supp}(\sigma)$

(b) Auf jeder  $\langle \sigma \rangle$ -Bahn (durch  $i \in \{1, \dots, n\}$ ) wirkt  $\sigma$  als “zyklische Permutation”, d.h.

$$\begin{array}{c}
 i_n := i \mapsto i_2 = \sigma(i) \mapsto i_3 = \sigma^2(i) \mapsto \cdots \mapsto i_r = \sigma^{r-1}(i) \\
 \qquad\qquad\qquad \swarrow \hspace{-0.8cm} \sigma \hspace{-0.8cm} \searrow \\
 \qquad\qquad\qquad (\text{mit } \#\{1 \dots n\}=r)
 \end{array}$$

*Beweis.* (a)

$$i \in \text{supp}(\sigma) \implies \sigma(i) \neq i \underset{\sigma \text{ anwenden}}{\implies} \sigma(\sigma(i)) \neq \sigma(i) \implies \sigma(i) \in \text{supp}(\sigma)$$

Falls  $\sigma(i) \in \text{supp}(\sigma)$ , so gilt  $\sigma(\sigma(i)) \neq \sigma(i) \xRightarrow[\sigma^{-1} \text{ anwenden}]{} \sigma(i) \neq i$

(b) Sei  $r$  die Länge der Bahn durch  $i$  unter  $\langle \sigma \rangle$ . Dann sind  $i_{j+1} := \sigma^j(i), j = 0, \dots, r-1$  paarweise verschieden. Sonst  $\exists 0 \leq j_1 < j_2 \leq r-1$  mit  $\sigma^{j_1}(i) = \sigma^{j_2}(i)$

$$\sigma^{-1} \text{ anwenden} \implies i = \sigma^{j_2 - j_1}(i) \quad (*)$$

$\implies$  Bahn durch  $i$  hat höchstens  $j_2 - j_1 < r$  Elemente, die Bahn ist wegen  $(*)$

$$= \{i, \sigma(i), \dots, \sigma^{j_2-j_1}(i)\}$$

Und nun: Wiederholtes Anwenden von  $\sigma$  gibt den Zykel

$$i_1 \xrightarrow{\quad} i_2 \xrightarrow{\quad} \cdots \xrightarrow{\quad} i_r \quad \square$$

**Lemma 2.20.** Sind  $\sigma, \tau \in S_n$  disjunkt, so gilt  $\sigma\tau = \tau\sigma$ .

*Beweis.* Zeige  $\sigma \circ \tau = \tau \circ \sigma$  als Abbildungen  $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$ , sei  $i \in \{1, \dots, n\}$

- Fall 1:  $i \in \text{supp}(\sigma) \implies \sigma(i) \in \text{supp}(\sigma) \implies i, \sigma(i) \notin \text{supp}(\tau)$ . Also  $\tau(i) = i, \tau(\sigma(i)) = \sigma(i)$
- Fall 2:  $i \in \text{supp}(\tau)$  analog zu Fall 1.
- Fall 3:  $i \notin \text{supp}(\sigma) \cup \text{supp}(\tau) \implies \sigma(i) = i = \tau(i)$ .

Also  $\sigma(\tau(i)) = \sigma(i) = i = \tau(i) = \tau(\sigma(i))$ . □

(Folge:  $\sigma, \tau$  disjunkt  $\implies \text{ord}(\sigma\tau) = \text{kgV}(\text{ord}(\sigma), \text{ord}(\tau))$ )

**Definition 2.21.** Seien  $i_1, \dots, i_r \in \{1, \dots, n\}$  paarweise verschieden. Der  $r$ -Zykel ist

$$(i_1 \ i_2 \ \cdots \ i_r)(j) = \begin{cases} j & j \notin \{i_1, \dots, i_r\} \\ i_{s+1} & j = i_s \ (s \in \{1, \dots, n\}) \\ i_1 & j = i_r \end{cases}$$

2-Zykel heißen **Transposition**. Konvention:  $(\cdot) := \text{id}_{\{1, \dots, n\}}$  (leerer Zykel).  
Beachte:

(i)  $(i) = (\cdot)$  für  $i \in \{1, \dots, n\}$

(ii)  $\text{supp}(i_1 \ i_2 \ \dots \ i_r) = \begin{cases} \{i_1, \dots, i_r\} & r \geq 2 \\ \emptyset & r = 1 \end{cases}$

(iii)  $(i_1 \ i_2 \ \dots \ i_r) = (i_r \ i_1 \ i_2 \ \dots \ i_{r-1})$  (Notation ist nicht eindeutig, können Einträge zyklisch weiterschieben.) z.B.

$$(1 \ 4 \ 7) = (7 \ 1 \ 4) = (4 \ 7 \ 1) = \begin{array}{ccc} & 1 & \\ \nearrow & & \searrow \\ 7 & \longleftarrow & 4 \end{array}$$

(iv)  $\text{ord}(i_1 \ \dots \ i_r) = r$ , z.B.  $\text{ord}(1 \ 2) = 2$

**Satz 2.22 (Zykeldarstellung von Permutationen).** Sei  $\sigma \in S_n$ , seien  $I_1, \dots, I_t \subseteq \{1, \dots, n\}$  die paarweise verschiedenen Bahnen von  $\langle \sigma \rangle$  auf  $\{1, \dots, n\}$  der Länge  $\geq 2$ , dann:

(a) Für  $j \in \{1, \dots, t\} \exists!$  Zykel  $\sigma_j \in S_n$  mit  $\text{supp}(\sigma_j) = I_j$ , und  $\sigma_j|_{I_j} = \sigma|_{I_j}$

(b)  $\sigma = \sigma_1 \cdot \dots \cdot \sigma_t$  und die  $\sigma_i$  kommutieren paarweise.

(c) Die Darstellung in (b) ist eindeutig bis auf Permutation der Faktoren.

(d) Für  $\sigma$  gilt:  $\text{ord}(\sigma) = \text{kgV}(\#I_j \mid j \in \{1, \dots, t\})$

*Beweis.* (a) Sei  $r_j$  die Länge von  $I_j$ . Sei  $i_j \in I_j$ , dann ist (vgl. Beweis von Korollar 19)

$$\sigma_j := (i_j, \sigma(i_j), \sigma^2(i_j), \dots, \sigma^{r_j-1}(i_j)) \in S_n$$

ein  $r_j$ -Zykel und  $\sigma|_{I_j} = \sigma_j$

(b) Die  $(\sigma_j)$  kommutieren paarweise, denn deren Träger, die Mengen  $I_j$ , sind paarweise disjunkt.

Um  $\sigma = \sigma_1 \cdot \dots \cdot \sigma_t$  zu prüfen, wende beide Abbildungen an auf  $i \in \{1, \dots, n\}$ .

- Fall  $j \in \{1, \dots, t\} : i \in I_j$

(\*) Es gilt  $\sigma_{j'}(i) = i$  für  $j' \neq j$  (da  $I_{j'} \cap I_j = \emptyset$ )

$$\implies \sigma(i) = \sigma_j(i) \stackrel{(*)}{=} \left( \sigma_j \cdot \prod_{j' \neq j} \sigma_{j'} \right)(i)$$

$$\stackrel{\sigma_j \text{ kommutieren}}{=} (\sigma_1 \cdot \dots \cdot \sigma_j \cdot \dots \cdot \sigma_t)(i)$$

- Fall 0 :  $i \in \{1, \dots, n\} \setminus \bigcup_{j \in \{1, \dots, t\}} I_j$ . Dann:  $\sigma(i) = i$  (1-elementige Bahn).

Da  $i \notin I_j : \sigma_j(i) = i, \forall j \in \{1, \dots, t\}$ . also  $(\sigma_1 \cdot \dots \cdot \sigma_t)(i) = i = \sigma(i)$

(c) Es gelte  $\sigma = \sigma'_1 \cdot \dots \cdot \sigma'_{t'}$  mit paarweise disjunkten Zykeln  $\sigma = \sigma'_1 \cdot \dots \cdot \sigma'_{t'}$  der Länge  $\geq 2$ . Sei  $I'_{j'} := \text{supp}(\sigma'_{j'})$  für  $j' \in \{1, \dots, t'\}$ . Dann:

$$\sigma|_{I'_{j'}} = \sigma'_{j'}|_{I'_{j'}}$$

$\implies I'_{j'}$  ist Bahn von  $\langle \sigma \rangle$  der Länge  $\geq 2$ .  $\implies t' = t$  und nach Umindizieren der  $I'_{j'}$  gelte

$$I'_j = I_j \text{ für } j \in \{1, \dots, t\}$$

$$\text{und } \sigma_j|_{I_j} = \sigma|_{I_j} = \sigma'_j|_{I_j} \xrightarrow[r_j = \#I_j\text{-Zykel}]{\sigma_j, \sigma'_j \text{ sind}} \sigma_j = \sigma' j$$

(d) (Übung). □

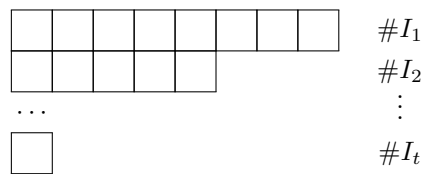
### Beispiel 2.23.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 8 & 4 & 1 & 6 & 3 & 7 \end{pmatrix} \in S_8$$

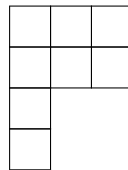
$\Rightarrow \langle \sigma \rangle$ -Bahnen:  $\{1, 2, 5\}, \{3, 8, 7\}, \{4\}, \{6\}$  und  $\sigma = (1\ 2\ 5)(3\ 8\ 7)$

**Definition 2.24 (Young-Diagramm/Partition).** Sei  $\sigma \in S_n$ , seien  $I_1, \dots, I_t$  die Bahnen von  $\langle \sigma \rangle$  (auch Bahnen der Länge 1), und gelte o.E.  $\#I_1 \geq \#I_2 \geq \dots \geq \#I_t$ .

(a) Das Young-Diagramm zu  $\sigma$  ist das Diagramm der Form:



im obigen Beispiel 23



(b) Eine Partition von  $n$  ist ein Tupel  $(n_1, \dots, n_t)$  aus  $\mathbb{N}$  mit  $n_1 \geq \dots \geq n_t$  und  $n = n_1 + \dots + n_t$ . (Young-Diagramm: Möglichkeit eine Partition zu veranschaulichen z.B. ist  $(\#I_1, \dots, \#I_t)$  eine Partition von  $n$ )

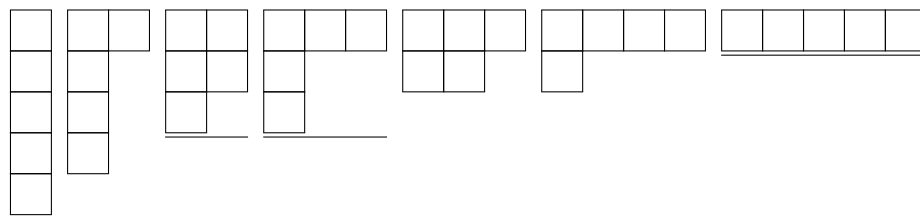
**Satz 2.25** (Übung).

(a) Seien  $i_1, \dots, i_r$  aus  $\{1, \dots, n\}$  paarweise verschiedene Elemente. Dann gilt  $\forall \sigma \in S_n$ :

$$\sigma \circ (i_1 \ i_2 \cdots i_r) \circ \sigma^{-1} = (\sigma(i_1) \ \sigma(i_2) \cdots \sigma(i_r))$$

(b)  $\sigma_1$  und  $\sigma_2$  aus  $S_n$  liegen in dieselben Konjugationsklasse  $\iff$  sie haben dasselbe Young-Diagramm.

**Beispiel.**  $S_5$  hat 7 Youngdiagramme



also auch 7 Konjugationsklassen.

**Definition (Signum-Funktion/Alternierende Gruppe).** Sei  $\text{sgn} : S_n \rightarrow \{\pm 1\}$  die Signum-Funktion aus der linearen Algebra.  $\text{sgn}$  ist eindeutig bestimmt durch:

(i)  $\text{sgn}$  ist ein Gruppenhomomorphismus.

(ii)  $\text{sgn}(\tau) = -1$ , für  $\tau$  eine Transposition.

(jedes  $\sigma \in S_n$  lässt sich schreiben als Produkt von Transpositionen)  $A_n = \text{Kern}(\text{sgn}) =$  die alternierende Gruppe auf  $n$  Elementen

$$A_n = \{\tau_1 \cdot \dots \cdot \tau_{2m} \mid \tau_i \in S_n, \text{sgn}(\tau_i) = -1, m \in \mathbb{N}\}$$

**Proposition 2.26** (Formeln für  $\text{sgn}$ ). (*Übung*)

(a) Jeder  $r$ -Zykel  $\sigma$  ist ein Produkt von  $r - 1$  Transpositionen, und also gilt  $\text{sgn}(\sigma) = (-1)^{r-1}$

(b) Hat  $\sigma$  die Zykeldarstellung  $\sigma = \sigma_1 \cdot \dots \cdot \sigma_t$  mit Zykellängen  $r_i$  (von  $\sigma_i$ ),  $i \in \{1, \dots, t\}$ , so gilt  $\text{sgn}(\sigma) = (-1)^{r_1 + \dots + r_t - t}$

**Bemerkung.** Man kann  $\text{sgn}$  durch (b) bestimmen und kann dann nachprüfen:  $\sigma$  ist ein Gruppenhomomorphismus.

**Lemma 2.27.** Sei  $C_3 = \{\sigma \in A_n \mid \sigma \text{ ist 3-Zykel}\}$  und sei  $C_{2,2} = \{\sigma \in A_n \mid \sigma = \tau_1 \cdot \tau_2 \text{ mit } \tau_1, \tau_2 \text{ disjunkt.}\}$ , dann

(a) Für  $n \geq 3$  gilt  $A_n = \langle C_3 \rangle =: H_3$

(b) Für  $n \geq 5$  gilt  $A_n = \langle C_{2,2} \rangle =: H_{2,2}$

(c) Für  $n \geq 5$  sind  $C_3$  und  $C_{2,2}$   $A_n$ -Konjugationsklassen.

*Beweis.*

$$A_n = \{\underbrace{\tau_1 \cdot \dots \cdot \tau_{2m}}_{\text{gerade Anzahl}} \mid \tau_i \in S_n \text{ Transpositionen.}\}$$

(a) Zeige:  $\tau, \tau' \in H_3$  für  $\tau, \tau'$  beliebige Transpositionen in  $S_n$

(i)  $\tau = \tau'$ :

$$\tau \cdot \tau' = \text{id} = \sigma^3 \text{ für jeden 3-Zykel } \sigma \in H_3$$

(ii)  $\tau \neq \tau'$  und  $\tau, \tau'$  nicht disjunkt:

$$\text{also } \tau = (a \ b), \tau' = (b \ c) \text{ mit } \#\{a, b, c\} = 3, a, b, c \in \{1, \dots, n\}.$$

$$\tau\tau' = (a \ b \ c) = (a \ b)(b \ c)$$

$$\begin{array}{c} a \leftarrow b \leftarrow c \\ c \leftarrow a \leftarrow b \\ b \leftarrow a \leftarrow c \end{array}$$

(iii)  $\tau \neq \tau'$  und  $\tau, \tau'$  disjunkt also  $\tau = (a \ b), \tau' = (c \ d), \#\{a, b, c, d\} = 4, \{a, b, c, d\} \subseteq \{1, \dots, n\}$ .

$$(a \ c \ b)(a \ c \ d) \stackrel{(\text{Übung})}{=} (a \ b)(c \ d)$$

(b) Zeige  $\tau \cdot \tau \in H_{2,2}$  für  $\tau, \tau' \in S_n$  Transpositionen.

- Fall (iii) trivial.
- Fall (i) trivial

$$(\tau_1 \cdot \tau_2)(\tau_1 \cdot \tau_2) \in \langle C_{2,2} \rangle = H_{2,2}$$

- Fall (ii)  $\tau = (a \ b), \tau' = (b \ c)$  (wie oben). Wegen  $n \geq 5$ , finde  $d \neq e \in \{1, \dots, n\} \setminus \{a, b, c\}$ . Dann

$$\tau \cdot \tau' = ((a \ b)(d \ e))((b \ c)(d \ e))$$

(c)  $C_3$  ist  $A_n$ -Konjugationsklasse.

Zu zeigen  $(a \ b \ c)$  ( $\{a, b, c\} \in \{1, \dots, n\}$  3 elementig) ist konjugiert zu  $(1 \ 2 \ 3)$ .

Wähle  $\sigma \in S_n$  mit  $\sigma(1) = a, \sigma(2) = b, \sigma(3) = c$ .

$$\stackrel{\text{Satz 25}}{\implies} \sigma(1 \ 2 \ 3)\sigma^{-1} \overset{(*)}{\left( \underbrace{a}_{\sigma(1)} \underbrace{b}_{\sigma(2)} \underbrace{c}_{\sigma(3)} \right)}$$

Aber  $\text{sgn}(\sigma)$  ist unklar  $+1, -1$ ?

Beachte:  $(*)$  gilt auch für  $\sigma(4 \ 5)$  und: entweder gilt  $\text{sgn}(\sigma) = 1$  oder  $\text{sgn}(\sigma(4 \ 5)) = 1 \implies (1 \ 2 \ 3) \in A_n$  konjugiert zu  $(a \ b \ c)$

Für  $C_{2,2}$ : zu zeigen  $(a \ b)(c \ d)$   $A_n$ -konjugiert zu  $(1 \ 2)(3 \ 4)$  für  $\{a, b, c, d\} \subseteq \{1, \dots, n\}$  4-elementig.

Wähle  $\sigma \in S_n$  mit  $\sigma(1) = a, \sigma(2) = b, \sigma(3) = c, \sigma(4) = d$

$$\implies \sigma(1 \ 2)(3 \ 4)\sigma^{-1} \overset{(**)}{=} (a \ b)(c \ d)$$

und  $(*)$  gilt auch für  $\sigma(1 \ 2) \dots$  etc. (Schließe wie für  $C_3$ .)

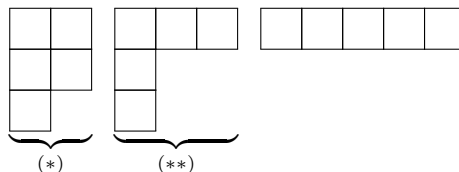
□

**Definition 2.28 (Einfache Gruppe).** Eine Gruppe  $G$  heißt **einfach**  $\iff \{e\}$  und  $G$  sind die einzigen Normalteiler von  $G$ . (d.h.  $G$  hat keine nicht-trivialen Normalteiler)

**Satz 2.29.** Für  $n \geq 5$  ist  $A_n$  einfach.

*Beweis.* Sei  $N \trianglelefteq A_n$  ein Normalteiler und  $\{e\} \subsetneq N$  und sei  $\sigma \in N \setminus \{e\}$ .

- $n = 5$ :

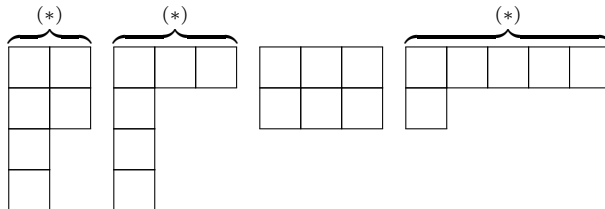


(\*) Doppeltranspositionen bilden  $A_5$ -Konjugationsklasse und erzeugen  $A_5$  (Lemma 27). Falls Doppeltranspositionen in  $N$ , so folgt  $N = A_5$ .

(\*\*) 3-Zykel bilden  $A_5$ -Konjugationsklasse und erzeugen  $A_5$  (Lemma 27). Falls  $\sigma$  ein 3-Zykel  $\implies N = A_5$ .

Gelte  $\sigma = 5$ -Zykel  $= (a \ b \ c \ d \ e)$ . Nun:  $N \ni \underbrace{(a \ b \ c)\sigma(a \ b \ c)^{-1}}_{\in N} \underbrace{\sigma}_{\in N} \stackrel{\text{Übung}}{=} (a \ b \ d)$  3-Zykel

- $n = 6$ : möglichen Youngdiagramme: (zu  $\sigma \in A_6 \setminus \{e\}$ )



(\*) wurden schon im  $A_5$ -Fall erklärt.

Sei also  $\sigma^2 = (a b c)(d e f) \in N$ , mit  $\{a, \dots, f\} = \{1, \dots, 6\}$ . Sei  $\tau = (a b c)$ , berechne  $\tau(\sigma)(\tau^{-1})$  (Satz 25)

$$\underbrace{\tau \sigma \tau^{-1}}_{\in N} \underbrace{\sigma}_{\in N} = \underbrace{(b d c)(a e f)(a c b)(e d f)}_{f \leftarrow f \leftarrow e \leftarrow e \leftarrow f} \stackrel{\text{Übung}}{=} (a b e c d) \in 5\text{-Zykel}$$

wurde schon bei  $n = 5$  geklärt.

- $n \geq 6$  : o.E. (Permutation von  $1, \dots, n$ )  $\sigma(1) \neq 1$  Wähle  $\{j, k\} \in \{1, \dots, n\} \setminus \{1, \sigma(1)\}$ . Sei  $\tau := (\sigma(1) j k) \implies \sigma^{-1} \tau \sigma \tau^{-1} \in N$  Dann:

(i)  $\varphi := \tau \sigma \tau^{-1} \sigma^{-1} \in N$

(ii)  $\varphi(\sigma(n)) = \tau \sigma \tau^{-1}(1) \stackrel{1 \notin \text{supp}(\tau)}{=} \tau \sigma(1) = j \neq \sigma(1)$ , also  $\varphi \neq \text{id}$ .

(iii)  $\# \text{supp}(\varphi) \leq 6$ , denn:

$$\varphi = \underbrace{\tau}_{3\text{-Zykel}} \cdot \underbrace{\sigma \tau^{-1}}_{3\text{-Zykel}} \sigma^{-1}$$

$$\text{o.E: } \text{supp}(\varphi) \subseteq \{1, \dots, 6\} \implies \varphi \in A_6 \setminus \{e\}$$

- Fälle  $n \leq 6$ : Nurmalteiler, der von  $\varphi$  erzeugt wird enthält 3-Zykel oder Doppeltransposition. Dann fertig wegen Lemma 27.  $\square$

**Bemerkung.** Es gibt eine Klassifikation aller endlich einfachen Gruppen: Liste:

- $\mathbb{Z}/(p), p$  prim
- $A_n, n \geq 5$
- endliche Gruppen vom Lie typ:
  - (i)  $\text{SL}_n(K)/Z(\text{SL}_n(K))$  bis auf einige kleine  $\#K$  sind einfach (endlich falls  $K$  endlich).
  - (ii) Weitere Untergruppen von  $\text{SL}_n$ , welche zu "linearen algebraischen Gruppen" korrespondieren.
- 26 weitere.

## 2.3 Sylow Theoreme

**Satz 2.30** (Sylow I, nach Wieland). *Sei  $G$  eine endliche Gruppe,  $p$  ein Primteiler von  $\#G$ ,  $k \in \mathbb{N}$  sodass  $p^k | \#G$ , setze*

$$n_k := \#\{H \leq G \mid \#H = p^k\}$$

Dann gilt:

$$n_k \equiv 1 \pmod{p}$$

Insbesondere ist  $n_k \neq 0$ , d.h.  $\exists H \leq G$  mit  $\#H = p^k$ .

**Übung** (Vorbereitung). Sei  $p$  eine Primzahl,  $k \in \mathbb{N}_0, m \in \mathbb{N}$ , dann:

$$\binom{mp^k}{p^k} = m \cdot u$$

wobei  $\mathbb{N} \ni u \equiv 1 \pmod{p}$ .

*Beweis.* (zu 30) Durch Analyse der Wirkung von  $G$  auf  $X := \{S \subseteq G \mid \#S = p^k\}$  gegeben durch

$$\lambda : G \times X \rightarrow X, (g, S) \mapsto g \cdot S = \{g \cdot s \mid s \in S\}$$

(beachte:  $\ell_g : h \mapsto g \cdot h$  ist bijektiv  $\implies \#gS = \#S = p^k$  d.h.  $g \cdot S \in X$ ) Setze  $m := \#G/p^k$ , für  $S \in X$  definiere

$$G_S := \text{Stab}_G(S) = \{g \in G \mid gS = S\}$$

1.  $\forall S \in X : \#G_S | p^k$ :

Beachte:  $G_S$  wirkt auf  $S$  (da  $gS = S \forall g \in G_S$ ) durch Linkstranslation:

$$G_S \times S \rightarrow S, (g, s) \mapsto g \cdot s$$

Schreibe  $S$  als disjunkte Vereinigung seiner  $G_S$ -Bahnen.

$$S = \bigsqcup_{i \in \{1, \dots, \ell\}} G_S h_i$$

wobei  $h_1, \dots, h_\ell$  ein Repräsentantensystem der Bahnen ist.

Beachte:  $r_{h_i} : g \mapsto gh_i$  ist bijektiv. Also folgt  $\#G_S h_i = \#G_S$

$$\implies p^k = \#S = \sum_{i=1}^{\ell} \#G_S h_i = \sum_{i=1}^{\ell} \#G_S = \ell \#G_S$$

d.h.  $\#G_S | p^k$ .

2. Sei  $X_0 := \{S \in X \mid \#G_S = p^k\}$  und  $X_1 := X \setminus X_0$

Behauptung:  $\#X_0 = m \cdot n_k$

(a) Sei  $H \leq G$  eine Untergruppe mit  $\#H = p^k$ , dann:

$$\{S \in X_0 \mid G_S = H\} = \{Hg \mid g \in G\}$$

Denn:



- “ $\subseteq$ ”: Gelte  $G_S = H$ , d.h.  $H \cdot S = S \implies H \cdot s \subseteq S, \forall s \in S$ .  
Aber:  $\#H \cdot s \underset{r_s \text{ ist bij.}}{=} \#H = p^k = \#S \implies H \cdot s = S \implies s$  (ist das gesuchte  $g$ )
- “ $\supseteq$ ”: Zu zeigen:  $\text{Stab}_G(H \cdot s) = H$ . Sei  $g \in G$ .

$$g \in \text{Stab}_G(Hs) \iff gHs = Hs \underset{r_s \text{ ist bij.}}{\iff} gH = H \underset{H \leq G}{\iff} g \in H$$

(b)

$$\begin{aligned} X_0 &= \bigsqcup_{H \leq G, \#H=p^k} \{S \in X \mid G_S = H\} \stackrel{(a)}{=} \bigsqcup_{H \leq G, \#H=p^k} \{Hg \mid g \in G\} \\ \#X_0 &= \sum_{H \leq G, \#H=p^k} \underbrace{\#\{Hg \mid g \in G\}}_{=H \setminus G} \stackrel{\text{Lagrange}}{=} \frac{\#G}{\#H} = \frac{\#G}{p^k} = m \\ &= m \left( \sum_{H \leq G, \#H=p^k} 1 \right) = m \cdot n_k \end{aligned}$$

3.  $pm \mid \#X_1$

- (a)  $G$  wirkt auf  $X_1$  (durch  $(g, S) \mapsto gS$ )  
d.h. gilt  $S \in X_1$  und  $g \in G$ , so auch  $gS \in X_1$ . Es genügt also zu zeigen:  $\#G_{gS} = \#G_S$   
Dazu:

$$G_{gS} = \text{Stab}_G(gS) = g \text{Stab}_G(S) g^{-1} = gG_S g^{-1} \underset{\substack{\text{Konj. mit } g \\ \text{ist Gruppenisom.}}}{\cong} G_S.$$

- (b) Betrachte nun  $G$ -Bahn durch  $S \in X_1$ , Behauptung:  $\#G \cdot S$  ist Vielfaches von  $p \cdot m$

Dazu: Bahngleichung:

$$\#G \cdot S = \#G / \#G_S = mp^k / \#G_S$$

da  $\#G_S$  echter Teiler von  $p^k$ , also Teiler von  $p^{k-1} \implies \#G_S$  ist Vielfaches von  $mp^k / p^{k-1} = mp$

$$(m \cdot 2^5 / 2^4 = m \cdot 2, \quad m \cdot 2^5 / 2^2 = m \cdot 2^3,)$$

- (c) Schreibe nun  $X_1$  als disjunkte Vereinigung seiner Bahnen

$$X_1 = \bigsqcup_{j \in I} G \cdot \underbrace{S_j}_{\text{Bahnrepr.}}$$

und  $\#G \cdot S_j = m \cdot p \cdot a_j, a_j \in \mathbb{N}$

$$\implies \#X_1 = \sum_{j \in J} \#G \cdot S_j = m \cdot p \cdot \underbrace{\sum_{j \in J} a_j}_{=: N \in \mathbb{N}}$$

$$4. \#X = \#X_0 + \#X_1 = m \cdot n_k + m \cdot p \cdot N = m(n_k + pN)$$

gleichzeitig:

$$\#X = \#\{S \subseteq G \mid \#S = p^k\} \stackrel{\#G=m \cdot p^k}{=} \binom{m \cdot p^k}{p^k} \stackrel{\text{Übung}}{=} m \cdot u$$

für ein  $u \in \mathbb{N} : u \equiv 1 \pmod{p}$ .

$$\implies m(n_k + pN) = n \cdot u \implies n_k + pN = u \cdot \frac{n}{m} \equiv u \equiv 1 \pmod{p}. \quad \square$$

**Korollar 2.31 (Satz von Cauchy).** Sei  $G$  eine endliche Gruppe mit  $p \mid \#G$  für  $p$  eine Primzahl, dann  $\exists g \in G : \text{ord}(g) = p$

*Beweis.* Nach Sylow I  $\exists H \leq G : \#H = p$ , sei  $g \in H \setminus \{e\}$ . Dann gilt  $\text{ord}(g) = p$ .  
( $\text{ord}(g) \neq 1$  und  $\text{ord}(g) \mid \#G = p$ ).  $\square$

**Definition 2.32 ( $p$ -Sylow Gruppe).** Sei  $G$  endlich, gelte  $\#G = p^f \cdot m$  für  $m, f \in \mathbb{N}$  sodass  $p \nmid m$ . Eine Untergruppe  $H \leq G$  mit  $\#H = p^f$  heißt  $p$ -Sylow (Unter-)Gruppe von  $G$ , schreiben

$$\text{Syl}_p(G) = \{H \leq G \mid H \text{ ist } p\text{-Sylow}\}$$

$$\text{syl}_p(G) = \#\text{Syl}_p(G)$$

**Definition 2.33 (Normalisator).** Der Normalisator einer Untergruppe  $H \leq G$  ist

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}$$

$$(c_g \text{ ist Automorphismus} \implies \#gHg^{-1} = \#H, \forall g \in G)$$

**Interpretation.** Sei  $X := \{H \mid H \leq G\}$ ,  $X$  ist eine  $G$ -Menge durch Konjugation  $c : G \times X \rightarrow X, (g, H) \mapsto gHg^{-1}$

**Proposition 2.34 (Übung).** (a)  $N_G(H) \stackrel{\text{für } H \leq G}{=} \text{Stab}_G(H)$

(Insbesondere ist  $N_G(H) \leq G$  eine Untergruppe.)

(b) Es gelten:  $H \trianglelefteq N_G(H)$  und  $N_G(H)$  ist die größte Untergruppe von  $G$ , sodass  $H$  ein Normalteiler in dieser ist.

**Lemma 2.35.** Sei  $H \leq G$  eine  $p$ -Gruppe,  $P \in \text{Syl}_p(G)$  ( $p$  eine Primzahl), dann:

(a) Gilt  $P \leq H$ , so folgt  $P = H$ .

(b) Ist  $H \leq N_G(P)$ , so gilt  $H \leq P$ .

(c) Gilt  $H \not\leq P$ , so folgt  $\text{Stab}_H(P) < H$  (ist echte Untergruppe)

*Beweis.* (a) Schreibe  $\#G = p^f \cdot m$ , so dass  $p \nmid m$  ( $m, f \in \mathbb{N}$ ),  $P$   $p$ -Sylow Untergruppe  $\implies \#P = p^f$ .

$$H \text{ eine } p\text{-Gruppe in } G \stackrel{\text{Lagrange}}{\implies} \#H \mid p^f \cdot m. \text{ also } \#H \mid p^f$$

$$\text{Nun: } P \subseteq H \text{ und } p^f = \#P \geq \#H \implies P = H \text{ (und } \#H = p^f)$$

(b) Sei  $G' = N_G(P)$ . Aus Proposition

$$\implies P \trianglelefteq G' \xrightarrow[\text{Voraussetzung}]{\text{Nach}} H \leq G' \xrightarrow[\text{Isomorphiesatz}]{\text{Erster}} P \trianglelefteq P \cdot H$$

und

$$(P \cdot H)/P \cong H/P \cap H$$

Ordnung ist  $p$ -Potenz, evtl  $p^f$

$$\xRightarrow{\text{Lagrange}} \#P \cdot H = \underbrace{\#P}_{p\text{-Potenz}} \cdot \underbrace{\#(P \cdot H)/P}_{p\text{-Potenz}}$$

Also ist  $P \cdot H$  eine  $p$ -Gruppe mit  $P \subseteq PH$

$$\xRightarrow{(a)} PH = P \xRightarrow{eH \subseteq P} H \subseteq P$$

(c) Gelte  $H \not\subseteq P$ . zu zeigen:  $\text{Stab}_H(P) < H$

$$\text{Angenommen: } H = \text{Stab}_H(P) = \underbrace{\{h \in H \mid hPh^{-1} = P\}}_{=H \cap \text{Stab}_G(P)} = H \cap N_G(P)$$

Dann folgt

$$H \subseteq N_G(P) \xRightarrow{(b)} H \subseteq G. \quad \square$$

**Satz 2.36 (Sylow II).** Sei  $G$  endlich,  $p$  ein Primteiler von  $\#G$ . Dann:

(a) Je 2  $p$ -Sylow Gruppen von  $G$  sind konjugiert.

(b) Jede  $p$ -Gruppe  $H$  mit  $H \leq G$  liegt in einer  $p$ -Sylow Gruppe von  $G$ .

(c)  $\forall P \in \text{Syl}_p(G) : \text{syl}_p(G) = [G : N_G(P)]$  und insbesondere  $(P \leq N_G(P))$  gilt  $\text{syl}_p(G) \mid [G : P]$

*Beweis.* (a)  $X := \text{Syl}_p(G)$  ist  $G$ -Menge via Konjugation ( $P \in \text{Syl}_p(G)$  und  $g \in G \implies \#gPg^{-1} = \#P \implies gPg^{-1} \in \text{Syl}_p(G)$ )

Zu zeigen:  $G$  wirkt transitiv auf  $X$ .

Annahme:  $X$  besteht aus  $t \geq 2$  Bahnen, also

$$X = \bigsqcup_{i \in \{1, \dots, t\}} G \circ P_i$$

für geeignete Repräsentantensystem  $P_1, \dots, P_t \in \text{Syl}_p(G)$  ( $g \circ P = gPg^{-1}$ )

Behauptung:  $p \mid \#G \circ P_i, \forall i \in \{1, \dots, t\}$ .

Dazu: Wähle  $j \neq i$  betrachte die  $P_j$ -Wirkung auf  $G \circ P_i$ . Schreibe wieder  $G \circ P_i$  als disjunkte Vereinigung von  $P_j$ -Bahnen:

$$G \circ P_i = P_j \circ Q_1 \sqcup \dots \sqcup P_j \circ Q_s \quad (*)$$

( $s \in \mathbb{N}$  geeignet,  $Q_\ell \in \text{Syl}_p(G)$  geeignet)

Bahngleichung:

$$\#P_j \circ Q_\ell = \#P_j / \# \text{Stab}_{P_j}(Q_\ell)$$

beachte:  $P_j \notin G \circ P_i$ , d.h.  $P_j \neq Q_\ell$

$$\xRightarrow{35(c)} \text{Stab}_{P_j}(Q_\ell) < P_j \implies \#P_j \circ Q_\ell \neq 1 \text{ und teilt } \#P_j \implies p | \#P_j \circ Q_\ell$$

$$\implies p \text{ alle Bahnlängen in } (*) \text{ von } G \circ P \text{ als } P_j\text{-Menge} \implies p | \#G \circ P_i, \forall i \implies p | \# \text{Syl}_p(G)$$

$$\implies \text{Syl}_p(G) = \bigsqcup_{i \in \{1, \dots, t\}} G \circ P_i$$

Widerspruch zu (0):  $\text{syl}_p(G) \equiv 1 \pmod{p}$ .

- (b) Annahme:  $H \leq G$  eine  $p$ -Gruppe liegt in keiner  $p$ -Sylow. Betrachte Konjugationswirkung von  $H$  auf  $X = \text{Syl}_p(G)$ . Schreibe

$$X = H \circ R_1 \sqcup \dots \sqcup H \circ R_w$$

( $w \in \mathbb{N}$ ) die  $R_i$  sind Repräsentanten der Bahnen. Beachte  $H \not\leq R_i$  ( $i \in \{1, \dots, w\}$ ). Wie in (a) gilt  $\text{Stab}_H(R_i) < H$  also, dass  $p | \#H \circ R_i, \forall i \implies p | \#X$  Widerspruch zu (0).

- (c) Bahngleichung für  $P \in \text{Syl}_p(G)$  (Verwenden (a), d.h.  $G \circ P = \text{Syl}_p(G)$ )

$$\text{syl}_p(G) = \# \text{Syl}_p(G) = \#G / \# \text{Stab}_G(P) : \#G / \#N_G(P) = [G : N_G(P)]$$

( $\text{syl}_p(G)$  teilt  $[G : P]$  schon oben eingesehen, da  $P \leq N_G(P)$ )

□

**Korollar 2.37.** Sei  $G$  endlich und  $p$  ein Primteiler von  $\#G$ , dann  $\text{syl}_p(G) = 1 \iff$  jede  $p$ -Sylow ist ein Nullteiler in  $G$ .

*Beweis.* Für  $P \in \text{Syl}_p(G)$  gilt:

$$P \trianglelefteq G \iff N_G(P) = G \xLeftrightarrow{36(c)} \text{syl}_p(G) = [G : N_G(P)] = 1. \quad \square$$

**Korollar 2.38.** Sei  $G$  endlich, seien  $p_1, \dots, p_t$  die paarweise verschiedenen Primteiler von  $\#G$ . Sei  $P_i \in \text{Syl}_{p_i}(G)$ . Dann gilt: sind  $P_1, \dots, P_t$  Normalteiler von  $G$ , so folgt: die Abbildung  $P_1 \times \dots \times P_t \rightarrow G, (g_1, \dots, g_t) \mapsto g_1 \cdot \dots \cdot g_t$  ist ein Gruppenisomorphismus.

*Beweis.*  $P_i \trianglelefteq G$  für  $i \in \{1, \dots, t\}$

und  $\text{ggT}(\#P_i, \#P_j) \stackrel{i \neq j}{=} 1$  ( $p_i, p_j$  versch. Primzahlen) und  $\prod_{i=1}^t \#P_i = \#G$

$\xRightarrow{\text{Kor. 1.55}}$  die angegebene Abbildung ist ein Gruppenisomorphismus. □

**Beispiel.** Ist  $G$  abelsch, so sind alle Untergruppen Normalteiler.

**Korollar 2.39.**  $G$  endlich abelsch und  $p_i$  und  $P_i$  wie in Korollar 38. So gilt:  $\times_{i=1}^t P_i \xrightarrow{\text{wie in Kor. 38}} G$  ist Gruppenisomorphismus. ( $P_i$  sind abelsche  $p_i$ -Gruppen).

**Satz 2.40.** Sei  $G$  eine endliche abelsche  $p$ -Gruppe, dann  $\exists! t \in \mathbb{N}, \exists! e_1 \geq e_2 \geq \dots \geq e_t \in \mathbb{N}$ , sodass

$$G \cong \times_{i=1}^t \mathbb{Z}/p^{e_i}$$

**Beispiel.**  $G$  abelsch mit  $\text{ord}(G) = 105 \implies G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$

**Wiederholung.**  $G$  heißt einfach  $\iff$  einzige Nullteiler von  $G$  sind  $\{e\}$  und  $G$ .

**Lemma 2.41** (Übung). *sei  $G$  endlich,  $\#G = p^f \cdot m$  mit  $f, m \in \mathbb{N}, p$  Primzahl und  $p \nmid m$ . Dann:  $p^f \nmid (m-1)! \implies G$  ist nicht einfach.*

*Beweis.* Idee: Sei  $P \in \text{Syl}_p(G)$ , betrachte  $G$ -Wirkung auf  $G/P$  durch Linkstranslation, d.h.

$$\rho : G \rightarrow \text{Bij}(G/P), g \mapsto \ell g$$

Trick:  $\text{Kern}(\rho)$  ist der gesuchte Normalteiler. □

**Satz 2.42.** *Ist  $G$  einfache Gruppe mit  $\#G < 60$ , so gilt  $G \cong \mathbb{Z}/p$  für  $p$  eine Primzahl.*

*Beweis.* Sei  $G$  einfach mit  $\#G < 60$ . o.E.  $\#G$  keine Primzahl, sonst fertig. o.E.  $G$  ist keine  $p$ -Gruppe für Primzahl  $p$ . (sonst:  $Z(G) \supsetneq \{e\} \xrightarrow[Z(G) \trianglelefteq G]{G \text{ einfach}} G = Z(G)$ ,

d.h.  $G$  abelsch.  $\implies G \cong \mathbb{Z}/p$ )

Fall  $\# = p^f m$  mit  $p^f \nmid (n-1)! \implies G$  nicht einfach (Lemma 41)

(Übung) Es bleiben  $\#G \in \{\underbrace{30}_{2 \cdot 3 \cdot 5}, \underbrace{40}_{2^3 \cdot 5}, \underbrace{56}_{2^3 \cdot 7}\}$

Fall 1:  $\#G = 2^3 \cdot 5$ , dann:  $\text{Syl}_5(G) \cong 1(5)$  (Sylow I)

$\text{Syl}_5(G)$  teilt  $\#G/5 = 8$  (Sylow II)

Teiler von 8 : 1, 2, 4, 8 Kongruenz erzwingt  $\text{Syl}_5(G) = 1 \xrightarrow[37]{\implies}$  die einzige

5-Sylow Untergruppe von  $G$  ist ein Normalteiler (Widerspruch zu  $G$  einfach)

Fall 2:  $\#G = 2^3 \cdot 7$ , dann (Schritte wie im Fall 1 für  $p = 7$ )

$$\text{Syl}_7(G) \in \{1, 8\}$$

(teilt 8,  $\cong 1 \pmod{7}$ )

Fall: Es gibt 8 7-Sylow Untergruppen, isomorph zu  $\mathbb{Z}/7$

Beachte: 2 7-Sylow's schneiden sich nur in  $\{e\}$  (sonst sind sie gleich, Elemente  $\neq e$  sind Erzeuger)

$\implies$  es gibt  $8 \cdot 6$  Elemente in  $G$  der Ordnung 7

$\implies$  Es gibt  $56 - 48 = 8$  Elemente in  $G$  der Ordnung  $\neq 7$

Aber: Es gibt (mindestens) eine 2-Sylow Untergruppe von  $G$  und die hat Ordnung  $8 = 2^3$ .

Es folgt: Die 8 obigen Elemente bilden die einzig mögliche 2-Sylow Untergruppe von  $G$ .

$\implies \text{Syl}_2(G) = 1 \implies$  die 2-Sylow ist ein nicht triviale Normalteiler von  $G$ .

Fall 3 (Übung) □

**Bemerkung.** Die Zahl 60 ist optimal, denn  $A_5$  ist einfach, nicht zyklisch (von Primzahlordnung) und hat 60 Elemente.

## 2.4 Auflösbare Gruppen

**Definition 2.43.**

(a) Eine aufsteigende Folge von Untergruppen

$$\{e\} = G_0 < G_1 < G_2 < \cdots < G_t = G$$

von  $G$  heißt Normalreihe (von  $G$ ), wenn  $\forall i \in \{1, \dots, t\} : G_{i-1} \trianglelefteq G_i$  ist Normalteiler.

Schreibe auch  $(G_i)_{i=0}^t$  oder  $\mathcal{G}$  für die Folge.

(b) die Faktorgruppe  $\left(G_i/G_{i-1}\right)_{i=1}^t$  heißen Faktoren der Normalreihe.

(c) Eine Normalreihe  $\mathcal{G}$  heißt Zerlegungsreihe  $\iff$  alle Faktoren sind einfach.

(d)  $\mathcal{G}$  heißt abelsch  $\iff$  alle Faktoren sind abelsch.

(e)  $G$  heißt auflösbar  $\iff G$  besitzt eine abelsche Normalreihe.

(f) Ist  $\mathcal{G}' : \{e\} = G'_0 < G'_1 < \cdots < G'_{t'} = G$  eine weitere Normalreihe, so heißt  $\mathcal{G}'$  (echt) feiner als  $\mathcal{G} \iff$

$$\underbrace{\{G_i \mid i \in \{0, \dots, t\}\}}_{\text{von } \mathcal{G}} \subsetneq \underbrace{\{G'_j \mid j \in \{0, \dots, t'\}\}}_{\text{von } \mathcal{G}'}$$

**Beispiel.**

$$\begin{array}{c} \overbrace{S_4}^{G_4} \triangleright \overbrace{A_4}^{G_3} \triangleright \underbrace{V}_{G_2} \triangleright \overbrace{\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}}^{G_1} \triangleright \overbrace{\{e\}}^{G_0} \end{array}$$

ist eine Zerlegungsreihe mit den Faktoren:

$i$	4	3	2	1
$G_i/G_{i-1}$	$\mathbb{Z}/2$	$\mathbb{Z}/3$	$\mathbb{Z}/2$	$\mathbb{Z}/2$

Insbesondere ist  $\mathcal{G}$  abelsch (und  $S_4$  ist auflösbar). Beachte:  $G_1 \triangleleft G_2$  ist Normalteiler  $G_1 \triangleleft G_3$  (Übung)

**Proposition 2.44.** Sei  $\mathcal{G} : \{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_t = G$  eine Normalreihe, dann:

(a)  $\mathcal{G}$  ist eine Zerlegungsreihe  $\iff \mathcal{G}$  besitzt keine echte Verfeinerung.

(b) Es gilt  $2^t \leq \#G$

(c) Ist  $G$  endlich, so besitzt  $\mathcal{G}$  eine Verfeinerung, die eine Zerlegungsreihe ist.

(d) Ist  $\mathcal{G}$  abelsch, so ist auch die Verfeinerung abelsch.

*Beweis.* (a)  $G$  ist keine Zerlegungsreihe

$$\iff \exists i \in \{1, \dots, t\} : G_i/G_{i-1} \text{ nicht einfach}$$

$$\iff \exists i \in \{1, \dots, t\} : \overline{H} \trianglelefteq G_i/G_{i-1} \text{ mit } \overline{H} \neq \{e\}, \overline{H} \subsetneq G_i/G_{i-1}$$

$$\stackrel{2. \text{ Isometriesatz}}{\iff} \exists i \in \{1, \dots, t\} : \exists H \triangleleft G_i \text{ mit } G_{i-1} \triangleleft H$$

$$\iff \exists i \in \{1, \dots, t\} : \mathcal{G} \text{ kann zwischen } G_{i-1} \text{ und } G_i \text{ echt verfeinert werden}$$

$$\iff \mathcal{G} \text{ besitzt eine echte Verfeinerung.}$$

(b) Lagrange: (Für  $H \leq G : \#G = \#H \cdot \#G/H$ )

$$\begin{aligned} \#G &= \#G_t = \#G_{t-1} \cdot \#G_t/G_{t-1} \\ &= \#G_{t-2} \cdot \#G_{t-1}/G_{t-2} \cdot \#G_t/G_{t-1} = \dots = \prod_{i=1}^t \# \underbrace{G_i/G_{i-1}}_{\substack{\text{nichttriviale} \\ \text{endliche Gruppe}}} \geq 2^t \\ &\implies t \leq \log_2 \#G \end{aligned}$$

(c) Sei  $\mathcal{G}'$  eine Verfeinerung von  $\mathcal{G}$ , maximaler Länge  $t'$ . Das gibt es, da  $t' \leq \log_2 \#G$ . Dieses  $\mathcal{G}'$  kann nicht echt verfeinert werden ( $t'$  maximal!)

$\implies \mathcal{G}'$  ist Zerlegungsreihe, die  $\mathcal{G}$  verfeinert.

(d) Sei  $\mathcal{G}$  abelsch und  $\mathcal{G}'$  eine Verfeinerung von  $\mathcal{G}$ , z.z.  $\mathcal{G}'$  ist abelsch.

$$(\mathcal{G}' : G'_0 = \{e\} \triangleleft G'_1 \triangleleft G'_2 \triangleleft \dots \triangleleft G'_{t'} = G)$$

Sei  $j \in \{1, \dots, t'\}$ , z.z.  $G'_j/G'_{j-1}$  ist abelsch. Finde zu  $j, j-1$  ein  $i \in \{1, \dots, t\}$ , sodass

$$\begin{array}{ccccccc} G & \cdots & G_{i-1} & & \triangleleft & G_i & \cdots \\ & & \parallel & & & \parallel & \\ & & G'_\ell & \leq & G'_{j-1} \triangleleft G'_{j'} & \leq & G'_m \end{array}$$

Wir wissen:  $G_i/G_{i-1} = G'_m/G'_\ell$  ist eine abelsche Gruppe, wir wissen auch:

$$G'_\ell/G'_\ell \leq G'_{j-1}/G'_\ell \leq G'_{j'}/G'_\ell \leq G'_m/G'_\ell$$

(2. Isomorphiesatz für  $G'_m \rightarrow G'_m/G'_\ell$ ) Beachte:  $G'_m/G'_\ell$  ist abelsch  $\implies G'_{j-1}/G'_\ell, G'_{j'}/G'_\ell$  sind abelsch, und (2. Isomorphiesatz)

$$G'_{j'}/G'_{j-1} \cong \underbrace{(G'_{j'}/G'_\ell)}_{\text{abelsch}} / (G'_{j-1}/G'_\ell) \implies G'_{j'}/G'_{j-1} \text{ abelsch.} \quad \square$$

**Satz 2.45 (Satz von Jordan-Hölder).** *Ist  $G$  endlich, so ist die Folge der Faktoren einer Zerlegungsreihe  $\mathcal{G}$  von  $G$  bis auf Reihenfolge der Faktoren unabhängig von der Wahl der Zerlegungsreihe von  $G$ .*

*Beweis.* Siehe Jantzen Schwermer Satz II. 2.4 oder Jacobson §4.6 □

**Korollar 2.46.** *Sei  $G$  endlich, dann ist  $G$  auflösbar  $\iff$  die Faktoren jeder Zerlegungsreihe sind abelsch und von Primzahlordnung.*

*Beweis.*

“ $\implies$ ”: Sei  $\mathcal{G}$  eine abelsche Normalreihe  $\xRightarrow{\text{Prop. 44}} \exists$  Zerlegungsreihe  $\mathcal{G}'$  die  $\mathcal{G}$  verfeinert, diese ist dann (stets) wieder abelsch. Ihre Faktoren sind einfach und abelsch (und endliche Gruppen), also zyklisch von Primzahlordnung. Wende nun Jordan-Hölder an.

“ $\impliedby$ ”: Hat man  $\mathcal{G}$  wie angegeben (zu  $G$ ), so ist  $\mathcal{G}$  abelsch, also  $G$  auflösbar. □

**Beispiel 2.47.** Sei  $G$  eine  $p$ -Gruppe  $\implies G$  ist auflösbar

*Beweis.* Sei  $\mathcal{G}$  eine Zerlegungsreihe von  $G$ , dann sind die Faktoren  $H_i$  einfache  $p$ -Gruppen. Wir wissen, dass  $Z(H_i) \supsetneq \{e\}$  nicht-trivial ist.

$$\begin{array}{c} H_i \xrightarrow{\text{einfach}} H_i = Z(H_i) \\ Z(H_i) \trianglelefteq H_i \end{array}$$

Da  $Z(H_i)$  eine einfache abelsche  $p$ -Gruppe ist folgt  $\mathcal{G}$  ist eine abelsche Normalreihe. Nach dem Satz von Cauchy finde  $\mathbb{Z}/p$  als Untergruppe von  $H_i \implies H_i$  einfach abelsch ( $\mathbb{Z}/p \trianglelefteq H_i$ ). □

**Beispiel 2.48.** Gilt  $\#G < 60$ , so ist  $G$  auflösbar.

*Beweis.* Sei  $\mathcal{G}$  eine Zerlegungsreihe mit einfachen Faktoren  $H_i$  mit  $\#H_i < 60$ . Nach Satz 42 sind  $H_i$  sind zyklisch von Primzahlordnung  $\implies G$  auflösbar. □

**Proposition 2.49** (übung). *Sei  $G$  endlich,  $N \trianglelefteq G$  ein Normalteiler,  $H \leq G$  eine Untergruppe, dann:*

- (a)  $G$  auflösbar  $\iff N$  und  $G/N$  sind auflösbar.
- (b)  $G$  auflösbar  $\implies H$  auflösbar.

**Wiederholung.** Die Kommutatoruntergruppe von  $G$  ist

$$[G, G] = \langle [g, h] := ghg^{-1}h^{-1} \mid g, h \in G \rangle$$

Eigenschaften:

- (a)  $[G, G] \trianglelefteq G$
- (b)  $G/[G, G]$  ist abelsch
- (c) Ist  $N \trianglelefteq G$  ein Normalteiler mit  $G/N$  abelsch, so gilt  $[G, G] \leq N$  ist Untergruppe.
- (d)  $H \leq G$  Untergruppe  $\implies [H, H] \leq [G, G]$  nach Definition.



(e)  $\pi : G \rightarrow G'$  ein surjektiver Gruppenhomomorphismus, dann:

$$\pi([G, G]) = [G', G']$$

Denn:

*Beweisskizze.*

$$\pi(\{[g, h] \mid g, h \in G\}) = \{[\pi(g), \pi(h)] \mid g, h \in G\} \stackrel{\pi \text{ surj.}}{=} \{[g', h'] \mid g', h' \in G'\} \cdots$$

□

**Definition 2.50 (Abgeleitete Reihe).** Die abgeleitete Reihe von  $G$  ist definiert als die Folge

$$D^0(G) \geq D^1(G) \geq D^2(G) \geq \cdots$$

mit  $D^0(G) := G$  und  $D^{i+1}(G) := [D^i(G), D^i(G)]$  für  $i \geq 0$

**Bemerkung 2.51.**

- (a) Gilt  $D^{i+1}(G) = D^i(G)$ , so folgt  $D^n(G) = D^i(G), \forall n \geq i$
- (b) Nach Wiederholung (a) folgt:  $D^i(G) \leq D^{i-1}(G), \forall i \geq 1$ . Es gilt sogar:  
(Übung 3)  $D^i(G) \leq G, \forall i \geq 0$

- (c)  $H \leq G \xrightarrow[\text{von Whg.}]{\text{vgl (d)}} D^i(H) \leq D^i(G) \cap H$  (induktiv)

- (d)  $\pi : G \rightarrow G'$  surjektiv  $\xrightarrow[\text{zu (e) Whg.}]{\text{Übung, Induktion}} \pi(D^i(G)) = D^i(G')$

**Satz 2.52 (Auflösbarkeitskriterium).** Sei  $G$  endlich, dann ist  $G$  auflösbar  $\iff \exists i : D^i(G) = \{e\}$ .

*Beweis.*

“ $\implies$ ”: Sei  $G = G_t \triangleright G_{t-1} \triangleright G_{t-2} \triangleright \cdots \triangleright G_1 \triangleright G_0 = \{e\}$  eine abelsche Normalreihe. Dann folgt aus Wiederholung (c)

$$\forall i : [G_i, G_i] \leq G_{i-1} \quad (\text{da } G_i/G_{i-1} \text{ abelsch})$$

$$\implies D^1(G) \leq G_{t-1} \implies D^2(G) \leq D^1(G_{t-1}) \leq G_{t-2} \text{ etc.}$$

$$\xRightarrow{\text{Ind.}} D^t(G) = \{e\} \quad (D^i(G) \leq G_{t-i}, \forall i \in \{0, \dots, t\})$$

“ $\impliedby$ ”: Trivial. Sei  $t \geq 0$  minimal mit  $D^t(G) = \{e\}$ , dann gilt

$$G = D^0(G) \triangleright D^1(G) \triangleright D^2(G) \triangleright \cdots \triangleright D^{t-1}(G) \triangleright D^t(G) = \{e\}$$

(echte Normalteiler wegen Sylow I (a) und  $t$  minimal.) ist eine Normalreihe, Faktoren sind abelsch nach Definition der abgeleiteten Reihe (da  $H/[H, H]$  abelsch). □

**Beispiel 2.53.**

- (a)  $G$  abelsch  $\implies D^1(G) = \{e\}$

- (b) (Übung)  $D^1(D_n) \leq C_n$ , wobei  $D_n$  die Diedergruppe bezeichnet.
- (c) (Übung) Für  $n \geq 5$  gezeigt  $D^1(A_n) = A_n \implies A_n$  nicht auflösbar. (Wissen auch  $A_n$  ist einfach und nicht abelsch  $\implies A_n$  ist nicht auflösbar.)

**Definition 2.54 (Perfekte Gruppe).** Eine Gruppe  $G$  heißt perfekt  $\iff G = [G, G] = D^1(G)$ . Damit (Übung) ist  $A_n$  perfekt für  $n \geq 5$ .

**Bemerkung** (ohne Beweis).  $\mathrm{SL}_n(K)$  ist perfekt, falls  $\#K \notin \{2, 3\}$

# Kapitel 3

## Ringe

**Wiederholung.**  $(R, 0, 1, +, \cdot)$  ist ein **Ring**  $\iff (R, 0, +)$  ist eine Gruppe,  $(R, 1, \cdot)$  ist ein Monoid und es gelten die Distributivgesetze.

$$R^\times = \{r \in R \mid \exists s \in R : rs = sr = 1\}$$

ist die Einheitengruppe von  $R$

**Beispiel.** (Übung)  $\mathbb{Z}_n^\times = \{\bar{a} \mid \text{ggT}(a, n) = 1\}$ , wobei  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(n)$

**Definition 3.1 (Ringhomomorphismus).** Seien  $R, R'$  Ringe, eine Abbildung  $\varphi : R \rightarrow R'$  heißt Ringhomomorphismus wenn:

- $\varphi : (R, 0, +) \rightarrow (R', 0', +')$  ist ein Gruppenhomomorphismus.
- $\varphi : (R, 1, \cdot) \rightarrow (R', 1', \cdot')$  ist ein Monoidhomomorphismus.

$\varphi$  ist ein Ringisomorphismus  $\iff \varphi$  ist bijektiver Ringhomomorphismus  $\xLeftrightarrow{\text{Übung}}$

$\exists \varphi' : R' \xrightarrow{\text{Ringhom.}} R$ , sodass  $\varphi \circ \varphi' = \text{id}_{R'}$  und  $\varphi' \circ \varphi = \text{id}_R$ . In diesem Fall schreibe  $R \cong R'$  ( $R$  isomorph zu  $R'$ ).

**Beispiel.**  $R$  heißt Nullring  $\iff 0_R = 1_R \xLeftrightarrow{\text{Übung}} R = \{0_R\}$  (alle Nullringe sind isomorph.)

**Beispiel.** (Übung) Sei  $R$  beliebig  $\implies \exists!$  Ringhomomorphismus  $\varphi : \mathbb{Z} \rightarrow R$  nämlich

$$\varphi : \mathbb{Z} \rightarrow R, n \mapsto \varphi(n) = n \cdot 1_R$$

(wegen  $\varphi(1) = 1_R$ )

**Definition 3.2 (Unterring).**  $S \subseteq R$  heißt Unterring, falls

- $1 \in S$
- $S - S = \{s_1 - s_2 \mid s_1, s_2 \in S\} \subseteq S$
- $S + S = \{s_1 + s_2 \mid s_1, s_2 \in S\} \subseteq S$

**Definition (Produkt von Ringen).** Seien  $R_1, R_2$  Ringe, dann ist  $(R_1 \times R_2, (0, 0), (1, 1), +, \cdot)$  ein Ring mit komponentenweiser Addition und Multiplikation.

$$+ : (R_1 \times R_2)^2 \rightarrow R_1 \times R_2, (r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$$

$$\cdot : (R_1 \times R_2)^2 \rightarrow R_1 \times R_2, (r_1, r_2) \cdot (s_1, s_2) = (r_1 \cdot s_1, r_2 \cdot s_2)$$

**Bemerkung (Übung).**

- (a) Sei  $R$  ein kommutativer Ring,  $S \subseteq R$  ein Unterring, dann ist  $S$  kommutativ.  
 (b) Seien  $R_1, R_2$  kommutative Ringe, so ist auch  $R_1 \times R_2$  kommutativ.

**Wiederholung.** Seien  $I, X$  Mengen. Eine Folge/Familie in  $X$  über (Indexmenge)  $I$ , geschrieben  $(x_i)_{i \in I}$  ist eine Abbildung  $x : I \rightarrow X, i \mapsto x_i$ . Schreibe  $X^I$  für die Menge aller Folgen in  $X$  über  $I$  ( $= \text{Abb}(I, X)$ )

**Beispiel 3.3 (Monoidring).** Sei  $R = (R, 0, 1, +, \cdot)$  ein kommutativer Ring und  $M = (M, e, \circ)$  ein Monoid. Definiere

(i)  $R[M] := \{(a_m)_{m \in M} \in R^M \mid (E) : \#\{m \in M : a_m \neq 0\} < \infty\}$

(ii)  $\underline{0}$  = die Abbildung  $M \rightarrow \{0\} \subseteq R$

(iii)  $\underline{1}$  = die Folge  $(\delta_{em})_{m \in M}$  mit  $\delta_{em} = \begin{cases} 1, & m = e, \\ 0, & m \neq e. \end{cases}$

(iv) Verknüpfungen  $+, \cdot : R[M] \times R[M] \rightarrow R[M]$  durch:

$$(a_m)_{m \in M} + (b_m)_{m \in M} := (a_m + b_m)_{m \in M}$$

und

$$(a_m)_{m \in M} \cdot (b_m)_{m \in M} := (c_m)_{m \in M}$$

mit (Übung)

$$c_m := \sum_{\substack{(m', m'') \in M \times M \\ m' \cdot m'' = m}} a_{m'} \cdot b_{m''}$$

die Summe ist endlich wegen (E) und wegen (E) gilt:  $\#\{m \mid c_m \neq 0\} < \infty$

**Notation.**

$$\sum_{m \in M} a_m \cdot m \text{ für } (a_m)_{m \in M} \in R[M]$$

**Übung 3.4.**

- a)  $(R[M], \underline{0}, \underline{1}, +, \cdot)$  ist ein Ring,  $(R[M])$  heißt **Monoidring** zu  $M$  über  $R$   
 b) Ist  $M$  abelsch, so ist  $R[M]$  kommutativ.  
 c) Ist  $\varphi : R \rightarrow S$  ein Ringhomomorphismus und  $\sigma : M \rightarrow (S, 1, \cdot)$  ein Monoidhomomorphismus, so  $\exists!$  Ringhomomorphismus  $\psi : R[M] \rightarrow S$  mit  $\psi|_R = \varphi$  und  $\psi|_M = \sigma$ . (dabei wir identifizieren  $R$  mit  $R \cdot e = R \cdot 1$  (1-Folge) und  $M$  mit  $1_R \cdot M$ ), nämlich:

$$\psi \left( \underbrace{\sum a_m \cdot m}_{\text{in } R[M]} \right) = \underbrace{\sum \varphi(a_m) \cdot \sigma(m)}_{\text{in } S}$$

**Konvention.** Ab nun seien alle Ringe  $R, R', S, R_i$  kommutativ, (und es Seien in §3 stets Ringe)

### 3.1 Polynomringe

**Beispiel 3.5.** Die folgenden Strukturen sind abelsche Monoide:

- (i)  $(\mathbb{N}_0, 0, +) = \mathbb{N}_0$
- (ii)  $(\mathbb{N}_0^n, (0, \dots, 0), +) = \times_{i \in \{1, \dots, n\}} \mathbb{N}_0$  (Komponentenweise Addition)
- (iii) Für  $I$  eine beliebige Menge:  $(\mathbb{N}_0^{(I)}, \underline{0}, \pm)$  mit

$$\mathbb{N}_0^{(I)} = \{(a_i)_{i \in I} \in \mathbb{N}_0 \text{ Folgen über } I \mid \#\{i \in I : a_i \neq 0\} < \infty\}$$

$\underline{0}$  = 0-Folge und  $\pm$  komponentenweise Addition in  $\mathbb{N}_0^{(I)}$ .

**Facts 3.6** (Übung).

(i)  $\mathbb{N}_0^n \cong \mathbb{N}_0^{\{1, \dots, n\}}, (a_i)_{i \in \{1, \dots, n\}} \mapsto (a_i)_{i \in \{1, \dots, n\}}$

(ii) Für  $i \in I$  sei  $e_i \in \mathbb{N}_0^{(I)}$  die Folge mit  $e_i(j) = \begin{cases} 1, & j = i, \\ 0 & j \neq i. \end{cases}$

(betrachte  $e_i : I \rightarrow \mathbb{N}_0$  als Abbildung) Damit ist jede Folge  $\underline{a} = (a_i)_{i \in I} \in \mathbb{N}_0^{(I)}$  eindeutige Linearkombination mit Koeffizienten in  $\mathbb{N}_0$ , nämlich:

$$\underline{a} = \sum_{i \in I} a_i \cdot e_i = \sum_{i \in I, a_i \neq 0} a_i \cdot e_i$$

Beachte:  $\mathbb{N}_0^{(I)} \subseteq \mathbb{Q}^{(I)}$  (analog definiert, Folgen in  $\mathbb{Q}$  über  $I$ ) mit Endlichkeitsbedingung  $(E)$ . Und  $(e_i)_{i \in I}$  ist eine Basis von  $\mathbb{Q}^{(I)}$  als  $\mathbb{Q}$ -Vektorraum. Man sagt auch  $\mathbb{N}_0^{(I)}$  ist freies abelsches Monoid über der Basis  $(e_i)_{i \in I}$ .

- (iii) Ist  $M$  ein abelsches Monoid und  $(m_i)_{i \in I}$  eine Folge in  $M$ , so  $\exists!$  Monoid-homomorphismus

$$\varphi : \mathbb{N}_0^{(I)} \rightarrow M, \varphi(e_i) = m_i$$

**Wiederholung.**  $R[X]$  ist der Polynomring über  $R$  in Variablen  $X$ . Elemente sind  $\sum_{n \geq 0} a_n X^n$ , ( $a_n \in R$ ) nur endlich viele  $a_n \neq 0$ .  $+$ ,  $\cdot$  auf  $R[X]$  sind definiert durch

$$\begin{aligned} \sum a_i X^i + \sum b_i X^i &= \sum (a_i + b_i) X^i \\ \left( \sum a_i X^i \right) \left( \sum b_i X^i \right) &= \sum_i \left( \sum_{j=0}^i a_j b_{i-j} \right) X^i \end{aligned}$$

**Proposition 3.7.** Die folgende Abbildung ist ein Ringisomorphismus.

$$\psi : R[\mathbb{N}_0] \rightarrow R[X], \sum_{i \in \mathbb{N}_0} r_i i \mapsto \sum_{i \in \mathbb{N}_0} r_i X^i$$

*Beweis.*

- $\psi$  wohldefiniert und bijektiv:

$$R[\mathbb{N}_0] = \text{Folgen } (r_i)_{i \in \mathbb{N}_0} \text{ mit } \#\{i \mid r_i \neq 0\} < \infty$$

$$R[X] = \text{analog}$$

• Ringstruktur:

- Addition (Übung)
- Multiplikation

$$\begin{aligned}
 & \underbrace{\left( \sum_{i \in \mathbb{N}_0} r_i \cdot i \right)}_{f \in R[\mathbb{N}_0]} \underbrace{\left( \sum_{j \in \mathbb{N}_0} s_j \cdot j \right)}_g \stackrel{\text{Nach Def.}}{=} \sum_{k \in \mathbb{N}_0} s_k \cdot k, \quad s_k \\
 &= \sum_{0 \leq i, j, i+j=k} r_i s_j = \sum_{j=0}^k r_j s_{k-j} \\
 &\implies \psi(f \cdot g) = \psi \left( \sum_k s_k \cdot k \right) = \sum_k g_k X^k \\
 &= \sum_i a_i \cdot \sum_j b_j X^j = \psi(f) \psi(g). \quad \square
 \end{aligned}$$

Formal:  $\{0, 1, \dots\} \rightarrow \{X^i \mid i \in \mathbb{N}_0\}$ .

**Proposition 3.8** (Universelle Eigenschaft von  $R[X] \cong R[\mathbb{N}_0]$ ).  $\forall \psi : R \rightarrow S$  Ringhomomorphismen und  $\forall s \in S \exists!$  Ringhomomorphismus  $\hat{\psi} : R[X] \rightarrow S$  mit  $\hat{\psi}|_R = \psi$  und  $\hat{\psi}(X) = s$

1. *Beweis.* Definiere  $\hat{\psi}(\sum_{i \geq 0} r_i X^i) := \sum_{i \geq 0} \underbrace{\psi(r_i)}_{\in S} s^i$ . Dann die Behauptung nachprüfen.  $\square$

2. *Beweis.* Facts 6(iii)  $\exists!$  Monoidhomomorphismus  $\sigma : \mathbb{N}_0 \rightarrow (S, 1, \cdot)$  mit  $\sigma(1) = s$  und Übung 4(c) (universelle Eigenschaft des Monoidrings)  $\exists!$  Ringhomomorphismus  $\hat{\psi} : R[\mathbb{N}_0] \rightarrow S$  mit  $\hat{\psi}|_R = \psi$  und  $\hat{\psi}|_{\mathbb{N}_0} = \sigma$ . Dieser erfüllt die Aussagen in Prop 8, denn  $\hat{\psi}(X) = \hat{\psi}(1) = s$ ,  $X$  entspricht  $1 \in \mathbb{N}_0$  (Unter Isomorphismus von Proposition 7).  $\square$

**Definition.** Für  $n \geq 1$  Variable: ( $n \in \mathbb{N}$ )

$$R[X_1, \dots, X_n] := (R[X_1, \dots, X_{n-1}])[X_n] = \dots = (\dots((R[X_1])[X_2])\dots)[X_n]$$

**Satz 3.9.** Sei  $\varphi : \mathbb{N}_0^n \rightarrow (R[X_1, \dots, X_n], 1, \cdot)$  der eindeutige Monoidhomomorphismus mit  $\varphi(e_i) = X_i$ , wobei  $e_i = (\delta_{i,j})_j = (0, \dots, 1, \dots, 0)$  für  $i \in \{1, \dots, n\}$ . Dann ist (nach 4(c) eindeutige) Ringhomomorphismus  $\hat{\psi} : R[\mathbb{N}_0^n] \rightarrow R[X_1, \dots, X_n]$  mit  $\hat{\psi}|_R = \text{id}_R$  und  $\hat{\psi}|_{\mathbb{N}_0^n} = \varphi$  ein Ringisomorphismus.

*Beweis.* (Übung) Hierbei wird  $m = (m_1, \dots, m_n) \in \mathbb{N}_0^n$  identifiziert (unter  $\hat{\psi}$ ) mit  $X_1^{m_1} \cdot \dots \cdot X_n^{m_n}$   $\square$

**Definition 3.10 (Polynomring).** Der **Polynomring** in den Variablen  $(X_i)_{i \in I}$  ( $I$  beliebige Menge) ist definiert als

$$R[X_i \mid i \in I] := R[\mathbb{N}_0^{(I)}]$$

Elemente in diesem Ring sind

$$\sum_{a \in \mathbb{N}_0^{(I)}} r_a \cdot a$$

mit  $r_a \in R$  und es gilt  $\#\{a \in \mathbb{N}_0^{(I)} \mid r_a \neq 0\} < \infty$ .

**Notation.** Andere Notation: Für  $a \in \mathbb{N}_0^{(I)}$  schreibe für  $a$

$$X^a \text{ oder } \prod_{i \in I, a_i \neq 0} X_i^{a_i}$$

Insbesondere ist  $X^{e_i} = X_i$ , wobei  $e_i$  die Folge in  $\mathbb{N}_0^{(I)}$  mit  $e_i(j) = \delta_{i,j}$  ist. Monoidaddition  $a + b$  entspricht

$$X^a \cdot X^b = X^{a+b}$$

(bilden  $a + b$  in  $(\mathbb{N}_0^{(I)}, \underline{0}, +)$  und  $(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i +_{\mathbb{N}_0} b_i)_{i \in I}$ ) Also  $+$  ist nicht die Addition im Ring.

**Definition (Primitives Monom).** Die Elemente in  $R[\mathbb{N}_0^{(I)}]$  sind Summen

$$\sum_{a \in \mathbb{N}_0^{(I)}} r_a \cdot X^a$$

(Polynome wie gewohnt.) Die Elemente  $X^a, a \in \mathbb{N}_0^{(I)}$  heißen **primitive Monome**. Jedes Element in  $R[X_i \mid i \in I]$  ist eine eindeutige Linearkombination in den Monomen  $X^a, a \in \mathbb{N}_0^{(I)}$ , mit Koeffizienten  $r_a$  aus  $R$ , sodass  $\#\{a \in \mathbb{N}_0^{(I)} \mid r_a \neq 0\} < \infty$ , d.h. als  $R$ -Modul ist  $R[X_i \mid i \in I]$  frei über  $R$  mit Basis  $X^a, a \in \mathbb{N}_0^{(I)}$

**Beispiel.**  $(2, 5, 3) \in \mathbb{N}_0^3$  entspricht  $X_1^2 X_2^5 X_3^3$

**Satz 3.11** (Universelle Eigenschaft von  $R[X_i \mid i \in I]$ ). Zu Ringhomomorphismus  $\psi : R \rightarrow S$  und einer Folge  $(s_i)_{i \in I}$  aus  $S$  über  $I$   $\exists!$  Ringhomomorphismus  $\hat{\psi} : R[X_i \mid i \in I] \rightarrow S$  mit  $\hat{\psi}|_R = \psi$  und  $\hat{\psi}(X_i) = s_i$

**Facts.**

(a) Für  $J \subseteq I$  existiert eindeutiger Monoidhomomorphismus  $\mathbb{N}_0^{(J)} \rightarrow \mathbb{N}_0^{(I)}$  mit  $e_j \mapsto e_j$  und ein induzierter Ringhomomorphismus (für  $j \in J$ )

$$\hat{\psi} : R[\mathbb{N}_0^{(J)}] = R[X_j \mid j \in J] \rightarrow R[\mathbb{N}_0^{(I)}] = R[X_i \mid i \in I]$$

mit  $\hat{\psi}|_R = \text{id}_R$  und  $\hat{\psi}(X_j) = X_j$  ( $j \in J$ ). Die Abbildung  $\hat{\psi}$  ist injektiv deswegen betrachten wir  $R[X_j \mid j \in J]$  als Unterring von  $R[X_i \mid i \in I]$

(b) Es gilt:

$$R[X_i \mid i \in I] = \bigcup_{J \subseteq I \text{ endl.}} R[X_j \mid j \in J]$$

d.h. jedes Polynom im Ring ist Polynom in nur endlich vielen Variablen.

**Definition 3.12.**

(a)  $\text{Grad} : R[X] \rightarrow \mathbb{N}_0 \cup \{-\infty\}$  ist die eindeutige Abbildung mit

$$\text{Grad}(f) = \text{Grad} \left( \sum_{i \geq 0} r_i X^i \right) = \begin{cases} -\infty, & f = 0, \\ \max\{i \in \mathbb{N}_0 \mid r_i \neq 0\}, & f \neq 0 \end{cases}$$

(b) Der **Leitkoeffizient** von  $f \neq 0$  ist  $a_{\text{Grad}(f)}$ .

(c)  $f \neq 0$  heißt **normiert**  $\iff a_{\text{Grad}(f)} = 1$ .

(d) Ist  $R = K$  ein Körper, so gelten außerdem

$$\text{Grad}(fg) = \text{Grad}(f) + \text{Grad}(g)$$

wobei  $-\infty + n = n + -\infty = -\infty + (-\infty) = -\infty$  für  $n \in \mathbb{N}_0$ . Genügt:  $R$  ist Integritätsbereich.

(e) Falls  $R$  ein Körper (oder Integritätsbereich), so gilt

$$\begin{aligned} (R[X])^\times &= \{f \in R[X] \mid \exists g \in R[X] : fg = 1\} \\ &\stackrel{\text{Übung}}{=} \{f \in R[X] \mid \text{Grad}(f) = 0, \exists g \in R[X] : \text{Grad } g = 0 : fg = 1\} \\ &= \{f \in R \mid \exists g \in R : fg = 1\} = R^\times \end{aligned}$$

## 3.2 Symmetrische Polynome

Sei  $R$  ein kommutativer Ring,  $n \in \mathbb{N}$  fest.

**Bezeichnung.** (a) Ein Monom in  $R[X_1, \dots, X_n]$  ist ein Polynom der Form  $aX^m = aX_1^{m_1} \cdots X_n^{m_n}$  für  $a \in R \setminus \{0\}$  und  $m = (m_i)_{i \in \{1, \dots, n\}} \in \mathbb{N}_0^n$  und  $X^m$  (falls  $a = 1$ ) heißt primitives Monom.

(b) Der (Total-)Grad des Monoms  $aX^m$  für  $a \in R \setminus \{0\}$  und  $m = (m_i)$  ist  $|m| := \sum_i m_i$ . Der (Total-)Grad von  $f = \sum a_m X^m$  ist  $\text{Grad}(f) = \max\{|m| : a_m \neq 0\}$ . ( $\max(\emptyset) := -\infty$ )

(c)  $f \in R[X_1, \dots, X_n]$  heißt homogen vom Grad  $t \iff f$  ist Summe von Monomen  $aX^m$ , die alle vom Grad  $|m| = t$  sind.

**Beispiel.** (a)  $f = X_1^3 X_2^2 X_3$  ist primitiver Monom mit  $\text{Grad}(f) = 11$

(b)  $g = X_1^3 X_2^2 + X_1 X_2^4$  ist homogen vom Grad 5

**Lemma 3.13.** (a)  $\forall \sigma \in S_n \exists!$  Ringhomomorphismus  $\tilde{\sigma} : R[X_1, \dots, X_n] \rightarrow R[X_1, \dots, X_n]$  mit  $\tilde{s}|_R = \text{id}_R$  und  $\tilde{\sigma}(X_i) = X_{\sigma(i)}$  für  $i \in \{1, \dots, n\}$



(b)  $\widetilde{\text{id}} = \text{id}_{R[X_1, \dots, X_n]}$  (für  $\text{id} \in S_n$  die Eins).

(c)  $\forall \sigma, \tau \in S_n : \widetilde{\sigma \circ \tau} = \widetilde{\sigma} \circ \tau$  Ringhomomorphismen.

*Beweis.* (a)  $\widetilde{\sigma}$  existiert und ist eindeutig nach universeller Eigenschaft (Satz 10) für  $R[X_1, \dots, X_n]$ .

(b)  $\alpha := \text{id}_{R[X_1, \dots, X_n]}$  ist ein Ringhomomorphismus  $R[X_1, \dots, X_n] \rightarrow R[X_1, \dots, X_n]$  mit  $\alpha|_R = \text{id}_R$  und  $\alpha(X_i) = X_i \xrightarrow{(a)} \alpha = \widetilde{\text{id}}$ .

(c) Wende universelle Eigenschaft von  $R[X_1, \dots, X_n]$  an. Wir haben:

$$\widetilde{\sigma \circ \tau}|_R \underset{\text{Def. in (a)}}{=} \text{id}_R = \text{id}_R \circ \text{id}_R = \widetilde{\sigma}|_R \circ \widetilde{\tau}|_R = \widetilde{\sigma \circ \tau}|_R$$

und

$$\widetilde{\sigma \circ \tau}(X_i) = X_{\sigma \circ \tau(i)} = X_{\sigma(\tau(i))} = \widetilde{\sigma}(X_{\tau(i)}) = \widetilde{\sigma}(\widetilde{\tau}(X_i)) = (\widetilde{\sigma} \circ \widetilde{\tau})(X_i)$$

$$\xrightarrow[\text{in (a)}]{\text{Eindeutigkeit}} \widetilde{\sigma \circ \tau} = \widetilde{\sigma} \circ \widetilde{\tau}. \quad \square$$

**Bemerkung** (Übung). Ist  $\alpha : R \rightarrow R$  ein Ringhomomorphismus, so ist  $R^\alpha := \{r \in R \mid \alpha(r) = r\}$  ein Unterring von  $R$ .

**Korollar 3.14.**  $R[X_1, \dots, X_n]^{S_n} := \{f \in R[X_1, \dots, X_n] \mid \widetilde{\sigma}(f) = f, \forall \sigma \in S_n\} = \bigcap_{\sigma \in S_n} R[X_1, \dots, X_n]^{\widetilde{\sigma}}$  ist ein Unterring von  $R[X_1, \dots, X_n]$ .

**Definition 3.15** (Symmetrische Polynom). Die Elemente in  $R[X_1, \dots, X_n]^{S_n}$  heißen symmetrische Polynome.

**Korollar 3.16.** Die Abbildung

$$\widetilde{\cdot} : S_n \rightarrow \text{Aut}(R[X_1, \dots, X_n]), \sigma \mapsto \widetilde{\sigma}$$

ist wohl-definiert und ein injektiver Gruppenhomomorphismus.

*Beweis.*

1)  $\widetilde{\cdot}$  wohl-definiert: Zu zeigen  $\widetilde{\sigma}$  ist Automorphismus (bijektiver Ringhomomorphismus). Dazu beachte

$$\widetilde{\sigma} \circ \widetilde{\sigma^{-1}} \underset{12}{=} \widetilde{\sigma \circ \sigma^{-1}} = \widetilde{\text{id}} = \text{id}_{R[X_1, \dots, X_n]} = \dots = \widetilde{\sigma^{-1}} \circ \widetilde{\sigma}$$

folglich:  $\widetilde{\sigma}$  ist Ringautomorphismus.

2) Gruppenhomomorphismus: folgt aus 12(c)

3)  $\sigma \mapsto \widetilde{\sigma}$  injektiv: Denn verschiedene  $\sigma, \tau$  wirken unterschiedlich auf  $\{X_1, \dots, X_n\}$   $\square$

**Bemerkung** (Ziel von diesem Abschnitt). Explizite Beschreibung von  $R[X_1, \dots, X_n]^{S_n}$

### 3.3 Elementar symmetrische Polynome

**Proposition.** Zu  $\sigma \in S_n$  erweitern  $\tilde{\sigma}$  zu  $\sigma'$  Ringautomorphismus von  $R[X_1, \dots, X_n][X]$  durch

$$\sigma'|_R = \text{id}_R, \sigma'(X_i) = X_{\sigma(i)} \text{ und } \sigma'(X) := X$$

*Behauptung:*  $g := \prod_{i=1}^n (X - X_i) \stackrel{!}{\in} R[X_1, \dots, X_n]^{S_n} \underset{\text{Übung}}{=} R[X_1, \dots, X_n]^{S_n}[X].$

*Beweis.*  $\sigma'(g) = \prod_{i=1}^n (\sigma'(X) - \sigma'(X_i)) = \prod_{i=1}^n (X - X_{\sigma(i)}) = \prod_{i=1}^n (X - X_i) = g$   
da  $\tilde{\sigma}$  eine Bijektion auf  $\{X_1, \dots, X_n\}$  definiert.  $\square$

**Bemerkung.** Schreibe  $g$  als Polynom in  $X$  mit Koeffizienten  $s_i$  in

$$R[X_1, \dots, X_n] \implies g = \sum_{i=0}^n (-1)^{n-i} X^i s_{n-i}(X_1, \dots, X_n)$$

$$= X^n - s_1(X_1, \dots, X_n)X^{n-1} + s_2(X_1, \dots, X_n)X^{n-2} \mp \dots + (-1)^n s_n(X_1, \dots, X_n)$$

Das definiert  $s_1, \dots, s_n \in R[X_1, \dots, X_n]^{S_n}$

Insbesondere:

- (i)  $s_1, \dots, s_n \in R[X_1, \dots, X_n]^{S_n}$
- (ii)  $s_i$  ist homogen vom Grad  $i$ , denn  $g$  ist homogen vom Grad  $n \implies$  Koeffizient von  $X^{n-i}$  in  $g$  ist homogen vom Grad  $i$ .

**Übung 3.17.** Es gelten:

$$s_1 = \sum_{i=1}^n X_i, \quad s_n = \prod_{i=1}^n X_i$$

$$s_i(X_1, \dots, X_n) = \sum_{1 \leq j_1 < j_2 < \dots < j_i \leq n} X_{j_1} X_{j_2} \dots X_{j_i}$$

$$(n=3, i=2 \rightsquigarrow s_2 = X_1 X_2 + X_1 X_3 + X_2 X_3)$$

**Definition 3.18.** Die Polynome  $s_1, \dots, s_n \in R[X_1, \dots, X_n]^{S_n}$  sind die elementar symmetrischen Polynome in  $X_1, \dots, X_n$  (homogen vom Grad  $1, 2, \dots, n$ ) ( $s_i = i$ -tes elementar symmetrisches Polynom)

**Satz 3.19.** Sei  $\psi : R[Y_1, \dots, Y_n] \rightarrow R[X_1, \dots, X_n]$  der Ringhomomorphismus

$$h(Y_1, \dots, Y_n) \mapsto h(s_1, \dots, s_n)$$

Dann gilt

(a)  $\psi$  ist Ringhomomorphismus mit  $\psi|_R = \text{id}_R$  und  $\psi(Y_i) = s_i$  und  $\text{Bild}(\psi) \subseteq R[X_1, \dots, X_n]^{S_n}$

(b)  $\psi$  definiert einen Ringisomorphismus

$$R[Y_1, \dots, Y_n] \rightarrow R[X_1, \dots, X_n]^{S_n}$$

**Beispiel.**  $n = 4, f = X_1^2 + X_2^2 + X_3^2 + X_4^2$

$$\begin{aligned} & \underbrace{(X_1 + \dots + X_4)^2}_{s_1} - 2 \underbrace{(X_1X_2 + X_1X_3 + X_2X_3 + X_1X_4 + X_2X_4 + X_3X_4)}_{s_2} \\ &= s_1^2 - 2s_2^2 = h(s_1, s_2), h = Y_1^2 - 2Y_2 \end{aligned}$$

**Wiederholung.**

(a)  $R[X_1, \dots, X_n] \subseteq R[X_1, \dots, X_n]^{S_n}$  symmetrische Polynome.

(b) Elementar symmetrische Polynome  $s_1, \dots, s_n \in K[X_1, \dots, X_n]^{S_n}$  mit

$$s_i(X_1, \dots, X_n) = \sum_{1 \leq j_1 < \dots < j_i \leq n} \prod_{1 \leq k \leq i} X_{j_k} = \sum_{1 \leq j_1 < \dots < j_i \leq n} X_{j_1} \cdot \dots \cdot X_{j_i}$$

*Beweis.* (zu Satz 3.19)

Teil (a) Klar

$$\text{Bild}(\psi) = \left\{ \sum_{m \in \mathbb{N}_0} \underbrace{a_m}_{\in R} \cdot \underbrace{s_1^{m_1} \cdot \dots \cdot s_n^{m_n}}_{\text{symm. Pol.}} \right\}$$

Teil (b) benötigt Vorbereitungen.

□

**Bemerkung.** Sei  $R = K$  ein Körper,  $\alpha_1, \dots, \alpha_n$  die Nullstellen von  $f = X^n - \alpha_1 X^{n-1} + a_2 X^{n-2} \mp \dots + (-1)^n a_n \in K[X]$ , dann gilt  $\alpha_i = s_i(\alpha_1, \dots, \alpha_n)$ , denn:  $f = (X - \alpha_1) \cdot \dots \cdot (X - \alpha_n)$ . (hatten  $s_i$  erhalten als die Koeffizienten von  $(-1)^i X^{n-i}$  in  $(X - X_1) \cdot \dots \cdot (X - X_n)$ )

**Definition 3.20** (Lex-Ordnung).

(a) Definiere auf  $\mathbb{N}_0^n$  die Relation  $\leq$  durch  $\ell = (\ell_1, \dots, \ell_n) \leq m = (m_1, \dots, m_n) :$   
 $\iff \ell = m$  oder  $\exists i \in \{1, \dots, n\}$  mit  $\ell_1 = m_1, \dots, \ell_{i-1} = m_{i-1}, \ell_i < m_i$ . Dies definiert eine Totalordnung auf  $\mathbb{N}_0^n$ , die lexikographische Ordnung. Schreibe  $\ell < m$  für  $\ell \leq m$  und  $\ell \neq m$ . Für primitive Monome schreibe

$$X^\ell \leq X^m \iff \ell \leq m$$

(b) Der leitgrad von  $f = \sum_{m \in \mathbb{N}_0^n} a_m X^m$  ist  $\text{in}(f) := \max\{m \in \mathbb{N}_0^n \mid a_m \neq 0\} \in \mathbb{N}_0^n \cup \{-\infty\}$  (mit der Konvention  $\text{in}(0) = -\infty$ ) der Leitkoeffizient von  $f \neq 0$  ist  $a_{\text{in}(f)}$ .

**Beispiel.**  $\text{in}(\underbrace{X_1^3 X_2^2 + X_1^4 X_3}_{\in R[X_1, X_2, X_3]}) = (4, 0, 1) \in \mathbb{N}_0^3$

**Proposition 3.21.** Seien  $f = \sum_{\ell \in \mathbb{N}_0^n} a_\ell X^\ell, g = \sum_{m \in \mathbb{N}_0^n} b_m X^m, \ell_0 = \text{in}(f), m_0 = \text{in}(g)$ . Dann:

(a) Für  $m, \ell, m', \ell' \in \mathbb{N}_0^n$  gilt

$$m \geq \ell, m' \geq \ell' \implies m + m' \geq \ell + \ell'$$

(gilt dabei  $m \neq \ell$  oder  $m' \neq \ell'$ , so folgt  $m + m' > \ell + \ell'$ )

(b)  $\text{in}(f \cdot g) \leq \ell_0 + m_0$  und es gilt  $\text{in}(f \cdot g) = \ell_0 + m_0$  falls die Leitkoeffizienten  $a_{\ell_0} \cdot b_{m_0} \neq 0$ .

(c)  $\text{in}(f \cdot g) \leq \max(\text{in}(f), \text{in}(g))$  und es gilt Gleichheit falls  $\text{in}(f) \neq \text{in}(g)$ .

(d)  $\text{in}(s_i) = (\underbrace{1, \dots, 1}_i, \underbrace{0, \dots, 0}_{n-i}) =: \xi_i \in \mathbb{N}_0^n$  für  $i \in \{1, \dots, n\}$ .

(e)  $\xi_1, \dots, \xi_n$  sind linear unabhängig als Elemente von  $\mathbb{Q}^n$ , und also ist  $\varphi_i : \mathbb{N}_0^n \rightarrow \mathbb{N}_0^n, (a_i) \mapsto \sum a_i \xi_i$  injektiv und  $\varphi^{-1}$  ist durch die Formel (für Elemente im Bild)

$$(b_i) \mapsto (b_1 - b_2, b_2 - b_3, \dots, b_{n-1} - b_n, b_n)$$

*Beweis.* (a) (Übung) Es genügt zu zeigen  $m \geq \ell \implies m + m' \geq \ell + m'$  (mit  $> \implies >$ ) genügt mit Induktion zu zeigen:  $m \geq \ell \implies m + e_j \geq \ell + e_j$ , ( $e_j = (0, \dots, 0, 1, 0, \dots, 0)$ )

(b)  $f \cdot g = (\sum a_\ell X^\ell)(\sum b_m X^m) = \sum_{\ell, m} a_\ell b_m X^{\ell+m}$  falls  $a_\ell b_m \neq 0$  (nur solche Terme tragen zu  $f \cdot g$  bei), so folgt  $\ell \leq \ell_0$  und  $m \leq m_0$ ,  $\ell_0, m_0$  die Leitkoeffizienten.  $\xRightarrow{(a)} \ell + m \geq \ell_0 + m_0 \implies \text{in}(f \cdot g) \leq \ell_0 + m_0$ .

Außerdem: (Koeffizient von  $X^{\ell_0+m_0} = ?$ ) gilt  $\ell + m = \ell_0 + m_0$ , so muss wegen (a)  $\ell = \ell_0$  und  $m = m_0$  gelten, falls  $a_\ell \neq 0$  und  $b_m \neq 0 \implies$  Koeffizient von  $X^{\ell_0+m_0}$  ist  $a_{\ell_0} \cdot b_{m_0}$ . Also  $\text{in}(fg) = m_0 + \ell_0$ , falls  $a_{\ell_0} b_{m_0} \neq 0$ .

(c)  $f + g = \sum_m (a_m + b_m) X^m$ : Im Fall  $a_m + b_m \neq 0$ , so folgt  $a_m \neq 0$  oder  $b_m \neq 0 \implies m \leq \ell_0$  oder  $m \leq m_0 \implies m \leq \max\{\ell_0, m_0\}$ .

Für Zusatz: Gelte o.E.  $\ell_0 < m_0$ , dann ist der Koeffizient von  $X^{m_0}$  gleich  $a_{m_0} + b_{m_0} \neq 0$ , wobei  $a_{m_0} = 0$  wegen  $m_0 \geq \text{in}(f)$ , und  $b_{m_0} \neq 0$ , da  $m_0 = \text{in}(f)$ . Also folgt  $\text{in}(f + g) = \max\{\ell_0, m_0\}$ .

(d)  $s_i = \sum_{i \leq j_1 < j_2 < \dots < j_i \leq n} X_{j_1} \cdot \dots \cdot X_{j_i}$  größtes Monom (mit Koeffizient  $\neq 0$ ) in der Summe ist  $X_1 \cdot \dots \cdot X_i \implies \text{in}(s_i) = (1, \dots, 1, 0, \dots, 0) = (\delta_{j \leq i})_{1 \leq j \leq n}$ .

(e) (Übung) zur linearen Algebra,  $\varphi$  hat Darstellungsmatrix

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & 1 \end{pmatrix}$$

und  $\varphi^{-1}$

$$\begin{pmatrix} 1 & -1 & & & \\ & 1 & -1 & & \\ & & \ddots & \ddots & \\ & & & 1 & -1 \\ & & & & 1 \end{pmatrix} : \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_{n-1} \\ t_n \end{pmatrix} \mapsto \begin{pmatrix} t_1 - t_2 \\ t_2 - t_3 \\ \vdots \\ t_{n-1} - t_n \\ t_n \end{pmatrix}. \quad \square$$

*Beweis von Satz 3.19.*  $\square$

**Definition 3.22.** Die Diskriminante von  $f(X) = X^n - a_1X^{n-1} + a_2X^{n-2} \mp \dots + (-1)^n a_n \in R[T]$  ist  $D(f) := d_n(a_1, \dots, a_n)$  Polynom in  $n$ -Variablen über  $R$ .

**Bedeutung.** Sei  $R$  ein Körper und seien  $\alpha_1, \dots, \alpha_n$  die Nullstellen von  $f$ , so dass  $\alpha_i = s_i(\alpha_1, \dots, \alpha_n)$ , dann folgt:

$$\begin{aligned} D(f) &= d_n(s_1(\alpha_1, \dots, \alpha_n), \dots, s_n(\alpha_1, \dots, \alpha_n)) \\ &= D_n(\alpha_1, \dots, \alpha_n) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2. \end{aligned}$$

d.h.  $D(f)$  erkennt ob mehrfache Nullstelle vorliegt. Jedes symmetrische Polynom in den Nullstellen von  $f$  lässt sich schreiben als ein Polynom in den Koeffizienten von  $f$ .

**Wiederholung 3.23.** Sei  $R$  ein kommutativer Ring (im Weiteren),  $I \subseteq R$  ist ein Ideal von  $R$ , falls  $RI \subseteq I, I + I \subseteq I$ .

**Notation.** Für  $a \in R$  sei  $(a) = Ra$  das Hauptideal in  $R$ , Erzeuger  $a$ . Für  $a_1, \dots, a_n \in R$  sei  $(a_1, \dots, a_n) = Ra_1 + Ra_2 + \dots + Ra_n \subseteq R$  Ideal.

**Bemerkung** (Übung). Für  $I \subseteq R$  ein Ideal:  $1 \in I \iff I = R$ , für  $S \subseteq R$  Unterring:  $S = R \iff RS \subseteq S$ .

**Proposition 3.24.** Sei  $\varphi : R \rightarrow R'$  ein Ringhomomorphismus, dann gelten:

- (i) Ist  $I' \subseteq R'$  ein Ideal, so ist  $\varphi^{-1}(I') \subseteq R$  ein Ideal.
- (ii) Kern  $\varphi = \varphi^{-1}(\{0\}) \subseteq R$  ist ein Ideal.
- (iii) Bild( $\varphi$ ) =  $\{\varphi(r) \mid r \in R\} \subseteq R'$  ist ein Unterring.
- (iv) Ist  $\varphi$  surjektiv und  $I \subseteq R$  ein Ideal, so ist  $\varphi(I) \subseteq R'$  ein Ideal.

*Beweis.* nur (iv)

(iv)

$$\varphi(I) + \varphi(I) = \underbrace{\{\varphi(a) + \varphi(b) \mid a, b \in I\}}_{\varphi(a+b)} = \varphi(I + I) \underset{I+I \subseteq I}{\subseteq} \varphi(I)$$

(benötigt nicht, dass  $\varphi$  surjektiv)

$$R' \cdot \varphi(I) \underset{\varphi \text{ surj.}}{=} \varphi(R)\varphi(I) = \{\varphi(r)\varphi(a) \mid r \in R, a \in I\} = \varphi(RI) \underset{RI \subseteq I}{\subseteq} \varphi(I)$$

Also  $\varphi(I) \subseteq R'$  ist ein Ideal. □

**Definition 3.25** (Charakteristik). Die Charakteristik von  $R$  ist

$$\text{char}(R) := \begin{cases} 0, & n \cdot 1_R \neq 0_R, \forall n \in \mathbb{N} \\ \min\{n \in \mathbb{N} \mid n \cdot 1_R = 0_R\}, & \exists n \in \mathbb{N} : n \cdot 1_R = 0_R \end{cases}$$

**Beispiel.**

$$\text{char}(\mathbb{Z}) = 0, \text{char}(\mathbb{Z}/_n\mathbb{Z}) = n, n \in \mathbb{N}$$

**Bemerkung** (Übung). (a) Sei  $\text{ord}(1_R)$  die Ordnung von  $1_R$  in  $(R, 0_R, +)$ , dann

$$\text{char}(R) = \begin{cases} \text{ord}(1_R), & \text{ord}(1_R) \neq \infty \\ 0, & \text{ord}(1_R) = \infty \end{cases}$$

(b) Sei  $\varphi: \mathbb{Z} \rightarrow R$  der eindeutige Ringhomomorphismus

$$\varphi(1_{\mathbb{Z}}) := 1_R \implies \varphi(n_{\mathbb{Z}}) = n \cdot 1_R, \forall n \in \mathbb{Z}$$

Dann gilt:  $\text{char}(R)$  ist der (eindeutige) Erzeuger in  $\mathbb{N}$  von  $\text{Kern}(\varphi) \subseteq \mathbb{Z}$  (ein Ideal) (“Grund für die Definition von  $\text{char}(R)$ ”)

**Proposition 3.26.** *Ist  $K$  ein Körper, so ist  $\text{char } K$  Null oder eine Primzahl.*

*Beweis.* Annahme:  $\text{char } K \in \mathbb{N}$  und ist keine Primzahl  $\implies \exists n, m \in \mathbb{N}$  mit  $n > 1, m > 1$ , sodass  $\text{char } K = n \cdot m > \max\{n, m\}$

Definition der Charakteristik gibt:

$$n \cdot m \cdot 1_K = 0_K \implies \underbrace{n \cdot 1_K}_{\neq 0 (*)} \cdot \underbrace{m \cdot 1_K}_{\neq 0 (*)} = 0$$

(\*) da  $n, m < n \cdot m = \text{char } K$ . Da  $K$  ein Körper  $\implies K$  ist nullteilerfrei  $\implies n \cdot 1_K = 0$  oder  $m \cdot 1_K = 0$ . Widerspruch zu (\*).  $\square$

**Beispiel** (Übung). Sei  $R$  ein Ring mit  $\text{char}(R) = p$  eine Primzahl, dann gelten:

(a)  $\varphi_R = R \rightarrow R, a \mapsto a^p$  ist ein Ringhomomorphismus.

(b) Es gilt  $\varphi_{\mathbb{F}_p} = \text{id}_{\mathbb{F}_p}$ , wobei  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ , d.h.  $\forall a \in \mathbb{F}_p$  gilt  $a^p = a$ .

**Wiederholung.** Für  $I \subseteq R$  ein Ideal, hatten Faktoring  $R/I$  und Faktorabbildung  $\pi: R \rightarrow R/I, r \mapsto r + I$  (vgl. Satz 1.49)

**Satz 3.27** (Homomorphiesatz für Ringe). *Sei  $\varphi: R \rightarrow R'$  ein Ringhomomorphismus und  $I \subseteq \text{Kern}(\varphi)$  ein Ideal von  $R$ , dann:*

(a)  $\exists!$  Ringhomomorphismus  $\bar{\varphi}: R/I \rightarrow R'$  mit  $\bar{\varphi}(r + I) = \varphi(r)$ , d.h. folgendes Diagramm kommutiert:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ \pi \downarrow & \nearrow \bar{\varphi} & \\ R/I & & \end{array}$$

(b) Ist  $I = \text{Kern}(\varphi)$ , so definiert  $\bar{\varphi}$  aus (a) einen Ringisomorphismus

$$R/\text{Kern}(\varphi) \rightarrow \text{Bild}(\varphi) \subseteq R', r + \text{Kern}(\varphi) \mapsto \varphi(r)$$

*Beweis.* (Übung) analog zum Beweis vom Homomorphiesatz für Gruppen (Satz 1.45).  $\square$

**Satz 3.28** (Isomorphiesatz für Ringe). Sei  $\varphi : R \rightarrow R'$  ein surjektiver Ringhomomorphismus  $\left(R' \cong R/\text{Kern}(\varphi)\right)$ , seien  $X = \{I \subseteq R \text{ Ideal} \mid \text{Kern}(\varphi) \subseteq I\}$ ,  $X' = \{I' \subseteq R' \mid I' \text{ Ideal}\}$ . Dann gelten:

(a) Die Abbildung  $X' \rightarrow X, I' \mapsto \varphi^{-1}(I')$  ist eine Bijektion mit Umkehrabbildung  $X \rightarrow X', I \mapsto \varphi(I)$ .

(b) Für  $I \subseteq R$  ein Ideal und  $I = \varphi^{-1}(I')$  ist die Abbildung

$$R/I \rightarrow R'/I', r + I \mapsto \varphi(r) + I'$$

ein Ringisomorphismus.

*Beweis.* (Übung) analog zum Beweis vom 2. Isomorphiesatz für Gruppen (Satz 1.51).  $\square$

**Notation.** Für  $I, J \subseteq R$  sei  $I \cdot J = \{\sum_i a_i b_i \mid a_i \in I, b_i \in J\}$ , d.h. (Übung)  $I \cdot J$  ist das kleinste Ideal in  $R$ , das  $\{a \cdot b \mid a \in I, b \in J\}$  enthält.

**Satz 3.29** (Chinesischer Restsatz). Seien  $I_1, \dots, I_t \subseteq R$  Ideale, die "paarweise koprim" sind, d.h.  $I_i + I_j = R$  für  $i \neq j \in \{1, \dots, t\}$ . Dann gelten:

(a)  $I_i$  und  $\prod_{j \neq i \in \{1, \dots, t\}} I_j$  sind koprim.

(b)  $I_1 \cdot \dots \cdot I_t = \bigcap_{i \in \{1, \dots, t\}} I_i$ .

(c) Die Abbildung

$$R/\prod_{i \in \{1, \dots, t\}} I_i = R/I_1 \cdot \dots \cdot I_t \xrightarrow{\cong} \prod_{i \in \{1, \dots, t\}} R/I_i = R/I_1 \times \dots \times R/I_t$$

$$r + I_1 \cdot \dots \cdot I_t \mapsto (r + I_1, \dots, r + I_t)$$

ist wohl-definiert und ein Ringisomorphismus. Also gilt

$$R/\prod_{i \in \{1, \dots, t\}} I_i \cong \prod_{i \in \{1, \dots, t\}} R/I_i$$

*Beweis.* In der LA2 für  $R$  ein Hauptidealring, allgemein: siehe Jantzen-Schwermer, Satz III.3.10  $\square$

### 3.4 Ringe von Brüchen/Lokalisierung

**Definition 3.30.** Eine Teilmenge  $S \subseteq R$  heißt multiplikativ abgeschlossen  $\iff$   $S$  ist ein Untermonoid von  $(R, 1, \cdot)$ .

**Beispiel.** (i)  $S = \mathbb{Z} \setminus \{0\} \subseteq \mathbb{Z}$  ist multiplikativ abgeschlossen.

(ii)  $S^p = \mathbb{Z} \setminus p\mathbb{Z} \subseteq \mathbb{Z}$  ist multiplikativ abgeschlossen.

(iii)  $S_p = \{p^n \mid n \in \mathbb{N}_0\} \subseteq \mathbb{Z}$  ist multiplikativ abgeschlossen.

Es gilt  $S = S^P \cdot S_p$

**Definition 3.31.** Definiere eine Äquivalenzrelation auf  $R \times S$  ( $S \subseteq R$  multiplikativ abgeschlossen) durch

$$(r, s) \sim (r', s') : \iff \exists t \in S : t(rs' - r's)$$

Denn:

$\sim$  reflexiv:  $(r, s) \sim r, s$ , da  $1 \cdot (rs - rs) = 0$ .

$\sim$  symmetrisch: Gelte  $(r, s) \sim (r', s')$ , d.h.  $\exists t \in S : t(rs' - r's) = 0 \implies t(r's - rs') = 0 \implies (r', s') \sim (r, s)$ .

$\sim$  transitiv: Gelte  $(r, s) \sim (r', s')$  und  $(r', s') \sim (r'', s'')$ , d.h.  $\exists t, t' \in S : t(rs' - r's) = 0$  und  $t'(r's'' - r''s') = 0$ . Gemeinsamer Nenner  $tt'ss's''$

$$\implies tt's''(rs' - r's) = 0, tt's(r's'' - r''s) = 0$$

$$\implies tt's''rs' - tt'sr''s' = 0 = tt's'(rs'' - r''s) \implies (r, s) \sim (r'', s'')$$

Schreibe:  $\frac{r}{s}$  für die Äquivalenzklasse von  $(r, s)$  und  $S^{-1}R$  für  $R \times S / \sim$ .

Beachte:  $\frac{r}{s} = \frac{r'}{s'} \iff \exists t \in S : \frac{ts'r}{tss'} = \frac{tsr'}{tss'}$  gilt  $ts'r = tsr'$ , beachte zudem  $\frac{r}{s} = \frac{tr}{ts}$ , für  $t \in S$ .

**Satz 3.32.** Sei  $S \subseteq R$  multiplikativ abgeschlossen, dann:

(a) Die Verknüpfungen  $+, \cdot$  auf  $S^{-1}R$  definiert durch

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}, \quad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$$

sind wohl-definiert.

(b)  $S^{-1}R = (S^{-1}R, \frac{0}{1}, \frac{1}{1}, +, \cdot)$  ist ein kommutativer Ring.

(c) Die Lokalisierung von  $R$  an  $S$

$$\varphi : R \rightarrow S^{-1}R, r \mapsto \frac{r}{1}$$

ist ein Ringhomomorphismus. (Klar aus der Definition von  $+$  und  $\cdot$ )

(d) (Universelle Eigenschaft) Ist  $\psi : R \rightarrow R'$  ein Ringhomomorphismus, so dass  $\psi(S) \leq (R')^\times$ , so existiert ein eindeutiger Ringhomomorphismus  $\hat{\psi} : S^{-1}R \rightarrow R'$  mit  $\hat{\psi}|_R = \psi$ , nämlich  $\hat{\psi}(\frac{r}{s}) = \psi(r) \cdot \psi(s)^{-1}$ .

**Beispiel.**  $(\mathbb{Z} \setminus \{0\})^{-1}\mathbb{Z} = \mathbb{Q}, \mathbb{Z}^{-1}\mathbb{Z} = 0\text{-Ring}$ .

*Beweis.*

(a)  $+$  und  $\cdot$  sind wohldefiniert: Gelte  $\frac{r}{s} = \frac{a}{b}$  und  $\frac{r'}{s'} = \frac{a'}{b'}$  mit  $r, r', a, a' \in R, s, s', b, b' \in S$ , zu zeigen ist:

$$\frac{rs' + r's}{ss'} = \frac{ab' + a'b}{bb'}$$

Voraussetzung:  $\exists t, t' \in S : t(rb - as) = 0, t'(r'b' - a's') = 0$ . Gemeinsamer Nenner:  $ss'bb'tt'$ , also

$$tt'b's'(rb - as) = 0, \quad tt'sb(r'b' - a's') = 0$$

$$\implies tt'b's'rb - tt'b's'as + tt'sbr'b' - tt'sba's' = 0$$

$$= tt'b'b(rs' + r's) - tt'ss'(ab' - a'b) \implies \frac{rs' + r's}{ss'} = \frac{ab' + a'b}{bb'}$$



(b) - (d) Siehe Jantzen Schwermer III.4.2 oder Übung. □

**Definition 3.33** (Nullteiler). (a)  $x \in R$  heißt Nullteiler  $\iff \exists y \in R \setminus \{0\}$  mit  $xy = 0$

(b)  $R$  heißt Integritätsbereich (IB)  $\iff 0_R \neq 1_R$  und  $0_R$  ist der einzige Nullteiler.

**Bemerkung 3.34.**  $R$  ist Integritätsbereich  $\iff$  man darf in  $R$  kürzen und  $0_R \neq 1_R$

$$\iff \forall a, b, c \in R : a \neq 0 : a \cdot b = a \cdot c \implies b = c$$

Übung

Denn  $ab = ac \iff a(b - c) = 0$

**Beispiel.** (i) Jeder Körper ist ein Integritätsbereich.

(ii)  $\mathbb{Z}, K[X]$  sind Integritätsbereich.

(iii) Jeder Unterring eines Körpers ist ein Integritätsbereich.

(iv) Jeder Unterring eines Integritätsbereichs ist ein Integritätsbereich.

**Lemma 3.35.** Sei  $S \subseteq R$  multiplikativ abgeschlossen, dann gilt: enthält  $S$  keine Nullteiler, so ist

$$\varphi : R \hookrightarrow S^{-1}R, r \mapsto \frac{r}{1}$$

injektiv.

*Beweis.* Für  $r \in R : \varphi(r) = 0 \iff \frac{r}{1} = \frac{0}{1} \iff \exists t \in S : t(r \cdot 1 - 0 \cdot 1) = 0 = tr$ , da  $S$  nullteilerfrei  $\iff r = 0$ . □

**Korollar 3.36.** Sei  $R$  ein Integritätsbereich, dann:

(a)  $S = R \setminus \{0\}$  multiplikativ abgeschlossen.

(b)  $S^{-1}R$  ist ein Körper.

(c)  $R \rightarrow S^{-1}R$  ist injektiv (also ist  $R$  Unterring des Körpers  $S^{-1}R$ )

*Beweis.* (a) Klar,  $a, b \neq 0 \implies a \cdot b \neq 0$  ( $a, b$  keine Nullteiler)

(b) Sei  $\frac{r}{s} \in S^{-1}R \setminus \{\frac{0}{1}\}$ , Behauptung:  $r \neq 0$  (also  $r \in S$ )  $\implies \frac{s}{r}$  ist Inverses von  $\frac{r}{s}$ . Beweis der Behauptung: Angenommen  $r = 0 \implies \frac{0}{s} \neq \frac{0}{1}$ , Widerspruch, da  $\frac{0}{1} = \frac{0}{1} (1 \cdot (0 \cdot 1 - 0 \cdot s) = 0)$

(c) Folgt aus Lemma 3.35. □

**Definition 3.37** (Quotientenkörper).  $S^{-1}R = \text{Quot}(R)$  heißt Quotientenkörper von  $R$ .

**Bemerkung 3.38.** Jeder Integritätsbereich ist Unterring eines Körpers (seinem Quotientenkörper).

### 3.5 Spezielle Ideale

**Definition 3.39.** Sei  $I \subseteq R$  ein echtes Ideal (d.h.  $I \subsetneq R$ ), dann

(a)  $I$  ist **Primideal**  $\iff \forall a, b \in R$  gilt:

$$a \cdot b \in I \implies a \in I \vee b \in I$$

(b)  $I$  heißt **maximales Ideal**  $\iff \forall J \subsetneq R$  Ideale mit  $I \subseteq J$  gilt  $I = J$

**Proposition 3.40.** Seien  $P, M \subseteq R$  Ideale, dann:

(a)  $P$  ist ein Primideal  $\iff R/P$  ist ein Integritätsbereich.

(b)  $R$  ist ein Körper  $\iff \{0\}$  und  $R$  sind die einzigen Ideale von  $R$  und  $0_R \neq 1_R$ .

(c)  $M$  ist ein maximales Ideal  $\iff R/M$  ist ein Körper.

(d) Jedes maximale Ideal ist ein Primideal.

*Beweis.*

(a)  $P$  Primideal  $\implies P \subsetneq R$  und  $\forall a, b \in R : a \cdot b \in P \implies a \in P \vee b \in P \implies R/P \neq 0\text{-Ring}$  und  $\forall a, b \in R :$

$$(a + P)(b + P) \subseteq P \implies a + P = P \vee b + P = P$$

$$\implies R/P \neq 0\text{-Ring} \text{ und } \forall \bar{a}, \bar{b} \in R/P :$$

$$\bar{a} \cdot \bar{b} = 0 \implies \bar{a} = 0 \vee \bar{b} = 0$$

$\implies R/P$  ist ein Integritätsbereich. Man kann auch "rückwärts laufen"  
 $\implies$  die Äquivalenz in (a).

(b) Übung.

(c) Folgt aus (b) und dem Isomorphiesatz für Ringe. (der postuliert Bijektion  
 $: \{\text{Ideale } J \subseteq R \mid M \subseteq J \subseteq R\} \text{ und } \{\text{Ideale } \bar{J} \subseteq R/M \mid \{\bar{0}\} \subseteq \bar{J} \subseteq R/M\}$ ).

(d) Folgt aus (c) und (a), da Körper Integritätsbereiche sind.  $\square$

**Beispiel 3.41.** (a) Ist  $R$  ein Integritätsbereich und kein Körper, so ist  $\{0\}$  ein Primideal, aber nicht maximal.

(b) In  $R = K[X, Y]$  sind  $\{0\} \subsetneq X \subsetneq (X, Y) \subsetneq K$  Primideal.

**Wiederholung** (Grundlagen). Eine Relation  $\leq$  auf einer Menge  $M$  heißt [Halbordnung]  
 $\iff \leq$  ist reflexiv, transitiv und antisymmetrisch. ( $\leq$  antisymmetrisch bedeutet:  $x \leq y \wedge y \leq x \implies x = y$ ). Eine Halbordnung heißt **Totalordnung**  
 $\iff \forall x, y \in M : x \leq y \vee y \leq x$ .

**Definition 3.42.** Sei  $(M, \leq)$  eine halbgeordnete Menge.

(a) Eine Teilmenge  $N \subseteq M$  heißt **Kette**  $\iff (N, \leq|_{N \times N})$  ist eine Totalordnung.

(b) Eine Teilmenge  $P \subseteq M$  besitzt eine obere Schranke (in  $M$ )  $\iff \exists m \in M$ , sodass  $\forall p \in P : p \leq m$ .

(c)  $m \in M$  heißt maximales Element  $\iff \nexists m' \in M : m' > m$

**Beispiel.** (a) Ist  $M$  eine beliebige Menge und  $\mathcal{P}(M)$  eine Potenzmenge, so ist  $(\mathcal{P}(M), \subseteq)$  eine Halbordnung.  $M$  ist obere Schranke für jede Teilmenge von  $\mathcal{P}(M)$ .

(b)  $\mathbb{N}_0$  besitzt keine obere Schranke.

Wir betrachten nun die folgenden beiden Axiome der axiomatischen Mengenlehre:

**Axiom** (Zorn's Lemma). Sei  $(M, \leq)$  eine Halbordnung ( $M \neq \emptyset$ ). Besitzt jede Kette in  $M$  eine obere Schranke, so besitzt  $M$  ein maximales Element. Dies nehmen wir als Axiom an.

**Axiom** (Auswahlaxiom). Ist  $I$  eine Menge und  $(A_i)_{i \in I}$  eine Familie von nichtleeren Mengen (indiziert mit  $I$ ), so  $\exists$  Funktion  $f : I \rightarrow \bigcup_{i \in I} A_i$ , mit  $f(i) \in A_i$ .

**Satz** (Halmos, Naive Set Theory, 62-65). Zorn's Lemma  $(\forall (M, \leq))$  und das Auswahlaxiom  $(\forall I, \forall (A_i)_{i \in I})$  sind äquivalent.

**Satz 3.43.** Sei  $I \subseteq R$  ein echtes Ideal, dann  $\exists$  maximales Ideal  $M \subsetneq R$  mit  $I \subseteq M$ . Insbesondere hat  $R$  maximale Ideale (Satz für  $I = (0)$ )

*Beweis.* Sei  $X$  die Menge aller Ideale  $J \subsetneq R$  mit  $I \subseteq J$ . Wegen  $I \in X$  gilt  $X \neq \emptyset$ .  $(X, \subseteq)$  ist halbgeordnete Menge.

Behauptung: Zorn's Lemma ist anwendbar.

Denn: Sei  $X_0 \subseteq X$  eine Kette (o.E.  $X_0 \neq \emptyset$ ). Definiere  $J_\infty := \bigcup_{J \in X_0} J$ .

Zu zeigen:  $J_\infty \in X \implies J_\infty$  ist obere Schranke von  $X_0$ . Klar ist  $I \subseteq J_\infty$  und  $1 \notin J_\infty (\implies J_\infty \subsetneq R)$

Zu zeigen:  $J_\infty$  ist ein Ideal. Seien  $a, b \in J_\infty$  und  $r \in R$ . Nach Definition von  $J_\infty \exists J, J' \in X_0$  mit  $a \in J, b \in J'$ . Nun ist aber  $X_0$  totalgeordnet unter  $\subseteq$ . D.h.  $J \subseteq J'$  oder  $J' \subseteq J$ . o.E.  $J' \subseteq J \implies a, b \in J \implies a + b, r \cdot a \in J \implies a + b, ra \in J_\infty$ , da  $J \subseteq J_\infty$ , damit ist die Behauptung gezeigt.

Sei  $M$  ein maximales Element von  $X$ . Dann ist  $M$  ein maximales Ideal von  $R$  (mit  $I \subseteq M$ ) sonst  $\exists J'' \subsetneq R$  ideal mit  $M \subsetneq J''$ , Widerspruch zu  $M$  maximales Element in  $X$ .  $\square$

**Übung.** (Plenarübung 3) Zorn's Lemma  $\implies$  jeder Vektorraum hat eine Basis.

## 3.6 Teilbarkeit in Integritätsbereichen

**Definition 3.44.** Sei bis auf Weiteres  $R$  ein Integritätsbereich,  $a, b \in R$ .

(a)  $a$  ist Teiler von  $b$  ( $a$  teilt  $b$ ,  $a \mid b$ ):  $\iff \exists c \in R : a \cdot c = b$ .

(b)  $a, b$  sind assoziiert ( $a \simeq b$ ):  $\iff \exists c \in R^\times : a \cdot c = b$ .

(c)  $a$  heißt irreduzibel (bzw. unzerlegbar) :  $\iff a \in R \setminus (R^\times \cup \{0\})$  und  $\forall c \in R : c \mid a \implies c \simeq a \vee c \simeq 1$ .

- (d)  $a$  heißt Primelement :  $\iff a \in R \setminus (R^\times \cup \{0\})$  und  $\forall b, c \in R : a \mid bc \implies a \mid b \vee a \mid c$ .

**Bemerkung 3.45** (Übung).

- (a)  $a \mid b \iff (b) \subseteq (a)$ .
- (b)  $a \simeq b \iff a \mid b \wedge b \mid a \iff (a) = (b)$  und  $\simeq$  ist eine Äquivalenzrelation. ("denn:"  $(R^\times, 1, \cdot)$  ist eine Gruppe).
- (c)  $Ra = (a) = (0) \iff a = 0$ .  $Ra = (1) \iff a \in R^\times \iff a \simeq 1$
- (d)  $a$  Primelement  $\iff (a)$  ist ein Primideal.
- (e)  $a$  ist irreduzibel  $\iff (0) \subsetneq (a) \subsetneq R$  und  $\nexists b \in R : (a) \subsetneq (b) \subsetneq R$ . (d.h.  $(a)$  ist maximal unter den Hauptidealen) und  $a \in R \setminus (R^\times \cup \{0\})$  ist reduzibel  $\iff \exists b, c \in R \setminus (R^\times \cup \{0\}) : a = b \cdot c \iff \exists b, c \in R : a = b \cdot c$  und  $(a) \subsetneq (b), (c) \subsetneq R$ .
- (f)  $a$  Primelement  $\implies a$  ist irreduzibel.

*Beweis zu (f).* Annahme:  $a$  ist reduzibel. Nach letzte Formulierung von (c)  $\exists b, c \in R : a = b \cdot c \wedge (a) \subsetneq (b), (c) \subsetneq R \implies$  in  $R/(a)$  gilt  $\bar{0} = \bar{a} = \bar{b} \cdot \bar{c}$  und  $\bar{0} \neq \bar{b}, \bar{c} \implies R/(a)$  kein Integritätsbereich  $\implies (a)$  kein Primideal, Widerspruch zu (d), da  $a$  Primelement.  $\square$

**Definition 3.46 (Hauptidealring).** Ein Integritätsbereich heißt **Hauptidealring** (HI-Ring), wenn jedes Ideal ein Hauptideal ist.

**Definition 3.47.** Ein Integritätsbereich  $R$  heißt **euklidischer Ring**, wenn  $\exists \lambda : R \setminus \{0\} \rightarrow \mathbb{N}_0$ , sodass gilt:

$$\forall a, b \in R \exists q, r \in R : a = qb + r, (r = 0 \vee \lambda(r) < \lambda(b)) \quad (*)$$

**Bezeichnung.**

- (a)  $(*)$  heißt Division mit Rest.
- (b)  $\lambda$  heißt euklidische Funktion.

**Beispiel 3.48.** (a)  $\mathbb{Z}$  ist ein euklidischer Ring mit

$$\lambda : \cdot : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}_0, n \mapsto |n|$$

(b)  $K[X]$  ist ein euklidischer Ring mit

$$\lambda = \text{Grad} : K[X] \setminus \{0\} \rightarrow \mathbb{N}_0, f \mapsto \text{Grad } f$$

**Proposition 3.49.** Ist  $R$  ein euklidischer Ring  $\implies R$  ist ein Hauptidealring.

*Beweis.* Sei  $I \neq \{0\}$  ein Ideal. Sei  $a \in I \setminus \{0\}$  ein Element, sodass

$$\lambda(a) = \min\{\lambda(b) \mid b \in I \setminus \{0\}\} \in \mathbb{N}_0$$

Behauptung:  $I = (a)$  ( $I \supseteq$  klar, da  $a \in I$ ).

Dazu: Sei  $b \in I$  beliebig. Wende Division mit Rest an

$$b = qa + r, \quad r = 0 \vee \lambda(r) < \lambda(a)$$

$$\implies r = b - qa \in I - I \subseteq I \implies b = qa \in (a). \quad \square$$

**Proposition 3.50.** Sei  $R$  ein Hauptidealring und  $a \in R \setminus (R^\times \cup \{0\})$ , dann sind äquivalent:

- (i)  $a$  irreduzibel.
- (ii)  $a$  Primelement.
- (iii)  $(a)$  ist Primideal.
- (iv)  $(a)$  ist maximales Ideal.
- (v)  $R/(a)$  ist ein Körper.

*Beweis.* • (iv)  $\iff$  (v) folgt aus Bemerkung 40(c)

- (i)  $\implies$  (iv) folgt aus Bemerkung 45(e) ( $a$  irreduzibel  $\implies (a)$  ist maximal unter Hauptidealen)
- (iv)  $\implies$  (iii) folgt aus Bemerkung 40(d)
- (iii)  $\implies$  (ii) folgt aus Bemerkung 45(d)
- (ii)  $\implies$  (i) folgt aus Bemerkung 45(f)

$\square$

**Definition 3.51.** Seien  $a, b \in R$

- (a)  $d \in R$  heißt ggT (**größter gemeinsamer Teiler**) von  $a, b$ , wenn  $d \mid a, d \mid b$  und  $\forall c \in R : c \mid a, c \mid b \implies c \mid d$ .
- (b)  $d \in R$  heißt kgV (**kleinstes gemeinsames Vielfaches**) von  $a, b$ , wenn  $a \mid d, b \mid d$  und  $\forall c \in R : a \mid c, b \mid c \implies d \mid c$ .
- (c)  $a, b$  heißen **teilerfremd**, wenn  $\text{ggT}(a, b) \simeq 1$ .

**Bemerkung** (Übung). ggT und kgV sind (sofern sie existieren) eindeutig bis auf Assoziiertheit.

**Notation.**  $d \simeq \text{ggT}(a, b)$  bedeutet  $d$  ist ggT von  $a, b$ .  $d \simeq \text{kgV}(a, b)$  bedeutet  $d$  ist kgV von  $a, b$ .

**Konvention 3.52.** Sei  $K[X]_+ = \{f \in K[X] \setminus \{0\} \mid f \text{ normiert}\} \cup \{0\}$ . In  $\left\{ \begin{smallmatrix} \mathbb{Z} \\ K[X] \end{smallmatrix} \right\}$  ist jedes Element zu einem eindeutigen Element in  $\left\{ \begin{smallmatrix} \mathbb{N}_0 \\ K[X]_+ \end{smallmatrix} \right\}$  assoziiert. Für  $f, g \in \left\{ \begin{smallmatrix} \mathbb{Z} \\ K[X] \end{smallmatrix} \right\}$  schreibe  $d = \text{ggT}(f, g)$  bzw.  $d = \text{kgV}(f, g)$   $\iff d \simeq \text{ggT}(f, g)$  bzw.  $d \simeq \text{kgV}(f, g)$  und  $d \in \left\{ \begin{smallmatrix} \mathbb{N}_0 \\ K[X]_+ \end{smallmatrix} \right\}$ .

**Satz 3.53.** Sei  $R$  ein Hauptidealring, dann gelten für  $a, b, c \in R$ :

- (a) (i)  $c \simeq \text{ggT}(a, b) \iff$  (ii)  $(c) = (a) + (b)$   
 (b) (i)  $c = \text{kgV}(a, b) \iff$  (ii)  $(c) = (a) \cap (b)$   
 (c)  $\text{ggT}(a, b)$  und  $\text{kgV}(a, b)$  existieren  $\forall a, b \in R$   
 (d) Es sind Äquivalent: (i)  $\text{ggT}(a, b) \simeq 1$  ( $a, b$  teilerfremd)  $\iff$  (ii)  $(a) + (b) = R \iff$  (iii)  $\exists \alpha, \beta \in R : \alpha a + \beta b = 1$

*Beweis.* (Übung) □

**Bemerkung.** (a) Hauptidealringe haben die Bezout-Eigenschaft, d.h. zu  $a, b \in R \exists \alpha, \beta \in R : \alpha a + \beta b \simeq \text{ggT}(a, b)$ .

- (b) In euklidischen Ringen kann man den ggT mit dem euklidischen Algorithmus berechnen und  $\alpha, \beta$  wie in (a) mit dem erweiterten euklidischen Algorithmus.

**Satz/Definition 3.54.** Für einen Integritätsbereich  $R$  sind äquivalent:

- (i)  $\forall a \in R \setminus (R^\times \cup \{0\}) \exists t \in \mathbb{N} \exists \text{ Primelemente } p_1, \dots, p_t \in R \text{ mit } a \simeq p_1 \cdot \dots \cdot p_t$   
 (ii)  $\forall a \in R \setminus (R^\times \cup \{0\}) \exists t \in \mathbb{N} \exists \text{ irreduzible Elemente } p_1, \dots, p_t \in R \text{ mit } a \simeq p_1 \cdot \dots \cdot p_t$  und diese Darstellung ist eindeutig bis auf Indexpermutation und Assoziiertheit, d.h. gilt  $a \simeq q_1 \cdot \dots \cdot q_s$  mit  $q_1, \dots, q_s$  irred., so gilt  $s = t$  und nach Indexpermutation  $q_i \simeq p_i$  für  $i = 1, \dots, t$ .

Ein Integritätsbereich, der (i) und (ii) erfüllt heißt faktorieller Ring (oder EPZ-Ring: Ring mit eindeutiger Primfaktorzerlegung)

**Bemerkung.**

- (a) (i)  $\implies$  irred. Elemente in  $R$  sind Primelemente. Denn: Sei  $q$  irred. in  $R$ , schreibe Faktorisierung wie in (i) für  $q$ , d.h.  $q \simeq p_1 \cdot \dots \cdot p_t \xRightarrow{q \text{ irred.}} t = 1$  also  $q \simeq p_1$ . Primelement.  
 (b) In (b) ist  $R$  beliebiger Integritätsbereich (so zwingt man mit Induktion) Ist  $p$  ein Primelement in  $R$  und ein Teiler von  $a_1 \cdot \dots \cdot a_t$  (mit  $a_i \in R$ ), so  $\exists i \in \{1, \dots, t\}$  mit  $p | a_i$ .  
 (c) Für  $R$  wie in 54 ist  $R$  faktoriell, so ist die Länge  $r$  einer Primfaktorzerlegung  $r \simeq p_1 \cdot \dots \cdot p_t$  ( $p_i$  prim) von  $r \in R \setminus \{0\}$  unabhängig von der Faktorisierung (vgl (ii)). Schreibe  $r(r) \in \mathbb{N}_0$  für diese Länge.

*Beweis.* (von Satz 54)

- (i)  $\implies$  (ii): Existenz der Faktorisierung in (ii) ist klar nach (i), da Primelemente irreduzibel sind.

Eindeutigkeit: Gelte  $p_1 \cdot \dots \cdot p_t \stackrel{(*)}{\simeq} q_1 \cdot \dots \cdot q_t, s \in \mathbb{N}, p_i \text{ prim}, q_i \text{ irred.}$  Zeige mit Induktion über  $t$ :  $s = t$  und nach Indexpermutation  $q_i \simeq p_i$

- $t = 1$ :  $p_1 \simeq q_1 \cdot \dots \cdot q_s \implies s = 1$  ( $p_1$  prim, also irred.)

- $t-1 \rightarrow t$ : (\*) und Bemerkung (b)  $\implies \exists j \in \{1, \dots, s\}$  mit  $p_t \mid q_j$ , o.E.  $j = s$  (Umindizieren) und also  $p_t \simeq q_s$  ( $q_s$  irreduzibel). teile beide Seiten durch  $p_t$

$$p_1 \cdot \dots \cdot p_{t-1} \simeq q_1 \cdot \dots \cdot q_{s-1} \underbrace{q_s}_{\in R^\times} \simeq q_1 \cdot \dots \cdot q_{s-1}$$

Nun: wende Induktionsvoraussetzung an.  $\implies s-1 = t-1$  (also  $s = t$ )  
und nach Indexpermutation:  $q_i \simeq p_i$  für  $i = \{1, \dots, t-1\}$

(ii)  $\implies$  (i): Zeige irred. Elemente in  $R$  sind Primelemente. Sei also  $q \in R$  irreduzibel. Seien weiter  $a, b \in R$ , sodass  $q \mid ab$ .

Zu zeigen:  $q \mid a$  oder  $q \mid b$ : o.E.  $a, b \neq 0$  (sonst  $q \mid a \vee q \mid b$ ), o.E.  $a, b \notin R^\times$ , ist z.B.  $a \in R^\times$ , so folgt aus  $q \mid ab$  direkt  $q \mid b$ . Sei  $c \in R$  mit  $qc = ab$ . Schreibe  $c, a, b$  einer Faktorisierung wie in (ii) geg.

$$a \simeq p_1 \cdot \dots \cdot p_t, \quad b \simeq q_1 \cdot \dots \cdot q_s, \quad c \simeq r_1 \cdot \dots \cdot r_u$$

( $p_i, q_j, r_k$  irred.  $t, s \in \mathbb{N}, u \in \mathbb{N}_0$ )

$$qr_1 \cdot \dots \cdot r_u \simeq p_1 \cdot \dots \cdot p_t \cdot q_1 \cdot \dots \cdot q_s$$

Wende Eindeutigkeitsaussage von (ii), um zu folgen:

$q \simeq p_i, i \in \{1, \dots, t\}$  oder  $q \simeq q_j, j \in \{1, \dots, s\} \implies q \mid a$  oder  $q \mid b$ .  $\square$

**Korollar 3.55** (Übung). Sei  $R$  ein faktorieller Ring und sei  $\mathbb{P}$  ein Repräsentantensystem der Primelemente von  $R$  modulo Assoziiertheit, dann gelten:

(a)  $\forall p \in \mathbb{P}$  ist die Abbildung  $v_p : R \setminus \{0\} \rightarrow \mathbb{N}_0, r \mapsto \max\{n \in \mathbb{N}_0 : p^n \mid r\}$  wohldefiniert (genauer  $v_p(r) \leq t(r)$ ) und  $v_p$  ist ein Monoidhomomorphismus (für  $(R, 1, \cdot)$ )

(b)  $\forall r \in R \setminus \{0\}$  gilt  $\#\{p \in \mathbb{P} : p \mid r\} \leq t(r) < \infty$

(c)  $\forall r \in R \setminus \{0\} \exists! u \in R^\times$  :

$$r = u \prod_{p \in \mathbb{P}} p^{v_p(r)} = u \prod_{p \in P, v_p > 0} p^{v_p(r)}$$

(Primfaktorzerlegung von  $r$ )

(d) Für  $r, s \in R \setminus \{0\}$  gilt:

$$r \mid s \iff \bigvee_{p \in \mathbb{P}} r_p(r) \leq v_p(s)$$

(e) Für  $r, s \in R \setminus \{0\}$  gelten:

$$\text{ggT}(r, s) \simeq \prod_{p \in \mathbb{P}} p^{\min(v_p(r), v_p(s))}, \quad \text{kgV}(r, s) \simeq \prod_{p \in \mathbb{P}} p^{\max(v_p(r), v_p(s))}$$

(ggT und kgV existieren also in faktoriellen Ringen)

- (f) Sei  $K = \text{Quot}(R)$ , dann  $\exists!$  Fortsetzung  $v_p : K^\times \rightarrow \mathbb{Z}$  (ein Gruppenhomomorphismus, der den Monoidhomomorphismus  $v_p : R \setminus \{0\} \rightarrow \mathbb{N}_0$  fortsetzt) und  $\forall r \in K^\times \exists! u \in R^\times$  :

$$r = u \prod_{p \in \mathbb{P}} p^{v_p(r)}$$

(dabei  $\#\{p : v_p(r) \neq 0\}$  endlich.)

**Übung 3.56** (vgl. LA2). Für einen (beliebigen kommutativen) Ring  $R$  sind äquivalent:

- (a) Jede aufsteigende Kette von Idealen

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots \subseteq R$$

( $\mathbb{N}_0$  indiziert) wird stationär, d.h.  $\exists n_0 : \forall n \in \mathbb{N}_0 : I_n = I_{n_0}$

- (b) Jede nichtleere Teilmenge  $\mathcal{M}$  von Idealen enthält ein bzgl. der Inklusion maximales Element.  
(c) Jedes Ideal  $I \subseteq R$  ist endlich erzeugt, d.h.  $\exists n \in \mathbb{N} \exists a_1, \dots, a_n \in R$  mit  $I = (a_1, \dots, a_n)$

**Definition** (Noetherscher Ring). Gelten (a)-(c) für  $R$ , so heißt  $R$  **noethersch**

**Bemerkung.**  $R$  noethersch  $\xRightarrow{\text{ohne Zorn's Lemma}} \forall$  echte Ideal  $I \subsetneq R \exists$  maximales Ideal mit  $I \subseteq \mathcal{M}$  denn ein solches findet sich in  $\mathcal{M} = \{J \subsetneq R \mid I \subseteq J\}$

**Korollar 3.57.** Ist  $R$  ein HI-Ring, so gelten:

- (a)  $R$  ist noethersch.  
(b)  $\forall r \in R \setminus (R^\times \cup \{0\}) \exists t \in \mathbb{N} \exists$  Primelemente  $p_1, \dots, p_t \in R$ , sodass  $r \simeq p_1 \cdot \dots \cdot p_t$   
(c)  $R$  ist faktoriell.

*Beweis.* (a) folgt aus 56, da jedes Ideal von  $R$  ein Hauptideal ist.

(b) folgt aus (b).

- (c) Bei HI-Ringen, wissen schon Primelemente sind irred. und umgekehrt. (Prop. 50). Zu zeigen: Sei  $r \in R \setminus (R^\times \cup \{0\})$ , dann existiert eine Faktorisierung wie in (b). Definiere:

$$\mathcal{M}_a := \{(b) \subseteq R \mid \exists t \in \mathbb{N} \exists \underbrace{q_1, \dots, q_t}_{\text{irred.}} \in R : bq_1 \cdot \dots \cdot q_t \simeq a\}$$

$\mathcal{M}_a \neq \emptyset$ : denn  $(a) \in \mathcal{M}_a$  für  $t = 0$ . Sei nun  $(b) \in \mathcal{M}_a$  ein maximales Element (bzgl.  $\subseteq$ ). Behauptung:  $(b) = R$  (Dann  $b \simeq 1 \implies q_1 \cdot \dots \cdot q_t \simeq a$  für Faktorisierung in Definition von  $\mathcal{M}_a$  zu  $b$ ). Dazu: Nehme an:  $(b) \subsetneq R$ , dann ist wegen  $R$  noethersch  $\exists$  maximales Ideal  $M \subsetneq R$  mit  $(b) \subseteq M$ , da  $R$  HI-Ring ist  $M = (p)$  für  $p$  ein Primelement (Proposition 50) und aus  $(b) \subseteq (p)$  folgt  $p \mid b$  und  $(\frac{b}{p}) \supsetneq (b)$  ( $p$  keine Einheit) und  $(\frac{b}{p}) \in \mathcal{M}_a$ , da  $\frac{b}{p} \cdot p \cdot q_1 \cdot \dots \cdot q_t \simeq a$ . Widerspruch zur Maximalität von  $(b)$ .  $\square$



**Bemerkung.** Nächstes Ziel  $R$  faktoriell  $\implies R[X]$  faktoriell.

**Proposition 3.58** (Übung).

(a) Für einen kommutativen Ring  $R$  sind äquivalent:

- (i)  $R$  ist ein Integritätsbereich.
- (ii)  $R[X]$  ist ein Integritätsbereich
- (iii)  $\forall f, g \in R[X]$  gilt:  $\text{Grad}(fg) = \text{Grad } f + \text{Grad } g$

(b) Ist  $R$  ein Integritätsbereich, so gilt  $(R[X])^\times = R^\times$

*Beweis.* (a) Zeige (i)  $\implies$  (iii)  $\implies$  (ii)  $\implies$  (i)

(b)  $u \in R[X]^\times \implies \exists r : vu = 1$ , dann Grad Identität anwenden...  $\square$

**Beispiel.**  $\mathbb{Z}[X]^\times = \mathbb{Z}^\times = \{\pm 1\}$ ,  $K[X_1, X_2]^\times = K^\times$ .

**Definition 3.59.** Sei bis auf Widerruf  $R$  ein faktorieller Ring mit Quotientenkörper  $K = \text{Quot}(R) \supseteq R$ ,  $f = \sum_{i=0}^n a_i X^i \in K[X] \setminus \{0\}$  heißt primitiv wenn:

(a)  $f \in R[X]$  (alle  $a_i \in R$ )

(b)  $\text{ggT}(a_0, \dots, a_n) \simeq 1$

**Lemma 3.60.** Sei  $f = \sum_{i=0}^n a_i X^i \in K[X] \setminus \{0\}$ , dann:

(a)  $\exists c \in K^\times \exists g \in K[X] \setminus \{0\}$  primitiv, so dass  $f = cg$

(b) Gelte  $cg = c'g'$  mit  $c, c' \in R^\times, g, g' \in K[X] \setminus \{0\}$  primitive Polynome, so folgt  $\frac{c}{c'} \in R^\times$ , d.h.  $c$  in (a) ist eindeutig bis auf Faktor in  $R^\times$

*Proof.* Beweis

(a) Schreibe  $a_i = \frac{b_i}{d_i}$  mit  $b_i \in R, d_i \in R \setminus \{0\}$  als gekürzten Bruch (d.h.  $\text{ggT}(b_i, d_i) \simeq 1$  geht  $R$  faktoriell.)

Sei  $d = \text{kgV}(d_0, \dots, d_n)$  (Hauptnenner),  $b = \text{ggT}(b_0, \dots, b_n)$ . Es folgt  $g := f \cdot \frac{a}{b} = \sum_{i=0}^n \left( \frac{b_i}{b} \cdot \frac{d}{d_i} \right) X^i \in R[X] \setminus \{0\}$ .

Behauptung:  $g$  ist primitiv.  $\left( \implies c = \frac{b}{d} = \frac{\text{ggT}(b_0, \dots, b_n)}{\text{kgV}(d_0, \dots, d_n)} \right)$ .

Annahme:  $g$  ist nicht primitiv. Dann  $\exists$  Primelement  $p \in R$ , sodass  $p \mid \frac{b_i}{b} \cdot \frac{d}{d_i}, \forall i$ . Nach der Wahl von  $b$  gilt  $\frac{b_0}{b}, \dots, \frac{b_n}{b}$  sind insgesamt teilerfremd  $\implies \exists i : p \nmid \frac{b_i}{b} \implies \exists i : p \mid \frac{d}{d_i} \implies p \mid d$ . Sei  $k = v_p(d)$ , d.h.  $p^k$  teilt  $d, p^{k+1} \nmid d \implies_{d=\text{kgV}(\dots)} \exists i : p^k \mid d_i, p^{k+1} \nmid d_j, j \in \{0, \dots, n\}$ , sei dieses  $i_0$ .

Insbesondere ist  $p \mid d_{i_0}$ .

Beachte:  $\frac{b_{i_0}}{d_{i_0}}$  gekürzter Bruch  $\implies p \nmid b_{i_0}$ , aber nach Voraussetzung ( $g$  nicht primitiv)  $p$  teilt  $\frac{b_{i_0}}{b} \cdot \frac{d}{d_{i_0}}$ . Widerspruch, da  $p$  kein Teiler von  $b$  oder  $d_{i_0}$  ist.

(b) Haben  $c \cdot g = c' \cdot g'$  für  $c, c' \in K^\times, g, g'$  primitiv. Schreibe  $u = \frac{c'}{c}$  als gekürzter Bruch  $u = \frac{d'}{d} \implies d \cdot h = d' \cdot g' = d \cdot \sum b_i X^i = d' \cdot \sum b'_i X^i$ .  $g, g'$  primitiv heißt  $\implies d = \text{ggT}(b_0 d, \dots, b_n d) = \text{ggT}(b'_0 d', \dots, b'_n d') = d' \implies \frac{d'}{d} \in R^\times$  und  $\frac{c'}{c} = \frac{d'}{d}$ .

$\square$

# Kapitel 4

## Körper

### 4.1 Grundlagen

**Definition** (Körper).  $K = (K, 0_K, 1_K, +, \cdot)$  ist Körper  $\iff K$  ist ein kommutativer Ring und  $(K \setminus \{0\}, 1_K, \cdot)$  ist eine Gruppe ( $0_K \neq 1_K$ ).

**Bemerkung.** Im weiteren seien  $K, K'$  stets Körper.

**Definition 4.1** (Unterkörper/Oberkörper). (i)  $L \subseteq K$  heißt Unterkörper :  $\iff L$  ist ein Unterring und  $L$  ist ein Körper.

(ii)  $E \supseteq K$  heißt Oberkörper :  $\iff E$  ist ein Körper und  $K \subseteq E$  ist ein Unterkörper.

**Bemerkung 4.2** (Übung). Sind  $(K_i)_{i \in I}$  Unterkörper von  $K$ , so ist  $\bigcap_{i \in I} K_i$  ein Unterkörper von  $K$ .

**Definition 4.3** (Körperhomomorphismus). Eine Abbildung  $\varphi : K \rightarrow K'$  heißt Körperhomomorphismus :  $\iff \varphi$  ist ein Ringhomomorphismus (der Ringe  $K \rightarrow K'$ )

**Bemerkung 4.4.** Sei  $R$  ein Ring mit  $0_R \neq 1_R$  und  $\varphi : K \rightarrow R$  ein Ringhomomorphismus, dann:

(a)  $\text{Kern}(\varphi) = \{0\}$  ( $\implies \varphi$  ist injektiv)

(b)  $R$  ist ein  $K$ -Vektorraum (vermöge  $\varphi$ ) durch

$$\cdot : K \times R \rightarrow R, (\alpha, r) \mapsto \varphi(\alpha) \cdot r, \quad + : R \times R \rightarrow R := +_R$$

*Beweis.* (a) Nur zu zeigen:  $\text{Kern}(\varphi) \subsetneq K$ . Dies ist klar wegen  $\varphi(1_K) = 1_R \neq 0_R$ . (einzige Ideale von  $K$  sind  $\{0\}, K$ )

(b) Übung. □

**Proposition 4.5 (Primkörper).** Jeder Körper  $K$  enthält einen kleinsten Unterkörper  $K_0 \subseteq K$ , der sogenannte **Primkörper** von  $K$ : es gilt:

$$K_0 \cong \begin{cases} \mathbb{Q}, & \text{char}(K) = 0, \\ \mathbb{F}_p, & \text{char}(K) = p > 0. \end{cases}$$

*Beweis.*

- Existenz: Nach Bemerkung 2 ist  $K_0 := \bigcap_{L \subseteq K \text{ Unterkörper}} L$  ein Körper, sicher auch der kleinste.
- Isomorphietyp: betrachte  $\varphi : \mathbb{Z} \rightarrow K, n \mapsto n \cdot 1_K$ 
  - Fall 1:  $\text{Kern}(\varphi) \supsetneq \{0\}$ : Hatten schon gesehen  $\text{Kern}(\varphi) = p\mathbb{Z}$  für  $p = \text{char}(K)$ . Homomorphiesatz gibt Isomorphismus

$$\underbrace{\mathbb{Z}/p\mathbb{Z}}_{\text{Körper}} \xrightarrow{\cong} \text{Bild}(\varphi) \underbrace{\subseteq}_{\text{Unterring}} K \implies \text{Unterkörper}.$$

$\text{Bild}(\varphi) \subseteq K_0$ , denn  $1_K \in K_0$  und also  $\mathbb{Z} \cdot 1_K \subseteq K_0 \implies \text{Bild}(\varphi) = K_0$  ist der kleinste  $\implies K_0 \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ .

- Fall 2:  $\text{Kern}(\varphi) = \{0\}$ , d.h.  $\varphi$  ist injektiv, und es gilt  $\text{char}(K) = 0$ . Beachte:

$$\underbrace{\varphi(\mathbb{Z} \setminus \{0\})}_S \underbrace{\subseteq}_{\varphi \text{ inj. Hom.}} K_0 \setminus \{0\} \subseteq K \setminus \{0\}$$

universelle Eigenschaft der Lokalisierung ( $S$  multiplikativ abgeschlossen,  $\varphi(S) \subseteq K^\times$ )  $\implies \exists!$  Ringhomomorphismus  $\hat{\varphi} : S^{-1}\mathbb{Z} = \mathbb{Q} \rightarrow K_0$ , der  $\varphi$  fortsetzt; und  $\hat{\varphi}(\frac{a}{b}) = \varphi(a)\varphi(b)^{-1}, z, b \in \mathbb{Z}, b \neq 0$ . Erhalten:

$\hat{\varphi}$  gibt Isomorphismus  $\mathbb{Q} \xrightarrow{\cong} \hat{\varphi}(\mathbb{Q}) \underbrace{\subseteq}_{\text{Unterkörper}} K_0, K_0 \text{ minimal} \implies \hat{\varphi}$  ist Isomorphismus  $\mathbb{Q} \cong K_0$ .  $\square$

**Definition 4.6.** Sei  $E \supseteq K$  ein Oberkörper. Der **Grad** von  $E$  über  $K$  ist die Vektorraumdimension.

$$[E : K] := \dim_K E \in \mathbb{N} \cup \{\infty\}$$

**Satz 4.7.** Sei  $E \supseteq K$  ein Oberkörper und  $V$  ein  $E$ -Vektorraum, dann gilt:  $\dim_K V = [E : K] \dim_E V$ .

*Beweis.* Sei  $B = (b_i)_{i \in I}$  eine Basis von  $E$  als  $K$ -Vektorraum,  $C = (c_j)_{j \in J}$  eine Basis von  $V$  als  $E$ -Vektorraum.

- Behauptung:  $D = (b_i c_j)_{(i,j) \in I \times J}$  ist eine Basis von  $V$  als  $K$ -Vektorraum ( $\implies \dim_K V = \#(I \times J) = \#I \#J = [E : K] \dim_E V$ ).
- Dazu:  $D$  ist Erzeugendensystem (von  $V$  als  $K$ -Vektorraum) Sei  $v \in V$ , schreibe  $v = \sum_{j \in J} \lambda_j c_j, (\lambda_j \in E)$ . Für jedes  $j$  schreibe

$$\lambda_j = \sum_{i \in I} \mu_{ij} b_i \implies v = \sum_{j \in J} \left( \sum_{i \in I} \mu_{ij} b_i \right) c_j = \sum_{(i,j) \in I \times J} \mu_{ij} (b_i c_j).$$

- $D$  ist linear unabhängig (über  $K$ ): Seien  $\beta_{ij} \in K$  für alle  $(i,j) \in I \times J$  (nur endlich viele  $\neq 0$ ), sodass

$$0 = \sum_{(i,j) \in I \times J} \beta_{ij} b_i c_j = \sum_{j \in J} \underbrace{\left( \sum_{i \in I} \beta_{ij} b_i \right)}_{\in E} \underbrace{c_j}_{\text{bilden } E\text{-Basis von } V}$$

$$\begin{aligned} \implies \forall j \in J : \sum_{i \in I} \underbrace{\beta_{ij}}_{\in K} \cdot \underbrace{b_i}_{\text{bilden } K\text{-Basis von } E} &= 0. \\ \implies \forall j \in J \forall i \in I : \beta_{ij} &= 0. \quad \square \end{aligned}$$

**Korollar 4.8** (Gradformel für Körpertürme). *Seien  $L \supseteq E$  und  $E \supseteq K$  Oberkörper. Dann ist  $L \supseteq K$  ein Oberkörper und*

$$[L : K] = [L : E] \cdot [E : K]$$

*Beweis.* (der Formel)

$$[L : K] = \dim_K L \stackrel{\text{Satz 7}}{=} [E : K] \cdot \dim_E L = [E : K] \cdot [L : E].$$

□

**Proposition 4.9** (Übung). *Sei  $K$  ein Körper mit  $\#K < \infty$  und seien  $p$  die Charakteristik,  $K_0$  der Primkörper von  $K$ , dann gilt*

$$\#K = p^n, \text{ für } n = \dim_{K_0} K$$

**Bemerkung.** Zu jeder Primpotenz  $p^n \exists K$  Körper mit  $\#K = p^n$

**Definition 4.10.** Sei  $E \supseteq K$  ein Oberkörper und  $S \subseteq E$  eine Teilmenge, dann:

(a)  $K(S) :=$  der kleinste Oberkörper von  $K$ , der  $S$  enthält, d.h.

$$K(S) := \bigcap \{L \subseteq E \text{ Unterkörper} \mid K \cup S \subseteq L\}$$

(b)  $K[S] :=$  der kleinste Oberring von  $K$ , der  $S$  enthält, d.h. (Übung)

$$K[S] := \bigcap \{L \subseteq E \text{ Unterring} \mid K \cup S \subseteq L\}$$

Falls  $S = \{\alpha_1, \dots, \alpha_n\}$ , schreibe auch  $K(\alpha_1, \dots, \alpha_n)$  für  $K(\{\alpha_1, \dots, \alpha_n\})$  und  $K[\alpha_1, \dots, \alpha_n]$  für  $K[\{\alpha_1, \dots, \alpha_n\}]$ .

**Bemerkung.**

(a)  $K[\alpha_1, \dots, \alpha_n] = \{f(\alpha_1, \dots, \alpha_n) \mid f \in K[X_1, \dots, X_n]\}$

(b)  $K(S) = \text{Quot}(K[S]) = \{\frac{f}{g} \mid f, g \in K[S], g \neq 0\}$

(c)  $K(S_1)(S_2) = K(S_1 \cup S_2)$  und  $K[S_1][S_2] = K[S_1 \cup S_2]$

**Beispiel.**

(a)  $E = \text{Quot}(K[X]) = K(X)$  rationaler Funktionenkörper über  $K$  in Variablen  $X$ . Hier gilt  $K[X] \subsetneq K(X)$  und  $[K(X) : K] = \infty$  ( $\dim_K K[X] = \infty$ )

(b)  $\sqrt{3} \subseteq \mathbb{R} \subseteq \mathbb{C}$ , dann

$$\mathbb{Q}[\sqrt{3}] = \{\alpha + \beta\sqrt{3} \mid \alpha, \beta \in \mathbb{Q}\} \subseteq \mathbb{R}$$

und

$$\mathbb{Q}(\sqrt{3}) \stackrel{\text{Übung}}{=} \mathbb{Q}[\sqrt{3}], ([\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2)$$

## 4.2 Algebraische und transzendente Elemente

**Definition 4.11.** Sei  $E \supseteq K$  ein Oberkörper und seien  $\alpha, \alpha_1, \dots, \alpha_n \in E$ . Dann

- (i)  $\alpha$  heißt algebraisch über  $K : \iff [K(\alpha) : K] < \infty$
- (ii)  $\alpha$  heißt transzendent über  $K : \iff [K(\alpha) : K] = \infty$

**Beispiele** (ohne Beweis).

- (a)  $X \in K(X)$  ist transzendent über  $K$ .
- (b)  $\sqrt{3} \in \mathbb{R}$  ist algebraisch über  $\mathbb{Q}$ .
- (c)  $e = \sum_{n \geq 0} \frac{1}{n!} \in \mathbb{R}$  ist transzendent über  $\mathbb{Q}$
- (d)  $\pi \in \mathbb{R}$  ist transzendent über  $\mathbb{Q}$

**Wiederholung 4.12.** (Propositionen 3.49 und 3.50)

- (a)  $K[X]$  ist Hauptidealring.
- (b)  $f \in K[X]$  irreduzibel  $\iff (f) \subseteq K[X]$  ist maximales Ideal.
- (c) Ist  $0 \neq P \subseteq K[X]$  Primideal, so  $\exists f \in K[X]$  irred.  $P = (f)$ .
- (d) (Übung, s. LA) für  $f \in K[X] \setminus K$  von Grad  $n > 0$ , dann hat  $K[X]_{(f)}$  als  $K$ -Vektorraum die Basis  $\{1, X, \dots, X^{n-1}\}$ .

**Definition.** Die Auswertungsabbildung an  $\alpha \in E$  ist der Ringhomomorphismus

$$\text{ev}_\alpha : K[X] \rightarrow E, f = \sum a_i X^i \mapsto f(\alpha) = \sum a_i \alpha^i$$

**Satz 4.13.** Für  $\alpha \in E$  sind äquivalent:

- (a)  $\alpha$  ist algebraisch über  $K$ .
- (b)  $\exists n \in \mathbb{N} : 1, \alpha, \dots, \alpha^n$  sind linear unabhängig über  $K$ .
- (c)  $\exists g \in K[X] \setminus \{0\}$  mit  $g(\alpha) = 0$ .
- (d)  $\text{Kern}(\text{ev}_\alpha) \subseteq K[X]$  ist maximales Ideal.
- (e)  $K(\alpha) = K[\alpha]$ .

*Beweis.*

- (a)  $\implies$  (b): Sei  $n := [K(\alpha) : K] = \dim_K K(\alpha) < \infty \implies 1, \alpha, \dots, \alpha^n$  sind l.u. über  $K$ .
- (b)  $\implies$  (c): Voraussetzung in (b)  $\implies \exists (c_0, \dots, c_n) \in K^{n+1} \setminus \{0\}$  mit  $\sum_{0 \leq i \leq n} c_i \alpha^i = 0$ , dann ist

$$\implies g(X) = \sum_{0 \leq i \leq n} c_i X^i \in K[X] \setminus \{0\}. \text{ und } g(\alpha) = 0$$

(c)  $\implies$  (d): Homomorphiesatz gibt und den Isomorphismus

$$K[X]_{/\text{Kern}(\text{ev}_\alpha)} \xrightarrow{\cong} \text{Bild}(\text{ev}_\alpha) \underset{\text{Unterring}}{\subseteq} E$$

$\text{Bild}(\text{ev}_\alpha)$  ist Integritätsbereich  $\implies \text{Kern}(\text{ev}_\alpha)$  ist Primideal. Da  $0 \neq g \in \text{Kern}(\text{ev}_\alpha)$  ( $g$  aus (c)) folgt:  $\text{Kern}(\text{ev}_\alpha)$  ist Primideal  $\neq 0$  also ein maximales Ideal.

(d)  $\implies$  (a): Voraussetzung:  $\mathfrak{m}_\alpha := \text{Kern}(\text{ev}_\alpha) \subseteq K[X]$  ist maximales Ideal.

$$\xrightarrow{\text{Homomorphiesatz}} \underbrace{K[X]_{/\mathfrak{m}_\alpha}}_{\text{Körper, da } \mathfrak{m}_\alpha \text{ max.}} \xrightarrow{\cong} \text{Bild}(\text{ev}_\alpha) \subseteq E$$

$\implies \text{Bild}(\text{ev}_\alpha)$  ist ein Körper. Aber:  $\text{Bild}(\text{ev}_\alpha) = K[\alpha]$ , also  $K[\alpha] = K(\alpha)$  (\*), und sei  $f \in K[X]$  irreduzibler Erzeuger von  $\mathfrak{m}_\alpha$ , dann:

$$\dim_K K[X]_{/(f)} = \text{Grad } f < \infty \implies \dim_K K(\alpha) = \text{Grad } f < \infty.$$

(d)  $\implies$  (e): gezeigt wegen (\*).

(e)  $\implies$  (a): Zu zeigen:  $K[\alpha] = K(\alpha) \implies [K(\alpha) : K] < \infty$ , wir zeigen (b). o.E.  $\alpha \neq 0$ , wesentliche Beobachtung:  $\alpha^{-1} \in K[\alpha]$ . d.h.  $\exists c_0, \dots, c_n \in K$  mit  $\alpha^{-1} = c_0 + c_1\alpha + \dots + c_n\alpha^n$

$$\implies 0 = -1 + c_0\alpha + c_1\alpha^2 + \dots + c_n\alpha^{n+1}$$

d.h.  $1, \alpha, \dots, \alpha^{n+1}$  sind linear abhängig über  $K$ . □

**Definition 4.14.** Sei  $\alpha \in E$  algebraisch über  $K$ . Das Minimalpolynom  $\mu_\alpha$  (oder  $\mu_{\alpha, K}$ ) von  $\alpha$  über  $K$  ist das normierte Polynom in  $K[X] \setminus \{0\}$  kleinsten Grades mit  $\mu_\alpha(\alpha) = 0$ .

**Proposition 4.15.** Sei  $\alpha \in E$  algebraisch über  $K$ , dann:

(a)  $(\mu_\alpha) = K[X] \cdot \mu_\alpha = \text{Kern}(\text{ev}_\alpha)$ .

(b)  $\mu_\alpha$  ist irred. und  $K[X]_{/(\mu_\alpha)}$  ist ein Körper.

(c)  $[K(\alpha) : K] = \text{Grad } \mu_\alpha$

*Beweis.*

- (a) • “ $\subseteq$ ”: Klar, da  $\mu_\alpha = 0$  also  $\text{ev}_\alpha(\mu_\alpha) = 0$   
 • “ $\supseteq$ ”:  $K[X]$  ist Hauptidealring  $\implies \exists g \in K[X] : (g) = \text{Kern}(\text{ev}_\alpha)$  mit  $g \neq 0, g \mid \mu_\alpha$  und  $\text{Kern}(\text{ev}_\alpha)$  ist ein maximales Ideal ( $\neq 0$ ) folgt aus 13.  $\mu_\alpha$  hat den kleinsten Grad unter allen solchen  $f \neq 0$  mit  $f(\alpha) = 0 \implies g \simeq \mu_\alpha \implies (g) = (\mu_\alpha)$ .

(b)  $\text{Kern}(\text{ev}_\alpha)$  maximal  $\neq 0 \implies$  Erzeuger  $\mu_\alpha$  von  $\text{Kern}(\text{ev}_\alpha)$  ist irred. und  $K[X]_{/(\mu_\alpha)}$  ist ein Körper, da  $(\mu_\alpha)$  maximal.

(c) Im Beweis von Satz 13:  $K(\alpha) \cong K[X]_{/(\mu_\alpha)}$

$$\implies [K(\alpha) : K] = \dim_K K[X]_{/(\mu_\alpha)} \underset{\text{Whg. 12}}{=} \text{Grad } \mu_\alpha. \quad \square$$

**Korollar 4.16.** Sei  $f \in K[X]$  irred. normiert und  $\alpha \in E$  eine Nullstelle von  $f$ , dann ist  $\alpha$  algebraisch über  $K$  und  $\mu_\alpha = f$  und  $[K(\alpha) : K] = \text{Grad } f$

**Beispiel.**  $X^2 - 3 \in \mathbb{Q}[X]$  ist irreduzibel (Eisenstein mit  $p = 3$ )

$$\implies \mu_{\sqrt{3}, \mathbb{Q}} = X^2 - 3$$

analog:  $\alpha = \sqrt[3]{2}$  algebraisch über  $\mathbb{Q}$  mit  $\mu_\alpha = X^3 - 2$  und

$$\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$$

**Korollar 4.17.** Für  $\alpha \in E$  sind äquivalent:

- (a)  $\alpha$  ist transzendent über  $K$
- (b)  $K[\alpha] \subsetneq K(\alpha)$
- (c)  $\text{ev}_\alpha : K[X] \rightarrow K[\alpha]$  ist ein Isomorphismus.

*Beweis.*

$$\neg(a) \iff \neg(b), \text{ folgt aus Satz 13 } (a) \iff (e).$$

Beachte weiter: (c)  $\iff \text{Kern}(\text{ev}_\alpha) = \{0\}$ , also:  $\neg(c) \iff \exists g \in K[X] \setminus \{0\} : g(\alpha) = a \iff \alpha \text{ ist algebraisch} \iff \neg(a)$ .  $\square$

**Bemerkung.** Ist  $\alpha \in E$  transzendent über  $K$ , so setzt sich  $\text{ev}_\alpha : K[X] \xrightarrow{\cong} K[\alpha]$  fort zu einem Körperisomorphismus  $K(X) = \text{Quot}(K[X]) \rightarrow K(\alpha)$ .

**Definition 4.18** (Algebraischer Oberkörper). Ein Oberkörper  $E \supseteq K$  heißt algebraisch über  $K$  :  $\iff$  jedes  $\alpha \in E$  ist algebraisch über  $K$ .

**Lemma 4.19.** Seien  $F \supseteq E \supseteq K$  Oberkörper, dann:

- (a)  $[E : K] < \infty \implies E$  ist algebraisch über  $K$ .
- (b)  $\alpha_1, \dots, \alpha_n \in E$  mit  $\alpha_i$  algebraisch über  $K, \forall i \implies K(\alpha_1, \dots, \alpha_n) \supseteq K$  algebraisch.
- (c)  $F \supseteq K$  ist algebraisch  $\iff F \supseteq E$  und  $E \supseteq K$  sind algebraisch.
- (d) Ist  $K = K_0 \subseteq K_1 \subseteq \dots$  eine Kette (indiziert über  $\mathbb{N}$ ) von Oberkörpern, so ist  $K_\infty = \bigcup_n K_n$  ein Oberkörper von  $K$ , und sind alle  $K_{i+1} \supseteq K_i$  algebraisch, so ist  $K_\infty \supseteq K$  algebraisch.
- (e) Ist  $S \subseteq E$  eine beliebige Teilmenge, so dass alle  $\alpha \in S$  algebraisch über  $K$  sind, so gilt  $K(S) = K[S]$  und  $K(S)$  ist algebraisch über  $K$ .

*Beweis.* (a) Für  $\alpha \in E$  gilt:  $K \subseteq K(\alpha) \subseteq E$  und wegen Gradformel folgt  $[K(\alpha) : K] \leq [E : K] < \infty \implies \alpha$  algebraisch über  $K$ .

- (b) Definiere  $K_i = K(\alpha_1, \dots, \alpha_i), i \in \{1, \dots, n\}$ , wir wissen  $\alpha_i$  algebraisch über  $K$ , d.h.  $\exists g \in K[X] \setminus \{0\} = g(\alpha_i) = 0 \implies g \in K_{i-1}[X] \setminus \{0\}$  ( $K_{i-1} \supseteq K$ ),  $\exists g \in K_{i-1} \setminus \{0\} : g(\alpha_i) = 0 \implies \alpha_i$  algebraisch über  $K_{i-1}$

$$\implies [K_i : K_{i-1}] = [K_{i-1}(\alpha_i) : K_{i-1}] < \infty \xrightarrow{\text{Ind.} + \text{Gradformel}} [K_n : K] < \infty$$

$$\xrightarrow{(a)} K_n = K(\alpha_1, \dots, \alpha_n) \supseteq K \text{ algebraisch.}$$

- (c) • “ $\implies$ ”: Sei  $F \supseteq K$  algebraisch, sei  $\alpha \in E \implies \alpha \in F \implies \alpha$  algebraisch über  $K$ . Und sei  $\alpha \in F$ . Dann argumentiere wie in (b) um  $\alpha$  algebraisch über  $E$  zu folgen  $\implies F \supseteq E$  algebraisch.
- “ $\impliedby$ ”: (Problem:  $[E : K]$  könnte unendlich sein.) Es gelte:  $F \supseteq E$  und  $E \supseteq K$  sind algebraisch.  $\alpha \in F$  (zz:  $[K(\alpha) : K] < \infty$ ). Wir wissen  $\alpha$  algebraisch über  $E \implies$  haben  $\mu_{\alpha,E} \in E[X] \setminus E$  schreibe  $\mu_{\alpha,E} = a_0 + a_1X + \dots + a_{n-1}X^{n-1} + X^n$  mit  $a_i \in E$  algebraisch über  $K \implies E' = K[a_0, \dots, a_{n-1}]$  hat endlichen Grad über  $K$  (nach (b)) und  $\alpha$  ist algebraisch über  $E'$ , da  $\mu_{\alpha,E} \in E'[X] \implies [E'[\alpha] : E'] < \infty$ . Nach Definition von algebraisch und Gradformel  $[E'[\alpha] : K] < \infty \implies \alpha$  algebraisch über  $K$ .
- Gegeben eine Körperkette  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n \subseteq \dots$ ,  $K_\infty = \bigcup K_n$  ist Oberkörper von  $K$  (Übung). Gilt zusätzlich  $K_{i+1} \supseteq K_i$  algebraisch  $\forall i$ , so folgt mit Induktion und (c):  $K_i \supseteq K$  algebraisch  $\forall i$ . Sei  $\alpha \in K_\infty \implies \exists n : \alpha \in K_n \implies \alpha$  ist algebraisch über  $K$ .
- Übung.

□

**Korollar 4.20.** Sei  $E \supseteq K$  ein Oberkörper und

$$F := \{\alpha \in E \mid \alpha \text{ algebraisch über } K\}$$

Dann gilt:

- (a)  $F \subseteq E$  Unterkörper.  
 (b)  $F \supseteq K$  algebraisch.  
 (c)  $K[F] = F$ .

*Beweis.* 19(e)  $\implies K[F] \supseteq K$  ist algebraischer Oberkörper und  $K[F] \subseteq E \implies K[F] = F$ , d.h. (c) gilt. Und (a), (b) folgen. ((a),(b) gelten für  $K[F]$  nach 19(e)). □

**Beispiel 4.21** (Übung). Sei  $\alpha_n := \sqrt[n]{2} \in R$  für  $n \geq 0$ , dann:  $[\mathbb{Q}(\alpha_n) : \mathbb{Q}] = 2^n$ .  $\implies \mathbb{Q}_\infty = \bigcup_n \mathbb{Q}(\alpha_n)$  ist algebraisch über  $\mathbb{Q}$ , aber  $[\mathbb{Q}_\infty : \mathbb{Q}] = \infty$ .

**Beispiel.**  $\tilde{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ ist algebraisch über } \mathbb{Q}\} \implies [\tilde{\mathbb{Q}} : \mathbb{Q}] = \infty$  und  $\tilde{\mathbb{Q}} \supseteq \mathbb{Q}$  ist algebraisch.

**Leitfragen.** (a) Gegeben  $f \in K[X]$  irred. Finde Oberkörper  $E$  und  $\alpha \in E$  mit  $f(\alpha) = 0$ .

(b) Finde Oberkörper  $E \supseteq K$  in dem alle irred.  $f \in K[X]$  eine Nullstelle (alle Nullstellen) haben.

Sei  $f = \sum_{0 \leq i \leq n} a_i X^i \in K[X] \setminus K$ , sei  $E \supseteq K$  Oberkörper, hatten schon gesehen  $f(\alpha) = 0 \iff \text{ev}_\alpha(f) = 0 \iff \mu_{\alpha,K} \mid f$ .

**Proposition 4.22.**  $\#\{\alpha \in E \mid f(\alpha) = 0\} \leq \text{Grad } f$ .

*Beweis.* TODO

□

**Definition 4.23.** (a)  $f \in K[X] \setminus K$  zerfällt in Linearfaktoren über  $K : \iff$  jeder irred. normierte Faktor von  $f$  ist der Form  $X - \alpha$  für ein  $\alpha \in K$ .



- (b)  $K$  heißt algebraisch abgeschlossen  $\iff$  jedes  $f \in K[X] \setminus K$  zerfällt in Linearfaktoren über  $K$ .

**Bemerkung 4.24.**  $K$  ist algebraisch abgeschlossen  $\iff$  jedes  $f \in K[X] \setminus K$  hat eine Nullstelle  $\alpha \in K$ .

*Beweis.*

- “ $\implies$ ”: Klar
- “ $\impliedby$ ”: Sei  $f \in K[X] \setminus K$  irred. normiert, nach Voraussetzung hat  $f$  eine Nullstelle  $\alpha \in K \implies f = X - \alpha$  (alle irred. Polynome sind linear).  $\square$

**Beispiel.**

$\mathbb{C}$  ist algebraisch abgeschlossen.

TODO

**Definition 4.25.** Sei  $f \in K[X]$  irred. Ein Oberkörper  $E \supseteq K$  heißt Stammkörper zu  $f \iff \exists \alpha \in E$  mit  $f(\alpha) = 0$  und  $E = K(\alpha)$ .

**Satz 4.26.** Sei  $f \in K[X]$  irred. von Grad  $n$ , dann:

- $E := K[X]/(f)$  ist ein Körper (schreibe  $\bar{g}$  für die Klasse zu  $g \in K[X]$ ).
- $K \rightarrow E, \alpha \rightarrow \bar{\alpha}$  ist ein Ringhomomorphismus, also Körperhomomorphismus. (Betrachte  $K$  als Unterkörper von  $E$ , schreibe  $\alpha$  für  $\bar{\alpha}$ )
- Es gilt  $f(\bar{X}) = 0$ , d.h.  $f$  hat keine Nullstelle in  $E$ .
- Es gilt  $E = K[\bar{X}]$  und  $[E : K] = n$
- Ist  $F$  ein Oberkörper von  $K$  mit Nullstelle  $\beta \in F$  von  $f$ , so gilt  $n \mid [F : K]$ , falls  $[F : K] < \infty$ .

*Beweis.* TODO  $\square$

**Korollar 4.27.** Seien  $f_1, \dots, f_t \in K[X]$  irred. Dann  $\exists$  Oberkörper  $E \supseteq K$  mit  $\beta_1, \dots, \beta_t \in E$ , so dass  $f_i(\beta_i) = 0, \forall i \in \{1, \dots, t\}$  und  $E = K(\beta_1, \dots, \beta_t)$ .

**Bemerkung.** Es gilt nur  $[E : K] \leq \prod_{1 \leq i \leq t} \text{Grad } f_i$ .

**Beispiel.** Seien  $f_1, f_2 \in \mathbb{R}[X]$  irred. quadr. Polynome  $\implies E = \mathbb{C}$  und  $[E : \mathbb{R}] = 2 < 2 \cdot 2$ . z.B.  $f_1 = X^2 + 1$  und  $f_2 = X^2 + \pi$ .

**Satz 4.28.** Jeder Körper  $K$  hat einen (inj.) Körperhomomorphismus in einen algebraisch abgeschlossenen Körper  $\tilde{K}$ .

**Definition 4.29** (Algebraischer Abschluss). Ein Oberkörper  $E \supseteq K$  heißt algebraischer Abschluss, wenn

- $E$  ist algebraisch abgeschlossen.
- $E \supseteq K$  ist algebraisch.

**Bezeichnung.**  $\bar{K}$  sei immer ein algebraischer Abschluss von  $K$ .

**Bemerkung** (zu Satz 28).  $\tilde{K}$  ist ein algebraischer Abschluss.

*Beweis.* (von Satz 28) TODO. □

**Proposition 4.30.**

- (a)  $K$  ist algebraisch abgeschlossen  $\iff \forall$  algebraischer Oberkörper  $E \supseteq K$  gilt  $E = K$
- (b) Ist  $E \supseteq K$  algebraischer Oberkörper und  $\bar{E} \supseteq E$  ein algebraischer Abschluss. Dann ist  $\bar{E} \supseteq K$  ein algebraischer Abschluss.
- (c) Ist  $E \supseteq K$  algebraisch abgeschlossen, so ist  $F := \{\alpha \in E \mid \alpha \text{ algebraisch über } K\}$  ein algebraischer Abschluss von  $K$ .

*Beweis.*

- (a) • “ $\implies$ ”: Sei  $\alpha \in E$ , z.z.  $\alpha \in K$ . Betrachte  $\mu_{\alpha,K} \in K[X]$ ,  $K$  algebraisch abgeschlossen  $\implies$  irred. Polynome haben Grad  $\implies$  Grad  $\mu_{\alpha,K} = 1 \implies \mu_{\alpha,K} = X - \alpha \in K[X]$  also  $\alpha \in K$ .
- “ $\impliedby$ ”: Sei  $f \in K[X]$  irred. normiert. Sei  $E$  sein Stammkörper  $\implies \exists \alpha \in E$  mit  $f(\alpha) = 0 \xRightarrow{E \supseteq K \text{ alg.}} E = K$  und also  $\alpha \in K \implies f = X - \alpha$ .

(b) Folgt aus Proposition 19.

(c) Nach Korollar 20 ist  $F$  ein alg. Oberkörper von  $K$ . Noch z.z:  $f \in F[X]$  irred. normiert  $\implies f$  linear.  $f$  faktorisiert in  $E[X]$  also  $f = \prod_{1 \leq i \leq n} (X - \alpha_i)$  ( $n = \text{Grad } f, \alpha_i \in E$ ). Nun sind die  $\alpha_i$  algebraisch über  $F$ , also auch über  $K \implies \alpha_1, \dots, \alpha_n \in F \xRightarrow{f \text{ irr.}} n = 1$ . □

**Beispiel 4.31.**  $\bar{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ ist alg. über } \mathbb{Q}\}$  ist ein algebraischer Abschluss von  $\mathbb{Q}$ . Es gilt  $\bar{\mathbb{Q}} \subsetneq \mathbb{C}$ , denn  $\bar{\mathbb{Q}}$  ist abzählbar,  $\mathbb{C}$  aber nicht.

**Bemerkung.** Nächste Ziele:

- (a)  $\bar{K}$  ist eindeutig bis auf Isomorphie.
- (b) “Verstehe” Körperautomorphismen von  $\bar{K}$  über  $K$ .

**Bezeichnungen 4.32.** Sei  $\varphi_i : K \rightarrow K'$  ein Körperhomomorphismus.

(a) Schreibe  $\varphi_*$  für den induzierten Ringhomomorphismus

$$\varphi_* : K[X] \rightarrow K'[X], \sum a_i X^i \mapsto \sum \varphi(a_i) X^i$$

(b) Sei  $L \supseteq K$  ein Oberkörper, Nenne einen Körperhomomorphismus  $\psi : L \rightarrow K'$  eine Ausdehnung von  $\varphi$ , falls  $\psi|_K = \varphi$ , also wenn

$$\begin{array}{ccc} L & \xrightarrow{\psi} & K' \\ \uparrow \varphi & \nearrow \psi & \\ K & & \end{array}$$

**Lemma 4.33.** Sei  $L \supseteq K$  ein Stammkörper zu  $f \in K[X]$  irred. und sei  $\alpha \in L$  eine Nullstelle von  $f$ , sei  $\varphi : K \rightarrow E$  ein Körperhomomorphismus, dann gilt: Die Abbildung

$$\begin{array}{ccc} \left\{ \begin{array}{l} \psi : L \rightarrow E \text{ eine} \\ \text{Ausdehnung von } \varphi \end{array} \right\} & \longrightarrow & \left\{ \beta \in E \mid \begin{array}{l} \beta \text{ ist eine} \\ \text{Nst. von } \varphi_*(f) \end{array} \right\} \\ \psi & \longmapsto & \psi(\alpha) \end{array}$$

ist wohl-definiert und bijektiv, insbesondere:

$$\# \left\{ \begin{array}{l} \psi : L \rightarrow E \text{ eine} \\ \text{Ausdehnung von } \varphi \end{array} \right\} = \# \left\{ \beta \in E \mid \begin{array}{l} \beta \text{ ist eine} \\ \text{Nst. von } \varphi_*(f) \end{array} \right\} \leq \text{Grad } f = [L : K]$$

*Beweis.* • Abbildung ist wohl-definiert: Sei  $f = \sum a_i X^i$

$$\begin{aligned} \varphi_*(f)(\psi(\alpha)) &= \sum_i \underbrace{\varphi(a_i)}_{\psi(a_i)} \psi(\alpha)^i \\ &\stackrel{\psi \text{ Körperhom.}}{=} \psi\left(\sum_i a_i \alpha^i\right) = \psi(f(\alpha)) = \psi(0) = 0 \end{aligned}$$

- Abbildung ist injektiv:  $L = K[\alpha] \implies$  Ausdehnungen  $\psi : L \rightarrow E$  sind eindeutig bestimmt durch  $\psi|_K = \varphi$  und Angabe von  $\psi(\alpha)$ . D.h. unterschiedliche Ausdehnungen führen auf verschiedene Nullstellen von  $\varphi_*(f)$ .
- Abbildung ist surjektiv: Sei  $\beta \in E$  Nullstelle von  $\varphi_*(f)$ . Betrachte den Ringhomomorphismus:

$$\xi : K[X] \rightarrow E, \sum \alpha_i X^i \mapsto \sum \varphi(\alpha_i) \beta^i$$

Beachte:  $f \in \text{Kern}(\xi)$ , nach der Wahl von  $\beta$ , nach dem Homomorphiesatz erhalten wir einen Ringhomomorphismus

$$\bar{\xi} : K[X]_{/(f)} \rightarrow E, [g] \mapsto \varphi_*(g)(\beta)$$

Wir erinnern uns, dass  $L$  konstruiert wurde als  $K[X]_{/(f)}$ , d.h. wir haben einen Isomorphismus

$$\bar{\rho} : K[X]_{/(f)} \rightarrow L, [g] \mapsto g(\alpha)$$

Erhalten  $\psi : L \rightarrow E$  als  $\psi = \bar{\xi} \circ \bar{\rho}^{-1}$  (prüfe  $\psi|_K = \varphi$  und  $\psi(\alpha) = \bar{\xi}(\bar{\rho}^{-1}(\alpha)) = \bar{\xi}(\bar{X}) = \beta$ ).  $\square$

**Lemma 4.34.** Sei  $L \supseteq K$  ein Oberkörper mit  $[L : K] < \infty$ , dann  $\exists$  Oberkörper  $F \supseteq K$  mit  $L \supsetneq F$  und  $f \in F[X]$  irred., sodass  $L \supseteq F$  Stammkörper von  $f$  ist.

*Beweis.* TODO.  $\square$

**Korollar 4.35.** Sei  $L \supseteq K$  ein Oberkörper mit  $[L : K] < \infty$  und sei  $\varphi : K \rightarrow E$  ein Körperhomomorphismus, dann gilt:

$$\#\{\psi : L \rightarrow E \text{ Ausdehnung von } \varphi\} \leq [L : K]$$

**Satz 4.36.** Sei  $E$  algebraisch abgeschlossener Körper,  $\varphi : K \rightarrow E$  ein Körperhom. Sei  $L \supseteq K$  ein algebraischer Oberkörper, dann  $\exists$  Ausdehnung  $\psi : L \rightarrow E$  von  $\varphi$ .

*Beweis.* TODO. □

**Definition 4.37.** Seien  $E_1, E_2$  Oberkörper von  $K$ . Ein Körperhomomorphismus  $\varphi : E_1 \rightarrow E_2$  heißt

- (a)  $K$ -Homomorphismus :  $\iff \varphi|_K = \text{id}_K$
- (b)  $K$ -Isomorphismus :  $\iff \varphi$  ist bij. und  $\varphi|_K = \text{id}_K$
- (c)  $K$ -Automorphismus :  $\iff E_1 = E_2$  und  $\varphi$  ist  $K$ -Isomorphismus.

**Notation.**

- (a)  $\text{Hom}_K(E_1, E_2) := \{\varphi : E_1 \rightarrow E_2 \mid \varphi \text{ ist } K\text{-Hom.}\}$
- (b)  $\text{Isom}_K(E_1, E_2) := \{\varphi : E_1 \rightarrow E_2 \mid \varphi \text{ ist } K\text{-Isom.}\}$
- (c)  $\text{Aut}_K(E_1) := \text{Isom}_K(E_1, E_1)$

**Korollar 4.38.** Sei  $E \supseteq K$  ein algebraischer Oberkörper und  $\overline{K} \supseteq K$  ein algebraischer Abschluss von  $K$ , dann:

- (a)  $\text{Hom}_K(E, \overline{K}) \neq \emptyset$  (Satz 36). Ist  $[E : K] < \infty$ , so gilt  $\# \text{Hom}_K(E, \overline{K}) \leq [E : K]$  (Kor 35). Ist  $E$  Stammkörper zu  $f \in K[X]$  irred, so gilt

$$\# \text{Hom}_K(E, \overline{K}) = \#\{\alpha \in E \mid f(\alpha) = 0\}$$

(Lemma 33)

- (b) Ist  $E$  algebraisch abgeschlossen, so gilt  $\text{Hom}_K(E, \overline{K}) = \text{Isom}(K)(E, \overline{K}) (\neq \emptyset$  wegen (a))
- (c) Ist  $\overline{E}$  ein algebraischer Abschluss von  $E$  und  $\varphi : E \rightarrow \overline{K}$  ein  $K$ -Homomorphismus, so  $\exists K$ -Isomorphismus  $\psi : \overline{E} \rightarrow \overline{K}$ , der  $\varphi$  ausdehnt. ((b) und Satz 36)

*Beweis.* TODO □

### 4.3 Normale Erweiterungen und Zerfällungskörper

**Bezeichnung.** Nenne Oberkörper  $E \supseteq K$  auch Erweiterungskörper oder Erweiterung.

**Definition 4.39.** (a) Eine algebraische Erweiterung  $E \supseteq K$  heißt normal :  
 $\iff \forall \alpha \in E : \mu_{\alpha, K}$  zerfällt in Linearfaktoren über  $E[X]$   $\iff \forall f \in$   
Übung

$K[X]$  irred. mit Nullstellen  $\alpha_1, \dots, \alpha_n$  in  $\overline{K}$  gilt: liegt ein  $\alpha_i$  in  $E$ , so folgt  $\{\alpha_1, \dots, \alpha_n\} \subseteq E$ .

- (b) Eine Erweiterung  $E \supseteq K$  heißt Zerfällungskörper (ZK) über  $K$  von  $f \in K[X] \setminus K$  normiert :  $\iff$

$$(i) \exists \alpha_1, \dots, \alpha_n \in E : f = \prod_{1 \leq i \leq n} (X - \alpha_i)$$

- (ii) Kein echter Unterkörper von  $E$  enthält  $\alpha_1, \dots, \alpha_n$ .

**Proposition 4.40.** Sei  $f \in K[X] \setminus K$  normiert, dann gilt:

- (a)  $f$  besitzt einen eindeutigen Zerfällungskörper in  $\overline{K}$ , nämlich  $E = K(\alpha_1, \dots, \alpha_n)$  mit  $\alpha_1, \dots, \alpha_n$  die Nst. von  $f$  in  $\overline{K}$ . (so dass  $f = \prod_{1 \leq i \leq n} (X - \alpha_i)$ ,  $n = \text{Grad } f$ )
- (b) Ist  $E$  ein Zerfällungskörper von  $f$ , und  $\varphi : E \rightarrow F$  ein Körperhomomorphismus, so ist  $\varphi(E)$  der Zerfällungskörper über  $\varphi(K)$  von  $\varphi_*(f)$
- (c) Je zwei Zerfällungskörper  $E, E'$  zu  $f$  (über  $K$ ) sind  $K$ -isomorph.

Beweis. TODO. □

**Beispiel 4.41.**

$$f = X^4 - 5 \underset{\text{Übung}}{=} (X - \sqrt[4]{5})(X - i\sqrt[4]{5})(X + \sqrt[4]{5})(X + i\sqrt[4]{5}) \in \mathbb{Q}[X]$$

Zerfällungskörper von  $f$  über  $\mathbb{Q}$  ist (Übung)

$$E = \mathbb{Q}(i, \sqrt[4]{5})$$

und es gilt (Übung)  $[E : \mathbb{Q}] = 8$ .

**Wiederholung.**  $E \supseteq K$  algebraische Erweiterung heißt normal  $\iff \forall \alpha \in E$  zerfällt  $\mu_{\alpha, K}$  in  $E[X]$  über Linearfaktoren.

**Satz 4.42.** Für eine algebraische Erweiterung  $E \supseteq K$  sind äquivalent:

- (i)  $\forall \psi, \psi' \in \text{Hom}_K(E, \overline{K})$  gilt  $\psi(E) = \psi'(E)$
- (i')  $\forall \psi \in \text{Hom}_K(E, \overline{K})$  gilt  $\psi(E) = E$
- (ii)  $E \supseteq K$  ist normale Erweiterung.

Gilt  $[E : K] < \infty$ , so sind (i), (ii) äquivalent zu

- (iii)  $E$  ist der Zerfällungskörper eines Polynoms in  $K[X]$ .

Beweis. TODO. □

**Korollar 4.43.** Sei  $E$  ein Oberkörper von  $K$  in  $\overline{K}$  mit  $[E : K] < \infty$ , dann  $\exists$  kleinster Oberkörper  $F \supseteq E$  in  $\overline{K}$ , sodass  $F \supseteq K$  normal ist, für diesen gilt  $[F : K] < \infty$ .

Beweis. TODO. □

**Definition 4.44.** Der Körper  $F \supseteq \overline{K}$  aus Korollar 43 heißt normale Hülle von  $E \supseteq K$ .

## 4.4 Seperabilität

Sei  $\overline{K}$  ein algebraischer Abschluss von  $K$ .

**Vorbereitung.** “Formale Ableitung.”

**Definition 4.45.**

$$\frac{d}{dX} : K[X] \rightarrow K[X],$$

$$f = \sum_{0 \leq i \leq n} a_i X^i \mapsto f' := \frac{d}{dX} f = \sum_{0 \leq i \leq n} i a_i X^{i-1}$$

Hierbei steht  $i$  für  $i \cdot 1 = 1 + \dots + 1 \in K$   $i$ -fache Summe.

**Proposition 4.46** (Rechenregeln).

(a)  $\frac{d}{dX}$  ist  $K$ -linear.

(b)  $\frac{d}{dX}(f \cdot g) = \frac{df}{dX} \cdot g + f \cdot \frac{dg}{dX}$ .

(c)  $\frac{d}{dX} f(g(X)) = \frac{df}{dX}(g(X)) \cdot \frac{d}{dX} g$ . Insbesondere  $\frac{d}{dX}(g^n) = n g^{n-1}$ .

*Beweis.* Übung. □

**Lemma 4.47.** Sei  $p = \text{char}(K)$ , sei  $f \in K[X] \setminus \{0\}$ , dann gilt

(a)  $p \nmid \text{Grad } f \implies \text{Grad } \frac{d}{dX} f = \text{Grad } f - 1$ .

(b)  $f' = 0 \iff f \in K[X^p]$  mit der Konvention  $X^0 = 1$

*Beweis.* TODO. □

**Definition 4.48.**  $f \in K[X]$  hat mehrfache Nullstelle in  $\overline{K} \iff \exists \alpha \in \overline{K}$  mit  $f(\alpha) = 0$  und  $(X - \alpha)^2$  teilt  $f$  in  $\overline{K}$ .

**Bemerkung 4.49** (Übung).  $\alpha \in \overline{K}$  ist mehrfache Nullstelle von  $f \iff f(\alpha) = f'(\alpha) = 0$ .

**Proposition 4.50.** Sei  $f \in K[X] \setminus \{0\}$  und  $g := \text{ggT}(f, f') \in K[X]$ . Dann:  $f$  hat mehrfache Nullstellen in  $\overline{K} \iff \text{Grad } g = 0$ .

*Beweis.* TODO. □

**Korollar 4.51.** Sei  $p = \text{char } K$  und  $f \in K[X]$  irred. Dann sind äquivalent:

(i)  $f$  hat mehrfache Nullstelle in  $\overline{K}$ .

(ii)  $p > 0$  und  $f' = 0$ .

(iii)  $p > 0$  und  $\exists g \in K[X]$  ohne mehrfache Nst. und  $\exists m > 0$  sodass  $f = g(X^{p^m})$  und  $g$  irred.

Insbesondere gelten für  $g, m$  aus (iii):

(a)  $p^m \mid \text{Grad } f$

(b)  $\#\{\beta \in \overline{K} \mid f(\beta) = 0\} = \text{Grad } g$

(c) Ist  $\xi : K \rightarrow K'$  ein Körperhomomorphismus, so gilt  $\xi_* f = (\xi_* g)(X^{p^m})$  und

$$\#\{\beta \in \overline{K}' \mid \xi_* f(\beta) = 0\} = \text{Grad } g = \text{Grad}(\xi_*(g))$$

*Beweis.* TODO. □

**Definition 4.52.** Sei  $f \in K[X] \setminus K$ , und  $E \supseteq K$  Oberkörper.

- (a)  $f$  heißt separabel  $\iff$  Kein irred. Faktor von  $f$  hat mehrfache Nst.
- (b)  $\alpha \in E$  heißt separabel über  $K \iff \mu_{\alpha, K}$  ist separabel.
- (c)  $E \supseteq K$  heißt separabel  $\iff$  alle  $\alpha \in E$  sind separabel über  $K$ .
- (d)  $K$  heißt perfekt  $\iff$  alle  $g \in K[X] \setminus K$  sind separabel ( $\iff$  alle algebraische Erweiterungen  $E \supseteq K$  sind separabel.)
- (e) Ist  $f$  irred., so heißt  $f$  rein inseparabel  $\iff f$  besitzt genau eine Nst. in  $\overline{K}$ .
- (f)  $E \supseteq K$  ist rein inseparabel  $\iff \forall \alpha \in E : \mu_{\alpha, K}$  ist rein inseparabel.

**Beispiel** (zu 52(e)). in 54 geg.  $X^p - Y$

**Beispiel 4.53.** Gelte  $\text{char } K = p > 0$ , sei  $f = X^p - a \in K[X]$  und sei  $b \in \overline{K}$  eine Nst. von  $f$ , dann:

- (a)  $(X - b)^p = f(X)$  in  $\overline{K}[X]$
- (b)  $f$  ist irred.  $\iff b \in \overline{K} \setminus K$ .

*Beweis.* Übung. □

**Beispiel 4.54.**  $K = \mathbb{F}_p(Y) = \text{Quot}(\mathbb{F}_p[Y])$ , sei  $f(X) = X^p - Y \in (\mathbb{F}_p[Y])[X] \subseteq K[X]$  irred. nach Existenz ( $Y \in \mathbb{F}_p[Y]$  prim). Haben TODO.

**Satz 4.55.**  $K$  ist perfekt  $\iff$  es gelten (i) oder (ii).

(i)  $\text{char } K = 0$ .

(ii)  $\text{char } K = p > 0$  und der Frobeniushomomorphismus

$$\varphi_K : K \rightarrow K, \alpha \mapsto \alpha^p$$

ist surjektiv. ( $\varphi_K$  ist Ringhomomorphismus, da  $\text{char } K = p$ , also ein Körperhomomorphismus)

**Beispiel.**

$$\varphi_K : \mathbb{F}_p \rightarrow \mathbb{F}_p(Y) = K, \quad \text{Bild}(\varphi_K) \stackrel{\text{Übung}}{=} \mathbb{F}_p(Y^p)$$

und  $\mathbb{F}_p$  ist perfekt.

**Korollar 4.56.**  $K$  endlicher Körper  $\implies K$  ist perfekt.

*Beweis.* TODO. □

**Beispiel 4.57.**  $K$  algebraisch abgeschlossen  $\implies K$  perfekt, denn jede algebraische Erweiterung  $E$  ist separabel, da  $E = K$ .

**Definition 4.58.** Sei  $E \supseteq K$  ein Oberkörper mit  $[E : K] < \infty$ , der separable Grad von  $E \supseteq K$  ist

$$[E : K]_s := \# \text{Hom}_K(E, \overline{K}) \quad (= \text{Hom}_K(E, \overline{E}))$$

**Facts 4.59.** (a)  $[E : K]_s \leq [E : K]$

(b) Ist  $E$  Stammkörper über  $K$  zu  $\alpha \in E \implies [E : K]_s \stackrel{38a}{=} \#\{\beta \in \overline{K} \mid \mu_{\alpha, K}(\beta) = 0\}$

(c) Seien  $E, \alpha$  wie in (b), dann ist  $\text{Grad } \mu_{\alpha, K} = [E : K] = [E : K]_s \iff \mu_{\alpha, K}$  ist separabel  $\iff \#\{\beta \in \overline{K} \mid \mu_{\alpha, K}(\beta) = 0\} = \text{Grad } \mu_{\alpha, K}$

**Lemma 4.60.** Seien  $K \subseteq E \subseteq F$  Oberkörper mit  $[F : K] < \infty$ , dann

$$[F : K]_s = [F : E]_s \cdot [E : K]_s \quad (*)$$

*Beweis.* TODO. □

**Satz 4.61.** Für Oberkörper  $E \supseteq K$  mit  $[E : K] < \infty$  sind äquivalent:

(i)  $E \supseteq K$  separabel.

(ii) Für  $\alpha_1, \dots, \alpha_n \in E : E = K[\alpha_1, \dots, \alpha_n]$ , gilt  $f = \prod_i \mu_{\alpha_i, K}$  ist separabel.

(iii)  $[E : K]_s = [E : K]$

**Korollar 4.62.** Seien  $F \supseteq E \supseteq K$  Oberkörper mit  $[F : K] < \infty$ , dann:  $F \supseteq K$  separabel  $\iff F \supseteq E$  und  $E \supseteq K$  sind separabel.

**Korollar 4.63** (Übung). Sei  $E \supseteq K$  algebraischer Oberkörper, dann ist  $E_0 = \{\alpha \in E \mid \alpha \text{ separabel über } K\}$  der größte Unterkörper von  $E$ , der separabel über  $K$  ist.

**Bemerkung.** Der Beweis verwendet, dass Kor. 62 auch dann gilt, wenn  $F \supseteq K$  eine beliebige algebraische Erweiterung ist und  $F \supseteq E \supseteq K$  Erweiterungen sind.

**Korollar 4.64.** Sei  $E \subseteq \overline{K}$  Oberkörper von  $K$  mit  $[E : K] < \infty$ , ist  $E \supseteq K$  separabel, so ist auch die normale Hülle  $F$  von  $E$  über  $K$  separabel.

*Beweis.* Gelte  $E = K[\alpha_1, \dots, \alpha_n]$  für  $\alpha_1, \dots, \alpha_n \in E$ , dann ist  $F$  der ZK in  $\overline{K}$  von  $\mu_{\alpha_1, K} \cdot \dots \cdot \mu_{\alpha_n, K}$ , es folgt, dass  $F$  separabel über  $K$  ist, wegen Satz 61, Formulierung in (ii) (Die  $\mu_{\alpha_i, K}$  sind separabel, da  $\alpha_i$  über  $K$  separabel.) □

**Satz 4.65** (Satz von primitiven Elementen). Sei  $E \supseteq K$  Oberkörper mit  $[E : K] < \infty$ , ist  $E \supseteq K$  separabel, so  $\exists \alpha \in E$  mit  $E = K(\alpha)$



## Kapitel 5

# Galoistheorie und Anwendungen

### 5.1 Galoistheorie und Anwendungen

**Definition 5.1** (Fixkörper). Seien  $E, K$  Körper, ist  $G \leq \text{Aut}(E)$  eine Untergruppe, so heißt

$$E^G = \{\alpha \in E \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\}$$

der Fixkörper von  $E$  unter  $G$ .

**Bemerkung.**  $E^G \subseteq E$  ist ein Unterkörper

*Beweis.* (Übung) Sei  $\alpha \in E^G \setminus \{0\}$ , dann:  $1 = \sigma(1) = \sigma(\alpha \cdot \alpha^{-1}) = \sigma(\alpha)\sigma(\alpha^{-1}), \forall \sigma \in G \implies \alpha^{-1} = \sigma(\alpha^{-1}) \forall \sigma \in G$ .  $\square$

**Definition 5.2.**

- (a)  $\Gamma_E := \{G \leq \text{Aut}(E)\}$
- (b)  $\Sigma_E := \{K \subseteq E \mid K \text{ Unterkörper}\}$
- (c)  $\text{Inv}_E : \Gamma_E \rightarrow \Sigma_E, G \mapsto E^G = \text{Inv}_E(G)$
- (d)  $\text{Gal}_E : \Sigma_E \rightarrow \Gamma_E, K \mapsto \text{Gal}_E(K) := \text{Aut}_K(E) = \{\sigma \in \text{Aut}(E) \mid \sigma|_K = \text{id}_K\}$

**Lemma 5.3.** (a) Die Abbildungen  $\text{Inv}_E$  und  $\text{Gal}_E$  sind inklusionsumkehrend.

(b)  $\text{Inv}_E(\text{Gal}_E(K)) \supseteq K$

(c)  $\text{Gal}_E(\text{Inv}_E(G)) \supseteq G$

*Beweis.* TODO  $\square$

**Bemerkung.** Ziel: Unter geeigneten Einschränkungen an  $G$  bzw.  $K$  wollen wir “Gleichheit” in (b) und (c) (für  $\Gamma_{E/K}$  und  $\Sigma_{E/K}$ ), dann erhalten wir eine Bijektion:

$$G \in \Gamma_{E/K} \xleftrightarrow{1-1} F \in \Sigma_{E/K}$$

**Satz 5.4.** Für eine endliche Körpererweiterung  $E \supset K$  sind äquivalent:

- (i)  $E$  ist Zerfällungskörper eines separablen Polynoms in  $K[X]$
- (ii)  $E \supseteq K$  ist normal und separabel.
- (iii)  $E \supseteq K$  ist separabel und  $\text{Hom}_K(E, \overline{E}) = \text{Aut}_K(E)$
- (iv)  $\# \text{Aut}_K(E) = [E : K]$

Beweis. TODO. □

**Definition 5.5** (Galoiserweiterung/Galoisgruppe). Erfüllt  $E \supseteq K$  Oberkörper mit  $[E : K] < \infty$  die äquivalenten Bedingungen aus Satz 4, so heißt  $E/K$  Galoissch (oder eine Galoiserweiterung von  $K$ ) (genauer  $E \supseteq K$  ist endlich Galoissch) In diesem Fall definiert man die **Galoisgruppe** von  $E$  über  $K$  als

$$\text{Gal}(E/K) := \text{Aut}_K(E) = \text{Gal}_E(K)$$

**Korollar 5.6.** Sei  $E \supseteq K$  Galoissch und sei  $F \subseteq E$  Unterkörper mit  $F \supseteq K$ , dann:

- (a)  $E \supseteq F$  ist Galoissch.
- (b) Es sind äquivalent:
  - (i)  $F \supseteq K$  Galoissch
  - (ii)  $F \supseteq K$  normal
  - (iii)  $\forall \sigma \in \text{Gal}(E/K) : \sigma(F) = F$ .

Beweis. TODO □

**Satz 5.7.** Sei  $G \leq \text{Aut}(E)$  endliche Untergruppe, dann gelten

- (a)  $[E : E^G] = \#G$
- (b)  $E \supseteq E^G$  ist Galoissch und  $G = \text{Gal}(E/E^G) = \text{Aut}_{E^G}(E)$

Beweis. TODO □

**Korollar 5.8.**  $G \leq \text{Aut}(E)$  endliche Untergruppe  $\implies G = \text{Gal}_E(\text{Inv}_E(G))$

**Korollar 5.9.** Sei  $E \supseteq K$  Galoissch, dann gilt  $\text{Inv}_E(\text{Gal}_E(K)) = K$

Beweis. TODO □

**Übung 5.10.** Sei  $G \leq \text{Aut}(E)$  endliche Untergruppe und  $K = E^G$ ,  $G$  wirkt auf  $E$  durch

$$G \times E \rightarrow E, (\sigma, \alpha) \mapsto \sigma(\alpha)$$

Sei  $\alpha \in E$  und  $A = G\alpha$  die  $G$ -Bahn durch  $\alpha$ , definiere  $\mu := \prod_{\beta \in A} (X - \beta)$ , dann gelten:  $\mu \in K[X]$ ,  $\mu = \mu_{\alpha, K}$  und  $\mu$  ist separabel.

**Satz 5.11** (Hauptsatz der Galoistheorie). Sei  $E \supseteq K$  Galoissch mit Galoisgruppe  $G = \text{Gal}(E/K)$ , seien

$$\Gamma_{E/K} = \{H \leq G\}, \quad \Sigma_{E/K} = \{F \subseteq E \text{ Unterkörper} \mid K \subseteq F\}$$

dann gelten:

(a) Die Abbildungen:

$$\Gamma_{E/K} \xrightleftharpoons[\text{Gal}(E/F) \leftarrow F : \text{Gal}_E]{\text{Inv}_E : H \mapsto E^H} \Sigma_{E/K}$$

sind zueinander inverse Bijektionen.

(b)  $\text{Inv}_E$  und  $\text{Gal}_E$  sind inklusionsumkehrend.

(c) Es gelten  $[E : E^H] = \#H$  und  $\# \text{Gal}(E/F) = [E : F]$

(d) Sei  $F \in \Sigma_{E/K}$  und  $H = \text{Gal}(E/F)$ , dann:

(i)  $\forall \sigma \in G$  gilt

$$\sigma(F) \xrightleftharpoons[\text{Inv}_E(\cdot)]{\text{Gal}_E(\cdot)} \sigma H \sigma^{-1}$$

d.h.  $E^{\sigma H \sigma^{-1}} = \sigma(E^H) = \sigma(F)$  und  $\text{Gal}(E/\sigma(F)) = \sigma \text{Gal}(E/F) \sigma^{-1}$

(ii) Die Abbildung

$$\begin{aligned} \psi : N_G(H)/H &\longrightarrow \text{Aut}_K(F) \\ \sigma H &\longmapsto \sigma|_F \end{aligned}$$

ist wohl-definiert und ein Gruppenisomorphismus.

(iii)  $F \supseteq K$  Galoissch  $\iff H \trianglelefteq G$  ist Normalteiler, in diesem Fall definiert  $\psi$  einen Gruppenisomorphismus

$$\begin{aligned} \psi : G/H &\longrightarrow \text{Gal}(F/K) \\ \sigma H &\longmapsto \sigma|_F \end{aligned}$$

**Wiederholung.**  $N_G(H) := \{g \in G \mid gHg^{-1} = H\}$

Beweis. TODO

□

**Korollar 5.12.**  $E \supseteq K$  endlich separabel, dann gilt:

$M = \{F \subseteq E \text{ Unterkörper} \mid K \subseteq F\}$  ist endlich.

Beweis. TODO

□

**Satz 5.13.** Jede endliche Gruppe  $G$  ist die Galoisgruppe für eine geeignete Galoiserweiterung  $E \supseteq K$ .

Beweis. TODO

□

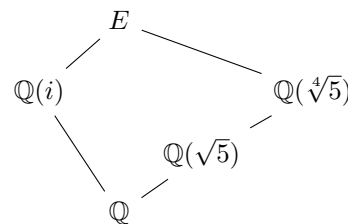
**Bemerkung 5.14.**

$$\begin{aligned} \psi : G = \text{Gal}(E/K) &\longrightarrow \text{Bij}(\{\alpha_1, \dots, \alpha_n\}) \cong S_n \\ \sigma &\longmapsto \sigma|_{\{\alpha_1, \dots, \alpha_n\}} \end{aligned}$$

ist wohl-definiert und ein injektiver Gruppenhomomorphismus. D.h.  $G$  ist isomorph zu einer Untergruppe von  $S_n$ . Ist  $f$  irred. so wirkt  $G$  transitiv.

**Beispiel 5.15.** Sei  $E \subseteq \mathbb{C}$  der Zerfällungskörper über  $\mathbb{Q}$  zu  $f = X^4 - 5 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$ . Wir wissen:

- (a)  $f$  separabel ( $\mathbb{Q}$  perfekt)
- (b)  $f$  irred. (Eisenstein mit  $p = 5$ )
- (c) Nullstellenmenge von  $f$  ist  $Z = \{\pm \sqrt[4]{5}, \pm i \sqrt[4]{5}\}$
- (d)  $E = \mathbb{Q}(Z) = \mathbb{Q}(i, \sqrt[4]{5})$
- (e) Einige Unterkörper von  $E$ :



- (f)  $[E : \mathbb{Q}] = 8$ .  $f$  ist irred. als Polynom in  $\mathbb{Q}(i)[X]$  und  $E \supseteq \mathbb{Q}(i)$  ist der Stammkörper zu  $f$ . (und auch der Zerfällungskörper von  $f$  über  $\mathbb{Q}(i)$ )
- (g)  $\mathbb{Q}(i) \supseteq \mathbb{Q}$  ist Galoissch, denn  $\mathbb{Q}(i) \supseteq \mathbb{Q}$  ist der Zerfällungskörper von  $X^2 + 1$ .
- (h)  $G = \text{Gal}(E/\mathbb{Q})$  ist eine Gruppe mit 8 Elementen.  $G$  wirkt auf  $Z \xrightarrow{\#Z} G$  ist isomorph zu einer Untergruppe von  $S_4$
- (i)  $[E : \mathbb{Q}(i)] = 4$  (nach (f) und (a)) und  $N := \text{Gal}(E/\mathbb{Q}(i)) \subseteq \text{Bij}(Z) \cong S_4$  und sie ist transitiv, da  $f \in \mathbb{Q}(i)[X]$  irred. Sei  $\rho \in N$  der Automorphismus mit  $\rho(\underbrace{\sqrt[4]{5}}_{\alpha_1}) = \underbrace{i \sqrt[4]{5}}_{\alpha_2}$  (Gruppe transitiv).

$$\implies \rho^2(\sqrt[4]{5}) = \rho(i \sqrt[4]{5}) \underset{\rho|_{\mathbb{Q}(i)} = \text{id}_{\mathbb{Q}(i)}}{=} i \rho(\sqrt[4]{5}) = ii \sqrt[4]{5} = \underbrace{-\sqrt[4]{5}}_{\alpha_3}$$

analog ist

$$\rho^3(\sqrt[4]{5}) = \underbrace{-i \sqrt[4]{5}}_{\alpha_4}, \quad \rho^4 = \text{id}_E$$

d.h.  $N = \langle \rho \rangle$  und  $\rho$  hat Ordnung 4 ( $N \cong \mathbb{Z}/4\mathbb{Z}$ )

- (j) Wir wissen  $N \trianglelefteq G$ , da  $\mathbb{Q}(i) \supseteq \mathbb{Q}$  Galoissch ( $\implies \text{Gal}(E/\mathbb{Q}(i)) \trianglelefteq \text{Gal}(E/\mathbb{Q})$  normal)

$$\xrightarrow[\text{von } S_4]{\text{als U.G.}} G \leq N_{S_4}(\underbrace{N}_{\langle (1 \ 2 \ 3 \ 4) \rangle})$$

Behauptung:  $\#N_{S_4}(N) = 8 \iff G = N_{S_4}(N)$  ist vollständig bestimmt.

*Beweis.* Sei  $\tau \in N_{S_4}(N) \implies \tau \rho \tau^{-1} \in \langle \rho \rangle \implies \tau \rho \tau^{-1} \in \{\rho, \rho^{-1}\}$

Fall 1: Betrachte  $\tau\rho\tau^{-1} = \rho$  ( $\iff \tau(1\ 2\ 3\ 4)\tau^{-1} = (1\ 2\ 3\ 4)$ )

$$(\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)) = (1\ 2\ 3\ 4)$$

Zykeldarstellung ist eindeutig bis auf Zykelpermutation der Einträge.

$$\implies \tau = \text{id}, \tau = \rho, \underbrace{\tau = \rho^2}_{(\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)) = (3\ 4\ 1\ 2)}, \tau = \rho^3$$

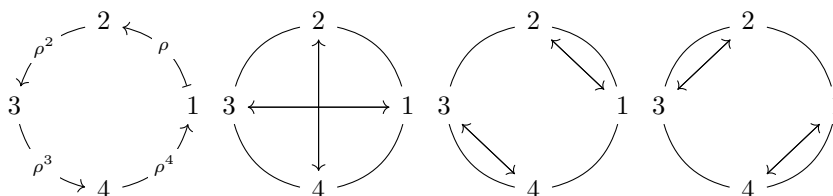
$$\iff \tau \in \langle \rho \rangle.$$

Fall 2: Für  $\tau\rho\tau^{-1} = \rho^{-1} \iff (\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)) = (4\ 3\ 2\ 1)$  also  
 $(= (3\ 2\ 1\ 4) = (2\ 1\ 4\ 3) = (1\ 4\ 3\ 2)) \implies 4$  Möglichkeiten für  $\tau$ :

$$\tau \in \{\underbrace{(1\ 3)}_{=: \sigma}, (2\ 4), (1\ 4)(2\ 3), (1\ 2)(4\ 3)\} = \sigma \cdot \langle \rho \rangle$$

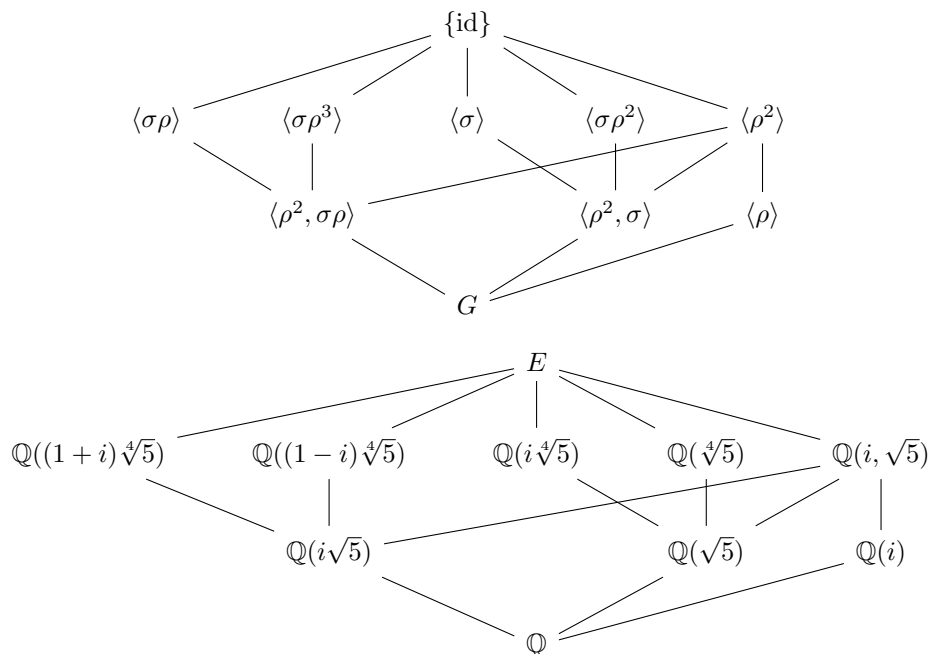
□

Fazit:  $G = N_{S_4}(N)$  hat 8 Elemente. Veranschaulichung der Permutationen  
 $(1\ 2\ 3\ 4)$ ,  $(1\ 3)(2\ 4)$ ,  $(1\ 2)(3\ 4)$  und  $(1\ 4)(2\ 3)$



$G \cong D_4$  Diedergruppe auf regulärem 4-Eck.

Untergruppenverband:



5 Unterkörper mit  $[E : F] = 2$ ,  $[F : \mathbb{Q}] = 4$  und 3 Unterkörper mit  $[F : \mathbb{Q}] = 2$

## 5.2 Beispielklassen von Galoiserweiterungen

### 5.2.1 Endliche Körper

Sei  $p$  Primzahl und  $\overline{\mathbb{F}}_p$  ein (fest gewählter) algebraischer Abschluss von  $\mathbb{F}_p$ . Sei  $\varphi : \overline{\mathbb{F}}_p \rightarrow \overline{\mathbb{F}}_p, \alpha \mapsto \alpha^p$ , es gilt  $\varphi \in \text{Aut}(\overline{\mathbb{F}}_p)$ .  $\varphi$  ist surjektiv, da  $\overline{\mathbb{F}}_p$  perfekt (als algebraischer Abschluss) und  $\varphi$  injektiv, Homom. klar  
 $\implies$  Es gibt auch  $\varphi^{-1}$ , d.h. jedes  $\alpha \in \overline{\mathbb{F}}_p$  besitzt eine eindeutige  $p$ -te Wurzel.  
 $\implies \forall m \in \mathbb{Z}$  haben  $\varphi^m \in \text{Aut}(\overline{\mathbb{F}}_p)$ , d.h.  $\mathbb{Z} \cong \{\varphi^m : m \in \mathbb{Z}\} \leq \text{Aut}(\overline{\mathbb{F}}_p)$  ist Untergruppe.

**Satz 5.16.**

- (a)  $\mathbb{F}_{p^n} := (\overline{\mathbb{F}}_p)^{\varphi^n} = \{\alpha \in \overline{\mathbb{F}}_p \mid \varphi^n(\alpha) = \alpha^{p^n} \stackrel{!}{=} \alpha\} \subseteq \overline{\mathbb{F}}_p$  ist Unterkörper.
- (b)  $\#\mathbb{F}_{p^n} = p^n$  und  $\mathbb{F}_{p^n}$  ist der Zerfällungskörper von  $f_n := X^{p^n} - X \in \mathbb{F}_p[X]$ .
- (c) Bis auf Isomorphie  $\exists!$  Körper mit  $p^n$  Elementen.
- (d) Für  $m, n \in \mathbb{N}$  gilt:  $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n$
- (e) Gilt  $m \mid n$ , so ist  $\mathbb{F}_{p^n} \supseteq \mathbb{F}_{p^m}$  Galoissch mit Gruppe  $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \varphi^m \rangle$  ist zyklisch von der Ordnung  $\ell = \frac{n}{m}$ .

*Beweis.* TODO □

### 5.2.2 Einheitswurzelkörper (Kreisteilungskörper)

**Definition 5.17.** Sei  $n \in \mathbb{N}$ , ein Element  $\rho \in \overline{K}^\times$  heißt primitive  $n$ -te Einheitswurzel (EW)  $\iff \text{ord}(\rho) = n$  als Element der Gruppe  $(\overline{K}^\times, 1, \cdot)$ .

**Lemma 5.18.** Sei  $G \leq (\overline{K}^\times, 1, \cdot)$  endliche Untergruppe, dann ist  $G$  zyklisch.

*Beweis.* Sei  $n = \#G$  und  $n' := \exp(G)$ , wir wissen  $n' \mid n$ . Da  $G$  abelsch:  $G$  zyklisch  $\iff n' = n$ . Annahme  $n' < n$  ( $\implies \forall \alpha \in G$  gilt  $\alpha^{n'} - 1 = 0$ )

$$\implies G \subseteq \underbrace{\{\alpha \in K \mid \alpha \text{ ist Nst. von } X^{n'} - 1\}}_{\text{Menge hat höchstens Kardinalität } n'} \implies n = \#G \leq n' \text{ Widerspruch.}$$

$$\implies n' = n \text{ (wissen schon } n' \text{ teilt } n).$$

□

**Beispiel.**  $\mathbb{F}_{p^n}^\times$  ist zyklische Gruppe der Ordnung  $p^{n-1}$

**Proposition 5.19.** Sei  $p = \text{char } K$ , sei  $n \in \mathbb{N}$ , dann:  $\overline{K}$  enthält eine primitive  $n$ -te Einheitswurzel  $\iff p \nmid n$ .

**Beispiel.**

- (a)  $\text{char } K = 0 \implies \overline{K}$  enthält primitive  $n$ -te Einheitswurzel für alle  $n \in \mathbb{N}$
- (b)  $K = \mathbb{C} \implies e^{2\pi i/n}$  ist primitive  $n$ -te Einheitswurzel. Die Elemente

$$\{(e^{2\pi i/n})^j \mid j \in \{0, \dots, n-1\}\}$$

bilden ein regelmäßiges  $n$ -Eck, deswegen heißt auch  $\mathbb{Q}(e^{2\pi i/n})$   $n$ -ter Kreisteilungskörper (über  $\mathbb{Q}$ ).  $e^{2\pi i/n}$  ist algebraisch, da Nst. von  $X^n - 1$

Beweis (von Proposition 19). TODO. □

**Proposition 5.20.** Sei  $\zeta \in \overline{K}^\times$  primitive  $n$ -te Einheitswurzel (insbesondere  $p = \text{char } K \nmid n$ ), dann:

- (a)  $K(\zeta)$  ist Zerfällungskörper des separablen Polynoms  $h_n = X^n - 1$  über  $K$  und insbesondere ist  $K(\zeta)$  Galoissch über  $K$ .
- (b) Sei  $H := \{\xi \in \overline{K}^\times \mid \xi^n = 1\}$ , dann gibt es zu  $\xi$  ein eindeutiges  $n_\xi \in \{1, \dots, n\}$  mit  $\zeta^{n_\xi} = \xi$ .
- (c) Die Abbildung

$$G := \text{Gal}(K(\zeta)/K) \rightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^\times, \sigma \mapsto n_{\sigma(\zeta)} \pmod n$$

ist wohl-definiert und ein Gruppenmonomorphismus. Insbesondere ist  $G$  abelsch (also auflösbar)

Beweis. TODO. □

**Satz 5.21.**

- (a)  $\phi_n$  ist irred. in  $\mathbb{Z}[X]$
- (b)  $\mathbb{Q}(\zeta_n) : \mathbb{Q} = \text{Grad } \phi_n = \#\mathbb{Z}_n^\times$
- (c)  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \rightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^\times, \sigma \mapsto \overline{m}_\sigma$  aus Bew. von 20 ist Gruppenisomorphismus.

Beweis. TODO. □

### 5.2.3 Galoiserweiterungen von Grad $p$ (eine Primzahl)

**Satz 5.22** (Kummererweiterungen). Gelte  $p$  Primzahl,  $p \nmid \text{char } K$ , gelte:  $K$  enthält eine primitive  $p$ -te Einheitswurzel  $\zeta_p$  (d.h.  $K^\times \supseteq N_p := \langle \zeta_p \rangle$  und  $N_p \cong \mathbb{Z}/p\mathbb{Z}$ ). Sei  $f = X^p - a, a \in K$ , sei  $E$  ein Zerfällungskörper von  $f$  und  $b \in \overline{K}$  eine Nullstelle von  $f$ . Dann:

- (a)  $f$  hat die Nullstelle  $b \cdot \zeta_p^i, i \in \{0, \dots, p-1\}$
- (b)  $E = K(b)$  ist Zerfällungskörper von  $f$  und  $E \supseteq K$  Galoissch. ( $f$  separabel)
- (c) Die Abbildung  $\varphi : \text{Gal}(E/K) \rightarrow N_p, \sigma \mapsto \frac{\sigma(b)}{b}$  ist wohl-definiert und ein Gruppenmonomorphismus.
- (d) Es sind äquivalent:
  - (i)  $[E : K] = p$
  - (ii)  $f$  ist irred.
  - (iii)  $f$  hat keine Nullstelle in  $K$
  - (iv)  $\varphi$  ist ein Isomorphismus.

- (e) Ist Umgekehrt  $E \supseteq K$  Galoissch mit  $\text{Gal}(E/K) \cong \mathbb{Z}/p\mathbb{Z}$ , so ist  $E$  ein Zerfällungskörper über  $K$  eines irred. Polynoms der Form  $X^p - c \in K[X]$ , wobei  $c \in K^\times / K^{\times p}$ .

**Proposition 5.23** (Übung, Lineare Algebra). Sei  $V$  ein endlich dimensionaler  $K$ -Vektorraum und  $\sigma \in \text{Aut}_K(V)$  mit  $\text{ord}(\sigma) = p$ , dann:

- (a) Das Minimalpolynom von  $\sigma$  ist  $X^p - 1$
- (b) Gilt  $p \neq \text{char } K$ , so besitzt  $\sigma$  einen Eigenwert  $\zeta$ , welcher eine primitive  $p$ -te Einheitswurzel ist.
- (c) Gilt  $p = \text{char } K$ , so enthält die Jordanform von  $\sigma$  einen  $d \times d$ -Block folgender Form mit  $d > 1$

$$\begin{pmatrix} 1 & 1 & & & \\ & \ddots & \ddots & & \\ & & \ddots & 1 & \\ & & & \ddots & 1 \\ & & & & 1 \end{pmatrix}$$

**Notation.** Für  $m \in \mathbb{N}$  mit  $\text{char } K \nmid m$ , so sei  $N_m := \{\zeta \in \overline{K} \mid \zeta^m = 1\} (= \mathbb{Z}/m\mathbb{Z})$

**Satz 5.24** (Kummererweiterungen). Sei  $p$  Primzahl mit  $p \nmid \text{char } K$  und gelte:  $K$  enthält eine primitive  $p$ -te Einheitswurzel  $\zeta_p$  (d.h.  $K^\times \supseteq N_p := \langle \zeta_p \rangle$  und  $N_p \cong \mathbb{Z}/p\mathbb{Z}$ ) und  $b \in \overline{K}$  eine Nst. von  $f$ , dann:

- (a)  $f$  hat die Nst.  $b \cdot \zeta_p^i, i \in \{0, \dots, p-1\}$
- (b)  $E = K(b)$  ist ZK von  $f$  und  $E/K$  galoissch. ( $f$  separabel)
- (c) Die Abbildung  $\varphi : \text{Gal}(E/K) \rightarrow N_p, \sigma \mapsto \frac{\sigma(b)}{b}$  ist wohl-def Gruppenmonomorphismus.
- (d) Es sind äquivalent:
- (i)  $[E : K] = p$
  - (ii)  $f$  ist irred.
  - (iii)  $f$  hat keine Nst in  $K$
  - (iv)  $\varphi$  ist ein Isomorphismus.
- (e) Ist umgekehrt  $E/K$  galoissch mit  $\text{Gal}(E/K) \cong \mathbb{Z}_p$ , so ist  $E$  ZK über  $K$  eines irred. Polynoms der Form  $X^p - c \in K[X]$  (wobei  $c \in K^\times \setminus K^{\times p}$ )

**Satz 5.25** (Artin-Schreier Erweiterungen). Sei  $p = \text{char } K > 0, f = X^p - X - a \in K[X]$  und sei  $E/K$  der ZK von  $f$  in  $\overline{K}$  und sei  $\beta \in E$  ein Nst. von  $f$ , dann:

- (a)  $E = K(\beta)$  und  $T = \{\beta + i \cdot 1_K\}, i$  in  $\{0, \dots, p-1\}$  ist die Nullstellenmenge von  $f$ .
- (b)  $E/K$  ist galoissch
- (c)  $\varphi : \text{Gal}(E/K) \rightarrow \mathbb{F}_p, \sigma \mapsto \sigma(\beta) - \beta$  ist ein Gruppenmonom. ( $\mathbb{F}_p$  sei identifiziert mit dem Primkörper von  $K$ )



(d) Es sind äquivalent

(i)  $[E : K] = p$

(ii)  $f$  ist irred.

(iii)  $f$  hat keine Nst. in  $K$

(iv)  $\varphi$  ist bijektiv

(v)  $a \in K \setminus y(K)$  für  $y : K \rightarrow K$  der Gruppenhom.  $X \mapsto X^p - X$

(e) Ist Umgekehrt  $F/K$  galoissch vom Grad  $p$ , so ist  $F$  ZK eines Polynoms der Form  $X^p - X - b \in K[X]$  mit  $b \in K \setminus y(K)$  (verwendet z.B. 23c)

## 5.3 Auflösbarkeit durch Radikale

**Definition 5.26.** Sei  $p = \text{char } K \geq 0$ ,

(i) Eine Kette von Körpererweiterungen  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n$  heißt:

(a) Wurzelturm  $\iff$  für  $i \in \{1, \dots, n\}$  existieren  $\alpha_i \in K_i$  und  $e_i \in \mathbb{N} \setminus p\mathbb{N}$  sodass  $K_i = K_{i-1}(\alpha_i)$  und  $\alpha_i^{e_i} \in K_{i-1}$ .

(b) Quadratwurzelturm  $\iff p \neq 2$  und für  $i \in \{1, \dots, n\}$  existieren  $\alpha_i \in K_i$  mit  $\alpha_i^2 \in K_{i-1}$  und  $K_i = K_{i-1}(\alpha_i)$ .

(ii) Ein Oberkörper  $E/K$  heißt (Quadrat-)Wurzelerweiterung  $\iff \exists$  (Quadrat-)Wurzelturm wie in (i) mit  $E \subseteq K_n$

(iii)  $f \in K[X]$  heißt auflösbar durch Radikale (Wurzelausdrücke)  $\iff$  der ZK von  $f$  ist eine Wurzelerweiterung.

**Notation.** QW = Quadratwurzel und W- = Wurzel

**Bemerkung** (Übung). Wegen  $e_i \in \mathbb{N} \setminus p\mathbb{N}$  ist  $K_i \supseteq K_{i-1}$  stets separabel ( $X^{e_i} - \alpha_i^{e_i} \in K_{i-1}[X]$ )

**Lemma 5.27.** Seien  $E, E' \subseteq \overline{K}$  Oberkörper von  $K$ , dann:

(a) Ist  $E/K$  eine  $(Q)W$ -Erweiterung und  $\sigma \in \text{Hom}_K(E, \overline{E})$ , so ist  $\sigma(E) \supseteq K$  eine  $(Q)W$ -Erweiterung

(b) Sind  $E, E'$   $(Q)W$ -Erweiterungen von  $K$ , so auch  $E[E'] = E'[E]$

(c) Ist  $E/K$  eine  $Q(W)$ -Erweiterung, so ist die normale Hülle von  $E$  eine  $(Q)W$ -Erweiterung von  $K$ .

**Bemerkung.** Gilt  $E' = K[\alpha_1, \dots, \alpha_n]$ , so hat man  $E[E'] = E[\alpha_1, \dots, \alpha_n]$

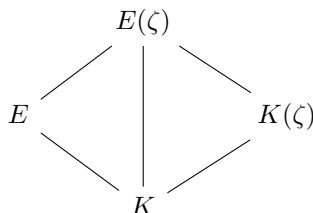
**Beispiel 5.28.** Sei  $n \in \mathbb{N}$  mit  $p \nmid n$  und  $\zeta \in \overline{K}$  eine primitive  $n$ -te EW, dann ist  $K[\zeta] \supseteq K$  eine W-Erweiterung ( $\zeta^n = 1 \in K$ )

**Bemerkung 5.29** (Übung). Sei  $\zeta \in \overline{K}$  eine primitive  $n$ -te EW, und  $E \subseteq \overline{K}$  ein Oberkörper von  $K$ , mit  $[E : K] < \infty$ , dann:

(a) Die Abbildung  $\varphi : \text{Gal}(E(\zeta)/E) \rightarrow \text{Gal}(K(\zeta)/K), \sigma \mapsto \sigma|_{K(\zeta)}$  ist wohl def und ein Gruppenmonom.

(b)  $[E(\zeta) : E]$  teilt  $[K(\zeta) : K]$

(c)  $[E(\zeta) : K]$  teilt  $[E : K]$



**Satz 5.30.** Für eine Galoiserweiterung  $E/K$  sind äquivalent:

(i)  $E/K$  ist Wurzelzerweiterung

(ii)  $\text{Gal}(E/K)$  ist auflösbar und  $\exists m \in \mathbb{N}, p \nmid m : p \nmid [E[N_m] : K[N_m]]$

**Bemerkung.** Im Fall  $p = 0$  entfällt.

**Korollar 5.31.** Sei  $f \in K[X] \setminus K$  separabel mit  $ZK E_f/K$ , dann:  $f$  ist auflösbar durch Radikale  $\iff \text{Gal}(E_f/K)$  ist auflösbar und  $\exists m$  (mit  $\text{char } K \nmid m$ ), sodass  $\text{char } K \nmid [E_f(\zeta_m) : K(\zeta_m)]$ .

In den Übungen:  $\exists f \in \mathbb{Q}[X] \setminus \mathbb{Q}, \deg f = 5, \text{Gal}(\mathbb{Q}_f/\mathbb{Q}) \cong S_5 \implies f$  nicht auflösbar durch Radikale.

Andersherum: Alle Untergruppen von  $S_n$  für  $n \leq 4$  sind auflösbar (Ordnung  $< 60$ )  $\implies$  ist  $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$  irred. vom Grad  $n \leq 4$ , so ist  $f$  auflösbar durch Radikale  $\implies$  Die allgemeine Gleichung vom Grad 5 (oder  $n \geq 5$ ) ist nicht auflösbar.

**Bemerkung 5.32.** Die Galoistheorie hilft auch, die Lösungsformeln zu finden ( $n \leq 4$ ) (Hungerford - Algebra).

## 5.4 Konstruierbarkeit mit Zirkel und Lineal

Sei  $S$  eine endliche Teilmenge der reellen Ebene  $\mathbb{R}^2$  (üblicherweise  $S = \{(0, 0), (1, 0)\}$ ), Frage: Welche Punkte der Ebene lassen sich mit Zirkel und Lineal aus  $S$  konstruieren?

Konkrete Fragen (alle Konstr. mit Zirkel und Lineal):

- A) Lassen sich beliebige Winkel 3-teilen?
- B) Kann ein zum Einheitskreis flächengleiches Quadrat konstruieren? (Quadratur des Kreises)
- C) Kann man die Seitenlänge eines Würfels mit Volumen 2 konstruieren?
- D) Für welche  $n \in \mathbb{N}$  kann man ein regelmäßiges  $n$ -Eck konstruieren.

Im Weiteren: Wir identifizieren  $\mathbb{R}^2$  mit  $\mathbb{C}$  und nehmen an,  $0, 1 \in S \subset \mathbb{C}$  mit der Metrik  $d(z, z') = |z - z'|$ .

- Für  $P \neq Q$  in  $\mathbb{C}$  sei  $\overline{PQ}$  die Gerade durch  $P$  und  $Q$

- Für  $P \in \mathbb{C}, r \in \mathbb{R}_{\geq 0}$  sei  $C_r(P) = \{z \in \mathbb{C} \mid |z - P| = r\}$  die Kreislinie um  $P$  zum Radius  $r$ .

**Definition 5.33** (Elementare Konstruktionen mit Zirkel und Lineal). Zu  $P_1 \neq P_2, P_3 \neq P_4, P_5 \neq P_6$  in  $S$  konstruiere

- (1) Schnittpunkt  $\overline{P_1 P_2} \cap \overline{P_3 P_4}$
- (2) Schnittpunkte  $\overline{P_1 P_2} \cap C_r(P_5), r = |P_6 - P_5|$
- (3) Schnittpunkte  $C_{r_1}(P_1) \cap C_{r_3}(P_3), r_1 = |P_1 - P_2|, r_3 = |P_3 - P_4|$

**Notation.** Zu geg.  $S$  definiere  $\tilde{S} = S \cup$  Menge der aus  $S$  elementar konstruierbaren Punkte.

**Definition 5.34.** (rekursiv)  $S_0 = S, S_{n+1} = \tilde{S}_n$  und  $C(S) = \bigcup_{n \in \mathbb{N}_0} S_n \subseteq \mathbb{C}$  Menge aller aus  $S$  konstruierbaren Punkte.

**Beispiel 5.35.** Folgende Konstruktionen sind mit Zirkel und Lineal durchführbar (siehe Schule Klasse 9)

- (a) Die Parallele zu einer Geraden durch einer geg. Punkt
- (b) Die Senkrechte zu einer Geraden durch einer geg. Punkt
- (c) die Mittelpunkt zu 2 geg. Punkten
- (d) Das Spiegelbild eines Punktes an einer Geraden
- (e) Die Summe von Winkeln
- (f) Die Halbierung von Winkeln
- (g) Die Negation von Winkeln

**Lemma 5.36.** Seien  $z, z_1, z_2 \in C(S), S \supseteq \{0, 1\}, z \neq 0$ , dann:

- (a)  $z_1 + z_2 \in C(S)$
- (b)  $-z \in C(S)$
- (c)  $\Re(z), \Im(z), \bar{z} \in C(S)$
- (d)  $|z| \in C(S)$
- (e)  $|z_1| \cdot |z_2|$  und  $z_1 \cdot z_2 \in C(S)$
- (f)  $|z|^{-1}, z^{-1} \in C(S)$
- (g)  $\sqrt{|z|} \in C(S)$
- (h)  $\{\xi \in \mathbb{C} \mid \xi^2 = z\} \subseteq C(S)$  (2 Punkte in  $\mathbb{C}$ )

**Satz 5.37.** Sei  $\bar{S} = \{\bar{z} \mid z \in S\}$ , dann gelten:

$C(S)$  ist ein Unterkörper von  $\mathbb{C}$  der  $C(S \cup \bar{S})$  enthält.

$z \in C(S) \iff \mathbb{Q}(S \cup \bar{S})(z)$  ist eine  $QW$ -Erweiterung von  $\mathbb{Q}(S \cup \bar{S})$

**Korollar 5.38.** Für  $S = \{0, 1\}$  sind äquivalent:

- (a)  $z \in C(S)$
- (b)  $\mathbb{Q}(z)/\mathbb{Q}$  ist eine  $QW$ -Erweiterung von  $\mathbb{Q}$
- (c)  $z$  ist algebraisch über  $\mathbb{Q}$  und der ZK  $E$  von  $\mu_{z,\mathbb{Q}}$  erfüllt  $[E:\mathbb{Q}]$  ist 2-Potenz
- (d)  $z$  ist algebraisch über  $\mathbb{Q}$  und für  $E$  aus (c) gilt  $\text{Gal}(E/\mathbb{Q})$  ist 2-Gruppe

## 5.5 Anwendungen

**Satz 5.39.**  $\pi, \sqrt[3]{2}, \zeta_n = e^{2\pi i/n}$  sind nicht konstruierbar über  $\mathbb{Q}$

**Bemerkung.** Frage D: reguläre  $n$ -Ecke. die eulersche  $\phi$ -Funktion ist die Abbildung:

$$\mathbb{N} \rightarrow \mathbb{N}, n \mapsto \#\mathbb{Z}_n^\times =: \phi(n)$$

**Lemma 5.40.** Sei  $p$  Primzahl,  $k \in \mathbb{N}$ , es gelten:

- (a)  $\phi(p^k) = p^k - p^{k-1} = \phi(p)p^{k-1}$  ( $\phi(p) = p - 1$ )
- (b)  $\phi(mn) = \phi(m)\phi(n)$  sofern  $\text{ggT}(n, m) = 1$
- (c) Für  $n = 2^k p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$  mit Primzahlen  $2 < p_1 < \dots < p_k$  und  $e_i \in \mathbb{N}$  gilt

$$\phi(n) = 2^{k-1}(p_1 - 1) \cdot \dots \cdot (p_k - 1)p_1^{e_1-1} \cdot \dots \cdot p_k^{e_k-1}$$

**Satz 5.41** (Gauß). Sei  $\zeta_n = e^{2\pi i/n}$ , dann sind äquivalent:

- (a) Das reguläre  $n$ -Eck (mit Umkreisradius 1) ist konstruierbar
- (b)  $\zeta_n \in C(\{0, 1\})$
- (c)  $\phi(n)$  ist 2-Potenz
- (d)  $n$  ist von der Form  $2^k p_1 \cdot \dots \cdot p_k$  mit  $p_1 < \dots < p_k$  Fermatprimzahlen

**Definition 5.42.**  $F_\ell = 2^{2^\ell} + 1$  heißt  $\ell$ -te Fermatzahl.

Fermat vermutet:  $F_\ell$  ist eine Primzahl  $\forall \ell \in \mathbb{N}_0$ , falsch! da  $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537, F_5 = 2^{32} + 1 \approx 4$  Milliarden. Nach Euler ist  $641 \mid F_5$ . Inzwischen ist bekannt  $F_5, \dots, F_{11}$  sind keine Primzahlen und für 324 Fermatzahlen bekannt, sie sind nicht Primzahlen. Außer  $F_0$  bis  $F_4$  keine Primzahlen bisher. Neue Vermutung: Das sind alle??