

# Algebra I und II

Prof. Richard Pink

Zusammenfassung  
Herbstsemester 2019  
Frühjahrssemester 2020  
ETH Zürich

vorläufige Version

21. April 2020

Die vorliegende Zusammenfassung enthält die in der Vorlesung behandelten Definitionen und Resultate und wichtigsten Beispiele, jedoch keine Beweise. Diese werden in der Vorlesung an der Tafel entwickelt. Dort werden auch wichtige Erklärungen gegeben, insbesondere zur anschaulichen Bedeutung der Begriffe, zu ihrem jeweiligen Stellenwert, zu möglichen Missverständnissen, zur Beweistechnik, und so weiter. Eine weitere wichtige Voraussetzung, sich das Material anzueignen, ist die aktive Mitarbeit in den begleitenden Übungen und das selbständige Lösen der Übungsreihen. Die darin behandelten Resultate gehören ebenfalls zum Stoff der Vorlesung. Ausserdem empfehle ich die begleitende Lektüre von mindestens einem richtigen Lehrbuch der Algebra. Die Vorlesung baut auf den Vorlesungen Lineare Algebra I+II aus dem Studienjahr 2018–19 auf; für deren Zusammenfassung siehe <http://people.math.ethz.ch/~pink/ftp/LA-Zusammenfassung-20190826.pdf>.

# Inhalt

<b>1</b>	<b>Ringe</b>	<b>4</b>
1.1	Grundbegriffe . . . . .	4
1.2	Einheiten . . . . .	5
1.3	Homomorphismen . . . . .	6
1.4	Unterringe, Produkte . . . . .	7
1.5	Polynomringe . . . . .	8
1.6	Matrizen . . . . .	11
1.7	Integritätsbereiche . . . . .	11
1.8	Quotientenkörper . . . . .	12
1.9	Ideale . . . . .	13
1.10	Faktorringe . . . . .	15
1.11	Primideale . . . . .	16
1.12	Moduln . . . . .	17
<b>2</b>	<b>Teilbarkeit</b>	<b>21</b>
2.1	Irreduzible und Primelemente . . . . .	21
2.2	Faktorielle Ringe . . . . .	22
2.3	Grösster gemeinsamer Teiler . . . . .	23
2.4	Hauptidealringe . . . . .	24
2.5	Euklidische Ringe . . . . .	25
2.6	Polynomringe . . . . .	26
2.7	Irreduzibilitätskriterien . . . . .	27
2.8	Elementarteilersatz . . . . .	28
2.9	Moduln über Hauptidealringen . . . . .	29
2.10	Jordansche Normalform . . . . .	30
<b>3</b>	<b>Gruppen</b>	<b>31</b>
3.1	Grundbegriffe . . . . .	31
3.2	Untergruppen . . . . .	33
3.3	Nebenklassen . . . . .	34
3.4	Ordnung, Index, Exponent . . . . .	35
3.5	Homomorphismen . . . . .	36
3.6	Isomorphismen . . . . .	37
3.7	Abelsche Gruppen . . . . .	37
3.8	Automorphismen . . . . .	38
3.9	Normalteiler . . . . .	39
3.10	Faktorgruppen . . . . .	39
3.11	Operationen . . . . .	40
3.12	Bahnen . . . . .	42
3.13	Eigenschaften von Operationen . . . . .	43
3.14	Symmetrische Gruppe . . . . .	44
3.15	Freie Gruppen . . . . .	46
3.16	Erzeugende und Relationen . . . . .	48

<b>4</b>	<b>Strukturtheorie von Gruppen</b>	<b>49</b>
4.1	Einfache Gruppen . . . . .	49
4.2	Subnormalreihen . . . . .	50
4.3	Kompositionsreihen ( <i>nicht behandelt</i> ) . . . . .	51
4.4	Auflösbare Gruppen . . . . .	52
4.5	Semidirekte Produkte . . . . .	53
4.6	$p$ -Gruppen . . . . .	54
4.7	Sylowsätze . . . . .	55
4.8	Kleine endliche Gruppen . . . . .	55
4.9	Klassifikation . . . . .	56
<b>5</b>	<b>Körper</b>	<b>57</b>
5.1	Körpererweiterungen . . . . .	57
5.2	Körpergrad . . . . .	58
5.3	Einfache Körpererweiterungen . . . . .	59
5.4	Algebraische Körpererweiterungen . . . . .	60
5.5	Konstruktionen mit Zirkel und Lineal . . . . .	61
5.6	Transzendente Körpererweiterungen . . . . .	62
5.7	Homomorphismen zwischen Körpererweiterungen . . . . .	63
5.8	Konstruktion von Körpererweiterungen . . . . .	64
5.9	Algebraischer Abschluss . . . . .	65
5.10	Separable und irreduzible Polynome . . . . .	66
5.11	Perfekte Körper . . . . .	67
5.12	Endliche Körper . . . . .	67
5.13	Separable Körpererweiterungen . . . . .	68
5.14	Inseparable Körpererweiterungen . . . . .	69
5.15	Normale Körpererweiterungen . . . . .	70
<b>6</b>	<b>Galoisttheorie</b>	<b>71</b>
6.1	Galoiserweiterungen . . . . .	71
6.2	Galoiskorrespondenz . . . . .	72
6.3	Symmetrische Funktionen . . . . .	74
6.4	Resultante und Diskriminante . . . . .	75
6.5	Explizite Konstruktion der Zwischenkörper . . . . .	77
6.6	Kreisteilungskörper . . . . .	78
6.7	Abelsche Körpererweiterungen . . . . .	79
6.8	Auflösbare Körpererweiterungen . . . . .	80
6.9	Explizite Bestimmung der Galoisgruppe ( <i>nur zum Teil behandelt</i> ) . . . . .	81
<b>7</b>	<b>Amuse Bouches</b>	<b>82</b>
7.1	$p$ -adische Zahlen ( <i>nicht behandelt</i> ) . . . . .	82
7.2	Topologische Gruppen ( <i>nicht behandelt</i> ) . . . . .	84
7.3	Unendliche Galoiserweiterungen ( <i>nicht behandelt</i> ) . . . . .	85
	<b>Literatur</b>	<b>86</b>

# 1 Ringe

Kommutative unitäre Ringe sowie Moduln über solchen sind Gegenstand des Gebiets der *Kommutativen Algebra*. Wir behandeln einige Grundlagen daraus.

## 1.1 Grundbegriffe

Sei  $R$  eine Menge mit Abbildungen

$$\begin{aligned} + : R \times R &\rightarrow R, & (x, y) &\mapsto x + y, \\ \cdot : R \times R &\rightarrow R, & (x, y) &\mapsto x \cdot y = xy, \end{aligned}$$

und ausgezeichneten Elementen  $0 = 0_R$  sowie  $1 = 1_R \in R$ . Betrachte die Axiome:

- |      |   |                                      |
|------|---|--------------------------------------|
| (1)  | $\forall x, y, z \in R: x + (y + z) = (x + y) + z$  | Assoziativität der Addition          |
| (2)  | $\forall x, y \in R: x + y = y + x$   | Kommutativität der Addition          |
| (3)  | $\forall x \in R: 0 + x = x$  | Neutrales Element der Addition       |
| (4)  | $\forall x \in R \exists x' \in R: x + x' = 0$  | Inverses Element der Addition        |
| (5)  | $\forall x, y, z \in R: x \cdot (y \cdot z) = (x \cdot y) \cdot z$  | Assoziativität der Multiplikation    |
| (6)  | $\forall x, y, z \in R: \left\{ \begin{array}{l} x \cdot (y + z) = x \cdot y + x \cdot z \\ (y + z) \cdot x = y \cdot x + z \cdot x \end{array} \right\}$ | Distributivität                      |
| (7)  | $\forall x, y \in R: x \cdot y = y \cdot x$   | Kommutativität der Multiplikation    |
| (8)  | $\forall x \in R: 1 \cdot x = x = x \cdot 1$  | Neutrales Element der Multiplikation |
| (9)  | $1 \neq 0$  | Nichttrivialität                     |
| (10) | $\forall x \in R \setminus \{0\} \exists x' \in R: x' \cdot x = 1 = x \cdot x'$   | Inverses Element der Multiplikation  |

**Definition:** Ein Tupel  $(R, +, \cdot, 0, 1)$

- (a) mit den Axiomen (1) bis (8) heisst ein *kommutativer unitärer Ring* oder *kommutativer Ring mit Eins*.
- (b) mit den Axiomen (1) bis (10) heisst ein *Körper*.

**Konvention:** Einen kommutativen unitären Ring nennen wir in diesem Abschnitt nur kurz *Ring*. (Aber Vorsicht: Gewisse weitere Begriffe werden beim Fehlen eines Einselementes anders definiert.) Wie üblich schreiben wir nur kurz  $R$  anstelle des ganzen Tupels und sehen die Zusatzdaten als implizit mitgegeben an.

Sei also  $R$  ein Ring.

**Bemerkung:** Die Axiome (1) bis (4) besagen, dass  $(R, +, 0)$  eine abelsche Gruppe ist, genannt die *additive Gruppe von  $R$* . Insbesondere ist das inverse Element  $-x$  von  $x$  bezüglich der Addition eindeutig bestimmt. Für  $x + (-y)$  schreibt man auch kürzer  $x - y$ . Für jede ganze Zahl  $n$  ist das  *$n$ -te Vielfache von  $x$*  definiert durch

$$n \cdot x := \begin{cases} x + \dots + x & \text{mit } n \text{ Summanden} & \text{falls } n > 0, \\ 0 & & \text{falls } n = 0, \\ -(x + \dots + x) & \text{mit } |n| \text{ Summanden} & \text{falls } n < 0. \end{cases}$$

**Rechenregeln:** Für alle  $x, y \in R$  und alle  $m, n \in \mathbb{Z}$  gilt:

$$\begin{aligned}(\pm n) \cdot x &= \pm(n \cdot x) \\(m \pm n) \cdot x &= m \cdot x \pm n \cdot x \\m \cdot (x \pm y) &= m \cdot x \pm m \cdot y \\(m \cdot n) \cdot x &= m \cdot (n \cdot x) \\m \cdot (x \cdot y) &= (m \cdot x) \cdot y\end{aligned}$$

**Bemerkung:** Für jede ganze Zahl  $n \geq 0$  ist die  $n$ -te Potenz von  $x$  definiert durch

$$x^n := \begin{cases} x \cdots x & \text{mit } n \text{ Faktoren} & \text{falls } n > 0, \\ 1 & & \text{falls } n = 0. \end{cases}$$

**Rechenregeln:** Für alle  $x, y \in R$  und alle  $m, n \geq 0$  gilt:

$$\begin{aligned}x^{m+n} &= x^m \cdot x^n \\(x \cdot y)^m &= x^m \cdot y^m \\x^{m \cdot n} &= (x^m)^n\end{aligned}$$

**Bemerkung:** Für Summen  $\sum_{i \in I} x_i$  und Produkte  $\prod_{i \in I} x_i$  in einem Ring gelten die gleichen Konventionen und Grundregeln wie in einem Körper.

**Proposition:** Es ist  $1 = 0$  genau dann, wenn der Ring der Nullring ist.

## 1.2 Einheiten

**Definition:** Ein Element  $x \in R$  mit der Eigenschaft

$$\exists x' \in R: x' \cdot x = 1$$

heißt *invertierbar* oder eine *Einheit* von  $R$ . Die Menge aller Einheiten von  $R$  bezeichnen wir mit  $R^\times$  (sprich „ $R$  Kreuz“) oder auch  $R^*$ .

**Proposition:** Die Menge  $R^\times$  ist bezüglich Multiplikation eine abelsche Gruppe, genannt die *Einheitengruppe* von  $R$ .

Insbesondere ist das inverse Element  $x'$  jeder Einheit  $x$  eindeutig bestimmt. Es wird bezeichnet mit  $x^{-1}$  oder  $\frac{1}{x}$ . Für  $\frac{1}{x} \cdot y$  schreibt man auch  $\frac{y}{x}$ . Weiter ist jedes Produkt und jeder Quotient von Einheiten eine Einheit, und das Einselement 1 ist eine Einheit. Für jede Einheit  $x$  und jede natürliche Zahl  $n$  definieren wir  $x^{-n} := (x^{-1})^n$ , mit denselben Rechenregeln wie oben.

**Beispiel:** Für jeden Körper  $K$  ist  $K^\times = K \setminus \{0\}$ .

**Beispiel:** Es ist  $\mathbb{Z}^\times = \{\pm 1\}$ .

### 1.3 Homomorphismen

Betrachte zwei Ringe  $R$  und  $S$ .

**Definition:** Ein (*Ring*)-*Homomorphismus*  $\varphi: R \rightarrow S$  ist eine Abbildung mit

- (a)  $\varphi(1_R) = 1_S$ .
- (b)  $\forall x, y \in R: \varphi(x + y) = \varphi(x) + \varphi(y)$ .
- (c)  $\forall x, y \in R: \varphi(xy) = \varphi(x)\varphi(y)$ .

**Proposition:** Für jeden Homomorphismus  $\varphi: R \rightarrow S$  gilt:

- (a)  $\varphi(0_R) = 0_S$ .
- (b)  $\forall x \in R \forall n \in \mathbb{Z}: \varphi(nx) = n\varphi(x)$ .
- (c)  $\forall x \in R \forall n \in \mathbb{Z}^{\geq 0}: \varphi(x^n) = \varphi(x)^n$ .
- (d)  $\varphi$  induziert einen Gruppenhomomorphismus  $R^\times \rightarrow S^\times$ .

**Proposition:** Die Identität  $\text{id}_R: R \rightarrow R$  ist ein Homomorphismus. Die Komposition zweier Homomorphismen ist ein Homomorphismus.

**Proposition:** Jeder Homomorphismus zwischen zwei Körpern ist injektiv.

**Beispiel:** Für jeden Ring  $R$  existiert genau ein Ringhomomorphismus  $\mathbb{Z} \rightarrow R$ , nämlich die Abbildung  $n \mapsto n \cdot 1_R$ .

**Definition:** Ein Homomorphismus  $\varphi: R \rightarrow S$  mit einem beidseitigem Inversen  $\varphi^{-1}$  heisst ein *Isomorphismus*, und wir schreiben dann  $\varphi: R \xrightarrow{\sim} S$ . Existiert ein Isomorphismus  $R \xrightarrow{\sim} S$ , so heissen  $R$  und  $S$  *isomorph* und wir schreiben  $R \cong S$ .

**Proposition:** Ein Ringhomomorphismus ist ein Isomorphismus genau dann, wenn er bijektiv ist.

**Proposition:** Die Komposition zweier Isomorphismen ist ein Isomorphismus. Das Inverse eines Isomorphismus ist eindeutig bestimmt und selbst ein Isomorphismus. Isomorphie von Ringen ist eine Äquivalenzrelation.

**Definition:** Ein Isomorphismus  $R \xrightarrow{\sim} R$  heisst ein *Automorphismus von  $R$* .

## 1.4 Unterringe, Produkte

**Definition:** Ein *Unterring von  $R$*  ist eine Teilmenge  $R' \subset R$  mit den Eigenschaften:

- (a)  $\forall x, y \in R': x + y \in R'$ .
- (b)  $\forall x, y \in R': xy \in R'$ .
- (c)  $\forall x \in R': -x \in R'$ .
- (d)  $1 \in R'$ .

Die Teilmenge  $R'$  bildet dann zusammen mit den Restriktion der Operationen von  $R$  selbst einen Ring, und die Inklusionsabbildung  $R' \hookrightarrow R$  einen Ringhomomorphismus.

**Beispiel:**  $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ .

**Proposition:** Der Durchschnitt jeder nichtleeren Kollektion von Unterringen von  $R$  ist ein Unterring von  $R$ .

**Proposition:** Für jeden Unterring  $R' \subset R$  und jede Teilmenge  $A \subset R$  existiert ein eindeutiger kleinster Unterring von  $R$ , welcher  $R'$  und  $A$  enthält. Dieser besteht aus den Elementen der Form

$$\sum_{i_1, \dots, i_n \geq 0} x_{i_1, \dots, i_n} a_1^{i_1} \cdots a_n^{i_n}$$

für alle  $n \geq 0$  und  $a_1, \dots, a_n \in A$  und  $x_{i_1, \dots, i_n} \in R'$ , fast alle gleich 0.

**Definition:** Dieser Unterring heisst *der von  $A$  über  $R'$  erzeugte Unterring* und wird bezeichnet mit  $R'[A]$ . Für endlich viele Elemente  $a_1, \dots, a_n \in R$  schreiben wir auch  $R'[a_1, \dots, a_n] := R'[\{a_1, \dots, a_n\}]$ .

**Beispiel:** Der Unterring  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$  von  $\mathbb{C}$ .

**Beispiel:** Es ist  $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ .

**Beispiel:** Der Unterring  $\mathbb{Z}[\sqrt{7}] = \{a + b\sqrt{7} \mid a, b \in \mathbb{Z}\}$  von  $\mathbb{R}$ .

**Beispiel:** Es ist  $\mathbb{Z}[\sqrt{7}]^\times = \{\pm(8 + 3\sqrt{7})^n \mid n \in \mathbb{Z}\}$ .

**Beispiel:** Der Unterring  $\mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{Z}^{\geq 0}\}$  von  $\mathbb{Q}$ .

**Beispiel:** Es ist  $\mathbb{Z}[\frac{1}{2}]^\times = \{\pm 2^n \mid n \in \mathbb{Z}\}$ .

**Proposition-Definition:** Das *kartesische Produkt* von Ringen  $R_1 \times \dots \times R_n$  mit komponentenweiser Addition und Multiplikation sowie dem Nullelement  $(0, \dots, 0)$  und dem Einselement  $(1, \dots, 1)$  ist ein Ring. Für diesen gilt weiter  $(R_1 \times \dots \times R_n)^\times = R_1^\times \times \dots \times R_n^\times$  und darin  $(x_1, \dots, x_n)^{-1} = (x_1^{-1}, \dots, x_n^{-1})$ .

**Proposition-Definition:** Für jeden Ring  $R$  und jede Menge  $X$  ist die Menge  $R^X$  aller Funktionen  $f: X \rightarrow R$  mit punktweiser Addition  $(f + g)(x) = f(x) + g(x)$  und Multiplikation  $(f \cdot g)(x) = f(x) \cdot g(x)$  sowie den konstanten Funktionen 0 als Nullelement und 1 als Einselement ein Ring.

**Bemerkung:** Für  $R^n = R \times \dots \times R = R^{\{1, \dots, n\}}$  stimmen beide Konstruktionen überein.

**Bemerkung:** Viele interessante Ringe sind Unterringe von Funktionenringen, zum Beispiel die Ringe aller stetigen oder differenzierbaren oder holomorphen Funktionen auf Teilmengen von  $\mathbb{R}$  oder  $\mathbb{R}^d$  oder  $\mathbb{C}$ .

## 1.5 Polynomringe

**Konstruktion:** Seien  $R$  ein Ring und  $n$  eine natürliche Zahl. Sei  $I_n$  die Menge aller Tupel  $\underline{i} = (i_1, \dots, i_n)$  in  $\mathbb{Z}^{\geq 0}$ . Betrachte die Menge

$$R_n := \{(a_{\underline{i}})_{\underline{i} \in I_n} \mid \text{alle } a_{\underline{i}} \in R \text{ und fast alle } a_{\underline{i}} = 0\}.$$

Für zwei Elemente von  $R_n$  definieren wir

$$\begin{aligned} (a_{\underline{i}})_{\underline{i}} + (b_{\underline{i}})_{\underline{i}} &:= (a_{\underline{i}} + b_{\underline{i}})_{\underline{i}} \\ (a_{\underline{i}})_{\underline{i}} \cdot (b_{\underline{i}})_{\underline{i}} &:= \left( \sum_{\underline{i} + \underline{j} = \underline{k}} a_{\underline{i}} \cdot b_{\underline{j}} \right)_{\underline{k}} \end{aligned}$$

Betrachte weiter die Abbildung

$$\iota: R \rightarrow R_n, a \mapsto \left( \begin{cases} a & \text{falls } \underline{i} = (0, \dots, 0), \\ 0 & \text{sonst,} \end{cases} \right)_{\underline{i}}$$

und bezeichne  $0 := \iota(0)$  und  $1 := \iota(1)$ . Für jedes  $1 \leq \nu \leq n$  sei

$$X_{\nu} := \left( \begin{cases} 1 & \text{falls } \underline{i} = (0, \dots, 0, \underset{\nu}{1}, 0, \dots, 0), \\ 0 & \text{sonst,} \end{cases} \right)_{\underline{i}} \in R_n.$$

Für jedes  $\underline{i} \in I_n$  kürzen wir ab

$$\underline{X}^{\underline{i}} := \prod_{\nu=1}^n X_{\nu}^{i_{\nu}}.$$

Für alle  $\underline{i}, \underline{j} \in I_n$  gilt dann

$$\underline{X}^{\underline{i}} \cdot \underline{X}^{\underline{j}} = \underline{X}^{\underline{i} + \underline{j}}.$$

**Proposition:** (a)  $(R_n, +, \cdot, 0, 1)$  ist ein Ring.

(b)  $\iota$  ist ein injektiver Ringhomomorphismus. Wir identifizieren  $R$  mit seinem Bild.

(c) Für jedes Element von  $R_n$  gilt

$$(a_{\underline{i}})_{\underline{i}} = \sum'_{\underline{i} \in I_n} a_{\underline{i}} \underline{X}^{\underline{i}}.$$

(d) Jedes Element von  $R_n$  hat eine eindeutige Darstellung der Form  $\sum'_{\underline{i} \in I_n} a_{\underline{i}} \underline{X}^{\underline{i}}$ .



Daher können wir die Elemente von  $R_n$  mit allen „formalen Ausdrücken“ der Form  $\sum'_{i \in I_n} a_i \underline{X}^i$  identifizieren, und zwei solche Elemente sind genau dann gleich, wenn ihre Koeffizienten  $a_i$  übereinstimmen. Diese Ausdrücke gehorchen den üblichen Rechenregeln in einem Ring. Einen solchen Ausdruck nennen wir ein *Polynom über  $R$* . Ein Polynom der speziellen Form  $a\underline{X}^i$  mit  $a \in R$  heisst ein *Monom*. Je nach Zusammenhang wählt man andere Symbole anstatt  $X_\nu$ ; die aber noch nicht belegt sein dürfen. Das System dieser „neuen Variablen“ kürzt man oft mit  $\underline{X} = (X_1, \dots, X_n)$  ab und schreibt den *Polynomring in den Variablen  $X_1, \dots, X_n$  über  $R$*  als

$$R[\underline{X}] := R[X_1, \dots, X_n] := R_n.$$

**Bemerkung:** Der Polynomring ist tatsächlich von den Elementen  $X_1, \dots, X_n$  über  $R$  erzeugt; somit ist die Notation  $R[X_1, \dots, X_n]$  mit der aus §1.4 verträglich.

**Proposition:** (*Universelle Eigenschaft*) Für jeden Ring  $S$ , jeden Ringhomomorphismus  $\varphi: R \rightarrow S$ , und jedes System  $\underline{x} = (x_\nu)_\nu \in S^n$  existiert genau ein Ringhomomorphismus  $\varphi_{\underline{x}}: R[\underline{X}] \rightarrow S$  mit  $\varphi_{\underline{x}} \circ \iota = \varphi$  und  $\varphi_{\underline{x}}(X_\nu) = x_\nu$  für alle  $1 \leq \nu \leq n$ , das heisst, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \ni x_\nu \\ & \searrow \iota & \nearrow \varphi_{\underline{x}} \\ & R[\underline{X}] \ni X_\nu & \end{array}$$

Genauer ist  $\varphi_{\underline{x}}$  die *Auswertungsabbildung*

$$R[\underline{X}] \rightarrow S, F(\underline{X}) = \sum'_{i \in I_n} a_i \underline{X}^i \mapsto F(\underline{x}) := \sum'_{i \in I_n} \varphi(a_i) \underline{x}^i.$$

Wir nennen  $F(\underline{x})$  den *Wert von  $F$  an der Stelle  $\underline{x}$* . Jedes Polynom  $F$  induziert somit für jedes  $\varphi: R \rightarrow S$  eine *Polynomfunktion*

$$S^n \rightarrow S, \underline{x} \mapsto F(\underline{x}).$$

**Vorsicht:** Ist  $R$  endlich, so können verschiedene Polynome über  $R$  dieselbe Polynomfunktion  $R \rightarrow R$  induzieren, z.B. die beiden Polynome  $0$  und  $X^2 - X$  über  $\mathbb{F}_2$ . Ein Polynom ist also etwas grundsätzlich Anderes als eine Polynomfunktion. Dagegen gilt:

**Proposition:** Sei  $K$  ein unendlicher Körper. Dann ist jedes Polynom über  $K$  durch die induzierte Polynomfunktion  $K^n \rightarrow K$  eindeutig bestimmt.

**Bemerkung:** Alternativ könnte man  $R[\underline{X}]$  durch die universelle Eigenschaft abstrakt definieren und zeigen, dass er dadurch bis auf eindeutige Isomorphie bestimmt ist.

**Proposition:** Für alle  $0 \leq m \leq n$  existiert ein natürlicher Isomorphismus

$$R[X_1, \dots, X_n] \cong R[X_1, \dots, X_m][X_{m+1}, \dots, X_n].$$

**Proposition:** (*Funktorialität*) Jeder Ringhomomorphismus  $\varphi: R \rightarrow S$  induziert einen eindeutigen Ringhomomorphismus  $\tilde{\varphi}: R[\underline{X}] \rightarrow S[\underline{X}]$  mit  $\tilde{\varphi}|_R = \varphi$  und  $\tilde{\varphi}(X_\nu) = X_\nu$ , nämlich

$$\sum'_{i \in I_n} a_i \underline{X}^i \mapsto \sum'_{i \in I_n} \varphi(a_i) \underline{X}^i.$$

**Proposition:** Seien  $K$  ein Körper und  $V$  ein  $K$ -Vektorraum mit Basis  $\underline{X} = (X_\nu)_{\nu=1}^n$ . Dann existiert ein natürlicher Isomorphismus auf die symmetrische Algebra

$$K[\underline{X}] \xrightarrow{\sim} SV := \bigoplus_{r \geq 0} S^r V, \quad \sum'_{i \in I_n} a_i \underline{X}^i \mapsto \sum'_{i \in I_n} a_i \underline{X}^i.$$

**Variante:** Für  $\underline{X} = (X_1, \dots, X_n)$  sei  $R[[\underline{X}]]$  die Menge aller Abbildungen  $(\mathbb{Z}^{\geq 0})^n \rightarrow R$ ,  $\underline{i} \mapsto a_i$ , ohne Endlichkeitsbedingungen. Definiere Summe und Produkt zweier Elemente von  $R[[\underline{X}]]$  sowie die Inklusion  $\iota: R \hookrightarrow R[[\underline{X}]]$  durch die gleichen Formeln wie oben.

**Proposition:**  $(R[[\underline{X}]], +, \cdot, 0, 1)$  ist ein Ring und  $\iota$  ein injektiver Ringhomomorphismus.

Wieder identifizieren wir  $R$  mit seinem Bild unter  $\iota$ . Ein Element von  $R[[\underline{X}]]$  schreiben wir in der Form

$$(a_i)_{\underline{i}} = \sum_{\underline{i} \in I_n} a_i \underline{X}^i,$$

was aber nur als Notation und nicht als irgendeine Art von unendlicher Summe oder Reihe zu verstehen ist. Einen solchen Ausdruck nennen wir eine *formale Potenzreihe in den Variablen  $X_1, \dots, X_n$  über  $R$* . Mit dieser Notation unterliegen alle Rechnungen denselben Regeln wie für Potenzreihen in der Analysis.

**Bemerkung:** Wir haben natürliche Einbettungen  $R \subset R[\underline{X}] \subset R[[\underline{X}]]$ .

**Variante:** Sei  $N$  eine beliebige, möglicherweise unendliche, Menge. Dann konstruieren wir den *Polynomring  $R[\underline{X}]$  über  $R$  in den Variablen  $X_\nu$  für alle  $\nu \in N$*  wie folgt.

Sei  $I_N$  die Menge aller Abbildungen  $\underline{i}: N \rightarrow \mathbb{Z}^{\geq 0}$ ,  $\nu \mapsto i_\nu$  mit endlichem Träger, das heißt, mit  $i_\nu = 0$  für fast alle  $\nu$ . Sei  $R[\underline{X}]$  die Menge aller Abbildungen  $I_N \rightarrow R$ ,  $\underline{i} \mapsto a_{\underline{i}}$  mit endlichem Träger, das heißt, mit  $a_{\underline{i}} = 0$  für fast alle  $\underline{i} \in I_N$ . Die Summe und das Produkt zweier Elemente von  $R[\underline{X}]$ , sowie die Abbildung  $\iota: R \rightarrow R[\underline{X}]$ , die Elemente  $0, 1 \in R[\underline{X}]$  und die Elemente  $X_\nu \in R[\underline{X}]$  für alle  $\nu \in N$  sind definiert wie oben. Dann ist wieder  $(R[\underline{X}], +, \cdot, 0, 1)$  ein Ring und  $\iota$  ein injektiver Ringhomomorphismus, und jedes Element von  $R[\underline{X}]$  ist eine endliche Summe

$$(a_{\underline{i}})_{\underline{i}} = \sum'_{\underline{i} \in I_N} a_{\underline{i}} \underline{X}^i$$

mit eindeutigen Koeffizienten  $a_{\underline{i}} \in R$ .

## 1.6 Matrizen

Für alle natürlichen Zahlen  $m, n$  bezeichnet  $\text{Mat}_{m \times n}(R)$  die Menge aller  $m \times n$ -Matrizen mit Koeffizienten in  $R$ . Summe und Produkt von Matrizen über  $R$  sind durch dieselben Formeln definiert wie über einem Körper.

**Meta-Proposition:** Jede Rechenregel für Matrizen und Skalare über  $\mathbb{Q}$ , die nur die Operationen  $+$  und  $-$  und  $\cdot$  sowie die Konstanten  $0$  und  $1$  beinhaltet, gilt auch für Matrizen und Skalare über einem beliebigen Ring.

**Beispiel:** Für alle Matrizen passender Grössen über einem beliebigen Ring gilt:

- (a)  $A(BC) = (AB)C$ .
- (b)  $I_m A = A I_n = A$ .
- (c)  $\det(AB) = \det(A) \det(B)$ .
- (d)  $A\tilde{A} = \tilde{A}A = \det(A) \cdot I_n$  für die Adjunkte  $\tilde{A} := ((-1)^{i+j} \cdot \det(A_{ji}))_{i,j}$  von  $A$ .
- (e)  $\text{char}_A(A) = 0$  für das charakteristische Polynom  $\text{char}_A(X) := \det(X \cdot I_n - A)$ .

**Proposition-Definition:** Für jede Matrix  $A \in \text{Mat}_{n \times n}(R)$  sind äquivalent:

- (a) Es existiert  $A' \in \text{Mat}_{n \times n}(R)$  mit  $AA' = A'A = I_n$ . Dann heisst  $A$  *invertierbar*.
- (b) Es existiert  $A' \in \text{Mat}_{n \times n}(R)$  mit  $AA' = I_n$ .
- (c) Es existiert  $A' \in \text{Mat}_{n \times n}(R)$  mit  $A'A = I_n$ .
- (d)  $\det(A) \in R^\times$ .

Die Matrix  $A'$  ist durch (b) oder (c) eindeutig bestimmt und heisst die *Inverse*  $A^{-1}$ .

**Proposition-Definition:** Die Menge  $\text{GL}_n(R)$  aller invertierbaren  $n \times n$ -Matrizen über  $R$  ist eine Gruppe mit der Matrixmultiplikation und dem neutralen Element  $I_n$ . Sie heisst die *allgemeine lineare Gruppe vom Grad  $n$  über  $R$* .

## 1.7 Integritätsbereiche

**Definition:** Ein *Nullteiler* von  $R$  ist ein Element  $x \in R \setminus \{0\}$  mit

$$\exists y \in R \setminus \{0\}: xy = 0.$$

**Definition:** Ein Ring mit  $1 \neq 0$  und ohne Nullteiler heisst ein *Integritätsbereich*.

**Äquivalent:** Für alle  $n \geq 0$  und  $a_i \in R \setminus \{0\}$  für  $1 \leq i \leq n$  ist  $\prod_{i=1}^n a_i \neq 0$ .

**Proposition:** In jedem Integritätsbereich gilt die *Kürzungsregel*:

$$\forall x, y, z \in R: (x \neq 0 \text{ und } xy = xz) \longrightarrow y = z.$$

**Beispiel:** Jeder Körper ist ein Integritätsbereich.

**Beispiel:** Jeder Unterring eines Integritätsbereichs ist ein Integritätsbereich.

**Proposition:** Für jeden Integritätsbereich  $R$  ist auch  $R[\underline{X}]$  und  $R[[\underline{X}]]$  ein Integritätsbereich.

## 1.8 Quotientenkörper

Sei  $R$  ein Integritätsbereich.

**Konstruktion-Proposition:** Auf der Menge der Paare  $R \times (R \setminus \{0\})$  ist durch

$$(x, y) \sim (x', y') : \iff xy' = x'y.$$

eine Äquivalenzrelation definiert. Bezeichne die Äquivalenzklasse eines Paares  $(x, y)$  mit  $[(x, y)]$  und die Menge aller Äquivalenzklassen mit  $\text{Quot}(R)$ . Dann sind die Operationen

$$\begin{aligned} [(x, y)] + [(x', y')] &:= [(xy' + x'y, yy')] \\ [(x, y)] \cdot [(x', y')] &:= [(xx', yy')] \end{aligned}$$

wohldefiniert auf  $\text{Quot}(R)$ . Betrachte weiter die Abbildung

$$\iota: R \rightarrow \text{Quot}(R), \quad x \mapsto [(x, 1)]$$

und bezeichne  $0 := \iota(0)$  und  $1 := \iota(1)$ . Dann ist  $(\text{Quot}(R), +, \cdot, 0, 1)$  ein Körper und  $\iota$  ein injektiver Ringhomomorphismus.

**Definition:** Der Körper  $\text{Quot}(R)$  heisst der *Quotientenkörper von  $R$* . Wir identifizieren  $R$  mit seinem Bild unter  $\iota$ . In  $\text{Quot}(R)$  gilt dann

$$[(x, y)] = \frac{\iota(x)}{\iota(y)} = \frac{x}{y}.$$

**Proposition:** (*Universelle Eigenschaft*) Für jeden injektiven Ringhomomorphismus  $\varphi: R \rightarrow K$  in einen Körper  $K$  existiert genau ein Körperhomomorphismus  $\tilde{\varphi}: \text{Quot}(R) \rightarrow K$  mit  $\tilde{\varphi} \circ \iota = \varphi$ , das heisst, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & K \\ & \searrow \iota & \nearrow \tilde{\varphi} \\ & \text{Quot}(R) & \end{array}$$

**Bemerkung:** Man könnte den Quotientenkörper auch durch die universelle Eigenschaft abstrakt definieren und zeigen, dass er durch diese bis auf eindeutige Isomorphie bestimmt ist.

**Folge:** (*Funktorialität*) Jeder injektive (und nur jeder solche) Ringhomomorphismus von Integritätsbereichen  $\varphi: R \rightarrow S$  setzt sich fort zu einem eindeutigen Ringhomomorphismus  $\tilde{\varphi}: \text{Quot}(R) \rightarrow \text{Quot}(S)$ .

**Beispiel:** Der Körper der rationalen Zahlen  $\mathbb{Q} = \text{Quot}(\mathbb{Z})$ .

**Beispiel:** Es ist  $\text{Quot}(\mathbb{Z}[i]) \cong \mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$ .

**Definition:** Für jeden Körper  $K$  heisst  $K(X_1, \dots, X_n) := \text{Quot}(K[X_1, \dots, X_n])$  der Körper der *rationalen Funktionen in den Variablen  $X_1, \dots, X_n$  über  $K$* .

**Beispiel:** In der Funktionentheorie definiert man den Körper der meromorphen Funktionen auf einer zusammenhängenden offenen Teilmenge  $U \subset \mathbb{C}$ . Dieser stellt sich heraus als der Quotientenkörper des Unterrings der holomorphen Funktionen.

## 1.9 Ideale

Sei  $R$  ein Ring.

**Definition:** Ein *Ideal von  $R$*  ist eine Teilmenge  $\mathfrak{a} \subset R$  mit den Eigenschaften:

- (a)  $\mathfrak{a} \neq \emptyset$ .
- (b)  $\forall a, b \in \mathfrak{a}: a + b \in \mathfrak{a}$ .
- (c)  $\forall x \in R \forall a \in \mathfrak{a}: xa \in \mathfrak{a}$ .

Wegen (c) gilt dann auch  $\forall a \in \mathfrak{a}: -a \in \mathfrak{a}$ ; wegen (a) und (b) ist das Ideal also eine additive Untergruppe von  $R$ . Die Bedingungen bedeuten auch, dass für alle  $n \geq 0$ , alle  $x_i \in R$ , und alle  $a_i \in \mathfrak{a}$  auch  $\sum_{i=1}^n x_i a_i \in \mathfrak{a}$  ist.

**Proposition-Definition:** Für jedes Element  $a \in R$  ist

$$(a) := \{xa \mid x \in R\}$$

ein Ideal von  $R$ , genannt das *von  $a$  erzeugte Hauptideal*.

**Beispiel:** Das *Nullideal*  $(0) = \{0\}$ .

**Beispiel:** Das *Einsideal*  $(1) = R$ .

**Proposition:** (a) Es ist  $(a) = (1)$  genau dann, wenn  $a$  eine Einheit von  $R$  ist.

(b) Ein Ideal  $\mathfrak{a}$  ist gleich  $(1)$  genau dann, wenn es das Einselement enthält.

**Proposition:** Für alle Elemente  $a, b$  eines Integritätsbereichs  $R$  gilt

$$a|b \iff (a) \ni b \iff (a) \supset (b).$$

**Proposition:** Der Durchschnitt jeder nichtleeren Kollektion von Idealen ist ein Ideal.

**Proposition-Definition:** Die Summe jeder Kollektion von Idealen  $\{\mathfrak{a}_\nu \mid \nu \in N\}$  ist ein Ideal:

$$\sum_{\nu \in N} \mathfrak{a}_\nu := \left\{ \sum_{\nu \in N}' a_\nu \mid \begin{array}{l} \text{alle } a_\nu \in \mathfrak{a}_\nu, \\ \text{fast alle } a_\nu = 0 \end{array} \right\}.$$

**Proposition-Definition:** Für jede Teilmenge  $A \subset R$  ist die folgende Menge ein Ideal:

$$(A) := \left\{ \sum_{a \in A}' x_a a \mid \begin{array}{l} \text{alle } x_a \in R, \\ \text{fast alle } x_a = 0 \end{array} \right\} = \sum_{a \in A} (a),$$

genannt *von  $A$  erzeugt*. Für endlich viele Elemente  $a_1, \dots, a_n \in R$  schreiben wir auch

$$(a_1, \dots, a_n) := (\{a_1, \dots, a_n\}) = (a_1) + \dots + (a_n)$$

und hoffen auf möglichst wenig Verwechslung mit dem Tupel  $(a_1, \dots, a_n)$ .

**Proposition:** Das Ideal  $(A)$  ist das eindeutige kleinste Ideal  $\mathfrak{a} \subset R$  mit  $(A) \subset \mathfrak{a}$ .

**Bemerkung:** Jeder gemeinsame Teiler von Elementen  $a_1, \dots, a_n$  ist ein gemeinsamer Teiler aller Elemente des Ideals  $(a_1, \dots, a_n)$ . Der Begriff des Ideals enthält also alle Informationen über Teilbarkeit, auch wenn der Ring nicht faktoriell ist. Genau zu diesem Zweck hat Dedekind den Begriff des Ideals erfunden, um seine Vorstellung von *idealen Zahlen* zu konkretisieren.

**Proposition:** Für jedes  $x \in R$  und jedes Ideal  $\mathfrak{a}$  ist die folgende Menge ein Ideal

$$x\mathfrak{a} := x \cdot \mathfrak{a} := \{xa \mid a \in \mathfrak{a}\}.$$

**Definition:** Das *Produkt* zweier Ideale  $\mathfrak{a}, \mathfrak{b}$  von  $R$  ist das von den Elementen  $ab$  für alle  $a \in \mathfrak{a}$  und  $b \in \mathfrak{b}$  erzeugte Ideal

$$\mathfrak{a}\mathfrak{b} := \mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{i=1}^n a_i b_i \mid \text{alle } n \geq 0, a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

**Definition:** Die *n-te Potenz* eines Ideals  $\mathfrak{a}$  ist definiert durch

$$\mathfrak{a}^n := \begin{cases} \mathfrak{a} \cdots \mathfrak{a} & \text{mit } n \text{ Faktoren falls } n > 0, \\ R & \text{falls } n = 0. \end{cases}$$

**Proposition:** Für alle  $x, y \in R$ , alle Ideale  $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ , und alle  $m, n \in \mathbb{Z}^{\geq 0}$  gilt

$$\begin{aligned} (x)\mathfrak{a} &= x\mathfrak{a} \\ (x)(y) &= (xy) \\ \mathfrak{a}\mathfrak{b} &= \mathfrak{b}\mathfrak{a} \\ \mathfrak{a}(\mathfrak{b} + \mathfrak{c}) &= \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c} \\ x(\mathfrak{a} + \mathfrak{b}) &= x\mathfrak{a} + x\mathfrak{b} \\ \mathfrak{a}(\mathfrak{b}\mathfrak{c}) &= (\mathfrak{a}\mathfrak{b})\mathfrak{c} \\ x(\mathfrak{a}\mathfrak{b}) &= (x\mathfrak{a})\mathfrak{b} \\ x(y\mathfrak{a}) &= (xy)\mathfrak{a} \\ (x)^n &= (x^n) \\ \mathfrak{a}^m \mathfrak{a}^n &= \mathfrak{a}^{m+n} \\ \mathfrak{a}^n \mathfrak{b}^n &= (\mathfrak{a}\mathfrak{b})^n \end{aligned}$$

**Proposition:** Für jeden Ringhomomorphismus  $\varphi: R \rightarrow S$  ist

$$\begin{aligned} \text{Kern}(\varphi) &:= \{a \in R \mid \varphi(a) = 0\} && \text{ein Ideal von } R, \text{ und} \\ \text{Bild}(\varphi) &:= \{\varphi(a) \mid a \in R\} && \text{ein Unterring von } S. \end{aligned}$$

Dabei ist  $\text{Kern}(\varphi) = (0)$  genau dann, wenn  $\varphi$  injektiv ist, und  $\text{Bild}(\varphi) = S$  genau dann, wenn  $\varphi$  surjektiv ist,

## 1.10 Faktorringe

Sei  $\mathfrak{a}$  ein Ideal von  $R$ . Für jedes  $x \in R$  heisst die Teilmenge

$$x + \mathfrak{a} := \{x + a \mid a \in \mathfrak{a}\} \subset R$$

eine *Nebenklasse* von  $\mathfrak{a}$ . Betrachte die Menge aller Nebenklassen

$$R/\mathfrak{a} := \{x + \mathfrak{a} \mid x \in R\}.$$

**Proposition:** Je zwei Nebenklassen  $x + \mathfrak{a}$  sind entweder gleich oder disjunkt, und die Vereinigung aller ist  $R$ . Genauer gilt für alle  $x, x' \in R$ :

$$x + \mathfrak{a} = x' + \mathfrak{a} \iff x \in x' + \mathfrak{a} \iff x' \in x + \mathfrak{a} \iff (x + \mathfrak{a}) \cap (x' + \mathfrak{a}) \neq \emptyset.$$

**Proposition:** Die Menge  $R/\mathfrak{a}$  besitzt eine eindeutige Ringstruktur, so dass gilt:

$$(a) \quad \forall x, y \in R : (x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}.$$

$$(b) \quad \forall x, y \in R : (x + \mathfrak{a}) \cdot (y + \mathfrak{a}) = xy + \mathfrak{a}.$$

Für diese gilt weiter:

$$(c) \quad \text{Das Nullelement von } R/\mathfrak{a} \text{ ist } 0 + \mathfrak{a} = \mathfrak{a}.$$

$$(d) \quad \text{Das Einselement von } R/\mathfrak{a} \text{ ist } 1 + \mathfrak{a}.$$

$$(e) \quad \text{Das additive Inverse von } x + \mathfrak{a} \text{ ist } (-x) + \mathfrak{a}.$$

$$(f) \quad \pi : R \rightarrow R/\mathfrak{a}, x \mapsto x + \mathfrak{a} \text{ ist ein surjektiver Ringhomomorphismus mit Kern } \mathfrak{a}.$$

**Definition:** Der Ring  $R/\mathfrak{a}$  heisst der *Faktorring* von  $R$  nach  $\mathfrak{a}$ .

**Beispiel:** (a) Es ist  $\mathfrak{a} = R$  genau dann, wenn  $R/\mathfrak{a}$  der Nullring ist.

(b) Es ist  $\mathfrak{a} = 0$  genau dann, wenn  $\pi$  ein Isomorphismus ist.

**Proposition:** (*Universelle Eigenschaft*) Für jeden Ring  $S$  und jeden Ringhomomorphismus  $\varphi : R \rightarrow S$  mit  $\mathfrak{a} \subset \text{Kern}(\varphi)$  existiert genau ein Ringhomomorphismus  $\bar{\varphi} : R/\mathfrak{a} \rightarrow S$  mit  $\bar{\varphi} \circ \pi = \varphi$ , das heisst, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ & \searrow \pi & \nearrow \bar{\varphi} \\ & R/\mathfrak{a} & \end{array}$$

**Proposition:** (*Homomorphiesatz*) Jeder Ringhomomorphismus  $\varphi : R \rightarrow S$  induziert einen Isomorphismus

$$R/\text{Kern}(\varphi) \xrightarrow{\sim} \text{Bild}(\varphi).$$

**Beispiel:** Es ist  $\mathbb{R}[X]/(X^2 + 1) \xrightarrow{\sim} \mathbb{C}$ .

**Beispiel:** Für jede ganze Zahl  $d$ , die kein Quadrat ist, gilt  $\mathbb{Z}[X]/(X^2 - d) \cong \mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$ .

## 1.11 Primideale

**Definition:** Ein *Primideal* von  $R$  ist ein echtes Ideal  $\mathfrak{p} \subsetneq R$  mit der Eigenschaft:

$$\forall x, y \in R: xy \in \mathfrak{p} \longrightarrow (x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p}).$$

**Proposition:** Ein von Null verschiedenes Hauptideal  $(p)$  in einem Integritätsbereich ist ein Primideal genau dann, wenn das Erzeugende  $p$  ein Primelement ist.

**Proposition:** Ein Ideal  $\mathfrak{p}$  von  $R$  ist ein Primideal genau dann, wenn der Faktorring  $R/\mathfrak{p}$  ein Integritätsbereich ist.

**Definition:** Ein *maximales Ideal* von  $R$  ist ein echtes Ideal  $\mathfrak{m} \subsetneq R$ , welches unter allen echten Idealen maximal ist, das heisst, so dass jedes Ideal  $\mathfrak{a}$  mit  $\mathfrak{m} \subset \mathfrak{a}$  entweder gleich  $\mathfrak{m}$  oder gleich  $R$  ist.

**Proposition:** Ein Ideal  $\mathfrak{m}$  von  $R$  ist maximal genau dann, wenn der Faktorring  $R/\mathfrak{m}$  ein Körper ist.

**Folge:** Jedes maximale Ideal ist ein Primideal.

**Beispiele:** (a) Das Nullideal ist prim genau dann, wenn  $R$  ein Integritätsbereich ist.

(b) Das Nullideal ist maximal genau dann, wenn  $R$  ein Körper ist.

(c) Das Ideal  $(X^2 + 1) \subset \mathbb{R}[X]$  ist ein maximales Ideal.

(d) Für jede ganze Zahl  $d$ , die kein Quadrat ist, ist das Ideal  $(X^2 - d) \subset \mathbb{Z}[X]$  ein Primideal, aber kein maximales Ideal.

(e) Betrachte eine Menge  $X$ , einen Körper  $K$ , und einen Unterring  $R$  des Rings aller Funktionen  $\text{Abb}(X, K)$ , welcher alle konstanten Funktionen  $X \rightarrow K$  enthält. Für jedes  $x \in X$  ist dann  $\mathfrak{m}_x := \text{Kern}(R \rightarrow K, f \mapsto f(x))$  ein maximales Ideal.

**Satz:** (*Krull*) Für jedes echte Ideal  $\mathfrak{a} \subsetneq R$  existiert ein maximales Ideal  $\mathfrak{m}$  mit  $\mathfrak{a} \subset \mathfrak{m}$ .

**Folge:** Jeder nichttriviale Ring besitzt ein maximales Ideal.

**Folge:** Jeder nichttriviale Ring besitzt ein Primideal.



## 1.12 Moduln

**Definition:** Ein *Modul über  $R$*  oder kurz ein  *$R$ -Modul* ist ein Tupel  $(M, +, \cdot, 0)$  bestehend aus einer Menge  $M$  mit zwei Abbildungen

$$\begin{aligned} + : M \times M &\rightarrow M, & (m, n) &\mapsto m + n \\ \cdot : R \times M &\rightarrow M, & (x, m) &\mapsto xm \end{aligned}$$

und einem ausgezeichneten Element  $0 \in M$ , so dass gilt:

- (a)  $(M, +, 0)$  ist eine abelsche Gruppe.
- (b)  $\forall x \in R \forall m, n \in M: x(m + n) = xm + xn$  (Links distributivität)
- (c)  $\forall x, y \in R \forall m \in M: (x + y)m = xm + ym$  (Rechts distributivität)
- (d)  $\forall x, y \in R \forall m \in M: x(y m) = (xy)m$  (Assoziativität)
- (e)  $\forall m \in M: 1 \cdot m = m$  (Einselement)

**Beispiel:** Ein Modul über einem Körper  $K$  ist also einfach ein  $K$ -Vektorraum.

**Beispiel:** Jede Menge mit einem Element besitzt eine eindeutige Struktur als  $R$ -Modul und heisst dann *Nullmodul*.

**Beispiel:** Mit den Operationen  $+$  und  $\cdot$  von  $R$  ist  $R$  selbst ein  $R$ -Modul.

**Definition:** Ein *Unterm modul* eines  $R$ -Moduls  $M$  ist eine Teilmenge  $N \subset M$  mit den Eigenschaften:

- (a)  $N \neq \emptyset$ .
- (b)  $\forall n, n' \in N: n + n' \in N$ .
- (c)  $\forall x \in R \forall n \in N: xn \in N$ .

**Proposition:** Eine Teilmenge  $N \subset M$  ist ein Untermodul genau dann, wenn sie zusammen mit den Restriktionen der Addition und der skalaren Multiplikation von  $M$  selbst einen  $R$ -Modul bildet.

**Beispiel:** Jeder  $R$ -Modul  $M$  hat die Untermoduln  $\{0\}$  und  $M$  selbst.

**Beispiel:** Die Untermoduln von  $R$  als  $R$ -Modul sind genau die Ideale von  $R$ .

**Proposition:** Der Durchschnitt jeder nichtleeren Kollektion von Untermoduln von  $M$  ist ein Untermodul von  $M$ .

**Proposition-Definition:** Für jede Teilmenge  $S$  eines  $R$ -Moduls  $M$  existiert ein eindeutiger kleinster Untermodul  $\langle S \rangle \subset M$ , welcher  $S$  enthält. Dieser heisst das *Erzeugnis von  $S$*  oder *von  $S$  erzeugt*. Für endlich viele Elemente  $m_1, \dots, m_n \in M$  gilt

$$\langle \{m_1, \dots, m_n\} \rangle = \{ x_1 m_1 + \dots + x_n m_n \mid \forall i: x_i \in R \}.$$

Ein von endlich vielen Elementen erzeugter Modul heisst *endlich erzeugt*.

**Proposition-Definition:** Die *Summe* von Untermoduln  $M_1, \dots, M_n$

$$M_1 + \dots + M_n := \{ m_1 + \dots + m_n \mid \forall i: m_i \in M_i \}$$

ist ein Untermodul. Ist die Abbildung

$$M_1 \times \dots \times M_n \rightarrow M_1 + \dots + M_n, (m_1, \dots, m_n) \mapsto m_1 + \dots + m_n$$

bijektiv, so heisst die Summe *direkt* oder eine *innere direkte Summe* und wird bezeichnet mit

$$M_1 \oplus \dots \oplus M_n = \bigoplus_{i=1}^n M_i.$$

**Proposition-Definition:** Das kartesische Produkt von  $R$ -Moduln  $M_1 \times \dots \times M_n$  versehen mit komponentenweiser Addition und skalarer Multiplikation sowie dem Nullelement  $(0, \dots, 0)$  ist ein  $R$ -Modul. Er heisst das (*direkte*) *Produkt* oder, da endlich, die *äussere direkte Summe* von  $M_1, \dots, M_n$  und wird bezeichnet mit

$$M_1 \boxplus \dots \boxplus M_n = \boxplus_{i=1}^n M_i.$$

Sind alle Faktoren gleich, so schreibt man auch  $M^n := \boxplus_{i=1}^n M$ .

**Konvention:** Oft werden innere und äussere direkte Summe mit demselben Symbol  $\oplus$  bezeichnet. Welche dann jeweils gemeint ist, muss man aus dem Zusammenhang erschliessen.

**Definition:** Eine Abbildung zwischen zwei  $R$ -Moduln  $\varphi: M \rightarrow N$  mit

- (a)  $\forall m, m' \in M: \varphi(m + m') = \varphi(m) + \varphi(m')$  und
- (b)  $\forall m \in M \forall x \in R: \varphi(xm) = x \cdot \varphi(m)$

heisst *R-linear* oder ein (*R-Modul*)-*Homomorphismus*. Die Menge aller Homomorphismen  $M \rightarrow N$  wird bezeichnet mit  $\text{Hom}_R(M, N)$ . Ein Homomorphismus  $M \rightarrow M$  heisst ein *Endomorphismus von M*, und wir schreiben  $\text{End}_R(M) := \text{Hom}_R(M, M)$ .

**Proposition:** Für jeden Homomorphismus  $\varphi: M \rightarrow N$  gilt:

- (a)  $\text{Kern}(\varphi) := \{m \in M \mid \varphi(m) = 0\}$  ist ein Untermodul von  $M$ .
- (b)  $\text{Bild}(\varphi)$  ist ein Untermodul von  $N$ .
- (c)  $\varphi$  ist injektiv genau dann, wenn  $\text{Kern}(\varphi) = 0$  ist.
- (d)  $\varphi$  ist surjektiv genau dann, wenn  $\text{Bild}(\varphi) = N$  ist.

**Beispiel:** Die *identische Abbildung*  $\text{id}_M: M \rightarrow M, m \mapsto m$  ist ein Homomorphismus.

**Proposition:** Die Komposition zweier Homomorphismen ist ein Homomorphismus.

**Proposition:** Schreibe die Elemente der  $R$ -Moduln  $R^n$  und  $R^m$  als Spaltenvektoren. Dann induziert jede Matrix  $A \in \text{Mat}_{m \times n}(R)$  einen Homomorphismus

$$L_A: R^n \rightarrow R^m, m \mapsto Am.$$

Umgekehrt ist jeder Homomorphismus  $R^n \rightarrow R^m$  gleich  $L_A$  für ein eindeutiges  $A$ . Weiter gilt für je zwei komponierbare Matrizen  $L_{AB} = L_A \circ L_B$ .

**Definition:** Ein Homomorphismus  $\varphi: M \rightarrow N$  mit einem beidseitigem Inversen  $\varphi^{-1}: N \rightarrow M$  heisst ein *Isomorphismus*, und wir schreiben dann  $\varphi: M \xrightarrow{\sim} N$ . Existiert ein Isomorphismus  $M \xrightarrow{\sim} N$ , so heissen  $M$  und  $N$  *isomorph* und wir schreiben  $M \cong N$ .

**Proposition:** Ein Homomorphismus ist ein Isomorphismus genau dann, wenn er bijektiv ist.

**Proposition:** Die Komposition zweier Isomorphismen ist ein Isomorphismus. Das Inverse eines Isomorphismus ist eindeutig bestimmt und selbst ein Isomorphismus. Isomorphie von  $R$ -Moduln ist eine Äquivalenzrelation.

**Definition:** Jeder zu  $R^n$  isomorphe  $R$ -Modul heisst *frei vom Rang  $n$* .

**Beispiel:** Für jedes Ideal  $(0) \subsetneq \mathfrak{a} \subsetneq R$  ist der  $R$ -Modul  $R/\mathfrak{a}$  nicht frei.

**Definition:** Ein Isomorphismus  $M \xrightarrow{\sim} M$  heisst ein *Automorphismus von  $M$* .

**Proposition-Definition:** Die Menge  $\text{Aut}_R(M)$  aller Automorphismen von  $M$  ist eine Gruppe bezüglich Komposition mit dem Einselement  $\text{id}_M$ , genannt die *Automorphismengruppe von  $M$* .

**Proposition:** Für jede natürliche Zahl  $n$  haben wir einen Gruppen-Isomorphismus

$$\text{GL}_n(R) \xrightarrow{\sim} \text{Aut}_R(R^n), A \mapsto L_A.$$

**Proposition-Definition:** Sei  $N$  ein Untermodul von  $M$ . Für jedes  $m \in M$  betrachte die *Nebenklasse*

$$m + N := \{m + n \mid n \in N\} \subset M.$$

Für alle  $m, m' \in M$  gilt

$$m + N = m' + N \iff m \in m' + N \iff m' \in m + N \iff (m + N) \cap (m' + N) \neq \emptyset.$$

Insbesondere ist  $M$  die disjunkte Vereinigung aller Nebenklassen von  $N$ . Die Menge aller Nebenklassen

$$M/N := \{m + N \mid m \in M\}$$

besitzt eine eindeutige Struktur eines  $R$ -Moduls, so dass gilt:

- (a)  $\forall m, m' \in M : (m + N) + (m' + N) = (m + m') + N.$
- (b)  $\forall m \in M \forall x \in R : x \cdot (m + N) = xm + N.$

Für diese gilt weiter:

- (c) Das Nullelement von  $M/N$  ist  $0 + N = N$ .
- (d) Das additive Inverse jedes Elements  $m + N$  ist  $-(m + N) = (-m) + N$ .

**Definition:** Der Modul  $M/N$  heisst der *Faktormodul von  $M$  nach  $N$* .

**Proposition:** Die Abbildung  $\pi: M \rightarrow M/N$ ,  $m \mapsto m + N$  ist ein surjektiver Modulhomomorphismus mit Kern  $N$ .

**Homomorphiesatz:** Jeder Homomorphismus  $\varphi: M \rightarrow N$  induziert einen Isomorphismus

$$M/\text{Kern}(\varphi) \xrightarrow{\sim} \text{Bild}(\varphi), \quad m + \text{Kern}(\varphi) \mapsto \varphi(m).$$

Das Tensorprodukt von  $R$ -Moduln wird genauso definiert und konstruiert wie das Tensorprodukt von Vektorräumen:

**Definition:** Ein *Tensorprodukt zweier  $R$ -Moduln  $M_1$  und  $M_2$*  besteht aus einem  $R$ -Modul  $\tilde{M}$  und einer  $R$ -bilinearen Abbildung  $\kappa: M_1 \times M_2 \rightarrow \tilde{M}$  mit der *universellen Eigenschaft*:

Für jeden  $R$ -Modul  $N$  und jede  $R$ -bilineare Abbildung  $\varphi: M_1 \times M_2 \rightarrow N$  existiert genau eine  $R$ -lineare Abbildung  $\bar{\varphi}: \tilde{M} \rightarrow N$  mit  $\bar{\varphi} \circ \kappa = \varphi$ , das heisst, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{\varphi} & N \\ & \searrow \kappa & \nearrow \bar{\varphi} \\ & & \tilde{M} \end{array}$$

**Proposition:** Ein Tensorprodukt ist eindeutig bis auf eindeutige Isomorphie, mit anderen Worten: Ist sowohl  $(\tilde{M}, \kappa)$  wie  $(\tilde{M}', \kappa')$  ein Tensorprodukt von  $M_1$  und  $M_2$ , so existiert ein eindeutiger  $R$ -Modul-Isomorphismus  $i: \tilde{M} \xrightarrow{\sim} \tilde{M}'$  mit  $i \circ \kappa = \kappa'$ , das heisst, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{\kappa'} & \tilde{M}' \\ & \searrow \kappa & \nearrow i \\ & & \tilde{M} \end{array} \quad \begin{array}{c} \cong \\ \nearrow \end{array}$$

**Satz:** Ein Tensorprodukt existiert immer.

**Konvention:** Wir fixieren ein für alle Mal ein Tensorprodukt  $(\tilde{M}, \kappa)$  und bezeichnen den Modul  $\tilde{M}$  mit  $M_1 \otimes_R M_2$  und die Abbildung  $\kappa$  mit

$$M_1 \times M_2 \rightarrow M_1 \otimes_R M_2, \quad (m_1, m_2) \mapsto m_1 \otimes m_2.$$

Deren Rechenregeln sowie die Grundeigenschaften des Tensorprodukts entsprechen denen im Fall von Vektorräumen. Analog werden höhere Tensorpotenzen, symmetrische und alternierende Potenzen, sowie die Tensor-, symmetrische, bzw. äussere Algebra eines Moduls konstruiert.

## 2 Teilbarkeit

In diesem Kapitel bezeichnet  $R$  einen Integritätsbereich.

### 2.1 Irreduzible und Primelemente

**Definition:** Betrachte Elemente  $a, b \in R$ .

- (a) Gilt  $\exists x \in R: ax = b$ , so schreiben wir  $a|b$  und sagen  $a$  teilt  $b$ , und nennen  $a$  einen *Teiler von  $b$* , und  $b$  ein *Vielfaches von  $a$* .
- (b) Gilt  $\exists x \in R^\times: ax = b$ , so schreiben wir  $a \sim b$  und nennen  $a$  und  $b$  *assoziiert*.

**Proposition:** Für alle  $a, b, c, a', b', x_i, b_i \in R$  gilt:

- (a)  $1|a$  und  $a|a$  und  $a|0$ .
- (b) Aus  $a|b$  und  $b|c$  folgt  $a|c$ .
- (c) Gilt  $a|b_i$  für alle  $i$ , so auch  $a | \sum_i x_i b_i$ .
- (d) Es ist  $a \sim b$  genau dann, wenn  $a|b$  und  $b|a$ .
- (e)  $\sim$  ist eine Äquivalenzrelation.
- (f) Gilt  $a \sim a'$  und  $b \sim b'$ , so ist  $a|b$  genau dann, wenn  $a'|b'$ .
- (g) Gilt  $a|b$  und  $b \in R^\times$ , so ist auch  $a \in R^\times$ .

**Definition:** Ein Element  $p \in R$  mit  $p \neq 0$  und  $p \notin R^\times$  heisst

- (a) *irreduzibel* oder *unzerlegbar*, wenn gilt

$$\forall a, b \in R: p = ab \longrightarrow (a \in R^\times \text{ oder } b \in R^\times).$$

- (b) *prim* oder ein *Primelement*, wenn gilt

$$\forall a, b \in R: p|ab \longrightarrow (p|a \text{ oder } p|b).$$

**Proposition:** Gilt  $p \sim p'$ , so ist  $p$  *irreduzibel* bzw. *prim* genau dann, wenn  $p'$  es ist.

**Proposition:** Jedes Primelement ist irreduzibel.

**Bemerkung:** Eine *Primzahl* ist nach Definition eine natürliche Zahl  $\geq 2$ , welche ausser der 1 und sich selbst keine natürlichen Zahlen als Teiler hat. Nach obiger Definition bedeutet dies irreduzibel und positiv. In dem Ring  $\mathbb{Z}$  ist irreduzibel aber äquivalent zu prim, und es hat sich herausgestellt, dass die Eigenschaft „prim“ die bessere Verallgemeinerung darstellt.

**Beispiel:** Im Ring  $\mathbb{Z}$  ist 2 ein Primelement. In  $\mathbb{Z}[i]$  gilt dagegen  $2 = (1+i)(1-i)$  mit Nichteinheiten  $1 \pm i$ , also ist 2 nicht irreduzibel in  $\mathbb{Z}[i]$ . In  $\mathbb{Z}[i\sqrt{5}]$  ist 2 zwar irreduzibel, aber nicht prim, denn es ist  $2 \cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5})$  und  $2 \nmid 1 \pm i\sqrt{5}$ .

## 2.2 Faktorielle Ringe

**Definition:** Ein Integritätsbereich, in dem jedes von 0 verschiedene Element ein Produkt von Einheiten und/oder Primelementen ist, heisst *faktoriell*.

**Beispiel:** Der Ring  $\mathbb{Z}$  ist faktoriell.

**Beispiel:** Jeder Körper ist ein faktorieller Ring. (Er hat zwar keine Primelemente, aber auch nichts zu faktorisieren.)

Sei nun  $R$  beliebig faktoriell. Dann hat jedes Element von  $R \setminus \{0\}$  die Form

$$a = u \cdot p_1 \cdots p_m$$

für eine Einheit  $u \in R^\times$ , eine Zahl  $m \geq 0$ , und Primelemente  $p_1, \dots, p_m$ .

**Satz:** Diese *Primfaktorzerlegung* ist eindeutig bis auf Umordnung und Assoziiertheit, das heisst: Für jede weitere Zerlegung mit  $v \in R^\times$  und Primelementen  $q_1, \dots, q_n$

$$a = v \cdot q_1 \cdots q_n$$

gilt  $m = n$  und es existiert eine Permutation  $\sigma \in S_m$  mit  $\forall i: p_i \sim q_{\sigma i}$ .

**Proposition:** In jedem faktoriellen Ring ist irreduzibel äquivalent zu prim.

**Proposition:** Sei  $R$  faktoriell, und sei  $\{p_i \mid i \in I\}$  ein Repräsentantensystem seiner Primelemente unter Assoziiertheit.

(a) Jedes Element von  $R \setminus \{0\}$  kann man auf eindeutige Weise schreiben in der Form

$$a = u \cdot \prod'_{i \in I} p_i^{\mu_i}$$

für eine Einheit  $u \in R^\times$  und Exponenten  $\mu_i \in \mathbb{Z}^{\geq 0}$ , fast alle gleich 0.

(b) Für  $a = u \cdot \prod'_{i \in I} p_i^{\mu_i}$  und  $b = v \cdot \prod'_{i \in I} p_i^{\nu_i}$  mit  $u, v \in R^\times$  gilt  $a|b$  genau dann, wenn für alle  $i$  gilt  $\mu_i \leq \nu_i$ .

(c) Jedes Element von  $\text{Quot}(R) \setminus \{0\}$  kann man auf eindeutige Weise schreiben in der Form

$$a = u \cdot \prod'_{i \in I} p_i^{\mu_i}$$

für eine Einheit  $u \in R^\times$  und Exponenten  $\mu_i \in \mathbb{Z}$ , fast alle gleich 0.

## 2.3 Grösster gemeinsamer Teiler

Sei  $R$  faktoriell.

**Proposition-Definition:** Betrachte Elemente  $a_1, \dots, a_n \in R$ .

- (a) Ein Element  $b \in R$  mit  $\forall i: b|a_i$  heisst ein *gemeinsamer Teiler* von  $a_1, \dots, a_n$ .
- (b) Es existiert ein gemeinsamer Teiler  $b$  von  $a_1, \dots, a_n$ , so dass für jeden gemeinsamen Teiler  $b'$  von  $a_1, \dots, a_n$  gilt  $b'|b$ .
- (c) Dieser *grösste gemeinsame Teiler* von  $a_1, \dots, a_n$  ist eindeutig bis auf Assoziiertheit. Wir bezeichnen jeden solchen mit  $\text{ggT}(a_1, \dots, a_n)$ .

Da der  $\text{ggT}$  nur eindeutig bis auf Assoziiertheit ist, sollte man ihn immer nur auf Assoziiertheit testen und nicht auf Gleichheit.

**Proposition:** Für alle  $a_1, \dots, a_n, x_1, \dots, x_n \in R$  gilt

$$\text{ggT}(a_1, \dots, a_n) \sim \text{ggT}(a_1, \dots, a_n, \sum_{i=1}^n x_i a_i).$$

**Definition:** Elemente  $a_1, \dots, a_n \in R$  mit

- (a)  $\text{ggT}(a_1, \dots, a_n) \sim 1$  heissen *teilerfremd*.
- (b)  $\text{ggT}(a_i, a_j) \sim 1$  für alle  $i \neq j$  heissen *paarweise teilerfremd*.

**Proposition-Definition:** Betrachte Elemente  $a_1, \dots, a_n \in R$ .

- (a) Ein Element  $b \in R$  mit  $\forall i: a_i|b$  heisst *gemeinsames Vielfaches* von  $a_1, \dots, a_n$ .
- (b) Es existiert ein gemeinsames Vielfaches  $b$  von  $a_1, \dots, a_n$ , so dass für jedes gemeinsame Vielfache  $b'$  von  $a_1, \dots, a_n$  gilt  $b|b'$ .
- (c) Dieses *kleinste gemeinsame Vielfache* von  $a_1, \dots, a_n$  ist eindeutig bis auf Assoziiertheit. Wir bezeichnen jedes solche mit  $\text{kgV}(a_1, \dots, a_n)$ .

**Proposition:** Für alle  $a, a_1, \dots, a_n \in R$  gilt

$$\begin{aligned} \text{ggT}(aa_1, \dots, aa_n) &\sim a \cdot \text{ggT}(a_1, \dots, a_n), \\ \text{kgV}(aa_1, \dots, aa_n) &\sim a \cdot \text{kgV}(a_1, \dots, a_n). \end{aligned}$$

**Proposition:** Für alle  $a_1, a_2 \in R$  gilt

$$\text{ggT}(a_1, a_2) \cdot \text{kgV}(a_1, a_2) \sim a_1 \cdot a_2.$$

## 2.4 Hauptidealringe

**Definition:** Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heisst ein *Hauptidealring*.

**Beispiel:** Für jeden Körper  $K$  ist  $K[[X]]$  ein Hauptidealring. Genauer sind seine Ideale das Nullideal  $(0)$  sowie die Ideale  $(X^n)$  für alle  $n \geq 0$ .

**Satz:** Sei  $R$  ein Hauptidealring.

- (a) Jede aufsteigende Folge von Idealen  $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \dots$  wird stationär, das heisst, es existiert  $n_0 \geq 0$  mit  $\mathfrak{a}_n = \mathfrak{a}_{n_0}$  für alle  $n \geq n_0$ . (Ein Ring mit dieser Eigenschaft heisst *noethersch*.)
- (b) Für jedes  $a \in R \setminus (\{0\} \cup R^\times)$  existiert ein Primelement  $p \in R$  mit  $p|a$ .
- (c) Der Ring  $R$  ist faktoriell.

**Proposition:** Ist  $R$  ein Hauptidealring, so gilt für alle  $a_1, \dots, a_n \in R$

$$(\text{ggT}(a_1, \dots, a_n)) = (a_1, \dots, a_n).$$

Insbesondere existieren  $x_1, \dots, x_n \in R$  mit

$$\text{ggT}(a_1, \dots, a_n) = x_1 a_1 + \dots + x_n a_n.$$

**Bemerkung:** Nicht jeder faktorielle Ring ist ein Hauptidealring. Zum Beispiel ist für jeden Körper  $K$  der Ring  $K[X, Y]$  faktoriell, aber sein Ideal  $(X, Y)$  ist kein Hauptideal. In diesem Fall ist  $\text{ggT}(X, Y) \sim 1$ , aber  $(X, Y) \neq (1)$ . Der ggT lässt sich hier nicht als Linearkombination von  $X$  und  $Y$  darstellen.

**Satz:** (*Chinesischer Restsatz*) Seien  $a_1, \dots, a_n$  paarweise teilerfremde Elemente eines Hauptidealrings  $R$ . Dann ist die folgende Abbildung ein Ring-Isomorphismus:

$$\begin{aligned} R/(a_1 \cdots a_n) &\longrightarrow R/(a_1) \times \dots \times R/(a_n), \\ x + (a_1 \cdots a_n) &\mapsto (x + (a_1), \dots, x + (a_n)). \end{aligned}$$

Der älteste bekannte Beleg dieses Satzes ist eine mathematische Veröffentlichung in China im 5. Jahrhundert unserer Zeitrechnung. Gemäss einer Legende benutzte ein chinesischer General den Satz für  $R = \mathbb{Z}$ , um seine Soldaten zu zählen. Er liess sie in Reihen von  $a_1 := 19$  aufstellen und erhielt den Rest 1, in Reihen von  $a_2 := 17$  mit dem Rest 14, sowie in Reihen von  $a_3 := 12$  mit dem Rest 1. Da er auch die ungefähre Grössenordnung wusste, konnte er die Gesamtzahl bestimmen, nämlich 3193 gegenüber  $19 \cdot 17 \cdot 12 = 3876$ .

Computeralgebrasysteme benutzen den chinesischen Restsatz, um eine Rechnung mit grossen Zahlen in  $\mathbb{Z}$  durch mehrere voneinander unabhängige Rechnungen in endlichen Körpern  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  zu ersetzen. Je nach Situation kann das den Rechenaufwand deutlich verringern; ausserdem eignet sich die Methode gut für parallele Programmierung.



## 2.5 Euklidische Ringe

**Definition:** Ein *euklidischer Ring* ist ein Integritätsbereich  $R$  zusammen mit einer Abbildung  $\delta: R \setminus \{0\} \rightarrow \mathbb{Z}^{\geq 0}$ , so dass gilt

$$\forall a \in R \forall b \in R \setminus \{0\}: \exists q, r \in R: a = bq + r \text{ und } (r = 0 \text{ oder } \delta(r) < \delta(b)).$$

Dieser Prozess heisst *Division mit Rest*, nämlich *Division von  $a$  durch  $b$  mit Quotient  $q$  und Rest  $r$* . Die Funktion  $\delta$  misst die Grösse oder Komplexität eines Elements.

**Satz:** Jeder euklidische Ring ist ein Hauptidealring.

**Beispiel:** Der Ring  $\mathbb{Z}$  ist euklidisch mit der Funktion  $\delta(a) := |a|$ .

- Seine Ideale sind genau die Ideale  $(n) = n\mathbb{Z}$  für alle  $n \geq 0$ .
- Die maximalen Ideale von  $\mathbb{Z}$  sind die  $(p)$  für alle Primzahlen  $p$ , mit dem zugehörigen Restklassenkörper  $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ .
- Das einzige weitere Primideal von  $\mathbb{Z}$  ist das Nullideal  $(0)$ .
- Die Einheitengruppe  $(\mathbb{Z}/n\mathbb{Z})^\times$  besteht aus den Restklassen  $a + n\mathbb{Z}$  für alle zu  $n$  teilerfremden Zahlen  $a$ .

**Beispiel:** Für jeden Körper  $K$  ist  $K[X]$  euklidisch mit der Funktion  $\delta(f) := \deg(f)$ .

**Beispiel:** Für eine natürliche Zahl  $d \geq 1$  ist der Ring  $\mathbb{Z}[i\sqrt{d}]$  euklidisch, bzw. ein Hauptidealring, bzw. faktoriell genau dann, wenn  $d \leq 2$  ist. Die Funktion  $\delta(a + i\sqrt{d} \cdot b) := a^2 + db^2$  erfüllt dann die gewünschte Bedingung.

**Vorsicht:** Nicht jeder Hauptidealring lässt sich zu einem euklidischen Ring machen. Zum Beispiel ist  $\mathbb{Z}[\frac{1}{2} \cdot (1 + i\sqrt{163})]$  ein Hauptidealring, aber nicht euklidisch.

**Euklidischer Algorithmus:** Sei  $(R, \delta)$  euklidisch und betrachte Elemente  $a_1, a_2 \in R$ , nicht beide gleich Null. Wir setzen diese fort zu einer Folge  $a_1, \dots, a_n$  wie folgt. Ist das letzte konstruierte Element  $a_n$  gleich Null, so halte an. Andernfalls benutze Division mit Rest und schreibe  $a_{n-1} = a_n q_n + a_{n+1}$  mit  $a_{n+1} = 0$  oder  $\delta(a_{n+1}) < \delta(a_n)$ .

**Proposition:** Dieser Algorithmus endet nach endlich vielen Schritten, und für das letzte von Null verschiedene Element  $a_{m-1}$  gilt

$$a_{m-1} \sim \text{ggT}(a_1, a_2).$$

**Bemerkung:** Der euklidische Algorithmus produziert zusätzlich Elemente  $u_n, v_n \in R$  mit  $a_n = u_n a_1 + v_n a_2$  für alle  $n \geq 1$ , nämlich durch  $(u_1, v_1) := (1, 0)$  und  $(u_2, v_2) := (0, 1)$  und  $(u_{n+1}, v_{n+1}) := (u_{n-1} - u_n q_n, v_{n-1} - v_n q_n)$  für alle  $n \geq 2$ . Für das letzte von Null verschiedene Element  $a_{m-1}$  liefert dies eine Linearkombination

$$\text{ggT}(a_1, a_2) \sim a_{m-1} = u_{m-1} a_1 + v_{m-1} a_2.$$

**Beispiel:** In  $\mathbb{Z}$  ist  $\text{ggT}(2019, 1959) \sim 3 = 98 \cdot 2019 - 101 \cdot 1959$ .

## 2.6 Polynomringe

**Proposition:** Für jeden Integritätsbereich  $R$  gilt  $R[X]^\times = R^\times$ .

Sei nun  $R$  ein faktorieller Ring mit Quotientenkörper  $K$ . Für zwei Elemente  $a, b \in K^\times$  schreiben wir  $a \sim b$  genau dann, wenn  $\frac{b}{a} \in R^\times$  ist. Für Elemente von  $R \setminus \{0\}$  stimmt dies mit der Definition aus §2.1 überein.

**Definition:** (a) Der *Inhalt* eines Polynoms  $f(X) = \sum_{i=0}^n a_i X^i \in R[X] \setminus \{0\}$  ist

$$I(f) := \text{ggT}(a_0, \dots, a_n) \in R \setminus \{0\}.$$

(b) Ein Polynom  $f \in R[X] \setminus \{0\}$  mit  $I(f) \sim 1$  heisst *primitiv*.

**Lemma:** Für alle  $f \in R[X] \setminus \{0\}$  und  $a \in R \setminus \{0\}$  gilt:

(a)  $\frac{f}{I(f)}$  ist ein primitives Element von  $R[X] \setminus \{0\}$ .

(b)  $I(af) \sim a \cdot I(f)$ .

**Lemma:** Der Inhalt setzt sich fort zu einer Abbildung  $K[X] \setminus \{0\} \rightarrow K^\times$ ,  $f \mapsto I(f)$  mit denselben Eigenschaften für alle  $f \in K[X] \setminus \{0\}$  und  $a \in K^\times$ .

**Lemma:** Für jedes  $f \in K[X] \setminus \{0\}$  gilt  $f \in R[X] \Leftrightarrow I(f) \in R$ .

**Gauss-Lemma:** Für alle  $f, g \in K[X] \setminus \{0\}$  gilt  $I(fg) \sim I(f) \cdot I(g)$ .

**Satz:** (a) Jedes Primelement von  $R$  ist ein Primelement von  $R[X]$ .

(b) Jedes primitive Polynom in  $R[X] \setminus \{0\}$ , das in  $K[X]$  prim ist, ist prim in  $R[X]$ .

(c) Jedes Primelement von  $R[X]$  ist eines der obigen.

(d) Der Ring  $R[X]$  ist faktoriell.

**Folge:** Ein primitives Polynom in  $R[X]$  ist irreduzibel in  $R[X]$  genau dann, wenn es irreduzibel in  $K[X]$  ist.

**Folge:** Für jedes normierte Polynom in  $R[X]$  liegt jede Nullstelle in  $K$  schon in  $R$ .

**Satz:** Für jeden faktoriellen Ring  $R$  und jedes  $n \geq 0$  ist  $R[X_1, \dots, X_n]$  faktoriell. Insbesondere ist für jeden Körper  $K$  der Ring  $K[X_1, \dots, X_n]$  faktoriell.

**Beispiel:** Für jeden Körper  $K$  ist  $X^3 - Y^5$  irreduzibel in  $K[X, Y]$ .

## 2.7 Irreduzibilitätskriterien

Betrachte einen faktoriellen Ring  $R$  und ein Primelement  $p$ . Der Reduktionshomomorphismus  $R \rightarrow R/(p)$ ,  $a \mapsto \bar{a} := a + (p)$  induziert einen Homomorphismus

$$R[X] \rightarrow (R/(p))[X], f = \sum' a_i X^i \mapsto \bar{f} := \sum' \bar{a}_i X^i.$$

Insbesondere gilt für alle  $f, g \in R[X]$  die Gleichung  $\overline{fg} = \bar{f} \cdot \bar{g}$ .

**Proposition:** Jedes primitive Element  $f \in R[X] \setminus \{0\}$  mit  $\deg(f) = \deg(\bar{f})$  und  $\bar{f}$  irreduzibel ist selbst irreduzibel.

**Beispiel:** Das Polynom  $X^5 + 2X^2 + 1 \in \mathbb{Z}[X]$  ist irreduzibel. (Benutze  $p = 3$ .)

**Beispiel:** Das Polynom  $X^4 + 3X^3 - X^2 + 1 \in \mathbb{Z}[X]$  ist irreduzibel. (Benutze  $p = 5$ .  
Aliter: Untersuche die Reduktionen bei  $p = 2$  und  $p = 3$  und vergleiche Grade.)

**Satz:** (*Eisenstein-Kriterium*) Sei  $f(X) = \sum_{i=0}^n a_i X^i \in R[X]$  primitiv mit  $n \geq 1$  und  $p \nmid a_n$  und  $\forall i < n: p \mid a_i$  und  $p^2 \nmid a_0$ . Dann ist  $f$  irreduzibel.

**Beispiel:** Das Polynom  $X^n - 2 \in \mathbb{Z}[X]$  ist irreduzibel für jedes  $n \geq 1$ .

**Beispiel:** Für jedes  $n \geq 1$  ist das Polynom  $X^n + Y^n + Z^n \in \mathbb{C}[X, Y, Z]$  irreduzibel.

**Proposition:** Für jede Primzahl  $p$  ist das  $p$ -te *Kreisteilungspolynom*

$$\Phi_p(X) := 1 + X + \dots + X^{p-1} = \frac{X^p - 1}{X - 1}$$

in  $\mathbb{Z}[X]$  irreduzibel.

**Satz:** (*Kronecker*) Es existiert ein Algorithmus, der jedes Polynom in beliebig vielen Variablen über  $\mathbb{Z}$  oder  $\mathbb{Q}$  in irreduzible Faktoren zerlegt.

## 2.8 Elementarteilersatz

**Satz:** Sei  $A$  eine  $m \times n$ -Matrix über einem Hauptidealring  $R$ . Dann existieren Matrizen  $U \in \text{GL}_m(R)$  und  $V \in \text{GL}_n(R)$  sowie eine Zahl  $0 \leq k \leq \min\{m, n\}$  und Elemente  $e_1, \dots, e_k \in R \setminus \{0\}$  mit  $e_1 | e_2 | \dots | e_k$ , so dass gilt

$$UAV = \left( \begin{array}{ccc|c} e_1 & & & \\ & \ddots & & \\ & & e_k & \\ \hline & & & \end{array} \right),$$

wobei alle nicht gezeigten Matrixkoeffizienten gleich 0 sind.

**Zusatz:** (a) Die Zahl  $k$  ist der Rang von  $A$  als Matrix über dem Körper  $\text{Quot}(R)$ .

(b) Für jedes  $1 \leq \ell \leq k$  ist  $e_1 \cdots e_\ell$  der grösste gemeinsame Teiler aller  $\ell \times \ell$ -Unterdeterminanten von  $A$ .

(c) Insbesondere sind sowohl  $k$ , als auch  $e_1, \dots, e_k$  bis auf Assoziiertheit, durch  $A$  eindeutig bestimmt.

**Definition:** Die Elemente  $e_1, \dots, e_k$  heissen die *Elementarteiler* von  $A$ .

**Folge:** Für alle  $n \geq 1$  und alle  $a_1, \dots, a_n$  in einem Hauptidealring  $R$  sind äquivalent:

(a)  $\text{ggT}(a_1, \dots, a_n) \sim 1$ .

(b) Es existiert eine Matrix in  $\text{GL}_n(R)$  mit erster Zeile  $(a_1, \dots, a_n)$ .

**Beispiel:** Sei  $p$  ein Primelement eines Hauptidealrings  $R$  und seien  $i, j \in \mathbb{Z}^{\geq 0}$  und  $a \in R$ . Ist  $a \neq 0$ , so sei  $k$  der grösste Exponent mit  $p^k | a$ . Dann sind die Elementarteiler

der Matrix  $\begin{pmatrix} p^i & a \\ 0 & p^j \end{pmatrix}$  gleich

$$(e_1, e_2) = \begin{cases} (p^i, p^j) & \text{falls } i \leq j \text{ und } p^i | a, \\ (p^j, p^i) & \text{falls } j \leq i \text{ und } p^j | a, \\ (p^k, p^{i+j-k}) & \text{falls } p^i \nmid a \text{ und } p^j \nmid a. \end{cases}$$

## 2.9 Moduln über Hauptidealringen

Sei  $R$  ein Hauptidealring.

**Proposition:** Jeder Untermodul von  $R^n$  ist von  $n$  Elementen erzeugt.

**Satz:** Für jeden endlich erzeugten  $R$ -Modul  $M$  existieren Zahlen  $r, k \geq 0$  und Elemente  $e_1, \dots, e_k \in R \setminus (\{0\} \cup R^\times)$  mit  $e_1 | e_2 | \dots | e_k$ , so dass gilt

$$M \cong R^r \boxplus \bigoplus_{i=1}^k R/(e_i).$$

**Definition:** Elemente  $m_1, \dots, m_\ell$  von  $M$  heissen *linear unabhängig*, wenn für alle  $a_1, \dots, a_\ell \in R$  gilt  $a_1 m_1 + \dots + a_\ell m_\ell = 0 \Rightarrow a_1 = \dots = a_\ell = 0$ .

**Zusatz:** (a) Die Zahl  $r$  ist die maximale Anzahl linear unabhängiger Elemente von  $M$ . Insbesondere ist sie eindeutig bestimmt. Sie heisst der „freie Rang“ von  $M$ .

(b) Die Zahl  $r + k$  ist die minimale Anzahl von Erzeugenden von  $M$ . Insbesondere ist  $k$  eindeutig bestimmt.

(c) Die Elemente  $e_1, \dots, e_k$  sind bis auf Assoziiertheit durch  $M$  eindeutig bestimmt. Sie heissen die *Elementarteiler* von  $M$ .

**Satz:** Für jeden endlich erzeugten  $R$ -Modul  $M$  existieren Zahlen  $r, \ell \geq 0$  und Primelemente  $p_i \in R$  und Exponenten  $\nu_i \geq 1$ , so dass gilt

$$M \cong R^r \boxplus \bigoplus_{i=1}^{\ell} R/(p_i^{\nu_i}).$$

**Zusatz:** Für jedes Primelement  $p \in R$  und jedes  $\nu \geq 0$  gilt

$$\dim_{R/(p)}(p^\nu M / p^{\nu+1} M) = r + |\{1 \leq i \leq \ell \mid p_i \sim p \wedge \nu_i > \nu\}|.$$

Insbesondere sind die Zahlen  $r$  und  $\ell$ , sowie die Paare  $(p_i, \nu_i)$  bis auf Vertauschung und Assoziiertheit der  $p_i$ , durch  $M$  eindeutig bestimmt.

**Beispiel:** Es gibt genau zwei Isomorphieklassen von endlichen  $\mathbb{Z}$ -Moduln der Kardinalität  $28 = 2^2 \cdot 7$ , nämlich die von

$$\begin{aligned} \mathbb{Z}/28\mathbb{Z} &\cong \mathbb{Z}/7\mathbb{Z} \boxplus \mathbb{Z}/4\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \boxplus \mathbb{Z}/14\mathbb{Z} &\cong \mathbb{Z}/7\mathbb{Z} \boxplus \mathbb{Z}/2\mathbb{Z} \boxplus \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

## 2.10 Jordansche Normalform

**Konstruktion:** Sei  $K$  ein Körper. Jeder  $K$ -Vektorraum  $V$  mit einem Endomorphismus  $\varphi \in \text{End}_K(V)$  wird durch

$$K[X] \times V \rightarrow V, \left( \sum' a_i X^i, v \right) \mapsto \sum' a_i \varphi^i(v)$$

zu einem  $K[X]$ -Modul. Umgekehrt können wir jeden  $K[X]$ -Modul als einen  $K$ -Vektorraum mit dem zusätzlichen Endomorphismus  $m \mapsto Xm$  ansehen. Die Theorie der  $K[X]$ -Moduln ist deshalb äquivalent zu der Theorie der Paare  $(V, \varphi)$ .

**Proposition:** Sei  $M \cong K[X]/(f)$  für ein normiertes Polynom  $f \in K[X]$ . Dann ist  $\dim_K(M) = \deg(f)$ , und der obige Endomorphismus  $\varphi \in \text{End}_K(M)$  hat das charakteristische Polynom  $f$  und das Minimalpolynom  $f$ .

**Satz:** Für jeden  $K[X]$ -Modul  $V$  mit  $\dim_K(V) < \infty$  existieren  $k \geq 0$  und normierte irreduzible Polynome  $p_i \in K[X]$  sowie Exponenten  $\nu_i \geq 1$ , so dass gilt

$$V \cong \bigoplus_{i=1}^k K[X]/(p_i^{\nu_i}).$$

Dabei sind  $k$ , und die Paare  $(p_i, \nu_i)$  bis auf Vertauschung, eindeutig bestimmt.

**Zusatz:** Für  $\varphi \in \text{End}_K(V)$  wie oben gilt:

- Das charakteristische Polynom von  $\varphi$  ist gleich  $p_1^{\nu_1} \cdots p_k^{\nu_k}$ .
- Das Minimalpolynom von  $\varphi$  ist gleich  $\text{kgV}(p_1^{\nu_1}, \dots, p_k^{\nu_k})$ .
- Der Hauptraum von  $\varphi$  zum normierten irreduziblen Polynom  $p$  entspricht den Summanden in der obigen Zerlegung mit  $p_i = p$ .
- Jordansche Normalform.

**Satz:** Sei  $\varphi$  ein Endomorphismus eines endlich-dimensionalen Vektorraums  $V$  über einem algebraisch abgeschlossenen Körper  $K$ .

- Es existieren ein diagonalisierbarer Endomorphismus  $\varphi_s$  und ein nilpotenter Endomorphismus  $\varphi_n$  mit  $\varphi_s \varphi_n = \varphi_n \varphi_s$  und  $\varphi_s + \varphi_n = \varphi$ .
- Diese sind durch  $\varphi$  eindeutig bestimmt.
- Beide können durch Polynome in  $\varphi$  mit Koeffizienten in  $K$  ausgedrückt werden.

**Definition:** Die Zerlegung  $\varphi = \varphi_s + \varphi_n$  heisst die *Jordan-Chevalley-Zerlegung* von  $\varphi$ . Die Endomorphismen  $\varphi_s$  und  $\varphi_n$  heissen der *halbeinfache*, beziehungsweise *nilpotente Anteil* von  $\varphi$ .

**Variante:** Für jede quadratische Matrix  $A$  über einem algebraisch abgeschlossenen Körper  $K$  existieren eine diagonalisierbare Matrix  $A_s$  und eine nilpotente Matrix  $A_n$  über  $K$  mit  $A_s A_n = A_n A_s$  und  $A_s + A_n = A$ . Diese sind durch  $A$  eindeutig bestimmt.

## 3 Gruppen

### 3.1 Grundbegriffe

**Definition:** Eine *Gruppe* ist ein Tripel  $(G, \circ, e)$  bestehend aus einer Menge  $G$  mit einer Abbildung

$$\circ : G \times G \rightarrow G, \quad (a, b) \mapsto a \circ b$$

und einem ausgezeichneten Element  $e \in G$ , so dass gilt:

$$\forall a, b, c \in G: \quad a \circ (b \circ c) = (a \circ b) \circ c \quad (\text{Assoziativitat})$$

$$\forall a \in G: \quad e \circ a = a \quad (\text{Linksneutrales Element})$$

$$\forall a \in G \exists a' \in G: \quad a' \circ a = e \quad (\text{Linksinverses Element})$$

Die Gruppe heisst *kommutativ* oder *abelsch*, wenn zusatzlich gilt:

$$\forall a, b \in G: \quad a \circ b = b \circ a \quad (\text{Kommutativitat})$$

**Proposition:** In jeder Gruppe  $(G, \circ, e)$  gilt:

- (a) Jedes linksneutrale Element  $e$  ist auch rechtsneutral, das heisst, es gilt  $\forall a \in G: a \circ e = a$ . Wir nennen  $e$  darum kurz *neutrales Element von  $G$* .
- (b) Jedes zu  $a \in G$  linksinverse Element  $a' \in G$  ist auch rechtsinvers, das heisst, es gilt  $a \circ a' = e$ . Wir nennen  $a'$  darum kurz *inverses Element zu  $a$* .
- (c) Das neutrale Element von  $G$  ist eindeutig bestimmt.
- (d) Zu jedem  $a \in G$  ist das inverse Element eindeutig bestimmt. Die Standardbezeichnung dafur ist  $a^{-1}$ .
- (e) Fur alle  $a \in G$  gilt  $(a^{-1})^{-1} = a$ .
- (f) Fur alle  $a, b \in G$  gilt  $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ .
- (g) Fur alle  $a, b \in G$  existiert ein eindeutiges  $x \in G$  mit  $a \circ x = b$ , namlich  $x = a^{-1} \circ b$ .
- (h) Fur alle  $a, b \in G$  existiert ein eindeutiges  $y \in G$  mit  $y \circ a = b$ , namlich  $y = b \circ a^{-1}$ .
- (i) Fur alle  $a, b, c \in G$  gilt  $b = c \iff a \circ b = a \circ c$ . (*Kurzungsregel links*)
- (j) Fur alle  $a, b, c \in G$  gilt  $b = c \iff b \circ a = c \circ a$ . (*Kurzungsregel rechts*)

**Proposition:** Fur jede naturliche Zahl  $n \geq 1$  und fur beliebige  $a_1, \dots, a_n \in G$  gilt: Bei jeder moglichen Klammerung der (a priori nicht wohldefinierten) Formel  $a_1 \circ \dots \circ a_n$  ist das Resultat gleich. Wir durfen hier also doch auf Klammern verzichten.

**Konvention:** Oft schreibt man nur kurz  $G$  fur das ganze Tripel und sieht die Zusatzdaten als implizit mitgegeben an. Wenn dabei keine Notation fur die Gruppenoperation angegeben wird, bezeichnet man diese multiplikativ in der Form  $g \cdot h$  oder  $gh$  und das neutrale Element mit  $1_G$  oder einfach  $1$ . Das tun ab sofort auch wir und verwenden ein spezielles Symbol wie  $\circ$  nur, wenn Verwechslungen zu vermeiden sind.

Sei also  $G$  eine Gruppe.

**Definition:** Für jedes Element  $g \in G$  und jede ganze Zahl  $n$  definieren wir die  $n$ -te Potenz von  $g$  induktiv durch

$$g^n := \begin{cases} 1 & \text{falls } n = 0, \\ g & \text{falls } n = 1, \\ g \cdot g^{n-1} & \text{falls } n > 1, \\ g^{-1} \cdot g^{n+1} & \text{falls } n < -1. \end{cases}$$

**Proposition:** Für alle  $g, h \in G$  und alle  $m, n \in \mathbb{Z}$  gilt:

$$\begin{aligned} g^{m+n} &= g^m \cdot g^n \\ g^{m-n} &= (g^m)^n \\ (g \cdot h)^m &= g^m \cdot h^m \quad \text{falls } gh = hg \text{ ist.} \end{aligned}$$

**Konvention:** Eine abelsche Gruppe (und nur eine abelsche) schreibt man oft additiv, das heisst mit dem Operator  $+$ , dem neutralen Element  $0_G$  oder  $0$ , und dem inversen Element  $-g$  zu  $g$ . Für  $g + (-h)$  schreibt man dann auch kürzer  $g - h$ . Anstatt der  $n$ -ten Potenz spricht man von dem  $n$ -ten Vielfachen  $n \cdot g$ . Die obigen Eigenschaften übersetzen sich dann in folgende:

**Proposition:** Jede additiv geschriebene abelsche Gruppe  $G$  ist auf eindeutige Weise ein  $\mathbb{Z}$ -Modul. Insbesondere gilt für alle  $g, h \in G$  und alle  $m, n \in \mathbb{Z}$ :

$$\begin{aligned} 0 \cdot g &= 0 \\ (\pm 1) \cdot g &= \pm g \\ (m \pm n) \cdot g &= m \cdot g \pm n \cdot g \\ (m \cdot n) \cdot g &= m \cdot (n \cdot g) \\ m \cdot (g \pm h) &= m \cdot g \pm m \cdot h \end{aligned}$$

**Beispiel:** (a) Die additive Gruppe eines Rings, eines Körpers, eines Vektorraums.

(b) Die Einheitengruppe eines Rings, eines Körpers.

(c) Die Matrizen Gruppen  $GL_n(K)$ ,  $SL_n(K)$ ,  $O(n)$ ,  $SO(n)$ ,  $U(n)$ .

(d) Die Symmetriegruppe einer Teilmenge  $X$  des euklidischen Raums  $\mathbb{R}^n$ :

$$\{A \in O(n) \mid A \cdot X = X\} \quad \text{oder} \quad \{A \in SO(n) \mid A \cdot X = X\}.$$

(e) Platonische Körper: Tetraeder, Würfel, Oktaeder, Dodekaeder, Ikosaeder.

(f) Ein regelmässiges ebenes Polygon im  $\mathbb{R}^3$ , aufgefasst als degenerierter regelmässiger Polyeder mit zwei Seitenflächen, heisst *Dieder* (gesprochen *Di-Eder*). Er ist invariant unter  $n$  Drehungen um seine Symmetrieachse, sowie  $n$  weiteren Drehungen um  $180^\circ$ , nämlich um alle durch den Mittelpunkt und eine Ecke oder Kantenmitte gehenden Geraden. Zusammen bilden diese  $2n$  Symmetrien die *Diedergruppe vom Grad  $n$* , bezeichnet mit  $D_n$ .

**Bemerkung:** Niemand beschreibt eine Gruppe durch Angabe ihrer Gruppentafel.



## 3.2 Untergruppen

**Definition:** Eine *Untergruppe* von  $G$  ist eine Teilmenge  $H \subset G$  mit den Eigenschaften:

- (a)  $1_G \in H$ .
- (b)  $\forall h, h' \in H: hh' \in H$ .
- (c)  $\forall h \in H: h^{-1} \in H$ .

Die Aussage „ $H$  ist eine Untergruppe von  $G$ “ bezeichnet man mit  $H < G$  oder  $G > H$ .

**Proposition:** Eine Teilmenge  $H \subset G$  ist eine Untergruppe genau dann, wenn sie zusammen mit der Restriktion der Gruppenoperation von  $G$  selbst eine Gruppe bildet. Dann ist weiter das Einselement von  $G$  gleich dem Einselement von  $H$ .

**Beispiel:** Die *triviale Untergruppe*  $1 = \{1_G\}$  und  $G$  selbst sind Untergruppen von  $G$ .

**Beispiel:** Die Untergruppen einer additiv geschriebenen abelschen Gruppe sind genau die  $\mathbb{Z}$ -Untermoduln. Insbesondere sind die Untergruppen von  $\mathbb{Z}$  genau die Ideale von  $\mathbb{Z}$ , also die Untergruppen  $n\mathbb{Z}$  für alle  $n \geq 0$ .

**Beispiel:** Die Untergruppen

$$\begin{array}{ccc} \mathrm{SO}_n(K) < & \mathrm{O}_n(K) \\ \wedge & \wedge \\ \mathrm{SL}_n(K) < & \mathrm{GL}_n(K). \end{array}$$

**Beispiel:** Die Untergruppen der Diedergruppe.

**Proposition:** Jede Untergruppe einer Untergruppe von  $G$  ist eine Untergruppe von  $G$ .

**Proposition:** Der Durchschnitt jeder nichtleeren Kollektion von Untergruppen von  $G$  ist ein Untergruppe von  $G$ .

**Proposition:** Für jede Teilmenge  $S \subset G$  existiert eine eindeutige kleinste Untergruppe von  $G$ , welche  $S$  enthält. Diese besteht aus allen Elementen der Form  $a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$  für alle  $n \geq 0$ , alle  $a_i \in S$ , und alle  $\varepsilon_i \in \{\pm 1\}$ .

**Definition:** Diese Untergruppe heisst *die von  $S$  erzeugte Untergruppe*  $\langle S \rangle$ . Im Fall einer endlichen Teilmenge schreiben wir auch kürzer  $\langle a_1, \dots, a_n \rangle = \langle \{a_1, \dots, a_n\} \rangle$  und nennen diese Untergruppe *endlich erzeugt*. Ist  $G = \langle S \rangle$ , so nennen wir  $G$  *von  $S$  erzeugt*.

**Definition:** Eine von einem Element erzeugte Gruppe  $G = \langle a \rangle$  heisst *zyklisch*.

**Beispiel:** Die additiven Gruppen von  $\mathbb{Z}$  und  $\mathbb{Z}/n\mathbb{Z}$  für jedes  $n \geq 1$  sind zyklisch. Die Untergruppen von  $\mathbb{Z}$  sind die  $m\mathbb{Z}$  für alle  $m \geq 0$ ; die Untergruppen von  $\mathbb{Z}/n\mathbb{Z}$  die  $m\mathbb{Z}/n\mathbb{Z}$  für alle  $m|n$ .

**Beispiel:** Die Gruppe der  $n$ -ten Einheitswurzeln  $\mu_n := \{\zeta \in \mathbb{C} \mid \zeta^n = 1\} < \mathbb{C}^\times$  ist zyklisch. Dass diese auf einem Kreis liegen, ist der Ursprung der Bezeichnung „zyklisch“.

Die Kommutativität oder Nichtkommutativität einer Gruppe hat mit einer Reihe von weiteren Untergruppen zu tun:

**Definition:** (a) Der *Kommutator* von  $g, h \in G$  ist das Element  $[g, h] := ghg^{-1}h^{-1}$ .

(b) Die *Kommutatorgruppe* von  $G$  ist die von allen Kommutatoren erzeugte Untergruppe

$$[G, G] := \langle \{[g, h] \mid g, h \in G\} \rangle.$$

(c) Der *Zentralisator* eines Elements  $g \in G$  ist die Untergruppe

$$\text{Cent}_G(g) := G_g := \{x \in G \mid xg = gx\}.$$

(d) Das *Zentrum* von  $G$  ist die Untergruppe

$$Z(G) := \{x \in G \mid \forall y \in G: xy = yx\}.$$

**Proposition:** (a)  $gh = hg \iff [g, h] = 1$ .

(b)  $\text{Cent}_G(g)$  ist die eindeutige grösste Untergruppe  $H < G$  mit  $g \in Z(H)$ .

(c)  $Z(G) = \bigcap_{g \in G} \text{Cent}_G(g) < G$ .

(d)  $g \in Z(G) \iff \text{Cent}_G(g) = G$ .

(e)  $G$  ist abelsch  $\iff Z(G) = G \iff [G, G] = 1$ .

**Beispiel:** (a) Die Kommutatorgruppe von  $\text{GL}_n(K)$  ist  $\text{SL}_n(K)$  ausser für  $|K| = n = 2$ .

(b) Sei  $g \in \text{GL}_n(K)$  eine Diagonalmatrix mit paarweise verschiedenen Diagonaleinträgen. Dann ist  $\text{Cent}_{\text{GL}_n(K)}$  die Gruppe aller invertierbarer Diagonalmatrizen.

(c) Das Zentrum von  $\text{GL}_n(K)$  ist die Untergruppe aller Skalarmatrizen  $K^\times \cdot I_n$ .

### 3.3 Nebenklassen

**Definition:** (*Rechnen mit Teilmengen*) Für beliebige Teilmengen  $X, Y \subset G$  und Elemente  $g \in G$  schreiben wir

$$XY := \{xy \mid x \in X, y \in Y\},$$

$$gX := \{gx \mid x \in X\},$$

$$Xg := \{xg \mid x \in X\},$$

$$X^{-1} := \{x^{-1} \mid x \in X\}.$$

Wegen der Assoziativität von  $G$  ist auch das Produkt von Teilmengen assoziativ, das heisst, es gilt  $X(YZ) = (XY)Z$  und  $g(XY) = (gX)Y$  und so weiter. Bei Produkten von mehreren Teilmengen und/oder Elementen können wir daher wieder die Klammern weglassen. Weiter gilt

$$(XY)^{-1} = Y^{-1}X^{-1}$$

$$(gX)^{-1} = X^{-1}g^{-1}$$

$$(Xg)^{-1} = g^{-1}X^{-1}$$

$$XY = YX \quad \text{falls } G \text{ abelsch ist,}$$

$$gX = Xg \quad \text{falls } G \text{ abelsch ist.}$$

**Definition:** Betrachte eine Untergruppe  $H < G$ . Für jedes Element  $g \in G$  heisst

$$\begin{aligned} gH &= \{gh \mid h \in H\} \text{ eine Linksnebenklasse von } H, \\ Hg &= \{hg \mid h \in H\} \text{ eine Rechtsnebenklasse von } H. \end{aligned}$$

Die Menge der jeweiligen Nebenklassen wird bezeichnet mit

$$\begin{aligned} G/H &= \{gH \mid g \in G\}, \\ H \backslash G &= \{Hg \mid g \in G\}. \end{aligned}$$

**Proposition:** Für jedes  $g \in G$  ist  $(gH)^{-1} = Hg^{-1}$  und  $(Hg)^{-1} = g^{-1}H$ . Insbesondere liefert dies eine natürliche Bijektion zwischen Links- und Rechtsnebenklassen

$$G/H \rightarrow H \backslash G, \quad gH \mapsto Hg^{-1}.$$

Alle folgenden Aussagen für Linksnebenklassen kann man damit in Aussagen für Rechtsnebenklassen übersetzen.

**Proposition:** Für alle  $g, g' \in G$  gilt

$$gH = g'H \iff g \in g'H \iff g' \in gH \iff gH \cap g'H \neq \emptyset.$$

Insbesondere ist  $G$  die disjunkte Vereinigung aller Linksnebenklassen von  $H$ .

**Proposition:** Für alle  $g \in G$  gilt  $|gH| = |H|$ .

**Bemerkung:** Die Menge  $G/H$  hat im allgemeinen keine natürliche Gruppenstruktur; vergleiche §3.10.

### 3.4 Ordnung, Index, Exponent

**Definition:** (a) Die *Ordnung* von  $G$  ist die Kardinalität  $|G|$ .

(b) Die *Ordnung* eines Elements  $g \in G$  ist die Kardinalität  $\text{ord}(g) := |\langle g \rangle|$ .

(c) Der *Index* einer Untergruppe  $H < G$  ist die Kardinalität  $[G : H] := |G/H|$ .

**Beispiel:** Es gilt  $[G : G] = 1$  und  $[G : 1] = |G|$ .

**Proposition:** Die Ordnung eines Elements  $g \in G$  ist die kleinste ganze Zahl  $n \geq 1$  mit  $g^n = 1$ , falls diese existiert, und andernfalls  $\infty$ .

**Satz:** (*Lagrange*) Für jede Untergruppe  $H < G$  gilt

$$|G| = [G : H] \cdot |H|.$$

**Folge 1:** In jeder endlichen Gruppe  $G$  sind  $|H|$  und  $[G : H]$  und  $\text{ord}(g)$  Teiler von  $|G|$ .

**Folge 2:** Jede endliche Gruppe  $G$  von Primzahlordnung ist zyklisch und besitzt nur die Untergruppen 1 und  $G$ .

**Satz:** Für alle Untergruppen  $K < H < G$  gilt

$$[G : K] = [G : H] \cdot [H : K].$$

**Definition:** Der *Exponent*  $\exp(G)$  von  $G$  ist die kleinste ganze Zahl  $n \geq 1$  mit der Eigenschaft  $\forall g \in G: g^n = 1$ , falls diese existiert, und andernfalls  $\infty$ .

Der Exponent ist also das kleinste gemeinsame Vielfache von  $\text{ord}(g)$  für alle  $g \in G$ .

**Folge 3:** Der Exponent jeder endlichen Gruppe teilt die Gruppenordnung.

**Bemerkung:** Der Exponent kann endlich sein, auch wenn die Gruppe selbst unendlich ist, zum Beispiel für die additive Gruppe eines unendlich-dimensionalen Vektorraums über  $\mathbb{F}_2$ .

**Proposition:** Jede Gruppe vom Exponenten 2 ist abelsch.

### 3.5 Homomorphismen

**Definition:** Ein *(Gruppen)-Homomorphismus*  $\varphi: G \rightarrow H$  ist eine Abbildung mit

$$\forall g, g' \in G: \varphi(gg') = \varphi(g)\varphi(g').$$

Dann heißen weiter

$$\begin{aligned} \text{Kern}(\varphi) &:= \{g \in G \mid \varphi(g) = 1_H\} && \text{der Kern von } \varphi, \\ \text{Bild}(\varphi) &:= \{\varphi(g) \mid g \in G\} && \text{das Bild von } \varphi. \end{aligned}$$

**Proposition:** Für jeden Homomorphismus  $\varphi: G \rightarrow H$  gilt

- (a)  $\varphi(1_G) = 1_H$ .
- (b)  $\forall g \in G: \varphi(g^{-1}) = \varphi(g)^{-1}$ .
- (c)  $\forall g \in G: \forall n \in \mathbb{Z}: \varphi(g^n) = \varphi(g)^n$ .
- (d)  $\text{Kern}(\varphi)$  ist eine Untergruppe von  $G$ .
- (e)  $\text{Bild}(\varphi)$  ist eine Untergruppe von  $H$ .
- (f)  $\varphi$  ist injektiv genau dann, wenn  $\text{Kern}(\varphi) = 1$  ist.
- (g)  $\varphi$  ist surjektiv genau dann, wenn  $\text{Bild}(\varphi) = H$  ist.

**Beispiel:** Die konstante Abbildung  $G \rightarrow H, g \mapsto 1_H$  ist ein Homomorphismus.

**Beispiel:** Die *identische Abbildung*  $\text{id}_G: G \rightarrow G, g \mapsto g$  ist ein Homomorphismus.

**Beispiel:** Für jedes  $g \in G$  ist die Abbildung  $\mathbb{Z} \rightarrow G, n \mapsto g^n$  ein Homomorphismus.

**Beispiel:** Ist  $G$  abelsch, so ist für jedes  $n \in \mathbb{Z}$  die Abbildung  $G \rightarrow G, g \mapsto g^n$  ein Homomorphismus. Ist umgekehrt  $g \mapsto g^{-1}$  ein Homomorphismus, so ist  $G$  abelsch.

**Beispiel:** Die Inklusion einer Untergruppe  $H \hookrightarrow G$  ist ein Homomorphismus.

**Proposition:** Die Komposition zweier Homomorphismen ist ein Homomorphismus.

### 3.6 Isomorphismen

**Definition:** Ein Homomorphismus  $\varphi: G \rightarrow H$ , für den ein beidseitiger *inverser Homomorphismus*  $\varphi^{-1}: H \rightarrow G$  existiert, heisst ein *Isomorphismus*, und wir schreiben dann  $\varphi: G \xrightarrow{\sim} H$ . Existiert ein Isomorphismus  $G \xrightarrow{\sim} H$ , so heissen  $G$  und  $H$  *isomorph* und wir schreiben  $G \cong H$ .

**Proposition:** Ein Homomorphismus ist ein Isomorphismus genau dann, wenn er bijektiv ist.

**Proposition:** Die Komposition zweier Isomorphismen ist ein Isomorphismus. Das Inverse eines Isomorphismus ist eindeutig bestimmt und selbst ein Isomorphismus. Isomorphie von Gruppen ist eine Äquivalenzrelation.

**Bemerkung:** Alle inneren Eigenschaften und Invarianten einer Gruppe sind invariant unter Isomorphismen, zum Beispiel die Kommutativität, die Ordnung, der Exponent.

**Proposition:** Jede zyklische Gruppe ist isomorph zur additiven Gruppe von  $\mathbb{Z}$  oder  $\mathbb{Z}/n\mathbb{Z}$  für eine eindeutige natürliche Zahl  $n > 0$ .

**Konvention:** Eine nicht näher bestimmte zyklische Gruppe der Ordnung  $n > 0$  wird bezeichnet mit  $Z_n$  oder  $C_n$ .

**Beispiel:** Die Homomorphismen bzw. Isomorphismen zwischen additiv geschriebenen abelschen Gruppen sind genau die  $\mathbb{Z}$ -Modul-Homomorphismen bzw. -Isomorphismen.

**Beispiel:** Die Abbildung  $x \mapsto \exp(x)$  ist ein Isomorphismus  $(\mathbb{R}, +) \rightarrow (\mathbb{R}^{>0}, \cdot)$ .

### 3.7 Abelsche Gruppen

**Klassifikationssatz:** Für jede endlich erzeugte abelsche Gruppe  $G$  existieren  $r, \ell \geq 0$  und Primzahlen  $p_i$  sowie Exponenten  $\nu_i \geq 1$ , so dass gilt

$$G \cong \mathbb{Z}^r \boxplus \bigoplus_{i=1}^{\ell} \mathbb{Z}/p_i^{\nu_i}\mathbb{Z}.$$

Dabei sind  $r$  und  $\ell$ , sowie die Paare  $(p_i, \nu_i)$  bis auf Vertauschung, eindeutig bestimmt.

**Bemerkung:** Die Zahl  $r$  heisst der „freie Rang“ von  $G$ . (Vergleiche §3.15.)

**Proposition:** Es gilt  $r = 0$  genau dann, wenn  $G$  endlich ist. In diesem Fall gilt

$$\begin{aligned} |G| &= p_1^{\nu_1} \cdots p_{\ell}^{\nu_{\ell}}, \\ \exp(G) &= \text{kgV}(p_1^{\nu_1}, \dots, p_{\ell}^{\nu_{\ell}}). \end{aligned}$$

### 3.8 Automorphismen

**Definition:** Ein Isomorphismus  $G \xrightarrow{\sim} G$  heisst ein *Automorphismus von  $G$* . Die Menge aller Automorphismen von  $G$  heisst die *Automorphismengruppe von  $G$*  und wird bezeichnet mit  $\text{Aut}(G)$ .

**Proposition:** Die Menge  $\text{Aut}(G)$  ist eine Gruppe bezüglich der Komposition von Abbildungen  $\circ$  und dem neutralen Element  $\text{id}_G$ .

**Beispiel:** Für alle  $r, n \geq 0$  gilt  $\text{Aut}((\mathbb{Z}/n\mathbb{Z})^r) \cong \text{GL}_r(\mathbb{Z}/n\mathbb{Z})$ .

**Definition:** Für alle  $g, x \in G$  kürzen wir ab

$${}^g x := gxg^{-1}$$

und nennen  $x$  und  ${}^g x$  *zueinander konjugiert*.

**Proposition:** Für alle  $g, h, x, y \in G$  gilt

$$\begin{aligned} {}^g({}^h x) &= {}^{gh}x \\ {}^g(xy) &= {}^g x {}^g y \\ {}^g(x^{-1}) &= ({}^g x)^{-1} \\ {}^g 1 &= 1 \\ {}^1 x &= x \end{aligned}$$

**Proposition:** Für jedes  $g \in G$  ist die Abbildung

$$\text{int}_g: G \rightarrow G, x \mapsto {}^g x$$

ein Automorphismus von  $G$ . Weiter ist die Abbildung

$$G \rightarrow \text{Aut}(G), g \mapsto \text{int}_g$$

ein Homomorphismus mit Kern  $Z(G)$ .

**Definition:** Die Abbildung  $\text{int}_g: G \rightarrow G$  heisst *Konjugation mit  $g$* . Ein Automorphismus der Form  $\text{int}_g$  heisst ein *innerer Automorphismus von  $G$* .

Für jedes  $g \in G$  und jede Teilmenge  $X \subset G$  schreiben wir analog

$${}^g X := gXg^{-1},$$

mit den entsprechenden Grundeigenschaften. Für jede Untergruppe  $H < G$  ist auch  ${}^g H$  eine solche.

### 3.9 Normalteiler

**Proposition:** Für jede Untergruppe  $N < G$  sind die folgenden Aussagen äquivalent:

- (a)  $\forall g \in G: {}^gN = N$
- (b)  $\forall g \in G: {}^gN \subset N$
- (c)  $\forall g \in G: gN = Ng$
- (d) Jede Linksnebenklasse von  $N$  ist gleichzeitig eine Rechtsnebenklasse von  $N$ .
- (e) Jede Rechtsnebenklasse von  $N$  ist gleichzeitig eine Linksnebenklasse von  $N$ .

**Definition:** Eine Untergruppe  $N$  mit den obigen Eigenschaften heisst *normal* oder ein *Normalteiler* von  $G$ . Die Aussage „ $N$  ist ein Normalteiler von  $G$ “ bezeichnet man kurz mit  $N \triangleleft G$  oder  $G \triangleright N$ .

**Vorsicht:** Aus  $K \triangleleft H$  und  $H \triangleleft G$  folgt im allgemeinen nicht  $K \triangleleft G$ . Vergleiche §4.2.

**Beispiel:** In einer abelschen Gruppe ist jede Untergruppe normal.

**Proposition:** Jede Untergruppe vom Index 2 ist normal.

**Beispiel:** Seien  $T$  eine Drehung um den Winkel  $\frac{2\pi}{n}$  und  $S$  eine Spiegelung in der Diedergruppe  $D_n$ . Dann ist  $\langle T \rangle = C_n$  vom Index 2 in  $D_n$  und folglich normal. Dagegen ist  $\langle S \rangle \cong C_2$  nur normal in  $D_n$  für  $n \leq 2$ . Für  $n = 4$  ist allerdings  $\langle S \rangle \triangleleft \langle S, T^2 \rangle \triangleleft D_n$ , weil der Index jeweils gleich 2 ist.

**Proposition:** Der Kern jedes Homomorphismus  $G \rightarrow H$  ist ein Normalteiler von  $G$ .

### 3.10 Faktorgruppen

Betrachte einen Normalteiler  $N \triangleleft G$ .

**Proposition:** Die Abbildung

$$G/N \times G/N \longrightarrow G/N, \quad (gN, g'N) \mapsto gNg'N = gg'N$$

ist wohldefiniert und induziert eine Gruppenstruktur auf  $G/N$  mit der Nebenklasse  $1N = N$  als neutrales Element, und die Abbildung

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

ist ein surjektiver Homomorphismus mit Kern  $N$ .

**Definition:** Die Gruppe  $G/N$  heisst die *Faktorgruppe* oder der *Quotient* von  $G$  nach  $N$ .

**Proposition:** (*Universelle Eigenschaft*) Für jede Gruppe  $H$  und jeden Homomorphismus  $\varphi: G \rightarrow H$  mit  $N \subset \text{Kern}(\varphi)$  existiert genau ein Homomorphismus  $\bar{\varphi}: G/N \rightarrow H$  mit  $\bar{\varphi} \circ \pi = \varphi$ , das heisst, so dass das folgende Diagramm kommutiert:

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

**Homomorphiesatz:** Jeder Homomorphismus  $\varphi: G \rightarrow H$  induziert einen Isomorphismus

$$G/\text{Kern}(\varphi) \xrightarrow{\sim} \text{Bild}(\varphi), \quad g\text{Kern}(\varphi) \mapsto \varphi(g).$$

**Erster Isomorphiesatz:** Für jede Untergruppe  $H < G$  ist  $H \cap N$  normal in  $H$ , und  $HN$  ist eine Untergruppe von  $G$ , und wir haben einen Isomorphismus

$$H/(H \cap N) \xrightarrow{\sim} HN/N, \quad h(H \cap N) \mapsto hN.$$

**Zweiter Isomorphiesatz:** (a) Die Untergruppen von  $G/N$  sind genau die Gruppen  $H/N$  für alle Untergruppen  $H < G$  mit  $N \subset H$ .

(b) Für solches  $H$  ist  $H/N$  normal in  $G/N$  genau dann, wenn  $H$  normal in  $G$  ist.

(c) In diesem Fall haben wir einen Isomorphismus

$$G/H \xrightarrow{\sim} (G/N)/(H/N), \quad gH \mapsto (gN)(H/N).$$

**Definition-Proposition:** Eine bijektive Abbildung einer Menge  $X$  in sich heisst eine *Permutation von  $X$* . Sei  $S(X)$  die Menge aller Permutationen von  $X$ . Dann ist  $(S(X), \circ, \text{id}_X)$  eine Gruppe, genannt die *symmetrische Gruppe der Menge  $X$* .

**Beispiel:** Sei  $k$  ein Körper und  $n \geq 0$ . Sei  $\mathbb{P}^n(k)$  die Menge aller eindimensionalen Untervektorräume des Raums der Spaltenvektoren  $k^{n+1}$ . Dann ist

$$\varphi: \text{GL}_{n+1}(k) \rightarrow S(\mathbb{P}^n(k)), \quad A \mapsto (U \mapsto AU)$$

ein Homomorphismus mit dem Kern  $k^\times I_{n+1}$ ; wir erhalten somit einen Isomorphismus der *projektiven linearen Gruppe*

$$\text{PGL}_{n+1}(k) := \text{GL}_{n+1}(k)/k^\times I_{n+1} \xrightarrow{\sim} \text{Bild}(\varphi) < S(\mathbb{P}^n(k)).$$

### 3.11 Operationen

**Definition:** Eine *Operation von links* oder kurz *Linksoperation* (englisch *left action*) von  $G$  auf einer Menge  $X$  ist eine Abbildung

$$\sigma: G \times X \rightarrow X, \quad (g, x) \mapsto \sigma(g, x)$$

mit den Eigenschaften:

$$\begin{aligned} \forall g, g' \in G \quad \forall x \in X: \quad \sigma(g, \sigma(g', x)) &= \sigma(gg', x) && \text{(Assoziativität)} \\ \forall x \in X: \quad \sigma(1_G, x) &= x && \text{(Neutrales Element)} \end{aligned}$$

**Proposition:** Jede Linksoperation  $\sigma$  von  $G$  auf  $X$  entspricht einem Homomorphismus  $\varphi: G \rightarrow S(X)$  vermöge  $\sigma(g, x) = \varphi(g)(x)$ , und umgekehrt.



**Definition:** Eine *Operation von rechts* oder kurz *Rechtsoperation* (englisch *right action*) von  $G$  auf einer Menge  $X$  ist eine Abbildung

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

mit den Eigenschaften:

$$\begin{aligned} \forall g, g' \in G \forall x \in X: \quad \rho(\rho(x, g), g') &= \rho(x, gg') && \text{(Assoziativität)} \\ \forall x \in X: \quad \rho(x, 1_G) &= x && \text{(Neutrales Element)} \end{aligned}$$

**Proposition:** Jede Linksoperation  $\sigma$  entspricht einer Rechtsoperation  $\rho$ , und umgekehrt, vermittelt der Gleichung  $\sigma(g, x) = \rho(x, g^{-1})$ .

**Beispiel:** (a) Die *Linkstranslation* auf  $G$  durch  $\sigma(g, x) := gx$  ist eine Linksoperation.

(b) Die *Rechtstranslation* auf  $G$  durch  $\rho(x, g) := xg$  ist eine Rechtsoperation. Die ihr zugeordnete Linksoperation ist  $\sigma(g, x) := xg^{-1}$ .

(c) Die *Konjugation* auf  $G$  durch  $\sigma(g, x) := {}^g x = gxg^{-1}$  ist eine Linksoperation. Die ihr zugeordnete Rechtsoperation ist  $\rho(x, g) := g^{-1}xg$ .

**Konvention:** Oft schreibt man auch eine allgemeine Linksoperation in der Form  $\sigma(g, x) = gx$  oder  $\sigma(g, x) = {}^g x$ , wenn Verwechslungen unwahrscheinlich erscheinen.

**Bemerkung:** Oft will man, dass eine Operation mit Zusatzstrukturen auf  $X$  verträglich ist, das heisst, dass für jedes  $g \in G$  die Abbildung  $X \rightarrow X, x \mapsto gx$  mit diesen Zusatzstrukturen verträglich ist, oder äquivalent dass der Homomorphismus  $G \rightarrow S(X)$  durch die Untergruppe aller strukturerehaltenden Automorphismen von  $X$  faktorisiert.

**Beispiel:** Sei  $H$  eine weitere Gruppe. Ein Homomorphismus  $\varphi: G \rightarrow \text{Aut}(H)$  entspricht einer Linksoperation  $\sigma$  von  $G$  auf der Menge  $H$  mit der weiteren Eigenschaft

$$\forall g \in G \forall h, h' \in H: \quad \sigma(g, hh') = \sigma(g, h)\sigma(g, h'),$$

genannt eine *Linksoperation von  $G$  auf der Gruppe  $H$* .

**Beispiel:** Sei  $V$  ein  $K$ -Vektorraum. Ein Homomorphismus  $\varphi: G \rightarrow \text{Aut}_K(V)$  entspricht einer Linksoperation  $\sigma$  von  $G$  auf der Menge  $V$  mit den weiteren Eigenschaften

$$\begin{aligned} \forall g \in G \forall v, v' \in V: \quad \sigma(g, v + v') &= \sigma(g, v) + \sigma(g, v'), \\ \forall g \in G \forall v \in V \forall \lambda \in K: \quad \sigma(g, \lambda v) &= \lambda \cdot \sigma(g, v). \end{aligned}$$

Eine solche Linksoperation heisst  *$K$ -linear* oder eine *Darstellung von  $G$  auf  $V$* .

### 3.12 Bahnen

Sei  $(g, x) \mapsto gx$  eine Linksoperation von  $G$  auf einer Menge  $X$ .

**Definition:** Die *Bahn* (englisch *orbit*) eines Elements  $x \in X$  ist die Teilmenge

$$O_G(x) := Gx := \{gx \mid g \in G\} \subset X.$$

**Proposition:** Für alle  $x, x' \in X$  gilt

$$Gx = Gx' \iff x \in Gx' \iff x' \in Gx \iff Gx \cap Gx' \neq \emptyset.$$

Insbesondere ist  $X$  die disjunkte Vereinigung aller Bahnen von  $G$ .

**Definition:** Der *Stabilisator* eines Elements  $x \in X$  ist die Untergruppe

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

**Proposition:** Für alle  $x \in X$  und  $g \in G$  gilt  $G_{gx} = {}^gG_x$ .

**Proposition:** Für jedes  $x \in X$  haben wir eine natürliche Bijektion

$$G/G_x \xrightarrow{\sim} Gx, \quad gG_x \mapsto gx.$$

Insbesondere gelten die *Bahnengleichungen*

$$\begin{aligned} [G : G_x] &= |Gx|, \\ |G| &= |G_x| \cdot |Gx|, \\ |X| &= \sum_{x \in \mathcal{R}} [G : G_x], \end{aligned}$$

für jedes Repräsentantensystem  $\mathcal{R} \subset X$  aller Bahnen von  $G$ .

**Definition:** Ein Element  $x \in X$  mit  $Gx = \{x\}$ , oder äquivalent  $G_x = G$ , heisst ein *Fixpunkt* von  $G$ . Die Menge aller Fixpunkte von  $G$  wird bezeichnet mit  $X^G$ .

**Beispiel-Definition:** Betrachte die Linksoperation von  $G$  auf sich durch Konjugation. Die Bahn eines Elements  $x \in G$

$$O_G(x) := \{{}^g x \mid g \in G\}$$

heisst die *Konjugationsklasse* von  $x$ . Der Stabilisator von  $x$  ist genau der Zentralisator  $\text{Cent}_G(x)$ . Die Menge der Fixpunkte von  $G$  ist das Zentrum  $Z(G)$ .

**Beispiel:** Die Konjugationsklassen in  $\text{GL}_n(K)$  sind genau die Ähnlichkeitsklassen invertierbarer Matrizen.

**Beispiel-Definition:** Betrachte die Linksoperation von  $G$  auf der Menge aller Untergruppen von  $G$  durch Konjugation  $(g, H) \mapsto {}^g H$ . Die Fixpunkte dieser Operation sind

genau die normalen Untergruppen von  $G$ . Der Stabilisator einer beliebigen Untergruppe  $H$  heisst der *Normalisator von  $H$* :

$$\text{Norm}_G(H) := \{g \in G \mid {}^g H = H\}.$$

**Definition:** Der *Zentralisator* einer Untergruppe  $H < G$  ist die Untergruppe

$$\text{Cent}_G(H) := \{g \in G \mid \forall h \in H: {}^g h = h\}.$$

**Proposition:** Für jedes  $H < G$  gilt  $H \triangleleft \text{Norm}_G(H)$  und  $\text{Cent}_G(H) \triangleleft \text{Norm}_G(H)$ .

**Beispiel:** Sei  $T < \text{GL}_n(K)$  die Untergruppe aller Diagonalmatrizen. Ist  $|K| > 2$ , so ist  $\text{Norm}_{\text{GL}_n(K)}(T)$  die Gruppe aller *monomialen* Matrizen, das heisst all solcher, die in jeder Zeile und jeder Spalte genau einen von Null verschiedenen Eintrag haben. Das sind genau die Matrizen, welche ein Produkt einer Diagonalmatrix mit einer Permutationsmatrix sind.

### 3.13 Eigenschaften von Operationen

**Definition:** Eine Operation von  $G$  auf  $X$  heisst

- (a) *transitiv*, wenn sie genau eine Bahn besitzt.  
Äquivalent: Es ist  $X \neq \emptyset$  und  $\forall x, x' \in X \exists g \in G: gx = x'$ .
- (b) *frei*, wenn gilt  $\forall x \in X: G_x = \{1\}$ .  
Äquivalent:  $\forall x \in X \forall g \in G \setminus \{1\}: gx \neq x$ .
- (c) *treu*, wenn gilt  $\bigcap_{x \in X} G_x = \{1\}$ .  
Äquivalent: Der entsprechende Homomorphismus  $G \rightarrow S(X)$  ist injektiv.
- (d) *trivial*, wenn gilt  $\forall g \in G \forall x \in X: gx = x$ .  
Äquivalent: Der entsprechende Homomorphismus  $G \rightarrow S(X)$  ist trivial.

**Beispiel:** Die Linkstranslation von  $G$  auf sich ist transitiv und frei und treu.

**Beispiel:** Für jede Untergruppe  $H < G$  haben wir eine transitive Linksoperation

$$G \times G/H \rightarrow G/H, (g, g'H) \mapsto gg'H.$$

Der Stabilisator der trivialen Nebenklasse ist in diesem Fall  $\text{Stab}_G(H) = H$ .

### 3.14 Symmetrische Gruppe

**Definition:** Die Gruppe  $S_n$  aller Permutationen von  $\{1, \dots, n\}$  heisst die *symmetrische Gruppe vom Grad  $n$* . Ihre Elemente bezeichnet man meist mit kleinen griechischen Buchstaben und schreibt ihre Operation klammernlos in der Form  $\sigma: i \mapsto \sigma i$ .

**Proposition:** Es gilt  $|S_n| = n!$ .

**Satz:** (*Cayley*) Jede endliche Gruppe ist isomorph zu einer Untergruppe einer  $S_n$ .

**Definition:** Ein Paar  $(i, j)$  mit  $1 \leq i < j \leq n$  und  $\sigma i > \sigma j$  heisst ein *Fehlstand* von  $\sigma$ . Die Zahl

$$\operatorname{sgn}(\sigma) := (-1)^{\text{Anzahl Fehlstände von } \sigma}$$

heisst das *Signum* oder die *Signatur* oder das *Vorzeichen* von  $\sigma$ . Eine Permutation mit  $\operatorname{sgn}(\sigma) = 1$  heisst *gerade*, eine mit  $\operatorname{sgn}(\sigma) = -1$  heisst *ungerade*.

**Proposition:** Die Abbildung  $\operatorname{sgn}: S_n \rightarrow \{\pm 1\}$  ist ein Gruppenhomomorphismus.

**Definition:** Der Kern von  $\operatorname{sgn}: S_n \rightarrow \{\pm 1\}$  heisst die *alternierende Gruppe*  $A_n$ .

**Proposition:** Für alle  $n \geq 2$  gilt  $[S_n : A_n] = 2$  und  $|A_n| = \frac{n!}{2}$ .

**Definition:** Für  $k \geq 1$  und paarweise verschiedene Ziffern  $i_1, \dots, i_k \in \{1, \dots, n\}$  bezeichnet  $(i_1 \dots i_k)$  die Permutation in  $S_n$  mit

$$i_1 \mapsto i_2 \mapsto \dots \mapsto i_k \mapsto i_1 \quad \text{und} \quad i \mapsto i \quad \text{für alle } i \notin \{i_1, \dots, i_k\}.$$

Eine solche Permutation heisst ein  *$k$ -Zykel*. Ein 2-Zykel heisst eine *Transposition*.

**Proposition:** (a) Zwei Zykel  $(i_1 \dots i_k)$  und  $(j_1 \dots j_\ell)$  sind gleich genau dann, wenn entweder  $k = \ell = 1$  ist, oder  $k = \ell > 1$  ist und ein  $1 \leq m \leq k$  existiert mit  $(j_1, \dots, j_\ell) = (i_{m+1}, \dots, i_k, i_1, \dots, i_m)$ .

(b) Für je zwei disjunkte Zykel  $\sigma$  und  $\tau$  gilt  $\sigma\tau = \tau\sigma$ .

(c) Für jeden Zykel gilt  $(i_1 \dots i_k)^{-1} = (i_k \dots i_1)$ .

(d) Für jeden Zykel und jedes  $\sigma \in S_n$  gilt  $\sigma(i_1 \dots i_k) = (\sigma i_1 \dots \sigma i_k)$ .

**Folge:** Je zwei  $k$ -Zykel in  $S_n$  sind konjugiert.

**Proposition:** Jede Permutation  $\sigma \in S_n$  ist ein Produkt disjunkter Zykel. Dabei kann man alle 1-Zykel weglassen, und danach sind die Faktoren bis auf die Reihenfolge eindeutig bestimmt. Sie entsprechen den Bahnen der Länge  $> 1$  von  $\langle \sigma \rangle$  auf  $\{1, \dots, n\}$ .

**Definition:** Eine Folge  $(d_1, d_2, \dots)$  in  $\mathbb{Z}^{\geq 0}$  mit  $\sum'_{k \geq 1} d_k k = n$  heisst eine (*ungeordnete*) *Partition von  $n$* . Die Anzahl  $p(n)$  solcher Partitionen heisst *Partitionsfunktion von  $n$* .

**Proposition:** Für jedes  $\sigma \in S_n$  sei  $d_k$  die Anzahl der Bahnen der Länge  $k$  von  $\langle \sigma \rangle$ . Dann induziert die Abbildung  $\sigma \mapsto (d_1, d_2, \dots)$  eine Bijektion von der Menge der

Konjugationsklassen von  $S_n$  auf die Menge der Partitionen von  $n$ . Die Anzahl der Konjugationsklassen von  $S_n$  ist also  $p(n)$ .

**Proposition:** Jede Permutation ist ein Produkt von Nachbartranspositionen, das heisst von Transpositionen der Form  $(i \ i+1)$  für gewisse  $1 \leq i < n$ .

**Folge:** Die  $S_n$  von allen Transpositionen erzeugt.

**Proposition:** Für jeden  $k$ -Zykel  $\sigma$  gilt  $\text{sgn}(\sigma) = (-1)^{k-1}$ .

**Proposition:** Die  $A_n$  ist von allen 3-Zykeln erzeugt.

**Spezialfall:** Die Untergruppen von  $S_n$  für  $n = 2, 3, 4$  sind bis auf Konjugation:

Untergruppe von $S_2$	isomorph zu	Ordnung	Anzahl Konjugierte
1	$C_1$	1	1 $\rightsquigarrow$ normal
$S_2$	$C_2$	2	1 $\rightsquigarrow$ normal

Untergruppe von $S_3$	isomorph zu	Ordnung	Anzahl Konjugierte
1	$C_1$	1	1 $\rightsquigarrow$ normal
$\langle(1 \ 2)\rangle$	$C_2$	2	3
$A_3$	$C_3$	3	1 $\rightsquigarrow$ normal
$S_3$	$D_3$	6	1 $\rightsquigarrow$ normal

Untergruppe von $S_4$	isomorph zu	Ordnung	Anzahl Konjugierte
1	$C_1$	1	1 $\rightsquigarrow$ normal
$\langle(1 \ 2)\rangle$	$C_2$	2	6
$\langle(1 \ 2)(3 \ 4)\rangle$	$C_2$	2	3
$\langle(1 \ 2 \ 3)\rangle$	$C_3$	3	4
$\langle(1 \ 2), (3 \ 4)\rangle$	$C_2 \times C_2$	4	3
$\langle(1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4)\rangle$	$C_2 \times C_2$	4	1 $\rightsquigarrow$ normal
$\langle(1 \ 2 \ 3 \ 4)\rangle$	$C_4$	4	3
$\langle(1 \ 2 \ 3), (1 \ 2)\rangle$	$S_3$	6	4
$\langle(1 \ 2 \ 3 \ 4), (1 \ 3)\rangle$	$D_4$	8	3
$A_4$	$A_4$	12	1 $\rightsquigarrow$ normal
$S_4$	$S_4$	24	1 $\rightsquigarrow$ normal

**Bemerkung:** Die Untergruppe

$$K := \langle(1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4)\rangle = \{\text{id}, (1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3)\}$$

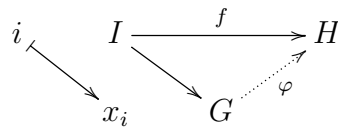
von  $S_4$  heisst die *Kleinsche Vierergruppe*. Sie ist normal und hat die Faktorgruppe  $S_4/K \cong S_3$ . Die drei Untergruppen der Ordnung 2 von  $K$  sind normal in  $K$ , aber nicht normal in  $S_4$ .

### 3.15 Freie Gruppen

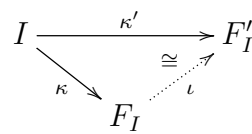
Betrachte eine Menge  $I$ .

**Definition:** Eine *freie abelsche Gruppe mit Erzeugenden  $x_i$  für alle  $i \in I$* , oder kurz eine *freie abelsche Gruppe über  $I$*  ist eine abelsche Gruppe  $F_I$  zusammen mit einer Abbildung  $\kappa: I \rightarrow F_I, i \mapsto x_i$ , so dass die folgende *universelle Eigenschaft* gilt:

Für jede abelsche Gruppe  $H$  und jede Abbildung  $f: I \rightarrow H$  existiert genau ein Gruppenhomomorphismus  $\varphi: F_I \rightarrow H$  mit  $\varphi \circ \kappa = f$ , das heisst, so dass das folgende Diagramm kommutiert:



**Proposition:** Eine freie abelsche Gruppe über  $I$  ist eindeutig bis auf eindeutige Isomorphie, mit anderen Worten: Ist sowohl  $(F_I, \kappa)$  wie  $(F'_I, \kappa')$  eine solche, so existiert ein eindeutiger Gruppenisomorphismus  $\iota: F_I \xrightarrow{\sim} F'_I$  mit  $\iota \circ \kappa = \kappa'$ , das heisst, so dass das folgende Diagramm kommutiert:



**Proposition:** Eine abelsche Gruppe  $F_I$  mit einer Abbildung  $\kappa: I \rightarrow F_I, i \mapsto x_i$  ist genau dann eine freie abelsche Gruppe über  $I$ , wenn sich jedes Element von  $G$  schreiben lässt in der Form  $\prod_{i \in I} x_i^{n_i}$  für eindeutige  $n_i \in \mathbb{Z}$ , von denen fast alle gleich 0 sind.

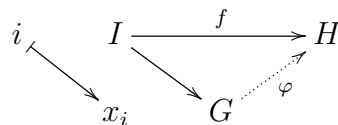
**Beispiel:** Der freie  $\mathbb{Z}$ -Modul

$$\mathbb{Z}^{(I)} := \{(a_i)_i \in \mathbb{Z}^I \mid \text{fast alle } a_i = 0\}$$

zusammen mit der Abbildung auf die Standardbasis  $i \mapsto e_i := (\delta_{ij})_j$  ist eine freie abelsche Gruppe über  $I$ .

**Definition:** Eine *freie Gruppe mit Erzeugenden  $x_i$  für alle  $i \in I$* , oder kurz eine *freie Gruppe über  $I$*  ist eine Gruppe  $F_I$  zusammen mit einer Abbildung  $\kappa: I \rightarrow F_I, i \mapsto x_i$ , so dass die folgende *universelle Eigenschaft* gilt:

Für jede Gruppe  $H$  und jede Abbildung  $f: I \rightarrow H$  existiert genau ein Gruppenhomomorphismus  $\varphi: F_I \rightarrow H$  mit  $\varphi \circ \kappa = f$ , das heisst, so dass das folgende Diagramm kommutiert:



**Konvention:** Eine freie Gruppe mit  $n$  Erzeugenden wird oft mit  $F_n$  bezeichnet.

**Proposition:** Eine freie Gruppe über  $I$  ist eindeutig bis auf eindeutige Isomorphie, mit anderen Worten: Ist sowohl  $(F_I, \kappa)$  wie  $(F'_I, \kappa')$  eine solche, so existiert ein eindeutiger Gruppenisomorphismus  $\iota: F_I \xrightarrow{\sim} F'_I$  mit  $\iota \circ \kappa = \kappa'$ , das heisst, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} I & \xrightarrow{\kappa'} & F'_I \\ & \searrow \kappa & \nearrow \cong \\ & & F_I \end{array}$$

**Satz:** Für jede Menge  $I$  existiert eine freie Gruppe über  $I$ .

**Konstruktion:** Sei  $\tilde{I}$  die Menge der Symbole  $i^\varepsilon$  für alle  $i \in I$  und alle  $\varepsilon \in \{\pm 1\}$ . Eine endliche Folge der Länge  $\geq 0$  in  $\tilde{I}$  heisst ein *Wort über dem Alphabet  $\tilde{I}$* . Wir schreiben ein Wort ohne Klammern als  $w = i_1^{\varepsilon_1} \dots i_n^{\varepsilon_n}$  und nennen die Zeichen  $i_\nu^{\varepsilon_\nu}$  die *Buchstaben von  $w$* . Sei  $W_{\tilde{I}}$  die Menge aller Wörter über  $\tilde{I}$ . Zusammensetzen zweier Wörter  $w, w'$  der Längen  $n, n'$  liefert ein Wort  $ww'$  der Länge  $n + n'$ . Diese Operation ist assoziativ, und das leere Wort ist ein beidseitiges neutrales Element.

Das Herausstreichen oder Einfügen zweier benachbarter Buchstaben der Form  $i^\varepsilon i^{-\varepsilon}$  heisst eine *elementare Transformation*. Wir nennen zwei Wörter  $w, w' \in W_{\tilde{I}}$  *äquivalent* und schreiben  $w \sim w'$ , wenn sie durch eine Folge elementarer Transformationen ineinander übergehen. Dies definiert eine Äquivalenzrelation auf  $W_{\tilde{I}}$ . Sei  $[w]$  die Äquivalenzklasse von  $w \in W_{\tilde{I}}$  und  $F_I := W_{\tilde{I}} / \sim$  die Menge aller Äquivalenzklassen.

**Proposition:** Es existiert eine eindeutige Gruppenstruktur auf  $F_I$ , so dass für alle  $w, w' \in W_{\tilde{I}}$  gilt  $[w][w'] = [ww']$ . Deren Einselement ist die Äquivalenzklasse des leeren Worts. Die Gruppe  $F_I$  zusammen mit der Abbildung  $I \rightarrow F_I, i \mapsto [i^1]$  ist eine freie Gruppe über  $I$ .

**Definition:** Ein Wort  $w \in W_{\tilde{I}}$ , welches kein zusammenhängendes Teilwort der Form  $i^\varepsilon i^{-\varepsilon}$  enthält, heisst *reduziert*.

**Proposition:** Jedes Wort  $w \in W_{\tilde{I}}$  ist äquivalent zu genau einem reduzierten Wort.

**Bemerkung:** Zu jedem gegebenen Wort findet man ein äquivalentes reduziertes Wort durch wiederholtes Herausstreichen benachbarter Buchstaben der Form  $i^\varepsilon i^{-\varepsilon}$ , bis dies nicht mehr möglich ist. Das resultierende reduzierte Wort ist dann der eindeutige reduzierte Repräsentant der Äquivalenzklasse. Mit diesem Algorithmus kann man entscheiden, ob zwei beliebige gegebene Wörter dasselbe Element von  $F_I$  darstellen.

### 3.16 Erzeugende und Relationen

Sei  $F_I := W_{\bar{I}} / \sim$  wie im vorigen Abschnitt, und sei  $J$  eine Teilmenge von  $W_{\bar{I}}$ .

**Definition:** Sei  $N_J \triangleleft F_I$  der von den Elementen  $g[w]g^{-1}$  für alle  $w \in J$  und  $g \in F_I$  erzeugte Normalteiler. Dann heisst  $F_I/N_J$  die *Gruppe mit Erzeugenden  $I$  und Relationen  $J$* . Im Fall  $I = \{1, \dots, n\}$  und  $J = \{w_1, \dots, w_m\}$  schreiben wir auch suggestiver

$$\langle x_1, \dots, x_n \mid w_1 = \dots = w_m = 1 \rangle := F_I/N_J.$$

Oder man listet die Relationen separat auf. Eine Relation der Form  $v = w$  ist äquivalent zu  $vw^{-1} = 1$ .

**Beispiele:**

$$\begin{aligned} \mathbb{Z} &\cong F_1 \cong \langle x \rangle \\ C_n &\cong \langle x \mid x^n = 1 \rangle \\ \mathbb{Z}^2 &\cong \langle x, y \mid xy = yx \rangle = \langle x, y \mid xyx^{-1}y^{-1} = 1 \rangle \\ D_n &\cong \langle a, b \mid a^n = b^2 = 1, bab^{-1} = a^{-1} \rangle \\ D_n &\cong \langle b, c \mid b^2 = c^2 = (bc)^n = 1 \rangle \\ D_\infty &:= \langle b, c \mid b^2 = c^2 = 1 \rangle \quad (\text{unendliche Diedergruppe}) \\ \{1\} &\cong \langle a, b \mid a^2b^3 = a^3b^4 = 1 \rangle \end{aligned}$$

**Bemerkung:** Das Rechnen in beliebigen durch Erzeugende und Relationen beschriebenen Gruppen bringt grosse algorithmische Probleme mit sich. Siehe zum Beispiel [https://en.wikipedia.org/wiki/Word\\_problem\\_for\\_groups](https://en.wikipedia.org/wiki/Word_problem_for_groups)

**Definition:** Betrachte Gruppen und Homomorphismen  $G_1 \xleftarrow{\varphi_1} G_{12} \xrightarrow{\varphi_2} G_2$ . Eine Gruppe  $G$  zusammen mit Homomorphismen  $G_1 \xrightarrow{\psi_1} G \xleftarrow{\psi_2} G_2$  heisst ein *Pushout* oder *amalgamiertes Produkt von  $G_1$  und  $G_2$  über  $G_{12}$* , wenn  $\psi_1 \circ \varphi_1 = \psi_2 \circ \varphi_2$  gilt und für jede Gruppe  $H$  und je zwei Homomorphismen  $G_1 \xrightarrow{\chi_1} H \xleftarrow{\chi_2} G_2$  mit  $\chi_1 \circ \varphi_1 = \chi_2 \circ \varphi_2$  genau ein Homomorphismus  $\chi: G \rightarrow H$  existiert mit  $\chi \circ \psi_1 = \chi_1$  und  $\chi \circ \psi_2 = \chi_2$ .

**Proposition:** Ein amalgamiertes Produkt existiert und ist eindeutig bis auf eindeutige Isomorphie.

**Proposition:** Das amalgamierte Produkt von  $G_1$  und  $G_2$  über  $G_{12}$  wird bezeichnet mit  $G_1 *_{G_{12}} G_2$ . Im Fall  $G_{12} = 1$  heisst es auch das *freie Produkt von  $G_1$  und  $G_2$*  und wird bezeichnet mit  $G_1 * G_2$ .

**Beispiel:** Für disjunkte Mengen  $I$  und  $J$  ist  $F_I * F_J \cong F_{I \sqcup J}$ .

**Beispiel:** Für alle  $m, n \geq 0$  ist  $F_m * F_n \cong F_{m+n}$ .

**Beispiel:** Für die Einbettungen der zyklischen Gruppen  $C_6 \hookrightarrow C_2 \hookrightarrow C_4$  gilt

$$\mathrm{SL}_2(\mathbb{Z}) \cong C_6 *_{C_2} C_4 \cong \langle R, S \mid R^3 = S^2, S^4 = 1 \rangle.$$

(Vergleiche [https://en.wikipedia.org/wiki/Modular\\_group](https://en.wikipedia.org/wiki/Modular_group))



## 4 Strukturtheorie von Gruppen

### 4.1 Einfache Gruppen

**Definition:** Eine Gruppe  $G$ , die nichttrivial ist und nur 1 und  $G$  als Normalteiler hat, heisst *einfach*.

**Proposition:** Eine abelsche Gruppe ist genau dann einfach, wenn sie zyklisch von Primzahlordnung ist.

**Satz:** Für jedes  $n \geq 5$  gilt:

- (a) Die Gruppe  $A_n$  ist einfach.
- (b) Die einzigen normalen Untergruppen von  $S_n$  sind 1 und  $A_n$  und  $S_n$ .

**Satz:** Für jeden Körper  $K$  und jedes  $n \geq 2$  ist die Gruppe

$$\mathrm{PSL}(n, K) := \mathrm{SL}_n(K) / \{\lambda I_n \mid \lambda \in K^\times, \lambda^n = 1\}$$

einfach, ausser für  $n = 2$  und  $|K| \leq 3$ .

(ohne Beweis)

**Bemerkung:** Für  $q := |K| < \infty$  ist

$$|\mathrm{PSL}(2, K)| = \begin{cases} q^3 - q & \text{für } q \text{ gerade,} \\ \frac{q^3 - q}{2} & \text{für } q \text{ ungerade.} \end{cases}$$

## 4.2 Subnormalreihen

**Definition:** (a) Eine Folge von Untergruppen  $1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_m = G$ , deren jede normal in der nächsten ist, heisst eine *Subnormalreihe von  $G$* .

(b) Eine Untergruppe, welche in einer Subnormalreihe von  $G$  auftaucht, heisst eine *subnormale Untergruppe von  $G$* .

**Definition:** Die *höheren Kommutatorgruppen von  $G$*  sind definiert durch  $G^{(0)} := G$  und  $G^{(i+1)} := [G^{(i)}, G^{(i)}]$  für alle  $i \geq 0$  und bilden eine Folge

$$G = G^{(0)} \triangleright \dots \triangleright G^{(i)} \triangleright G^{(i+1)} \triangleright \dots$$

Dabei sind alle Subfaktoren  $G^{(i)}/G^{(i+1)}$  abelsch.

**Proposition:** Betrachte eine Subnormalreihe  $1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_m = G$ .

(a) Für jede Untergruppe  $H < G$  ist  $1 = H \cap G_0 \triangleleft H \cap G_1 \triangleleft \dots \triangleleft H \cap G_m = H$  eine Subnormalreihe von  $H$ , und für alle  $1 \leq i \leq m$  gilt

$$\frac{H \cap G_i}{H \cap G_{i-1}} \cong \frac{(H \cap G_i)G_{i-1}}{G_{i-1}} < \frac{G_i}{G_{i-1}}.$$

(b) Für jeden Normalteiler  $N \triangleleft G$  ist  $1 = G_0N/N \triangleleft G_1N/N \triangleleft \dots \triangleleft G_mN/N = G/N$  eine Subnormalreihe von  $G/N$ , und für alle  $1 \leq i \leq m$  gilt

$$\frac{G_iN/N}{G_{i-1}N/N} \cong \frac{G_i/G_{i-1}}{(G_i \cap N)G_{i-1}/G_{i-1}} \ll \frac{G_i}{G_{i-1}}.$$

### 4.3 Kompositionsreihen (*nicht behandelt*)

**Definition:** Eine Subnormalreihe  $1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_m = G$ , bei der alle Subfaktoren  $G_i/G_{i-1}$  einfache Gruppen sind, heisst *Kompositionsreihe von  $G$* .

**Proposition:** Jede endliche Gruppe besitzt eine Kompositionsreihe.

**Beispiel:** Für jedes  $n \geq 5$  ist  $1 \triangleleft A_n \triangleleft S_n$  eine Kompositionsreihe von  $S_n$ . Eine Kompositionsreihe von  $S_4$  ist zum Beispiel, mit den jeweiligen Indizes:

$$1 \stackrel{2}{\triangleleft} \langle (1\ 2)(3\ 4) \rangle \stackrel{2}{\triangleleft} \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle \stackrel{3}{\triangleleft} A_4 \stackrel{2}{\triangleleft} S_4.$$

**Beispiel:** Die Gruppe  $\mathbb{Z}$  besitzt keine Kompositionsreihe.

**Beispiel:** Die Gruppe  $\mathbb{Z}/6\mathbb{Z}$  besitzt genau die zwei Kompositionsreihen

$$\begin{aligned} 0 &\stackrel{2}{\triangleleft} 3\mathbb{Z}/6\mathbb{Z} \stackrel{3}{\triangleleft} \mathbb{Z}/6\mathbb{Z}, \\ 0 &\stackrel{3}{\triangleleft} 2\mathbb{Z}/6\mathbb{Z} \stackrel{2}{\triangleleft} \mathbb{Z}/6\mathbb{Z}. \end{aligned}$$

**Definition:** Zwei Subnormalreihen  $1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_m = G$  und  $1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_n = G$  heissen *äquivalent*, wenn  $m = n$  ist und ein  $\sigma \in S_n$  existiert mit

$$\forall 1 \leq i \leq n: G_i/G_{i-1} \cong H_{\sigma_i}/H_{\sigma_i-1}.$$

**Satz:** (*Jordan-Hölder*) Je zwei Kompositionsreihen sind äquivalent.

**Bemerkung:** In gewissem Sinn kann man eine Kompositionsreihe als feinstmögliche Faktorisierung einer Gruppe ansehen. Die einfachen Subfaktoren spielen dann die Rolle der Primzahlen, und der Satz von Jordan-Hölder entspricht der eindeutigen Primfaktorzerlegung.

**Definition:** Eine Subnormalreihe, welche aus einer gegebenen Subnormalreihe durch Hinzufügen weiterer Terme entsteht, heisst eine *Verfeinerung*.

**Satz:** (*Schreier*) Je zwei Subnormalreihen besitzen äquivalente Verfeinerungen.

**Schmetterlingslemma:** (*Zassenhaus*) Für alle  $H' \triangleleft H < G$  und  $K' \triangleleft K < G$  gilt:

$$\begin{aligned} H'(H \cap K') &\triangleleft H'(H \cap K) < H, \\ (H' \cap K)K' &\triangleleft (H \cap K)K' < K, \text{ und} \\ \frac{H'(H \cap K)}{H'(H \cap K')} &\cong \frac{(H \cap K)K'}{(H' \cap K)K'}. \end{aligned}$$

## 4.4 Auflösbare Gruppen

**Definition:** Eine Gruppe  $G$  heisst *auflösbar*, wenn sie eine Subnormalreihe  $1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_m = G$  besitzt, bei der alle Subfaktoren  $G_i/G_{i-1}$  abelsch sind.

**Beispiel:** Jede abelsche Gruppe ist auflösbar.

**Beispiel:** Für jedes  $n \geq 1$  ist die Diedergruppe  $D_n$  auflösbar.

**Satz:** Die symmetrische Gruppe  $S_n$  ist auflösbar genau dann, wenn  $n \leq 4$  ist.

**Proposition:** Eine einfache Gruppe ist auflösbar genau dann, wenn sie abelsch ist.

**Beispiel:** Für jeden Ring  $R$  und jede natürliche Zahl  $n$  ist die Gruppe  $B$  der oberen Dreiecksmatrizen in  $\mathrm{GL}_n(R)$  auflösbar. Genauer ist für jedes  $1 \leq k \leq n$

$$U_k := \{(a_{ij})_{i,j} \in \mathrm{GL}_n(R) \mid a_{ij} = \delta_{ij} \text{ für alle } i > j - k\}$$

eine normale Untergruppe von  $B$ , und die Subnormalreihe  $1 = U_n \triangleleft \dots \triangleleft U_1 \triangleleft U_0 := B$  hat abelsche Subquotienten

$$U_k/U_{k+1} \cong \begin{cases} (R^\times)^n & \text{für } k = 0, \\ R^{n-k} & \text{für } 1 \leq k \leq n-1. \end{cases}$$

**Proposition:** (a) Jede Untergruppe und jede Faktorgruppe einer auflösbaren Gruppe ist auflösbar.

(b) Für jeden Normalteiler  $N \triangleleft G$  ist  $G$  auflösbar genau dann, wenn  $N$  und  $G/N$  auflösbar sind.

**Proposition:** Eine Gruppe ist auflösbar genau dann, wenn eine ihrer höheren Kommutatorgruppen gleich 1 ist.

## 4.5 Semidirekte Produkte

**Proposition-Definition:** Das kartesische Produkt von Gruppen  $G_1 \times \dots \times G_m$  mit komponentenweiser Multiplikation und dem Einselement  $(1, \dots, 1)$  ist eine Gruppe, genannt das (*äussere direkte*) *Produkt von  $G_1, \dots, G_m$* .

**Proposition:** Für Untergruppen  $G_1, \dots, G_m$  von  $G$  ist die Abbildung

$$G_1 \times \dots \times G_m \rightarrow G, (g_1, \dots, g_m) \mapsto g_1 \cdots g_m$$

ein Gruppenhomomorphismus genau dann, wenn gilt:

$$\forall i \neq j \forall g_i \in G_i \forall g_j \in G_j: g_i g_j = g_j g_i.$$

**Definition:** Ist die obige Abbildung ein injektiver Gruppenhomomorphismus, so heisst ihr Bild das (*innere*) *direkte Produkt von  $G_1, \dots, G_m$* .

**Beispiel:** Die Kleinsche Vierergruppe ist das innere direkte Produkt

$$\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle \text{ "=" } \langle (1\ 2)(3\ 4) \rangle \times \langle (1\ 3)(2\ 4) \rangle.$$

**Proposition-Definition:** Betrachte eine Linksoperation einer Gruppe  $H$  auf einer Gruppe  $N$ , geschrieben  $H \times N \rightarrow N, (h, n) \mapsto {}^h n$ . Dann ist das kartesische Produkt  $N \times H$  mit der Multiplikation

$$(n, h) \cdot (n', h') := (n \cdot {}^h n', hh')$$

und dem Einselement  $(1, 1)$  eine Gruppe, genannt das (*äussere*) *semidirekte Produkt von  $N$  und  $H$*  und geschrieben  $N \rtimes H$ . Diese besitzt  $N \times \{1\} \cong N$  als Normalteiler und die Faktorgruppe ist isomorph zu  $H$ .

**Proposition-Definition:** Seien  $H < G \triangleright N$  mit  $G = NH$  und  $N \cap H = 1$ . Wie üblich sei  ${}^h n := hnh^{-1}$ . Dann ist die Abbildung

$$N \rtimes H \rightarrow G, (n, h) \mapsto nh$$

ein Isomorphismus, und wir nennen  $G$  das (*innere*) *semidirekte Produkt von  $N$  und  $H$* . Als missbräuchliche Notation schreibt man dann auch oft  $G = N \rtimes H = H \rtimes N$ .

**Beispiel:** Für alle  $n \geq 1$  ist  $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes \{\pm 1\}$  vermöge der Operation

$$\{\pm 1\} \times \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, (i, k) \mapsto ik.$$

**Beispiel:** Für alle  $n \geq 2$  ist  $S_n = A_n \rtimes \langle (1\ 2) \rangle$ .

**Beispiel:** Für alle  $n \geq 6$  ist  $S_n = A_n \rtimes \langle (1\ 2)(3\ 4)(5\ 6) \rangle$ .

Diese beiden Beispiele zeigen, dass der Kofaktor  $H$  in einem inneren semidirekten Produkt durch den Normalteiler  $N$  im allgemeinen nicht eindeutig bestimmt ist, auch nicht bis auf Konjugation.

**Beispiel:** Die Gruppe aller abstandserhaltenden Bewegungen im  $\mathbb{R}^n$  ist das semidirekte Produkt des Normalteilers aller Translationen mit der orthogonalen Gruppe  $O(n)$ .

**Beispiel:** Für jeden Ring  $R$  und beliebige  $m, n \geq 0$  betrachte die Linksoperation von  $GL_m(R) \times GL_n(R)$  auf  $Mat_{m \times n}(R)$  durch  ${}^{(A,C)}B := ABC^{-1}$ . Dann haben wir einen Isomorphismus

$$\begin{aligned} Mat_{m \times n}(R) \rtimes (GL_m(R) \times GL_n(R)) &\xrightarrow{\sim} \begin{pmatrix} * & * \\ O & * \end{pmatrix} < GL_{m+n}(R), \\ (B, (A, C)) &\mapsto \begin{pmatrix} I_m & B \\ O & I_n \end{pmatrix} \begin{pmatrix} A & O \\ O & C \end{pmatrix} = \begin{pmatrix} A & BC \\ O & C \end{pmatrix}. \end{aligned}$$

## 4.6 $p$ -Gruppen

Sei  $p$  eine Primzahl.

**Definition:** Eine endliche Gruppe von  $p$ -Potenz-Ordnung heisst eine  $p$ -Gruppe.

**Satz:** Jede nichttriviale  $p$ -Gruppe hat ein nichttriviales Zentrum.

**Folge:** Jede  $p$ -Gruppe ist auflösbar.

**Proposition:** Jede echte Untergruppe einer  $p$ -Gruppe ist echt in ihrem Normalisator enthalten.

**Beispiel:** Jede Gruppe der Ordnung  $p^2$  ist abelsch.

**Beispiel:** Es gibt genau 5 Isomorphieklassen von Gruppen der Ordnung  $p^3$ . Darunter sind die abelschen die Isomorphieklassen von

$$\mathbb{Z}/p^3\mathbb{Z} \quad \text{und} \quad \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \quad \text{und} \quad (\mathbb{Z}/p\mathbb{Z})^3.$$

Im Fall  $p > 2$  sind die nichtabelschen die Isomorphieklassen der semidirekten Produkte

$$\begin{aligned} \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z} &\text{ mit } {}^ab := (1 + pa)b \text{ für alle } a \in \mathbb{Z}/p\mathbb{Z} \text{ und } b \in \mathbb{Z}/p^2\mathbb{Z}, \\ (\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z} &\text{ mit } {}^a(b, c) := (b + ac, c) \text{ für alle } a \in \mathbb{Z}/p\mathbb{Z} \text{ und } (b, c) \in (\mathbb{Z}/p\mathbb{Z})^2. \end{aligned}$$

Im Fall  $p = 2$  sind die nichtabelschen die Isomorphieklassen der Diedergruppe  $D_4$  sowie der Quaternionengruppe

$$Q := \{\pm 1, \pm i, \pm j, \pm k\}$$

mit  $i^2 = j^2 = k^2 = -1$  und  $ij = k = -ji$  und  $jk = i = -kj$  und  $ki = j = -ik$ .

**Bemerkung:** Die Quaternionengruppe ist kein semidirektes Produkt von echten Untergruppen.

## 4.7 Sylowsätze

Sei  $G$  eine endliche Gruppe und  $p$  ein Primteiler der Gruppenordnung  $|G|$ . Schreibe

$$|G| = p^k m \quad \text{für } k, m \geq 1 \text{ mit } p \nmid m.$$

**Definition:** Jede Untergruppe von  $G$  der Ordnung  $p^k$  heisst eine  $p$ -Sylowuntergruppe oder  $p$ -Sylowgruppe von  $G$ . Sei  $\text{Syl}_p(G)$  die Menge aller  $p$ -Sylowgruppen von  $G$ .

**Satz:** (Sylowsätze)

- (a) Es existiert eine  $p$ -Sylowgruppe von  $G$ .
- (b) Jede  $p$ -Untergruppe von  $G$  ist in einer  $p$ -Sylowgruppe von  $G$  enthalten.
- (c) Alle  $p$ -Sylowgruppen von  $G$  sind zueinander konjugiert.
- (d) Die Anzahl der  $p$ -Sylowgruppen von  $G$  ist  $\equiv 1 \pmod{p}$  und ein Teiler von  $m$ .

**Folge:** (e) Die Gruppe  $G$  besitzt ein Element der Ordnung  $p$ .

## 4.8 Kleine endliche Gruppen

**Proposition:** Jede Gruppe der Ordnung  $pq$  oder  $p^2q$  oder  $pqr$  für Primzahlen  $p, q, r$  ist auflösbar.

**Satz:** (Burnside) Jede Gruppe der Ordnung  $p^a q^b$  für Primzahlen  $p, q$  ist auflösbar. (ohne Beweis)

**Lemma:** Eine nichtabelsche einfache Gruppe besitzt keine Untergruppe vom Index 2, 3, oder 4.

**Proposition:** Jede Gruppe der Ordnung  $< 60$  ist auflösbar.

**Lemma:** Jede nichtabelsche einfache Gruppe mit einer Untergruppe vom Index 5 ist isomorph zur  $A_5$ .

**Proposition:** Jede einfache Gruppe der Ordnung 60 ist isomorph zu  $A_5$ .

## 4.9 Klassifikation

Das Klassifikationsproblem der endlichen Gruppen ist die Aufgabe, alle endlichen Gruppen bis auf Isomorphie explizit zu beschreiben.

Hat eine endliche Gruppe  $G$  einen nichttrivialen echten Normalteiler  $N$ , so reduziert sich diese Aufgabe darauf, die Gruppen  $N$  und  $G/N$  sowie alle Möglichkeiten, die Gruppe  $G$  als *Erweiterung von  $G/N$  und  $N$*  zu konstruieren, zu beschreiben. Hat man das Erweiterungsproblem im Griff, so reduziert sich das allgemeine Problem also durch Induktion auf die Klassifikation aller endlichen einfachen Gruppen.

**Satz:** (*Feit-Thompson 1963*) Jede endliche Gruppe ungerader Ordnung ist auflösbar. (Beweis etwa 270 Seiten)

Jede nichtabelsche endliche einfache Gruppe besitzt daher ein Element der Ordnung 2, genannt eine *Involution*. Als Programm zur Lösung des Klassifikationsproblem schlug der Gruppentheoretiker Richard Brauer vor, nichtabelsche endliche einfache Gruppen vermittle ihrer Involutionen, derer Zentralisatoren, und jeder Menge weiterer davon abgeleiteter Untergruppen zu studieren. Dabei ist von Nutzen:

**Proposition:** Je zwei Involutionen erzeugen zusammen eine Diedergruppe.

Die Klassifikation aller endlichen einfachen Gruppen wurde Anfang der 1980er Jahre im wesentlichen abgeschlossen. Demnach sind die endlichen einfachen Gruppen bis auf Isomorphie genau:

- (a) die zyklischen Gruppen  $C_p$  von Primzahlordnung  $p$ ,
- (b) die alternierenden Gruppen  $A_n$  für  $n \geq 5$ ,
- (c) die einfachen Gruppen *vom Lie-Typ*, konstruiert als Matrixgruppen über endlichen Körpern  $K$  wie zum Beispiel  $\text{PSL}(n, K)$ ,
- (d) sowie 26 weitere *sporadische einfache Gruppen* verschiedener Ordnungen von  $2^4 \cdot 3^2 \cdot 5 \cdot 11 = 7920$  bis

$$\begin{aligned} & 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ & = 808017424794512875886459904961710757005754368000000000. \end{aligned}$$

Die kleinsten nichtabelschen einfachen Gruppen haben die Ordnungen 60, 168, 360, 504, 660, 1092, ... Vergleiche

[http://en.wikipedia.org/wiki/List\\_of\\_finite\\_simple\\_groups](http://en.wikipedia.org/wiki/List_of_finite_simple_groups).



## 5 Körper

Körpertheorie ist das Studium von Körpererweiterungen, insbesondere ihre Konstruktion, Klassifikation, und das Lösen von Gleichungen darin.

### 5.1 Körpererweiterungen

**Definition:** Ein Unterring  $K$  eines Körpers  $L$ , welcher selbst ein Körper ist, heisst ein *Unterkörper von  $L$* . Dann heisst  $L$  ein *Oberkörper von  $K$* , und wir sprechen von der *Körpererweiterung  $L/K$* . Für Körpererweiterungen  $M/L/K$  nennen wir  $L$  einen *Zwischenkörper von  $M/K$* . Eine endliche oder unendliche Folge von Körpererweiterungen  $\dots/K_{i+1}/K_i/K_{i-1}/\dots$  heisst ein *Körperturm*.

**Bemerkung:** Die Notation  $L/K$  bezeichnet hier kein neues mathematisches Objekt wie etwa einen Faktorraum, sondern dient nur als sprachliche Abkürzung.

**Proposition:** Jeder Körper  $K$  besitzt einen eindeutigen kleinsten Unterkörper. Dieser ist entweder isomorph zu  $\mathbb{Q}$  oder zu  $\mathbb{F}_p$  für eine eindeutige Primzahl  $p$ .

**Definition:** Dieser Unterkörper heisst der *Primkörper von  $K$* , und die Zahl

$$\text{char}(K) := \begin{cases} 0 & \text{falls der Primkörper } \mathbb{Q} \text{ ist,} \\ p & \text{falls der Primkörper } \mathbb{F}_p \text{ ist,} \end{cases}$$

heisst die *Charakteristik von  $K$* .

**Proposition:** Jeder Körperhomomorphismus  $K \rightarrow L$  ist injektiv, und wenn einer existiert, so ist  $\text{char}(K) = \text{char}(L)$ .

**Bemerkung:** Durch einen Körperhomomorphismus  $K \hookrightarrow L$  kann man  $K$  mit einem Unterkörper von  $L$  identifizieren. Man sollte dies aber nur dann tun, wenn der Homomorphismus später nicht mehr abgeändert wird.

**Proposition:** Für jede Körpererweiterung  $L/K$  und jede Teilmenge  $A \subset L$  existiert ein eindeutiger kleinster Zwischenkörper von  $L/K$ , welcher  $A$  enthält. Dieser ist der Quotientenkörper des von  $A$  über  $K$  erzeugten Unterrings  $K[A]$ , besteht also aus den Elementen  $\frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)}$  für alle  $n \geq 0$ , alle  $a_1, \dots, a_n \in A$ , und alle  $f, g \in K[X_1, \dots, X_n]$  mit  $g(a_1, \dots, a_n) \neq 0$ .

**Definition:** Dieser Zwischenkörper heisst *von  $A$  über  $K$  erzeugt* und wird bezeichnet mit  $K(A)$ . Für endlich viele Elemente  $a_1, \dots, a_n \in L$  schreiben wir auch  $K(a_1, \dots, a_n) := K(\{a_1, \dots, a_n\})$  und nennen diesen Körper *endlich erzeugt über  $K$* . Eine Körpererweiterung der Form  $K(a)/K$  nennen wir *einfach*.

**Proposition:** (a) Für alle  $a \in K$  gilt  $K(a) = K$ .

(b) Für alle  $0 \leq m \leq n$  gilt  $K(a_1, \dots, a_n) = K(a_1, \dots, a_m)(a_{m+1}, \dots, a_n)$ .

**Beispiel:** Der Körper  $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$ .

## 5.2 Körpergrad

**Definition:** Der *Grad* einer Körpererweiterung  $L/K$  ist die Zahl

$$[L/K] := \dim_K(L) \in \mathbb{Z}^{\geq 1} \cup \{\infty\}.$$

Eine Körpererweiterung mit  $[L/K] < \infty$  heisst *endlich*. Eine Körpererweiterung vom Grad 2 heisst *quadratisch*, vom Grad 3 *kubisch*, vom Grad 4 *biquadratisch*.

**Proposition:** Es ist  $[L/K] = 1$  genau dann, wenn  $L = K$  ist.

**Beispiel:** Es ist  $[\mathbb{C}/\mathbb{R}] = 2$  und  $[\mathbb{R}/\mathbb{Q}] = \infty$ .

**Proposition:** Für jeden Körperturm  $M/L/K$  gilt

$$[M/K] = [M/L] \cdot [L/K].$$

Insbesondere ist  $M/K$  endlich genau dann, wenn  $M/L$  und  $L/K$  endlich sind.

**Proposition:** Jede endliche Körpererweiterung  $L/K$  vom Primzahlgrad ist einfach, und für jedes  $a \in L \setminus K$  gilt  $L = K(a)$ .

**Proposition:** Für jede Körpererweiterung  $L/K$  vom Grad 2 mit  $\text{char}(K) \neq 2$  existiert ein  $a \in L$  mit  $L = K(a)$  und  $b := a^2 \in K$ . Wir können dieses  $a$  als *eine Quadratwurzel aus  $b$*  ansehen.

**Vorsicht:** Die Notation  $a = \sqrt{b}$  ist sehr gefährlich wegen fehlender Eindeutigkeit! Nur in  $\mathbb{R}^{\geq 0}$  sind Wurzeln eindeutig definiert.

**Proposition:** Sei  $L/K$  eine Körpererweiterung, und sei  $R \subset L$  ein Unterring mit  $K \subset R$  und  $\dim_K(R) < \infty$ . Dann ist  $R$  ein Zwischenkörper.

**Definition:** Für je zwei Zwischenkörper  $K_1$  und  $K_2$  einer Körpererweiterung  $L/K$  bezeichnen wir den von  $K_1 \cup K_2$  erzeugten Zwischenkörper mit  $K_1 K_2$ .

**Proposition:** In dieser Situation gilt, falls  $K_1/K$  endlich ist,

$$\begin{aligned} K_1 K_2 &= \left\{ \sum_i x_i y_i \mid x_i \in K_1, y_i \in K_2 \right\}, \\ [K_1 K_2 / K_2] &\leq [K_1 / K] \quad \text{und} \\ [K_1 K_2 / K] &\leq [K_1 / K] \cdot [K_2 / K]. \end{aligned}$$

**Definition:** Gilt  $[K_1 K_2 / K] = [K_1 / K] \cdot [K_2 / K] < \infty$ , so heissen  $K_1$  und  $K_2$  *linear disjunkt über  $K$* .

**Vorsicht:** Dies impliziert  $K_1 \cap K_2 = K$ , ist aber nicht äquivalent dazu.

**Beispiel:**  $\mathbb{Q}(i)$  und  $\mathbb{Q}(\sqrt{2})$  sind quadratisch und linear disjunkt über  $\mathbb{Q}$ .

**Beispiel:**  $\mathbb{Q}(\sqrt[3]{2})$  und  $\mathbb{Q}(\sqrt[3]{2} e^{2\pi i/3})$  sind vom Grad 3 und nicht linear disjunkt über  $\mathbb{Q}$ .

### 5.3 Einfache Körpererweiterungen

Betrachte eine Körpererweiterung  $L/K$  und ein Element  $a \in L$ .

**Definition:** Existiert ein Polynom  $f \in K[X] \setminus \{0\}$  mit  $f(a) = 0$ , so heisst  $a$  *algebraisch über  $K$* , andernfalls *transzendent über  $K$* .

**Definition:** Eine komplexe Zahl heisst *algebraisch* bzw. *transzendent*, wenn sie algebraisch bzw. transzendent über  $\mathbb{Q}$  ist.

**Beispiel:** Die Zahlen  $i$  und  $\sqrt{2}$  sind algebraisch.

**Satz:** Die reellen Zahlen  $e$  und  $\pi$  sind transzendent. (ohne Beweis)

Betrachte nun den Auswertungshomomorphismus

$$\text{eval}_a: K[X] \rightarrow K[a] \subset L, f \mapsto f(a).$$

**Proposition:** Es sind äquivalent:

- (a)  $a$  ist algebraisch über  $K$ .
- (b)  $\text{Kern}(\text{eval}_a) \neq (0)$ .
- (c)  $\dim_K(K[a]) < \infty$ .
- (d)  $[K(a)/K] < \infty$ .

**Proposition:** Es sind äquivalent:

- (a)  $a$  ist transzendent über  $K$ .
- (b)  $\text{eval}_a$  ist injektiv.
- (c)  $\text{eval}_a$  induziert einen Isomorphismus  $K(X) \xrightarrow{\sim} K(a)$ .
- (d)  $[K(a)/K] = \infty$ .

**Bemerkung:** Insbesondere sind  $\mathbb{Q}(e)$  und  $\mathbb{Q}(\pi)$  isomorph zu  $\mathbb{Q}(X)$ .

**Proposition:** Sei  $a$  algebraisch über  $K$ . Dann gilt:

- (a)  $\text{Kern}(\text{eval}_a) = (m_a)$  für genau ein normiertes Polynom  $m_a = m_{a,K} \in K[X]$ .
- (b)  $m_a$  ist das eindeutige normierte Polynom von minimalem Grad in  $\text{Kern}(\text{eval}_a)$ .
- (c)  $m_a$  ist das eindeutige irreduzible normierte Polynom  $f \in K[X]$  mit  $f(a) = 0$ .
- (d)  $\text{eval}_a$  induziert einen Isomorphismus

$$K[X]/(m_a) \xrightarrow{\sim} K(a), f + (m_a) \mapsto f(a).$$

- (e)  $[K(a)/K] = \deg(m_a)$ .

**Definition:** Das Polynom  $m_a = m_{a,K}$  heisst das *Minimalpolynom von  $a$  über  $K$* . Sein Grad heisst auch der *Grad von  $a$  über  $K$* .

**Beispiel:** Die reelle Zahl  $\omega := \cos \frac{\pi}{9}$  ist algebraisch mit  $m_{\omega, \mathbb{Q}}(X) = X^3 - \frac{3}{4}X - \frac{1}{8}$  und  $[\mathbb{Q}(\omega)/\mathbb{Q}] = 3$ .

**Bemerkung:** Im Fall  $n := [K(a)/K] < \infty$  ist jedes Element von  $K(a)$  gleich  $f(a)$  für ein eindeutiges Polynom  $f \in K[X]$  vom Grad  $< n$ . Die Summe zweier solcher Elemente berechnet sich direkt, das Produkt durch Division mit Rest als  $f(a)g(a) = r(a)$  für  $q, r \in K[X]$  mit  $fg = qm_a + r$  und  $\deg(r) < n$ . Ist  $f(a) \neq 0$ , so gilt  $\text{ggT}(f, m_a) \sim 1$  in  $K[X]$ . Mit dem euklidischen Algorithmus findet man dann Polynome  $u, v \in K[X]$  mit  $uf + vm_a = 1$ . Auswerten in  $a$  liefert dann die Gleichung  $u(a)f(a) = 1$ , also  $f(a)^{-1} = u(a)$ .

**Beispiel:** Für  $a := \sqrt[3]{2}$  ist  $m_{a, \mathbb{Q}}(X) = X^3 - 2$  und  $\frac{1}{1+a} = \frac{1-a+a^2}{3}$ .

## 5.4 Algebraische Körpererweiterungen

**Definition:** Eine Körpererweiterung  $L/K$  heisst *algebraisch*, wenn jedes Element von  $L$  algebraisch über  $K$  ist; andernfalls heisst sie *transzendent*.

**Proposition 1:** Für jeden Körperturm  $M/L/K$  und jedes Element  $a \in M$  gilt: Ist  $a$  algebraisch über  $K$ , so ist es auch algebraisch über  $L$ .

**Proposition 2:** Sind  $a_1, \dots, a_n$  algebraisch über  $K$ , so ist  $K(a_1, \dots, a_n)/K$  endlich.

**Proposition 3:** Ist  $L/K$  endlich, so ist  $L/K$  algebraisch.

**Proposition 4:** Eine Körpererweiterung ist endlich genau dann, wenn sie endlich erzeugt und algebraisch ist.

**Proposition 5:** Für  $L = K(A)$  ist  $L/K$  algebraisch genau dann, wenn jedes Element von  $A$  algebraisch über  $K$  ist.

**Bemerkung:** Dies bedeutet, dass für alle über  $K$  algebraischen Elemente  $a, b \in L$  auch  $a \pm b$  und  $ab$  sowie, falls definiert,  $a/b$  algebraisch über  $K$  sind.

**Beispiel:** Die reelle Zahl  $a := \sqrt{2} + \sqrt{3}$  ist algebraisch. Ihr Minimalpolynom ist  $m_{a, \mathbb{Q}}(X) = X^4 - 10X^2 + 1$ , und es ist  $[\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}] = 4$ .

**Proposition 6:** Für jeden Körperturm  $M/L/K$  und jedes Element  $a \in M$  gilt: Ist  $L/K$  algebraisch, und ist  $a$  algebraisch über  $L$ , so ist  $a$  auch algebraisch über  $K$ .

**Proposition 7:** Für jeden Körperturm  $M/L/K$  ist  $M/K$  algebraisch genau dann, wenn  $M/L$  und  $L/K$  algebraisch sind.

**Beispiel:** Die reelle Zahl  $a := \sqrt{1 + \sqrt{2}}$  ist algebraisch über  $\mathbb{Q}(\sqrt{2})$ , also algebraisch über  $\mathbb{Q}$ . Ihr Minimalpolynom ist  $m_{a, \mathbb{Q}}(X) = X^4 - 2X^2 - 1$ .

## 5.5 Konstruktionen mit Zirkel und Lineal

In der euklidischen Ebene erlauben wir die folgenden Konstruktionen:

- (a) Mit dem Lineal die Gerade durch zwei verschiedene gegebene Punkte zeichnen.
- (b) Mit dem Zirkel den Abstand zweier verschiedener gegebener Punkte aufnehmen und den Kreis mit diesem Radius um einen gegebenen Punkt zeichnen.
- (c) Einen Schnittpunkt zweier Geraden oder Kreise bilden bzw. auswählen.

Für jede Menge  $A$  von Punkten sei  $\text{Kons}(A)$  die Menge aller Schnittpunkte, die man durch iterierte Anwendung dieser Operationen aus  $A$  konstruieren kann. Die Abstände  $d(P, Q)$  für alle Punkte  $P, Q \in \text{Kons}(A)$  heißen die *aus  $A$  konstruierbaren Längen*. Die Winkel  $\sphericalangle PQR$  für alle paarweise verschiedenen Punkte  $P, Q, R \in \text{Kons}(A)$  heißen die *aus  $A$  konstruierbaren Winkel*. Unser Ziel ist es, die Menge  $\text{Kons}(A)$  und die Menge aller aus  $A$  konstruierbaren Längen bzw. Winkel zu beschreiben.

Um dieses geometrische Problem zu algebraisieren, identifizieren wir die euklidische Ebene mit  $\mathbb{C}$  mit dem üblichen Abstand  $d(P, Q) := |P - Q|$ . Damit man überhaupt neue Punkte konstruieren kann, nehmen wir an, dass  $A$  mindestens zwei verschiedene Punkte enthält. Durch Translation, Drehung und Streckung reduzieren wir uns dann darauf, dass  $A$  mindestens die Punkte 0 und 1 enthält.

**Satz:** Dann ist  $\text{Kons}(A)$  der eindeutige kleinste Unterkörper  $K \subset \mathbb{C}$  mit den Eigenschaften

- (a)  $A \subset K$ .
- (b)  $\forall z \in K: \bar{z} \in K$ .
- (c)  $\forall z \in \mathbb{C}: z^2 \in K \longrightarrow z \in K$ .

Weiter gilt:

- (d) Die aus  $A$  konstruierbaren Längen sind genau die Zahlen in  $\text{Kons}(A) \cap \mathbb{R}^{\geq 0}$ .
- (e) Die aus  $A$  konstruierbaren Winkel sind genau die  $\alpha \in \mathbb{R}$  mit  $\cos \alpha \in \text{Kons}(A)$ .

**Satz:** Setze  $\bar{A} := \{\bar{a} \mid a \in A\}$ . Dann ist  $\text{Kons}(A)$  die Vereinigung aller Körper  $L \subset \mathbb{C}$ , für die ein Körperturm der Form

$$L = K_n / \dots / K_1 / K_0 = \mathbb{Q}(A \cup \bar{A})$$

existiert mit  $[K_i / K_{i-1}] = 2$  für alle  $1 \leq i \leq n$ .

**Folge:** Jedes Element von  $\text{Kons}(A)$  ist algebraisch über  $\mathbb{Q}(A \cup \bar{A})$  und sein Grad über  $\mathbb{Q}(A \cup \bar{A})$  ist eine Zweierpotenz.

**Satz:** (*Verdoppelung des Würfels*) Es gibt kein endliches Verfahren mit Zirkel und Lineal, um die Zahl  $\sqrt[3]{2}$  zu konstruieren.

**Satz:** (*Dreiteilung des Winkels*) Es gibt kein endliches Verfahren mit Zirkel und Lineal, um aus einem beliebigen Winkel  $\alpha$  den Winkel  $\frac{\alpha}{3}$  zu konstruieren.

**Satz:** (*Quadratur des Kreises*) Es gibt kein endliches Verfahren mit Zirkel und Lineal, um aus einem beliebigen Kreis mit Radius  $r$  den Kreisinhalt  $\pi r^2$  zu konstruieren.

## 5.6 Transzendente Körpererweiterungen

Betrachte eine Körpererweiterung  $L/K$ .

**Definition:** Eine Kollektion paarweise verschiedener Elemente  $A = \{a_\nu \mid \nu \in N\} \subset L$  heisst *algebraisch abhängig über  $K$* , wenn ein Polynom  $f \in K[(X_\nu)_{\nu \in N}] \setminus \{0\}$  existiert mit  $f((a_\nu)_\nu) = 0$ . Andernfalls heisst sie *algebraisch unabhängig über  $K$* .

**Proposition:** Für jede Teilmenge  $A \subset L$  sind äquivalent:

- (a)  $A$  ist algebraisch unabhängig über  $K$ , und  $L/K(A)$  ist algebraisch.
- (b)  $A$  ist eine maximale über  $K$  algebraisch unabhängige Teilmenge.
- (c)  $A$  ist eine minimale Teilmenge von  $L$ , so dass  $L/K(A)$  algebraisch ist.

**Definition:** Eine solche Teilmenge  $A \subset L$  heisst *Transzendenzbasis von  $L/K$* .

**Proposition:** (*Austauschsatz*) Für je zwei Transzendenzbasen  $A$  und  $B$  von  $L/K$  und jedes Element  $b \in B \setminus A$  existiert ein  $a \in A \setminus B$ , so dass  $(A \setminus \{a\}) \cup \{b\}$  eine Transzendenzbasis von  $L/K$  ist.

**Satz:** Es existiert eine Transzendenzbasis, und je zwei Transzendenzbasen von  $L/K$  haben dieselbe Kardinalität.

**Definition:** Diese Kardinalität heisst der *Transzendenzgrad von  $L/K$*  und wird bezeichnet mit  $\text{trdeg}_{L/K}$ .

**Proposition:** Es ist  $L/K$  algebraisch genau dann, wenn  $\text{trdeg}_{L/K} = 0$  ist.

**Proposition:** Für jede endlich erzeugte Körpererweiterung  $L = K(a_1, \dots, a_n)/K$  gilt  $\text{trdeg}_{L/K} \leq n < \infty$ .

**Beispiel:** Es ist  $\text{trdeg}_{\mathbb{R}/\mathbb{Q}} = \text{card}(\mathbb{R})$ .

**Proposition:** Für jeden Körperturm  $M/L/K$  gilt  $\text{trdeg}_{M/K} = \text{trdeg}_{M/L} + \text{trdeg}_{L/K}$ .

**Definition:** Eine Körpererweiterung  $L/K$ , welche von einer Transzendenzbasis erzeugt ist, heisst *rein transzendent*.

**Beispiel:** Der rationale Funktionenkörper  $K(X_1, \dots, X_n)$  ist rein transzendent über  $K$  vom Transzendenzgrad  $n$ .

**Beispiel:** Der *elliptische Funktionenkörper*  $\mathbb{C}(x, y)$  für über  $\mathbb{C}$  transzendente Elemente  $x$  und  $y$  mit  $y^2 = x^3 - x$  ist nicht rein transzendent über  $\mathbb{C}$ .

## 5.7 Homomorphismen zwischen Körpererweiterungen

Betrachte zwei Körpererweiterungen  $L/K$  und  $L'/K$ .

**Definition:** Ein Körperhomomorphismus  $L \rightarrow L'$ , der auf  $K$  die Identität ist, heisst ein *Homomorphismus über  $K$* . Die Menge aller Homomorphismen  $L \rightarrow L'$  über  $K$  bezeichnen wir mit  $\text{Hom}_K(L, L')$ . Ein Homomorphismus über  $K$ , der ein Isomorphismus ist, heisst ein *Isomorphismus über  $K$* .

**Beispiel:** Die komplexe Konjugation  $\mathbb{C} \rightarrow \mathbb{C}$  ist ein Isomorphismus über  $\mathbb{R}$ .

**Beispiel:** Die Abbildung  $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$  mit  $a + b\sqrt{2} \mapsto a - b\sqrt{2}$  für alle  $a, b \in \mathbb{Q}$  ist ein Isomorphismus über  $\mathbb{Q}$ .

**Proposition:** Ist  $[L/K] = [L'/K] < \infty$ , so ist jeder Homomorphismus  $L \rightarrow L'$  über  $K$  ein Isomorphismus.

**Proposition:** Für jedes  $\varphi \in \text{Hom}_K(L, L')$  gilt: Ein Element  $a \in L$  ist algebraisch über  $K$  genau dann, wenn  $\varphi(a)$  algebraisch über  $K$  ist. In diesem Fall haben  $a$  und  $\varphi(a)$  dasselbe Minimalpolynom und denselben Grad über  $K$ .

**Proposition:** Für jedes  $a \in L$  haben wir eine natürliche Bijektion

$$\text{Hom}_K(K(a), L') \xrightarrow{\sim} \{a' \in L' \mid m_{a,K}(a') = 0\}, \quad \varphi \mapsto \varphi(a).$$

**Proposition:** Ist  $L/K$  endlich, so gilt  $|\text{Hom}_K(L, L')| \leq [L/K]$ .

**Satz:** Ist  $L/K$  algebraisch und  $L'$  algebraisch abgeschlossen, so ist  $\text{Hom}_K(L, L') \neq \emptyset$ .

**Definition:** Ein Körperautomorphismus von  $L$ , der auf  $K$  die Identität ist, heisst ein *Automorphismus über  $K$* . Die Menge aller Automorphismen von  $L$  über  $K$  bezeichnen wir mit  $\text{Aut}_K(L)$ .

**Proposition:** Ist  $L/K$  algebraisch, so ist  $\text{Hom}_K(L, L) = \text{Aut}_K(L)$ .

**Beispiel:** Die Abbildung  $K(X) \rightarrow K(X)$ ,  $f(X) \mapsto f(X^2)$  ist ein Homomorphismus über  $K$ , aber kein Automorphismus.

## 5.8 Konstruktion von Körpererweiterungen

**Definition:** Sei  $f \in K[X]$  irreduzibel. Ein Oberkörper von  $K$  der Form  $K(a)$  mit  $f(a) = 0$  heisst ein *Stammkörper von  $f$  über  $K$* .

**Beispiel:** Für jede Körpererweiterung  $L/K$  und jedes über  $K$  algebraische Element  $a \in L$  ist  $K(a)$  ein Stammkörper des Minimalpolynoms  $m_{a,K}$  über  $K$ .

**Proposition:** Jedes irreduzible Polynom  $f \in K[X]$  besitzt einen Stammkörper  $L$  über  $K$ . Dabei ist das Paar  $(L, a)$  bis auf eindeutige Isomorphie über  $K$  bestimmt.

**Definition:** Sei  $f \in K[X] \setminus \{0\}$ . Ein Oberkörper von  $K$  der Form  $L = K(a_1, \dots, a_n)$  mit  $f(X) = \alpha \prod_{i=1}^n (X - a_i)$  in  $L[X]$  für ein  $\alpha \in L^\times$  heisst ein *Zerfällungskörper von  $f$  über  $K$* .

**Proposition:** Jedes Polynom  $f \in K[X] \setminus \{0\}$  besitzt einen Zerfällungskörper über  $K$ . Dieser ist bis auf Isomorphie über  $K$  bestimmt; der Isomorphismus ist aber im allgemeinen nicht eindeutig.

**Beispiel:** Betrachte die reellen Zahlen  $a_1 := \sqrt[4]{5}$  und  $a_2 := -a_1$  sowie die komplexen Zahlen  $a_3 := ia_1$  und  $a_4 := -a_3$ . Dann besitzt  $f(X) := X^4 - 5$  die Faktorisierung  $(X - a_1)(X - a_2)(X - a_3)(X - a_4)$  über  $\mathbb{C}$ . Nach dem Eisensteinkriterium für  $p = 5$  ist  $f(X)$  irreduzibel über  $\mathbb{Q}$ . Für jedes  $j$  ist somit  $\mathbb{Q}(a_j)$  ein Stammkörper von  $f$  über  $\mathbb{Q}$ , und es gilt  $[\mathbb{Q}(a_j)/\mathbb{Q}] = 4$ . Dabei sind  $\mathbb{Q}(a_1) = \mathbb{Q}(a_2)$  und  $\mathbb{Q}(a_3) = \mathbb{Q}(a_4)$ , aber mit jeweils verschiedenen Erzeugenden. Weiter ist  $L := \mathbb{Q}(a_1, a_2, a_3, a_4) = \mathbb{Q}(\sqrt[4]{5}, i)$  ein Zerfällungskörper von  $f$  über  $\mathbb{Q}$ . Wegen  $i^2 + 1 = 0$  und  $i \notin \mathbb{Q}(a_1)$  gilt  $[\mathbb{Q}(\sqrt[4]{5}, i)/\mathbb{Q}(\sqrt[4]{5})] = 2$  und folglich  $[L/\mathbb{Q}] = 8$ .

**Proposition:** Für jeden Zerfällungskörper  $L$  eines Polynoms vom Grad  $n$  über  $K$  ist der Körpergrad  $[L/K]$  ein Teiler von  $n!$ .

**Beispiel:** Der Körper  $\mathbb{C}$  ist gleichzeitig Stamm- und Zerfällungskörper des Polynoms  $X^2 + 1$  über  $\mathbb{R}$ . Verschiedene konkrete Realisierungen unterscheiden sich um einen Isomorphismus; zu jedem Isomorphismus gibt es aber auch den dazu komplex konjugierten Isomorphismus. Ich empfehle  $\mathbb{C}$  zu betrachten als eine quadratische Erweiterung von  $\mathbb{R}$  zusammen mit einem ausgewählten Element  $i$  mit  $i^2 + 1 = 0$ .



## 5.9 Algebraischer Abschluss

**Proposition:** Für jeden Körper  $K$  sind die folgenden Bedingungen äquivalent:

- (a) Jedes nichtkonstante Polynom in  $K[X]$  besitzt eine Nullstelle in  $K$ .
- (b) Jedes von Null verschiedene Polynom in  $K[X]$  zerfällt in Linearfaktoren über  $K$ .
- (c) Jedes Polynom vom Grad  $n \geq 0$  in  $K[X]$  besitzt, mit Vielfachheiten gezählt, genau  $n$  Nullstellen in  $K$ .
- (d) Jede endliche Erweiterung von  $K$  ist gleich  $K$ .
- (e) Jede algebraische Erweiterung von  $K$  ist gleich  $K$ .

**Definition:** Ein Körper mit diesen Eigenschaften heisst *algebraisch abgeschlossen*.

**Definition:** Ein Oberkörper von  $K$ , welcher algebraisch über  $K$  und selbst algebraisch abgeschlossen ist, heisst ein *algebraischer Abschluss von  $K$* . Ein solcher wird oft bezeichnet mit  $\overline{K}$ .

**Beispiel:** Der Körper  $\mathbb{C}$  ist ein algebraischer Abschluss von  $\mathbb{R}$ .

**Beispiel:** Der Unterkörper aller algebraischer Zahlen in  $\mathbb{C}$  ist ein algebraischer Abschluss von  $\mathbb{Q}$ .

**Satz:** Je zwei algebraische Abschlüsse von  $K$  sind isomorph über  $K$ .

**Vorsicht:** Der Isomorphismus ist im allgemeinen nicht eindeutig. Deshalb sollte man stets nur von *einem* algebraischen Abschluss sprechen, und den bestimmten Artikel erst verwenden, nachdem man einen algebraischen Abschluss gewählt hat.

**Satz:** Jeder Körper besitzt einen algebraischen Abschluss.

## 5.10 Separable und irreduzible Polynome

Betrachte einen algebraischen Abschluss  $\overline{K}$  von  $K$ . Aufgrund der Eindeutigkeit von  $\overline{K}$  bis auf Isomorphie ist der folgende Begriff unabhängig von der Wahl von  $\overline{K}$ .

**Definition:** Ein Polynom in  $K[X] \setminus \{0\}$ , das keine mehrfachen Nullstellen in  $\overline{K}$  besitzt, heisst *separabel*.

**Vorsicht:** Manche Autoren verwenden diese Definition nur für irreduzible Polynome und eine *dazu nicht äquivalente* für reduzible Polynome. Die hier benutzte Definition hat den folgenden Vorteil:

**Proposition:** Für jede Körpererweiterung  $L/K$  gilt: Ein Polynom  $f \in K[X] \setminus \{0\}$  ist separabel über  $K$  genau dann, wenn es separabel als Polynom über  $L$  ist.

**Proposition:** Für jede Körpererweiterung  $L/K$  gilt: Zwei Polynome  $f, g \in K[X] \setminus \{0\}$  sind teilerfremd in  $K[X]$  genau dann, wenn sie teilerfremd in  $L[X]$  sind.

**Definition:** Die *formale Ableitung* eines Polynoms  $f(X) = \sum_k a_k X^k$  ist das Polynom

$$f'(X) := \frac{df}{dX}(X) := \sum_k a_k k X^{k-1}.$$

**Proposition:** Die formale Ableitung erfüllt die üblichen Regeln:

$$\begin{aligned} \forall f, g \in K[X]: \quad (f \pm g)' &= f' \pm g' \\ \forall a \in K \forall f \in K[X]: \quad (af)' &= af' \\ \forall f, g \in K[X]: \quad (fg)' &= f'g + fg' \quad (\text{Leibniz-Regel}) \end{aligned}$$

**Proposition:** Ein Polynom  $f \in K[X] \setminus \{0\}$  ist separabel genau dann, wenn  $f$  und  $f'$  teilerfremd in  $K[X]$  sind.

**Proposition:** Ein irreduzibles  $f \in K[X]$  ist separabel genau dann, wenn  $f' \neq 0$  ist.

**Satz:** (a) Ist  $\text{char}(K) = 0$ , so ist jedes irreduzible Polynom über  $K$  separabel.

(b) Ist  $p := \text{char}(K) > 0$ , so hat jedes irreduzible Polynom über  $K$  die Form

$$f(X) = g(X^{p^r})$$

für ein eindeutiges  $r \geq 0$  und ein separables irreduzibles Polynom  $g$  über  $K$ .

**Beispiel:** Betrachte den rationalen Funktionenkörper  $K := \mathbb{F}_p(Y)$  und das Polynom  $g(X) := X - Y \in K[X]$ . Für jedes  $r \geq 1$  ist dann  $g(X^{p^r}) = X^{p^r} - Y$  irreduzibel über  $K$ , aber nicht separabel.

## 5.11 Perfekte Körper

**Definition:** Ein Körper  $K$  heisst *vollkommen* oder *perfekt*, wenn jedes irreduzible Polynom über  $K$  separabel ist.

**Proposition:** Jeder Körper der Charakteristik 0 ist perfekt.

**Proposition-Definition:** Sei  $R$  ein Ring, und sei  $p$  eine Primzahl mit  $p \cdot 1_R = 0_R$ . Dann ist für jedes  $r \geq 1$  die Abbildung

$$\text{Frob}_{p^r} : R \rightarrow R, x \mapsto x^{p^r}$$

ein Ringhomomorphismus, genannt der *Frobenius-Endomorphismus vom Grad  $p^r$* .

Insbesondere besitzt jeder Körper  $K$  der Charakteristik  $p > 0$  den Endomorphismus  $\text{Frob}_p : K \rightarrow K$ . Als Körperhomomorphismus ist dieser injektiv.

**Proposition:** Ein Körper  $K$  der Charakteristik  $p > 0$  ist perfekt genau dann, wenn der Frobenius-Endomorphismus  $\text{Frob}_p : K \rightarrow K$  bijektiv ist.

**Proposition:** Jeder endliche Körper ist perfekt.

**Beispiel:** Der rationale Funktionenkörper  $\mathbb{F}_p(Y)$  ist nicht perfekt.

## 5.12 Endliche Körper

**Satz:** Für jeden endlichen Körper  $k$  gilt:

- (a)  $p := \text{char}(k) > 0$ .
- (b)  $|k| = p^n$  für  $n := [k/\mathbb{F}_p]$ .
- (c) Die multiplikative Gruppe  $k^\times$  ist zyklisch der Ordnung  $p^n - 1$ .
- (d)  $a^{p^n} = a$  für alle  $a \in k$ . (*Kleiner Satz von Fermat*)
- (e)  $k$  ist ein Zerfällungskörper des Polynoms  $X^{p^n} - X$  über  $\mathbb{F}_p$ .

**Satz:** Für jede Primpotenz  $p^n$  existiert ein endlicher Körper der Ordnung  $p^n$ . Dieser ist bis auf Isomorphie bestimmt; der Isomorphismus ist aber im allgemeinen nicht eindeutig. Eine häufige Bezeichnung dafür ist  $\mathbb{F}_{p^n}$ .

**Proposition:** Für jeden endlichen Körper  $k$  der Ordnung  $p^n$  ist

$$\text{Aut}(k) = \text{Aut}_{\mathbb{F}_p}(k) = \langle \text{Frob}_p|_k \rangle$$

zyklisch der Ordnung  $n$ .

**Definition:** Ein Ring, der alle Körperaxiome ausser vielleicht die Kommutativität der Multiplikation erfüllt, heisst eine *Divisionsalgebra* oder ein *Schiefkörper*.

**Satz:** (*Wedderburn*) Jeder endliche Schiefkörper ist kommutativ. (ohne Beweis)

### 5.13 Separable Körpererweiterungen

**Definition:** Betrachte eine algebraische Körpererweiterung  $L/K$ .

- (a) Ein Element von  $L$ , dessen Minimalpolynom über  $K$  separabel ist, heisst *separabel über  $K$* .
- (b) Ist jedes Element von  $L$  separabel über  $K$ , so heisst  $L/K$  *separabel*.

**Proposition:** Ein Körper  $K$  ist perfekt genau dann, wenn jede algebraische Erweiterung von  $K$  separabel ist.

**Bemerkung:** Die Folgerung gilt insbesondere im Fall  $\text{char}(K) = 0$  oder  $|K| < \infty$ .

**Proposition:** Sei  $L = K(a_1, \dots, a_n)/K$  endlich, und sei  $\bar{K}$  ein algebraischer Abschluss von  $K$ . Dann sind äquivalent:

- (a)  $L/K$  ist separabel.
- (b) Jedes  $a_i$  ist separabel über  $K$ .
- (c)  $|\text{Hom}_K(L, \bar{K})| = [L/K]$ .

**Proposition:** Eine algebraische Körpererweiterung  $L = K(A)/K$  ist separabel genau dann, wenn jedes Element von  $A$  separabel über  $K$  ist.

**Proposition:** Für jeden algebraischen Körperturm  $M/L/K$  ist  $M/K$  separabel genau dann, wenn  $M/L$  und  $L/K$  separabel sind.

**Satz vom primitiven Element:** Jede endliche separable Körpererweiterung ist einfach.

## 5.14 Inseparable Körpererweiterungen

**Proposition:** Sei  $L = K(A)$  algebraisch über  $K$  mit  $p := \text{char}(K) > 0$ , und sei  $\overline{K}$  ein algebraischer Abschluss von  $K$ . Dann sind äquivalent:

- (a) Für jedes  $a \in L$  existiert ein  $r \geq 0$  mit  $a^{p^r} \in K$ .
- (b) Für jedes  $a \in A$  existiert ein  $r \geq 0$  mit  $a^{p^r} \in K$ .
- (c)  $|\text{Hom}_K(L, \overline{K})| = 1$ .

**Definition:** Eine Körpererweiterung  $L/K$  mit den obigen Eigenschaften heisst *rein inseparabel* oder *total inseparabel* oder *radiziell*.

**Beispiel:** Betrachte den rationalen Funktionenkörper  $L := \mathbb{F}_p(X_1, X_2)$  und den Unterkörper  $K := \mathbb{F}_p(X_1^p, X_2^p)$ . Für jedes  $f \in L$  gilt dann  $f(X_1, X_2)^p = f(X_1^p, X_2^p) \in K$ . Insbesondere ist  $L/K$  rein inseparabel, und für jedes  $f \in L \setminus K$  gilt  $[K(f)/K] = p$ . Wegen  $[L/K] = p^2$  ist  $L/K$  also nicht einfach.

**Proposition:** Für jeden algebraischen Körperturm  $M/L/K$  ist  $M/K$  rein inseparabel genau dann, wenn  $M/L$  und  $L/K$  rein inseparabel sind.

**Proposition:** Jede algebraische Körpererweiterung  $L/K$  besitzt einen eindeutigen Zwischenkörper  $K'$ , so dass  $K'/K$  separabel und  $L/K'$  rein inseparabel ist, nämlich

$$K' := \{a \in L \mid a \text{ separabel über } K\}.$$

**Vorsicht:** Eine Faktorisierung in die andere Richtung, das heisst ein Zwischenkörper  $K''$  mit  $L/K''$  separabel und  $K''/K$  rein inseparabel, existiert im allgemeinen nicht.

## 5.15 Normale Körpererweiterungen

**Proposition:** Sei  $L = K(A)$  algebraisch über  $K$ , und sei  $\bar{L}$  ein algebraischer Abschluss von  $L$ . Dann sind äquivalent:

- (a) Jedes irreduzible Polynom  $f \in K[X]$ , das eine Nullstelle in  $L$  besitzt, zerfällt in  $L[X]$  in Linearfaktoren.
- (b) Für jedes  $a \in L$  enthält  $L$  einen Zerfällungskörper des Minimalpolynoms  $m_{a,K}$ .
- (c) Für jedes  $a \in A$  enthält  $L$  einen Zerfällungskörper des Minimalpolynoms  $m_{a,K}$ .
- (d) Für jedes  $\varphi \in \text{Hom}_K(L, \bar{L})$  gilt  $\varphi(L) = L$ .
- (e) Für jedes  $\varphi \in \text{Hom}_K(L, \bar{L})$  gilt  $\varphi(L) \subset L$ .

**Definition:** Eine Körpererweiterung  $L/K$  mit den obigen Eigenschaften heisst *normal*.

**Proposition:** Eine endliche Körpererweiterung ist normal genau dann, wenn sie Zerfällungskörper eines Polynoms ist.

**Beispiel:** Die triviale Erweiterung  $K/K$  ist normal.

**Beispiel:** Jeder algebraische Abschluss  $\bar{K}/K$  ist normal.

**Beispiel:** Jede quadratische Körpererweiterung ist normal.

**Beispiel:** Die Erweiterung  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  ist nicht normal.

**Proposition:** Sind  $M/L/K$  algebraisch und ist  $M/K$  normal, so ist auch  $M/L$  normal.

**Vorsicht:** Sind  $M/L/K$  algebraisch und ist  $M/K$  normal, so ist  $L/K$  nicht notwendig normal, zum Beispiel für  $K = \mathbb{Q}$  und  $L = \mathbb{Q}(\sqrt[3]{2})$  und  $M$  ein Zerfällungskörper von  $X^3 - 2$  über  $\mathbb{Q}$ .

**Vorsicht:** Sind  $M/L$  und  $L/K$  algebraisch und normal, so ist  $M/K$  nicht notwendig normal. Zum Beispiel sind  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$  und  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$  jeweils normal vom Grad 2, aber  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$  ist nicht normal.

**Definition:** Eine *normale Hülle* einer algebraischen Erweiterung  $L/K$  ist eine minimale algebraische Erweiterung  $\tilde{L}/L$ , so dass  $\tilde{L}/K$  normal ist.

**Proposition:** Ist  $L = K(a_1, \dots, a_n)$  endlich über  $K$ , so ist jeder Zerfällungskörper von  $m_{a_1,K} \cdots m_{a_n,K}$  über  $K$ , der  $L$  umfasst, eine normale Hülle von  $L/K$ .

**Proposition:** Jede algebraische Erweiterung  $L/K$  besitzt eine normale Hülle. Diese ist eindeutig bis auf Isomorphie über  $L$ . (Der Isomorphismus ist aber im allgemeinen nicht eindeutig.)

**Proposition:** Sei  $\tilde{L}$  eine normale Hülle einer algebraischen Erweiterung  $L/K$ .

- (a) Ist  $L/K$  endlich, so ist auch  $\tilde{L}/K$  endlich.
- (b) Ist  $L/K$  separabel, so ist auch  $\tilde{L}/K$  separabel.

## 6 Galoistheorie

Die Galoistheorie besteht darin, Körpererweiterungen  $L/K$  via ihrer Symmetrien, das heisst, via der Gruppe  $\text{Aut}_K(L)$  zu studieren.

### 6.1 Galoiserweiterungen

**Definition:** Eine separable normale algebraische Körpererweiterung  $L/K$  nennt man *galoissch* oder eine *Galoiserweiterung*. Die zugehörige Gruppe  $\text{Gal}(L/K) := \text{Aut}_K(L)$  nennt man dann die *Galoisgruppe von  $L/K$* .

**Proposition:** Eine endliche Erweiterung  $L/K$  ist galoissch genau dann, wenn  $|\text{Aut}_K(L)| = [L/K]$  ist. Dann ist also  $\text{Gal}(L/K)$  eine endliche Gruppe der Ordnung  $[L/K]$ .

**Beispiel:** Jede Erweiterung von endlichen Körpern  $\ell/k$  ist endlich galoissch mit zyklischer Galoisgruppe  $\langle \text{Frob}_{|k|} |_{\ell} \rangle$  der Ordnung  $[\ell/k]$ .

**Proposition-Definition:** Sei  $L$  ein Körper und  $\Gamma$  eine Untergruppe von  $\text{Aut}(L)$ . Dann ist

$$L^{\Gamma} := \{a \in L \mid \forall \gamma \in \Gamma: \gamma(a) = a\}$$

ein Unterkörper von  $L$ , genannt der *Fixkörper von  $\Gamma$* .

**Satz:** Für jede endliche Untergruppe  $\Gamma < \text{Aut}(L)$  ist  $L/L^{\Gamma}$  endlich galoissch mit Galoisgruppe  $\Gamma$ .

**Proposition:** Für jede Galoiserweiterung  $L/K$  und jeden Zwischenkörper  $K'$  ist auch  $L/K'$  galoissch, und  $\text{Gal}(L/K')$  ist eine Untergruppe von  $\text{Gal}(L/K)$ .

## 6.2 Galoiskorrespondenz

**Hauptsatz der Galoistheorie:** Sei  $L/K$  endlich galoissch mit Galoisgruppe  $\Gamma$ . Dann haben wir natürliche zueinander inverse Bijektionen

$$\begin{array}{ccc} \{\text{Zwischenkörper von } L/K\} & \xleftrightarrow{\sim} & \{\text{Untergruppen von } \Gamma\} \\ K' & \xrightarrow{\quad} & \text{Gal}(L/K') \\ L^{\Gamma'} & \xleftarrow{\quad} & \Gamma' \end{array}$$

Weiter gilt für beliebige einander entsprechende  $K' \rightsquigarrow \Gamma'$  und  $K'' \rightsquigarrow \Gamma''$ :

- (a)  $[L/K'] = |\Gamma'|$  und  $[K'/K] = [\Gamma : \Gamma']$ .
- (b)  $K' \subset K'' \iff \Gamma' > \Gamma''$ .
- (c) Für jedes  $\gamma \in \Gamma$  entspricht der Zwischenkörper  $\gamma(K')$  der Untergruppe  ${}^\gamma\Gamma'$ .
- (d) Es existiert ein natürlicher Isomorphismus

$$\text{Norm}_\Gamma(\Gamma')/\Gamma' \xrightarrow{\sim} \text{Aut}_K(K'), \quad \gamma\Gamma' \mapsto \gamma|_{K'}.$$

- (e)  $K'/K$  ist galoissch genau dann, wenn  $\Gamma'$  normal in  $\Gamma$  ist, und dann ist die Abbildung in (d) ein natürlicher Isomorphismus

$$\Gamma/\Gamma' \xrightarrow{\sim} \text{Gal}(K'/K).$$

**Satz:** Jede endliche separable Erweiterung besitzt nur endlich viele Zwischenkörper.

**Bemerkung:** Jedes Element von  $L$ , das in keinem von  $L$  verschiedenen Zwischenkörper liegt, ist ein primitives Element von  $L/K$ .

Sei nun  $f \in K[X]$  ein separables Polynom vom Grad  $n \geq 0$ . Seien  $a_1, \dots, a_n$  die Nullstellen von  $f$  in einem Zerfällungskörper  $L = K(a_1, \dots, a_n)$  von  $f$  über  $K$ . Dann ist  $L/K$  galoissch, und wir nennen seine Galoisgruppe  $\text{Gal}(L/K)$  auch die *Galoisgruppe von  $f$  über  $K$* .

**Proposition:** Es existiert eine eindeutige Linksoperation von  $\Gamma$  auf  $\{1, \dots, n\}$  mit der Eigenschaft

$$\forall \gamma \in \text{Gal}(L/K) \quad \forall 1 \leq i \leq n: \quad \gamma(a_i) = a_{\gamma i}.$$

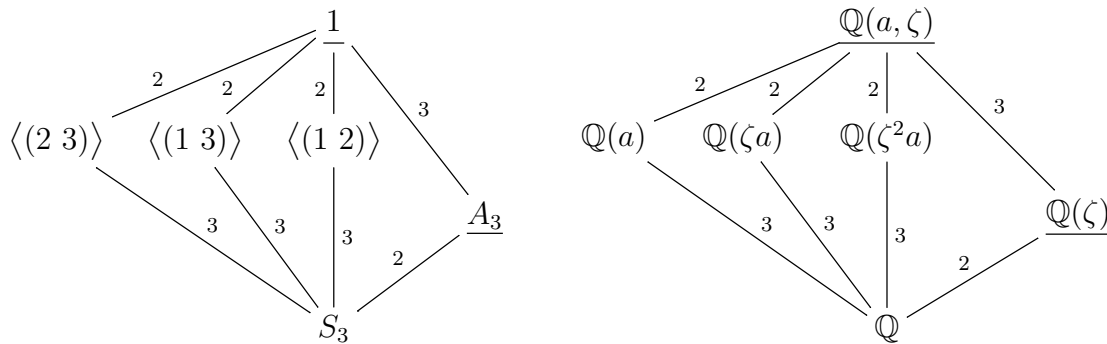
Diese ist treu, entspricht also einem injektiven Homomorphismus  $\text{Gal}(L/K) \hookrightarrow S_n$ .

Dadurch können wir  $\text{Gal}(L/K)$  mit einer Untergruppe von  $S_n$  identifizieren. Die Identifikation hängt allerdings von der gewählten Reihenfolge der Nullstellen ab. Jede andere Reihenfolge hat die Form  $a_{\sigma 1}, \dots, a_{\sigma n}$  für eine Permutation  $\sigma \in S_n$ , und die Umordnung ändert den Homomorphismus ab um den inneren Automorphismus  $\text{int}_\sigma$  von  $S_n$  und sein Bild somit um Konjugation mit  $\sigma$ .

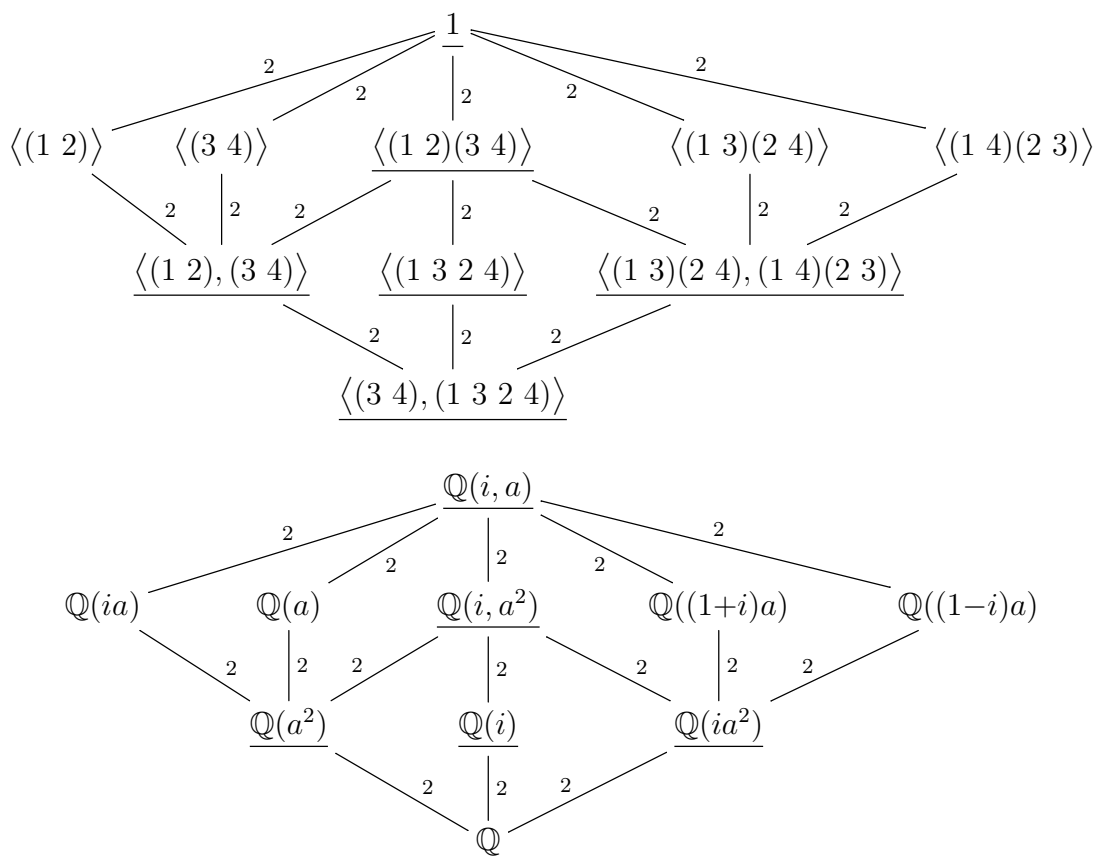
**Proposition:** Die Bahnen der Operation von  $\text{Gal}(L/K)$  auf  $\{1, \dots, n\}$  entsprechen genau den normierten irreduziblen Faktoren von  $f$  in  $K[X]$ . Insbesondere ist die Operation transitiv genau dann, wenn  $f$  irreduzibel ist.



**Beispiel:** Das Polynom  $f(X) := X^3 - 2 \in \mathbb{Q}[X]$  hat die Galoisgruppe  $S_3$ . Genauer seien  $a := \sqrt[3]{2} \in \mathbb{R}$  und  $\zeta := \exp \frac{2\pi i}{3} \in \mathbb{C}$ . Die komplexen Nullstellen von  $f$  sind dann  $(a_1, a_2, a_3) := (a, \zeta a, \zeta^2 a)$ . Mit  $L := \mathbb{Q}(a_1, a_2, a_3) = \mathbb{Q}(a, \zeta)$  liefert die Galoiskorrespondenz die folgenden Entsprechungen, wobei normale Untergruppen bzw. Erweiterungen unterstrichen sind:



**Beispiel:** Das Polynom  $f(X) := X^4 - 2 \in \mathbb{Q}[X]$  hat Galoisgruppe  $D_4$ . Genauer sei  $a := \sqrt[4]{2} \in \mathbb{R}$ ; die komplexen Nullstellen von  $f$  sind dann  $(a_1, a_2, a_3, a_4) := (a, -a, ia, -ia)$ . Mit  $L := \mathbb{Q}(a_1, a_2, a_3, a_4) = \mathbb{Q}(i, a)$  liefert die Galoiskorrespondenz die folgenden Entsprechungen, wobei normale Untergruppen bzw. Erweiterungen unterstrichen sind:



### 6.3 Symmetrische Funktionen

Wir betrachten Polynome in  $\underline{X} = (X_1, \dots, X_n)$  über einem beliebigen Ring  $R$ .

**Definition:** Ein Polynom der Form  $f(\underline{X}) = \sum_i' a_i \underline{X}^i$ , bei der die Summe sich nur über Multiindizes  $\underline{i}$  mit  $\sum_\nu i_\nu = d$  erstreckt, heisst *homogen vom Grad  $d$* .

**Proposition:** Jedes Polynom ist eine eindeutige Summe  $f = \sum_{d \geq 0}' f_d$  mit  $f_d$  homogen vom Grad  $d$ .

**Definition:** Der *Totalgrad*  $\deg(f)$  eines Polynoms  $f \in R[\underline{X}] \setminus \{0\}$  ist das grösste  $d$  mit  $f_d \neq 0$ .

**Proposition:** Für alle  $f, g \in R[\underline{X}] \setminus \{0\}$  gilt  $\deg(fg) \leq \deg(f) + \deg(g)$ , mit Gleichheit wenn  $R$  ein Integritätsbereich ist.

**Variante:** Für jede Variable  $X_\nu$  sei ein Gewicht  $\mu_\nu \in \mathbb{R}$  gegeben. Ein Polynom der Form  $f(\underline{X}) = \sum_i' a_i \underline{X}^i$ , bei der die Summe sich nur über Multiindizes  $\underline{i}$  mit  $\sum_\nu i_\nu \mu_\nu = \lambda$  erstreckt, heisst dann *isobar vom Gewicht  $\lambda$* . Jedes Polynom ist eine eindeutige Summe  $f = \sum_\lambda' f_\lambda$  mit  $f_\lambda$  isobar vom Gewicht  $\lambda$ .

**Definition:** Ein Polynom  $f \in R[X_1, \dots, X_n]$  heisst *symmetrisch*, wenn gilt

$$\forall \sigma \in S_n: f(X_{\sigma 1}, \dots, X_{\sigma n}) = f(X_1, \dots, X_n).$$

**Definition:** Für jedes  $1 \leq m \leq n$  ist das  $m$ -te *elementarsymmetrische Polynom* in  $X_1, \dots, X_n$  das homogene symmetrische Polynom vom Grad  $m$

$$S_m := \sum_{1 \leq \nu_1 < \dots < \nu_m \leq n} X_{\nu_1} \cdots X_{\nu_m} \in \mathbb{Z}[X_1, \dots, X_n].$$

Eine äquivalente Charakterisierung ist die Identität

$$\begin{aligned} \prod_{i=1}^n (X - X_i) &= X^n + \sum_{m=1}^n (-1)^m S_m X^{n-m} \\ &= X^n - S_1 X^{n-1} + \dots + (-1)^n S_n \in \mathbb{Z}[X, X_1, \dots, X_n]. \end{aligned}$$

Betrachte nun weitere Variablen  $U_1, \dots, U_n$ .

**Hauptsatz:** Für jedes symmetrische Polynom  $f \in R[X_1, \dots, X_n]$  existiert ein eindeutiges Polynom  $g \in R[U_1, \dots, U_n]$  mit  $f = g(S_1, \dots, S_n)$ .

**Zusatz:** Ist  $f$  symmetrisch und homogen vom Grad  $d$ , so ist  $g$  isobar vom Gewicht  $d$ , wobei jedes  $U_\nu$  mit dem Gewicht  $\nu$  versehen wird.

**Beispiel:** Für jedes  $d \geq 1$  ist  $\sum_{\nu=1}^n X_\nu^d$  ein symmetrisches Polynom. Zum Beispiel sind

$$\begin{aligned} \sum_{\nu=1}^n X_\nu &= S_1, \\ \sum_{\nu=1}^n X_\nu^2 &= S_1^2 - 2S_2, \\ \sum_{\nu=1}^n X_\nu^3 &= S_1^3 - 3S_1S_2 + 3S_3. \end{aligned}$$

**Bemerkung:** Aus dem Hauptsatz folgt, dass für jedes von Null verschiedene Polynom  $g \in R[U_1, \dots, U_n]$  auch das Polynom  $g(S_1, \dots, S_n)$  ungleich Null ist.

**Variante:** Sei  $K$  ein Körper. Eine rationale Funktion  $f \in K(X_1, \dots, X_n)$  heisst *symmetrisch*, wenn gilt

$$\forall \sigma \in S_n: f(X_{\sigma_1}, \dots, X_{\sigma_n}) = f(X_1, \dots, X_n).$$

**Satz:** Für jede symmetrische rationale Funktion  $f \in K(X_1, \dots, X_n)$  existiert eine eindeutige rationale Funktion  $g \in K(U_1, \dots, U_n)$  mit  $f = g(S_1, \dots, S_n)$ .

**Folge:** Die Körpererweiterung  $K(X_1, \dots, X_n)/K(S_1, \dots, S_n)$  ist endlich galoissch mit Galoisgruppe  $S_n$ .

**Beispiel:** Es sind

$$\begin{aligned} \sum_{\nu=1}^n X_{\nu}^{-1} &= \frac{S_{n-1}}{S_n}, \\ \sum_{\nu=1}^n X_{\nu}^{-2} &= \frac{S_{n-1}^2 - 2S_{n-2}S_n}{S_n^2}, \\ \sum_{\nu=1}^n X_{\nu}^{-3} &= \frac{S_{n-1}^3 - 3S_{n-1}S_{n-2}S_n + 3S_{n-3}S_n^2}{S_n^3}. \end{aligned}$$

### 6.4 Resultante und Diskriminante

**Definition:** Die *Sylvestermatrix* zweier Polynome der Form  $f(X) = \sum_{i=0}^m a_i X^i$  und  $g(X) = \sum_{j=0}^n b_j X^j$  über einem Ring  $R$  ist die  $(m+n) \times (m+n)$ -Matrix

$$\text{Sylv}_{f,g} := \begin{pmatrix} a_m & \dots & \dots & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & a_m & \dots & \dots & \dots & a_1 & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & 0 \\ 0 & \dots & 0 & a_m & \dots & \dots & \dots & a_1 & a_0 \\ \hline b_n & \dots & \dots & b_1 & b_0 & 0 & \dots & \dots & 0 \\ 0 & b_n & \dots & \dots & b_1 & b_0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & b_n & \dots & \dots & b_1 & b_0 \end{pmatrix}$$

in der die ersten  $n$  Zeilen aus den Koeffizienten von  $f$  und die restlichen  $m$  Zeilen aus den Koeffizienten von  $g$  gebildet sind. Die Determinante der Sylvestermatrix heisst die *Resultante von  $f$  und  $g$*  und wird bezeichnet mit  $\text{Res}_{f,g} \in R$ .

Offenbar ist die Resultante ein ganzzahliges Polynom in  $a_0, \dots, a_m, b_0, \dots, b_n$ , und zwar homogen vom Grad  $n$  in  $a_0, \dots, a_m$  und homogen vom Grad  $m$  in  $b_0, \dots, b_n$ .

**Proposition:** Es gilt  $\text{Res}_{g,f} = (-1)^{mn} \text{Res}_{f,g}$ .

**Proposition:** Seien  $f, g \in K[X]$  vom Grad  $m$  bzw.  $n$  für einen Körper  $K$ . Dann ist  $\text{Res}_{f,g} = 0$  genau dann, wenn  $f$  und  $g$  einen gemeinsamen Teiler vom Grad  $> 0$  haben.

**Proposition:** Für alle Polynome der Form  $f(X) = a_m \prod_{i=1}^m (X - \alpha_i)$  und  $g(X) = b_n \prod_{j=1}^n (X - \beta_j)$  gilt

$$\text{Res}_{f,g} = a_m^n \cdot b_n^m \cdot \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j).$$

**Proposition:** Für alle Polynome der Form  $f(X) = a_m \prod_{i=1}^m (X - \alpha_i)$  und  $g(X) = \sum_{j=0}^n b_j X^j$  gilt

$$\text{Res}_{f,g} = a_m^n \cdot \prod_{i=1}^m g(\alpha_i).$$

Im Spezialfall  $g = f'$  ist  $n = m - 1$  und  $b_{m-1} = ma_m$ ; also ist die erste Spalte der Sylvestermatrix  $\text{Sylv}_{f,f'}$  durch  $a_m$  teilbar. Es existiert daher ein eindeutiges ganzzahliges Polynom  $P_f$  in  $a_0, \dots, a_m$  mit  $\text{Res}_{f,f'} = a_m P_f$ .

**Definition:** Die *Diskriminante* eines Polynoms  $f(X) = \sum_{i=0}^m a_i X^i$  vom Grad  $m$  über einem Ring  $R$  ist

$$\text{Disc}_f := (-1)^{\frac{m(m-1)}{2}} P_f \in R.$$

**Proposition:** Für jedes Polynom der Form  $f(X) = a_m \prod_{i=1}^m (X - \alpha_i)$  gilt

$$\text{Disc}_f = a_m^{2m-2} \cdot \prod_{1 \leq i < j \leq m} (\alpha_i - \alpha_j)^2.$$

**Folge:** Ein Polynom  $f$  über einem Körper ist separabel genau dann, wenn  $\text{Disc}_f \neq 0$  ist.

**Anwendung:** Für jedes normierte Polynom  $f \in \mathbb{Z}[X]$  ist  $\text{Disc}_f \in \mathbb{Z}$ , und für eine beliebige Primzahl  $p$  ist  $f \bmod (p)$  separabel in  $\mathbb{F}_p[X]$  genau dann, wenn  $p \nmid \text{Disc}_f$  ist.

**Beispiel:** In kleinen Graden ist

$f(X)$	$\text{Disc}_f$
$aX + b$	1
$aX^2 + bX + c$	$b^2 - 4ac$
$aX^3 + bX^2 + cX + d$	$b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$

**Bemerkung:** Resultante und Diskriminante kann man auch als symmetrische Funktionen der Nullstellen konstruieren. Der obige Weg liefert aber schneller die richtigen Formeln, insbesondere für nicht normierte Polynome.

## 6.5 Explizite Konstruktion der Zwischenkörper

Sei  $L/K$  endlich galoissch mit Galoisgruppe  $\Gamma$ , und sei  $\Gamma' < \Gamma$  eine Untergruppe. Um den zugehörigen Zwischenkörper  $L^{\Gamma'}$  zu beschreiben, verschafft man sich zuerst geeignete Elemente  $b_1, \dots, b_k \in L^{\Gamma'}$ , die man entweder vermittle expliziter Erzeugenden von  $L$  errät oder durch eine  $\Gamma'$ -invariante Konstruktion findet. Wenn dann  $[K(b_1, \dots, b_k)/K] = [\Gamma : \Gamma']$  ist, so folgt direkt  $K(b_1, \dots, b_k) = L^{\Gamma'}$ . In der Praxis genügt dafür oft schon ein einzelnes Element  $b_1$ .

**Beispiel:** Sei  $\Gamma < S_n$  die Galoisgruppe eines separablen Polynoms  $f \in K[X]$  mit den Nullstellen  $a_1, \dots, a_n \in L$ . Betrachte die Quadratwurzel der Diskriminante

$$b := \prod_{1 \leq i < j \leq n} (a_i - a_j) \in L.$$

Sei ausserdem  $\text{char}(K) \neq 2$ . Dann ist  $\Gamma < A_n$  genau dann, wenn  $b \in K$  ist. Andernfalls ist  $K(b)$  der Zwischenkörper vom Grad 2 über  $K$ , welcher der Untergruppe  $\Gamma \cap A_n < \Gamma$  entspricht.

**Allgemeine Konstruktion:** Nach dem Satz vom primitiven Element ist  $L = K(a)$  für ein geeignetes  $a \in L$ . Betrachte das Hilfspolynom

$$F(X) := \sum_{i=0}^m b_i X^i := \prod_{\gamma \in \Gamma'} (X - \gamma(a)) \in L[X].$$

**Satz:** Dann gilt  $L^{\Gamma'} = K(b_0, \dots, b_m)$ .

Weiter ist der folgende Satz nützlich:

**Satz:** Die Menge  $\Gamma = \text{Gal}(L/K)$ , betrachtet als Teilmenge des  $L$ -Vektorraums aller Abbildungen  $L \rightarrow L$ , ist  $L$ -linear unabhängig.

**Folge:** Für jede Untergruppe  $\Gamma' < \text{Gal}(L/K)$  haben wir eine surjektive Abbildung

$$L \rightarrow L^{\Gamma'}, \quad x \mapsto \sum_{\gamma \in \Gamma'} \gamma(x).$$

Auch damit kann man also explizite Elemente von  $L^{\Gamma'}$  konstruieren.

## 6.6 Kreisteilungskörper

Sei  $n$  eine natürliche Zahl mit  $\text{char}(K) \nmid n$ , und sei  $\overline{K}$  ein algebraischer Abschluss von  $K$ .

**Proposition:** Die Gruppe der  $n$ -ten Einheitswurzeln

$$\mu_n := \mu_n(\overline{K}) := \{\zeta \in \overline{K} \mid \zeta^n = 1\}$$

ist eine zyklische Untergruppe der Ordnung  $n$  von  $\overline{K}^\times$ .

**Proposition:** Die Körpererweiterung  $K(\mu_n)/K$  ist endlich galoissch, und es existiert ein eindeutiger Homomorphismus  $e: \text{Gal}(K(\mu_n)/K) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$  mit der Eigenschaft

$$\forall \gamma \in \text{Gal}(K(\mu_n)/K) \forall \zeta \in \mu_n: \gamma(\zeta) = \zeta^{e(\gamma)}.$$

Dieser Homomorphismus ist injektiv. Insbesondere ist  $\text{Gal}(K(\mu_n)/K)$  abelsch.

**Beispiel:** Ist  $k$  ein endlicher Körper der Kardinalität  $q$ , so entspricht  $\text{Gal}(k(\mu_n)/k)$  der von der Restklasse  $q + n\mathbb{Z}$  erzeugten Untergruppe von  $(\mathbb{Z}/n\mathbb{Z})^\times$ . Zum Beispiel ist  $\text{Gal}(\mathbb{F}_2(\mu_{17})/\mathbb{F}_2)$  zyklisch der Ordnung 8.

**Satz:** Es ist  $\text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$ .

(Beweis im allgemeinen Fall: Siehe z.B. Jantzen, Schwermer: Algebra, Kap. 6, §2.)

**Satz:** Ein regelmässiges  $n$ -Eck ist mit Zirkel und Lineal konstruierbar genau dann, wenn  $|(\mathbb{Z}/n\mathbb{Z})^\times|$  eine Zweierpotenz ist.

**Bemerkung:** Dies ist genau dann der Fall, wenn  $n$  ein Produkt einer Zweierpotenz mit paarweise verschiedenen Fermat-Primzahlen, d.h. Primzahlen der Form  $2^{2^m} + 1$ , ist. Die einzigen bisher bekannten Fermat-Primzahlen sind 3, 5, 17, 257, 65537. Für  $n = 7, 9, 11, 13, 19$  ist dagegen ein regelmässiges  $n$ -Eck nicht konstruierbar.

**Satz:** (*Kronecker-Weber*) Jede endliche Galoiserweiterung von  $\mathbb{Q}$  mit abelscher Galoisgruppe ist einem *Kreisteilungskörper*  $\mathbb{Q}(\mu_n)$  enthalten. (ohne Beweis)

## 6.7 Abelsche Körpererweiterungen

**Definition:** Eine Galoiserweiterung heisst *abelsch*, bzw. *zyklisch*, bzw. *auflösbar*, wenn ihre Galoisgruppe die entsprechende Eigenschaft hat.

**Definition:** Eine Erweiterung der Form  $L = K(a)/K$  mit  $a^n \in K$  heisst eine *einfache Radikalerweiterung*.

**Satz:** (*Kummer-Theorie*) Sei  $L/K$  endlich und  $n$  eine natürliche Zahl mit  $\text{char}(K) \nmid n$  und  $\mu_n \subset K$ . Dann sind äquivalent:

- (a)  $L/K$  ist eine einfache Radikalerweiterung der Form  $L = K(a)$  mit  $a^n \in K$ .
- (b)  $L/K$  ist zyklisch vom Grad ein Teiler von  $n$ .

**Beispiel:** Im Fall  $\text{char}(K) \neq 2, 3$  ist jede zyklische Erweiterung vom Grad 3 von  $K$  enthalten in  $K(\sqrt{-3}, \sqrt[3]{b})$  für ein  $b \in K$  und eine geeignete Wahl der Wurzeln.

**Bemerkung:** Da jede endliche abelsche Gruppe ein direktes Produkt von zyklischen Gruppen ist, hat jede abelsche Körpererweiterung  $L/K$  die Form  $L_1 \cdots L_m$  für zyklische Erweiterungen  $L_i/K$ . Diese  $L_i$  kann man mittels Kummer-Theorie beschreiben.

**Beispiel:** Für beliebige paarweise verschiedene Primzahlen  $p_1, \dots, p_n$  ist der Körper  $K := \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$  endlich galoissch über  $\mathbb{Q}$  mit Galoisgruppe  $\text{Gal}(K/\mathbb{Q}) \cong \{\pm 1\}^n$ . Ausserdem gilt

$$K = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1} + \dots + \sqrt{p_n}).$$

## 6.8 Auflösbare Körpererweiterungen

**Lemma:** Betrachte eine Körpererweiterung  $L'/K$  der Form  $L' = LK'$  für Zwischenkörper  $L$  und  $K'$ . Ist  $L/K$  galoissch, so ist auch  $L'/K'$  galoissch und es gibt einen natürlichen injektiven Homomorphismus

$$\text{Gal}(L'/K') \hookrightarrow \text{Gal}(L/K), \gamma \mapsto \gamma|_L.$$

**Definition:** (a) Ein Körperturm  $K_m/\dots/K_0$ , bei dem jedes  $K_i/K_{i-1}$  eine einfache Radikalerweiterung ist, heisst ein *Radikalturm*.

(b) Ein Polynom  $f \in K[X]$  heisst *auflösbar durch Radikale*, wenn es einen Radikalturm  $K_m/\dots/K_0 = K$  gibt, so dass  $f$  über  $K_m$  in Linearfaktoren zerfällt.

Letzteres bedeutet, dass jede Nullstelle von  $f$  in einem algebraischen Abschluss von  $K$  durch eine explizite Formel in Termen der vier Grundrechenarten und Wurzeln beliebiger Ordnung, ausgehend von Elementen von  $K$ , darstellbar ist.

**Satz:** (*Abel-Ruffini*) Sei  $L/K$  endlich galoissch mit  $\text{char}(K) = 0$ . Dann sind äquivalent:

- (a) Es existiert ein Radikalturm  $K_m/\dots/K_0 = K$  mit  $L \subset K_m$ .
- (b)  $\text{Gal}(L/K)$  ist auflösbar.

Dies ist der Ursprung der Bezeichnung „auflösbare Gruppe“.

**Satz:** Für  $n \geq 5$  existiert keine Formel in Termen der vier Grundrechenarten und beliebigen Wurzeln, welche für beliebige Wahl der Variablen  $b_0, \dots, b_n$  in einem Körper  $K$  der Charakteristik Null eine Nullstelle des Polynoms  $\sum_{i=0}^n b_i X^i$  produziert.

Man sagt also: *Die allgemeine Gleichung vom Grad  $n \geq 5$  ist nicht auflösbar durch Radikale*. Die vom Grad  $\leq 4$  dagegen schon:

**Spezialfall:** Jedes quadratische Polynom  $aX^2 + bX + c$  über einem Körper  $K$  der Charakteristik  $\neq 2$  hat die Nullstellen

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \in \bar{K}.$$

**Spezialfall:** Betrachte ein kubisches Polynom  $aX^3 + bX^2 + cX + d$  über einem Körper  $K$  der Charakteristik  $\neq 2, 3$ . Division durch  $a$  und die Variablensubstitution  $X = Y - \frac{b}{3a}$  transformieren es in die Form  $Y^3 + 3pY - 2q$  für gewisse  $p, q \in K$ . Dieses hat die Nullstellen

$$y_i := \zeta^i \cdot \sqrt[3]{q - \sqrt{p^3 + q^2}} + \zeta^{-i} \cdot \sqrt[3]{q + \sqrt{p^3 + q^2}} \in \bar{K}$$

für  $i = 0, 1, 2$  mit  $\zeta := \frac{-1 + \sqrt{-3}}{2}$  und einer geeigneten Wahl der Wurzeln in  $\bar{K}$ .

**Spezialfall:** Jedes Polynom  $aX^4 + bX^3 + cX^2 + dX + e$  vom Grad 4 über einem Körper der Charakteristik  $\neq 2, 3$  ist auflösbar durch Radikale. Explizite Lösungsformeln werden in der Vorlesung und den Übungen entwickelt.



## 6.9 Explizite Bestimmung der Galoisgruppe (nur zum Teil behandelt)

Betrachte das Polynom in  $2n + 1$  Variablen

$$G := \prod_{\sigma \in S_n} \left( Z - \sum_{i=1}^n Y_i X_{\sigma i} \right) \in \mathbb{Z}[Z, Y_1, \dots, Y_n, X_1, \dots, X_n].$$

Da es in den Variablen  $X_1, \dots, X_n$  symmetrisch ist, existiert ein eindeutiges Polynom in  $1 + 2n$  Variablen  $\overline{G} \in \mathbb{Z}[Z, Y_1, \dots, Y_n, U_1, \dots, U_n]$ , so dass mit den elementarsymmetrischen Polynomen  $S_1, \dots, S_n \in \mathbb{Z}[X_1, \dots, X_n]$  gilt

$$G = \overline{G}(Z, Y_1, \dots, Y_n, S_1, \dots, S_n).$$

Betrachte nun ein separables Polynom

$$f(X) = \sum_{i=0}^n (-1)^i b_i X^{n-i} = X^n - b_1 X^{n-1} + \dots + (-1)^n b_n \in K[X].$$

Seien  $a_1, \dots, a_n \in L = K(a_1, \dots, a_n)$  seine Nullstellen und  $\Gamma = \text{Gal}(L/K) < S_n$  seine Galoisgruppe. Betrachte das Hilfspolynom

$$g := \overline{G}(Z, Y_1, \dots, Y_n, b_1, \dots, b_n) \in K[Z, Y_1, \dots, Y_n].$$

**Satz:** Für jeden irreduziblen Faktor  $h$  von  $g$  existiert ein  $\sigma \in S_n$  mit

$$\{\tau \in S_n \mid h(Z, Y_{\tau 1}, \dots, Y_{\tau n}) = h\} = \sigma \Gamma.$$

**Folge:** Sei  $K$  ein Körper, für den ein Algorithmus existiert, der jedes Polynom in beliebig vielen Variablen über  $K$  in irreduzible Faktoren zerlegt. Dann existiert ein Algorithmus zur Bestimmung der Galoisgruppe jedes separablen Polynoms über  $K$ .

**Spezialfall:** (Vgl. §2.7) Insbesondere existiert ein solcher Algorithmus für  $K = \mathbb{Q}$ .

**Satz:** Sei zusätzlich  $f \in \mathbb{Z}[X]$ . Sei  $p$  eine Primzahl, welche die Diskriminante von  $f$  nicht teilt. Sei  $f \bmod (p)$  ein Produkt irreduzibler Polynome in  $\mathbb{F}_p[X]$  der Grade  $n_1 + \dots + n_r = n$ . Dann enthält  $\Gamma$  eine Permutation, deren zugehörige Partition von  $n$  die Form  $n_1 + \dots + n_r = n$  hat.

**Beispiel:** Die Galoisgruppe von  $f(X) := X^4 + 3X^3 - X^2 + 1$  über  $\mathbb{Q}$  ist die  $S_4$ .

Die Galoisgruppe von  $f(X) := X^5 + 2X^2 + 1$  über  $\mathbb{Q}$  ist die  $S_5$ .

Die Galoisgruppe von  $f(X) := X^7 + 3X^2 + 5$  über  $\mathbb{Q}$  ist die  $S_7$ .

Die Galoisgruppe von  $f(X) := X^5 + 20X + 16$  über  $\mathbb{Q}$  ist die  $A_5$ .

## 7 Amuse Bouches

### 7.1 $p$ -adische Zahlen (*nicht behandelt*)

Sei  $p$  eine Primzahl. Für alle  $n \geq m \geq 0$  betrachte den Ringhomomorphismus

$$\text{proj}_m^n: \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p^m\mathbb{Z}, \quad a + p^n\mathbb{Z} \mapsto a + p^m\mathbb{Z}.$$

Setze

$$\begin{aligned} \mathbb{Z}_p &:= \left\{ \underline{a} = (a_n)_{n \geq 0} \in \prod_{n \geq 0} \mathbb{Z}/p^n\mathbb{Z} \mid \forall n \geq m \geq 0: \text{proj}_m^n(a_n) = a_m \right\} \\ &:= \varprojlim (\dots \rightarrow \mathbb{Z}/p^3\mathbb{Z} \rightarrow \mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow 0). \end{aligned}$$

**Proposition:** Mit komponentenweiser Addition und Multiplikation, dem Nullelement  $(0)_n$  und dem Einselement  $(1)_n$  ist  $\mathbb{Z}_p$  ein kommutativer unitärer Ring. Der natürliche Ringhomomorphismus  $\mathbb{Z} \rightarrow \mathbb{Z}_p, a \mapsto (a + p^n\mathbb{Z})_{n \geq 0}$  ist injektiv; wir identifizieren  $\mathbb{Z}$  mit seinem Bild.

**Proposition:** Es gibt eine natürliche Bijektion

$$\prod_{i=1}^{\infty} \{0, 1, \dots, p-1\} \longrightarrow \mathbb{Z}_p, \quad (\alpha_i)_{i \geq 0} \mapsto \left( \sum_{i=0}^{n-1} \alpha_i p^i + p^n\mathbb{Z} \right)_{n \geq 0}.$$

Wir schreiben die Elemente von  $\mathbb{Z}_p$  in  $p$ -adischer Ziffernentwicklung als  $\dots \alpha_2 \alpha_1 \alpha_0$ . Solche Zahlen addiert und multipliziert man genauso wie natürliche Zahlen zur Basis  $p$ .

**Bemerkung:** Die Situation ähnelt der von formalen Potenzreihen in  $\mathbb{F}_p[[X]]$ , nur dass man hier mit Übertrag rechnet.

**Beispiel:** Es ist  $\dots (p-1)(p-1)(p-1) = -1$  und  $\dots 111 = \frac{1}{1-p}$ .

**Bemerkung:** Anders als bei reellen Zahlen ist die Ziffernentwicklung hier eindeutig.

**Definition:** Für jedes  $\underline{a} = (a_n)_{n \geq 0} \in \mathbb{Z}_p$  mit Ziffernfolge  $(\alpha_i)_{i \geq 0}$  sei

$$\text{ord}_p(\underline{a}) := \begin{cases} \min\{n \geq 0 \mid a_{n+1} \neq 0\} \stackrel{!}{=} \min\{i \geq 0 \mid \alpha_i \neq 0\} & \text{falls } \underline{a} \neq 0, \\ \infty & \text{falls } \underline{a} = 0. \end{cases}$$

**Proposition:** Für jede ganze Zahl  $a$  ist  $\text{ord}_p(a) = \sup\{n \geq 0 : p^n \mid a\}$ .

**Grundeigenschaften:** Für alle  $\underline{a}, \underline{b} \in \mathbb{Z}_p$  gilt:

- (a)  $\text{ord}_p(\underline{a}) = \infty \Leftrightarrow \underline{a} = 0$ .
- (b)  $\text{ord}_p(\underline{a} \cdot \underline{b}) = \text{ord}_p(\underline{a}) + \text{ord}_p(\underline{b})$ .
- (c)  $\text{ord}_p(\underline{a} + \underline{b}) \geq \min\{\text{ord}_p(\underline{a}), \text{ord}_p(\underline{b})\}$ .

**Proposition:** Der Ring  $\mathbb{Z}_p$  ist ein Integritätsbereich. Seine Einheitengruppe ist

$$\mathbb{Z}_p^\times = \{\underline{a} \in \mathbb{Z}_p \mid \text{ord}_p(\underline{a}) = 0\} = \mathbb{Z}_p \setminus p\mathbb{Z}_p.$$

Seine Ideale sind das Nullideal (0) und die Ideale  $p^n\mathbb{Z}_p$  für alle  $n \geq 0$ . Insbesondere ist  $\mathbb{Z}_p$  ein Hauptidealring. Sein Quotientenkörper ist

$$\text{Quot}(\mathbb{Z}_p) = \bigcup_{m \geq 0} p^{-m}\mathbb{Z}_p = \mathbb{Z}_p[\frac{1}{p}].$$

**Definition:** Die Elemente von  $\mathbb{Z}_p$  heißen *ganze  $p$ -adische Zahlen*. Die Elemente von  $\mathbb{Q}_p := \text{Quot}(\mathbb{Z}_p)$  heißen (*rationale*)  *$p$ -adische Zahlen*.

**Definition:** Hat  $\underline{a} \in \mathbb{Z}_p$  die Ziffernentwicklung  $\dots \alpha_2 \alpha_1 \alpha_0$ , so schreiben wir  $p^{-m}\underline{a}$  mit Nachkommastellen in der Form  $\dots \alpha_{m+1} \alpha_m, \alpha_{m-1} \dots \alpha_0 00 \dots$ . Für jedes  $i \in \mathbb{Z}$  ist also die  $i$ -te Ziffer von  $p^{-m}\underline{a}$  gleich  $\alpha_{i+m}$  falls  $i \geq -m$  ist, und gleich 0 sonst.

Das Rechnen mit solchen Ausdrücken folgt denselben Regeln wie bei Dezimalbrüchen.

**Proposition-Definition:** Die obige Abbildung  $\text{ord}_p$  besitzt eine wohldefinierte Fortsetzung  $\text{ord}_p: \mathbb{Q}_p \rightarrow \mathbb{Z} \cup \{\infty\}$  mit  $\text{ord}_p(p^{-m}\underline{a}) = \text{ord}_p(\underline{a}) - m$  für alle  $\underline{a} \in \mathbb{Z}_p$  und  $m \in \mathbb{Z}^{\geq 0}$ . Diese Fortsetzung erfüllt dieselben Grundeigenschaften wie oben.

**Definition:** Die  *$p$ -adische Norm* von  $\underline{a} \in \mathbb{Q}_p$  ist

$$|\underline{a}|_p := \begin{cases} p^{-\text{ord}_p(\underline{a})} & \text{falls } \underline{a} \neq 0 \\ 0 & \text{falls } \underline{a} = 0 \end{cases} \in \mathbb{R}^{\geq 0}.$$

**Grundeigenschaften:** Für alle  $\underline{a}, \underline{b} \in \mathbb{Q}_p$  gilt:

- (a)  $|\underline{a}|_p = 0 \Leftrightarrow \underline{a} = 0$
- (b)  $|\underline{a} \cdot \underline{b}|_p = |\underline{a}|_p \cdot |\underline{b}|_p$
- (c)  $|\underline{a} + \underline{b}|_p \leq \max\{|\underline{a}|_p, |\underline{b}|_p\} \leq |\underline{a}|_p + |\underline{b}|_p$  (*verschärfte Dreiecksungleichung*)

**Folge:** Mit  $d(\underline{a}, \underline{b}) := |\underline{a} - \underline{b}|_p$  wird  $\mathbb{Q}_p$  zu einem metrischen Raum.

Damit haben wir die üblichen Begriffe von Stetigkeit und Konvergenz zur Verfügung.

**Proposition:** (a) Eine Folge  $(x_n)_{n \geq 0}$  in  $\mathbb{Q}_p$  konvergiert genau dann, wenn sie eine *Cauchyfolge* ist, das heisst, wenn gilt

$$\forall N \exists n_0 \forall n \geq m \geq n_0: \text{ord}_p(x_n - x_m) \geq N.$$

Mit anderen Worten ist  $\mathbb{Q}_p$  ein *vollständiger metrischer Raum*.

- (b) Der Grenzwert einer konvergenten Folge ist eindeutig bestimmt.
- (c) Eine Reihe  $\sum_{n \geq 0} x_n$  in  $\mathbb{Q}_p$  konvergiert genau dann, wenn  $\lim_{n \rightarrow \infty} \text{ord}_p(x_n) = \infty$  ist.
- (d) Konvergente Reihen in  $\mathbb{Q}_p$  kann man beliebig umordnen und aufteilen, wobei die Konvergenz und der Grenzwert erhalten bleibt.

**Proposition:** Für jede rationale  $p$ -adische Zahl  $\underline{a}$  mit Ziffernfolge  $(\alpha_i)_{i \in \mathbb{Z}}$  gilt

$$\underline{a} = \sum_{i \in \mathbb{Z}} \alpha_i p^i.$$

**Beispiel:** Es gilt  $\sum_{i \geq 0} p^i = \frac{1}{1-p}$  (*geometrische Reihe*).

**Proposition:** Für alle  $x \in p\mathbb{Z}_p$  und  $r, s \in \mathbb{Z}$  mit  $p \nmid s$  liefert die *binomische Reihe*

$$y := \sum_{n \geq 0} \binom{r/s}{n} \cdot x^n$$

eine Lösung der Gleichung  $y^s = (1+x)^r$  in  $\mathbb{Z}_p$ , also ein Element „ $(1+x)^{r/s}$ “.

**Beispiel:** In  $\mathbb{Z}_3$  konvergiert  $\underline{a} := \sum_{n \geq 0} \binom{1/2}{n} \cdot 6^n$  und erfüllt  $\underline{a}^2 = 1 + 6 = 7$ .

**Literatur:** Gouvêa: *p-adic Numbers*. Springer Verlag, ISBN 3-540-62911-4.

## 7.2 Topologische Gruppen (*nicht behandelt*)

**Definition:** Eine Gruppe  $G$  versehen mit einer Topologie, so dass die Abbildungen

$$\begin{aligned} G \times G &\rightarrow G, & (g, h) &\mapsto gh, \\ G &\rightarrow G, & g &\mapsto g^{-1} \end{aligned}$$

stetig sind, heisst eine *topologische Gruppe*.

**Beispiel:** Jede Gruppe wird mit der diskreten Topologie eine topologische Gruppe.

**Beispiel:** Die Gruppe  $GL_n(\mathbb{R})$  ist mit der von  $\text{Mat}_{n \times n}(\mathbb{R}) \cong \mathbb{R}^{n^2}$  induzierten Topologie eine topologische Gruppe. Analog für  $GL_n(\mathbb{C})$ , sowie für die abgeschlossenen Untergruppen  $O(n)$  und  $SO(n)$  und  $U(n)$ .

**Proposition:** Jede Untergruppe einer topologischen Gruppe wird mit der induzierten Topologie eine topologische Gruppe.

**Proposition:** Jedes (endliche oder unendliche) Produkt von topologischen Gruppen ist, versehen mit der Produkttopologie, eine topologische Gruppe.

**Proposition:** Für jede topologische Gruppe  $G$  und jedes  $g \in G$  sind die Abbildungen  $G \rightarrow G$ ,  $x \mapsto gx$  bzw.  $x \mapsto xg$  bzw.  $x \mapsto {}^g x$  Homöomorphismen.

**Proposition:** Jede offene Untergruppe einer topologischen Gruppe ist abgeschlossen.

**Definition:** Ein Gruppenisomorphismus zwischen topologischen Gruppen, der gleichzeitig ein Homöomorphismus ist, heisst ein *topologischer Isomorphismus*.

**Definition:** Eine topologische Gruppe, die topologisch isomorph zu einer abgeschlossenen Untergruppe eines (möglicherweise unendlichen) Produkts von diskreten endlichen Gruppen ist, heisst eine *pro-endliche Gruppe*.

**Proposition:** Für jede pro-endliche Gruppe  $G$  gilt:

- (a)  $G$  ist kompakt und hausdorffsch.
- (b) Jede offene Untergruppe von  $G$  hat endlichen Index.
- (c) Die offenen normalen Untergruppen von  $G$  bilden eine Umgebungsbasis des Einselements.

**Beispiel:** Die von der  $p$ -adischen Metrik auf  $\mathbb{Z}_p$  induzierte Topologie ist dieselbe wie die, welche von der Produkttopologie von  $\prod_{n \geq 0} \mathbb{Z}/p^n\mathbb{Z}$  induziert ist. Folglich sind die additive Gruppe  $(\mathbb{Z}_p, +)$  und die Einheitengruppe  $(\mathbb{Z}_p^\times, \cdot)$  pro-endliche Gruppen.

### 7.3 Unendliche Galoiserweiterungen (*nicht behandelt*)

Sei  $L/K$  eine beliebige Galoiserweiterung.

**Proposition:** Es existiert ein natürlicher injektiver Gruppenhomomorphismus

$$\text{Gal}(L/K) \rightarrow \prod_{K'} \text{Gal}(K'/K), \quad \gamma \mapsto (\gamma|_{K'})_{K'},$$

wobei das Produkt sich über alle Zwischenkörper  $K'$  erstreckt, welche endlich galoissch über  $K$  sind. Sein Bild ist die abgeschlossene Untergruppe

$$\{(\gamma_{K'})_{K'} \mid \forall K''/K'/K: \gamma_{K''}|_{K'} = \gamma_{K'}\}.$$

Damit wird  $\text{Gal}(L/K)$  zu einer pro-endlichen Gruppe.

**Hauptsatz der Galoistheorie:** Sei  $L/K$  galoissch mit der pro-endlichen Galoisgruppe  $\Gamma$ . Dann haben wir natürliche zueinander inverse Bijektionen

$$\begin{array}{ccc} \{\text{Zwischenkörper von } L/K\} & \xrightleftharpoons{\sim} & \{\text{abgeschlossene Untergruppen von } \Gamma\} \\ K' \longmapsto & & \longrightarrow \text{Gal}(L/K') \\ L^{\Gamma'} \longleftarrow & & \longleftarrow \Gamma' \end{array}$$

**Beispiel:** Die Erweiterung  $L := \mathbb{Q}(\bigcup_{n \geq 0} \mu_{p^n})/\mathbb{Q}$  ist unendlich galoissch mit Galoisgruppe  $\text{Gal}(L/K) \cong \mathbb{Z}_p^\times$ .

**Bemerkung:** Galoiserweiterungen eines Zahlkörpers mit Galoisgruppe  $\mathbb{Z}_p$  sind von besonderer Bedeutung in der Zahlentheorie und heissen  $\mathbb{Z}_p$ -Erweiterungen.

**Bemerkung:** Viele Grundfragen der Zahlentheorie, darunter hochinteressante Vermutungen, kann man als Fragen über die Struktur der Galoisgruppe  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  auffassen.

## Literatur

Dies sind einige Lehrbücher der Algebra, die ich als Begleitliteratur empfehlen kann. In der Stoffauswahl stimmt aber keines ganz mit der Vorlesung überein. Zu speziellen Themen, insbesondere zur Körpertheorie, gibt es weitere empfehlenswerte Bücher.

- *Bosch: Algebra. Springer Verlag, ISBN 978-3-540-29880-9.*  
Vor allem für die Galoistheorie empfohlen.
- *Fischer: Lehrbuch der Algebra. Vieweg Verlag, ISBN 978-3-8348-0226-2.*
- *Jantzen, Schwermer: Algebra. Springer Verlag, ISBN 978-3-540-21380-2.*  
Behandelt auch nichtkommutative Ringe, Dedekindringe und mehr zu Moduln.
- *Karpfinger, Meyberg: Algebra. Spektrum Verlag, ISBN 978-3-8274-2018-3.*  
Sehr ausführliche Beweise, greift aber auch weniger weit.
- *Kunz: Algebra, Vieweg Verlag. ISBN 3-528-17243-6.*
- *van der Waerden: Algebra I und II. Springer Verlag, ISBN 978-0-387-40624-4, ISBN 978-0-387-40625-1.* (Im Doppelpack günstiger?)  
Der Klassiker schlechthin, Ersterscheinung 1930, nach wie vor empfehlenswert.
- *Wüstholtz: Algebra, Vieweg Verlag. ISBN 978-3-528-07291-9.*  
Ehemaliger Kollege an der ETH Zürich.
- *Knapp: Basic Algebra. Springer Verlag, ISBN 978-0-8176-3248-9.*  
Englischsprachiges Lehrbuch.
- *Lang: Algebra. Springer Verlag, ISBN 978-0-387-95385-4.*  
Exzellentes englischsprachiges Werk, vor allem zum Nachschlagen und weniger fürs Selbststudium.