Algebra I und II

Prof. Richard Pink

Zusammenfassung
Herbstsemester 2015
Frühjahrssemester 2016
ETH Zürich

vorläufige Version

13. November 2015

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 Übungsserien. 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 2014–15 auf; für deren Zusammenfassung siehe
`people.math.ethz.ch/~pink/ftp/LA-Zusammenfassung-20150901.pdf`.

Inhalt

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

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

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)	$\forall x \in R$:	$1 \cdot x = x$	Neutrales Element der Multiplikation
(9)		$1 \neq 0$	Nichttrivialität
(10)	$\forall x \in R \smallsetminus \{0\}\ \exists x' \in R$:	$x' \cdot x = 1$	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

$$n \cdot x \ := \ \left\{ \begin{array}{ll} x + \ldots + x \ \text{ mit } n \text{ Summanden} & \text{falls } n > 0, \\ 0 & \text{falls } n = 0, \\ -(x + \ldots + x) \ \text{ mit } |n| \text{ Summanden} & \text{falls } n < 0. \end{array} \right.$$

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 $n \geqslant 0$ 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 $x, y \in K$ und alle $m, n \geqslant 0$ 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

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

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 $K^\times = K \smallsetminus \{0\}$.

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

1.3 Homomorphismen

Betrachte zwei Ringe R und S.

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

(a) $\varphi(1_R) = 1_S$.

(b) $\forall x, y \in R\colon\ \varphi(x+y) = \varphi(x) + \varphi(y)$.

(c) $\forall x, y \in R\colon\ \varphi(xy) = \varphi(x)\varphi(y)$.

Proposition: Für jeden Homomorphismus $\varphi\colon R \to S$ gilt:

(a) $\forall x \in R\ \forall n \in \mathbb{Z}\colon\ \varphi(nx) = n\varphi(x)$.

(b) $\forall x \in R\ \forall n \in \mathbb{Z}^{\geqslant 0}\colon\ \varphi(x^n) = \varphi(x)^n$.

(c) φ induziert einen Gruppenhomomorphismus $R^\times \to S^\times$.

Proposition: Die Identität $\mathrm{id}_R\colon R \to R$ 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 $\mathbb{Z} \to R$, nämlich die Abbildung $n \mapsto n \cdot 1_R$.

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

Proposition: Ein 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 Ringen ist eine Äquivalenzrelation.

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

1.4 Polynomringe

Sei N eine Menge, und sei $\underline{X} = (X_\nu)_{\nu\in N}$ ein System paarweise verschiedener neuer Symbole X_ν.

Konstruktion: Sei I_N die Menge aller Abbildungen $\underline{i}\colon N \to \mathbb{Z}^{\geqslant 0}$, $\nu \mapsto i_\nu$ mit endlichem Träger, das heisst, mit $i_\nu = 0$ für fast alle ν. Sei $R[\underline{X}]$ die Menge aller Abbildungen $I_N \to R$, $\underline{i} \mapsto a_{\underline{i}}$ mit endlichem Träger, das heisst, mit $a_{\underline{i}} = 0$ für fast alle $\underline{i}$. Für zwei Elemente von $R[\underline{X}]$ definieren wir

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

Betrachte weiter die Abbildung

$$\iota\colon\ R \to R[\underline{X}],\ a \mapsto \Big(\begin{cases} a & \text{wenn alle } i_\nu = 0 \text{ sind,} \\ 0 & \text{sonst} \end{cases} \Big)_{\underline{i}}$$

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

$$X_\nu\ :=\ \Big(\begin{cases} 1 & \text{wenn } i_\nu = 1 \text{ ist und alle anderen } i_{\nu'} = 0, \\ 0 & \text{sonst} \end{cases} \Big)_{\underline{i}} \in R[\underline{X}].$$

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

Wir identifizieren R mit seinem Bild unter ι. Für alle $\underline{i} \in I_N$ schreiben wir

$$\underline{X}^{\underline{i}}\ :=\ \prod_{\nu\in N}{}' X_\nu^{i_\nu}\ \overset{!}{=}\ \Big(\begin{cases} 1 & \text{wenn } \underline{i}' = \underline{i}, \\ 0 & \text{sonst} \end{cases} \Big)_{\underline{i}'}.$$

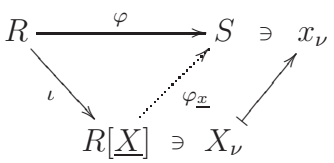
Dann hat jedes Element von $R[\underline{X}]$ die Form

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

Einen solchen Ausdruck nennen wir ein *Polynom*. Ein Ausdruck der Form $a\underline{X}^{\underline{i}}$ für $a \in R$ heisst ein *Monom*. Für alle $\underline{i}, \underline{j} \in I_N$ gilt

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

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



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

$$R[\underline{X}] \to S,\ F(\underline{X}) = \sum_{\underline{i}\in I_N}{}' a_{\underline{i}}\underline{X}^{\underline{i}} \mapsto F(\underline{x}) := \sum_{\underline{i}\in I_N}{}' \varphi(a_{\underline{i}})\underline{x}^{\underline{i}}.$$

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

$$S^N \to S,\ \underline{x} \mapsto F(\underline{x}).$$

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

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

$$\sum_{\underline{i}\in I_N}{}' a_{\underline{i}}\underline{X}^{\underline{i}} \ \mapsto \sum_{\underline{i}\in I_N}{}' \varphi(a_{\underline{i}})\underline{X}^{\underline{i}}.$$

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

$$K[\underline{X}] \xrightarrow{\sim} SV := \coprod_{r\geqslant 0} S^r V, \quad \sum_{\underline{i}\in I_N}{}' a_{\underline{i}}\underline{X}^{\underline{i}} \ \mapsto \sum_{\underline{i}\in I_N}{}' a_{\underline{i}}\underline{X}^{\underline{i}}.$$

Notation: Im Fall $\underline{X} = (X_1, \ldots, X_n)$ schreiben wir auch $R[X_1, \ldots, X_n] := R[\underline{X}]$.

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

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

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

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

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

$$(a_{\underline{i}})_{\underline{i}} \ = \ \sum_{\underline{i}\in I_N} a_{\underline{i}}\underline{X}^{\underline{i}},$$

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 $X_1, \ldots, X_n$ über R*. Mit dieser Notation unterliegen alle Rechnungen denselben Regeln wie für Potenzreihen in der Analysis.

1.5 Unterringe, Produkte

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

(a) $\forall x, y \in R' \colon\ x + y \in R'$.
(b) $\forall x, y \in R' \colon\ xy \in R'$.
(c) $\forall x \in R' \colon\ -x \in R'$.
(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: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Beispiel: $R \subset R[\underline{X}] \subset R[[\underline{X}]]$.

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 allen Elementen der Form

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

mit $n \geqslant 0$ 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 $R'[a_1, \dots, a_n] := R'[\{a_1, \dots, a_n\}]$.

Bemerkung: Dies bewirkt keine Kollision mit der Notation für den Polynomring $R[X_1, \dots, X_n]$, da letzterer tatsächlich der von den Elementen $X_1, \dots, X_n$ über R erzeugte Unterring von $R[X_1, \dots, X_n]$ ist.

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 $\mathbb{Z}[\sqrt{7}\,]^\times = \{\pm(8 + 3\sqrt{7})^n \mid n \in \mathbb{Z}\}$.

Proposition-Definition: Das *kartesische Produkt* von Ringen $R_1 \times \ldots \times R_n$ mit komponentenweiser Addition und Multiplikation sowie dem Nullelement $(0, \dots, 0)$ und dem Einselement $(1, \dots, 1)$ ist ein Ring. Für diesen gilt weiter $(R_1 \times \ldots \times R_n)^\times = R_1^\times \times \ldots \times R_n^\times$ 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 $f\colon X \to R$ 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 $R^n = R \times \ldots \times R = R^{\{1,\ldots,n\}}$ 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 $\mathbb{C}$.

1.6 Matrizen

Für alle natürlichen Zahlen m, n bezeichnet $\mathrm{Mat}_{m\times n}(R)$ 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.

Lemma: Sei K ein unendlicher Körper, und sei $f \in K[X_1, \ldots, X_n]$ mit $f(\underline{a}) = 0$ für alle $\underline{a} \in K^n$. Dann ist $f = 0$.

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

Beispiel: Für alle Matrizen entsprechender Grösse 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 $\tilde{A} := \big((-1)^{i+j} \cdot \det(A_{ji})\big)_{i,j}$ von A.

(e) $\mathrm{char}_A(A) = 0$ für das charakteristische Polynom $\mathrm{char}_A(X) := \det(X \cdot I_n - A)$.

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

(a) Es existiert $A' \in \mathrm{Mat}_{n\times n}(R)$ mit $AA' = A'A = I_n$. Dann heisst A *invertierbar*.

(b) Es existiert $A' \in \mathrm{Mat}_{n\times n}(R)$ mit $AA' = I_n$.

(c) Es existiert $A' \in \mathrm{Mat}_{n\times n}(R)$ 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 $\mathrm{GL}_n(R)$ 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 $x \in R \smallsetminus \{0\}$ mit

$$\exists y \in R \smallsetminus \{0\}\colon \ xy = 0.$$

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

Proposition: In jedem Integritätsbereich gilt die *Kürzungsregel*:

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

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 $R \times (R \smallsetminus \{0\})$ ist durch

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

eine Äquivalenzrelation definiert. Bezeichne die Äquivalenzklasse eines Paars (x,y) mit $[(x,y)]$ und die Menge aller Äquivalenzklassen mit $\mathrm{Quot}(R)$. 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 $\mathrm{Quot}(R)$. Betrachte weiter die Abbildung

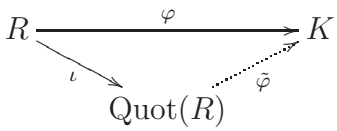
$$\iota\colon\ R \to \mathrm{Quot}(R),\ x \mapsto [(x,1)]$$

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

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

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

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



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 $\varphi\colon R \to S$ setzt sich fort zu einem eindeutigen Ringhomomorphismus $\tilde{\varphi}\colon \mathrm{Quot}(R) \to \mathrm{Quot}(S)$.

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

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

Definition: Für jeden Körper K heisst $K(X_1, \ldots, X_n) := \mathrm{Quot}(K[X_1, \ldots, X_n])$ der Körper der *rationalen Funktionen in den Variablen $X_1, \ldots, X_n$ 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) $\mathfrak{a} \neq \varnothing$.

(b) $\forall a, b \in \mathfrak{a}\colon\ a + b \in \mathfrak{a}$.

(c) $\forall x \in R\ \forall a \in \mathfrak{a}\colon\ xa \in \mathfrak{a}$.

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

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

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

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

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

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

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

Proposition: Für jede Teilmenge A eines Ideals $\mathfrak{a}$ gilt $(A) \subset \mathfrak{a}$.

Bemerkung: Jeder gemeinsame Teiler von Elementen $a_1, \ldots, a_n$ ist ein gemeinsamer Teiler aller Elemente des Ideals $(a_1, \ldots, a_n)$. 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

$$\mathfrak{a}\mathfrak{b} \;:=\; \mathfrak{a} \cdot \mathfrak{b} := \; \Big\{ \sum_{i=1}^{n} a_i b_i \;\Big|\; \text{alle } n \geqslant 0,\ a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \Big\}.$$

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

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

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

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

Proposition: Für jeden Ringhomomorphismus $\varphi\colon R \to S$ ist

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

Dabei ist $\operatorname{Kern}(\varphi) = (0)$ genau dann, wenn φ injektiv ist, und $\operatorname{Bild}(\varphi) = S$ genau dann, wenn φ 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 $x, x' \in R$:

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

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

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

(b) $\forall x, x' \in R : (x + \mathfrak{a}) \cdot (x' + \mathfrak{a}) = xx' + \mathfrak{a}$.

Für diese gilt weiter:

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

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

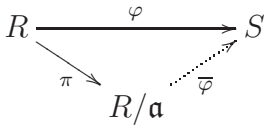
(e) $\pi\colon R \to R/\mathfrak{a}$, $x \mapsto x + \mathfrak{a}$ ist ein surjektiver Ringhomomorphismus mit Kern $\mathfrak{a}$.

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 π ein Isomorphismus ist.

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



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

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

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

1.11 Primideale

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

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

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.

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

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

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.

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

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

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

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

(a) $(M, +, 0)$ ist eine abelsche Gruppe.
(b) $\forall x \in R\ \forall m, n \in M\colon\ x(m+n) = xm + xn$ (Linksdistributivität)
(c) $\forall x, y \in R\ \forall m \in M\colon\ (x+y)m = xm + ym$ (Rechtsdistributivität)
(d) $\forall x, y \in R\ \forall m \in M\colon\ x(ym) = (xy)m$ (Assoziativität)
(e) $\forall m \in M\colon\ 1 \cdot m = m$ (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 *Untermodul* eines R-Moduls M ist eine Teilmenge $N \subset M$ mit den Eigenschaften:

(a) $N \neq \varnothing$.
(b) $\forall n, n' \in N\colon\ n + n' \in N$.
(c) $\forall x \in R\ \forall n \in N\colon\ xn \in N$.

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 $m_1, \ldots, m_n \in M$ gilt

$$\langle \{m_1, \ldots, m_n\} \rangle \;=\; \left\{\, x_1 m_1 + \ldots + x_n m_n \;\middle|\; \forall i\colon x_i \in R \,\right\}.$$

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

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

$$M_1 + \ldots + M_n \;:=\; \left\{\, m_1 + \ldots + m_n \;\middle|\; \forall i\colon m_i \in M_i \,\right\}$$

ist ein Untermodul. Ist die Abbildung

$$M_1 \times \ldots \times M_n \to M_1 + \ldots + M_n,\ (m_1, \ldots, m_n) \mapsto m_1 + \ldots + m_n$$

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

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

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

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

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 $\bigoplus$ bezeichnet. Welche dann jeweils gemeint ist, muss man aus dem Zusammenhang erschliessen.

Definition: Eine Abbildung zwischen zwei R-Moduln $\varphi\colon M \to N$ 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 $M \to N$ wird bezeichnet mit $\mathrm{Hom}_R(M, N)$. Ein Homomorphismus $M \to M$ heisst ein *Endomorphismus von M*, und wir schreiben $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$.

Proposition: Für jeden Homomorphismus $\varphi\colon M \to N$ gilt:

(a) $\mathrm{Kern}(\varphi) := \{m \in M \mid \varphi(m) = 0\}$ ist ein Untermodul von M.

(b) $\mathrm{Bild}(\varphi)$ ist ein Untermodul von N.

(c) φ ist injektiv genau dann, wenn $\mathrm{Kern}(\varphi) = 0$ ist.

(d) φ ist surjektiv genau dann, wenn $\mathrm{Bild}(\varphi) = N$ ist.

Beispiel: Die *identische Abbildung* $\mathrm{id}_M\colon M \to M$, $m \mapsto m$ 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 $A \in \mathrm{Mat}_{m\times n}(R)$ einen Homomorphismus

$$L_A\colon\ R^n \to R^m,\ m \mapsto Am.$$

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

Definition: Ein Homomorphismus $\varphi\colon M \to N$ mit einem beidseitigem Inversen $\varphi^{-1}\colon N \to M$ heisst ein *Isomorphismus*, und wir schreiben dann $\varphi\colon M \xrightarrow{\sim} N$. 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 $(0) \subsetneqq \mathfrak{a} \subsetneqq R$ 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 $\mathrm{Aut}_R(M)$ aller Automorphismen von M ist eine Gruppe bezüglich Komposition mit dem Einselement id_M, genannt die *Automorphismengruppe von M*.

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

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

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

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

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 $\pi\colon M \to M/N$, $m \mapsto m + N$ ist ein surjektiver Modulhomomorphismus mit Kern N.

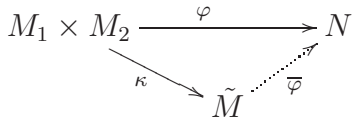
Homomorphiesatz: Jeder Homomorphismus $\varphi\colon M \to N$ induziert einen Isomorphismus

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

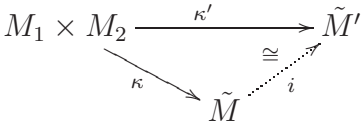
Das Tensorprodukt von R-Moduln wird genauso definiert und konstruiert wie das Tensorprodukt von Vektorräumen:

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

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



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 $i\colon \tilde{M} \xrightarrow{\sim} \tilde{M}'$ mit $i \circ \kappa = \kappa'$, das heisst, so dass das folgende Diagramm kommutiert:



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 κ mit

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

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 $\exists x \in R\colon ax = b$, 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 $\exists x \in R^\times\colon ax = b$, 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 $a \mid \sum_i x_i b_i$.

(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

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

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

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

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 $\geqslant 2$, 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 $m \geqslant 0$, und Primelemente $p_1, \ldots, p_m$.

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

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

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

Bemerkung: Wegen der eindeutigen Primfaktorzerlegung nennt man einen faktoriellen Ring auch einen *ZPE-Ring* für *„Zerlegung in Primfaktoren Eindeutig“*.

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

Proposition: Sei $\{p_i \mid i \in I\}$ ein Repräsentantensystem der 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 $\mu_i \in \mathbb{Z}^{\geqslant 0}$, 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 $\mu_i \leqslant \nu_i$.

(c) Jedes Element von $\mathrm{Quot}(R) \setminus \{0\}$ 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 $a_1, \ldots, a_n \in R$.

(a) Ein Element $b \in R$ mit $\forall i\colon b|a_i$ heisst ein *gemeinsamer Teiler von* $a_1, \ldots, a_n$.

(b) Es existiert ein gemeinsamer Teiler b von $a_1, \ldots, a_n$, so dass für jeden gemeinsamen Teiler b' von $a_1, \ldots, a_n$ gilt $b'|b$.

(c) Dieser *grösste gemeinsame Teiler von* $a_1, \ldots, a_n$ ist eindeutig bis auf Assoziiertheit. Wir bezeichnen jeden solchen mit $\mathrm{ggT}(a_1, \ldots, a_n)$.

Da der ggT nur eindeutig bis auf Assoziiertheit ist, sollte man ihn immer nur auf Assoziiertheit testen und nicht auf Gleichheit.

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

$$\mathrm{ggT}(a_1, \ldots, a_n) \;\sim\; \mathrm{ggT}(a_1, \ldots, a_n, \textstyle\sum_{i=1}^{n} x_i a_i).$$

Definition: Elemente $a_1, \ldots, a_n \in R$ mit

(a) $\mathrm{ggT}(a_1, \ldots, a_n) \sim 1$ heissen *teilerfremd*.

(b) $\mathrm{ggT}(a_i, a_j) \sim 1$ für alle $i \neq j$ heissen *paarweise teilerfremd*.

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

(a) Ein Element $b \in R$ mit $\forall i\colon a_i|b$ heisst *gemeinsames Vielfaches von* $a_1, \ldots, a_n$.

(b) Es existiert ein gemeinsames Vielfaches b von $a_1, \ldots, a_n$, so dass für jedes gemeinsame Vielfache b' von $a_1, \ldots, a_n$ gilt $b|b'$.

(c) Dieses *kleinste gemeinsame Vielfache von* $a_1, \ldots, a_n$ ist eindeutig bis auf Assoziiertheit. Wir bezeichnen jedes solche mit $\mathrm{kgV}(a_1, \ldots, a_n)$.

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

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

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

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

2.4 Hauptidealringe

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

Satz: Sei R ein Hauptidealring.

(a) Jede aufsteigende Folge von Idealen $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots$ wird stationär, das heisst, es existiert $n \geqslant 0$ mit $\mathfrak{a}_n = \mathfrak{a}_m$ für alle $m \geqslant n$. (Ein Ring mit dieser Eigenschaft heisst *noethersch*.)

(b) Für jedes $a \in R \smallsetminus (\{0\} \cup R^\times)$ existiert ein Primelement $p \in R$ mit $p|a$.

(c) R ist faktoriell.

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

$$\big(\mathrm{ggT}(a_1, \ldots, a_n)\big) \;=\; (a_1, \ldots, a_n).$$

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

$$\mathrm{ggT}(a_1, \ldots, a_n) \;=\; x_1 a_1 + \ldots + x_n a_n.$$

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 $\mathrm{ggT}(X,Y) \sim 1$, aber $(X,Y) \neq (1)$. Der ggT lässt sich hier nicht als Linearkombination von X und Y darstellen.

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

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

$$\begin{array}{ccc} R/(a_1 \cdots a_n) & \longrightarrow & R/(a_1) \times \ldots \times R/(a_n), \\ x + (a_1 \cdots a_n) & \mapsto & \big(x + (a_1), \ldots, x + (a_n)\big). \end{array}$$

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 $\delta\colon R \smallsetminus \{0\} \to \mathbb{Z}^{\geqslant 0}$, so dass gilt

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

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

Satz: Jeder euklidische Ring ist ein Hauptidealring.

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

(a) Seine Ideale sind genau die Ideale $(n) = n\mathbb{Z}$ für alle $n \geqslant 0$.

(b) Die maximalen Ideale von $\mathbb{Z}$ sind die (p) für alle Primzahlen p, mit dem zugehörigen Restklassenkörper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

(c) Das einzige weitere Primideal von $\mathbb{Z}$ ist das Nullideal (0).

(d) 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 $d \geqslant 1$ ist der Ring $\mathbb{Z}[i\sqrt{d}]$ euklidisch, bzw. ein Hauptidealring, bzw. faktoriell genau dann, wenn $d \leqslant 2$ 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 $\mathbb{Z}\big[\frac{1}{2} \cdot (1 + i\sqrt{163})\big]$ ein Hauptidealring, aber nicht euklidisch.

Euklidischer Algorithmus: Sei (R, δ) euklidisch und betrachte Elemente $a_1, a_2 \in R$, nicht beide gleich Null. Wir setzen diese fort zu einer Folge $a_1, \ldots, a_n$ 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

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

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 $n \geqslant 1$, 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 $n \geqslant 2$. Für das letzte von Null verschiedene Element a_{m-1} liefert dies eine Linearkombination

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

Beispiel: In $\mathbb{Z}$ ist $\mathrm{ggT}(2015, 1959) \sim 1 = 35 \cdot 2015 - 36 \cdot 1959$.

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

$$I(f) \;:=\; \mathrm{ggT}(a_0, \ldots, a_n) \;\in\; R \setminus \{0\}.$$

(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 $K[X] \setminus \{0\} \to K^\times$, $f \mapsto I(f)$ mit denselben Eigenschaften für alle $f \in K[X] \setminus \{0\}$ und $a \in K^\times$.

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

Satz: (a) Die Primelemente von $R[X]$ sind genau die Primelemente von R sowie die primitiven Polynome in $R[X] \setminus \{0\}$, die in $K[X]$ prim sind.

(b) 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 $n \geqslant 0$ ist $R[X_1, \ldots, X_n]$ faktoriell. Insbesondere ist für jeden Körper K der Ring $K[X_1, \ldots, X_n]$ 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 $R \twoheadrightarrow R/(p)$, $a \mapsto \overline{a} := a + (p)$ induziert einen Homomorphismus

$$R[X] \twoheadrightarrow (R/(p))[X],\ f = \sum{}' a_i X^i \mapsto \overline{f} := \sum{}' \overline{a_i} X^i.$$

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

Proposition: Jedes primitive Element $f \in R[X] \smallsetminus \{0\}$ mit $\deg(f) = \deg(\overline{f})$ und $\overline{f}$ 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 $n \geqslant 1$ und $p \nmid a_n$ und $\forall i < n\colon p | a_i$ und $p^2 \nmid a_0$. Dann ist f irreduzibel.

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

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

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

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

Beispiel: Für jedes $n \geqslant 1$ ist das Polynom $X^n + Y^n + Z^n \in \mathbb{C}[X, Y, Z]$ 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 $U \in \mathrm{GL}_m(R)$ und $V \in \mathrm{GL}_n(R)$ sowie eine Zahl $0 \leqslant k \leqslant \min\{m, n\}$ und Elemente $e_1, \ldots, e_k \in R \smallsetminus \{0\}$ mit $e_1 | e_2 | \ldots | e_k$, 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 $\mathrm{Quot}(R)$.

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

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

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

Folge: Für alle $n \geqslant 1$ und alle $a_1, \ldots, a_n$ in einem Hauptidealring R sind äquivalent:

(a) $\mathrm{ggT}(a_1, \ldots, a_n) \sim 1$.

(b) Es existiert eine Matrix in $\mathrm{GL}_n(R)$ mit erster Spalte $(a_1, \ldots, a_n)^T$.

Beispiel: Sei p ein Primelement eines Hauptidealrings R und seien $i, j \in \mathbb{Z}^{\geqslant 0}$ 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 $(e_1, e_2) = \begin{cases} (p^i, p^j) & \text{falls } i \leqslant j \text{ und } p^i | a, \\ (p^j, p^i) & \text{falls } j \leqslant i \text{ und } p^j | a, \\ (p^k, p^{i+j-k}) & \text{falls } p^i \nmid a \text{ und } p^j \nmid a. \end{cases}$

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 $r, k \geqslant 0$ und Elemente $e_1, \ldots, e_k \in R \smallsetminus (\{0\} \cup R^\times)$ mit $e_1 | e_2 | \ldots | e_k$, so dass gilt

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

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

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 $e_1, \ldots, e_k$ sind bis auf Assoziiertheit durch M eindeutig bestimmt. Sie heissen die *Elementarteiler von M*.

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

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

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

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

Insbesondere sind die Zahlen r und ℓ, sowie die Paare (p_i, ν_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 $\varphi \in \mathrm{End}_K(V)$ wird durch

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

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, φ).

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 $\varphi \in \mathrm{End}_K(M)$ hat das charakteristische Polynom f und das Minimalpolynom f.

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

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

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

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

(a) Das charakteristische Polynom von φ ist gleich $p_1^{\nu_1} \cdots p_k^{\nu_k}$.

(b) Das Minimalpolynom von φ ist gleich $\mathrm{kgV}(p_1^{\nu_1}, \ldots, p_k^{\nu_k})$.

(c) Der Hauptraum von φ zum normierten irreduziblen Polynom p entspricht den Summanden in der obigen Zerlegung mit $p_i = p$.

(d) Jordansche Normalform.

Satz: Sei φ ein Endomorphismus eines endlich-dimensionalen Vektorraums V über einem algebraisch abgeschlossenen Körper K.

(a) Es existieren ein diagonalisierbarer Endomorphismus φ_s und ein nilpotenter Endomorphismus φ_n mit $\varphi_s\varphi_n = \varphi_n\varphi_s$ und $\varphi_s + \varphi_n = \varphi$.

(b) Diese sind durch φ eindeutig bestimmt.

(c) Beide können durch Polynome in φ mit Koeffizienten in K ausgedrückt werden.

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

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 $A_sA_n = A_nA_s$ 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

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

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

$$\begin{array}{rll} \forall a, b, c \in G: & a \circ (b \circ c) = (a \circ b) \circ c & \text{(Assoziativität)} \\ \forall a \in G: & e \circ a = a & \text{(Linksneutrales Element)} \\ \forall a \in G\ \exists a' \in G: & a' \circ a = e & \text{(Linksinverses Element)} \end{array}$$

Die Gruppe heisst *kommutativ* oder *abelsch*, wenn zusätzlich gilt:

$$\forall a, b \in G: \quad a \circ b = b \circ a \qquad \text{(Kommutativität)}$$

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 dafür ist a^{-1}.

(e) Für alle $a \in G$ gilt $(a^{-1})^{-1} = a$.

(f) Für alle $a, b \in G$ gilt $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

(g) Für alle $a, b \in G$ existiert ein eindeutiges $x \in G$ mit $a \circ x = b$, nämlich $x = a^{-1} \circ b$.

(h) Für alle $a, b \in G$ existiert ein eindeutiges $y \in G$ mit $y \circ a = b$, nämlich $y = b \circ a^{-1}$.

(i) Für alle $a, b, c \in G$ gilt $b = c \iff a \circ b = a \circ c$. *(Kürzungsregel links)*

(j) Für alle $a, b, c \in G$ gilt $b = c \iff b \circ a = c \circ a$. *(Kürzungsregel rechts)*

Proposition: Für jede natürliche Zahl $n \geqslant 1$ und für beliebige $a_1, \ldots, a_n \in G$ gilt: Bei jeder möglichen Klammerung der (a priori nicht wohldefinierten) Formel $a_1 \circ \ldots \circ a_n$ ist das Resultat gleich. Wir dürfen hier also doch auf Klammern verzichten.

Konvention: Oft schreibt man nur kurz G für das ganze Tripel und sieht die Zusatzdaten als implizit mitgegeben an. Wenn dabei keine Notation für 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:

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

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 Matrizengruppen $\mathrm{GL}_n(K)$, $\mathrm{SL}_n(K)$, $\mathrm{O}(n)$, $\mathrm{SO}(n)$, $\mathrm{U}(n)$.

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

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

(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*. Er ist invariant unter n Drehungen um seine Symmetrieachse, sowie n weiteren Drehungen um 180°, 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) $H \neq \varnothing$.

(b) $\forall h, h' \in H\colon\ hh' \in H$.

(c) $\forall h \in H\colon\ h^{-1} \in H$.

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 abelsche 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 $n \geqslant 0$.

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 $n \geqslant 0$, 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 $\langle a_1, \ldots, a_n \rangle = \langle \{a_1, \ldots, a_n\} \rangle$. Ist $G = \langle S \rangle$, so nennen wir G selbst *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 $n \geqslant 1$ sind zyklisch. Die Untergruppen von $\mathbb{Z}$ sind die $m\mathbb{Z}$ für alle $m \geqslant 0$; 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

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

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

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

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

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

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

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

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

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

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

Beispiel: (a) Die Kommutatorgruppe von $\mathrm{GL}_n(K)$ ist $\mathrm{SL}_n(K)$, falls $|K| > 2$ ist.

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

(c) Das Zentrum von $\mathrm{GL}_n(K)$ 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

$$\begin{aligned} XY &:= \{xy \mid x \in X, y \in Y\}, \\ gX &:= \{gx \mid x \in X\}, \\ Xg &:= \{xg \mid x \in X\}, \\ X^{-1} &:= \{x^{-1} \mid x \in X\}. \end{aligned}$$

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

$$\begin{aligned} (XY)^{-1} &= Y^{-1}X^{-1} \\ (gX)^{-1} &= X^{-1}g^{-1} \\ (Xg)^{-1} &= g^{-1}X^{-1} \\ XY &= YX \qquad \text{falls } G \text{ abelsch ist,} \\ gX &= Xg \qquad \text{falls } G \text{ abelsch ist.} \end{aligned}$$

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

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

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

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

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

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

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

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 $\mathrm{ord}(g) := |\langle g \rangle|$.

(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 $n \geqslant 1$ mit $g^n = 1$, falls diese existiert, und andernfalls ∞.

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 $\mathrm{ord}(g)$ 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 $n \geqslant 1$ mit der Eigenschaft $\forall g \in G\colon\ g^n = 1$, falls diese existiert, und andernfalls ∞.

Der Exponent ist also das kleinste gemeinsame Vielfache von $\mathrm{ord}(g)$ 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

Betrachte Gruppen G und H.

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

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

Dann heissen weiter

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

Proposition: Für jeden Homomorphismus $\varphi\colon G \to H$ gilt

(a) $\forall g \in G\colon\ \forall n \in \mathbb{Z}\colon\ \varphi(g^n) = \varphi(g)^n$.
Insbesondere ist $\varphi(1_G) = 1_H$ und $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(b) $\mathrm{Kern}(\varphi)$ ist eine Untergruppe von G.

(c) $\mathrm{Bild}(\varphi)$ ist eine Untergruppe von H.

(d) φ ist injektiv genau dann, wenn $\mathrm{Kern}(\varphi) = 1$ ist.

(e) φ ist surjektiv genau dann, wenn $\mathrm{Bild}(\varphi) = H$ ist.

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

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

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

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

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 $\varphi\colon G \to H$, für den ein beidseitiger *inverser Homomorphismus* $\varphi^{-1} : H \to G$ existiert, heisst ein *Isomorphismus*, und wir schreiben dann $\varphi\colon G \xrightarrow{\sim} H$. 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 ausgewählte 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 $(\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$.

3.7 Abelsche Gruppen

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

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

Dabei sind r und ℓ, sowie die Paare (p_i, ν_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

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

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 $\mathrm{Aut}(G)$.

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

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

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

$$ \mathrm{int}_g \colon G \to G,\ x \mapsto {}^g x $$

ein Automorphismus von G. Weiter ist die Abbildung

$$ G \to \mathrm{Aut}(G),\ g \mapsto \mathrm{int}_g $$

ein Homomorphismus mit Kern $Z(G)$.

Definition: Die Abbildung $\mathrm{int}_g \colon G \to G$ heisst *Konjugation mit g*. Ein Automorphismus der Form 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) $\forall g \in G\colon\ {}^gN = N$

(b) $\forall g \in G\colon\ {}^gN \subset N$

(c) $\forall g \in G\colon\ gN = Ng$

(d) Jede Linksnebenklasse von N ist gleichzeitig eine Rechtsnebenklasse 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 $N \lhd G$ oder $G \rhd N$.

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

Beispiel: In einer abelschen Gruppe ist jede Untergruppe normal.

Proposition: Jede Untergruppe vom Index 2 ist normal.

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

3.10 Faktorgruppen

Betrachte einen Normalteiler $N \lhd G$.

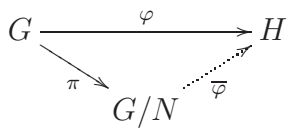
Proposition: Die Menge G/N besitzt eine eindeutige Gruppenstruktur mit

$$\forall g, g' \in G\colon\ (gN)(g'N) = gg'N.$$

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

Proposition: Die Abbildung $\pi\colon G \to G/N$, $g \mapsto gN$ ist ein Homomorphismus.

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



Homomorphiesatz: Jeder Homomorphismus $\varphi\colon G \to H$ induziert einen Isomorphismus

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

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

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

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

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

3.11 Operationen

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

$$\sigma\colon G \times X \to X,\ (g,x) \mapsto \sigma(g,x)$$

mit den Eigenschaften:

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

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

$$\rho\colon X \times G \to X,\ (x,g) \mapsto \rho(x,g)$$

mit den Eigenschaften:

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

Proposition: Jede Linksoperation σ entspricht einer Rechtsoperation ρ, und umgekehrt, vermittels 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.

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 $(S(X), \circ, \mathrm{id}_X)$ eine Gruppe, genannt die *symmetrische Gruppe der Menge* X.

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

Bemerkung: Oft will man, dass eine Operation mit Zusatzstrukturen auf X verträglich ist, das heisst, dass der Homomorphismus $G \to S(X)$ durch die Untergruppe aller strukturerhaltenden Automorphismen von X faktorisiert.

Beispiel: Sei H eine weitere Gruppe. Ein Homomorphismus $\varphi\colon G \to \mathrm{Aut}(H)$ entspricht einer Linksoperation σ von G auf der Menge H mit der weiteren Eigenschaft

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

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

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

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

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

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

Insbesondere ist X die disjunkte Vereinigung aller Bahnen von G.

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

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

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

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

Insbesondere gelten die *Bahnengleichungen*

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

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 $\mathrm{Cent}_G(x)$. Die Menge der Fixpunkte von G ist das Zentrum $Z(G)$.

Beispiel: Die Konjugationsklassen in $\mathrm{GL}_n(K)$ 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:

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

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

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

Proposition: Für jedes $H < G$ gilt $H \lhd \mathrm{Norm}_G(H)$ und $H \lhd \mathrm{Cent}_G(H) \lhd \mathrm{Norm}_G(H)$.

Beispiel: Sei $T < \mathrm{GL}_n(K)$ die Untergruppe aller Diagonalmatrizen. Ist $|K| > 2$, so ist $\mathrm{Norm}_{\mathrm{GL}_n(K)}(T)$ 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 $X \neq \varnothing$ und $\forall x, x' \in X\ \exists g \in G\colon\ gx = x'$.

(b) *frei*, wenn gilt $\forall x \in X\colon G_x = \{1\}$.

(c) *treu*, wenn gilt $\bigcap_{x \in X} G_x = \{1\}$.
Äquivalent: Der entsprechende Homomorphismus $G \to S(X)$ ist injektiv.

(d) *trivial*, wenn gilt $\forall g \in G\ \forall x \in X\colon gx = x$.

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

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

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

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

3.14 Symmetrische Gruppe

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

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 $1 \leqslant i < j \leqslant n$ und $\sigma i > \sigma j$ heisst ein *Fehlstand von* σ. Die Zahl

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

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

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

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

Proposition: Für $n \geqslant 2$ gilt $|A_n| = \frac{n!}{2}$.

Definition: Für paarweise verschiedene Elemente $i_1, \ldots, i_k \in \{1, \ldots, n\}$ bezeichnet $(i_1 \;\ldots\; i_k)$ die Permutation in S_n mit

$$\begin{aligned} &i_1 \mapsto i_2 \mapsto \ldots \mapsto i_k \mapsto i_1 \quad \text{und} \\ &i \mapsto i \;\text{ für alle } i \notin \{i_1, \ldots, i_k\}. \end{aligned}$$

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

Proposition: (a) Zwei Zykel $(i_1 \;\ldots\; i_k)$ und $(j_1 \;\ldots\; j_\ell)$ sind gleich genau dann, wenn $k = \ell$ ist und ein $1 \leqslant m \leqslant k$ existiert mit $(j_1, \ldots, j_\ell) = (i_{m+1}, \ldots, i_k, i_1, \ldots, i_m)$.

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

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

(d) Für jeden Zykel und jedes $\sigma \in S_n$ gilt ${}^{\sigma}(i_1 \;\ldots\; i_k) = (\sigma i_1 \;\ldots\; \sigma i_k)$.

Proposition: Je zwei k-Zykel in S_n sind konjugiert.

Proposition: Jede Permutation ist ein Produkt von benachbarten Transpositionen, das heisst von Transpositionen der Form $(i \;\; i{+}1)$ für gewisse $1 \leqslant i < n$.

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

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 $\{1, \ldots, n\}$.

Definition: Eine Folge $(d_1, d_2, \ldots)$ in $\mathbb{Z}^{\geqslant 0}$ mit $\sum'_{k\geqslant 1} d_k k = n$ heisst eine *(ungeordnete) Partition von n.*

Proposition: Für jedes $\sigma \in S_n$ sei d_k die Anzahl der Bahnen der Länge k von σ. Dann induziert die Abbildung $\sigma \mapsto (d_1, d_2, \ldots)$ eine Bijektion von der Menge der Konjugationsklassen von S_n auf die Menge der Partitionen von n.

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

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

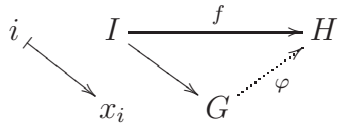
von S_4 heisst die *Kleinsche Vierergruppe*. Sie ist normal und hat die Faktorgruppe $S_4/K \cong S_3$. Die drei Untergruppen der Ordnung 2 von K sind normal in K, aber nicht normal in S_4.

3.15 Freie Gruppen

Betrachte eine Menge I.

Definition: Eine abelsche Gruppe G mit Elementen x_i für alle $i \in I$ heisst eine *freie abelsche Gruppe mit Erzeugenden x_i für alle $i \in I$*, wenn jedes Element von G sich schreiben lässt in der Form $\prod'_{i\in I} x_i^{n_i}$ für eindeutige $n_i \in \mathbb{Z}$, fast alle gleich 0.

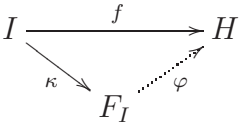
Proposition: *(Universelle Eigenschaft)* Sei G eine freie abelsche Gruppe mit Erzeugenden x_i für alle $i \in I$. Für jede abelsche Gruppe H und jede Abbildung $f\colon I \to H$, $i \mapsto h_i$ existiert genau ein Gruppenhomomorphismus $\varphi\colon G \to H$ mit $\varphi(x_i) = h_i$ für alle $i \in I$, das heisst, so dass das folgende Diagramm kommutiert:



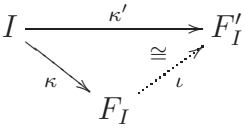
Beispiel: Die Gruppe $\mathbb{Z}^r$ ist eine freie abelsche Gruppe bezüglich der Standardbasis.

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 $\kappa\colon I \to F_I$, $i \mapsto x_i$, so dass die folgende *universelle Eigenschaft* gilt:

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



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



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

Konstruktion: Sei $\tilde{X}$ die Menge der Symbole x_i^ε für alle $i \in I$ und alle $\varepsilon \in \{\pm 1\}$. Eine endliche Folge der Länge $\geqslant 0$ in $\tilde{X}$ heisst ein *Wort über dem Alphabet $\tilde{X}$*. Wir schreiben ein Wort ohne Klammern als $w = x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n}$ und nennen $x_{i_\nu}^{\varepsilon_\nu}$ die *Buchstaben von w*. Sei $W_{\tilde{X}}$ die Menge aller Wörter über $\tilde{X}$. 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 $x_i^\varepsilon x_i^{-\varepsilon}$ heisst eine *elementare Transformation*. Wir nennen zwei Wörter $w, w' \in W_{\tilde{X}}$ *äquivalent* und schreiben $w \sim w'$, wenn sie durch eine Folge elementarer Transformationen ineinander übergehen. Dies definiert eine Äquivalenzrelation auf $W_{\tilde{X}}$. Sei $[w]$ die Äquivalenzklasse von $w \in W_{\tilde{X}}$ und $F_I := W_{\tilde{X}}/\sim$ die Menge aller Äquivalenzklassen.

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

Definition: Ein Wort $w \in W_{\tilde{X}}$, welches keine benachbarten Buchstaben der Form $x_i^\varepsilon x_i^{-\varepsilon}$ enthält, heisst *reduziert*.

Proposition: Jedes Wort $w \in W_{\tilde{X}}$ 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 $x_i^\varepsilon x_i^{-\varepsilon}$, 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 $F_I := W_{\tilde{X}}/\sim$ wie im vorigen Abschnitt, und sei J eine Teilmenge von $W_{\tilde{X}}$.

Definition: Sei $N_J \lhd F_I$ 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 $I = \{1, \ldots, n\}$ und $J = \{w_1, \ldots, w_m\}$ schreiben wir auch suggestiver

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

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

Beispiele:

$$\begin{aligned}
\mathbb{Z} &\cong F_{\{1\}} \cong \langle x \rangle \\
\mathbb{Z}/n\mathbb{Z} &\cong \langle x \mid x^n = 1 \rangle \\
\mathbb{Z}^2 &\cong \langle x, y \mid xy = yx \rangle = \langle x, y \mid xyx^{-1}y^{-1} = 1 \rangle \\
D_n &\cong \langle a, b \mid a^n = b^2 = 1, bab^{-1} = a^{-1} \rangle \\
D_n &\cong \langle b, c \mid b^2 = c^2 = (bc)^n = 1 \rangle \\
D_\infty &:= \langle b, c \mid b^2 = c^2 = 1 \rangle \qquad \text{(unendliche Diedergruppe)} \\
? &\cong \langle a, b \mid a^2b^3 = a^3b^4 = 1 \rangle \\
\mathrm{SL}_2(\mathbb{Z}) &\cong \langle R, S \mid R^3 = S^2, S^4 = 1 \rangle
\end{aligned}$$

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 einfach genau dann, wenn sie zyklisch von Primzahlordnung ist.

Lemma: (a) Jedes Element von A_n ist ein Produkt von 3-Zykeln.

(b) Für jedes $n \geqslant 5$ sind alle 3-Zykel in S_n konjugiert unter A_n.

Satz: Für jedes $n \geqslant 5$ 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 mit $|K| \geqslant 4$ ist die folgende Gruppe einfach:

$$\mathrm{PSL}(2,K) \;:=\; \mathrm{SL}_2(K)/\{\pm I_2\}$$

Satz: Für jeden Körper K und jedes $n > 2$ ist die folgende Gruppe einfach:

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

(ohne Beweis)

4.2 Subnormalreihen

Definition: (a) Eine Folge von Untergruppen $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_m = G$, 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 $G^{(m+1)} := [G^{(m)}, G^{(m)}]$ für alle $m \geqslant 0$ und bilden eine Folge

$$G = G^{(0)} \rhd \ldots \rhd G^{(m)} \rhd G^{(m+1)} \rhd \ldots .$$

Proposition: Betrachte eine Subnormalreihe $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_m = G$.

(a) Für jede Untergruppe $H < G$ ist $1 = H \cap G_0 \lhd H \cap G_1 \lhd \ldots \lhd H \cap G_m = H$ eine Subnormalreihe von H, und für alle $1 \leqslant i \leqslant m$ 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 $N \lhd G$ ist $1 = G_0N/N \lhd G_1N/N \lhd \ldots \lhd G_mN/N = G/N$ eine Subnormalreihe von G/N, und für alle $1 \leqslant i \leqslant m$ gilt

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

4.3 Kompositionsreihen

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

Definition: Eine Subnormalreihe $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_m = G$, 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 $n \geqslant 5$ ist $1 \lhd A_n \lhd S_n$ eine Kompositionsreihe von S_n. Eine Kompositionsreihe von S_4 ist zum Beispiel

$$1 \lhd \big\langle (1\ 2)(3\ 4) \big\rangle \lhd \big\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \big\rangle \lhd A_4 \lhd S_4.$$

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

$$\forall 1 \leqslant i \leqslant n\colon\ G_i/G_{i-1} \cong H_{\sigma i}/H_{\sigma i-1}.$$

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

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.

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

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

4.4 Auflösbare Gruppen

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

Beispiel: Jede abelsche Gruppe ist auflösbar.

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

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

Proposition: Jede Untergruppe und jede Faktorgruppe einer auflösbaren Gruppe ist auflösbar.

Proposition: Für jeden Normalteiler $N \lhd G$ ist G auflösbar genau dann, wenn N und G/N auflösbar sind.

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

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 $G_1 \times \ldots \times G_m$ mit komponentenweiser Multiplikation und dem Einselement $(1, \ldots, 1)$ ist eine Gruppe, genannt das *(äussere direkte) Produkt von* $G_1, \ldots, G_m$.

Definition: Sind $G_1, \ldots, G_m$ Untergruppen von G, so dass die Abbildung

$$G_1 \times \ldots \times G_m \to G,\ (g_1, \ldots, g_m) \mapsto g_1 \cdots g_m$$

ein injektiver Gruppenhomomorphismus ist, so heisst das Bild dieser Abbildung das *(innere direkte) Produkt von* $G_1, \ldots, G_m$.

Beispiel: Die Kleinsche Vierergruppe ist das innere direkte Produkt

$$\big\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \big\rangle \ = \ \big\langle (1\ 2)(3\ 4) \big\rangle \times \big\langle (1\ 3)(2\ 4) \big\rangle.$$

Proposition-Definition: Betrachte eine Linksoperation einer Gruppe H auf einer Gruppe N, geschrieben $H \times N \to N$, $(h, n) \mapsto {}^h n$. 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 $N \rtimes H$.

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

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

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

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

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

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

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 $m, n \geqslant 0$ betrachte die Linksoperation von $\mathrm{GL}_m(R) \times \mathrm{GL}_n(R)$ auf $\mathrm{Mat}_{m \times n}(R)$ durch ${}^{(A,C)}B := ABC^{-1}$. Dann haben wir einen Isomorphismus

$$\begin{array}{rcl} \mathrm{Mat}_{m\times n}(R) \rtimes \big(\mathrm{GL}_m(R) \times \mathrm{GL}_n(R)\big) & \xrightarrow{\sim} & \begin{pmatrix} * & * \\ O & * \end{pmatrix} \ < \ \mathrm{GL}_{m+n}(R), \\ (B, (A, C)) & \mapsto & \begin{pmatrix} I_m & B \\ O & I_n \end{pmatrix} \begin{pmatrix} A & O \\ O & C \end{pmatrix} = \begin{pmatrix} A & BC \\ O & C \end{pmatrix}. \end{array}$$

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 Gruppe der Ordnung p^2 ist abelsch.

Proposition: 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

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

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

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

Definition: Jede Untergruppe von G der Ordnung p^k heisst eine *p-Sylowuntergruppe* oder *p-Sylowgruppe von G*. Sei $\mathrm{Syl}_p(G)$ 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 $\equiv 1 \bmod p$ und ein Teiler von $|G|$.

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

4.8 Kleine endliche Gruppen

Proposition: Jede Gruppe der Ordnung pq oder pq^2 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)

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

Proposition: Jede Gruppe der Ordnung < 60 ist auflösbar.

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 vermittels 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 $n \geqslant 5$,

(c) die einfachen Gruppen *vom Lie-Typ*, konstruiert als Matrixgruppen über endlichen Körpern K wie zum Beispiel $\mathrm{PSL}(n, K)$,

(d) sowie 26 weitere *sporadische einfache Gruppen* verschiedener Ordnungen von $2^4 \cdot 3^2 \cdot 5 \cdot 11 = 7920$ bis

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

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 $\ldots/K_{i+1}/K_i/K_{i-1}/\ldots$ 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

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

heisst die *Charakteristik von K*.

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

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 $K[A]$.

Definition: Dieser Zwischenkörper heisst *von A über K erzeugt* und wird bezeichnet mit $K(A)$. Für endlich viele Elemente $a_1, \ldots, a_n \in L$ schreiben wir auch $K(a_1, \ldots, a_n) := K(\{a_1, \ldots, a_n\})$ 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 $0 \leqslant m \leqslant n$ gilt $K(a_1, \ldots, a_n) = K(a_1, \ldots, a_m)(a_{m+1}, \ldots, a_n)$.

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

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

Eine Körperweiterung mit $[L/K] < \infty$ heisst *endlich*. Eine Körperweiterung 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 $[\mathbb{C}/\mathbb{R}] = 2$.

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 von jedem Element in $L \smallsetminus K$ erzeugt.

Proposition: Für jede Körpererweiterung L/K vom Grad 2 mit $\mathrm{char}(K) \neq 2$ 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.

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_1K_2.

Proposition: In dieser Situation gilt

$$\begin{aligned} [K_1K_2/K_2] \;&\leqslant\; [K_1/K] \quad \text{und} \\ [K_1K_2/K] \;&\leqslant\; [K_1/K] \cdot [K_2/K]. \end{aligned}$$

Definition: Gilt $[K_1K_2/K] = [K_1/K] \cdot [K_2/K] < \infty$, so heissen K_1 und K_2 *linear disjunkt über* K.

Beispiel: $\mathbb{Q}(i)$ und $\mathbb{Q}(\sqrt{2})$ sind quadratisch und linear disjunkt über $\mathbb{Q}$.

Beispiel: $\mathbb{Q}(\sqrt[3]{2})$ und $\mathbb{Q}(\sqrt[3]{2}\, e^{2\pi i/3})$ haben Grad 3 und sind 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 $f \in K[X] \smallsetminus \{0\}$ 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 Zahlen e und π sind transzendent. (ohne Beweis)

Betrachte nun den Auswertungshomomorphismus

$$\mathrm{eval}_a \colon K[X] \twoheadrightarrow K[a] \subset L,\ f \mapsto f(a).$$

Proposition: Es sind äquivalent:

(a) a ist algebraisch über K.

(b) $\mathrm{Kern}(\mathrm{eval}_a) \neq (0)$.

(c) $\dim_K(K[a]) < \infty$.

(d) $[K(a)/K] < \infty$.

Proposition: Es sind äquivalent:

(a) a ist transzendent über K.

(b) eval_a ist injektiv.

(c) 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) $\mathrm{Kern}(\mathrm{eval}_a) = (m_a)$ 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 $\mathrm{Kern}(\mathrm{eval}_a)$.

(c) m_a ist das eindeutige irreduzible normierte Polynom $f \in K[X]$ mit $f(a) = 0$.

(d) 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 $\mathrm{ggT}(f, m_a) \sim 1$ 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 $a_1, \ldots, a_n \in L$ algebraisch über K, so ist $K(a_1, \ldots, a_n)/K$ 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 $m_{a,\mathbb{Q}}(X) = X^4 - 10X^2 + 1$.

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 und/oder Kreise nehmen bzw. auswählen.

Für jede Menge A von Punkten sei $\mathrm{Kons}(A)$ die Menge aller Schnittpunkte, die man durch iterierte Anwendung dieser Operationen aus A konstruieren kann. Die Abstände $d(P,Q)$ für alle Punkte $P,Q \in \mathrm{Kons}(A)$ heissen die *aus A konstruierbaren Längen*. Die Winkel $\sphericalangle PQR$ für alle paarweise verschiedenen Punkte $P,Q,R \in \mathrm{Kons}(A)$ heissen die *aus A konstruierbaren Winkel*. Unser Ziel ist es, die Menge $\mathrm{Kons}(A)$ 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 $\mathrm{Kons}(A)$ der eindeutige kleinste Unterkörper $K \subset \mathbb{C}$ mit den Eigenschaften

(a) $A \subset K$.

(b) $\forall z \in K\colon\ \overline{z} \in K$.

(c) $\forall z \in \mathbb{C}\colon\ z^2 \in K \longrightarrow z \in K$.

Weiter gilt:

(d) Die aus A konstruierbaren Längen sind genau die Zahlen in $\mathrm{Kons}(A) \cap \mathbb{R}^{\geqslant 0}$.

(e) Die aus A konstruierbaren Winkel sind genau die $\alpha \in \mathbb{R}$ mit $\cos\alpha \in \mathrm{Kons}(A)$.

Satz: Setze $\overline{A} := \{\overline{a} \mid a \in A\}$. Dann ist $\mathrm{Kons}(A)$ die Vereinigung aller Körper $L \subset \mathbb{C}$, für die ein Körperturm der Form

$$L = K_n/\ldots/K_1/K_0 = \mathbb{Q}(A \cup \overline{A})$$

existiert mit $[K_i/K_{i-1}] = 2$ für alle $1 \leqslant i \leqslant n$.

Folge: Jedes Element von $\mathrm{Kons}(A)$ ist algebraisch über $\mathbb{Q}(A \cup \overline{A})$ und sein Grad über $\mathbb{Q}(A \cup \overline{A})$ 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 α 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 πr^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 $f \in K[(X_\nu)_{\nu\in N}] \smallsetminus \{0\}$ 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.

Satz: Es existiert eine Transzendenzbasis.

Proposition: *(Austauschsatz)* Für je zwei Transzendenzbasen A und B von L/K und jedes Element $b \in B \smallsetminus A$ existiert ein $a \in A \smallsetminus B$, so dass $(A \smallsetminus \{a\}) \cup \{b\}$ eine Transzendenzbasis von L/K ist.

Satz: Je zwei Transzendenzbasen von L/K haben dieselbe Kardinalität.

Definition: Diese Kardinalität heisst der *Transzendenzgrad von* L/K und wird bezeichnet mit $\mathrm{trdeg}_{L/K}$.

Proposition: Es ist L/K algebraisch genau dann, wenn $\mathrm{trdeg}_{L/K} = 0$ ist.

Proposition: Für jede endlich erzeugte Körpererweiterung $L = K(a_1, \ldots, a_n)/K$ gilt $\mathrm{trdeg}_{L/K} \leqslant n < \infty$.

Beispiel: Es ist $\mathrm{trdeg}_{\mathbb{R}/\mathbb{Q}} = |\mathbb{R}|$.

Proposition: Für jeden Körperturm $M/L/K$ gilt $\mathrm{trdeg}_{M/K} = \mathrm{trdeg}_{M/L} + \mathrm{trdeg}_{L/K}$.

Definition: Eine Körpererweiterung L/K, welche von einer Transzendenzbasis erzeugt ist, heisst *rein transzendent*.

Beispiel: Der rationale Funktionenkörper $K(X_1, \ldots, X_n)$ ist rein transzendent über K vom Transzendenzgrad n.

Beispiel: Der *elliptische Funktionenkörper* $\mathbb{C}(X, \sqrt{X^3 - X})$ ist nicht rein transzendent über $\mathbb{C}$.

5.7 Homomorphismen zwischen Körpererweiterungen

Betrachte zwei Körpererweiterungen L/K und L'/K.

Definition: Ein Körperhomomorphismus $L \to L'$, der auf K die Identität ist, heisst ein *Homomorphismus über K*. Die Menge aller Homomorphismen $L \to L'$ über K bezeichnen wir mit $\mathrm{Hom}_K(L, L')$. Ein Homomorphismus über K, der ein Isomorphismus ist, heisst ein *Isomorphismus über K*.

Beispiel: Die komplexe Konjugation $\mathbb{C} \to \mathbb{C}$ ist ein Isomorphismus über $\mathbb{R}$.

Beispiel: Die Abbildung $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ ist ein Isomorphismus über $\mathbb{Q}$.

Proposition: Ist $[L/K] = [L'/K] < \infty$, so ist jeder Homomomorphismus $L \to L'$ über K ein Isomorphismus.

Proposition: Für jedes $\varphi \in \mathrm{Hom}_K(L, L')$ 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

$$\mathrm{Hom}_K(K(a), L') \xrightarrow{\sim} \{a' \in L' \mid m_{a,K}(a') = 0\}, \quad \varphi \mapsto \varphi(a).$$

Proposition: Ist L/K endlich, so gilt $|\mathrm{Hom}_K(L, L')| \leqslant [L/K]$.

Satz: Ist L/K algebraisch und L' algebraisch abgeschlossen, so ist $\mathrm{Hom}_K(L, L') \neq \varnothing$.

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 $\mathrm{Aut}_K(L)$.

Proposition: Ist L/K algebraisch, so ist $\mathrm{Hom}_K(L, L) = \mathrm{Aut}_K(L)$.

Beispiel: Die Abbildung $K(X) \to K(X)$, $f(X) \mapsto f(X^2)$ 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 $L = K(a)$ mit $f(a) = 0$ heisst ein *Stammkörper von f 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.

Beispiel: Für jede algebraische Zahl $a \in \mathbb{C}$ ist $\mathbb{Q}(a)$ ein Stammkörper des Minimalpolynoms $m_{a,\mathbb{Q}}$ über $\mathbb{Q}$.

Beispiel: Seien $a_1, a_2, a_3 \in \mathbb{C}$ die drei verschiedenen dritten Wurzeln aus 2. Dann ist jedes $\mathbb{Q}(a_i)$ ein Stammkörper von $X^3 - 2$ über $\mathbb{Q}$. Nur einer davon ist reell, aber sie sind alle isomorph. Über $\mathbb{Q}(a_i)$ hat das Polynom die Faktorisierung $X^3 - 2 = (X - a_i)(X^2 + a_i X + a_i^2)$, wobei der zweite Faktor irreduzibel in $\mathbb{Q}(a_i)[X]$ ist.

Definition: Sei $f \in K[X] \smallsetminus \{0\}$. Ein Oberkörper von K der Form $L = K(a_1, \ldots, a_n)$ 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 $f \in K[X] \smallsetminus \{0\}$ besitzt einen Zerfällungskörper über K. Dieser ist bis auf Isomorphie über K bestimmt; der Isomorphismus ist aber im allgemeinen nicht eindeutig.

Proposition: Für jeden Zerfällungskörper L eines Polynoms vom Grad n über K gilt $[L/K] \leqslant n!$.

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

Zur Erinnerung: Ein Körper K heisst *algebraisch abgeschlossen*, wenn die folgenden äquivalenten Bedingungen gelten:

(a) Jedes nichtkonstante Polynom in $K[X]$ besitzt eine Nullstelle in K.

(b) Jedes Polynom in $K[X]$ zerfällt in Linearfaktoren über K.

(c) Jedes Polynom vom Grad $n \geqslant 0$ in $K[X]$ besitzt, mit Vielfachheiten gezählt, genau n Nullstellen in K.

Proposition: Diese sind auch äquivalent zu:

(d) Jede endliche Erweiterung von K ist gleich K.

(e) Jede algebraische Erweiterung von K ist gleich K.

Definition: Ein Oberkörper von K, welcher algebraisch über K und selbst algebraisch abgeschlossen ist, heisst ein *algebraischer Abschluss von K*.

Beispiel: Der Körper $\mathbb{C}$ ist ein algebraischer Abschluss von $\mathbb{R}$.

Satz: Jeder Körper besitzt einen algebraischen Abschluss.

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.

5.10 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 $K[X] \smallsetminus \{0\}$, 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 $f \in K[X] \smallsetminus \{0\}$ ist separabel über K genau dann, wenn es separabel als Polynom über L ist.

Definition: Die *formale Ableitung* eines Polynoms $f(X) = \sum'_k a_k X^k$ ist das Polynom

$$f'(X) \;:=\; \tfrac{df}{dX}(X) \;:=\; \textstyle\sum'_k a_k k X^{k-1}.$$

Proposition: Die formale Ableitung erfüllt die üblichen Regeln:

$$\begin{aligned} \forall f,g \in K[X]\colon \quad (f \pm g)' &= f' \pm g' \\ \forall a \in K\ \forall f \in K[X]\colon \quad (af)' &= af' \\ \forall f,g \in K[X]\colon \quad (fg)' &= f'g + fg' \quad \text{(Leibniz-Regel)} \end{aligned}$$

Proposition: Ein $f \in K[X] \smallsetminus \{0\}$ ist separabel genau dann, wenn $\mathrm{ggT}(f, f') \sim 1$ ist.

Proposition: Ein irreduzibles $f \in K[X]$ ist separabel genau dann, wenn $f' \neq 0$ ist.

Satz: (a) Ist $\mathrm{char}(K) = 0$, so ist jedes irreduzible Polynom über K separabel.

(b) Ist $p := \mathrm{char}(K) > 0$, so hat jedes irreduzible Polynom über K die Form

$$f(X) = g(X^{p^r})$$

für ein eindeutiges $r \geqslant 0$ und ein separables irreduzibles Polynom g über K.

Beispiel: Betrachte den rationalen Funktionenkörper $K := \mathbb{F}_p(Y)$ und das Polynom $g(X) := X - Y \in K[X]$. Dann ist $g(X^{p^r}) = X^{p^r} - Y$ irreduzibel über K für jedes $r \geqslant 0$.

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 p eine Primzahl mit $p \cdot 1_R = 0_R$. Dann ist für jedes $r \geqslant 0$ die Abbildung

$$\mathrm{Frob}_{p^r} \colon R \to R,\ x \mapsto x^{p^r}$$

ein Ringhomomorphismus, genannt der *Frobenius-Endomorphismus bezüglich* p^r.

Insbesondere besitzt jeder Körper K der Charakteristik $p > 0$ den Endomorphismus $\mathrm{Frob}_{p^r} \colon K \to K$. Als Körperhomomorphismus ist dieser injektiv.

Proposition: Ein Körper K der Charakteristik $p > 0$ ist perfekt genau dann, wenn der Frobenius-Endomorphismus $\mathrm{Frob}_p \colon K \to K$ bijektiv ist.

Proposition: Jeder endliche Körper ist perfekt.

5.12 Endliche Körper

Satz: Für jeden endlichen Körper k gilt:

(a) $p := \mathrm{char}(k) > 0$.

(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 $a \in k$.

(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.

Proposition: Für jeden endlichen Körper k mit $|k| = p^n$ ist

$$\mathrm{Aut}(k) \ = \ \mathrm{Aut}_{\mathbb{F}_p}(k) \ = \ \left\langle \mathrm{Frob}_p\,|_k \right\rangle$$

zyklisch der Ordnung n.

6 Galoistheorie

Die Galoistheorie besteht darin, Körpererweiterungen L/K via ihrer Symmetrien, das heisst via der Gruppe $\mathrm{Aut}_K(L)$ zu studieren.

6.1 Symmetrische Funktionen

Wir betrachten Polynome in $\underline{X} = (X_1, \ldots, X_n)$ über einem beliebigen Ring R.

Definition: Ein Polynom der Form $f(\underline{X}) = \sum'_{\underline{i}} a_{\underline{i}} \underline{X}^{\underline{i}}$, 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 $f = \sum'_{d \geqslant 0} f_d$ mit f_d homogen vom Grad d.

Definition: Der *Totalgrad* $\deg(f)$ eines Polynoms $f \in R[\underline{X}] \smallsetminus \{0\}$ ist das grösste d mit $f_d \neq 0$.

Proposition: Für alle $f, g \in R[\underline{X}] \smallsetminus \{0\}$ gilt $\deg(fg) \leqslant \deg(f) + \deg(g)$, mit Gleichheit wenn R ein Integritätsbereich ist.

Variante: Für jede Variable X_ν sei ein Gewicht $\mu_\nu \in \mathbb{R}$ gegeben. Ein Polynom der Form $f(\underline{X}) = \sum'_{\underline{i}} a_{\underline{i}} \underline{X}^{\underline{i}}$, bei der die Summe sich nur über Multiindices $\underline{i}$ mit $\sum_\nu i_\nu \mu_\nu = \lambda$ erstreckt, heisst dann *isobar vom Gewicht* λ. Jedes Polynom ist eine eindeutige Summe $f = \sum'_\lambda f_\lambda$ mit f_λ isobar vom Gewicht λ.

Definition: Ein Polynom $f \in R[X_1, \ldots, X_n]$ heisst *symmetrisch*, wenn gilt

$$\forall \sigma \in S_n\colon \ f(X_{\sigma 1}, \ldots, X_{\sigma n}) = f(X_1, \ldots, X_n).$$

Definition: Für jedes $1 \leqslant m \leqslant n$ ist das *m-te elementarsymmetrische Polynom in* $X_1, \ldots, X_n$ das homogene symmetrische Polynom vom Grad m

$$S_m \ := \sum_{1 \leqslant \nu_1 < \ldots < \nu_m \leqslant n} X_{\nu_1} \cdots X_{\nu_m} \ \in \ \mathbb{Z}[X_1, \ldots, X_n].$$

Eine äquivalente Charakterisierung ist die Identität

$$\begin{aligned} \prod_{i=1}^{n} (X - X_i) \ &= \ X^n + \sum_{m=1}^{n} (-1)^m S_m X^{n-m} \\ &= \ X^n - S_1 X^{n-1} + - \ldots + (-1)^n S_n \ \in \ \mathbb{Z}[X, X_1, \ldots, X_n]. \end{aligned}$$

Betrachte nun weitere Variablen $\tilde{S}_1, \ldots, \tilde{S}_n$.

Hauptsatz: Für jedes symmetrische Polynom $f \in R[X_1, \ldots, X_n]$ existiert ein eindeutiges Polynom $\overline{f} \in R[\tilde{S}_1, \ldots, \tilde{S}_n]$ mit $f = \overline{f}(S_1, \ldots, S_n)$.

Zusatz: Ist f symmetrisch und homogen vom Grad d, so ist $\overline{f}$ isobar vom Gewicht d, wobei jedes $\tilde{S}_\nu$ mit dem Gewicht ν versehen wird.

Beispiel: Für jedes $d \geqslant 1$ ist $\sum_{\nu=1}^n X_\nu^d$ ein symmetrisches Polynom. Zum Beispiel sind

$$\begin{aligned} \textstyle\sum_{\nu=1}^n X_\nu &= S_1, \\ \textstyle\sum_{\nu=1}^n X_\nu^2 &= S_1^2 - 2S_2, \\ \textstyle\sum_{\nu=1}^n X_\nu^3 &= S_1^3 - 3S_1S_2 + 3S_3. \end{aligned}$$

Bemerkung: Aus dem Hauptsatz folgt, dass für jedes von Null verschiedene Polynom $\overline{g} \in R[\tilde{S}_1, \ldots, \tilde{S}_n]$ auch das Polynom $\overline{g}(S_1, \ldots, S_n)$ ungleich Null ist.

Variante: Sei K ein Körper. Eine rationale Funktion $f \in K(X_1, \ldots, X_n)$ heisst *symmetrisch*, wenn gilt

$$\forall \sigma \in S_n\colon\ f(X_{\sigma 1}, \ldots, X_{\sigma n}) = f(X_1, \ldots, X_n).$$

Satz: Für jede symmetrische rationale Funktion $f \in K(X_1, \ldots, X_n)$ existiert eine eindeutige rationale Funktion $\overline{f} \in K(\tilde{S}_1, \ldots, \tilde{S}_n)$ mit $f = \overline{f}(S_1, \ldots, S_n)$.

Beispiel: Es sind

$$\begin{aligned} \textstyle\sum_{\nu=1}^n X_\nu^{-1} &= \frac{S_{n-1}}{S_n}, \\ \textstyle\sum_{\nu=1}^n X_\nu^{-2} &= \frac{S_{n-1}^2 - 2S_{n-2}S_n}{S_n^2}, \\ \textstyle\sum_{\nu=1}^n X_\nu^{-3} &= \frac{S_{n-1}^3 - 3S_{n-1}S_{n-2}S_n + 3S_{n-3}S_n^2}{S_n^3}. \end{aligned}$$

6.2 Resultante und Diskriminante

Definition: Die *Sylvestermatrix* zweier Polynome der Form $f(X) = \sum_{i=0}^n a_i X^i$ und $g(X) = \sum_{j=0}^m b_j X^j$ über einem Ring R ist die $(n+m) \times (n+m)$-Matrix

$$\mathrm{Sylv}_{f,g} := \left(\begin{array}{ccccccccc} a_n & \ldots & \ldots & \ldots & a_1 & a_0 & 0 & \ldots & 0 \\ 0 & a_n & \ldots & \ldots & \ldots & a_1 & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & a_n & \ldots & \ldots & \ldots & a_1 & a_0 \\ \hline b_m & \ldots & \ldots & b_1 & b_0 & 0 & \ldots & \ldots & 0 \\ 0 & b_m & \ldots & \ldots & b_1 & b_0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & \ddots & \ddots & 0 \\ 0 & \ldots & \ldots & 0 & b_m & \ldots & \ldots & b_1 & b_0 \end{array}\right)$$

in der die ersten m Zeilen aus den Koeffizienten von f und die restlichen n Zeilen aus den Koeffizienten von g gebildet sind. Die Determinante der Sylvestermatrix heisst die *Resultante von f und g* und wird bezeichnet mit $\mathrm{Res}_{f,g} \in R$.

Proposition: Für alle Polynome f, g vom Grad n, m in X über einen Körper K ist $\mathrm{Res}_{f,g} = 0$ genau dann, wenn f und g einen gemeinsamen Teiler vom Grad > 0 haben.

Proposition: Für alle Polynome der Form $f(X) = a_n \prod_{i=1}^{n}(X - \alpha_i)$ und $g(X) = b_m \prod_{j=1}^{n}(X - \beta_j)$ gilt

$$\mathrm{Res}_{f,g} \;=\; a_n^m \cdot b_m^n \cdot \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) \;=\; a_n^m \cdot \prod_{i=1}^{n} g(\alpha_i) \;=\; (-1)^{mn} \cdot b_m^n \cdot \prod_{j=1}^{m} f(\beta_j).$$

Offenbar ist die Resultante ein ganzzahliges Polynom in $a_0, \ldots, a_n, b_0, \ldots, b_m$, und zwar homogen vom Grad m in $a_0, \ldots, a_n$ und homogen vom Grad n in $b_0, \ldots, b_m$.

In dem Spezialfall $g = f'$ ist $m = n - 1$ und $b_m = na_n$; also ist die erste Spalte der Sylvestermatrix durch a_n teilbar. Es existiert daher ein eindeutiges ganzzahliges Polynom P_f in $a_0, \ldots, a_n$ mit $\mathrm{Res}_{f,f'} = a_n P_f$.

Definition: Die *Diskriminante* eines Polynoms der Form $f(X) = \sum_{i=0}^{n} a_i X^i$ über einem Ring R ist

$$\mathrm{Disc}_f \;:=\; (-1)^{\frac{n(n-1)}{2}} P_f \;\in\; R.$$

Proposition: Für jedes Polynom der Form $f(X) = a_n \prod_{i=1}^{n}(X - \alpha_i)$ gilt

$$\mathrm{Disc}_f \;=\; a_n^{2n-2} \cdot \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2.$$

Proposition: Ein Polynom f vom Grad n über einem Körper ist separabel genau dann, wenn $\mathrm{Disc}_f \neq 0$ ist.

Beispiel: In kleinen Graden ist

$f(X)$	Disc_f
$aX + b$	a
$aX^2 + bX + c$	$b^2 - 4ac$
$aX^3 + bX^2 + cX + d$	$b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$

Bemerkung: Resultante und Diskriminante kann man auch als symmetrische Funktionen der Nullstellen konstruieren. Der obige Weg liefert aber schneller die richtigen Formeln für nicht normierte Polynome.

6.3 Normale Körpererweiterungen

Proposition: Sei $L = K(A)$ algebraisch über K, und sei $\overline{L}$ ein algebraischer Abschluss von L. Dann sind äquivalent:

(a) Jedes irreduzible Polynom $f \in K[X]$, welches 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 $\varphi \in \mathrm{Hom}_K(L, \overline{L})$ gilt $\varphi(L) = L$.

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 $\overline{K}/K$ 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 minmale algebraische Erweiterung $\tilde{L}/L$, so dass $\tilde{L}/K$ normal ist.

Proposition: Ist $L = K(a_1, \ldots, a_n)$ 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.

Folge: Jede normale Hülle einer endlichen Erweiterung von K ist endlich über K.

6.4 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: Jede algebraische Körpererweiterung in Charakteristik 0 ist separabel.

Proposition: Ein Körper K ist perfekt genau dann, wenn jede algebraische Erweiterung von K separabel ist.

Proposition: Sei $L = K(a_1, \ldots, a_n)/K$ endlich, und sei $\overline{K}$ ein algebraischer Abschluss von K. Dann sind äquivalent:

(a) L/K ist separabel.

(b) Jedes a_i ist separabel über K.

(c) $|\operatorname{Hom}_K(L, \overline{K})| = [L/K]$.

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.

Beispiel: Für beliebige paarweise verschiedene Primzahlen $p_1, \ldots, p_n$ gilt

$$\mathbb{Q}\big(\sqrt{p_1}, \ldots, \sqrt{p_n}\big) \;=\; \mathbb{Q}\big(\sqrt{p_1} + \ldots + \sqrt{p_n}\big).$$

6.5 Inseparable Körpererweiterungen

Proposition: Sei $L = K(A)$ algebraisch über K mit $p := \mathrm{char}(K) > 0$, und sei $\overline{K}$ ein algebraischer Abschluss von K. Dann sind äquivalent:

(a) Für jedes $a \in L$ existiert ein $r \geqslant 0$ mit $a^{p^r} \in K$.

(b) Für jedes $a \in A$ existiert ein $r \geqslant 0$ mit $a^{p^r} \in K$.

(c) $|\mathrm{Hom}_K(L, \overline{K})| = 1$.

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. Wegen $[L/K] = p^2$ ist diese Körpererweiterung 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.

6.6 Galoiserweiterungen

Definition: Eine separable normale algebraische Körpererweiterung L/K heisst *galoissch* oder eine *Galoiserweiterung*, und dann heisst die Gruppe $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ die *Galoisgruppe von* L/K.

Proposition: Für L/K endlich galoissch ist $\mathrm{Gal}(L/K)$ eine endliche Gruppe der Ordnung $[L/K]$.

Proposition-Definition: Sei L ein Körper und Γ eine Untergruppe von $\mathrm{Aut}(L)$. Dann ist

$$L^\Gamma := \{a \in L \mid \forall \gamma \in \Gamma\colon \gamma(a) = a\}$$

ein Unterkörper von L, genannt der *Fixkörper von* Γ.

Satz: Für jede endliche Untergruppe $\Gamma < \mathrm{Aut}(L)$ ist L/L^Γ endlich galoissch mit Galoisgruppe Γ.

Beispiel: Sind $S_1, \ldots, S_n$ die elementarsymmetrischen Polynome in den Variablen $X_1, \ldots, X_n$, so ist

$$K(X_1, \ldots, X_n) \,/\, K(X_1, \ldots, X_n)^{S_n} = K(S_1, \ldots, S_n)$$

endlich galoissch mit Galoisgruppe S_n.

Proposition: Jede Erweiterung von endlichen Körpern ℓ/k ist endlich galoissch mit zyklischer Galoisgruppe $\langle \mathrm{Frob}_{|k|} \,|_\ell \rangle$.

Proposition: Für jede Galoiserweiterung L/K und jeden Zwischenkörper K' ist auch L/K' galoissch.

6.7 Galoiskorrespondenz

Hauptsatz der Galoistheorie: Sei L/K endlich galoissch mit Galoisgruppe Γ. Dann haben wir natürliche zueinander inverse Bijektionen

$$\begin{array}{ccc} K' & \longmapsto & \mathrm{Gal}(L/K') \\ \big\{\text{Zwischenkörper von } L/K\big\} & \underset{\longleftarrow}{\overset{\sim}{\longrightarrow}} & \big\{\text{Untergruppen von } \Gamma\big\} \\ L^{\Gamma'} & \longmapsfrom & \Gamma' \end{array}$$

Weiter gilt für beliebige einander entsprechende $K' \leftrightsquigarrow \Gamma'$ und $K'' \leftrightsquigarrow \Gamma''$:

(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

$$\mathrm{Norm}_\Gamma(\Gamma')/\Gamma' \xrightarrow{\sim} \mathrm{Aut}_K(K'),\ \gamma\Gamma' \mapsto \gamma|_{K'}.$$

(e) K'/K ist galoissch genau dann, wenn Γ' normal in Γ ist, und dann ist die Abbildung in (d) ein natürlicher Isomorphismus

$$\Gamma/\Gamma' \xrightarrow{\sim} \mathrm{Gal}(K'/K).$$

Satz: Jede endliche separable Erweiterung besitzt nur endlich viele Zwischenkörper.

Sei nun $f \in K[X]$ ein separables Polynom vom Grad $n \geqslant 0$. Seien $a_1, \ldots, a_n$ die Nullstellen von f in einem Zerfällungskörper $L = K(a_1, \ldots, a_n)$ von f über K. Dann ist L/K galoissch, und wir nennen seine Galoisgruppe $\mathrm{Gal}(L/K)$ auch die *Galoisgruppe von f über K*.

Proposition: Es existiert eine eindeutige Linksoperation von Γ auf $\{1, \ldots, n\}$ mit der Eigenschaft

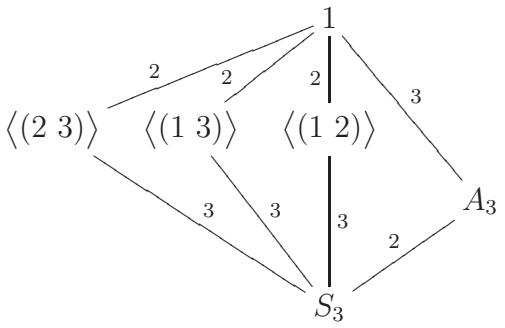
$$\forall \gamma \in \mathrm{Gal}(L/K)\ \forall 1 \leqslant i \leqslant n\colon\ \gamma(a_i) = a_{\gamma i}.$$

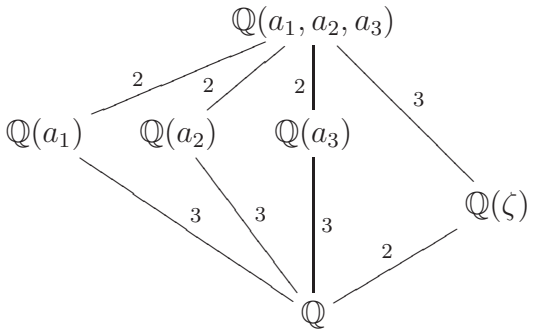
Diese Operation ist treu, entspricht also einem injektiven Homomorphismus $\mathrm{Gal}(L/K) \hookrightarrow S_n$.

Dadurch können wir $\mathrm{Gal}(L/K)$ mit einer Untergruppe von S_n identifizieren. Die Identifikation hängt allerdings von der gewählten Reihenfolge der Nullstellen ab. Jede andere Reihenfolge hat die Form $a_{\sigma 1}, \ldots, a_{\sigma n}$ für eine Permutation $\sigma \in S_n$, und die Umordnung ändert den Homomorphismus ab um den inneren Automorphismus int_σ von S_n und sein Bild somit um Konjugation mit σ.

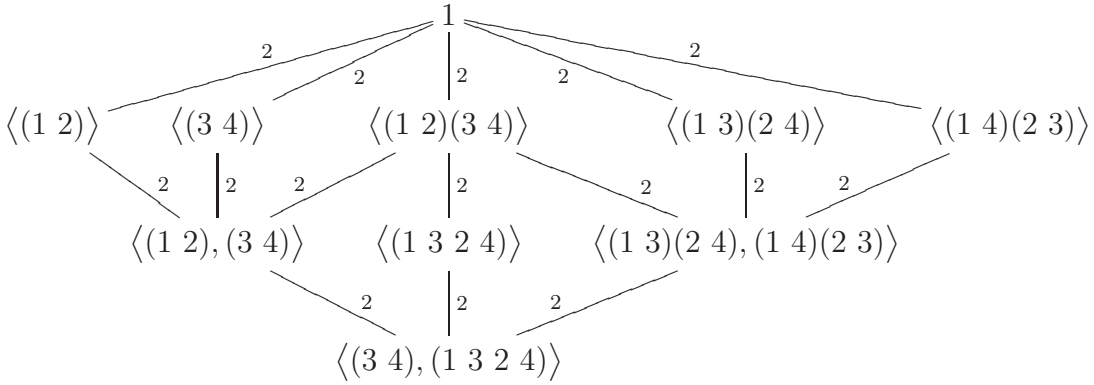
Proposition: Die Operation von $\mathrm{Gal}(L/K)$ auf $\{1, \ldots, n\}$ ist transitiv genau dann, wenn f irreduzibel ist.

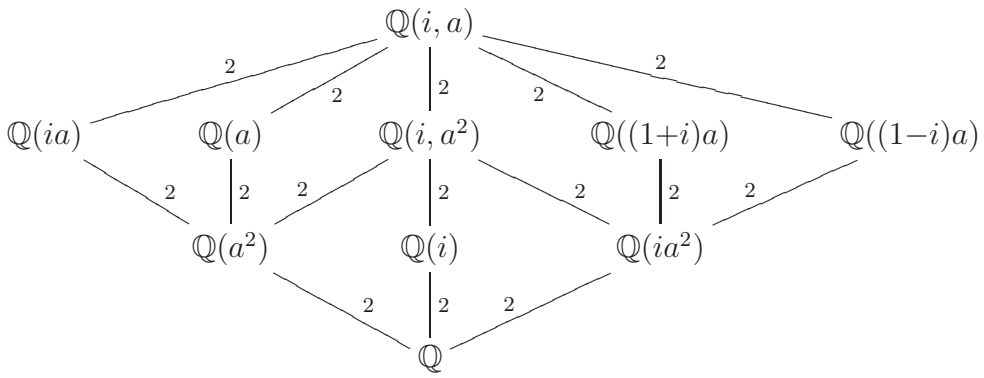
Beispiel: Das Polynom $f(X) := X^3 - 2 \in \mathbb{Q}[X]$ hat die Galoisgruppe S_3. Genauer seien $a := \sqrt[3]{2} \in \mathbb{R}$ und $\zeta := \exp\frac{2\pi i}{3} \in \mathbb{C}$. Die komplexen Nullstellen von f sind dann $(a_1, a_2, a_3) := (a, \zeta a, \zeta^2 a)$. Mit $L := \mathbb{Q}(a_1, a_2, a_3) = \mathbb{Q}(a, \zeta)$ liefert die Galoiskorrespondenz die folgenden Entsprechungen:





Beispiel: Das Polynom $f(X) := X^4 - 2 \in \mathbb{Q}[X]$ hat die 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:





6.8 Explizite Konstruktion der Zwischenkörper

Sei L/K endlich galoissch. Nach dem Satz vom primitiven Element ist dann $L = K(a)$ für ein geeignetes $a \in L$. Zu einer Untergruppe $\Gamma' < \mathrm{Gal}(L/K)$ assoziieren wir das Hilfspolynom

$$F(X) \;:=\; \sum_{i=0}^{m} b_i X^i \;:=\; \prod_{\gamma\in\Gamma'} (X - \gamma(a))$$

mit Koeffizienten $b_i \in L$.

Satz: Dann gilt $L^{\Gamma'} = K(b_0, \ldots, b_m)$.

Bemerkung: In der Praxis genügt oft schon ein einzelner Koeffizient zur Erzeugung von $L^{\Gamma'}$. Oft kann man auch auf anderem Weg Elemente $c_1, \ldots, c_k \in L^{\Gamma'}$ erraten. Wie auch immer man sich solche Elemente beschafft hat; wenn dann $[K(c_1, \ldots, c_k)/K] = [\mathrm{Gal}(L/K) : \Gamma']$ ist, so folgt direkt $K(c_1, \ldots, c_k) = L^{\Gamma'}$.

Beispiel: Sei $\Gamma \subset S_n$ die Galoisgruppe eines separablen Polynoms $f \in K[X]$ mit den Nullstellen $a_1, \ldots, a_n \in L$. Betrachte die Quadratwurzel der Diskriminante

$$b \;:=\; \prod_{1\leqslant i<j\leqslant n} (a_i - a_j) \;\in L.$$

Sei ausserdem $\mathrm{char}(K) \neq 2$.

Proposition: In dieser Situation 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.

6.9 Kreisteilungskörper

Sei n eine natürliche Zahl mit $\mathrm{char}(K) \nmid n$, 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 $e\colon \mathrm{Gal}(K(\mu_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ mit der Eigenschaft

$$\forall \gamma \in \mathrm{Gal}(L/K)\ \forall \zeta \in \mu_n\colon\ \gamma(\zeta) = \zeta^{e(\gamma)}.$$

Dieser Homomorphismus ist injektiv. Insbesondere ist $\mathrm{Gal}(K(\mu_n)/K)$ abelsch.

Beispiel: Ist k ein endlicher Körper der Kardinalität q, so entspricht $\mathrm{Gal}(k(\mu_n)/k)$ der von der Restklasse $q + n\mathbb{Z}$ erzeugten Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$. Zum Beispiel ist $\mathrm{Gal}(\mathbb{F}_2(\mu_{17})/\mathbb{F}_2)$ zyklisch der Ordnung 8.

Satz: Es ist $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$.

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, das heisst von Primzahlen der Form $2^{2^m} + 1$ ist. Dies ist zum Beispiel so für $n = 5$, 15, 17, 32, 65537, aber nicht für $n = 7$, 9, 19.

Definition: Ein Zwischenkörper von $\mathbb{Q}(\mu_n)/\mathbb{Q}$ heisst ein *Kreisteilungskörper*.

Satz: *(Kronecker-Weber)* Jede endliche Galoiserweiterung von $\mathbb{Q}$ mit abelscher Galoisgruppe ist ein Kreisteilungskörper. (ohne Beweis)

6.10 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 separabel vom Grad n mit $\mathrm{char}(K) \nmid n$ und $\mu_n \subset K$. Dann sind äquivalent:

(a) L/K ist eine einfache Radikalerweiterung.

(b) L/K ist zyklisch.

Beispiel: Im Fall $\mathrm{char}(K) \neq 2, 3$ 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 $p_1, \ldots, p_n$ ist die Erweiterung $\mathbb{Q}\big(\sqrt{p_1}, \ldots, \sqrt{p_n}\big)/\mathbb{Q}$ abelsch mit Galoisgruppe isomorph zu $\{\pm 1\}^n$.

6.11 Auflösbare Körpererweiterungen

Definition: (a) Ein Körperturm $K_m/\ldots/K_0$, 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 $K_m/\ldots/K_0$ 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 beliebigen Wurzeln aus Elementen von K darstellbar ist.

Satz: *(Abel-Ruffini)* Sei L/K endlich galoissch mit $\mathrm{char}(K) = 0$. Dann sind äquivalent:

(a) Es existiert ein Radikalturm $K_m/\ldots/K_0$ mit $L \subset K_m$.

(b) L/K ist auflösbar.

Dies ist der Ursprung der Bezeichnung „auflösbare Gruppe“.

Satz: Für $n \geqslant 5$ existiert keine Formel in Termen der vier Grundrechenarten und beliebigen Wurzeln, welche für beliebige Wahl der Variablen $b_0, \ldots, b_n$ 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 $n \geqslant 5$ ist nicht auflösbar durch Radikale.* Die vom Grad $\leqslant 4$ dagegen schon:

Spezialfall: Jedes quadratische Polynom $aX^2 + bX + c$ über einem Körper K der Charakteristik $\neq 2$ hat die Nullstellen

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \ \in \ \overline{K}.$$

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

$$y_i \ := \ \zeta^i \cdot \sqrt[3]{q - \sqrt{p^3 + q^2}} \ + \ \zeta^{-i} \cdot \sqrt[3]{q + \sqrt{p^3 + q^2}} \ \in \ \overline{K}$$

für $i = 0, 1, 2$ für $\zeta := \frac{-1+\sqrt{-3}}{2}$ und eine geeignete Wahl der Wurzeln in $\overline{K}$.

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 entwickelt.

6.12 Explizite Bestimmung der Galoisgruppe

Betrachte das Polynom in $2n+1$ Variablen

$$G \;:=\; \prod_{\sigma\in S_n}\Big(Z-\sum_{i=1}^{n} Y_iX_{\sigma i}\Big) \;\in\; \mathbb{Z}[Z,Y_1,\ldots,Y_n,X_1,\ldots,X_n].$$

Da es in den Variablen $X_1,\ldots,X_n$ symmetrisch ist, existiert ein eindeutiges Polynom in $2n+1$ Variablen $\overline{G}\in\mathbb{Z}[Z,Y_1,\ldots,Y_n,\tilde{S}_1,\ldots,\tilde{S}_n]$, so dass mit den elementarsymmetrischen Polynomen $S_1,\ldots,S_n\in\mathbb{Z}[X_1,\ldots,X_n]$ gilt

$$G \;=\; \overline{G}(Z,Y_1,\ldots,Y_n,S_1,\ldots,S_n).$$

Betrachte nun ein separables Polynom

$$f(X) \;=\; \sum_{i=0}^{n}(-1)^i b_i X^{n-i} \;=\; X^n-b_1X^{n-1}+-\ldots+(-1)^n b_n \;\in\; K[X].$$

Seien $a_1,\ldots,a_n\in L=K(a_1,\ldots,a_n)$ seine Nullstellen und $\Gamma=\mathrm{Gal}(L/K)<S_n$ seine Galoisgruppe. Betrachte das Hilfspolynom

$$g \;:=\; \overline{G}(Z,Y_1,\ldots,Y_n,b_1,\ldots,b_n) \;\in\; K[Z,Y_1,\ldots,Y_n].$$

Satz: Für jeden irreduziblen Faktor h von g existiert ein $\sigma\in S_n$ mit

$$\big\{\tau\in S_n \;\big|\; h(Z,Y_{\tau 1},\ldots,Y_{\tau n})=h\big\} \;=\; {}^{\sigma}\Gamma.$$

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 $n_1+\ldots+n_r=n$. Dann enthält Γ eine Permutation, deren zugehörige Partition von n die Form $n_1+\ldots+n_r=n$ hat.

Beispiel: Die Galoisgruppe von $f(X):=X^7+3X^2+5$ über $\mathbb{Q}$ ist die S_7.

7 Amuse Bouches

7.1 Topologische Gruppen

Definition: Eine Gruppe G versehen mit einer Topologie, so dass die Abbildungen

$$\begin{aligned} G \times G \to G, &\quad (g,h) \mapsto gh, \\ G \to G, &\quad g \mapsto g^{-1} \end{aligned}$$

stetig sind, heisst eine *topologische Gruppe*.

Beispiel: Jede Gruppe wird mit der diskreten Topologie eine topologische Gruppe.

Beispiel: Die Gruppe $\mathrm{GL}_n(\mathbb{R})$ ist mit der von $\mathrm{Mat}_{n\times n}(\mathbb{R}) \cong \mathbb{R}^{n^2}$ induzierten Topologie eine topologische Gruppe. Analog für $\mathrm{GL}_n(\mathbb{C})$, 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 $G \to G$, $x \mapsto gx$ 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.

7.2 p-Adische Zahlen

Sei p eine Primzahl. Für alle $n \geqslant m \geqslant 0$ betrachte den Ringhomomorphismus

$$\mathrm{res}^n_m\colon\ \mathbb{Z}/p^n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^m\mathbb{Z},\ a+p^n\mathbb{Z} \mapsto a+p^m\mathbb{Z}.$$

Setze

$$\mathbb{Z}_p\ :=\ \Big\{(a_n)_{n\geqslant 0} \in \bigtimes_{n\geqslant 0} \mathbb{Z}/p^n\mathbb{Z}\ \Big|\ \forall n \geqslant m \geqslant 0\colon\ \mathrm{res}^n_m(a_n) = a_m\Big\}.$$

Proposition: Mit komponentenweiser Addition und Multiplikation, dem Nullelement $(0)_n$ und dem Einselement $(1)_n$ ist $\mathbb{Z}_p$ ein kommutativer unitärer Ring.

Proposition: Dieser ist ein Integritätsbereich mit Einheitengruppe $\mathbb{Z}_p^\times = \mathbb{Z}_p \smallsetminus p\mathbb{Z}_p$. Seine Ideale sind genau das Nullideal (0) und die Ideale $p^n\mathbb{Z}_p$ für alle $n \geqslant 0$. Insbesondere ist $\mathbb{Z}_p$ ein Hauptidealring.

Definition: Die Elemente von $\mathbb{Z}_p$ heissen *ganze p-adische Zahlen*. Die Elemente seines Quotientenkörpers $\mathbb{Q}_p := \mathrm{Quot}(\mathbb{Z}_p)$ heissen *p-adische Zahlen*.

Proposition: Jedes Element von $\mathbb{Q}_p$ lässt sich schreiben in der Form $\frac{u}{p^n}$ für ein $n \geqslant 0$ und ein $u \in \mathbb{Z}_p$, insbesondere ist $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$.

Definition: Wir versehen $\mathbb{Q}_p$ mit der Topologie, bei der für jedes $u \in \mathbb{Q}_p$ die Teilmengen $u + p^n\mathbb{Z}_p$ für alle $n \in \mathbb{Z}$ eine Umgebungsbasis von u bilden.

Proposition: Die Abbildungen

$$\begin{aligned}
\mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p,&\quad (u,v) \mapsto u+v,\\
\mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p,&\quad (u,v) \mapsto uv,\\
\mathbb{Z}_p^\times \to \mathbb{Z}_p,&\quad u \mapsto u^{-1}
\end{aligned}$$

sind stetig, machen also $\mathbb{Z}_p$ zu einem *topologischen Ring*.

Definition: Für jedes $u \in \mathbb{Q}_p$ sei

$$\mathrm{ord}_p(u) := \begin{cases} \max\{n \in \mathbb{Z} \mid u \in p^n\mathbb{Z}_p\} & \text{falls } u \neq 0,\\ \infty & \text{falls } u = 0.\end{cases}$$

Proposition: (a) Die Topologie auf $\mathbb{Q}_p$ ist hausdorffsch. Jede konvergente Folge hat daher einen eindeutigen Grenzwert.

(b) Eine Folge $(u_n)_{n\geqslant 0}$ in $\mathbb{Q}_p$ konvergiert genau dann, wenn sie eine Cauchyfolge ist, das heisst, wenn gilt

$$\forall N\ \exists n_0\ \forall n \geqslant m \geqslant n_0\colon\ \ \mathrm{ord}_p(u_n - u_m) \geqslant N.$$

(c) Eine Reihe $\sum\limits_{n\geqslant 0} u_n$ in $\mathbb{Q}_p$ konvergiert genau dann, wenn $\lim\limits_{n\to\infty} \mathrm{ord}_p(u_n) = \infty$ ist.

Damit kann man in $\mathbb{Q}_p$ eine Analysis treiben, die in vieler Hinsicht der in $\mathbb{R}$ ähnelt.

Beispiel: Für alle $u \in p\mathbb{Z}_p$ und $n, m \in \mathbb{Z}$ mit $p \nmid m$ liefert die binomische Reihe

$$v \;:=\; \sum_{k \geqslant 0} \tbinom{n/m}{k} \cdot u^k$$

eine Lösung der Gleichung $v^m = (1+u)^n$ in $\mathbb{Z}_p$, also ein Element „ $(1+u)^{n/m}$ “.

Proposition: Die von $\mathbb{Q}_p$ auf $\mathbb{Z}_p$ induzierte Topologie ist dieselbe wie die, welche von der Produkttopologie von $\bigtimes_{n \geqslant 0} \mathbb{Z}/p^n\mathbb{Z}$ induziert ist.

Proposition: Die additive Gruppe von $\mathbb{Z}_p$ ist eine pro-endliche Gruppe.

Proposition: Die Einheitengruppe $\mathbb{Z}_p^\times$ ist eine pro-endliche Gruppe.

7.3 Unendliche Galoiserweiterungen

Sei L/K eine beliebige Galoiserweiterung.

Proposition: Es existiert ein natürlicher injektiver Gruppenhomomorphismus

$$\mathrm{Gal}(L/K) \to \bigtimes_{K'} \mathrm{Gal}(K'/K),\ \gamma \mapsto (\gamma|_{K'})_{K'},$$

wobei das Produkt sich über alle Zwischenkörper K' erstreckt, welche endlich galoissch über K sind. Sein Bild ist die abgeschlossene Untergruppe

$$\big\{(\gamma_{K'})_{K'} \;\big|\; \forall K''/K'/K\colon \gamma_{K''}|_{K'} = \gamma_{K'}\big\}.$$

Damit wird $\mathrm{Gal}(L/K)$ zu einer pro-endlichen Gruppe.

Hauptsatz der Galoistheorie: Sei L/K galoissch mit der pro-endlichen Galoisgruppe Γ. Dann haben wir natürliche zueinander inverse Bijektionen

$$\begin{array}{ccc} K' & \longmapsto & \mathrm{Gal}(L/K') \\ \big\{\text{Zwischenkörper von } L/K\big\} & \underset{\sim}{\rightleftarrows} & \big\{\text{abgeschlossene Untergruppen von } \Gamma\big\} \\ L^{\Gamma'} & \longmapsfrom & \Gamma' \end{array}$$

Beispiel: Die Erweiterung $L := \mathbb{Q}(\bigcup_{n \geqslant 0} \mu_{p^n})/\mathbb{Q}$ ist unendlich galoissch mit Galoisgruppe $\mathrm{Gal}(L/K) \cong \mathbb{Z}_p^\times$.

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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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.
- *Wüstholz: 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.