

Inhaltsverzeichnis

1	Kommutative Ringe	2
1.1	Ringe	2
1.2	Einheiten, Teilbarkeit, Quotientenkörper (Seite 34)	3
1.3	Ring der Polynome (Seite 41)	4
1.4	Ideale und Faktorringe	5
1.5	Charakteristik eines Körpers	7
1.6	Primideale und Maximalideale	7
1.7	Unterring	7
1.8	Matrizen	8
2	Faktorisierungen von Ringen	9
2.1	Euklidische Ringe	9
2.2	Hauptidealring	9
2.3	Faktorielle Ringe	10
2.4	Einige algebraische Euklidische Ringe	11
2.5	Polynomringe	12
3	Gruppentheorie	15
3.1	Definition und Beispiele	15
3.2	Konjugation	16
3.3	Untergruppen und Erzeuger	16
3.4	Nebenklassen und Quotienten	17
3.5	Gruppenwirkungen	18
3.6	Nilpotente und auflösbare Gruppen	20
3.7	Satz von Sylow	20
3.8	Symmetrische und Alternierende Gruppen	21
3.9	Gruppen kleiner Ordnung & Klassifikation	22
3.10	Freie Gruppen und Relationen	22
4	Modultheorie	23
4.1	Definition & Beispiel	23
4.2	Freie Moduln	24
4.3	Torsionsmoduln	24
4.4	Struktur von endlich erzeugten Moduln über Hauptidealringe	25
4.5	Endlich erzeugte abelsche Gruppen	26
4.6	Jordan-Normalform	26

Kapitel 1: Kommutative Ringe

1.1 Ringe

Definition. Ein *Ring* ist eine Menge R ausgestattet mit Elementen $0 \in R$, $1 \in R$ und drei Abbildungen

$$\begin{cases} + : R \times R \rightarrow R \\ - : R \rightarrow R \\ \cdot : R \times R \rightarrow R \end{cases}$$

so dass folgende Axiome gelten.

$(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0 und Inverse $-$ d.h.

$$\begin{aligned} (a + b) + c &= a + (b + c) \\ 0 + a &= a \\ (-a) + a &= 0 \\ a + b &= b + a \end{aligned}$$

für alle $a, b, c \in R$.

(R, \cdot) : Assoziativität $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ und Einselement $1 \cdot a = a = a \cdot 1$.

Distributivität: $a(b + c) = ab + ac$ und $(b + c)a = ba + ca$.

Falls zusätzlich Kommutativität von \cdot gilt: $ab = ba$, dann sprechen wir von einem *kommutativen Ring*.

Bemerkung. • 0 ist eindeutig durch die Axiome bestimmt.

- Ebenso ist $-a$ durch die Axiome für jedes $a \in R$ eindeutig bestimmt.
- $0 \neq 1$ wurde nicht verlangt.
- $0 \cdot a = 0$ für jedes $a \in R$:

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \Rightarrow 0 = 0 \cdot a.$$

Konvention. • Klammern bei $+$ (und ebenso bei \cdot) lassen wir auf Grund der Assoziativität der Addition (Mult.) weg also $a + b + c + d$.

- Punktrechnung vor Strichrechnung, d.h. $a \cdot b + c = (a \cdot b) + c$.
- Den Multiplikationspunkt lässt man oft weg.

Notation.

$$\begin{aligned} 0 \cdot a &= 0 & 1 \cdot a &= a & 2 \cdot a &= a + a & 3 \cdot a &= a + a + a \\ (n + 1) \cdot a &= n \cdot a + a, & (-n) \cdot a &= -(n \cdot a) \text{ für } n \in \mathbb{N}. \end{aligned}$$

Dies definiert eine Abbildung $\mathbb{Z} \times R \rightarrow R$, $(n, a) \mapsto n \cdot a$. Diese erfüllt: $(m + n) \cdot a = m \cdot a + n \cdot a$, $n \cdot (a + b) = n \cdot a + n \cdot b$.

Ebenso definieren wir

$$a^0 = 1_R \quad a^1 = a \quad a^2 = a \cdot a \quad a^{n+1} = a^n \cdot a \text{ für } n \in \mathbb{N}$$

Diese erfüllt

$$a^{m+n} = a^m + a^n \quad (a^m)^n = a^{m \cdot n} \quad (ab)^n = a^n b^n$$

in kommutativen Ringen.

Definition. Angenommen R, S sind Ringe und $f : R \rightarrow S$ ist eine Abbildung. Wir sagen f ist ein *Ringhomomorphismus* falls

$$f(1_R) = 1_S \quad f(a+b) = f(a) + f(b) \quad f(a \cdot b) = f(a) \cdot f(b)$$

für alle $a, b \in R$. Falls f invertierbar ist, so nennen wir f einen *Ringisomorphismus*.

Bemerkung. $f(0_R = 0_S)$ denn $f(0_R) = f(0+0) = f(0) + f(0) \geq 0_S = f(0_R)$.
 $f(-a) = -f(a)$ für $a \in R$ (ähnlicher Beweis).

Definition. Sei R ein Ring und $S \subseteq R$ auch ein Ring. Wir sagen S ist ein *Unterring*, falls $\text{id} : S \rightarrow R, s \mapsto s$ ein Ringhomomorphismus ist.

Lemma. Falls in einem Ring R gilt $0 = 1$, dann ist $R = \{0\}$.

Lemma (Binomialformel). Sei R ein Ring und $a, b \in R$ mit $ab = ba$ (z.B. weil R kommutativ ist). Dann gilt für jedes $n \in \mathbb{N}$ $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$.

Falls $n = 2$ ist und $(a+b)^2 = a^2 + 2ab + b^2$ gilt. Dann folgt $ab = ba$.

⚠ Achtung. Ab nun werden wir nur kommutative Ringe betrachten.

1.2 Einheiten, Teilbarkeit, Quotientenkörper (Seite 34)

Definition. Sei R ein Ring. Ein Element $a \in R \setminus \{0\}$ heißt ein Nullteiler falls es ein $b \in R \setminus \{0\}$ mit $ab = 0$ gibt.

Definition. Ein kommutativer Ring heißt ein Integritätsbereich falls $0 \neq 1$ und falls aus $ab = ac$ und $a \neq 0$ $b = c$ folgt (Kürzen).

Lemma. Sei R ein kommutativer Ring mit $0 \neq 1$. Dann ist R ein Integritätsbereich gdw. R keine Nullteiler besitzt.

Definition. Sei R ein kommutativer Ring und $a, b \in R$. Wir sagen a teilt b , $a|b$ [in R] falls es ein c in R gibt mit $b = a \cdot c$.

Definition. Wir sagen $a \in R$ ist eine *Einheit* falls $a|1 \Leftrightarrow \exists b$ mit $ab = 1 \Leftrightarrow \exists a^{-1} \in R$. Einheiten mit $R^\times = \{a \in R \mid a|1\}$

Bemerkung. R^\times bildet eine Gruppe, $1 \in R^\times$, $a, b \in R^\times \Rightarrow (ab)(a^{-1}b^{-1}) = aa^{-1}bb^{-1} = 1 \Rightarrow ab \in R^\times$.

Definition. Ein *Körper* (field) K ist ein kommutativer Ring in dem $0 \neq 1$ und jede Zahl ungleich Null eine multiplikative Inverse besitzt.

Lemma. Ein Körper ist ein Integritätsbereich.

Proposition. Sei $m \geq 1$ eine natürliche Zahl. Dann ist \mathbb{Z}_m ein Körper genau dann wenn m eine Primzahl ist.

Satz (Quotientenkörper (S.38)). Sei R ein Integritätsbereich. Dann gibt es einen Körper K , der R enthält und so dass $K = \{\frac{p}{q} : p, q \in R, q \neq 0\}$. z.B. für $R = \mathbb{Z}$ haben wir $K = \mathbb{Q}$.

Ab sofort schreiben wir $\frac{a}{b} = [(a, b)]_{\sim}$. Wir identifizieren $a \in R$ mit $\frac{a}{1} \in K$. Hierzu bemerken wir, dass $\iota : a \in R \mapsto \frac{a}{1} \in K$ ein injektiver Ringhomomorphismus ist.

Definition. Sei K ein Körper und $L \subseteq K$ ein Unterring der auch ein Körper ist. Dann nennen wir L auch einen *Unterkörper*.

1.3 Ring der Polynome (Seite 41)

Im Folgenden ist R immer ein kommutativer Ring. Wir wollen einen neuen Ring, den Ring $R[X]$ der Polynome in der Variablen X und Koeffizienten in R definieren.

Definition. Sei R ein kommutativer Ring. Wir definieren den *Ring der formalen Potentreihen* (in einer Variable über dem Ring R) als

1. die Menge aller Folgen $(a_n)_{n=0}^{\infty} \in R^{\mathbb{N}}$
2. $0 = (0)_{n=0}^{\infty}, 1 = (1, 0, 0, \dots)$
3. $+: (a_n)_{n=0}^{\infty} + (b_n)_{n=0}^{\infty} = (a_n + b_n)_{n=0}^{\infty}$
4. $\cdot: (a_n)_{n=0}^{\infty} \cdot (b_n)_{n=0}^{\infty} = (c_n)_{n=0}^{\infty}$ wobei

$$c_n = \sum_{i=0}^n a_i b_{n-i} = \sum_{\substack{i+j=n \\ i,j \geq 0}}^{\infty} a_i b_j.$$

Die Menge aller Folgen mit $a_n = 0$ für alle hinreichend großen $n \geq 0$ wird als der *Polynomring* (in einer Variable und über R) bezeichnet.

Notation. Wir führen ein neues Symbol, eine Variable, z.B. X ein und identifizieren X mit

$$X^0 = 1 = (1, 0, 0, \dots) \quad X^1 = (0, 1, 0, 0, \dots) \quad X^2 = (0, 0, 1, 0, \dots) \quad \dots$$

Allgemeiner: Sei a ein Polynom, dann ist

$$X \cdot a = (0, a_0, a_1, a_2, \dots)$$

denn $(X \cdot a)_n = \sum_{i+j=n} X_i a_j = a_{n-1}$ da $X = 0$ außer wenn $i = 1$ ist. $(X \cdot a)_0 = X_0 \cdot a_0 = 0$.

Wir schreiben $R[X] = \{\sum_{i=0}^n a_i X^i : n \in \mathbb{N}, a_0, \dots, a_n \in R\}$ (R -adjungiert- X) für den *Ring der Polynome in der Variablen X* und $R[[X]] = \{\sum_{n=0}^{\infty} a_n X^n : a_0, a_1, \dots \in R\}$ für den *Ring der formalen Potenzreihen in der Variable X*

Definition. Sei $p \in R[X] \setminus \{0\}$. Der Grad von p $\deg(p)$ ist gleich $n \in \mathbb{N}$ falls $p_n \neq 0$ ist und $p_k = 0$ für $k > n$. In diesem Fall nennen wir p_n auch den *führenden Koeffizienten*.

Wir definieren $\deg(0) = -\infty$.

Proposition. Sei R ein Integritätsbereich. Dann ist $R[X]$ auch ein Integritätsbereich. Des weiteren gilt für $p, q \in R[X] \setminus \{0\}$

- $\deg(pq) = \deg(p) + \deg(q)$ und der führende Koeffizient von pq ist das Produkt der führenden Koeffizienten von p und q .
- $\deg(p+q) \leq \max(\deg(p), \deg(q))$
- Falls $p \mid q$, dann gilt $\deg(p) \leq \deg(q)$.

Definition. Sei K ein Körper. Dann wird der Quotientenkörper von $K[X]$ als der *Körper der rationalen Funktionen* $K(X) = \{\frac{f}{g} : f, g \in K[x], g \neq 0\}$ bezeichnet.

Wenn wir obige Konstruktion (des Polynomrings) iterieren, erhalten wir den Ring der Polynome in mehreren Variablen

$$R[X_1, X_2, \dots, X_d] := (R[X_1])[X_2][X_3] \dots [X_d].$$

Falls $R = K$ ein Körper ist, definieren wir auch

$$K(X_1, X_2, \dots, X_d) = \text{Quot}(K[X_1, \dots, X_d]).$$

Bemerkung. Auf $R[X_1, \dots, X_d]$ gibt es mehrere Grad-Funktionen

$$\begin{aligned} \deg(x_1), \deg(x_2), \dots, \deg(x_d) \\ \deg_{\text{total}}(f) = \max\{m_1 + \dots + m_d \mid f_{m_1, \dots, m_d} \neq 0\} \end{aligned}$$

für $f = \sum_{m_1, \dots, m_d} f_{m_1, \dots, m_d} X_1^{m_1} \dots X_d^{m_d}$. z.B.

$$\deg_{\text{total}}(1 + X_1^3 + X_2 X_3) = 3 \quad \deg_{X_2}(1 + X_1^3 + X_2 X_3) = 1.$$

Satz. Seien R, S zwei kommutative Ringe. Ein Ringhomomorphismus Φ von $R[x]$ nach S ist eindeutig durch seine Einschränkung $\varphi = \Phi|_R$ und durch das Element $x = \Phi(X) \in S$ bestimmt. Des weiteren definiert

$$\Phi\left(\sum_{n=0}^{\infty} a_n X^n\right) = \sum_{n=0}^{\infty} \phi(a_n) x^n \quad (*)$$

einen Ringhomomorphismus falls $\varphi : R \rightarrow S$ ein Ringhomomorphismus ist und $x \in S$ beliebig ist.

Notation. Wir schreiben für zwei kommutative Ringe R, S

$$\text{Hom}_{\text{Ring}}(R, S = \{\varphi : R \rightarrow S \mid \varphi \text{ ist ein Ringhomomorphismus}\})$$

in dieser Notation können wir obigen Satz in der Form

$$\text{Hom}_{\text{Ring}}(R[X], S) \cong \text{Hom}_{\text{Ring}}(R, S) \times S$$

schreiben. Dies kann iteriert werden:

$$\text{Hom}_{\text{Ring}}(R[x_1, \dots, x_d], S) \cong \text{Hom}_{\text{Ring}}(R, S) \times \underbrace{S \times \dots \times S}_{d\text{-mal}}.$$

1.4 Ideale und Faktorringer

Definition. Sei R ein kommutativer Ring. Ein Ideal in R ist eine Teilmenge $I \subseteq R$ so dass

- (i) $0 \in I$
- (ii) $a, b \in I \Rightarrow a + b \in I$
- (iii) $a \in I, x \in R \Rightarrow xa \in I$

Satz. Sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal.

1. Die Relation $a \sim b \Leftrightarrow a - b \in I$ ist eine Äquivalenzrelation auf R . Wir schreiben auch $a \equiv b \pmod{I}$ für die Äquivalenzrelation und R/I für den Quotienten, den wir Faktoring nennen wollen.

2. Die Addition, Multiplikation, das Negative induzieren wohldefinierte Abbildungen

$$R/I \times R/I \rightarrow R/I \quad \text{bzw.} \quad R/I \rightarrow R/I.$$

3. Mit diesen Abbildungen, $0_{R/I} = [0]_{\sim}$, $1_{R/I} = [1]_{\sim}$ ist R/I ein Ring und die kanonische Projektion $p : R \rightarrow R/I$ mit $a \in R \mapsto [a]_{\sim} = a + I$ ist ein surjektiver Ringhomomorphismus.

Lemma. Sei $I \subseteq R$ ein Ideal in einem kommutativen Ring. Dann gilt

$$I = R \Leftrightarrow 1 \in I \Leftrightarrow I \cap R^X \neq \emptyset.$$

Definition. Sei R ein kommutativer Ring und seien $a_1, \dots, a_n \in R$. Dann wird

$$I = (a_1, \dots, a_n) = \{x_1 a_1 + x_2 a_2 + \dots + x_n a_n : x_1, \dots, x_n \in R\}$$

das von a_1, \dots, a_n erzeugte Ideal genannt.

Für $a \in I$ wird $I = (a) = Ra$ das von a erzeugte Hauptideal genannt.

Lemma. Sei R ein kommutativer Ring.

- 1) $(a) \subseteq (b) \Leftrightarrow b \mid a$
- 2) Falls R ein Integritätsbereich ist, dann gilt $(a) = (b) \Leftrightarrow \exists u \in R^x$ mit $b = ua$

Falls $I \subseteq R$ ein Ideal ist und $a \in R$, dann ist die Restklasse für Äquivalent modulo I gleich

$$[a]_N = \{x \in R : x \sim a\} = a + I.$$

Satz (Erster Isomorphiesatz). Angenommen R, S sind kommutative Ringe und $\varphi : R \rightarrow S$ ist ein Ringhomomorphismus.

1. Dann induziert φ einen Ringisomorphismus

$$\bar{\varphi} : R/\text{Ker}(\varphi) \rightarrow \text{Im}(\varphi) = \varphi(R) \subseteq S$$

so dass $\varphi = \bar{\varphi} \circ p$ wobei $p : R \rightarrow R/\text{Ker}(\varphi)$ die kanonische Projektion ist (Diagramm links).

2. Sei $I \subseteq \text{Ker}(\varphi)$ ein Ideal in R . Dann induziert φ einen Ringhomomorphismus $\bar{\varphi} : R/I \rightarrow S$ mit $\varphi = \bar{\varphi} \circ p_I$ (Diagramm rechts). Des weiteren gilt $\text{Ker}(\bar{\varphi}) = \text{Ker}(\varphi)/I$ und $\text{Im}(\bar{\varphi}) = \text{Im}(\varphi)$

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \downarrow p & \nearrow \bar{\varphi} & \\ R/\text{Ker}(\varphi) & & \end{array} \qquad \begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \downarrow p_I & \nearrow \bar{\varphi} & \\ R/I & & \end{array}$$

Bemerkung. Sei $I_0 \subseteq R$ ein Ideal in einem kommutativen Ring. Dann gibt es eine Korrespondenz (kanonische Bijektion) zwischen Idealen in R/I_0 und Idealen in R , die I_0 enthalten.

$$\begin{aligned} I \subseteq R, I_0 \subseteq I & \mapsto I/I_0 = \{x + I_0 : x \in I\} \subseteq R/I_0 \\ J \subseteq R/I_0 & \mapsto p_{I_0}^{-1}(J) \subseteq R \quad (p_{I_0} : \begin{cases} R \rightarrow R/I_0 \\ x \mapsto x + I_0 \end{cases}). \end{aligned}$$

Definition. Wir sagen zwei Ideale I, J in einem kommutativen Ring sind *coprim*, falls $I + J = R$ ist. D.h. $\exists a \in I, b \in J$ mit $1 = a + b$.

Proposition (Chinesischer Restsatz). Sei R ein kommutativer Ring und seien I_1, \dots, I_n paarweise coprime Ideale. Dann ist der Ringhomomorphismus $\varphi : R \rightarrow R/I_1 \times \dots \times R/I_n$ mit $x \mapsto (x + I_1, \dots, x + I_n)$ surjektiv mit $\text{Ker}(\varphi) = I_1 \cap \dots \cap I_n$.

Dies induziert einen Ringisomorphismus $R/I_1 \cap \dots \cap I_n \rightarrow R/I_1 \times \dots \times R/I_n$.

1.5 Charakteristik eines Körpers

Sei K ein Körper. Dann gibt es einen Ringhomomorphismus $\varphi : \mathbb{Z} \rightarrow K$ mit

$$\begin{cases} n \in \mathbb{N} \mapsto \underbrace{1 + \dots + 1}_{n\text{-mal}} \\ -n \in \mathbb{N} \mapsto -(\underbrace{1 + \dots + 1}_{n\text{-mal}}) \end{cases}$$

Sei $I = \text{Ker}(\varphi)$ so, dass $\mathbb{Z}/I \cong \text{Im}(\varphi) \subseteq K$. Da K ein Körper ist, ist $\text{Im}(\varphi)$ ein Integritätsbereich.

Lemma. Sei $I \subseteq \mathbb{Z}$ ein Ideal. Dann gilt $I = (m)$ für ein $m \in \mathbb{N}$. Der Quotient ist ein Integritätsbereich genau dann wenn $m = 0$ oder m eine Primzahl ist.

Definition. Sei K ein Körper. Wir sagen, dass K Charakteristik 0 hat, falls $\varphi : \mathbb{Z} \rightarrow K$ injektiv ist. Wir sagen, dass K Charakteristik $p \in \mathbb{N}_{>0}$ hat falls $\varphi : \mathbb{Z} \rightarrow K$ den Kern (p) hat.

Proposition. Sei K ein Körper mit Charakteristik $p > 0$. Dann ist die Frobeniusabbildung $F : x \in K \rightarrow x^p \in K$ ein Ringhomomorphismus. Falls $|K| < \infty$, dann ist F ein Ringautomorphismus.

1.6 Primideale und Maximalideale

Definition. Sei R ein kommutativer Ring, und sei $I \subseteq R$ ein Ideal. Wir sagen I ist ein *Primideal*, falls R/I ein Integritätsbereich ist. Wir sagen I ist ein *Maximalideal*, falls R/I ein Körper ist.

Proposition. Sei $I \subseteq R$ ein Ideal in einem kommutativen Ring.

- 1) Dann ist I ein Primideal genau dann wenn $I \neq R$ und für alle $a, b \in R$ gilt $ab \in I \Rightarrow a \in I$ oder $b \in I$.
- 2) Dann ist I ein Maximalideal genau dann wenn $I \neq R$ und es gibt kein Ideal J mit $I \subsetneq J \subsetneq R$.

Bemerkung. Der Hilbert'sche Nullstellensatz besagt, dass jedes Maximalideal in $\mathbb{C}[X_1, \dots, X_n]$ von dieser Gestalt ist.

Satz. Sei R ein kommutativer Ring, und $I \subsetneq R$ ein Ideal. Dann existiert ein Maximalideal $m \supseteq I$. Insbesondere existiert in jedem Ring $R \neq [0]$ ein Maximalideal.

1.7 Unterring

Definition. Sei R ein Ring und $S \subseteq R$ auch ein Ring. Wir sagen S ist ein *Unterring* falls $\text{id} : S \rightarrow R, s \mapsto s$ ein Ringhomomorphismus ist.

Alternativ Definition: Sei R ein Ring und $S \subseteq R$. Dann ist S ein Unterring falls

1. $0, 1 \in S$.
2. $a - b \in S$ für alle $a, b \in S$.
3. $a \cdot b \in S$ für alle $a, b \in S$.

Notation. Sei $S \subseteq R$ ein Unterring in einem Ring R . Seien $a_1, \dots, a_n \in R$. Wir definieren

$$S[a_1, \dots, a_n] = \bigcap_{\substack{T \subseteq R \text{ Unterring} \\ T \supseteq S \\ a_1, \dots, a_n \in T}} T.$$

genannt „s-adjungiert a_1, \dots, a_n “.

$$= \text{ev}_{a_1, \dots, a_n}(S[x_1, \dots, x_n]) = \left\{ \sum_{k_1, \dots, k_n \in M} c_{k_1, \dots, k_n} a_1^{k_1} \dots a_n^{k_n} \right\}.$$

mit $|M| < \infty$, $M \subseteq \mathbb{N}^n$, $c_{k_1, \dots, k_n} \in S$.

1.8 Matrizen

Sei R ein kommutativer Ring, $m, n \in \mathbb{N}_{>0}$. Dann bezeichnen wir die Menge $\text{Mat}_{mn}(R)$ als die Menge aller $m \times n$ -Matrizen

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}.$$

mit Koeffizienten oder Eintragungen $a_{11}, \dots, a_{mn} \in R$. Für $m = n$ definieren wir auch auf $\text{Mat}_{mm}(R)$ auf übliche Weise die Addition und Multiplikation. Dies definiert auf $\text{Mat}_{mm}(R)$ gemeinsam mit dem Einselement $I_m = (\delta_{ij})_{i,j}$ eine Ringstruktur. Sobald $m > 1$ ist, ist dieser Ring nichtkommutativ.

Die Einheiten in $\text{Mat}_{mm}(R)$ werden auch als invertierbare Matrizen bezeichnet. Die Menge wird auch die allgemeine lineare Gruppe vom Grad m über R genannt:

$$\text{GL}_m(R) = \text{Mat}_{mm}(R)^\times = \{A \in \text{Mat}_{mm}(R) \mid \text{es existiert ein } B \in \text{Mat}_{mm}(R) \text{ mit } AB = BA = I_n\}.$$

Proposition (Meta). *Jede Rechenregel für Matrizen über \mathbb{R} die nur $+$, $-$, \cdot , 0 , 1 beinhalten, gilt auch über einem beliebigen kommutativen Ring.*

Proposition. *Sei R ein kommutativer Ring*

- $\text{Mat}_{mm}(R)$ erfüllt die Ringaxiome, also z.B. $A(BC) = (AB)C$
- $\det(AB) = \det(A)\det(B)$
- $A\tilde{A} = \tilde{A}A = \det(A)I_m$, wobei \tilde{A} die komplementäre Matrix

$$\tilde{A} = ((-1)^{i+j} \det(A_{ji}))_{i,j}.$$

- $\text{char}_A(A) = 0$ für das charakteristische Polynom $\text{char}_A(X) = \det(XI_m - A)$ einer Matrix A .

Bemerkung. $\det(A)$, jeder Koeffizient von $A(BC)$, $(AB)C$, $A\tilde{A}$, $\tilde{A}A$, $\det(A)I$, $\text{char}_A(X)$, $\text{char}_A(A)$ hängt polynomiell von den Eintragungen von A, B, C ab, wobei die Koeffizienten in \mathbb{Z} liegen z.B.

$$\det(A) = \sum_{\sigma \in S_n} \underbrace{\text{sgn}(\sigma)}_{\in \mathbb{Z}} a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}$$

welche Monome in den Eintragungen von A sind.

Lemma. *Wenn ein Polynom $f \in \mathbb{R}[X_1, \dots, X_n]$ auf ganz \mathbb{R}^n verschwindet, dann ist $f = 0$.*

Bemerkung. Das Lemma gilt analog für jeden Körper K mit $|K| = \infty$.

Kapitel 2: Faktorisierungen von Ringen

Buch Seiten 83-114. Wir wollen in diesem Kapitel Ringe mit eindeutiger Primfaktorzerlegung betrachten. Im Folgenden ist R immer ein Integritätsbereich.

Definition (Wiederholung). $a \mid b \Leftrightarrow \exists c$ mit $b = ac$ für $a, b \in R$.
 $a \in R^\times$ ist eine Einheit $\Leftrightarrow a \mid 1$.

Definition. Wir sagen $p \in R \setminus \{0\}$ ist *irreduzibel*, falls $p \notin R^\times$ und für alle $a, b \in R$ gilt $p = ab \Rightarrow a \in R^\times$ oder $b \in R^\times$.

Definition. Wir sagen $p \in R \setminus \{0\}$ ist *prim* falls (p) ein Primideal ist, in anderen Worten falls $p \notin R^\times$ und für alle $a, b \in R$ gilt $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$.

Lemma. Sei R ein Integritätsbereich. Dann ist jedes prim $p \in R$ auch irreduzibel.

Bemerkung. Die Umkehrung des Lemmas stimmt im Allgemeinen nicht. Wenn sie doch stimmt, so hilft dies für die Eindeutigkeit in einer Primfaktorzerlegung. Siehe später in 3.3.

2.1 Euklidische Ringe

Definition. Ein Integritätsbereich R heißt ein *Euklidischer Ring* falls es eine gradfunktion $N : R \setminus \{0\} \rightarrow \mathbb{N}$ gibt, so dass die beiden folgenden Eigenschaften gelten:

- *Gradungleichung:* $N(f) \leq N(fg)$ für alle $f, g \in R \setminus \{0\}$.
- *Division mit Rest:* Für $f, g \in R$ mit $f \neq 0$ gibt es $q, r \in R$ mit $g = q \cdot f + r$ wobei $r = 0$ oder $N(r) < N(f)$ ist. Wir nennen r den *Rest* (bei Division durch f).

Satz. In einem Euklidischen Ring ist jedes Ideal ein Hauptideal.

2.2 Hauptidealring

Definition. Sei R ein Integritätsbereich. Dann heißt R ein *Hauptidealring* falls jedes Ideal in R ein Hauptideal ist.

Bemerkung. Der Ring $\mathbb{Z}[\frac{1}{2}(1 + i \cdot \sqrt{163})]$ ist ein Hauptidealring und kann nicht zu einem Euklidischen Ring gemacht werden.

Proposition. Sei R ein Hauptidealring. Für je zwei Elemente $f, g \in R \setminus \{0\}$ gibt es einen größten gemeinsamen Teiler d mit $(d) = (f) + (g)$.

Definition. Seien $f, g, d \in R \setminus \{0\}$. Wir sagen d ist ein gemeinsamer Teiler von f und g falls $d \mid f$ und $d \mid g$. Wir sagen d ist ein größter gemeinsamer Teiler falls d ein gemeinsamer Teiler ist und jeder gemeinsame Teiler t auch d teilt.

Bemerkung. Zwei ggT's unterscheiden sich um eine Einheit (wenn R ein Integritätsbereich ist).

In einem Euklidischen Ring kann man einen ggT von $f, g \in R \setminus \{0\}$ durch den *euklidischen Algorithmus* bestimmen.

- 0) Falls $N(f) > N(g)$, so vertauschen wir f und g . Also dürfen wir annehmen, dass $N(f) \leq N(g)$.

- 1) Dividiere g durch f mit Rest: $g = qf + r$
- 2) Falls $r = 0$ ist, so ist f ein ggT und der Algorithmus stoppt.
- 3) Falls $r \neq 0$ ist, so ersetzen wir (f, g) durch (r, f) und springen nach 1).

Lemma. *Der Euklidische Algorithmus (wie oben beschrieben) endet nach endlich vielen Schritten und berechnet einen ggT.*

Satz (Prime Elemente). *Sei R ein Hauptidealring.*

- 1) *Dann ist $p \in R \setminus \{0\}$ prim genau dann wenn p irreduzibel ist.*
- 2) *Jedes $f \in R \setminus \{0\}$ lässt sich als Produkt einer Einheit und endlich vielen primen Elementen schreiben.*

Satz. *Sei R ein Hauptidealring und $p \in R$ irreduzibel. Dann ist (p) ein Maximalideal. Insbesondere ist p prim.*

Für den Beweis vom Satz über Prime Elemente Eigenschaft 2 verwenden wir:

Proposition. *Sei R ein Hauptidealring und seien $J_0 \subseteq J_1 \subseteq J_2 \subseteq \dots$ eine ansteigende Kette von Idealen in R . Dann gibt es ein $n \in \mathbb{N}$ mit $J_m = J_n$ für alle $m \geq n$.*

Beispiel. Einige Primzahlen in $\mathbb{Z}[i]$, z.B. sind $1 \pm i, 3, 2 \pm i$ Primzahlen in $\mathbb{Z}[i]$.

2 ist keine Primzahl in $\mathbb{Z}[i]$, da $2 = (1+i)(1-i)$. 5 ist auch keine Primzahl in $\mathbb{Z}[i]$, da $5 = (2+i)(2-i)$.

Nach dem ersten folgenden Lemma ergibt sich nun, dass $1 \pm i, 2 \pm i$ Primzahlen in $\mathbb{Z}[i]$ sind. Nach dem zweiten Lemma sind 3, 7 Primzahlen in $\mathbb{Z}[i]$.

Lemma. *Sei $z \in \mathbb{Z}[i]$ so dass $N(z) = p \in \mathbb{N}$ eine Primzahl in \mathbb{N} ist. Dann ist z irreduzibel (also prim) in $\mathbb{Z}[i]$.*

Lemma. *Angenommen $p \in \mathbb{N}$ ist eine Primzahl in \mathbb{N} , die sich nicht als Summe zweier Quadratzahlen schreiben lässt. Dann ist p auch eine Primzahl in $\mathbb{Z}[i]$.*

2.3 Faktorielle Ringe

Definition. Ein Integritätsbereich R heißt ein *faktorieller Ring* falls jedes $a \in R \setminus \{0\}$ sich als ein Produkt von einer Einheit und endlich vielen Primelemente von R schreiben lässt: $a = u \cdot p_1 \cdot \dots \cdot p_m$ für $u \in R^\times, m \in \mathbb{N}, p_1, \dots, p_m \in R$ prim.

Proposition. *Sei R ein faktorieller Ring. Dann ist $p \in R \setminus \{0\}$ irreduzibel gdw. p prim ist.*

Korollar. *Sei R ein Integritätsbereich. Dann ist R faktoriell gdw. jedes Element von $R \setminus \{0\}$ eine Zerlegung als ein Produkt von einer Einheit und endlich vielen irreduziblen Elementen besitzt und jedes irreduzible Element auch ein Primelement ist.*

Definition. Sei R ein kommutativer Ring und $a, b \in R$. Wir sagen a, b sind *assoziiert* und schreiben $a \sim b$ falls es eine Einheit $u \in R^\times$ gibt mit $a = ub$.

Lemma. *Dies definiert eine Äquivalenzrelation auf R .*

Lemma. *Sei R ein Integritätsbereich. Seien $p, q \in R \setminus \{0\}$ irreduzibel und $p \mid q$. Dann gilt $p \sim q$.*

Definition (Wh.). Für $n \in \mathbb{N}_{>0}$. sei S_n die *symmetrische Gruppe* auf der Menge $\{1, \dots, n\}$, d.h.

$$S_n = \{\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\} \text{ bijektiv}\}.$$

Satz (Eindeutige Primfaktorzerlegung). *Sei R ein faktorieller Ring, dann besitzt jedes nichttriviale Element von R eine bis auf Permutation und Assoziierung eindeutige Primfaktorzerlegung. Genauer gilt also für jedes $a \in R \setminus \{0\}$ gibt es eine Einheit $u \in R^\times$, $m \in \mathbb{N}$, und Primelemente p_1, \dots, p_m mit $a = up_1 \dots p_m$. Falls $a = vq_1 \dots q_n$ eine weitere Zerlegung ist, wobei $v \in R^\times$, $n \in \mathbb{N}$ und q_1, \dots, q_n prim sind, dann gibt es $\sigma \in S_n$ so dass $q_j \sim p_{\sigma(j)}$ für $j = 1, \dots, n$ und $m = n$.*

Die Existenz der Zerlegung ist die Definition von „faktorieller Ring“. Wir nennen p_1, \dots, p_m die Primfaktorzerlegung von a .

Definition. Sei R ein faktorieller Ring. Wir sagen $P \subseteq R$ ist eine *Repräsentantenmenge* (der Primelemente) falls jedes $p \in P$ ein Primelement in R ist und es zu jedem Primelement $q \in R$ ein eindeutig bestimmtes $p \in P$ gibt mit $q \sim p$.

Lemma. *Sei R ein faktorieller Ring. Dann existiert eine Repräsentantenmenge.*

Satz (Eindeutige Primfaktorzerlegung). *Sei R ein faktorieller Ring und $P \subseteq R$ eine Repräsentantenmenge. Dann besitzt jedes $a \in R \setminus \{0\}$ eine eindeutige Primfaktorzerlegung der Form*

$$a = u \prod_{p \in P} p^{n_p} \left[= u \prod_{\substack{p \in P \\ n_p > 0}} p^{n_p} \right]$$

wobei $n_p = 0$ für alle bis auf endlich viele $p \in P$.

Lemma. *Sei R ein faktorieller Ring und $P \subseteq R$ eine Repräsentantenmenge. Sei $a = u \prod_{p \in P} p^{m_p}$ und $b = v \prod_{p \in P} p^{n_p}$. Dann gilt $a \mid b$ gdw. $m_p \leq n_p$ für alle $p \in P$.*

Proposition (ggT). *Sei R ein faktorieller Ring mit Repräsentantenmenge P . Dann existiert für jedes Paar $a, b \in R$, nicht beide 0, ein ggT. Falls $a = u \prod_{p \in P} p^{m_p}$, $b = v \prod_{p \in P} p^{n_p}$ ist, so ist $\prod_{p \in P} p^{\min(m_p, n_p)}$ ein ggT von a und b .*

Wir können analog den ggT von mehreren Elementen $a_1, \dots, a_l \in R$ definieren und die obige Proposition gilt analog.

Definition. Sei R ein faktorieller Ring. Wir sagen $a_1, \dots, a_l \in R$ sind *coprim* falls 1 ein ggT von a_1, \dots, a_l ist, oder äquivalenterweise falls es zu jedem Primelement p in R ein a_j gibt so dass a_j nicht durch p teilbar ist.

Korollar. *Sei R ein faktorieller Ring mit Quotientenkörper K . Dann hat jedes $x \in K$ eine Darstellung $x = \frac{a}{b}$ mit $a, b \in R$ coprim, $b \neq 0$.*

Korollar. *Sei R faktoriell und $K = \text{Quot}(R)$. Dann hat jedes $x \in K$ eine Darstellung der Form*

$$x = u \prod_{p \in P} p^{n_p},$$

wobei $n_p \in \mathbb{Z}$ und gleich 0 für alle bis auf endlich viele $p \in P$ ist.

2.4 Einige algebraische Euklidische Ringe

Alle Beispiele, die wir hier betrachten wollen, leben in einem quadratischen Zahlkörper: $K = \mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ mit $d \in \mathbb{Z}$, das kein Quadrat ist. Isomorph dazu $\mathbb{Q}[x]/(x^2 - d)$.

Wir definieren auf K die Konjugation $\tau : K \rightarrow K, a + b\sqrt{d} \mapsto a - b\sqrt{d}$. Dies definiert einen Körperautomorphismus.

Auf K definieren wir die Normfunktion

$$N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$$

so dass $N : K \rightarrow \mathbb{Q}$ multiplikativ ist, daher

$$N(zw) = (zw) \underbrace{\tau(zw)}_{\tau(z)\tau(w)} = N(z)N(w) \quad \text{für } z, w \in K.$$

Weiters $N(z) = 0 \Leftrightarrow z = 0$ für alle $z = a + b\sqrt{d} \in K$.

Wir werden den Ring $R = \mathbb{Z}[\sqrt{d}]$ betrachten und wollen $\phi(z) = |N(z)|$ als Gradfunktion verwenden.

Satz. Für $d = -1, -2, 2, 3$ ist $R = \mathbb{Z}[\sqrt{d}]$ ein Euklidischer Ring, wobei wir $\phi(z) = |N(z)|$ als Gradfunktion verwenden.

Sei $R = \mathbb{Z}[\sqrt{d}]$.

Lemma. Es gilt $u \in R^\times \Leftrightarrow N(u) = \pm 1$.

Lemma. Falls $z \in R$ eine Primzahl in \mathbb{Z} als Norm hat, so ist z in R irreduzibel.

Lemma. Falls $p \in \mathbb{Z}$ eine Primzahl in \mathbb{Z} ist, so dass weder p noch $-p$ eine Norm von einem Element in R ist, so ist p ein irreduzibles Element in R .

Satz (Gaußsche ganze Zahlen). Sei $R = \mathbb{Z}[i]$ der Ring der Gaußschen ganzen Zahlen. Dann ist R ein Euklidischer Ring. Wir können in R die Repräsentantenmenge

$$P = \{z = a + ib \in R \mid z \text{ prim, } -a < b \leq a\}$$

verwenden. Diese Menge P enthält

- (Ramified): $z = 1 + i$ mit $2 = -i(1 + i)^2$
- (Inert): $p \in \mathbb{N}$ prim mit $p \equiv 3 \pmod{4}$, z.B. 3, 7, 11, ...
- (Split): $z = a \pm bi$ prim in R , wobei $a, b \in \mathbb{N}, b < a$ und $a^2 + b^2 = p \equiv 1 \pmod{4}$ mit $p \in \mathbb{N}$ prim. $p = (a + ib)(a - ib)$ z.B. 5, 13, ...

Lemma. Sei $p \in \mathbb{N}$ prim. Dann ist $(p - 1)! \equiv -1 \pmod{p}$.

Proposition. Sei $p \in \mathbb{N}$ kongruent $1 \pmod{4}$. Dann gibt es in \mathbb{F}_p zwei Lösungen der quadratischen Gleichung $x^2 = -1$.

Korollar. Sei $p \in \mathbb{N}$ kongruent $1 \pmod{4}$. Dann ist p keine Primzahl in $\mathbb{Z}[i]$.

Satz. Im $R_{\text{falsch}} = \mathbb{Z}[\sqrt{3}i]$ funktioniert Division mit Rest nicht wie in den obigen Fällen. Aber in $R_{\text{richtig}} = \mathbb{Z}[\zeta] = \{a + b\zeta : a, b \in \mathbb{Z}\}$ für $\zeta = \frac{1+\sqrt{3}i}{2}$ funktioniert dies wieder.

2.5 Polynomringe

Seite 108

Satz (Gauss). Falls R ein faktorieller Ring ist, so ist auch $R[x]$ ein faktorieller Ring.

Korollar. Der Ring $\mathbb{Z}[x_1, \dots, x_n]$ und der Ring $K[x_1, \dots, x_n]$ für einen Körper K sind faktoriell,

Definition. Sei R ein faktorieller Ring und $f \in R[x] \setminus \{0\}$. Dann nennen wir den ggT der Koeffizienten von f den *Inhalt* $I(f)$ von f (welcher bis auf Einheiten in R eindeutig bestimmt ist).

Wir sagen f ist *primitiv* falls $I(f) \sim 1$.

Beobachtungen

- Jedes normierte Polynom ist primitiv.
- Für $a \in R \setminus \{0\}, f \in R[x] \setminus \{0\}$ gilt $I(af) \sim aI(f)$.
- Falls $f \in R[x]$ irreduzibel ist, so ist entweder $f \in R$ oder f ist primitiv. (Grad $f = 0 \Rightarrow f \in R$, Grad $f > 0 \Rightarrow f = af^*, a \in R, f^*$ primitiv. Folgt a oder f^* ist eine Einheit $\Rightarrow \deg(f^*) = \deg(f) > 0$ also f^* ist keine Einheit)

Lemma. Sei R ein faktorieller Ring und $K = \text{Quot}(R)$. Dann hat jedes $f \in K[x] \setminus \{0\}$ eine Darstellung $f = df^*$ wobei $d \in K^\times$ und $f^* \in R[x]$ ist primitiv. Diese Darstellung ist bis auf Assoziierung eindeutig:

Falls $f = d_1 f_1^* = d_2 f_2^*, d_1, d_2 \in K^\times, f_1^*, f_2^* \in R[x]$ primitiv, dann ist $d_1 \sim_R d_2, f_1^* \sim_R f_2^*$.

Wobei \sim_R assoziiert über eine Einheit in R bedeutet.

Definition. Für $f \in K[x] \setminus \{0\}$ nennen wir das $d \in K^\times$ mit $f = df^*, f^* \in R[x]$ primitiv, wieder den *Inhalt* von f .

Proposition (Gauss). Sei R faktoriell. Für $f, g \in R[x]$ gilt $I(fg) \sim I(f)I(g)$. Insbesondere ist das Produkt von primitiven Elementen von $R[x]$ wieder primitiv.

Im folgenden werden wir die „Reduktion der Koeffizienten“ verwenden: Für ein $p \in R$ gibt es einen Ringhomomorphismus $f \in R[x] \mapsto f \bmod p \in R/(p)[x], \sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n (a_i + (p)) X^i$. Dies folgt aus dem Satz von 4. VO (wobei $\varphi(a) = a + (p)$ und $\Phi(X) = X$).

Satz (Gauss). Sei R ein faktorieller Ring. Dann ist auch $R[x]$ faktoriell. Des Weiteren hat $R[x]$ genau die beiden Typen von Primelementen:

- $p \in R$ prim ist auch ein Primelement von $R[x]$.
- $f \in R[x]$ primitiv so dass f irreduzibel als Element von $K[x]$ ist, ist ein Primelement von $R[x]$.

Korollar. Sei $f \in R[x]$ primitiv. Dann ist f irreduzibel als Element von $R[x]$ gdw. f ist irreduzibel als Element von $K[x]$.

Lemma. Sei K ein Körper und $a \in K$. Dann gilt für jedes $f \in K[x]$

$$f(x) = (x - a)g(x) + r \quad \text{für} \quad g(x) \in K[x], r \in K.$$

Daher gilt $f(a) = 0 \Leftrightarrow (x - a) \mid f(x)$.

Proposition. Sei K ein Körper. Dann sind lineare Polynome der Form $x - a$ für $a \in K$ irreduzibel als Elemente von $K[x]$. Für quadratische ($\deg(f) = 2$) und kubische ($\deg(f) = 3$) Polynome $f \in K[x]$ gilt

$$f \text{ ist irreduzibel} \Leftrightarrow f \text{ hat keine Nullstelle } (\forall a \in K \text{ gilt } f(a) \neq 0)$$

Satz (Fundamentalsatz der Algebra). Jedes Polynom $f \in \mathbb{C}[x]$ mit $\deg(f) > 0$ hat eine Nullstelle in \mathbb{C} .

Die irreduziblen Elemente von $\mathbb{C}[x]$ sind genau die linearen Polynome. Insbesondere hat jedes $f \in \mathbb{C}[x]$ eine Faktorisierung in Linearfaktoren

$$f(x) = a \prod_{j=1}^{\deg(f)} (x - z_j).$$

für gewisse $a \in \mathbb{C} \setminus \{0\}$ und $z_1, \dots, z_{\deg(f)} \in \mathbb{C}$.

Korollar (Fundamentalsatz für \mathbb{R}). Ein Polynom in $\mathbb{R}[x]$ ist irreduzibel gdw. entweder $\deg(f) = 1$ ist oder $\deg(f) = 2$ ist und f keine Nullstellen in \mathbb{R} besitzt.

Proposition. Sei R ein faktorieller Ring. Sei $f \in R[x]$ und $\frac{a}{b} \in K$ mit $b \neq 0, (a, b)$ coprim. Falls $f(\frac{a}{b}) = 0$ ist, so ist b ein Teiler von führenden Koeffizienten von f und a ein Teiler vom konstanten Term von f .

Proposition. Sei R ein faktorieller Ring und $p \in R$ ein Primelement. Angenommen $f \in R[x]$ erfülle:

- f primitiv
- $\deg(f) = \deg(f \bmod p)$ mit $f \bmod p \in R/(p)[x]$
- $f \bmod p \in \frac{R}{(p)}[x]$ ist irreduzibel

Dann ist $f \in R[x]$ ein Primelement.

Satz (Eisenstein-Kriterium). Sei R ein faktorieller Ring und $p \in R$ ein Primelement. Sei $f(x) = \sum_{i=0}^n a_i x^i$ primitiv mit $n \geq 1, p \nmid a_n, p \mid a_i$ für $i = 0, \dots, n-1$ und $p^2 \nmid a_0$. Dann ist f irreduzibel.

Korollar. Für jede Primzahl $p \in \mathbb{N}$ ist das p -te Kreisteilungspolynom

$$\Phi_p(x) = 1 + x + x^2 + \dots + x^{p-1} = \frac{x^p - 1}{x - 1}$$

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

Bemerkung. Für $p \in \mathbb{N}$ prim gilt allerdings

$$(x + y - z)^p = x^p + y^p - z^p \in \mathbb{F}_p[x, y, z].$$

nicht irreduzibel.

Kapitel 3: Gruppentheorie

3.1 Definition und Beispiele

Definition. Eine Menge G gemeinsam mit einer Abbildung $\cdot : G \times G \rightarrow G$ heißt eine Gruppe falls folgende Axiome erfüllt sind:

- 1) Assoziativität: $\forall a, b \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- 2) Einheit: $\exists e \in G \forall a \in G : e \cdot a = a \cdot e = a$
- 3) Inverse: $\forall a \in G \exists x \in G : a \cdot x = x \cdot a = e$ (wobei e wie in 2) ist)

Lemma. Sei G eine Gruppe. Die Einheit e wie in 2) ist eindeutig bestimmt durch $e \cdot a = a$ für alle $a \in G$, oder auch durch $e \cdot e = e$. Für jedes $a \in G$ ist die Inverse $x \in G$ durch $a \cdot x = e$ eindeutig bestimmt, wie schreiben $a^{-1} = x$. Insbesondere gilt $e^{-1} = e$, $(a^{-1})^{-1} = a$ und $(ab)^{-1} = b^{-1}a^{-1}$ für alle $a, b \in G$.

Bemerkung. Wir bezeichnen die Einheit auch als das Einselement und schreiben $e = e_G = 1 = 1_G$.

Definition. Sei G eine Gruppe und $a, b \in G$. Falls $ab = ba$ gilt, so sagen wir, dass a und b kommutieren. Falls alle Paare in G kommutieren, so heißt G kommutativ oder auch abelsch.

Bemerkung. Für abelsche Gruppen verwenden wir manchmal auch additive Notation $+: G \times G \rightarrow G$.

Definition. Für eine Gruppe G und $a \in G$ definiere wir die Potenzen von a durch

$$a^k := \begin{cases} \underbrace{a \cdot \dots \cdot a}_{k\text{-fache}} & \text{für } k > 0 \\ e & \text{für } k = 0 \\ \underbrace{a^{-1} \cdot \dots \cdot a^{-1}}_{|k|\text{-fache}} & \text{für } k < 0 \end{cases} \quad \text{für alle } k \in \mathbb{Z}.$$

Lemma (Potenzregel). a) $a^k a^l = a^{k+l}$ für $k \in \mathbb{Z}$.

b) $(a^k)^l = a^{kl}$ für $k \in \mathbb{Z}$.

c) Falls $a, b \in G$ kommutieren so kommutieren auch a^k und b^l und es gilt $(ab)^k = a^k b^k$.

Lemma (Gleichungen und Kürzen). Für alle $a, b \in G$ existiert ein eindeutig bestimmtes $x \in G$ mit $ax = b$, nämlich $x = a^{-1}b$. Für alle $a, b, c \in G$ gilt $a = b \Leftrightarrow ac = bc \Leftrightarrow ca = cb$.

Definition. Angenommen G_1, G_2 sind Gruppen. Ein *Homomorphismus* von G_1 nach G_2 ist eine Abbildung $\varphi : G_1 \rightarrow G_2$ mit $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in G_1$. Wir definieren den *Kern* $\text{Ker}(\varphi) = \varphi^{-1}\{e_{G_2}\} = \{a \in G_1 \mid \varphi(a) = e_{G_2}\}$ und das *Bild* $\text{Im}(\varphi) = \varphi(G_1) = \{b \in G_2 \mid \exists a \in G_1 \text{ mit } \varphi(a) = b\}$. Falls φ bijektiv ist, so sprechen wir auch von einem *Isomorphismus* der Gruppen und sagen G_1 und G_2 sind *isomorph*.

Definition. Sei G eine Gruppe. Eine Untergruppe von G ist eine nichtleere Teilmenge $H \subseteq G$ mit $ab^{-1} \in H$ für alle $a, b \in H$. Wir schreiben $H < G$.

Übung. Sei G eine Gruppe und $H \subseteq G$. Äquivalent sind:

- 1) H ist eine Untergruppe

- 2) $e \in H$, und $a, b \in H \Rightarrow ab \in H$ und $a^{-1} \in H$
 3) H ist eine Gruppe und $\iota : H \rightarrow G$ ist ein Homomorphismus.

Falls $|H| < \infty$, so ist auch folgende Aussage mit obigen Aussagen äquivalent:

- 4) H ist nichtleer, und $a, b \in H \Rightarrow ab \in H$.

Lemma. Sei G eine Gruppe und $a \in G$. Dann definiert $k \in \mathbb{Z} \mapsto a^k \in G$ einen Gruppenhomomorphismus. Entweder ist φ injektiv oder es gibt ein $n_0 > 0$ mit $\text{Ker}(\varphi) = (n_0) = \mathbb{Z}n_0$.

Definition. Falls φ wie im Lemma injektiv ist, so sagen wir, dass a unendliche Ordnung hat. Falls $\text{Ker}(\varphi) = (n_0)$ mit $n_0 > 0$ ist, so sagen wir, dass a Ordnung n_0 hat.

3.2 Konjugation

Lemma. Sei G eine Gruppe.

- a) Für jedes $g \in G$ ist $\gamma_g : G \rightarrow G, x \mapsto gxg^{-1}$ ein Automorphismus von G , welche ein innerer Automorphismus genannt wird.
 b) Die Abbildung $g \in G \mapsto \gamma_g \in \text{Aut}(G)$ ist ein Homomorphismus. Der Kern von Φ ist das Zentrum $Z_G = \{g \in G \mid gx = xg \forall x \in G\}$.

Definition. Sei G eine Gruppe und $g \in G$. Dann ist die Menge der Fixpunkte γ_g gleich dem Zentralisator von g :

$$\text{Cent}_g = \{x \in G \mid gx = xg\}.$$

Definition. Sei G eine Gruppe und $x, y \in G$. Wir sagen x, y sind zueinander konjugiert, falls es ein $g \in G$ mit $gxg^{-1} = y$.

Lemma. „Konjugiert sein“ definiert eine Äquivalenzrelation auf jeder Gruppe.

Manchmal ist G sehr kompliziert und unüberschaubar aber die Konjugationsklassen sind einfacher zu verstehen.

3.3 Untergruppen und Erzeuger

Wiederholung: $H \subseteq G$ nichtleer ist eine Untergruppe ($H < G$) falls für alle $a, b \in H$ gilt $ab^{-1} \in H$.

Lemma. Eine Untergruppe von einer Untergruppe ist eine Untergruppe.

Lemma. Sei G eine Gruppe und I eine Menge und $H_i < G$ für jedes $i \in I$. Dann ist $\bigcap_{i \in I} H_i < G$.

Definition. Sei G eine Gruppe und $X \subseteq G$ eine Teilmenge. Die Untergruppe, die von X erzeugt wird ist definiert als

$$\langle X \rangle = \bigcap_{\substack{H < G \\ X \subseteq H}} H.$$

Wir nennen X die Erzeugendenmenge von $\langle X \rangle$. Falls $\langle X \rangle = G$ sagen wir, dass G durch X erzeugt wird. Falls $X = \{g\}$ dann nennen wir $\langle X \rangle = \langle g \rangle$ die von g erzeugte zyklische Untergruppe von G .

Lemma. Sei G eine Gruppe und $X \subseteq G$. Dann ist $\langle X \rangle = \{x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} \mid n \in \mathbb{N}, x_1, \dots, x_n \in X, \varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}\}$.

Lemma. Sei G eine Gruppe und $a \in G$. Dann gilt $\langle a \rangle \cong \mathbb{Z}/(n_0)$ für ein $n_0 \in \mathbb{N}$.

Bemerkung. Es gibt keinen „Basis- oder Dimensionsbegriff“: Denn in S_6 gibt es eine Untergruppe, die von 3 oder mehr Elementen erzeugt wird, aber nicht von weniger:

$$H = \langle \tau_{1,2}, \tau_{3,4}, \tau_{5,6} \rangle \cong \mathbb{F}_2^3.$$

Definition. Sei G eine Gruppe. Der *Kommutator* von $a, b \in G$ ist

$$[a, b] = aba^{-1}b^{-1}.$$

Die *Kommutatorgruppe* ist

$$[G, G] = \langle [a, b] : a, b \in G \rangle.$$

3.4 Nebenklassen und Quotienten

Definition. Sei G eine Gruppe und $H < G$. Wir definieren zwei Relationen auf G

$$a \sim_H b \Leftrightarrow b^{-1}a \in H \quad a {}_H \sim b \Leftrightarrow ba^{-1} \in H.$$

Wir nennen die Menge $aH = \{ah \mid h \in H\}$ die Linksnebenklasse mit Linksrepräsentanten a und schreiben auch

$$G/H = \{aH \mid a \in G\}.$$

Außerdem nennen wir die Menge $Ha = \{ha \mid h \in H\}$ die Rechtsnebenklasse mit Rechtsrepräsentanten a und schreiben

$$H/G = \{Ha \mid a \in G\}.$$

Lemma. Sei G eine Gruppe und $H < G$. Dann ist \sim_H eine Äquivalenzrelation und $[a]_{\sim_H}$ und G/H ist der Quotient von G bzgl. \sim_H . Dies gilt analog für ${}_H \sim$.

Satz. Sei G eine Gruppe und $H < G$.

- (1) G/H und H/G sind (auf natürliche Weise) gleichmächtig.
- (2) [Lagrange] Falls $|G| < \infty$, dann gilt $|G| = |G/H| \cdot |H|$. Insbesondere gilt $|H|$ ist ein Teiler von $|G|$.

Definition. Die Kardinalität von G wird auch die *Ordnung* von G genannt. Die Kardinalität von G/H wird der *Index* $[G : H]$ von H in G genannt.

Korollar. Sei G eine endliche Gruppe und $g \in G$. Dann teilt die Ordnung von g die Ordnung von G . Des Weiteren gilt $g^{|G|} = e$.

Korollar. In $\mathbb{F}_p = \mathbb{Z}/(p)$ gilt $a^{p-1} = \begin{cases} 0 & a = 0 \\ 1 & \text{für alle } a \in \mathbb{F}_p^\times \end{cases}$

Korollar (Erste Klassifikation von Gruppen). Sei G eine endliche Gruppe und $|G| = p \in \mathbb{N}$ prim. Dann ist G isomorph zu $\mathbb{Z}/(p)$.

\Rightarrow Es gibt bis auf Isomorphie nur eine Gruppe der Ordnung $2, 3, 5, 7, \dots$

Im Allgemeinen haben G/H und H/G keine natürliche Gruppenstruktur.

Satz. Sei G eine Gruppe und $H < G$. Die folgenden Bedingungen sind äquivalent

- (1) Für alle $x \in G$ ist $xH = Hx$.

- (2) Für alle $x \in G$ ist $xHx^{-1} = H$.
 (3) Es existiert eine Gruppe G_1 und ein Gruppenhomomorphismus $\varphi : G \rightarrow G_1$ mit $H = \text{Ker}(\varphi)$.
 (4) Für alle $x, y \in G$ gilt $(xH)(yH) = (xy)H$.
 (5) G/H ist (auf natürliche Weise) eine Gruppe so dass $\varphi : G \rightarrow G/H, g \mapsto gH$ ein Gruppenhomomorphismus ist.

Definition. Sei G eine Gruppe und $H < G$. Wir sagen H ist *normal* in G oder ein *Normalteiler* von G falls H die Bedingungen in obigem Satz erfüllt. Wir schreiben in diesem Fall auch $H \triangleleft G$. Falls $H \triangleleft G$ so nennen wir G/H die *Faktorgruppe* von G modulo H .

Definition. Sei $G \neq \{e\}$ eine Gruppe. Wir sagen G ist *einfach* falls G nur $\{e\}$ und G als Normalteiler besitzt.

Satz (Erster Isomorphiesatz). Sei $\varphi : G \rightarrow H$ eine Homomorphismus zwischen zwei Gruppen G und H . Dann induziert φ einen Isomorphismus $|\varphi| : G/\text{Ker}(\varphi) \rightarrow \text{Im}(\varphi)$ so dass folgendes Diagramm kommutiert

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \pi \downarrow & & \uparrow \iota \\ G/\text{Ker}(\varphi) & \xrightarrow{|\varphi|} & \text{Im}(\varphi) < H \end{array}$$

mit π als der kanonischen Projektion und ι der Einbettung. Also gilt $\varphi = \iota \circ |\varphi| \circ \pi$.

Korollar (Zweiter Isomorphiesatz). Sei G eine Gruppe, $H \triangleleft G$ und $K < G$. Dann gilt $KH = HK < G, H \triangleleft KH, H \cap K \triangleleft K$ und

$$K/H \cap K \cong KH/H.$$

mit $xH \cap K \leftrightarrow xH$ für $x \in K$

Übung: Das Produkt von zwei Untergruppen ist im Allgemeinen keine Untergruppen. Das Produkt von zwei normalen Untergruppen ist eine normale Untergruppe.

Korollar (Dritter Isomorphiesatz). Sei G eine Gruppe, $H \triangleleft G, K \triangleleft G$ und $K < H$. Dann ist $H/K \triangleleft G/K$ und es gilt

$$G/K/H/K \cong G/H$$

wobei $(xK)^{H/K} \cong xH$ einander im Isomorphismus entsprechen.

Korollar. Sei G eine Gruppe und $H \triangleleft G$. Für eine beliebige weitere Gruppe K gibt es eine natürliche Bijektion zwischen

$$\text{Hom}(G/H, K) = \{\varphi : G/H \rightarrow K \text{ Homomorphismus}\} \quad \text{und} \quad \{\varphi : \text{Hom}(G, K) \mid \varphi|_H \equiv e_K\}.$$

Korollar. Sei G eine Gruppe und $H \triangleleft G$. Dann sind die folgenden beiden Abbildungen invers zueinander:

$$(K < G \text{ mit } H < K) \mapsto K/H < G/H \quad \text{und} \quad (\pi^{-1}(\overline{K}) < G \text{ mit } H < \pi^{-1}(\overline{K})) \mapsto \overline{K} < G/H.$$

Übung: Sei G eine Gruppe und $H < G$ mit Index 2. Dann gilt $H \triangleleft G$.

Übung: Klassifizieren/Beschreiben Sie alle Gruppen der Ordnung $\leq 7 / \leq 8 / \leq 10$.

3.5 Gruppenwirkungen

Definition. Sei G eine Gruppe und T eine Menge. Eine *Gruppenwirkung* (Linkswirkung, Linksaktion) von G auf T ist eine Abbildung $\cdot : G \times T \rightarrow T, (g, t) \mapsto g \cdot t$, so dass

- $e \cdot t = t$ für $t \in T$
- $g_1 \cdot (g_2 \cdot t) = (g_1 g_2) \cdot t$ für $g_1, g_2 \in G$ und $t \in T$.

Wir sagen in diesem Fall auch kurz, dass T eine G -Menge ist.

Bemerkung. Obige Definition können wir äquivalent auch in folgender Form formulieren:

Es gibt einen Gruppenhomomorphismus $\alpha : G \rightarrow \text{Bij}(T), g \in G \mapsto \alpha_g$.

Der Zusammenhang zur obigen Definition ergibt sich durch die Formel $\alpha_g(t) = g \cdot t$

Definition. Sei G eine Gruppe und T eine G -Menge.

- $S \subseteq T$ heißt *invariant* falls $g \cdot S = S$ für alle $g \in G$.
- $t_0 \in T$ heißt *Fixpunkt* falls $g \cdot t_0 = t_0$ für alle $g \in G$. Die Menge der Fixpunkte wird mit $\text{Fix}_G(T) = \{t_0 \in T \mid t_0 \text{ ist ein Fixpunkt}\}$ bezeichnet.
- Für $t_0 \in T$ wird $G \cdot t_0 = \{g \cdot t_0 \mid g \in G\}$ als die *Bahn* (G -Bahn) bezeichnet.
- Für $t_0 \in T$ heißt $\text{Stab}_G(t_0) = \{g \in G \mid g \cdot t_0 = t_0\}$ der *Stabilisator* von t_0 .
- Falls $g \in G \mapsto \alpha_g \in \text{Bij}(T)$ wie in obiger Bemerkung injektiv ist, so heißt die Gruppenwirkung *treu*.
- Die Gruppenwirkung heißt *transitiv* falls es zu jedem Paar $t_1, t_2 \in T$ ein $g \in G$ mit $g \cdot t_1 = t_2$ gibt. Die Gruppenwirkung heißt *scharf transitiv* falls es zu jedem Paar $t_1, t_2 \in T$ genau ein $g \in G$ mit $g \cdot t_1 = t_2$ gibt.
- Die Menge der G -Bahnen wird mit $G \backslash T = \{G \cdot t_0 \mid t_0 \in T\}$ bezeichnet.

Lemma. Sei G eine Gruppe und T eine G -Menge. Dann definiert $t_1 \sim_G t_2 \Leftrightarrow \exists g \in G$ mit $g \cdot t_1 = t_2$ eine Äquivalenzrelation auf T . Die Bahnen sind genau die Äquivalenzklassen und $G/\sim_G = G \backslash T$ ist der Quotientenraum.

Definition. Sei G eine Gruppe und T_1, T_2 zwei G -Mengen. Ein G -Morphismus von T_1 nach T_2 ist eine Abbildung $f : T_1 \rightarrow T_2$ mit

$$f(g \underbrace{\cdot}_{\text{in } T_1} t) = g \underbrace{\cdot}_{\text{in } T_2} f(t)$$

für alle $t \in T_1$ und $g \in G$. g ist ein G -Isomorphismus falls f zusätzlich bijektiv ist.

Satz (Satz (über Bahnen und Stabilisator)). Sei G eine Gruppe und T eine G -Menge. Sei $t_0 \in T$, $T_0 = G \cdot t_0$ und $H = \text{Stab}_G(t_0)$. Dann ist $H < G$, T_0 ist invariant und

$$f : G/H \rightarrow T_0, gH \mapsto g \cdot t_0$$

ist ein wohldefinierter G -Isomorphismus. In diesem Satz ist also die Bahn isomorph zu G modulo Stabilisator.

Korollar. Sei G eine Gruppe und T eine G -Menge. Falls $|G| < \infty$, dann gilt

$$|G| = |G \cdot t_0| \cdot |\text{Stab}_G(t_0)|$$

Korollar. Sei G eine Gruppe und T eine endliche G -Menge. Dann gilt

$$|T| = |\text{Fix}_G(T)| + \sum_{|G \cdot t| > 1} [G : \text{Stab}_G(t)],$$

also die summe über die nicht trivialen Bahnen.

Satz (Cayley). Sei G eine endliche Gruppe. Dann ist G isomorph zu einer Untergruppe einer symmetrischen Gruppe S_n für $n \in \mathbb{N}$.

Bemerkung. Falls $H < G$ mit endlichem Index, so gibt es einen Homomorphismus $\alpha : G \rightarrow S_n$ mit $n = [G : H]$ und $\text{Ker}(\alpha) < H$.

3.6 Nilpotente und auflösbare Gruppen

Definition. Sei G eine Gruppe. Wir sagen G ist *nilpotent mit Nilpotenzgrad 1* falls G abelsch ist. Wir sagen G ist nilpotent mit *Nilpotenzgrad $n + 1$* (für $n \in \mathbb{N}_{\geq 1}$) falls G/Z_G nilpotent mit Nilpotenzgrad n ist.

Wir sagen G ist *nilpotent* falls es ein $n \in \mathbb{N}$ gibt so dass G nilpotent mit Nilpotenzgrad n ist.

Definition. Sei G eine Gruppe und $p \in \mathbb{N}$ eine Primzahl. Wir sagen G ist eine p -Gruppe falls $|G| = p^k$ für ein $k \in \mathbb{N}$.

Lemma (Fixpunkte von p -Gruppen). *Sei $p \in \mathbb{N}$ eine Primzahl und G eine p -Gruppe. Sei T eine G -Menge. Dann gilt $|\text{Fix}_G(T)| \equiv |T| \pmod{p}$.*

Satz. *Eine p -Gruppe ist nilpotent.*

Korollar. *Sei $p \in \mathbb{N}$ eine Primzahl und G eine Gruppe mit $|G| = p^2$. Dann ist G abelsch.*

Definition. Sei G eine Gruppe. Eine *Subnormalreihe in G* ist eine Folge von Untergruppen so dass

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_n = G$$

jede Untergruppe in der nächsten normal ist.

Definition. Sei G eine Gruppe. Wir sagen G ist *auflösbar* falls es eine Subnormalreihe in G (wie oben) gibt, so dass G_{k+1}/G_k eine abelsche Gruppe (für $k = 0, \dots, n-1$) ist.

Proposition. *Sei G eine Gruppe. Dann ist $[G, G] = \langle \{[a, b] \mid a, b \in G\} \rangle \triangleleft G$, und $G/[G, G]$ ist abelsch. Falls H eine abelsche Gruppe ist und $\varphi : G \rightarrow H$ ein Homomorphismus ist, so ist $\varphi([G, G]) = \{e_H\}$ und φ induziert einen Gruppenhomomorphismus $\bar{\varphi} : G/[G, G] \rightarrow H$. In diesem Sinne ist $G/[G, G]$ die größte abelsche Faktorgruppe von G .*

Proposition. *Sei G eine Gruppe. Dann ist G auflösbar genau dann wenn die folgende induktiv definierten höheren Kommutatorgruppen nach endlich vielen Schritten die triviale Untergruppe $\{e\}$ erreicht:*

$$\begin{aligned} G^{(0)} &= G \\ G^{(1)} &= [G^{(0)}, G^{(0)}] \text{ (Kommutatorgruppe)} \\ G^{(2)} &= [G^{(1)}, G^{(1)}] \text{ (2. Kommutatorgruppe)} \\ &\vdots \\ G^{(n+1)} &= [G^{(n)}, G^{(n)}] \end{aligned}$$

3.7 Satz von Sylow

Für eine endliche Gruppe G besagt der Satz von Lagrange, dass für $H < G$ sowohl die Ordnung $|H|$ als auch der Index $[G : H]$ Teiler von $|G|$ sind.

Satz (Sylow). *Sei G eine endliche Gruppe, $p \in \mathbb{N}$ prim und $n = |G| = p^k m$ für $k \geq 1$ und m teilerfremd zu p .*

- 1) *Es existiert eine maximale p -Untergruppe H_p mit $|H_p| = p^k$, welche Sylow p -Untergruppen genannt werden.*
- 2) *Falls $H < G$ eine p -Untergruppe ist, so existiert eine p -Sylow Untergruppe H_p mit $H < H_p$.*
- 3) *Je zwei Sylow p -Untergruppen sind konjugiert.*

Lemma. *Sei $p \in \mathbb{N}$ prim, $n = p^k m$ mit m teilerfremd zu p . Dann ist $\binom{n}{p^k}$ nicht durch p teilbar.*

3.8 Symmetrische und Alternierende Gruppen

Definition. Sei $n \geq 1$ natürlich, dann ist $S_n = \text{Bij}(\{1, \dots, n\})$. Die Elemente von S_n heißen *Permutationen*.

Satz. Sei $n \geq 1$. Auf S_n gibt es einen Homomorphismus $\text{sgn} : S_n \rightarrow \{\pm 1\}$, der jeder Permutation ein Vorzeichen zuordnet und einer Vertauschung τ_{ij} für $i \neq j$ das Vorzeichen -1 mit

$$\tau_{ij}(k) = \begin{cases} i & \text{für } k = j \\ j & \text{für } k = i \\ k & \text{sonst} \end{cases}.$$

Definition. $\sigma \in S_n$ heißt *gerade* falls $\text{sgn}(\sigma) = 1$, *ungerade* falls $\text{sgn}(\sigma) = -1$. Die *alternierende Gruppe* $A_n = \text{Ker}(\text{sgn})$ ist die Gruppe aller geraden Permutationen.

Notation (für $\sigma \in S_n$).

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Besser:

Notation (mittels Zyklen für $\sigma \in S_n$). Falls $\sigma = \text{id}$ schreiben wir einfach $\sigma = \text{id}$. Sei nun $\sigma \neq \text{id}$ und $i_1 \in \{1, \dots, n\}$ der erste Nichtfixpunkt (also i_1 minimal mit $\sigma(i_1) \neq i_1$). Wir bestimmen

$$\sigma(i_1), \sigma^2(i_1), \dots, \sigma^{k_1}(i_1) = i_1 \quad \text{für } k_1 > 1 \text{ minimal}.$$

Falls dies alle Nichtfixpunkte von σ sind, so nennen wir σ einen (k) -Zyklus und schreiben

$$\sigma = (i_1, \sigma(i_1), \sigma^2(i_1), \dots, \sigma^{k-1}(i_1)).$$

Falls nicht, so sei $i_2 > i_1$ der nächste Nichtfixpunkt (der noch nicht gefunden wurde) und bestimme

$$i_2, \sigma(i_2), \dots, \sigma^{k_2}(i_2) = i_2 \quad \text{für } k_2 > 1 \text{ minimal}$$

etc. Nach endlich vielen Schritten haben wir alle Nichtfixpunkte gefunden und schreiben

$$\sigma = (i_1, \sigma(i_1), \dots, \sigma^{k_1-1}(i_1))(i_2, \sigma(i_2), \dots, \sigma^{k_2-1}(i_2)) \dots (i_r, \sigma(i_r), \dots, \sigma^{k_r-1}(i_r)).$$

In diesem Fall sagen wir auch, dass σ *Zyklentyp*(Struktur) k_1, k_2, \dots, k_r hat (wobei die Zahlen k_1, \dots, k_r auch in einer anderen Reihenfolge auftreten dürfen).

Proposition. Zwei Permutationen sind in S_n genau dann konjugiert, falls sie dieselbe Zyklenstruktur haben.

Satz. A_n und S_n sind auflösbar für $n \leq 4$. A_n ist einfach für $n \geq 5$.

Für $n \geq 5$ wollen wir die Gruppenwirkung von A_n auf $\{1, \dots, n\}$ und folgende Lemmas verwenden.

Lemma. Sei $n \geq 3$. Dann ist die Wirkung von A_n auf $\{1, \dots, n\}$ transitiv.

Lemma. Sei $n \geq 5$ und $H \triangleleft A_n$ nicht die triviale Gruppe. Dann enthält H eine Permutation $\sigma \neq e$ mit mindestens einem Fixpunkt.

3.9 Gruppen kleiner Ordnung & Klassifikation

Satz. Sei G eine Gruppe der Ordnung $n = |G| < 100$. Dann ist entweder G auflösbar oder $n = 60$ und $G \simeq A_5$.

Für den Beweis des Satzes bedienen wir uns vieler bereits bewiesenen kleinen Lemmas, dem Sylowsatz und weiteren Lemmas mit zunehmender Komplexität. Des Weiteren verwenden wir Induktion nach n und eine grundlegende Eigenschaft von Auflösbarkeit.

Definition (Wiederholung). Sei G eine Gruppe. Wir sagen G ist *auflösbar* falls es eine Subnormalreihe

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_k = G$$

gibt für die die Faktorgruppen $\frac{G_j}{G_{j-1}}$ für $j = 1, \dots, k$ alle abelsch sind.

Proposition (Lagereigenschaft und Auflösbarkeit). Sei G eine Gruppe und $N \triangleleft G$. Falls N und G/N auflösbar sind, so gilt dasselbe für G .

3.10 Freie Gruppen und Relationen

Definition. Sei $n \geq 1$ eine natürliche Zahl. Dann wird \mathbb{Z}^n als die *freie abelsche Gruppe* mit n Erzeugenden $b_1 = (1, 0, \dots, 0)^T, \dots, b_n = (0, \dots, 0, 1)^T$ bezeichnet.

Lemma. Sei G eine abelsche Gruppe und $a_1, \dots, a_n \in G$. Dann gibt es einen eindeutig bestimmten Gruppenhomomorphismus $\phi : \mathbb{Z}^n \rightarrow G$ mit $\phi(b_j) = a_j$ für $j = 1, \dots, n$.

Satz. Sei $n \geq 1$ und b_1, \dots, b_n paarweise verschieden. Dann existiert eine „freie Gruppe“ F_n , welche von b_1, \dots, b_n erzeugt wird, mit folgender „universeller“ Eigenschaft: Für jede Gruppe G und Elemente $a_1, \dots, a_n \in G$ gibt es einen eindeutig bestimmten Homomorphismus $\phi : F_n \rightarrow G$ mit $\phi(b_j) = a_j$ für $j = 1, \dots, n$.

Kapitel 4: Modultheorie

(siehe Seite 288, aber „kommutativ“)

4.1 Definition & Beispiel

„Moduln verhalten sich zu Ringen wie Vektorräume zu Körpern.“

Definition. Sei R ein Ring. Ein R -Modul M ist eine abelsche Gruppe gemeinsam mit einer Skalarmultiplikation $R \times M \rightarrow M, (a, m) \mapsto a \cdot m$ mit folgenden Eigenschaften:

- $a \cdot (m_1 + m_2) = am_1 + am_2$ für $a \in R, m_1, m_2 \in M$.
- $(a + b) \cdot m = am + bm$ für $a, b \in R, m \in M$.
- $a \cdot (b \cdot m) = (ab) \cdot m$ für $a, b \in R, m \in M$.
- $1 \cdot m = m$ für $m \in M$.

Definition. Seien R ein Ring und M, N R -Moduln. Wir sagen $\phi : M \rightarrow N$ ist R -linear (ein *Modulmorphismus über R*) falls ϕ ein Gruppenmorphismus ist und $\phi(am) = a\phi(m)$ für alle $a \in R$ und $m \in M$.

Definition. Sei R ein Ring und M ein R -Modul. Ein *Untermodul* ist eine Untergruppe $N < M$ mit $a \cdot n \in N$ für alle $a \in R$ und $n \in N$.

Lemma. Sei R ein Ring, M ein R -Modul und $N < M$ ein Untermodul. Dann induziert die R -Modulstruktur auf M eine R -Modulstruktur auf M/N so dass die kanonische Projektion

$$\begin{cases} \pi : M \rightarrow M/N \\ m \mapsto m + N \end{cases} \quad R\text{-linear ist.}$$

Proposition (Erster Isomorphiesatz). Seien R ein Ring, M, N R -Moduln, $\phi : M \rightarrow N$ R -linear. Dann sind $\text{Ker}(\phi) < M, \text{Im}(\phi) < N$ Untermoduln und ϕ induziert einen R -linearen Isomorphismus

$$\bar{\phi} : M/\text{Ker}(\phi) \rightarrow \text{Im}(\phi).$$

Lemma. Seien R ein Ring und M_1, \dots, M_n R -Moduln. Dann ist auch $M_1 \times \dots \times M_n$ ein R -Modul mit koordinatenweiser Skalarmultiplikation

$$a \cdot (m_1, \dots, m_n) = (am_1, \dots, am_n) \quad \text{für } a \in R, (m_1, \dots, m_n) \in M_1 \times \dots \times M_n.$$

Lemma. Seien R, S zwei Ringe, M ein R -Modul und N ein S -Modul. Dann ist $M \times N$ ein $R \times S$ -Modul mit koordinatenweiser Skalarmultiplikation

$$(a, b) \cdot (m, n) = (am, bn) \quad \text{für } (a, b) \in R \times S, (m, n) \in M \times N.$$

Übung: Charakterisiere die Untermoduln von $M \times N$ (über $R \times S$).

Welche Ringe könnten interessant sein?

$$\text{Körper} \rightarrow \text{Vektorräume} \quad \mathbb{Z} \rightarrow \text{Abelsche Gruppen} \quad K[X] \rightarrow ?$$

Satz. Sei K ein Körper und M ein Vektorraum über K . Die Definition einer Modulstruktur auf M über $K[X]$ (die mit der Vektorraumstruktur von M über K kompatibel ist) ist gleichzusetzen

mit der Auswahl einer K -linearen Abbildung $\varphi : M \rightarrow M$. Formaler formuliert sind die folgenden beiden Abbildungen invers zueinander:

Eine Skalarmultiplikation auf M über $K[X]$ dessen Einschränkung auf $K \times M$ die Skalarmultiplikation von M über K ist.

Eine K -lineare Abbildung $\varphi : M \rightarrow M$

$$\begin{array}{ccc} & \cdot & \longmapsto \varphi(m) = X \cdot m \text{ für } m \in M \\ f \cdot m = (f(\varphi))(m) = (\sum_k a_k \varphi^k)(m) \text{ für } & \longleftarrow & \varphi \\ f = \sum_k a_k X^k \in K[X] & & \end{array}$$

Wir wollen endlich erzeugte Moduln über Hauptidealringen klassifizieren!

$\xrightarrow{\mathbb{Z}}$ Klassifikation von endlich erzeugten abelschen Gruppen.

$\xrightarrow{K[X]}$ Satz über Jordan Normalform.

4.2 Freie Moduln

Definition. Sei I eine Menge und R ein Rnig. Wir bezeichnen

$$R^{(I)} = \{x : I \rightarrow R \mid x_i = 0 \text{ für alle bis auf endlich viele } i \in I\}$$

als den *freien R -Modul* (über der Indexmenge I). Wir nennen

$$e_i = \mathbb{1}_{\{i\}} \quad \text{für } i \in I$$

die *Standardbasis* von $R^{(I)}$. Ein *freier Modul* M ist ein Modul isomorph zu $R^{(I)}$ für eine Menge I . Die Kardinalität von I wird als der *Rang* von $M \cong R^{(I)}$ bezeichnet.

Lemma. Sei $R \neq \{0\}$ ein Ring. Dann ist der Rang eines Moduls wohldefiniert.

Behauptung. Freie Moduln verhalten sich am ehesten wie Vektorräume ...

Proposition. Seien $m, n \geq 1$ natürliche Zahlen und R ein Ring. Dann gilt

$$\text{Hom}(R^n, R^m) \cong \text{Mat}_{mn}(R)$$

wie in der Linearen Algebra.

Definition. Sei M ein R -Modul über einem Ring R . Wir sagen $x_1, \dots, x_n \in M$ sind *frei* oder *linear unabhängig* (l.u.) falls die Abbildung $a \in R^n \mapsto \sum_{i=1}^n a_i x_i$ injektiv ist.

Falls $x_1, \dots, x_n \in M$ l.u. sind, so ist das Bild der Abbildung ein freier Untermodul von M .

4.3 Torsionsmoduln

Definition. Sei R ein Ring und M ein R -Modul. Wir sagen $m \in M$ ist ein *Torsionselement*, falls es ein $a \in R \setminus \{0\}$ gibt mit $a \cdot m = 0$. Wir sagen M ist ein *Torsionsmodul* falls jedes $m \in M$ ein Torsionselement ist. Wir sagen M ist *torsionsfrei* falls $m = 0$ das einzige Torsionselement von M ist.

4.4 Struktur von endlich erzeugten Moduln über Hauptidealringen

Definition. Sei R ein Ring und M ein R -Modul. Für eine Teilmenge $X \subseteq M$ wird

$$\langle X \rangle_R = \left\{ \sum_{x \in E} a_x x \mid a_x \in R \text{ für } x \in E \text{ und } E \subseteq X \text{ endlich} \right\}$$

als die R -lineare Hülle von X oder als der von X erzeugte Untermodul bezeichnet. Falls es eine Teilmenge $X \subseteq M$ mit $|X| < \infty$ und $\langle X \rangle_R = M$ gibt, so heißt M endlich erzeugt.

Wir wollen ab nun nur Hauptidealringe betrachten - dort wäre jeder Untermodul von R wieder frei mit Rang 0 oder 1.

Satz (Klassifikationssatz (1. Teil)). Sei R ein Hauptidealring und M ein endlich erzeugter Modul über R . Dann ist M isomorph zu einem direkten Produkt $R^n \times T$ wobei

$$T = M_{\text{tors}} = \{m \in M \mid m \text{ ist ein Torsionselement von } M\}$$

und n ist der Rang von M/M_{tors} . Insbesondere ist M ein freier Modul genau dann wenn $M_{\text{tors}} = \{0\}$.

Proposition. Sei R ein Hauptidealring und $n \geq 1$. Dann ist jeder Untermodul $M \subseteq R^n$ ein freier R -Modul mit Rang $\leq n$.

Satz (Klassifikationssatz (2. Teil)). Sei R ein Hauptidealring und M_{tors} ein endlich erzeugter Torsionsmodul. Dann existieren $d_1 \mid d_2 \mid \dots \mid d_n$ in $R \setminus \{0\}$ so dass

$$M_{\text{tors}} = R/(d_1) \times \dots \times R/(d_n).$$

Alternativ gilt

$$M_{\text{tors}} \cong \prod_{j=1}^k M_{\text{tors}}^{(p_j)}$$

wobei $p_1, \dots, p_k \in R$ inäquivalente Primzahlen in R sind und

$$M_{\text{tors}}^{(p_j)} = \{m \in M_{\text{tors}} \mid \text{es existiert ein } l \in \mathbb{N} \text{ mit } p_j^l m = 0\} \cong R/(p_j^{n_{j,1}}) \times \dots \times R/(p_j^{n_{j,n}}).$$

Satz (Smith Normalform). Sei R ein Hauptidealring, $k, l \geq 1$ natürliche Zahlen und $A \in \text{Mat}_{kl}(R)$. Dann existieren $g \in \text{GL}_k(R)$ und $h \in \text{GL}_l(R)$ so dass

$$gAh^{-1} = \begin{pmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_n & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}$$

für $d_1 \mid d_2 \mid \dots \mid d_n$ in $R \setminus \{0\}$.

- Wir beweisen diesen Satz nur für Euklidische Ringe.
- Im Gauss'schen Eliminationsalgo entsprechen Zeilenoperationen einer Linksmultiplikation und Spaltenoperationen einer Rechtsmultiplikation.
- Wir kombinieren Gauss mit Division mit Rest.
- Falls $R = K$ ein Körper ist, so können wir $d_1 = d_2 = \dots = d_n = 1$ annehmen und $n = \text{Rang von } A$.

4.5 Endlich erzeugte abelsche Gruppen

Satz. Sei G eine endlich erzeugte (additiv geschriebene) abelsche Gruppe. Dann gilt

$$G \cong \mathbb{Z}/(d_1) \times \dots \times \mathbb{Z}/(d_n) \times \mathbb{Z}^k$$

wobei $1 \leq d_1 \mid d_2 \mid \dots \mid d_n \neq 0$ und $k \geq 0$.

Alternativ gilt

$$G \cong \prod_{p>0 \text{ prim}} G_p \times \mathbb{Z}^k \quad \text{und} \quad G_p \cong \mathbb{Z}/(p^{k_{p,1}}) \times \dots \times \mathbb{Z}/(p^{k_{p,n}}).$$

wobei G_p die Sylow p -Untergruppe ist.

4.6 Jordan-Normalform

Satz. Sei V ein endlich dimensionaler Vektorraum über \mathbb{C} und $\varphi : V \rightarrow V$ linear. Dann existiert eine Basis von V , so dass φ eine Matrixdarstellung der folgenden Form besitzt:

$$\begin{pmatrix} J_1 & & \\ & J_2 & \\ & & \ddots \end{pmatrix} \quad \text{und jeder Block } J_k \text{ hat die Form} \quad \begin{pmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & \ddots \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix}.$$

Dies ist die Jordan-Normalform von φ .