Inhaltsverzeichnis

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

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

so dass folgende Axiome gelten.

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

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

Dies definiert eine Abbildung $\mathbb{Z} \times R \to R, (n, a) \mapsto n \cdot a$. 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 $f : R \to S$ 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 $\mathrm{id} : S \to R, s \mapsto s$ 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 $a \in \mathbb{R} \setminus \{0\}$ heißt ein Nullteiler falls es ein $b \in \mathbb{R} \setminus \{0\}$ 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 $R^x = \{a \in R \mid a|1\}$

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

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. $0 = (0)_{n=0}^\infty, 1 = (1, 0, 0, \ldots)$
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

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

Allgemeiner: Sei a ein Polynom, dann ist

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

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

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

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

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

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

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

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

$$\deg_{\text{total}}(1 + X_1^3 + X_2X_3) = 3 \qquad \deg_{X_2}(1 + X_1^3 + X_2X_3) = 1.$$

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

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

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

Notation. Wir schreiben für zwei kommutative Ringe R, S

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

in dieser Notation können wir obigen Satz in der Form

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

schreiben. Dies kann iteriert werden:

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

1.4 Ideale und Faktorringe

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 un $I \subseteq R$ ein Ideal.*

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

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

$$^{R}/_{I} \times {}^{R}/_{I} \to {}^{R}/_{I} \quad \text{bzw.} \quad {}^{R}/_{I} \to {}^{R}/_{I}.$$

3. *Mit diesen Abbildungen,* $0_{R/I} = [0]_\sim, 1_{R/I} = [1]_\sim$ *ist* $^{R}/_{I}$ *ein Ring und die kanonische Projektion* $p : R \to {}^{R}/_{I}$ *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*

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

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

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

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* $\varphi : R \to S$ *ist ein Ringhomomorphismus.*

1. *Dann induziert* φ *einen Ringisomorphismus*

$$\overline{\varphi} : {}^{R}/_{\mathrm{Ker}(\varphi)} \to \mathrm{Im}(\varphi) = \varphi(R) \subseteq S$$

so dass $\varphi = \overline{\varphi} \circ p$ *wobei* $p : R \to {}^{R}/_{\mathrm{Ker}(\varphi)}$ *die kanonische Projektion ist (Diagramm links).*

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

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "p"] & S \\ {}^{R}/_{\mathrm{Ker}(\varphi)} \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd} \qquad \begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "p_I"] & S \\ {}^{R}/_{I} \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$

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.

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

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* $\varphi : R \to {}^{R}/_{I_1} \times \ldots \times {}^{R}/_{I_n}$ *mit* $x \mapsto (x + I_1, \dots, x + I_n)$ *surjektiv mit* $\mathrm{Ker}(\varphi) = I_1 \cap \ldots \cap I_n$.
Dies induziert einen Ringisomorphismus $^{R}/_{I_1 \cap \ldots \cap I_n} \to {}^{R}/_{I_1} \times \ldots \times {}^{R}/_{I_n}$.

1.5 Charakteristik eines Körpers

Sei K ein Körper. Dann gibt es einen Ringhomomorphismus $\varphi : \mathbb{Z} \to K$ mit $\begin{cases} n \in \mathbb{N} \mapsto \underbrace{1 + \ldots + 1}_{n-\text{mal}} \\ -n \in \mathbb{N} \mapsto -(\underbrace{1 + \ldots + 1}_{n-\text{mal}}) \end{cases}$

Sei $I = \mathrm{Ker}(\varphi)$ so, dass $\mathbb{Z}/I \equiv \mathrm{Im}(\varphi) \subseteq K$. Da K ein Körper ist, ist $\mathrm{Im}(\varphi)$ 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 $\varphi : \mathbb{Z} \to K$ injektiv ist. Wir sagen, dass K Charakteristik $p \in N_{>0}$ hat falls $\varphi : \mathbb{Z} \to K$ den Kern (p) hat.

Proposition. *Sei K ein Körper mit Charakteristik $p > 0$. Dann ist die* Frobeniusabbildung *$F : x \in K \to x^p \in K$ 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 $\mathbb{C}[X_1, \ldots, X_n]$ 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 $\mathrm{id} : S \to R, s \mapsto s$ 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 $a_1, \ldots, a_n \in R$. Wir definieren

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

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

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

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

1.8 Matrizen

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

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m_1} & \dots & a_{mn} \end{pmatrix}.$$

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

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

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

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*

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

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

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

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

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

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 $N : R \setminus \{0\} \to \mathbb{N}$ 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 $J_0 \subseteq J_1 \subseteq J_2 \subseteq \ldots$ eine aufsteigende 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 Primelementen von R schreiben lässt: $a = u \cdot p_1 \cdot \ldots \cdot p_m$ für $u \in R^\times, m \in \mathbb{N}, p_1, \ldots p_m \in R$ 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 $\{1, \ldots, n\}$, d.h.

$$S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} \text{ bijektiv}\}.$$

Satz (Eindeutige Primfaktorzerlegung)**.** *Sei R ein faktorieller Ring, dann besitzt jedes nichttriviale Element von R eine bist 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 $p_1, \ldots, p_m$ mit $a = up_1 \ldots p_m$.
Falls $a = vq_1 \ldots q_n$ eine weitere Zerlegung ist, wobei $v \in R^\times$, $n \in \mathbb{N}$ und $q_1, \ldots, q_n$ prim sind, dann gibt es $\sigma \in S_n$ so dass $q_j \sim p_{\sigma(j)}$ für $j = 1, \ldots, n$ und $m = n$.

Die Existenz der Zerlegung ist die Definition von „faktorieller Ring“. Wir nennen $p_1, \ldots p_m$ 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 $a_1, \ldots, a_l \in R$ definieren und die obige Proposition gilt analog.

Definition. Sei R ein faktorieller Ring. Wir sagen $a_1, \ldots, a_l \in R$ sind *coprim* falls 1 ein ggT von $a_1, \ldots, a_l$ 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 $K = \mathrm{Quot}(R)$. 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 Zahlenkörper: $K = \mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ mit $d \in \mathbb{Z}$, das kein Quadrat ist. Isomorph dazu ${}^{\mathbb{Q}[x]}\!/\!{}_{(x^2 - d)}$.

Wir definieren auf K die Konjugation $\tau : K \to K, a + b\sqrt{d} \mapsto a - b\sqrt{d}$. 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 $N : K \to \mathbb{Q}$ multiplikativ ist, daher

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

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

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

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

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

Satz. *Im $R_{falsch} = \mathbb{Z}[\sqrt{3}i]$ funktioniert Division mit Rest nicht wie in den obigen Fällen. Aber in $R_{richtig} = \mathbb{Z}[\zeta] = \{a + b\zeta : a, b \in \mathbb{Z}\}$ 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 $f \in \mathbb{R}[x] \setminus \{0\}$. 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 *primitv* 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* $K = \mathrm{Quot}(R)$. *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 $f \in R[x] \mapsto f \mod p \in R/(p)[x], \sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n (a_i + (p))X^i$. 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 $a \in C \setminus \{0\}$ und $z_1, \ldots, z_{\deg(f)} \in \mathbb{C}$.

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 $i = 0, \ldots, n-1$ und $p^2 \nmid a_0$. Dann ist f irreduzibel.*

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

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

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 $\cdot : G \times G \to G$ 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 $+ : G \times G \to G$.

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

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

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 $\varphi : G_1 \to G_2$ mit $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in G$. Wir definieren den *Kern* $\operatorname{Ker}(\varphi) = \varphi^{-1}\{e_{G_2}\} = \{a \in G \mid \varphi(a) = e_{G_2}\}$ und das *Bild* $\operatorname{Im}(\varphi) = \varphi(G_1) = \{b \in G_2 \mid \exists a \in G \text{ mit } \varphi(a) = b\}$. 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 $\iota : H \to G$ 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 $\mathrm{Ker}(\varphi) = (n_0) = \mathbb{Z}n_0$.*

Definition. Falls φ wie im Lemma injektiv ist, so sagen wird, dass a *unendliche Ordnung* hat. Falls $\mathrm{Ker}(\varphi) = (n_0)$ 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 $\gamma_g : G \to G, x \mapsto gxg^{-1}$ ein Automorphismus von G, welche ein innerer Automorphismus *genannt wird.*
b) Die Abbildung $g \in G \mapsto \gamma_g \in \mathrm{Aut}(G)$ 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 ein Gruppe und $g \in G$. Dann ist die Menge der Fixpunkte γ_g gleich dem Zentralisator von g :

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

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 ist 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

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

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 $2, 3, 5, 7, \ldots$.

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 $\varphi : G \to G_1$ mit $H = \mathrm{Ker}(\varphi)$.
(4) Für alle $x, y \in G$ gilt $(xH)(yH) = (xy)H$.
(5) ${}^{G}/_{H}$ ist (auf natürliche Weise) eine Gruppe so dass $\varphi : G \to {}^{G}/_{H}, g \mapsto gH$ 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 $H \lhd G$. Falls $H \lhd G$ 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 $\varphi : G \to H$ eine Homomorphismus zwischen zwei Gruppen G und H. Dann induziert φ einen Isomorphismus $|\varphi| : {}^{G}/_{\mathrm{Ker}(\varphi)} \to \mathrm{Im}(\varphi)$ so dass folgendes Diagramm kommutiert*

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[d, "\pi"'] & & H \\ {}^{G}/_{\mathrm{Ker}(\varphi)} \arrow[r, "\overline{\varphi}"] & \mathrm{Im}(\varphi) < H \arrow[ur, "\iota"'] & \end{tikzcd}$$

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

Korollar (Zweiter Isomorphiesatz). *Sei G eine Gruppe, $H \lhd G$. und $K < G$. Dann gilt $KH = HK < G, H \lhd KH, H \cap K \lhd K$ 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, $H \lhd G$, $K \lhd G$ und $K < H$. Dann ist ${}^{H}/_{K} \lhd {}^{G}/_{K}$ und es gilt*

$$ {}^{{}^{G}/_{K}}/_{{}^{H}/_{K}} \cong {}^{G}/_{H} $$

wobei $(xK)\,{}^{H}/_{K} \mathrel{\widehat{=}} xH$ einander im Isomorphismus entsprechen.

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

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

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

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

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

Übung: Klassifizieren/Beschreiben Sie alle Gruppen der Ordnung ≤ 7 / ≤ 8 / ≤ 10.

3.5 Gruppenwirkungen

Definition. Sei G eine Gruppe und T eine Menge. Eine *Gruppenwirkung* (Linkswirkung, Linksaktion) von G auf T ist eine Abbildung $\cdot : G \times T \to T, (g,t) \mapsto g \cdot t$, 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 $\alpha : G \to \mathrm{Bij}(T), g \in G \mapsto \alpha_g$.

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 $\mathrm{Fix_G}(T) = \{t_0 \in T \mid t_0 \text{ ist ein Fixpunkt}\}$ bezeichnet.
- Für $t_0 \in T$ wird $G \cdot t_0 = \{g \cdot t_0 : g \in G\}$ als die *Bahn (G-Bahn)* bezeichnet.
- Für $t_0 \in T$ heißt $\mathrm{Stab}_G(t_0) = \{g \in G \mid g \cdot t_0 = t_0\}$ der *Stabilisator von t_0*.
- Falls $g \in G \mapsto \alpha_g \in \mathrm{Bij}(T)$ 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 $G \setminus T = \{G \cdot t_0 \mid t_0 \in T\}$ 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 ${}^{G}/_{\sim_G} = G \setminus T$ 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 $f : T_1 \to T_2$ 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 $H = \mathrm{Stab}_G(t_0)$. Dann ist $H < G$, T_0 ist invariant und*

$$f : {}^{G}/_{H} \to T_0, gH \mapsto g \cdot t_0$$

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*

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

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

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

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 $\alpha : G \to S_n$ mit $n = [G : H]$ und $\mathrm{Ker}(\alpha) < H$.

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 $|\mathrm{Fix}_G(T)| \equiv |T| \mod p$.*

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

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_n = G$$

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 $k = 0, \ldots, n-1$) ist.

Proposition. *Sei G eine Gruppe. Dann ist $[G,G] = \langle\{[a,b] \mid a,b \in G\}\rangle \lhd G$, und ${}^{G}/_{[G,G]}$ ist abelsch. Falls H eine abelsche Gruppe ist und $\varphi : G \to H$ ein Homomorphismus ist, so ist $\varphi([G,G]) = \{e_H\}$ und φ induziert einen Gruppenhomomorphismus $\overline{\varphi} : {}^{G}/_{[G,G]} \to H$. 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:*

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

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 $S_n = \mathrm{Bij}(\{1, \ldots, n\})$. Die Elemente von S_n heißen *Permutationen.*

Satz. *Sei $n \geq 1$. Auf S_n gibt es einen Homomorphismus* $\mathrm{sgn} : S_n \to \{\pm 1\}$*, 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 $\mathrm{sgn}(\sigma) = 1$, ungerade falls $\mathrm{sgn}(\sigma) = -1$. Die *alternierende Gruppe* $A_n = \mathrm{Ker}(\mathrm{sgn})$ ist die Gruppe aller geraden Permutationen.

Notation (für $\sigma \in S_n$).

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

Besser:

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

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

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

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

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

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

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

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

In diesem Fall sagen wir auch, dass σ *Zyklentyp*(Struktur) $k_1, k_2, \ldots, k_r$ hat (wobei die Zahlen $k_1, \ldots, k_r$ 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 $\{1, \ldots, n\}$ und folgende Lemmas verwenden.

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

Lemma. *Sei $n \geq 5$ und $H \lhd A_n$ 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 der $n = 60$ 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 einen grundlegende Eigenschaft von Auflösbarkeit.

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

$$\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_k = G$$

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

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

Für den Rest dieses Beweises siehe Algebra 21 und 22

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 $b_1 = (1, 0, \ldots, 0)^T, \ldots, b_n = (0, \ldots, 0, 1)^T$ bezeichnet.

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

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

Konstruktion von F_n : $F_n = \{\text{reduzierte Wörter in } b_1, b_1^{-1}, \ldots, b_n, b_n^{-1}\}$. Eine endliche Liste mit Eintragungen $b_1^{\pm 1}, \ldots, b_n^{\pm 1}$ wird *Wort* genannt. Die leere Liste bezeichnen wir mit e und gilt als reduziert.

Ein Wort w wird *reduziert* genannt falls in w nie direkt ein b_j auf b_j^{-1} oder ein b_j^{-1} auf ein b_j folgt ($b_1 \underbrace{b_2 b_2^{-1}} b_3$ ist nicht reduziert, $b_1 b_2 b_3 b_2^{-1} b_3^{-1}$ ist reduziert).

Durch Löschen von aufeinanderfolgenden b_j & b_j^{-1} oder b_j^{-1} & b_j kann ein Word reduziert werden.

Dadurch kann F_n zu einer Gruppe gemacht werden: Für $w_1, w_2 \in F_n$ hängen wir an w_1 das Wort w_2 an und wenn nötig reduzieren wir $w_1 w_2$ zu einem Element von F_n. - Dies definiert $w_1 \cdot w_2 \in F_n$.

Universelle Eigenschaft beruht auf der Definition

$$\phi(\underbrace{b_{j_1}^{\varepsilon_1} b_{j_2}^{\varepsilon_2} \dots b_{j_k}^{\varepsilon_k}}_{\in F_n}) = a_{j_1}^{\varepsilon_1} \dots a_{j_k}^{\varepsilon_k}.$$

Wir überspringen den formalen Beweis des Satzes.

Definition (Relation)**.** Sei F_n die freie Gruppe mit n Erzeugenden, $W \subseteq F_n$ eine Teilmenge. Sei $N = \langle gwg^{-1} \mid g \in F_n, w \in W \rangle$ der von W erzeugte Normalteiler von F_n. Dann heißt ${}^{F_n}\!/_{N}$ die *Gruppe mit Erzeugenden* $b_1, \dots, b_n$ und Relationen $w \in W$ und wird mit $\langle b_1, \dots, b_n \mid w = e \text{ für } w \in W \rangle$ bezeichnet.

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 $R \times M \to M, (a, m) \mapsto a \cdot m$ 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 $\phi : M \to N$ 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*

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

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

$$\overline{\phi} : {}^{M}/_{\operatorname{Ker}(f)} \to \operatorname{Im}(f).$$

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

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

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*

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

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

Welche Ringe könnten interessant sein?

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

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 $\varphi : M \to M$. 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 $\varphi : M \to M$*
$\cdot$	$\longmapsto$	$\varphi(m) = X \cdot m$ *für* $m \in M$
$f \cdot m = (f(\varphi))(m) = (\sum_k a_k \varphi^k)(m)$ *für* $f = \sum_k a_k X^k \in K[X]$	$\longleftarrow$	φ

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 Ring. Wir bezeichnen

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

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

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

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*

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

wie in der Linearen Algebra.

Definition. Sei M ein R-Modul über einem Ring R. Wir sagen $x_1, \ldots, x_n \in M$ 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 $x_1, \ldots, x_n \in M$ 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

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

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*

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

und n ist der Rang von ${}^{M}/_{M_{\text{tors}}}$. 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 $d_1 \mid d_2 \mid \ldots \mid d_n$ in $R \setminus \{0\}$ so dass*

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

Alternativ gilt

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

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

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

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

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

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

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

4.5 Endlich erzeugte abelsche Gruppen

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

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

wobei $1 \leq s_1 \mid d_2 \mid \ldots \mid d_n \neq 0$ und $k \geq 0$.
Alternativ gilt

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

wobei G_p die Sylow p-Untergruppe ist.

4.6 Jordan-Normalform

Satz. *Sei V ein endlich dimensionaler Vektorraum über $\mathbb{C}$ und $\varphi : V \to V$ 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.

Kapitel 5: Körpertheorie

5.1 Körpererweiterungen

Bemerkung. Ein Ringhomomorphismus $\varphi : K \to L$ von einem Körper zu einem anderen Körper ist immer injektiv

Definition. Sei L ein Körper und $K \subseteq L$ ein Unterring und auch ein Körper. Dann heißt $K \subseteq L$ auch ein *Unterkörper* und L wird eine *Körpererweiterung* von K genannt. Wir schreiben auch $L \mid K$ („L über K“) falls L eine Körpererweiterung von K ist. Da L in diesem Fall ein Vektorraum über K ist, können wir die Dimension von L über K betrachten - diese wir als der *Grad* $[L : K]$ *der Körpererweiterung* $L \mid K$ bezeichnet. Falls $[L : K] < \infty$, so heißt L eine *endliche Körpererweiterung von* K.

Satz (Multiplikativität dere Grade)**.** *Angenommen $F \mid L$ und $L \mid K$ sind (endliche) Körpererweiterungen. Dann gilt $[F : K] = [F : L][L : K]$.*

Definition. Sei $L \mid K$ eine Körpererweiterung, $x \in L$, und $\varphi_x : K[T] \to L, f \mapsto f(x)$ der Auswertungshomomorphismus.

Falls φ_x injektiv ist, so heißt x *transzendent* über K

Falls φ_x nicht injektiv ist, so heißt x *algebraisch* über K. In diesem Fall ist $\mathrm{Ker}(\varphi_x) = (m_x(T))$ & $m_x(T)$ heißt das *Minimalpolynom von* X, der Grad von $m_x(T)$ ist auch der *Grad von* X.

Proposition. *Sei $L \mid K$ und $x \in L$. Falls x transzendent ist, so ist*

$$K[X] = \mathrm{Im}(\varphi_x) \cong K[T].$$

und der kleinste Unterkörper $K(X)$ von L, der sowohl K als auch x enthält ist, erfüllt

$$K(X) \cong K(T)$$

mit $K(T)$ der Körper der rationalen Funktionen.

Falls x algebraisch ist, so ist

$$K[X] = \mathrm{Im}(\varphi_x) \cong {}^{K[T]}/_{(m_x(T))}$$

bereits der kleinste Unterkörper $K(X)$, der sowohl K als auch e enthält. Es gilt

$$[K(x) : K] = \deg(m_x(T)).$$

Definition. Sei $L \mid K$ und $x_1, \ldots, x_n \in L$. Dann bezeichnen wir den kleinsten Unterkörper der sowohl K als auch $x_1, \ldots, x_n$ enthält mit

$$K(x_1, \ldots, x_n) = \{\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} \mid f, g \in K[T_1, \ldots, T_n], g(x_1, \ldots, x_n) \neq 0\}.$$

Korollar (Wantzel, 1837)**.** *Mit Zirkel und Linear lassen sich weder $\sqrt[3]{2}$ noch ein Winkel von 29° konstruieren. Des Weiteren gilt: Falls $p > 2$ eine Primzahl ist und das regelmäßige p-Ecke mit Zirkel und Lineal konstruierbar ist, so ist p eine Fermat-Primzahl ($p - 1 = 2^{2^n}$).*

Definition. Eine Körpererweiterung $L \mid K$ heißt *algebraisch* falls jedes $x \in L$ algebraisch über K ist.

Lemma. *Eine endliche Körpererweiterung ist algebraisch.*

Korollar. *Sei $L \mid K$ und $x, y \in L$ algebraisch über K. Dann sind auch $x + y, x \cdot y, x - y, \frac{1}{x}$ für $x \neq 0$ algebraisch über K.*

Korollar. *Angenommen $F \mid L$ und $L \mid K$. Dann ist $F \mid K$* ist algebraisch *genau dann wenn $F \mid L$* algebraish ist und $L \mid K$ algebraisch ist.

5.2 Zerfällungskörper

Satz (Kronecker)**.** *Sei K ein Körper, $f \in K[T]$ mit $n = \deg(f) > 0$. Dann existiert eine Körpererweiterung L von K, so dass*

$$f(T) = a \prod_{i=1}^{n} (T - \alpha_i),$$

$a \in k$, $\alpha_1, \dots, \alpha_n \in L$.

Definition. Sei K ein Körper, $f \in K[T]$ mit $\deg(f) > 0$. Ein *Zerfällungskörper von f über K* ist eine Körpererweiterung $L \mid K$ so dass

1) f zerfällt (in Linearfaktoren) in $L[i]$.
2) Falls $K \subseteq E \subsetneq L$, dann zerfällt f über E nicht.

Bemerkung.
- Ein Zerfällungskörper existiert immer (und ist bis auf Isomorphie eindeutig). Falls $f \in K[T]$ und $F \mid K$ eine Körpererweiterung, so dass f in $F[T]$ zerfällt (Kronecker) mit Nullstellen $\alpha_1, \dots, \alpha_n \in F$ so ist $L := K(\alpha_1, \dots, \alpha_n)$ ein Zerfällungskörper.
- Ein Zerfällungskörper ist eine algebraische Körpererweiterung von K.

Bemerkung. Sei K ein Körper, $f \in K[T]$ und L ein Zerfällungskörper von f über K, dann gilt

$$[L : K] \leq (\deg(f))!.$$

Ist f über K irreduzibel, so gilt $[L : K] \geq \deg(f)$.

- $T^3 - 2$ irreduzibel über $\mathbb{Q}$ mit Grad 6.
- $T^2 + 1$ irreduzibel über $\mathbb{Q}$ mit Grad 2.
- $T^3 - 2$ nicht irreduzibel über $\mathbb{R}$ und hat Zerfällungskörper mit Grad 2.

5.3 Algebraischer Abschluss

Definition. Sei K ein Körper. K ist *algebraisch abgeschlossen*, falls jedes Polynom $f \in K[T]$ mindestens eine Nullstelle in K hat.

Es folgt (Induktion), dass f über K zerfällt.

Bemerkung. Ein algebraisch abgeschlossener Körper hat unendlich viele Elemente.

Proposition. *Sei $L \mid K$ eine Körpererweiterung und L algebraisch abgeschlossen. Dann ist*

$$E = \{x \in L \mid x \text{ ist algebraisch über } K\}$$

eine algebraisch abgeschlossene algebraische Körpererweiterung von K.

Definition. Wir nennen E wie in der Proposition den *algebraischen Abgschluss* $\overline{K}$ von K

Bemerkung.
- K endlich $\Rightarrow \overline{K}$ ist abzählbar
- K abzählbar $\Rightarrow \overline{K}$ ist abzählbar [Bsp: $\mathbb{Q}, \overline{\mathbb{Q}} = \mathbb{Q}_{\text{alg}} = \{z \in \mathbb{C} \mid z \text{ alg. über } \mathbb{Q}\}$ genannt algebraische Zahlen]

Satz. *Sei K ein Körper, dann existiert eine Körpererweiterung $L \mid K$ mit L algebraisch abgeschlossen (L ist bis auf Isomorphie eindeutig).*

5.4 Eindeutigkeit

(Seite 343, Teile auch Seite 88)

Wir haben gesehen:

- Für jedes $f \in K[T]$ gibt es einen Zerfällungskörper.
- Es gibt einen algebraischen Abschluss.

Sind diese (bis auf Isomorphie) eindeutig?

Satz. *Sei K ein Körper, $L \mid K$ eine Körpererweiterung und L algebraisch abgeschlossen.*

1. *Falls $E = K[\alpha]$ eine endliche Körpererweiterung von K ist, so gibt es mindestens eine und höchstens $[E : K]$ Körpereinbettungen $\sigma : E \to L$ mit $\underbrace{\sigma |_K = \mathrm{id}_K}_{\sigma\ K\text{-linear}}$. Falls $\mathrm{char}(K) = 0$, so gibt es genau $[E : K]$ derartige Einbettungen.*
2. *Falls $E \mid K$ eine algebraische Körpererweiterung ist, so gibt es eine K-lineare Körpereinbettung $\sigma : E \to L$.*

Lemma. *Sei K eine Körper, $m(T) \in K[T]$ coprim zu $m'(T)$. Dann hat m in einer algebraisch abgeschlossenen Körpererweiterung genau $\deg(m(T))$ viele einfache Nullstellen.*

Dies gilt z.B. wenn $\mathrm{char}(K) = 0$ und $m(T)$ irreduzibel in $K[T]$ ist.

Bemerkung. Für $K = \mathbb{F}_p$ und $m(T) = T^p$ gilt $m'(T) = 0$ und daher nicht $\deg(m'(T)) = \deg(m(T)) - 1$.

Korollar. *Sei K ein Körper*

1) *Für jedes $f \in K[T]$ ist die Zerfällungskörper bis auf einen K-linearen Körperisomorphismus eindeutig bestimmt.*
2) *Je zwei algebraische Abschlüsse von K sind K-linear isomorph.*

5.5 Endliche Körper

$\mathbb{F}_p = {}^{\mathbb{Z}}/_{(p)}$ für $p \in \mathbb{N}$ prim ist ein endlicher Körper.
Gibt es weitere? Können wir diese klassifizieren?

Satz (Gauss, Galois)**.**
1. *Falls K ein endlicher Körper ist, so ist $|K| = p^n$ für eine Primzahl $p \in \mathbb{N}$ und ein $n \geq 1$.*
2. *Für jede Primzahlpotenz p^n gibt es einen bis auf Isomorphie eindeutig bestimmten Körper mit p^n Elementen.*
3. *Sei $p \in \mathbb{N}$ prim und K ein algebraischer Abschluss von $\mathbb{F}_p$. Dann enthält K einen eindeutig bestimmten Unterkörper $\mathbb{F}_{p^n}$ mit p^n Elementen.*

$$\mathbb{F}_{p^n} = \{x \in K \mid x^{(p^n) = x}\}.$$

4. *Für* $m, n \geq 1$ *und die Körper wie in* 3) *gilt*

$$F^{p^m} \subseteq F^{p^n} \Leftrightarrow m \mid n.$$

Satz. *Sei* K *ein Körper und* $G \subseteq K^\times$ *eine endliche Untergruppe. Dann ist* G *zyklisch. Insbesondere ist* $\mathbb{F}_{p^n}^\times$ *zyklisch für jede Primzahlpotenz* p^n.

Korollar. *Sei* $p > 2$ *eine Primzahl. Für* $a \in \mathbb{F}_p$ *gilt*

$$a^{\frac{p-1}{2}} = \begin{cases} 0 & \textit{falls } a = 0 \\ 1 & \textit{falls } a = b^2 \textit{ für ein } b \in \mathbb{F}_p^\times \\ -1 & \textit{sonst} \end{cases}$$

Kapitel 6: Galois Theorie

6.1 Einleitung

Das motivierende Problem der Galois Theorie ist folgendes: Finde eine „Formel“ für die Lösungen der Gleichung $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ in Funktion von den Koeffizienten $a_0, \ldots, a_{n-1}$.

Methoden für den linearen und quadratischen Fall waren schon babylonischen Mathematikern bekannt. $\sim$ 1700 B.C.
Euklid ($\sim$ 300 B.C.) hat die Lösung von Quadratischen Gleichungen auf geometrische Probleme zurückgeführt.
al-Khwarizmi $(780 - 850)$: Systematische Behandlung von linearen und quadratischen Gleichungen.
16. Jh: Gleichung 3. Grades: Seipione del Ferro 1515. 4.Grades: Ludovico Ferrarr.

Cardano „Ars Magna“ 1545: Cardano's Formeln für 3. Grad. Sei $x^3 + ax^2 + bx + c = 0$. Durch die Substitution $z = x - \frac{a}{3}$ erhält man eine Gleichung der Form: $z^3 + pz + q = 0$.

Idee: $z = y + u$ wobei man später u geeignet wählen kann. Durch Substitution in $z^3 + pz + q = 0$ erhalten wir:

$$y^3 + \underbrace{2y^2u + 3yu^2}_{3yu(y+u)} + u^3 + p(y+u) + q = 0$$

und erhalten $y^3 + (y+u)(3yu + p) + u^3 + q = 0$. Setze $3yu + p = 0$ also $u = -\frac{p}{3y}$.

$$y^4 - \frac{p^3}{27y^3} + q = 0 \Rightarrow y^6 + py^3 - (\frac{p}{3})^3 = 0 \quad \text{(Resolvente)}.$$

Diese Gleichung ist quadratisch in y^3:

$$y^3 = \frac{-q \pm \sqrt{q^2 + 4(\frac{p}{3})^3}}{2}.$$

und bekommt für z die Formel:

$$z = \sqrt[3]{-\frac{p}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{p}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

Wesentlicher Schritt: Lagrange (1736-1813): Falls z_1, z_2, z_3 Lösungen von $z^3 + pz + q = 0$ sind. Sind $w = e^{\frac{2}{3}\pi i}$ primitive 3. Wurzeln von 1. Dann sind die 6 Lösungen der Resolvente $y^6 + qy^3 - \left(\frac{p}{3}\right)^3 = 0$ sind gegeben durch

$$y_\sigma := \frac{1}{3}\left(z_{\sigma(1)} + wz_{\sigma(2)} + w^2 z_{\sigma(3)}\right)$$

wobei σ die Menge der Permutationen über 3 Elemente durch läuft.

Fundamentale Einsicht: $\left(z_{\sigma(1)} + wz_{\sigma(2)} + w^2 z_{\sigma(3)}\right)^3$ nimmt nur 2 Werte an.

Paolo Raffini: Zeige dass die allgemeine Gleichung 5. Grades keine „Lösung“ besitzt. Rationale Funktionen $f(z_1, \ldots, z_5)$ wobei $z_1, \ldots, z_5$ Wurzeln der Gleichung $z_5 + \ldots + a_0 = 0$ sind. Hat realisiert, dass die Menge der $\sigma \in S_5$ für welche $f(z_1, \ldots, z_5) = f(z_{\sigma(1)}, \ldots, z_{\sigma(5)})$ ist eine *Untergruppe* von S_5.

Untergruppen von S_5 klassifiziert. Niels Abels (1812-1829)

Satz (Abels-Raffini)**.** *Die allgemeine Gleichung* 5*. Grades* $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$ *ist mittels Radikalen nicht auflösbar.*

Eine Lösung mittels Radikalen ist eine *Formel* die endlich viele arithmetische Operationen und Wurzelziehen der Koeffizienten zulässt.

Galois Theorie und Thm. Die alternierende Gruppe A_5 ist nicht abelsch und einfach.

Wir werden jedem Polynom $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K[x]$, K Körper ordnen wir eine Gruppe $\mathrm{Gal}(f) < S_n$.

Satz. *Falls* K *gute Eigenschaften besitzt (z.B.* $\mathrm{char} = 0$*)* $f(x) = 0$ *ist genau dann Mittels Radikalen Lösbar falls* $\mathrm{Gal}(f)$ auflösbar*.*

6.2 Galois Gruppe einer Körpererweiterung: grundlegende Eigenschaften und Beispiele

Sei E ein Körper. Die Menge $\mathrm{Aut}(E) = \{\sigma : E \to E \mid \sigma \text{ ist eine Körperisomorphismus}\}$ ist für die Operation der Verkettung von Abbildungen eine Gruppe.

Sei $K \subseteq E$ eine Unterkörper; E ist eine Körpererweiterung von K.

$$\mathrm{Gal}(E/K) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma(x) = x \ \forall x \in K\}$$

ist eine Untergruppe von $\mathrm{Aut}(E)$.

Definition. $\mathrm{Gal}(E/K)$ ist eine Galoisgruppe der Erweiterung E/K.

Aus der Algebra I wissen wir, dass E ein K-Vektorraum ist.

Übung: Jedes $\sigma \in \mathrm{Gal}(E/K)$ ist ein Isomorphismus des K-Vektorraums E.

Übung: Sei $K = \mathbb{R}$ und $E = \mathbb{C}$ dann ist $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \sigma\}$ wobei $\sigma(x+iy) = x-iy, x, y \in \mathbb{R}$. Wie *groß* ist $\mathrm{Aut}(\mathbb{C})$.

Sei $f \in K[x]$ ein Polynom und E/K eine Körpererweiterung so dass in $E[x] f$ Produkt von linearen Faktoren ist. Sei $R(f) \subseteq E$ die Menge der Nullstellen von f.

Lemma. *Jedes* $\sigma \in \mathrm{Gal}(E/K)$ *induziert eine Permutation der Menge* $R(f)$ *der Nullstellen von* f*.*

Sei $f \in K[X]$.

Definition. Die Galois Gruppe $\mathrm{Gal}(f)$ von f ist die Galois Gruppe $\mathrm{Gal}(E/K)$ wobei E/K ein Zerfällungskörper von f bezeichnet.

Existenz: Kronecker + Eindeutigkeit bis auf Isomorphismus siehe Algebra I

Übung: Zeige dass falls E/K und E'/K Zerfällungskörper von f bezeichnen, die Gruppen $\mathrm{Gal}(E/K)$ und $\mathrm{Gal}(E'/K)$ isomorph sind.

Notation. Sei X eine Menge. Wir bezeichnen mit S_X die Gruppe aller Bijektionen (Permutationen) von $X \to X$. Falls $X = \{1, 2, \ldots, n\}$ dann setzen wir $S_X = S_n$.

Lemma. *Sei* E/K *Zerfällungskörper eines Polynoms* $f \in K[X]$ *und* $R(f) \subseteq E$ *die Menge der Nullstellen. Dann ist die Restriktionsabbildung*

$$\begin{aligned} \mathrm{Gal}(E/K) &\to S_{R(f)} \\ \sigma &\mapsto \sigma \mid_{R(f)} \end{aligned}$$

ist eine injektiver *Gruppenhomomorphismus.*

Sei E/K eine Körpererweiterung, $\alpha \in E$. Dann ist $K[\alpha] :=$ Bild des Evaluationshomomorphismus $\begin{matrix} K[X] \to E] \\ P \mapsto P(\alpha) \end{matrix}$ Da E Körper ist $K[X]$ ein Integritätsbereich und $K(X)$ der Quotientenkörper von $K[\alpha]$.

Im allgemeinen ist $|R(f)| \leq \deg(f)$.

Ziel: $f \in K[X]$ irreduzibles Polynom mit $|R(f)| = \deg(f)$ dann ist $|\mathrm{Gal}(E/K)| = [E : K]$.

Definition. Ein Polynom $f \in K[X]$ hat keine mehrfachen Nullstellen falls in einem Zerfällungskörper $|R(f)| = \deg(f)$.

Lemma (Übung)**.** *Sei $f \in K[X]$ und $f' \in K[X]$ die (formelle) Ableitung von f. f hat keine mehrfachen Nullstellen genau dann wenn* $\mathrm{ggT}(f, f') = 1$.

Bemerkung. Gegeben $f, g \in K[X]$, der euklidische Algorithmus berechnet $\mathrm{ggT}(f, g)$.

Korollar. *Sei $f \in K[X]$ irreduzibel und sei eine der folgenden Voraussetzungen erfüllt:*

(1) $\mathrm{char}(K) = 0$

(2) Falls $\mathrm{char}(K) > 0$ *dann teilt* $\mathrm{char}(K)$ *nicht* $d = \deg(f)$.

Dann hat f keine mehrfachen Nullstellen.

Definition. (1) Ein irreduzibles Polynom ist *separabel* falls es keine mehrfachen Nullstellen besitzt.

(2) Ein Polynom ist *separabel* falls alle seiner irreduziblen Faktoren separabel sind.

Definition (Wiederholung)**.** Sei E/K eine Körpererweiterung und $\alpha \in E$: $\begin{matrix} \varphi_\alpha : K[X] \to E \\ P \mapsto P(\alpha) \end{matrix}$ ist ein Ringhomomorphismus. Sei $\mathrm{Ker}(\varphi_\alpha)$ sein Kern, dann ist $\mathrm{Ker}(\varphi_\alpha)$ ist ein Ideal in $K[X]$. Zwei Möglichkeiten

(1) $\mathrm{Ker}(\varphi_\alpha) = (0)$ dann heißt α transzendent über K.

(2) $\mathrm{Ker}(\varphi_\alpha) \neq (0)$ dann ist α algebraisch. Da $K[X]$ ein Hauptidealring ist gibt es genau ein unitäres Polynom $\mathrm{irr}(\alpha, K)$, das Minimalpolynom von α über K, das $\mathrm{Ker}(\varphi_\alpha)$ erzeugt: $\mathrm{Ker}(\varphi_\alpha) = \mathrm{irr}(\alpha, K) \cdot K[X]$.

Aus der Tatsache, dass $\mathrm{irr}(\alpha, K)$ irreduzibel ist und $K[X]$ ein euklidischer Ring folgt $K[X]/\mathrm{Ker}(\varphi_\alpha)$ ist ein Körper und

Lemma. *φ_α induziert einen Körperisomorphismus* $\overline{\varphi_\alpha} : K[X]/\mathrm{Ker}(\varphi_\alpha) \xrightarrow{\sim} K(\alpha)(= K[\alpha])$

Sei $\varphi : K \to K'$ ein Körperisomorphismus; dieser induziert einen Ring Isomorphismus $\varphi_* : K[X] \to K'[X]$ mit

$$\varphi_*(a_n X^n + \ldots + a_0) := \varphi_*(a_n) X^n + \ldots + \varphi_*(a_0).$$

Da φ_* ein Ringisomorphismus ist folgt $p \in K[X]$ ist genau dann irreduzibel, falls $\varphi_*(p)$ irreduzibel ist. Bemerke: $\deg(\varphi_*(p)) = \deg(p)$.

Lemma. *Sei $p \in K[X]$ irreduzibel, $p_* = \varphi_*(p) \in K'[X]$; seien $E \supseteq K$ und $E' \supseteq K'$ mit $R(p) \subseteq E$ und $R(p_*) \subseteq E'$. Dann gilt: $\forall \alpha \in R(p)$ $\forall \alpha' \in R(p_*)$ gibt es einen Isomorphismus $\widehat{\varphi} : K(\alpha) \to K'(\alpha')$ der φ erweitert und $\widehat{\varphi}(\alpha) = \alpha'$*

$$\begin{tikzcd} K \arrow[r, "\varphi"] \arrow[d, hook] & K' \arrow[d, hook] \\ K(\alpha) \arrow[r, "\widehat{\varphi}"'] & K'(\alpha') \end{tikzcd} .$$

Satz. *Sei $\varphi : K \to K'$ ein Isomorphismus, $f \in K[X]$, $f_* = \varphi_*(f)$. Sei E/K ein Zerfällungskörper von f und E_* ein Zerfällungskörper von f_*.*

(1) Annahme f ist separabel. Dann gibt es genau $[E : K]$ Isomorphismen

$$\begin{tikzcd} E \arrow[r, "\Phi"] & E_* \\ K \arrow[u, hook] \arrow[r, "\varphi"] & K' \arrow[u, hook] \end{tikzcd}$$

die φ erweitern, d.h. $\Phi\mid_K = \varphi$

(2) Sei E/K Zerfällungskörper eines separablen Polynoms dann ist $|\mathrm{Gal}(E/K)| = [E : K]$

Korollar. *Sei E/K ein Zerfällungskörper eines separablen Polynom $f \in K[X]$ von $\deg(f) = n$. Falls f irreduzibel folgt: n dividiert $|\mathrm{Gal}(E/K)|$.*

Satz. *Sei p eine Primzahl, $n \in \mathbb{N}, n \geq 1$. Dann ist $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ ein erzeugendes Element ist gegeben durch $Fr : \begin{matrix} \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \\ x \mapsto x^p \end{matrix}$*

Satz. *Sei p eine Primzahl und $f \in \mathbb{Q}[X]$ mit $\deg(f) = p$ und Zerfällungskörper E. Annahme:*

1. *f ist irreduzibel*
2. *f hat genau $p - 2$ reelle Nullstellen.*

Dann ist $\mathrm{Gal}(E/\mathbb{Q}) \cong S_p$.

Korollar. *p dividiert die Ordnung von $\mathrm{Gal}(E/\mathbb{Q})$.*

Lemma (Cauchy)**.** *Sei G eine endliche Gruppe und p eine Primzahl die die Ordnung von G dividiert. Dann enthält G eine Element der Ordnung p.*

Korollar. *Die Galois Gruppe von $X^5 - 4x + 2 \in \mathbb{Q}[X]$ ist $\cong S_5$.*

6.2.1 Zusammenhang zwischen Irreduzibilität und Transitivität der Galois Gruppe

Korollar. *Sei $f \in K[X]$ und E ein Zerfällungskörper von f. Dann gilt: f irreduzibel $\Leftrightarrow$ $\mathrm{Gal}(E/K)$ wirkt transitiv auf $R(f)$.*

Sei $G \times X \to X$ eine Gruppenwirkung. Die Wirkung ist *transitiv* falls $\forall x, y \in X \ \exists g \in G : g(x) = y$.

Behauptung. $\Rightarrow$: Gilt auch ohne Voraussetzung an die Nullstellen von f.

Definition. Eine Erweiterung E/K heißt normal falls sie Zerfällungskörper eines Polynoms $f \in K[X]$ ist.

Behauptung. Seien $K \subseteq B \subseteq E$ Körpererweiterungen. Falls E/K normal ist so folgt, dass E/B auch normal ist.

Satz. *Seien $K \subseteq B \subseteq E$ (endliche) Erweiterungen mit der der Eigenschaft, dass sowohl E/K wie B/K normale Erweiterungen sind. Dann folgt $\forall \sigma \in \mathrm{Gal}(E/K)$ ist $\sigma(B) = B$.*

Und der Homomorphismus $\begin{matrix} \mathrm{Gal}(E/K) \to \mathrm{Gal}(B/K) \\ \sigma \mapsto \sigma\mid_B \end{matrix}$ *ist surjektiv mit Kern $\mathrm{Gal}(E/B)$.*

Satz. *Eine endliche Erweiterung E/K ist genau dann normal falls jedes irreduzible Polynom in $K[X]$, dass eine Nullstelle in E besitzt, in linear Faktoren in E zerfällt.*

Kapitel 7: Lösung durch Radikale und auflösbare Gruppen

Sei $K = k(u)$ eine Körpererweiterung von k, $u \neq 0$. Dann ist $\{n \in \mathbb{Z} \mid u^n \in k\}$ ist eine Untergruppe von $\mathbb{Z}$ und deshalb von der Form $m\mathbb{Z}$ wobei $m \in \mathbb{N}$ eindeutig bestimmt.

Definition. $k(u)/k$ ist eine reine Erweiterung vom Typ m falls $m\mathbb{Z} = \{n \in \mathbb{Z} \mid u^n \in k\} \neq 0$

Definition. Eine Körpererweiterung K/k heißt radikal falls es einen Turm von Zwischenkörpern gibt

$$k = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_t = K$$

so dass $K_{i+1}/K_i \; \forall 0 \leq i \leq t-1$ reine Erweiterungen sind.

Definition. Ein Polynom $f \in k[x]$ ist mittels *redikalen Lösbar* falls ein Zerfällungskörper von f in einer radikalen Erweiterung von k enthalten ist.

$k(u)/k : u^m \in k$ u ist m-te Wurzel von einem Element in k. Sei E der Zerfällungskörper von f.

Sei $k(u)/k$ eine reine Erweiterung von Typ $m \geq 1$. Sei $m = p_1 \cdot \ldots \cdot p_r$ eine Zerlegung in Primzahlen.

$$k(u) \supseteq k(u^{p_1}) \supseteq k(u^{p_1 p_2} \supseteq \ldots \supseteq k(u^m) = k$$

wobei die erste Erweiterung von Typ p_1, die zweite von Typ p_2 etc. ist. Dies Führt zum Studium von $x^p - c \in k[x]$.

Lemma. *Sei p ein Primzahl. Sei $f(x) = x^p - c \in k[x]$.*

(1) Folgende Dichotomie:
- *(1.1) (f) ist irreduzibel*
- *(1.2) c ist eine p-te Potenz eines Elements in k*

(2) Sei E/k der Zerfällungskörper von f. Wir nehmen an, k enthält alle p-ten Wurzeln von 1. Sei $u \in E, u \in R(f)$. Dann ist $E = k(u)$.
- *(2.1) f irreduzibel:*
  - *Falls $\mathrm{char}(k) \neq p$ ist $\mathrm{Gal}(E/k) \cong \mathbb{Z}/p\mathbb{Z}$*
  - *Falls $\mathrm{char}(k) = p$ ist $\mathrm{Gal}(E/k) \cong e$.*
- *(2.2) f reduzibel so ist $E = k$ und $\mathrm{Gal}(E/k) \cong (e)$.*

Sei $f \in k[x]$. $k \subseteq E \subseteq K$ mit E Zerfällungskörper, K Radikale Erweiterung. In Verbindung bringen mit Galois Gruppe. Wir wollen zeigen, dass jede radikale Erweiterung K/k in einer normalen radikalen Erweiterung F enthalten ist.

$$k \subseteq E \subseteq K \subseteq F$$

normal und Radikal. Aus Satz 2.26 folgt $\begin{array}{c}\mathrm{Gal}(F/k) \to \mathrm{Gal}(E/k) \\ \sigma \mapsto \sigma\,|_E\end{array}$ surjektiv. Falls wir zeigen, dass $\mathrm{Gal}(F/k)$ von $\frac{f}{k}$ normal radikal auflösbar ist. Dann folgt, dass $\mathrm{Gal}(E/k)$ auflösbar ist. In Algebra I hatten wir den Satz

Satz. *Jede Untergruppe und jeder Quotient einer auflösbaren Gruppe ist auflösbar.*

Kontext folgender zwei Lemmata: Sei $B = k(u_1, \ldots, u_t)$ eine endliche Erweiterung von k. Insbesondere sind $u_1, \ldots, u_t$ algebraisch über k. Sei $p_i = \mathrm{irr}(u_i, k) \in k[x]$ das Minimalpolynom von u_i über k. Sei $f = p_1 \ldots p_t \in k[x]$. Sei E Zerfällungskörper von f und $G = \mathrm{Gal}(E/k) = \{\sigma_1, \ldots, \sigma_l\}$.

Lemma. $E = k(\sigma(u_1), \dots, \sigma(u_t), \sigma \in G) = k \begin{pmatrix} \sigma_1(u_1), & \dots, & \sigma_l(u_1) \\ \vdots & & \vdots \\ \sigma_1(u_t), & \dots, & \sigma_l(u_t) \end{pmatrix}$

Lemma. *Im Kontext von Lemma 3.6 nehmen wir an, dass:* $u_1^{m_1} \in k, u_2^{m_2} \in k(u_1), \dots, u_t^{m_t} \in k(u_1, \dots, u_{t-1})$. *Dann ist E/k eine radikale Erweiterung.*

Korollar. *Sei K/k eine radikale Erweiterung. Dann gibt es $k \subseteq K \subseteq F, F/k$ radikal und normal.*

Definition (Algebra I)**.** Eine Gruppe G ist auflösbar falls es eine subnormale Folge

$$\{e\} = G_0 \lhd G_1 \lhd g_2 \lhd \dots \lhd G_t = G$$

gibt mit ${}^{G_{i+1}}/{}_{G_i}$ abelsch $0 \leq i \leq t-1$.

Es gibt ein Kriterium für Auflösbarkeit, dass iterierte Kommutatorunterguppen benützt. Für eine Gruppe G bezeichnet $[G, G]$ die von $\{[a, b] \mid a, b \in G\}$ erzeugte Untergruppe. Hier ist $[a, b] = aba^{-1}b^{-1}$. Die Untergruppe $[G, G]$ ist *charakteristisch* d.h. $\forall \alpha \in \mathrm{Aut}(G)$ ist $\alpha([G, G]) = [G, G]$.

Wir führen folgende Notation ein $G^{(1)} = [G, G] =$ Kommutatorgruppe, $G^{(j)} = [G^{(j-1)}, G^{(j-1)}]$.

Proposition. *G ist genau dann auflösbar falls es n gibt mit $G^{(n)} = (e)$.*

Proposition. *(1) $H < G : G$ auflösbar $\Rightarrow H$ auflösbar.*
(2) $N \lhd G : G$ ist gdw. auflösbar falls N und ${}^{G}/{}_{N}$ auflösbar ist.

Satz. *Sei $f \in k[X]$, E ein Zerfällungskörper von f. Falls f mittels Radikalen lösbar ist, folgt, dass* $\mathrm{Gal}(E/k)$ *auflösbar ist.*

Lemma. *Sei $k = K_0 \subseteq K_1 \subseteq \dots \subseteq K_t$ ein Turm von Erweiterungen wobei*
(1) K_t/k normale Erweiterung
(2) K_i ist eine reine Erweiterung von Primzahlen p_i mit $1 \leq i \leq t$.
(3) k enthält alle p_i-ten Wurzeln von 1, $1 \leq i \leq t$.
Dann ist $\mathrm{Gal}(K_t/k)$ *auflösbar.*

Korollar (Abels-Ruffini)**.** *Für $n \geq 5$ ist das „allgemeine Polynom“*

$$f(x) = \prod_{i=1}^{n}(X - y_i)$$

mittels Radikalen nicht lösbar.

Korollar. *$f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ ist nicht mittels Radikalen lösbar, da* $\mathrm{Gal}(f) \cong S_5$.

Sei R ein angeordneter Körper mit

1. jedes $x \geq 0$ ist ein Quadrat
2. jedes $P \in R[X]$ mit $\deg(P)$ ungerade hat eine Nullstelle in R

dann ist $R(\sqrt{-1})$ algebraisch abgeschlossen.

Kapitel 8: Galois Korrespondenz

Definition. Sei E ein Körper und $H \subseteq \mathrm{Aut}(E)$ dann ist $E^H := \{x \in E \mid \sigma(x) = x \ \forall \sigma \in H\}$ ist ein Unterkörper von E. Dann ist E^H der *Fixkörper* von H.

Bemerkung. Die Korrespondenz $H \mapsto E^H$ hat folgende Monotonie Eigenschaft: $H_1 \subseteq H_2 \Rightarrow E^{H_2} \subseteq E^{H_1}$.

Ziel: Bestimmung des Grades $[E : E^H]$ wobei $H < \mathrm{Aut}(E)$ eine *endliche Untergruppe* bezeichnet.

Definition. Sei G eine Gruppe, E ein Körper. Ein *Charakter von G in E* ist ein Gruppenhomomorphismus $G \to E^\times$. Wobei $E^\times$ die Multiplikative Gruppe $E \setminus \{0\}$ ist.

Die Menge der Charaktere von G in E wird mit $\mathrm{Hom}(G, E^\times)$ bezeichnet. Man kann $H(G, E^\times)$ als Teilmenge des Vektorraums $F(G, E)$ aller E-wertigen Funktionen auf G.

Proposition (Dedekind)**.** $\mathrm{Hom}(G, E^\times) \subseteq F(G, E)$ *ist linear unabhängig.*

Benutze diesen Satz um eine untere Schranke von $[E : E^H]$ zu bestimmen falls $H \subseteq \mathrm{Aut}(E)$ eine *endliche Teilmenge* besitzt.

Lemma (Sublemma)**.** *Sei E ein Körper, S eine Menge und $\{\sigma_1, \dots, \sigma_n\} \subseteq G(S, E)$ linear unabhängig. Dann gibt es $s_1, \dots, s_n \in S$ mit*

$$\begin{pmatrix} \sigma_1(s_1) \\ \vdots \\ \sigma_n(s_1) \end{pmatrix}, \dots, \begin{pmatrix} \sigma_1(s_n) \\ \vdots \\ \sigma_n(s_n) \end{pmatrix}$$

in E^n linear unabhängig sind.

Lemma. *Sei $H = \{\sigma_1, \dots, \sigma_n\} \subseteq \mathrm{Aut}(E)$, Teilmenge mit n Elementen. Dann gilt $[E : E^H] \geq n$.*

Behauptung. Falls $\langle H \rangle$ die von H erzeugte Untergruppe von $\mathrm{Aut}(E)$ bezeichnet so ist $E^H = E^{\langle H \rangle}$.

Proposition. *Sei $G < \mathrm{Aut}(E)$ eine endliche Untergruppe. Dann gilt $[E : E^G] = |G|$.*

Korollar. *Seien G, H endliche Untergruppen von $\mathrm{Aut}(E)$. Dann gilt $E^G \subseteq E^H \Leftrightarrow H < G$.*

Korollar. *Seien G, H endliche Untergruppen von $\mathrm{Aut}(E)$. Dann ist $E^G = E^H \Leftrightarrow H = G$.*

Definition (Wiederholung)**.**
- Ein irreduzibles Polynom ist separabel, falls es keine mehrfachen Nullstellen besitzt.
- Ein Polynom ist separabel falls jeder seiner irreduziblen Faktoren separabel ist.

Zwei wichtige Resultate:

- Falls E/k Zerfällungskörper eines separablen Polynoms $f \in k[x]$ ist, dann ist $[E : k] = |\mathrm{Gal}(E/k)|$.
- Ist $G \subseteq \mathrm{Aut}(E)$ eine endliche Untergruppe, wobei E beliebiger Körper, dann ist $[E : E^G] = |G|$.

Satz. *Sei E/k eine endliche Erweiterung mit Galois Gruppe $G = \mathrm{Gal}(E/k)$. Folgende Eigenschaften sind äquivalent:*

(1) E ist Zerfällungskörper eines separablen Polynoms in $k[x]$.
(2) $k = E^G$.
(3) Jedes irreduzible Polynom in $k[x]$ mit einer Nullstelle in E ist separabel und zerfällt in E.

Definition. Eine endliche Erweiterung E/k ist eine *Galoiserweiterung von k*, falls E die äquivalenten Eigenschaften von vorherigem Theorem 4.11 besitzt.

$k \subseteq B \subseteq E$. Falls E/k Galois ist, dass muss B/k nicht unbedingt Galois sein, weil eine Galois Erweiterung insbesondere normal ist. Andererseits sei $f \in k[x]$ separabel mit Zerfällungskörper E, dann ist $f \in B[x]$ immer noch separabel und folglich ist E/B Galois.

Korollar. *Falls $k \subseteq B \subseteq E$ wobei E/k Galois dann ist E/B Galois.*

Proposition. *Sei $k \subseteq B \subseteq E$ mit E/k Galois. Dann ist B/k Galois genau dann, wenn $\sigma(B) = B\ \forall \sigma \in \mathrm{Gal}(E/k)$.*

Definition. Sei G eine Gruppe, dann bezeichnet $\mathrm{Sub}(G)$ die Menge der Untergruppen von G, geordnet via Inklusion. Sei E/k Körpererweiterung. Dann bezeichnet $\mathrm{Int}(E/k)$ die Menge der Zwischenkörper von E/k d.h. Körpererweiterungen B/k mit $B \subseteq E$. Auch $\mathrm{Int}(E/k)$ ist geordnet via Inklusion.

Satz (Galois Korrespondenz)**.** *Sei E/k eine (endliche) Galois Erweiterung.*

(1) Die Abbildung $\gamma : \begin{array}{c} \mathrm{Sub}(\mathrm{Gal}(E/k)) \to \mathrm{Int}(E/k) \\ H \mapsto E^H \end{array}$ ist eine inklusionsumkehrende Bijektion mit Inverser $\delta : \begin{array}{c} \mathrm{Int}(E/k) \to \mathrm{Sub}(\mathrm{Gal}(E/k)) \\ B \mapsto \mathrm{Gal}(E/B) \end{array}$.
(2) $B \in \mathrm{Int}(E/k)$ ist genau denn eine Galoiserweiterung von k falls $\mathrm{Gal}(E/B)$ eine normale *Untergruppe von $\mathrm{Gal}(E/k)$ ist. In diesem Fall ist ${}^{\mathrm{Gal}(E/k)}/_{\mathrm{Gal}(E/B)} \cong \mathrm{Gal}(B/k)$.*

Einfache Folgerungen der Galois Korrespondenz

Korollar. *Eine endliche Galois Erweiterung hat nur endlich viele Zwischenkörper.*

Definition. Eine Erweiterung E/k ist *einfach* falls es $u \in E$ gibt mit $E = k(u)$.

Proposition. *Eine endliche Erweiterung E/k ist genau dann einfach, falls es nur endlich viele Zwischenkörper gibt.*

Korollar. *Eine (endliche) Galois Erweiterung E/k ist immer einfach.*

Satz. *Sei E/k eine endliche Galois Erweiterung mit $\mathrm{char} = 0$. Falls $\mathrm{Gal}(E/k)$ auflösbar ist, so ist E in einer radikalen Erweiterung von k enthalten.*

G endlich auflösbar mit $|G| \geq 2 \Rightarrow [G, G] \subsetneq G$. ${}^{G}/_{[G,G]}$ ist eine endliche abelsche Gruppe $\neq (e)$. Also ein Produkt von ${}^{\mathbb{Z}}/_{p^n\mathbb{Z}}$ wobei p Primzahl und $n \geq 1$.

Insbesondere: ${}^{\mathbb{Z}}/_{p^n\mathbb{Z}} \supseteq {}^{\mathbb{Z}}/_{p^{n-1}\mathbb{Z}}$ mit Index p. Also enthält ${}^{G}/_{[G,G]}$ eine Untergruppe $M < {}^{G}/_{[G,G]}$ mit Index p. Sei $p : G \to {}^{G}/_{[G,G]}$ und $N := p^{-1}(M)$. Dann ist $N \lhd G$ und hat Index p.

$N \lhd G = \mathrm{Gal}(E/k)$ und $E^N \supseteq k$. E^N ist eine Galois Erweiterung von k von Grad p, p eine Primzahl.

Lemma. *E/k endliche Galois Erweiterung mit $p := [E : k]$ Primzahl. Falls k eine p-te Wurzel von 1 enthält mit $w \neq 1$ dann gibt es $\xi \in E$ mit $\xi^p \in k$ und $E = k(\xi)$.*

8.1 Kreisteilunskörper (Cyclotomic fields)

Sei $n \geq 1$ natürliche Zahl; k ein Körper. Sei $k[n]$ ein Zerfällungskörper von $X^n - 1 \in k[x]$. Sei $\mu \subseteq k[n]$ die Menge der Nullstellen. Dann ist μ_n eine endliche Untergruppe von $k[n]^\times$ und daher zyklisch. Wir nennen *n-te primitive Einheitswurzel* einen erzeugender dieser Gruppe. Falls $\xi \in \mu_n$ eine n-te primitive Einheitswurzel ist, so folgt $k[n] = k(\xi)$.

Annahme: Entweder char $= 0$ oder char t teilt n nicht. Das ist nach Lemma 2.10 äquivalent zur Eigenschaft, dass $X^n - 1$ keine mehrfachen Nullstellen besitzt (weil $X^n - 1$ und nX^{n-1} teilerfremd sind). Insbesondere ist $X^n - 1$ separabel und daher (Def 4.12 und Satz 4.11) ist $k[n]$ eine Galois Erweiterung von k. Das Problem ist $\mathrm{Gal}(k[n]/k)$ zu bestimmen.

Sei ξ eine n-te primitive Einheitswurzel: $\begin{array}{c} \mathbb{Z}/n\mathbb{Z} \to \mu_n \\ k \mapsto \xi^k \end{array}$. Sei $\sigma \in \mathrm{Gal}(k[n]/k) < \mathrm{Aut}(\mu_n)$. Dann gibt es $a_\sigma \in \mathbb{Z}/n\mathbb{Z}$ so dass $\sigma(\xi) = \xi^{a_\sigma}$, also ist $a_\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Damit erhalten wir einen injektiven Homomorphismus $\begin{array}{c} \mathrm{Gal}(k[n]/k) \to (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma \mapsto \alpha_\sigma \end{array}$: Was ist das Bild?

Satz. $\begin{array}{c} \mathrm{Gal}(\mathbb{Q}[n]/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma \mapsto a_\sigma \end{array}$ *ist ein Isomorphismus.*

Beweis stammt von Dedekind 1857.

Lemma (Gauss)**.** *Sei $p = R \cdot Q$ wobei $p \in \mathbb{Z}[X]$ und $R, Q \in \mathbb{Q}[X]$. So gibt es $\lambda, \mu \in \mathbb{Q}^\times$ mit $q = \lambda \mathbb{Q} \in \mathbb{Z}[X], r = \mu R \in \mathbb{Z}[X]$. und $p = rq$. Falls zudem p, R und Q unitär sind so folgt $R, Q \in \mathbb{Z}[X]$.*

Sei $\xi \in \mathbb{C}$ eine n-te primitive Einheitswurzel von 1 ; $\xi = e^{\frac{2\pi i}{n}}$ dann $\mathbb{Q}[n] \subseteq \mathbb{C}$.

Definition. Das n-te Zyklotomische Polynom $\Phi_n(x) = \prod_{\substack{(a,n)=1 \\ 1 \leq a \leq n-1}} (X - \xi^a)$

Korollar. *$\Phi_n \in \mathbb{Z}[X]$ und ist in $\mathbb{Q}[x]$ irreduzibel.*

- Φ_n ist irreduzibel: $\mathbb{Q}[n] = \mathbb{Q}(\xi)$ ist Zerfällungskörper von Φ_n und $\mathrm{Gal}(\mathbb{Q}[n]/\mathbb{Q})$ wirkt transitiv auf den Nullstellen von $\Phi_n \Rightarrow \Phi_n$ ist irreduzibel.
- $\deg(\Phi_n) = \varphi(n)$ (Eulersche Phi Funktion). Insbesondere, falls p Primzahl ist $\Phi_p(x) = X^{p-1} + \ldots + x + 1$.
- Φ_{105} ist das erste Zyklotomische Polynom das einen Koeffizienten $a \notin \{-1, 0, 1\}$ hat.

Proposition.
1. *$X^n - 1 = \prod_{d|n} \Phi_d(x)$ (also $\Phi_1(x) = x - 1$, und $\Phi_n(x)$ kommen vor)*
2. *p Primzahl: $\Phi_p(x) = X^{p-1} + x^{p-2} + \ldots + 1$*
3. *$n \geq 2$: $\Phi_n(x) = X^{\varphi(n)} \Phi_n(\frac{1}{x})$*
4. *$\Phi_{p^r}(x) = \Phi_p(X^{p^{r-1}})$*
5. *p Primzahl und $(p, n) = 1$ dann ist*

$$\Phi_{pn} = \frac{\Phi_n(X^p)}{\Phi_n(x)}.$$

6. *$\Phi_n(x) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}$ Wobei* $\mu : \mathbb{N}^* \to -1, 0, 1$

$$\mu(n) = \begin{cases} 0 & \textit{falls } n \textit{ durch } p^2 \textit{ für eine Primzahl } p \textit{ teilbar ist} \\ (-1)^r & \textit{falls } n = p_1 \cdot \ldots \cdot p_r \textit{ paarweise verschieden sind} \\ 1 & \textit{falls } n = 1 \end{cases}$$

Satz. $(p, n) = 1$. $\mathrm{Gal}(\mathbb{F}_p[n]/\mathbb{F}_p) \to (\mathbb{Z}/n\mathbb{Z})^\times$ *Das Bild ist gleich der durch p modulo n erzeugten zyklischen Gruppe.*

$p \equiv 1(n) \Leftrightarrow \mathbb{F}_p[n] = \mathbb{F}_p$.

Dirichlet: $\exists! p$ Primzahlen, $p \equiv a(n)$ wobei a und n Teilerfremd.