# 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.

**Beispiel** (Ringe)**.** (1) $R = \{0\}$. Hier ist $0 = 1$.
(2) $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ sind jeweils Unterringe.
(3) Sei $V$ ein Vektorraum, dann ist

$$\mathrm{End}(V) = \{f : V \to V \text{ linear}\}$$

ein Ring, wobei $+$ punktweise definiert wird und $\cdot$ die Verknüpfung ist.
(4) $\mathrm{Mat}_{n,n}(\mathbb{Q})$ bzw. $\mathbb{R}, \mathbb{C}, \mathbb{Z}$.
(5) Sei $m \geq 1$. Dann ist $Z_m = \mathbb{Z}/Z_m$ ein Ring. Wenn dies die Übersicht erhöht können wir die Restklasse $[a]_{\equiv \mod m}$ einer Zahl $a$ einfach mit $\overline{a}$. In dieser Notation haben wir

$$\overline{a} + \overline{b} = \overline{a + b} \quad \overline{a} \cdot \overline{b} = \overline{ab}.$$

(6) $\mathbb{Z}$-adjungiert-$i$ : $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.
$\mathbb{Z}$-adjungiert-$\sqrt{2}$ : $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$.

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2}.$$

(7) Sei $X$ eine Menge und $R = \mathbb{Z}^X = \{f : X \to \mathbb{Z}\}$ mit punktweise Operationen. Dies ist ein kommutativer Ring z.B. $C([0, 1]) = \{f : [0, 1] \to \mathbb{C} \text{ stetig}\}$.
Antibeispiel: $C_0(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{C} \text{ stetig und } \lim_{|x| \to \infty} f(x) = 0\}$ ist kein Ring

**Beispiel** (Ringhomomorphismen)**.** (1) $R = \{0\} \xrightarrow{f} \mathbb{Z}, 0 \mapsto 0$, $0_R = 1_R \mapsto f(1_R) = f(0_R) = 0_\mathbb{Z} \neq 1_\mathbb{Z}$
(2) $R \to \{0\}, a \mapsto 0$ ist ein Ringhomomorphismus.
(3) $\mathbb{Z} \to R, n \mapsto n \cdot 1_R$ ist ein Ringhomomorphismus.
(4) $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$ da Unterringe.
(5) $\mathbb{R} \to \mathrm{Mat}_{n,n}(\mathbb{R}), t \mapsto tI_n$. Umgekehrt geht nicht.
(6) $C([0, 1] \to \mathbb{C}, f \mapsto f(x_0)$ für ein festes $x_0 \in [0, 1]$
(7) $\mathbb{Z} \to \mathbb{Z}_m, a \mapsto \overline{a}$
(8) $\mathrm{Mat}_{n,n}(\mathbb{C}) \to \mathrm{End}(\mathbb{C}^n), A \mapsto (x \in \mathbb{C}^n \mapsto Ax)$ ist ein Ringisomorphismus.

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

*Beweis.* Sei $a \in R$. Dann gilt $a = a \cdot 1 = a \cdot 0 = 0$ □

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

*Beweis.* Die Eigenschaften von $\binom{n}{k}$ sind bekannt, und damit funktioniert der übliche Beweis. $\square$

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)

**Beispiel.** In $\mathbb{Z}_{15}$ gilt $\overline{3} \cdot \overline{15} = \overline{15} = \overline{0}$ aber $\overline{3} \neq \overline{0} \neq \overline{5}$.

**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.*

*Beweis.* Angenommen $R$ ist ein Integritätsbereich und $a \in R \setminus \{0\}, b \in R$ erfüllt $a \cdot b = 0 \Rightarrow a \cdot b = a \cdot 0 \Rightarrow b = 0$. Also kann es keine Nullteiler geben.

Angenommen $R$ hat keine Nullteiler und $a, b, c \in R, a \neq 0$ erfüllen $ab = ac \Rightarrow ab - ac = 0, a(b-c) = 0 \Rightarrow b = c$. $\square$

**Beispiel.**
1. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$
2. Antibeispiel: $C([0,1])$ ist kein Integritätsbereich.
3. Wann ist $\mathbb{Z}_m$ ein Integritätsbereich?

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

**Beispiel.**
1. $\mathbb{C}^x = \mathbb{C} \setminus \{0\}$
2. $\mathbb{Z}^x = \{\pm 1\}$
3. $\mathbb{Z}[i]^x = \{1, -1, i, -i\}$
4. $\mathbb{Z}[\sqrt{2}]^x = ?$. Aufjedenfall enthält es $(1+\sqrt{2})(\sqrt{2}-1) = 1$.

**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.*

*Beweis.* Angenommen $a \neq 0, b, c \in R$.

$$ab = ac \overset{a^{-1}}{\Rightarrow} a^{-1}ab = a^{-1}ac \Rightarrow b = c.$$

$\square$

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

*Beweis.* Falls $m = 1$ ist, dann ist $\mathbb{Z}_1 = \{\overline{0}\}$ sicher kein Körper (da $0 \neq 1$ gelten muss).
Falls $m = ab$ mit $a, b < m$, dann ist $\overline{0} = \overline{m} = \overline{a}\overline{b}$ mit $\overline{a} \neq 0 \neq \overline{b}$. Also hat $\mathbb{Z}_m$ Nullteiler, ist kein Integritätsbereich und kein Körper.

Sei nun $m$ eine Primzahl und $\overline{a} \neq 0$. Sei $d = \mathrm{ggT}(m, a)$. Nach Definition ist $d \geq 1$ ein Teiler von $m$. Falls $d = m$ wäre, dann folgt $m|a \Rightarrow \overline{a} = \overline{0}$ ↯ . Also ist $d = 1$. Nach dem Lemma vom letzten Mal folgt daraus, dass es $k, l \in \mathbb{Z}$ mit $1 = k \cdot m + l \cdot a$. Modulo $m$ ist die $\overline{1} = \overline{l} \cdot \overline{a}$. Dies zeigt, dass $\overline{a} \neq 0$ die multiplikative Inverse $l$ besitzt. □

**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 $K = \mathbb{Q}$.*

*Beweis.* Wir definieren die Relation $\sim$ auf $X = R \times (R \setminus \{0\})$ :

$$(a, b) \sim (p, q) \Leftrightarrow aq = pb \quad [\text{in } R] \quad [\text{versteckt wollen wir } \frac{a}{b} = \frac{p}{q}].$$

Äquivalenzrelation:

- $(a, b) \sim (a, b)$ denn $ab = ab$.
- $(a, b) \sim (p, q) \Rightarrow (p, q) \sim (a, b)$ denn $aq = pb$ ist $pb = aq$.
- $(a, b) \sim (p, q)$ und $(p, q) \sim (m, n)$. $aq = pb$ und $pn = mq$. Multipliziere erste mit $n$ und zweite mit $b$.
$$aqn = pbn = pnb = mqb \Rightarrow aqn = mqb \overset{q \neq 0}{\Rightarrow} an = mb.$$
und somit $(a, b) \sim (m, n)$.

Wir definieren $K = X/\sim$ und die Elemente $0_K = [(0, 1)]_\sim$ und $1_K = [(1, 1)]_\sim$. und die Operationen $+$ und $\cdot$:

$$[(a, b)]_\sim + [(p, q)]_\sim = [(aq + pb, bq)]_\sim$$
$$[(a, b)]_\sim \cdot [(p, q)]_\sim = [(ap, bp)]_\sim.$$

Diese Operationen sind wohldefiniert (für $+$ siehe Buch).
Angenommen $(a, b) \sim (a', b'), (p, q) \sim (p', q')$ somit $ab' = a'b$ und $pq' = p'q$. Schließlich multipliziere beide Gleichungen $(ap)(b'q') = (a'p')(bq)$ und somit $(ap, bq) \sim (a'p', b'q')$.
Wir überprüfen Schritt für Schritt die Axiome eines Körpers:

- Kommutativität der Addition:
$$[(a, b)]_\sim + [(p, q)]_\sim = [(aq + pb, bp)]_\sim = [(pq + aq, qb)]_\sim = [(p, q)]_{sim} + [(a, b)]_\sim.$$
unter Verwendung der Kommutativität der Addition und Multiplikation in $R$.

$K$ ist sogar ein Körper.
$$[(0, 1)]_\sim \neq [(1, 1)]_\sim \text{ da } 0 \cdot 1 \neq 1 \cdot 1 \text{ in } R$$
Falls $[(a, b)]_\sim \neq [(0, 1)]_\sim$, dann ist $[(a, b)]_\sim^{-1} = [(b, a)]_\sim$, da

$$[(a, b)]_\sim \cdot [(b, a)]_\sim = [(ab, ab)]_\sim = [(1, 1)]_\sim$$

□

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.

*Beweis.* Angenommen $a \neq 0$, dann gilt $\frac{a}{1} \neq \frac{0}{1}$. Also gilt $\operatorname{Ker} \iota = \{0\}$ und $\iota$ ist injektiv.
$\iota(1) = \frac{1}{1} = 1_K$ und $\iota(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \iota(a) + \iota(b)$ sowie $\iota(ab) = \frac{a \cdot b}{1 \cdot 1} = \iota(a)\iota(b)$ $\square$

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

**Beispiel.** Verwenden sie SageMath um herauszufinden für welche $p = 2, 3, \ldots, 100$ er ein $g \in (\mathbb{Z}/p\mathbb{Z})^X$ mit

$$(\mathbb{Z}/p\mathbb{Z})^X = \{g^k : k = 0, 1, \ldots\}$$

gibt ($k < p$ genügt)?

## 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.

**Beispiel.** Sei $K = \mathbb{F}_2 = \{\overline{0}, \overline{1}\} = \mathbb{Z}/2\mathbb{Z}$. Dann soll $X^2 + X$ *nicht* das Nullpolynom sein, obwohl die zugehörige Polynomfunktion gleich 0 ist:

$$\begin{aligned} 0 \in \mathbb{F}_2 &\mapsto 0^2 + 0 = 0 \\ 1 \in \mathbb{F}_2 &\mapsto 1^2 + 1 = 1 + 1 = 0 \end{aligned}$$

Wir verwenden die Koeffizienten um Polynome zu 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.

*Beweis.* Wir überprüfen die Axiome welche die Multiplikation betreffen und überlassen die anderen dem Leser.

1. $a \cdot b = b \cdot a$ gilt, denn $\sum_{i+j=n} a_i b_j = \sum_{i+j=n} b_i a_j$.
2. $(1 \cdot a)_n = \sum_{i+j=n} 1_i a_j = a_n$, da $1_i = 0$ außer wenn $i = 0$.
3. $\underbrace{(ab)c}_{=d} = a(bc)$ gilt, denn

$$d_n = \sum_{i+j=n} \underbrace{(ab)_i}_{=\sum_{k+l=i} a_k b_l} c_i = \sum_{i+j+k=n} a_i b_j c_k$$

ohne Klammern wegen Assoziativität von $\cdot$ in $R$. Rechts ergibt sich dieselbe Antwort.

4.
$$((a+b)\cdot c)_n = \sum_{i+j=n} \underbrace{(a+b)_i c_j}_{a_i c_j + b_i c_j} = \sum_{i+j=n} a_i c_j + \sum_{i+j=n} b_i c_j = (ac+bc)_n$$

Des Weiteren überprüfen wir, dass der Polynomring unter $+$ und $\cdot$ abgeschlossen ist: Angenommen $a, b$ sind Polynome, so dass $a_i = 0$ für $i > I$ und $b_j = 0$ für $j > J$. Draus folgt

$$(a+b)_n = 0 \text{ für } n > \max(I,J) \qquad (a\cdot b)_n = 0 \text{ für } n > I+J$$

denn $(a\cdot b)_n = \sum_{i+j=n} \underbrace{a_i b_j}_{=0}$. Falls $a_i b_j \neq 0$ wäre, dann würde $a_i \neq 0$ und $b_j \neq 0$ folgen, was wiederum $i \leq I, j \leq J$ und damit $n = i+j \leq I+J$ impliziert. □

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

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

Allgemeiner: Sei $a$ ein Polynom, dann ist

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

denn $(X\cdot a)_n = \sum_{i+j=n} X_i a_j = a_{n-1}$ da $X = 0$ außer wenn $i = 1$ ist. $(X\cdot a)_0 = X_0 \cdot a_0 = 0$.
Wir schreiben $R[X] = \{\sum_{i=0}^n a_i X^i : n \in \mathbb{N}, a_0, \dots, a_n \in R\}$ ($R$-adjungiert-$X$) für den *Ring der Polynome in der Variablen* $X$ und $R[\![X]\!] = \{\sum_{n=0}^\infty a_i X^i : a_0, a_1, \dots \in R\}$ für den *Ring der formalen Potenzreihen in der Variable* $X$

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

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

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

*Beweis.* Sei $f = p\cdot q$, also $f_n = \sum_{i+j} p_i p_j$ für alle $n \in \mathbb{N}$.

- Angenommen $n > \deg(p) + \deg(q) \Rightarrow p_i p_j = 0$ für alle $i + j = n \Rightarrow f_n = 0$.
- Angenommen $n = \deg(p) + \deg(q)$. Behauptung: $f_n = p_{\deg(p)} q_{\deg(q)}$ (führende Koeffizienten $\in R \setminus \{0\}$) da
$$f_n = \sum_{i+j=\deg(p)+\deg(q)} p_i q_j$$
Falls $i < \deg(p)$ ist, so ist $j > \deg(q) \Rightarrow q_i = 0$ und vize versa.
Somit ist $f_n \neq 0$, da $R$ ein Integritätsbereich ist.

Diese beiden Punkte beweisen $\deg(f) = \deg(p\cdot q) = \deg(p) + \deg(q)$ also die erste Behauptung in der Proposition.

Angenommen $p \mid q$, dann gibt es ein Polynom $g$ so dass $q = p \cdot g$ ist $\deg(q) = \deg(p) + \underbrace{\deg(g)}_{\geq 0} \geq \deg(p)$. Beweise die dritte Aussage in der Proposition.

Angenommen $p = \sum_{n=0}^{\deg(p)} p_n X^n, q = \sum_{n=0}^{\deg(q)} q_n X^n$, dann ist

$$p + q = \sum_{n=0}^{\max(\deg(p),\deg(q))} (p_n + q_n) X^n.$$

Daraus folgt $\deg(p+q) \leq \max(\deg(p), \deg(q))$. □

**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 $\Phi$ 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.*

*Beweis.* Sei $\Phi : R[X] \to S$ ein Ringhomomorphismus, $\varphi = \Phi\mid_R, x = \Phi(X) \in S$. Dann gilt

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

wie im Satz behauptet. Dies zeigt bereits den ersten Teil des Satzes, da die rechte Seite der Formel nur $\varphi$ und $x = \Phi(X)$ benötigt.

Sei nun $\varphi : R \to S$ ein Ringhomomorphismus und $x \in S$ beliebig. Wir verwenden $(*)$ um $\Phi$ zu definieren $\Phi : R[X] \to S$ ist nun definiert.

- $\Phi(1) = \phi(1_R) \underbrace{x^0}_{=1_S} = 1_S$.

- $$\begin{aligned}\Phi(a+b) &= \Phi(\sum_{n=0}^{\infty}(a_n+b_n)X^n = \sum_{n=0}^{\infty}\varphi(a_n+b_n)x^n \\ &= \sum_{n=0}^{\infty}\varphi(a_n)x^n + \sum_{n=0}^{\infty}\varphi(b_n)x^n = \Phi(a)+\Phi(b)\end{aligned}$$

- $$\begin{aligned}\Phi(a\cdot b) &= \Phi(\sum_{n=0}^{\infty}(\sum_{i+j=n}a_ib_j)X^n) = \sum_{n=0}^{\infty}\underbrace{\varphi(\sum_{i+j=n}a_ib_j)}_{\sum_{i+j=n}\varphi(a_i\varphi(b_j)}\ x^n \\ &= \sum_{i,j}\varphi(a_i)\varphi(b_j)x^{i+j} = (\sum_i\varphi(a_i)x^i)(\sum_j\varphi(b_j)x^j) = \Phi(a)\Phi(b).\end{aligned}$$

Also ist $\Phi$ in der Tat ein Ringhomomorphismus von $R[X]$ nach $S$. □

*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:

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

**Beispiel.** Falls wir $R = S$ und $\varphi = \mathrm{id}$ setzen, so erhalten wir für jedes $a \in R$ die entsprechende Auswertungsabbildung

$$\mathrm{ev}_a : f \mapsto f(a) = \sum_{n=0}^{\infty} f_n a^n.$$

Wenn wir $a \in R$ variieren, ergibt sich auch eine Abbildung

$$\Psi : f \in R[X] \to \left(f(\cdot) : \begin{cases} R \to R \\ a \mapsto f(a)\end{cases}\right) \in R^R.$$

Wir statten $R^R$ mit den punktweise Operationen aus, womit $\Psi : R[X] \to R^R$ ein Ringhomomorphismus ist.

Falls $|R| < \infty$ und $R \neq \{0\}$, so kann $\Psi$ nicht injektiv sein.

**Beispiel.** Sei $R = \mathbb{Z}$ und $S = \mathbb{Z}/m\mathbb{Z}[X]$ für ein $m \geq 1$. Dann gibt es einen Ringhomomorphismus

$$f \in \mathbb{Z}[X] \mapsto \overline{f} = \sum_{n=0}^{\infty}(f_n \mod m)X^n \in \mathbb{Z}/m\mathbb{Z}[X^n].$$

Hier ist $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}[X], a \mapsto a \mod m$.

**Beispiel.** $R = \mathbb{C}, S = \mathbb{C}[X], \varphi(a) = \overline{a}, a \in \mathbb{C}$.

$$f \in \mathbb{C}[X] \mapsto \sum_{n=0}^{\infty}\overline{f_n}X^n \in \mathbb{C}[X].$$

ist sogar ein Ringautomorphismus.

## 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) $a \in I, x \in R \Rightarrow xa \in I$

**Beispiel.** Seien $R, S$ zwei kommutative Ringe und $\varphi : R \to S$ ein Ringhomomorphismus. Dann ist

$$\mathrm{Ker}(\varphi) = \{a \in R \mid \varphi(a) = 0\}$$

ein Ideal.

Beweis von (iii): Falls $a \in \mathrm{Ker}(\varphi), x \in R$ dann gilt $\varphi(xa) = \varphi(x)\underbrace{\varphi(a)}_{=0} = 0 \Rightarrow xa \in \mathrm{Ker}(\varphi)$.

**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*
$$R/I \times R/I \to R/I \quad \textit{bzw.} \quad R/I \to R/I.$$
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.*

*Beweis.* 1) :

1. $a \sim a$ dann $a \cdot a = 0 \in I$.
2. $a \sim b \Rightarrow b \sim a$ denn $b - a = \underbrace{(-1)}_{\in R}\underbrace{(a - b)}_{\in I} \in I$
3. $a \sim b$ und $b \sim c \Rightarrow a \sim c$ denn $a - c = \underbrace{(a - b)}_{\in I} + \underbrace{(b - c)}_{\in I} \in I$

Also ist $\sim$ eine Äquivalenzrelation und wir können den Quotienten $R/\sim = R/I$ betrachten.

2) : Wir zeigen, dann $+ : R/I \times R/I \to R/I$ wohldefiniert ist:

$$[a]_\sim + [b]_\sim = [a + b]_\sim$$

über die Identifikation $[a]_\sim \rightsquigarrow a, [b]_\sim \rightsquigarrow b$ und $(a, b) \mapsto a + b \mapsto [a + b]_\sim$.

Also müssen wir zeigen: $a \sim a'$, $b \sim b' \Rightarrow a + b \sim a' + b'$. Dies gilt da $a - a' \in I, b - b' \in I \Rightarrow (a + b) - (a' - b') \in I$ wegen Eigenschaft (ii) von Idealen.

Angenommen $a \sim a', b \sim b' \Rightarrow ab \sim a'b'$.

$$ab - a'b' = ab - a'b + a'b - a'b' = b\underbrace{(a - a')}_{\in I} + a'\underbrace{(b - b')}_{\in I} \in I.$$

wegen (iii) in der Definition von Idealen Dies zeigt, dass die Multiplikation von Restklassen

$$[a]_\sim \cdot [b]_\sim = [a \cdot b]_\sim$$

wohldefiniert ist. Der Beweis für $-a$ ist analog, oder ergibt sich aus der Multiplikation mit $[-1]_\sim$. Dies beweist 2).

3): Da die Ringaxiome nur Gleichungen enthalten, sind die Ringaxiome in $R/I$ direkte Konsequenzen der Ringaxiome in $R$: z.B. Kommutativität von $+$ in $R/I$

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$

wobei das zweite Gleich wegen der Kommutativität in $R$ gilt.

Alle anderen Axiome folgen auf dieselbe Weise. Des Weiteren gilt für die Projektion $p : R \to R/I, a \mapsto [a]_\sim$

$$\begin{aligned} &p(0) = [0]_\sim, p(1) = [1]_\sim \\ &p(a + b) = [a + b]_\sim = [a]_\sim + [b]_\sim = p(a) + p(b) \\ &p(a \cdot b) = [a \cdot b]_\sim = [a]_\sim \cdot [b]_\sim = p(a) \cdot p(b) \end{aligned}$$

Also ist $p : R \to R/I$ ein Ringhomomorphismus. □

**Beispiel.**
- $I = \mathbb{Z}_m \subseteq \mathbb{Z}$ ist ein Ideal
- $I = R, I = \{0\}$ (Nullideal) sind Ideale in einem beliebigen kommutativen Ring.

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

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

*Beweis.* „$\Leftarrow$“: Angenommen $u = v^{-1} \in I$ und $v \in R, a \in R$. Dann gilt

$$a = a \cdot \underbrace{v \cdot u}_{=1} \in I.$$

Da $a \in R$ beliebig war folgt also $I = R$. □

**Beispiel.** Welche Ideale gibt es in einem Körper? Nur $\{0\}$ und $K$. Da jede andere Teilmenge von $K$ eine Einheit besitzt (Lemma).

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

$$I = (a_1, \ldots, a_n) = \{x_1a_1 + x_2a_2 + \ldots + x_na_n : x_1, \ldots, x_n \in R\}$$

das von $a_1, \ldots, a_n$ *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 $b = ua$*

*Beweis.* Angenommen $(a) \subseteq (b)$ wie in 1). Da $a = 1 \cdot a \in (a)$ folgt $a \in (b) = Rb$. Also gilt $a = x \cdot b$ für ein $x \in R$, also $b \mid a$.

Falls umgekehrt $b \mid a$, dann ist $a \in (b) \Rightarrow (a) = Ra \subseteq (b)$.

Die Implikation $\Leftarrow$ in 2) folgt aus 1). Also nehmen wir nun an, dass $(a) = (b)$. Dies impliziert $a = xb$ und $b = ya$ für $x, y \in R$. Daraus folgt $a = xb = xya$.
Falls $a = 0$ ist, so ist auch $b = 0$ und wir setzen $u = 1$.
Falls $a \neq 0$, so können wir kürzen und erhalten $1 = xy$ also $x, y \in R^X$ und wir setzen $u = y$. □

**Beispiel.** Sei $R = C_{\mathbb{R}}([0,3])$.

$$a = \begin{cases} -x+1 & \text{für } x \in [0,1] \\ 0 & \text{für } x \in (1,2) \\ x-2 & \text{für } x \in [2,3] \end{cases} \qquad b = \begin{cases} x-1 & \text{für } x \in [0,1] \\ 0 & \text{für } x \in (1,2) \\ x-2 & \text{für } x \in [2,3] \end{cases}.$$

Behauptung: $(a) = (b)$ aber $b \notin R^X a$. Es gilt $a \in (b)$, denn $a = b \cdot f$ und $b = a \cdot f$ für

$$f = \begin{cases} -1 & \text{für } x \in [0,1] \\ 2x-3 & \text{für } x \in (1,2) \\ 1 & \text{für } x \in [2,3] \end{cases}$$

$b \notin R^X a$ folgt aus dem Zwischenwertsatz.

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 $\varphi$ 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 $\varphi$ 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* $\mathrm{Im}(\overline{\varphi}) = \mathrm{Im}(\varphi)$

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

*Beweis.* Wir beginnen mit 2) und definieren $\overline{\varphi}(x+I) = \varphi(x)$. Dies ist wohldefiniert: Falls $x + I = y + I$ ist, so ist $x - y \in I \subseteq \mathrm{Ker}(\varphi)$. Daher gilt $\varphi(x) - \varphi(y) = \varphi(x-y) = 0$.
Da $\varphi$ ein Ringhomomorphismus ist, gilt

$$\begin{aligned} &\varphi(1_R) = 1_S \Rightarrow \overline{\varphi}(1+I) = 1_S \\ &\varphi(x+y) = \varphi(x) + \varphi(y) \Rightarrow \overline{\varphi}(X + I + y + I) = \varphi(x+I) + \varphi(y+I) \\ &\varphi(xy) = \varphi(x)\varphi(y) \Rightarrow \overline{\varphi}((x+I)(y+I) = \overline{\varphi}(xy+I) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}(x+I)\overline{\varphi}(y+I) \end{aligned}$$

$\varphi = \overline{\varphi} \circ p_I$ denn für $x \in R$ gilt $p_I(x) = x + I$, $\overline{\varphi} \circ p_I(x) = \overline{\varphi}(x+I) = \varphi(x)$ nach Definition von $\overline{\varphi}$. Da dies für alle $x \in R$ gilt ergibt sich obiges und das kommutative Diagramm.

$$\begin{aligned} \mathrm{Ker}(\overline{\varphi}) &= \{x + I : \underbrace{\varphi(x)}_{\overline{\varphi}(x+I)} = 0\} = \mathrm{Ker}(\varphi/I) \\ \mathrm{Im}(\overline{\varphi}) &= \{\overline{\varphi}(x) : x \in R/I\} = \{\varphi(x) : x \in R\} = \mathrm{Im}(\varphi) \end{aligned}$$

Dies beweist 2) vom Satz.

Wir wollen nun 1) beweisen und wenden 2) für $I = \mathrm{Ker}(\varphi)$ an. Also ist $\overline{\varphi}(x + \mathrm{Ker}(\varphi)) = \varphi(x)$ für $x + \mathrm{Ker}(\varphi) \in R/\mathrm{Ker}(\varphi)$ ein Ringhomomorphismus mit Bild $\mathrm{Im}(\varphi)$.

Hier gilt $\operatorname{Ker}(\overline{\varphi}) = {}^{\operatorname{Ker}(\varphi)}/_{\operatorname{Ker}(\varphi)} = \{0 + \operatorname{Ker}(\varphi)\}$, also ist $\overline{\varphi}$ injektiv. Daher ist $\overline{\varphi}$ ein Ringhomomorphismus von ${}^{R}/_{\operatorname{Ker}(\varphi)}$ nach $\operatorname{Im}(\varphi)$ wie in 1) behauptet. □

*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.

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

**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 $1 = a + b$.

**Beispiel.** $I = (p)$ und $J = (q) \subseteq \mathbb{Z} = R$ falls $p, q$ verschiedene (positive) Primzahlen sind.

**Proposition** (Chinesischer Restsatz)**.** *Sei $R$ ein kommutativer Ring und seien $I_1, \ldots, I_n$ paarweise coprime Ideale. Dann ist der Ringhomomorphismus $\varphi : R \to {}^{R}/_{I_1} \times \ldots \times {}^{R}/_{I_n}$ mit $x \mapsto (x + I_1, \ldots, x + I_n)$ surjektiv mit $\operatorname{Ker}(\varphi) = I_1 \cap \ldots \cap I_n$.*
*Dies induziert einen Ringisomorphismus ${}^{R}/_{I_1 \cap \ldots \cap I_n} \to {}^{R}/_{I_1} \times \ldots \times {}^{R}/_{I_n}$.*

*Beweis.* Dass der Kern $\operatorname{Ker}(\varphi)$ genau $I_1 \cap \ldots \cap I_n$ ist, ergibt sich aus den Definitionen. Wir zeigen, dass $\varphi$ surjektiv ist. Hierfür wollen wir für jedes $i \in \{1, \ldots, n\}$ ein $x_i \in R$ finden so dass

$$\varphi(x_i) = (0 + I_1, \ldots, \underbrace{1 + I_i}_{i\text{-te Stelle}}, \ldots, 0 + I_n).$$

Zur Vereinfachung der Notation betrachten wir den Fall $i = 1$.

**Behauptung:** $I_1$ und $I_2 \cap \ldots \cap I_n$ sind coprim, d.h. es existieren $a \in I_1$ und $b \in I_2 \cap \ldots I_n$ so dass $a + b = 1$.
Aus der Behauptung folgt, dass $x_1 = b$ erfüllt:

$$\varphi(x_1) = (b + I_1, b + I_2, \ldots, b + I_n) = (1 + I_1, 0 + I_2, \ldots, 0 + I_n)$$

wegen der Definition von $b$ und $a + b = 1$.

Wir zeigen die Behauptung mittels Induktion nach $n$ :
$n = 2$ : $I_1$ und $I_2$ sind coprim. Dies gilt nach Annahme in der Proposition.
Induktionsschritt ($n - 1 \to n$): Wir nehmen an, dass $I_1$ und $I_2 \cap \ldots I_{n-1}$ coprim sind, d.h. es gibt $a \in I_1$, $b \in I_2 \cap \ldots, I_{n-1}$ mit $a + b = 1$. Des weiteren ist $I_1$ coprim zu $I_n$, d.h. es gibt $c \in I_1, d \in I_n$ mit $c + d = 1$.

$$\Rightarrow a + b(\underbrace{c + d}_{=1}) = 1 \Rightarrow \underbrace{a + bc}_{\in I_1} + \underbrace{bd}_{\in I_2 \cap \ldots I_{n-1} \cap I_n} = 1.$$

Folgt $I_1$ ist coprim zu $I_2 \cap \ldots \cap I_n$, Also haben wie die Behauptung mittels Induktion gezeigt.

Wir können $x_1, \ldots, x_n$ wie oben verwenden um die Surjektivität zu zeigen: Sei $(a_1 + I_1, \ldots, a_n + I_n) \in {}^{R}/_{I_1} \times \ldots \times {}^{R}/_{I_n}$ beliebig. Dann gilt

$$\varphi(a_1 x_1 + \ldots + a_n x_n) = (a_1 x_1 + \ldots + a_n x_n + I_1, \ldots, a_1 x_1 + \ldots + a_n x_n + I_n) = (a_1 + I_1, a_2 + I_2, \ldots, a_n + I_n).$$

da $x_i$ modulo $I_i$ gleich 1 ist und ansonsten $x_i \in I_j$ ($j \neq i$) gilt und daher $x_i$ modulo $I_j$ gleich 0 ist. □

## 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.*

*Beweis.* Falls $I \cap \mathbb{N}_{>0} = \{\}$ ist, so ist $I = (0)$. Ansonsten können wir das kleinste Element $m$ in $I \cap \mathbb{N}_{>0}$ finden . Falls $n \in I$ ist, so können wir Division mit Rest anwenden und erhalten $\underbrace{n}_{\in I} = \underbrace{k \cdot m}_{\in I} + r$ für $k \in \mathbb{Z}, r \in \{0, \ldots, m-1\}$. Folgt $r \in I \Rightarrow r = 0$ da $m$ das kleinste Element von $I \cap \mathbb{N}_{>0}$ war. Da $n \in I$ beliebig war, folgt $I = (m)$.
Falls $m = a \cdot b$ für $a, b < m$ ist, so ist $\mathbb{Z}/(m)$ kein Integritätsbereich, da $(a + (m))(b + (m)) = ab + (m) = 0 + (m)$ ist. Falls $m > 0$ eine Primzahl ist, so ist $\mathbb{Z}/(m)$ ein Körper und damit auch ein Integritätsbereich. □

**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.

**Beispiel.** Charakteristik 0: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$ Wenn $K$ Charakteristik 0 hat, dann enthält $K$ eine isomorphe Kopie von $\mathbb{Q}$.
Charakteristik $p : \mathbb{F}_p = \mathbb{Z}/(p), \mathbb{F}_p(X)$

**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.*

*Beweis.* Es gilt $F(0) = 0^p, F(1) = 1^p = 1, F(xy) = (xy)^p = x^p y^p = F(x)F(y)$. Wir müssen noch $F(x + y) = F(x) + F(y)$ zeigen.

$$(x+y)^p = x^p + \underbrace{\binom{p}{1}}_{=p \cdot 1_K = 0} x^{p-1}y + \binom{p}{2} x^{p-2}y^2 + \ldots + \binom{p}{p-1} xy^{p-1} + y^p = x^p + y^p \quad [\text{in } K].$$

**Behauptung:** Für $0 < k < p$ gilt $p \mid \binom{p}{k}$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\ldots(p-k+1)}{k!} \Rightarrow k! \binom{p}{k} = p(p-1)\ldots(p-k+1) = 0 \mod p.$$

aber $k! \mod p \neq 0$. Da Rechnen modulo $p$ einen Körper definiert, erhalten wir $k! \not\equiv 0, k!\binom{p}{k} \equiv 0 \mod p \Rightarrow \binom{p}{k} \equiv 0 \mod p$. Folgt $p \mid \binom{p}{k}$.
Wenn $|K| < \infty$, dann ist $F$ auch surjektiv! Warum: $\mathrm{Ker}(f) \subseteq K$ ist ein Ideal $\Rightarrow \mathrm{Ker}(F) = \{0\}$ und $F$ ist injektiv. Wenn $|K| < \infty$, folgt aus der Injektivität auch die Surjektivität. □

## 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 $I \subsetneq J \subsetneq R$.*

*Beweis.* 1) $I$ ist ein Primideal $\Leftrightarrow$ $R/I \neq \{0 + I\}$ und $([a][b] = 0 \Rightarrow [a] = 0$ oder $[b] = 0 \Leftrightarrow$ $I \neq R$ und $(ab \in I \Rightarrow a \in I$ oder $b \in I)$.

2) $I$ ist ein Maximalideal $\Leftrightarrow$ $R/I$ ist ein Körper $\Leftrightarrow$ $I \neq R$ und es gibt kein Ideal $J \subseteq R$ mit $I \subsetneq J \subsetneq R$.

Letztes „genau dann wenn“: $\Rightarrow$: Sei $J \subseteq R$ ein Ideal un $I \subseteq J$ un $x \in J \setminus I$. Dann ist $x + I \in R/I \setminus \{0+I\}$ ist invertierbar in $R/I$, also $(x+I)^{-1} = y+I$ Daraus folgt $\underbrace{x}_{\in J} y-1 \in I \subseteq J \Rightarrow 1 \in J$, also $J = R$.

$\Leftarrow$: Angenommen $x + I \neq 0 + I$, dann können wir $J = (x) + I$ definieren. Dies ist ein Ideal $I \subsetneq J \subseteq R$. Also ist $J = R$ und es gibt ein $y \in R$ mit $xy + I = 1 + I$ □

**Beispiel.** In $R = \mathbb{Z}$ gilt:

- $I = (m)$ ist ein Primideal $\Leftrightarrow$ $m = 0$ oder $m = \pm p$ eine Primzahl ist.
- $I = (m)$ ist ein Maximalideal $\Leftrightarrow$ $m = \pm p$ eine Primzahl ist.

z.B. $(0) \leq (2)$ mit $(0)$ Primideal und $(2)$ Prim- und Maximalideal.

**Beispiel.** Sei $K$ ein Körper und $a_1, \dots, a_n \in K$. Wir definieren dass Ideal

$$I = (X_1 - a_1, \dots, X_n - a_n) \subseteq K[X_1, \dots, X_n]$$

Dann ist $I$ ein Maximalideal, und ist gleich dem Kern $\operatorname{Ker}(\mathrm{ev}_{a_1,\dots,a_n})$ des Auswertungshomomorphismus

$$\mathrm{ev}_{a_1,\dots,a_n}(f) = f(a_1, \dots, a_n).$$

*Beweis.* $I \subseteq \operatorname{Ker}(\mathrm{ev}_{a_1,\dots,a_n})$ da $\mathrm{ev}(X_j - a_j) = a_j - a_j = 0$ für $j = 1, \dots, n$. Sei nun $f \in \operatorname{Ker}(\mathrm{ev}_{a_1,\dots,a_n})$.

$$f = \sum a_{(k_1,\dots,k_n)} X_1^{k_1} \dots X_n^{k_n}$$

Wir schreiben $X_j^{k_j} = (a_j + X_j - a_j)^{k_j} = a_j^{k_j} + \underbrace{k_j a_j^{k_j-1}(X_j - a_j) + \dots}_{\in I}$.

Also gilt $X_j^{k_j} + I = a_j^{k_j} + I$

$$\Rightarrow f + I = \underbrace{\sum a_{(k_1,\dots,k_n)} a_1^{k_1} \dots a_n^{k_n}}_{f(a_1,\dots,a_n)=0} + I \in I$$

Weiters folgt $I = \operatorname{Ker}(\mathrm{ev}_{a_1,\dots,a_n})$

$$\Rightarrow K[X_1, \dots, X_n]/I = K[X_1, \dots, X_n]/\operatorname{Ker}(\mathrm{ev}_{a_1,\dots,a_n}) \cong K$$

ist ein Körper $\Rightarrow$ $I$ ist ein Maximalideal. □

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

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

*Beweis.* Wir werden das Zornsche Lemma verwenden. Hierzu definieren wir

$$X = \{J \subsetneq R \mid J \text{ ist ein Ideal und } I \subseteq J\}$$

und betrachten die Inklusion von Teilmengen als unsere Relation auf $X$. Wir müssen zeugen, dass jede Kette $K$ in $X$ eine obere Schranke besitzt. Falls $K = \varnothing$, dann ist $I \in X$ eine obere Schranke. Sei nun $K$ eine nichtleere Kette in $X$.

Wir behaupten, dass $\widetilde{J} = \bigcup_{J \in K} J$ eine obere Schranke von $K$ in $X$ darstellt. Für jedes $J \in K$ gilt $J \subseteq \widetilde{J}$ nach Definition von $\widetilde{J}$. Weiters gilt:

- $\widetilde{J} \neq R$ weil ($J \in K \Rightarrow 1 \notin J$ ) gilt $1 \notin \widetilde{J}$
- $\widetilde{J} \supseteq I$, weil $K \neq \varnothing$, also ein $J \in K$ existiert, welches nach Definition von $X \supseteq K$ $I$ enthalten muss.
- $\widetilde{J}$ ist auch ein Ideal.
  - $0 \in \widetilde{J}$ da $0 \in I \subseteq \widetilde{J}$
  - Sei $x \in R$ und $a \in \widetilde{J}$, dann gibt es ein $J \in K$ mit $a \in J$. Dies impliziert $xa \in J \subseteq \widetilde{J}$.
  - Sei un $a, b \in \widetilde{J}$, dann gibt es ein $J_a \in K$ mit $a \in J_a$ und $J_b \in K$ mit $b \in J_b$, Da $K$ eine Kette ist, gilt $J_a \subseteq J_b$ oder $J_a \supseteq J_b$ also entweder $a, b \in J_b \Rightarrow a + b \in J_b \subseteq \widetilde{J}$ oder $a, b \in J_a \Rightarrow a + b \in J_a \subseteq \widetilde{J}$.

Somit ist $\widetilde{J}$ eine obere Schranke in $X$. Zusammenfassend folgt $X$ ist induktiv geordnet, also existiert nach dem Zorn'schen Lemma ein maximales Element in $X$, d.h. es existiert ein Ideal $m$, welches $I$ enthält, nicht gleich $R$ ist und so sodass es zwischen $m$ und $R$ kein weiteres Ideal gibt. □

## 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 $a_1, \dots, a_n \in R$. Wir definieren

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

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

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

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

*Beweis von $\subseteq$.* Wir wissen aus der Serie, dass $S[a_1, \dots, a_n]$ ein Unterring ist, der nach Definition $S$ und $a_1, \dots, a_n$ enthält. Auch wissen wir, dass $\mathrm{ev}_{a_1, \dots, a_n}(S[x_1, \dots, x_n])$ ein Unterring ist (da $S[x_1, \dots, x_n]$ ein Ring ist und $\mathrm{ev}_{a_1, \dots, a_n}$ ein Ringhomomorphismus ist). Also tritt $T = \mathrm{ev}_{a_1, \dots, a_n}(S[x_1, \dots, x_n])$ als eine der Mengen im Durchschnitt auf und wir erhalten

$$S[a_1, \dots, a_n] \subseteq \mathrm{ev}_{a_1, \dots, a_n}(S[x_1, \dots, x_n]).$$

□

*Beweis von* $\supseteq$. Wir wissen $S[a_1,\dots,a_n]$ ist ein Unterring. Ebenso haben wir $S$ und $a_1,\dots,a_n$ sind in diesem Unterring enthalten. Folgt

$$\sum_{(k_1,\dots,k_n)\in M} \underbrace{c_{k_1,\dots,k_n}}_{\in S} a_1^{k_1}\dots a_n^{k_n} \subseteq S[a_1,\dots,a_n].$$

Durch variieren von $M \subseteq \mathbb{N}^n, |M| < \infty$ und der Koeffizienten zeigt $\supseteq$. □

**Beispiel.**
- $\mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^n} : a \in \mathbb{Z}, n \in \mathbb{N}\} \subseteq \mathbb{Q}$.
- $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.
- $\mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}b : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$.
- $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ ist ein Körper:

  $$\frac{a+\sqrt{2}b}{\underbrace{c+\sqrt{2}d}_{\neq 0}}\frac{c-\sqrt{2}d}{c-\sqrt{2}d} = \frac{ac-2bd+\sqrt{2}(ad-bc)}{c^2-2d^2}$$

  mit Nenner in $\mathbb{Q}$.

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

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

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 $f = 0$.*

*Beweis.* Sei $f = \sum_{k_1,\dots,k_n} c_{k_1,\dots,k_n} X_1^{k_1} \dots X_n^{k_n}$ ein Polynom für das die zugehörige Polynomfunktion $f : \mathbb{R}^n \to \mathbb{R}, (a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n)$ verschwindet. Dies gilt dann auch für jede partielle Ableitung von $f$. Sei $(l_1, \dots, l_n) \in \mathbb{N}^n$ mit $k_i \geq l_i$ für $i \in \{1, \dots, n\}$. Dann gilt

$$\begin{aligned} 0 &= \partial_{x_1}^{l_1} \dots \partial_{x_n}^{l_n} f(0) \\ &= \sum_{k_1,\dots,k_n} c_{k_1,\dots,k_n} k_1(k_1-1)\dots(k_1-l_1+1) x_1^{k_1-l_1} \dots k_n(k_n-1)\dots(k_n-l_n+1) x_n^{k_n-l_n} \\ &= c_{l_1,\dots,l_n} l_1! \dots l_n! \end{aligned}$$

Da dies für alle $(l_1, \dots, l_n)$ gilt, folgt $f = 0$. □

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

*Beweis der Proposition.* Wir bemerken zuerst, dass

- Jede Eintragung von $A(BC) - (AB)C$ ein Polynom mit ganzzahligen Koeffizienten in den Variablen
$$a_{11}, \dots, a_{mm}, b_{11}, \dots, b_{mm}, c_{11}, \dots, c_{mm}$$
ist.
- $\det(AB) - \det(A)\det(B)$ ein Polynom mit ganzzahligen Koeffizienten in den Variablen $a_{11}, \dots, a_{mm}, b_{11}, \dots, b_{mm}$ ist.
- jede Eintragung von $A\widetilde{A} - (\det(A))I_m$ (oder $\widetilde{A}A - (\det(A))I_m$) ein Polynom mit ganzzahligen Koeffizienten in den Variablen $a_{11}, \dots, a_{mm}$ ist.
- jede Eintragung von $\operatorname{char}_A(A)$ ein Polynom mit ganzzahligen Koeffizienten in den Variablen $a_{11}, \dots, a_{mm}$ ist.

Für $R = \mathbb{R}$ wissen wir, dass diese Polynome ausgewertet an einer beliebigen Stelle gleich Null sind. D.h. mit dem Lemma sind bereits die Polynome gleich Null. Wenn wir den Ringhomomorphismus von $\mathbb{Z}$ nach $R$ auf die Koeffizienten anwenden, erhalten wir wieder das Nullpolynom. $\Rightarrow$ All diese Gleichungen gelten auch für Matrizen über $R$. □

# 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.*

*Beweis.* Angenommen $p \in R \setminus \{0\}$ ist prim und angenommen $p = ab$ (wie in der Definition von irreduzibel). Daraus folgt $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$.
Angenommen $p \mid a$, dann ist $a = p \cdot c$ für ein $c \in R$. Folgt $p = p \cdot c \cdot b \Rightarrow 1 = c \cdot b$ weil $R$ ein Integritätsbereich ist, also $b, c \in R^\times$. Des Weiteren ist auch $p \notin R^\times$. Also ist $p$ irreduzibel. $\square$

*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 $f$).

**Beispiel.** 0) z.B. erfüllt jeder Körper $K$ mit $N(f) = 0$ für alle $f \in K$ diese Axiome (uninteressant, da es hier nur Einheiten und keine irreduziblen oder primen Elemente gibt).

1) Der $R = \mathbb{Z}$ und $N(n) = |n|$ für $n \in \mathbb{Z}$ (erfüllt alle Eigenschaften auf Grund bekannter Eigenschaften von $\mathbb{Z}$ ).
2) Sei $K$ ein Körper, $R = K[x]$ und $N(f) = \deg(f)$ für $f \in R \setminus \{0\}$.
3) Sei $R = \mathbb{Z}[i]$ der Ring der *Gausschen ganzen Zahlen* und $N(a + ib) = |a + ib|^2$
4) Sei $R = \mathbb{Z}[\sqrt{2}]$ und $N(a + \sqrt{2}b) = |a^2 - 2b^2|$ für $a + \sqrt{2}b \in R$ (algebraische Zahlentheorie betrachtet solche Beispiele).

*Beweis von Beispiel* 2.

- Gradungleichung: Seien $f, g \in K[X] \setminus \{0\}$. Dann gilt

$$N(fg) = \deg(fg) = \deg(f) + \underbrace{\deg(g)}_{\geq 0} \geq \deg(f) = N(f).$$

- Division mit Rest: Sei $f \neq 0, g \in R = K[X]$. Dann gibt es $q, r \in K[X]$ mit $g = fq + r$ und $\deg(r) < \deg(f)$.

*Beweis.* Falls $\deg(g) < \deg(f)$, dann setzen wir $q = 0$ $r = g$. Wir verwenden Induktion nach $\deg(g)$. Obiger Fall ist unser Induktionsanfang.
Sei $m \in \mathbb{N}$ und angenommen wir haben Division mit Rest bereits für alle Polynome mit Grad $< m$ bewiesen. Sei $g \in K[X]$ mit Grad $\deg(g) = m$. Aufgrund des Induktionsanfangs haben wir $m \geq \deg(f) =: n$.
Sei $g = g_m X^m + \dots$, $f = f_n X^n + \dots$. Wir definieren

$$\widetilde{g} = g - \underbrace{g_m f_n^{-1} X^{m-m} f}_{\substack{\text{hat führenden Koeffizient } g_m \\ \text{und auch Grad } m \text{ (wie g)}}}.$$

womit $\deg(\widetilde{g}) < \deg(g) = m$. Auf Grund der Induktionsvorraussetzung können wie $\widetilde{q}$ und $\widetilde{r}$ finden, so dass

$$\begin{aligned} \widetilde{g} &= f\widetilde{q} + \widetilde{r} \qquad \deg(\widetilde{r}) < \deg(f) \\ g - g_m f_n^{-1} X^{m-n} f &= f\widetilde{g} + \widetilde{r} \\ g &= f(\underbrace{g_m f_n^{-1} X^{m-1} + \widetilde{q}}_{=q}) + \underbrace{\widetilde{r}}_{=r} \end{aligned}$$

Dies beendet den Induktionsschritt. □

□

**Beispiel** (Bsp für Polynomdivision)**.** $g = x^6 + x^4 + 4x^3 + 2$, $f = x^2 + 5$

$$\begin{array}{ccccccccc}
x^6+ & 0x^5+ & x^4+ & 3x^3+ & 0x^2+ & 0x+ & 2 & : & x^2+5 = x^4 - 4x^2 + 3x \\
-x^6 & & -5x^4 & & & & & & \\
\hline
 & & -4x^4 & +4x^3 & +0x^2 & & +2 & & \\
 & & -4x^4 & & +20x^2 & & & & \\
\cline{3-7}
 & & & 4x^3 & +20x^2 & +0x & +2 & & \\
 & & & -3x^3 & & -15x & & & \\
\cline{4-7}
 & & & & 20x^2 & -15x & +2 & & \\
 & & & & -20x^2 & & -100 & & \\
\cline{5-7}
 & & & & & -15x & -98 & = r &
\end{array}$$

*Beweis von Beispiel* 3 . $R = \mathbb{Z}[i]$ der Ring der Gausschen ganzen Zahlen

$$\begin{aligned} N(a+ib) &= |a+ib|^2 \text{ für } a+ib \in \mathbb{Q}[i] \\ &\in \mathbb{N} \text{ für } a+ib \in \mathbb{Z}[i] \\ N(z \cdot w) &= N(z)N(w) \text{ für } z, w \in \mathbb{Q}[i] \\ N(z) &= 0 \Leftrightarrow z = 0 \text{ multiplikativ} \end{aligned}$$

**Normungleichung:** Sei $z, w \in \mathbb{Z}[i] \setminus \{0\}$. Dann gilt

$$N(zw) = N(z)\underbrace{N(w)}_{\geq 1} \geq N(z).$$

**Lemma.** *Die Division mit Rest gilt in $\mathbb{Z}[i]$.*

*Beweis.* Seien $f, g \in \mathbb{Z}[i], f \neq 0$. Wir definieren $z = \frac{g}{f} \in \mathbb{Q}[i], z = a + ib$ f+r $a, b \in \mathbb{Q}$. Sei $[r] =$

die beste Näherung von $r \in \mathbb{Q}$ innerhalb von $\mathbb{Z}$. Definiere $q = [a] + i[b] \in \mathbb{Z}[i]$. Dann gilt

$$|z - q| \leq \sqrt{\underbrace{(a-[a])^2}_{\leq \frac{1}{2}} + \underbrace{(b-[b])^2}_{\leq \frac{1}{2}}} \leq \frac{1}{\sqrt{2}} \quad \text{und} \quad N(z-q) < 1$$

Definiere $r = g - fq \Rightarrow g = fq + r$. Dann gilt

$$N(r) = |r|^2 = |g - fq|^2 = |f|^2 \underbrace{|z-q|^2}_{<1} < N(f).$$

□

□

*Beweis von Beispiel* 4. Der Ring $R = \mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}b : a, b \in \mathbb{Z}\}$ ist ein euklidischer Ring. Wir definieren $\phi : a + \sqrt{2}b \in \mathbb{Q}[\sqrt{2}] \mapsto \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \in \mathrm{Mat}_{22}(\mathbb{Q})$. Dann ist $\phi$ ein Ringhomomorphismus. In der Tat ist $\phi$ auch $\mathbb{Q}$-linear,

$$\phi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$
$$\phi(\sqrt{2}) = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \phi(\sqrt{2})^2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} = 2I_2 = \phi(\sqrt{2}^2)$$

daraus folgt $\phi(fg) = \phi(f)\phi(g)$ für $f, g \in \mathbb{Q}[\sqrt{2}]$. Wir definieren die Normfunktion

$$N(f) = |\det(\phi(f))| = \left|\det\left(\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\right)\right| = \left|a^2 - 2b^2\right|.$$

mit $f = a + \sqrt{2}b \in \mathbb{Q}[\sqrt{2}]$. Daher gilt $N(fg) = N(f)N(g)$ für $f, g \in \mathbb{Q}[\sqrt{2}]$. Des weiteren gilt $N(f) \geq 1$ für $f \in \mathbb{Z}[\sqrt{2}]$ Folgt die Normungleichung

$$N(fg) = N(f)\underbrace{N(g)}_{\geq 1} \geq N(f)$$

für $g \in \mathbb{Z}[\sqrt{2}] \setminus \{0\}$.

**Lemma.** *In $\mathbb{Z}[\sqrt{2}]$ gilt die Division mit Rest.*

*Beweis.* Seien $f, g \in \mathbb{Z}[\sqrt{2}], f \neq 0$ und $z = \frac{g}{f} = a + \sqrt{2}b \in \mathbb{Q}[\sqrt{2}]$ mit $a, b \in \mathbb{Q}$. Wir definieren $q = [a] + \sqrt{2}[b] \in \mathbb{Z}[\sqrt{2}]$. Dann gilt

$$N(z - q) = \left|(a - [a])^2 - 2(b - [b])^2\right| \leq \frac{1}{4} + 2\frac{1}{4} < 1.$$

Der restliche Beweis läuft analog zu $\mathbb{Z}[i]$. □

□

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

*Beweis.* Sei $I \subseteq R$ ein Ideal in einem Euklidischen Ring $R$. Falls $I = \{0\}$, so ist $I = (0)$ ein Hauptideal. Wir nehmen nun an, dass $I \neq \{0\}$. Wir definieren $f \in I$ als ein Element mit $N(f) = \min\{\underbrace{N(g) : g \in I \setminus \{0\}}_{\subseteq \mathbb{N} \text{ nichtleer}}\}$.

**Behauptung:** $I = (f)$. Da $f \in I$ ist, gilt auch $(f) \subseteq I$. Für die Umkehrung nehmen wir an, dass $g \in I$. Nach Division mit Rest gibt es $q, r \in R$ mit $g = qf + r$ und $r = 0$ oder $N(r) < N(f)$.

Falls $r = 0$ ist, so ergibt sich $g = qf \in (f)$.
Falls $r \neq 0$ ist, so ergibt sich

$$r = \underbrace{g}_{\in I} - q \underbrace{f}_{\in I} \in I$$

mit $N(r) < N(f)$. Aber dies widerspricht der Definition von $f$. Folgt $I = (f)$ wie behauptet und dies ist der Satz. □

## 2.2 Hauptidealring

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

**Beispiel.** Jeder euklidische Ring ist ein Hauptidealring.

*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).

*Beweis.* Da $I = (f) + (g)$ ein Ideal ist und $R$ ein Hauptidealring ist, gibt es ein $d \in R$ mit $I = (d) = (f) + (g)$. Daraus folgt, $(f) \subseteq (d)$ und damit $d \mid f$. Genauso $(g) \subseteq (d)$ und damit $d \mid g$. Also ist $d$ ein gemeinsamer Teiler. Falls $t \in R$ ein weiterer gemeinsamer Teiler von $f$ und $g$ ist, so folgt $(f) \subseteq (t), (g) \subseteq (t)$ und somit $(d) = (f) + (g) \subseteq (t)$ und damit $t \mid d$. Also ist $d$ ein größter gemeinsamer Teiler. □

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.*

*Beweis.* Nach Schritt 0) gilt $\min(N(f), N(g)) = N(f)$. Bei jedem Durchlauf von 1) − 3) wird diese natürliche Zahl echt kleiner. Nach endlich vielen Schritten müssen wir also im Fall 2) sein.

Im Schritt 0) ändern wir $I = (f)+(g)$ nicht. In 1) erhalten wir $q, r \in R$ mit $r = g-qf \in I$, $f \in I$. Außerdem ist $f \in I' = (r) + (f), g = qf + r \in I'$. Dies impliziert $(f) + (g) = I = I' = (r) + (f)$. Also ändert sich das Ideal $I$ nicht während des Algorithmus. Nach endlich vielen Schritten erreichen wir Falls 2) im Algorithmus:

$$I = (f) + (g) = (a) + (b).$$

mit $f, g$ den ursprünglichen Elementen und $a, b$ denen nach endlich vielen Schritten. Nun gilt $b = q \cdot a + \underbrace{0}_{r=0}$ und somit $I = (f) + (G) = (a)$. Mit dem Beweis von der Proposition folgt $a$ ist ein ggT von $f$ und $g$ und $a$ ist dann auch der Output vom Algorithmus. □

**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.*

*Beweis von* 1) . Wir wissen bereits, dass jedes prime Element irreduzibel ist (siehe Lemma in 3.0). Wir nehmen nun an, dass $p \in R \setminus \{0\}$ irreduzibel ist. Wie nehmen weiters an, dass $p \mid ab$ für $a, b \in R$. Falls $p \mid a$, so gibt es nichts zu beweisen. Also nehmen wir an, dass $p \nmid a$.

Sei $d$ ein ggT von $p$ und $a$, also insbesondere ist $d \mid p = d \cdot e$. Da $p$ irreduzibel ist gilt $d \in R^\times$ oder $e \in R^\times$. Angenommen $e \in R^\times$ dann folgt $d = pe^{-1}$ also $p \mid d, d \mid a$ folgt $p \mid a$ was unserer Annahme widerspricht.

Somit ist $d \in R^\times$. $d = xp + ya$ für $x, y \in R$ da dies nach der Proposition in einem Hauptidealring gilt. Multipliziert man dies $bd^{-1}$ so erhält man

$$b = \underbrace{xbd^{-1}p}_{p|-''-} + \underbrace{yd^{-1}ab}_{p|ab}.$$

Somit folgt $p \mid b$. □

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

*Beweis.* Sei $R$ ein Hauptideal Ring und $p \in R$ irreduzibel. Sei $J \subseteq R$ ein Ideal mit $J \supsetneq (p)$. Da $R$ ein Hauptidealring ist, gibt es ein $d \in R$ mit $J = (d) \supsetneq (p)$. Also gibt es ein $c$ mit $p = d \cdot c$. Also folgt $d \in R^\times$ oder $c \in R^\times$ (da $p$ irreduzibel ist).

Falls $c \in R^\times$ ist, so ist $d = p \cdot c^{-1} \in (p)$ und damit $J = (d) = (p)$ - ein Widerspruch zur Annahme an $J$.

Also gilt $d \in R^\times$ und $1 = dd^{-1} \in (d) = J = R$. Da $J \subseteq R$ mit $(p) \subsetneq J$ beliebig war, ist $(p)$ ein Maximalideal. □

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

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

*Beweis.* Wir definieren $J = \bigcup_{n \in \mathbb{N}} J_n$ und erhalten, dass $J$ ein Ideal ist. Da $R$ ein Hauptidealring ist, gibt es also ein $d \in R$ mit $J = (d)$. Also gibt es ein $n \in \mathbb{N}$ mit $d \in J_n$. Daraus folgt

$$J = \bigcup_{i \in \mathbb{N}} J_i = (d) \subseteq J_n \subseteq J_m \subseteq J = (d).$$

für alle $m \geq n$.

$\square$

*Beweis vom Satz über Prime Elemente Eigenschaft 2.* Sei $f \in R \setminus \{0\}$. Für diesen Beweis sagen wir, dass $f$ *zerlegbar* ist. Falls sich $f$ als ein Produkt einer Einheit und endlich vielen ($n \in \mathbb{N}$) irreduziblen Elementen schreiben lässt. Falls $f \in R^\times$ ($n = 0$) oder $f$ irreduzibel ($n = 1$) ist, so ist $f$ zerlegbar.

Wir beweisen die Aussage mit einem Widerspruchsbeweis und nehmen an $f \in R \setminus \{0\}$ sei nicht zerlegbar. Also ist $f$ nicht irreduzibel, $f = f_0 = f_1 \widetilde{f_1}$ wobei $f_1, \widetilde{f_1} \notin R^\times$. Falls $f_1$ und $\widetilde{f_1}$ beider zerlegbar wären, so würde dies auch für $f$ folgen.

O.B.d.A. dürfen wir also annehmen, dass $f_1$ nicht zerlegbar ist. Wir iterieren dieses Argument und erhalten

$$f_0 = f_1 \widetilde{f_1} \quad f_1 = f_2 \widetilde{f_2} \quad f_2 = f_3 \widetilde{f_3} \dots .$$

mit $f_0, f_1, f_2, f_3, \dots$ nicht zerlegbar und $\widetilde{f_1}, \widetilde{f_2}, \widetilde{f_3}, \dots \notin R^\times$.

Es gilt $f_{n+1} \mid f_n$ und daher $(f_n) \subseteq (f_{n+1})$ für alle $n \in \mathbb{N}$. Wir wenden also die Proposition von vorhin an und erhalten, dass es ein $n \in \mathbb{N}$ mit $(f_n) = (f_{n+1})$ gibt. Da $R$ ein Integritätsbereich ist, folgt aus $(f_n) = (f_{n+1})$, dass sich $f_n$ und $f_{n+1}$ multiplikativ um eine Einheit unterscheiden. Also gilt

$$\frac{f_n}{f_{n+1}} = \widetilde{f_{n+1}} \in R^\times,$$

was den Konstruktion von $f_n, \widetilde{f_n}$ widerspricht. Dieser Widerspruch zeigt, dass jedes Element $f \in R \setminus \{0\}$ wie im Satz formuliert zerlegbar ist. $\square$

**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 $\mathbb{Z}[i]$.*

*Beweis.* Angenommen $z = u \cdot v$ ist ein Produkt von $u, v \in \mathbb{Z}[i]$. Dann ist $p = N(z) = \underbrace{N(u)}_{\in \mathbb{N}} \cdot \underbrace{N(v)}_{\in \mathbb{N}}$ und daher $N(u) = 1$ ($u \in \mathbb{Z}[i]^\times$ ) oder $N(v) = 1$ ($v \in \mathbb{Z}[i]^\times$ ). $\square$

**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 $\mathbb{Z}[i]$.*

*Beweis.* Wir zeigen, dass $p$ in $\mathbb{Z}[i]$ irreduzibel ist. Also angenommen $p = z \cdot w$ für $z, w \in \mathbb{Z}[i]$. Dann folgt $N(p) = N(z)N(w) = p^2$ und damit $N(z) \mid p^2$ in $\mathbb{N}$, womit $N(z)), N(w) \in \{1, p, p^2\}$ ist. Dabei ist aber $N(z) = N(a+ib) = a^2 + b^2 = p$ nicht möglich. Also gilt $N(z), N(w) \in \{1, p^2\}$ und es folgt $N(z) = 1$ (und $N(w) = p^2$ ) oder $N(w) = 1$ (und $N(z) = p^2$ ). Also ist $z \in \mathbb{Z}[i]^\times$ oder $w \in \mathbb{Z}[i]^\times$. $\square$

**Beispiel.** Im Ring der Polynome $K[x]$ mit einer Variable über einem Körper $K$ gibt es irreduzible Elemente:

Grad 1: jedes Polynom vom Grad 1 ist irreduzibel.

Grad 2: ein Polynom vom Grad 2 ist irreduzibel genau dann wenn es keine Nullstellen im Körper $K$ hat.

Grad 3: selbes wie bei Grad 2.

Grad 4: das betrachten von Nullstellen ist nicht mehr ausreichend.

Dies hängt stark vom Körper $K$ ab.

## 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.

**Beispiel.** Jeder Euklidische und jeder Hauptidealring. Es gibt noch weitere Bsp, wir werden zeigen, dass z.B. $\mathbb{Z}[x, y, z]$ ein faktorieller Ring ist.

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

*Beweis.* $\Leftarrow$: ✓schon gezeigt
$\Rightarrow$: Sei also $p$ irreduzibel. Dann ist $p = u \cdot q_1, \ldots, q_n$ ein Produkt einer Einheit $u \in R^\times$ und Primelementen $q_1, \ldots, q_n \in R$ nach Annahme an $R$. Da $p$ irreduzibel ist folgt $n = 1$ und $(p) = (q_1)$, womit $(p)$ ein Primideal ist und $p$ selbst ein Primelement 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 $R$.*

*Beweis.*
- $a \sim a$ da $a = 1 \cdot a$ und $1 \in R^\times$.
- $a \sim b \Rightarrow b \sim a$: Gilt $a = ub \Rightarrow b = u^{-1}b$ mit $u^{-1} \in R^\times$-
- $a \sim b$ und $b \sim c \Rightarrow a \sim c$ : Gilt $a = ub$ und $b = vc \Rightarrow a = (uv)c$ mit $uv \in R^\times$. Also $a \sim c$.

□

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

*Beweis.* Nach Annahme gibt es ein $a \in R$ mit $q = a \cdot p$. Da $q$ irreduzibel ist folgt $a \in R^\times$ oder $p \in R^\times$. Da $p$ irreduzibel ist, kann $p \in R^\times$ nicht gelten. Also ist $a \in R^\times$ und $p \sim q$. □

**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 $p_1, \dots p_m$ die Primfaktorzerlegung von $a$.

*Beweis der Eindeutigkeit.* Angenommen $a = up_1 \dots p_m = vq_1 \dots q_n$ mit $u, v \in R^\times, m, n \in \mathbb{N}$ und $p_1, \dots, p_m, q_1, \dots, q_n$ Primelemente in $R$. Falls $n = 0$ ist, so ist $a = v \in R^\times$. Daraus folgt aber auch $m = 0$ (Falls $m > 0$ wäre, so folgt mit $p_1 \mid a$ und $a \mid 1$ dass $p_1 \mid 1$ - ein Widerspruch zur Annahme an $p_1$ prim).

Wir verwenden Induktion nach $n$ und nehmen an, dass die Eindeutigkeit bereits gilt falls eine der beiden Zerlegungen weniger als $n$ Faktoren besitzt. Wir nehmen an $n > 0$. Da $a = up_1 \dots p_m = vq_1 \dots q_n$ gilt $q_n \mid a$. Da $q_n$ ein Primelement von $R$ ist, gibt es einen Index $i = \sigma(n)$, so dass $q_n \mid p_{\sigma(n)}$. Nach einem Lemma vom letzten Mal folgt daraus $q_n \sim p_{\sigma(n)}$. Wir verwenden nun die Induktionsannahme für

$$\frac{a}{q_n} = \underbrace{u\frac{p_{\sigma(n)}}{q_n}}_{\in R^\times} p_1 \cdots p_{\sigma(n)-1} p_{\sigma(n)+1} \cdots p_m = vq_1 \cdots q_{n-1}.$$

Es folgt $n - 1 = m - 1$ und es gibt eine Bijektion

$$\sigma : \{1, \dots, n-1\} \to \{1, \dots, \sigma(n) - 1, \sigma(n) + 1, \dots, m\}$$

so dass $q_j \sim p_{\sigma(j)}$ für $j = 1, \dots, n-1$. Dies gilt auch für $j = n$. Dies beendet den Induktionsschritt. □

**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 $q \sim p$.

**Beispiel.** Für $R = \mathbb{Z}$ betrachten wir $P = \{p \in \mathbb{Z} \text{ prim und positiv}\}$. Für $R = K[x]$ betrachten wir

$$P = \{f \in K[x] \text{ irreduzibel und } f \text{ normiert}\}.$$

Normiert: Der führende Koeffizient von $f$ ist gleich 1.
Für $R = \mathbb{Z}[i]$ verwenden wir $P = \{a + ib : a, b \in \mathbb{Z}, a + ib \text{ prim und } -a < b \leq a\}$

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

*Beweis.* Wir verwenden das Auswahlaxiom für die Menge $\{[p]_\sim : p \in R \text{ prim}\}$ und erhalten $P$ als Bild der Auswahlfunktion. □

**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 $p \in P$.*

*Beweis der Existenz.* Falls $a \in R^\times$ so setzen wir $u = a$ und $n_p = 0$ für alle $p \in P$. Ansonsten ist $a = up_1 \dots p_n$, wie in der Definition von faktoriellen Ringen. Zu jedem $p_j$ gibt es ein eindeutig bestimmtes $p \in P$ mit $p_j \sim p$. Damit erhalten wird

$$a = \underbrace{u \frac{p_1 \cdots p_m}{\prod_{p \in P} p^{n_p}}}_{\in R^\times} \prod_{p \in P} p^{n_p}$$

wobei $n_p = \#j$ mit $p_j \sim p$. $\square$

*Beweis der Eindeutigkeit.* Angenommen $a = u\prod_{p\in P} p^{n_p} = v\prod_{p\in P} p^{n'_p}$. Falls $n'_p = 0$ für alle $p \in P$, so ist $a = v \in R^\times$ und $n_p = 0$ für alle $p \in P$ und $a = u$.

Ansonsten ist $n'_p > 0$ für ein $p_0 \in P$ und daher gilt $p_0 \mid a = u\prod_{p\in P} p^{n_p}$, was $n_{p_0} > 0$ impliziert auf Grund der Eigenschaften der Repräsentantenmenge. Wir verwenden Induktion nach $\sum_{p\in P} n'_p$. $\square$

**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. $m_p \le n_p$ für alle $p \in P$.*

*Beweis.* „$\Rightarrow$“: $b = ac$ und $c = w\prod_{p\in P} p^{k_p}$. Dann folgt

$$v\prod_{p\in P} p^{n_p} = b = uw\prod_{p\in P} p^{m_p+k_p}$$

und daher $n_p = m_p + k_p \ge m_p$ für alle $p \in P$.

„$\Leftarrow$“: Wir definieren $c = vu^{-1}\prod_{p\in P} p^{n_p-m_p} \in R$. Dann gilt

$$ac = u\prod_{p\in P} p^{m_p} \cdot vu^{-1}\prod_{p\in P} p^{n_p-m_p} = v\prod_{p\in P} p^{n_p} = b.$$

also $a \mid b$. $\square$

**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 $b$.*

*Beweis.* Wir haben $d \mid a$ und $d \mid b$ auf Grund des Lemmas. Falls $t = w\prod_{p\in P} p^{k_p}$ ein weiterer gemeinsamer Teiler von $a$ und $b$ ist, so folgt $k_p \le m_p$, $k_p \le n_p$ und damit $k_p \le \min(m_p, n_p)$ für alle $p \in P$. Daraus folgt $t \mid d$. $\square$

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

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

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

*Beweis.* Angenommen $x = \frac{\widetilde{a}}{\widetilde{b}} \in K$ und sei $d$ der ggT von $\widetilde{a}$ und $\widetilde{b}$. Wir definieren $a = \frac{\widetilde{a}}{d}$ und $b = \frac{\widetilde{b}}{d}$ und erhalten, dass $a, b$ coprim sind und

$$x = \frac{\widetilde{a}}{\widetilde{b}} = \frac{\frac{\widetilde{a}}{d}}{\frac{\widetilde{b}}{d}} = \frac{a}{b}.$$

$\square$

**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.*

**Beispiel** (Ein Gegenbeispiel)**.** Wir definieren $R = \mathbb{Z}[i\sqrt{5}] \subseteq K = \mathbb{Q}[i\sqrt{5}] \subseteq \mathbb{C}$. Also $R = \{a + i\sqrt{5}b : a, b \in \mathbb{Z}\}$. Zerlegungen der 6 :

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

1. Behauptung: $2, 3, 1 \pm i\sqrt{5}$ sind alle irreduzibel in $R$.
2. Behauptung: $2 \not\sim 1 \pm i\sqrt{5}$ und $3 \not\sim 1 \pm i\sqrt{5}$.

*Beweis der 2. Behauptung.*

$$\frac{1 \pm i\sqrt{5}}{2} = \frac{1}{2} \pm i\sqrt{5}\frac{1}{2} \notin R \quad \text{und} \quad \frac{1 \pm i\sqrt{5}}{3} = \frac{1}{3} \pm i\sqrt{5}\frac{1}{3} \notin R.$$

Folgt die 2. Behauptung. □

**2 ist irreduzibel:**
Angenommen $2 = z \cdot w$, $z, w \in R$. Wir verwenden die Normfunktion $N(a+i\sqrt{5}b) = \left|a + i\sqrt{5}b\right|^2 = a^2 + 5b^2$ für $a + i\sqrt{5}b \in R$ hat diese Normfunktion Werte in $\mathbb{N}$.

$$\Rightarrow 4 = N(2) = N(z)N(w) \Rightarrow N(z), N(w) \in \{1, 2, 4\}.$$

2 kann nicht sein also $\{N(z), N(w)\} = \{1, 4\}$. Falls $N(z) = 1$ ist, so ist $z \pm 1$ eine Einheit in $R$. Analog für $N(w) = 1$.

**3 ist irreduzibel:**
Analog: $N(z) = 3 = a^2 + 5b^2$ ist nicht möglich.

**Auch $1 \pm i\sqrt{5}$ sind irreduzibel:**
$1 \pm i\sqrt{5} = zw \Rightarrow N(1 \pm i\sqrt{5}) = 6 = N(z)N(w) \Rightarrow N(z)N(w) \in \{1, \cancel{2, 3}, 6\}$ Also ist $z$ oder $w$ eine Einheit in $R$.

Beispiele dieser Art führten zur Erfindung von „idealisierten Primfaktoren“ (heute Primideale). $(6) = (2, 1 + i\sqrt{5})^2(3, 1 + i\sqrt{5})(3, 1 - i\sqrt{5})$

## 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.

*Beweis.* Wir definieren $\mathrm{ev}_{\sqrt{d}} : \mathbb{Q}[x] \to K, f \mapsto f(\sqrt{d})$. $\mathrm{ev}_{\sqrt{d}}(x^2 - d) = 0$. Da $x^2 - d$ keine Nullstellen in $\mathbb{Q}$ hat (Annahme an $d$), ist $x^2 - d$ irreduzibel/prim in $\mathbb{Q}[x]$. Daher folgt $(x^2 - d)$ ist ein Maximalideal. Gemeinsam mit $(x^2 - d) \subseteq \mathrm{Ker}(\mathrm{ev}_{\sqrt{d}})$, erhalten wir $(x^2 - d) = \mathrm{Ker}(\mathrm{ev}_{\sqrt{d}})$. Der erste Isomorphiesatz ergibt nun

$$\mathbb{Q}[x]/(x^2 - d) = \mathbb{Q}[x]/\mathrm{Ker}(\mathrm{ev}_{\sqrt{d}}) \overset{\varphi_+}{\cong} \mathbb{Q}[\sqrt{d}] = K.$$

Beweis Körperautomorphismus:

$$\begin{tikzcd} K \arrow[r, "\varphi_+"] \arrow[rr, bend right, "\tau"] & \mathbb{Q}[x]/(x^2-d) \arrow[r, "\varphi_-"] & K \end{tikzcd}$$

$$\sqrt{d} \longmapsto X + (x^2+d) \longmapsto -\sqrt{d}$$

Wobei der Isomorphismus $\varphi_+$ Auswertungen bei $\sqrt{d}$ verwendet und analog dazu der Isomorphismus $\varphi_-$ Auswertungen bei $\sqrt{-d}$ verwendet. □

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.*

*Beweis.* Seien $f, g \in R, f \neq 0$. Wir definieren $z = \frac{g}{f} \in \mathbb{Q}[\sqrt{d}] = a + b\sqrt{d}$ mit $a, b \in \mathbb{Q}$. Wir definieren $q = \underbrace{[a]}_{\in\mathbb{Z}} + \underbrace{[b]}_{\in\mathbb{Z}}\sqrt{d} \in R$ als die beste Approximation. Dann gilt

$$\phi(z-q) = |N(z-q)| = \left|(\underbrace{a-[a]}_{\le\frac{1}{2}})^2 - d(\underbrace{b-[b]}_{\le\frac{1}{2}})^2\right| \le \frac{1}{4} + |d|\frac{1}{4} < 1 \qquad (*)$$

für $d = -1, -2, 2$. Für $d = 3$ gilt in $(*)$ Gleichheit, aber da die beiden Ausdrücke im Absolutbetrag verschiedene Vorzeichen haben, gilt auch hier $\phi(z-q) < 1$.
Wir definieren $r = g - f \cdot q \in \mathbb{Z}[\sqrt{d}]$, und erhalten $g = fq + r$ und

$$\phi(r) = |N(r)| = |N(g - f \cdot q)| = |N(f)N(z-q)| < |N(f)| = \phi(f).$$

□

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 $R$.*

*Beweis von Lemma 1.* Sei $u \in R^\times$. Dann gibt es $v \in R^\times$ mit $uv = 1$. Daraus folgt $\underbrace{N(u)}_{\in\mathbb{Z}}\underbrace{N(v)}_{\in\mathbb{Z}} = N(uv) = 1$ und daher $N(u) = \pm 1$.

Angenommen $u \in R$ erfüllt $N(u) = \pm 1$. Dann gilt $u \cdot (\pm\tau(u)) = \pm N(u) = 1$ also $u^{-1} = \pm\tau(u)$. $\square$

*Beweis von Lemma 2.* Angenommen $z \in R$ erfüllt $N(z) = p$, wobei $p \in \mathbb{Z}$ eine Primzahl ist. Angenommen $z = v \cdot w$ für $v, w \in R$. Dann folgt $p = N(z) = N(v)N(w)$. Da $p \in \mathbb{Z}$ irreduzibel in $\mathbb{Z}$ ist, folgt daraus $\underbrace{N(v) = \pm 1}_{v \in R^\times}$ oder $\underbrace{w = \pm 1}_{w \in R^\times}$. $\square$

*Beweis von Lemma 3.* Sei $p \in \mathbb{Z}$ prim und weder $p$ noch $-p$ eine Norm. Angenommen $p = vw$ für $v, w \in R$. Dann folgt $p^2 = N(p) = N(v)N(w)$. Da $p$ eine Primzahl ist folgt daraus $N(v), N(w) \in \{\pm 1, \pm p, \pm p^2\}$. Wobei $\pm p$ nach Annahme nicht auftritt. Also gilt $\underbrace{N(v) = \pm 1}_{v \in R^\times}$ (und $N(w) = \pm p^2$) oder $\underbrace{N(w) = \pm 1}_{w \in R^\times}$ (und $N(v) = \pm p^2$ ). $\square$

**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*

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

*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 $(p-1)! \equiv -1 \mod p$ .*

*Beweis.*

$$(p-1)! = \prod_{k=1}^{p-1} k \overset{(*)}{=} 1 \cdot \left( \prod_{\substack{1<a<p<p-1 \\ a \cdot b = 1 \mod p}} (ab) \right) \cdot (p-1) \equiv -1 \mod p.$$

Wann gilt $x = x^{-1}$ für $x \in \mathbb{F}_p^\times$?

$$x = x^{-1} \Leftrightarrow x^2 = 1 \Leftrightarrow x^2 - 1 = 0 \Leftrightarrow (x+1)(x-1) = 0 \Leftrightarrow x = \pm 1$$

in $\mathbb{F}_p$ ist. Dies beweist $(*)$. $\square$

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

**Beispiel.** $p = 5, x = 2 \Rightarrow x^2 = 4 = -1$ in $\mathbb{F}_5$.
$p = 13, x = 5 \Rightarrow x^2 = 25 = -1$ in $\mathbb{F}_{13}$.

*Beweis.* Wir definieren $x = \left(\frac{p-1}{2}\right)!$ in $\mathbb{F}_p$. Dann gilt

$$x^2 = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \left(p - \frac{1}{2}\right) \cdot \underbrace{\left(\frac{p-1}{2}\right) \ldots \cdot 3 \cdot 2 \cdot 1}_{\frac{p-1}{2}-\text{Faktoren}} \cdot (-1)^{\frac{p-1}{2}}.$$

und $\frac{p-1}{2}$ ist gerade.

$$\begin{aligned}
&= 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \left(\frac{p-1}{2}\right)\left(-\frac{p-1}{2}\right) \ldots (-3) \cdot (-2) \cdot (-1) \\
&= 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right) \ldots (p-3) \cdot (p-2) \cdot (p-1) \\
&= (p-1)! = -1 \text{ in } \mathbb{F}_p.
\end{aligned}$$

□

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

*Beweis.* Wir betrachten $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[x]/(x^2+1)$, $a+ib+(p) \mapsto a+bX \mod p$. Aber $x^2+1$ ist über $\mathbb{F}_p$ nicht irreduzibel, da $x^2+1$ zwei Nullstellen in $\mathbb{F}_p$ hat (siehe Proposition). Also ist $\mathbb{Z}[i]/(p)$ kein Integritätsbereich und $p$ kein Primelement. □

*Alternativer Beweis.* Angenommen $a \in \mathbb{Z}$ erfüllen $a^2 \equiv -1 \mod p$. Insbesondere gilt damit $p \mid (a^2+1) = (a^2-i^2) = (a+i)(a-i)$. Da aber $a \in \mathbb{Z}$ ist, gilt $p \nmid (a+i)$ und $p \nmid (a-i)$. □

*Beweis der Beschreibung der Primzahlen in $\mathbb{Z}[i]$.* $N(1+i) = 2$ und Lemma 2 zeigt, dass $1+i$ irreduzibel , also prim, ist. Angenommen $p \in \mathbb{N}$ ist kongruent $3 \mod 4$. Dann gilt

$$p \not\equiv a^2 + b^2 \in \{0, 1, 2 \mod 4\}$$

für $a, b \in \mathbb{Z}$ gilt $a^2 \equiv 0, 1 \mod 4$. Also ist $p$ (und auch $-p$ ) keine Norm $N(a+ib) = a^2+b^2 > 0$ eines Elements von $Z[i]$. Lemma 3 zeigt also, dass $p$ eine Primzahl in $\mathbb{Z}[i]$ ist.

Sei nun $p \in \mathbb{N}$ kongruent $1 \mod 4$ und prim in $\mathbb{Z}$. Dann ist $p$ keine Primzahl in $\mathbb{Z}[i]$ wegen dem Korollar. Also kann Lemma 3 nicht angewendet werden und daher gibt es ein $z \in \mathbb{Z}[i]$ mit $\underbrace{N(z)}_{>0} = p$. Anders formuliert haben wir also $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$ gefunden. O.B.d.A. dürfen wir $a, b \in \mathbb{N}$ und $b < a$ annehmen. Dann gilt $a+ib, a-ib \in P$, $p = (a+ib)(a-ib)$ und $a \pm ib$ sind nicht assoziiert, da $\pm 1, \pm i$ die einzigen Einheiten sind und der Winkel zwischen $a+ib$ und $a-ib$ echt kleiner als $90°$ ist.

Wir zeigen noch, dass obige drei Fälle alle Primzahlen in $P \subseteq \mathbb{Z}[i]$ liefern. Angenommen $z \in \mathbb{Z}[i]$ ist eine Primzahl. Dann ist $n = N(z) = z\overline{z}$ eine natürliche Zahl. Sei $p \in \mathbb{N}$ ein Primfaktor von $n$.

- $p = 2 \Rightarrow 2 = (1+i)(1-i) \mid n = z\overline{z} \Rightarrow (1+i) \mid z\overline{z} \Rightarrow 1+i \mid z$ oder $1+i \mid \overline{z}$. Folgt $1-i \mid z$. Also $1+i \sim z$ und $1+i \sim 1-i \sim z$.
- $p \equiv 3 \mod 4$: Und $p \mid z\overline{z}$ und $p$ ist prim in $\mathbb{Z}[i]$. Also $p \mid z$ oder $p \mid \overline{z}$. Und somit $p \sim z$.
- $p \equiv 1 \mod 4$: $(a+ib) \mid p = (a+ib)(a-ib) \mid z\overline{z}$. Folgt $a+ib \mid z \Rightarrow a+ib \sim z$ oder $a+ib \sim \overline{z} \Rightarrow a-ib \mid z \Rightarrow a-ib \sim z$.

□

**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.*

*Beweis Skizze.* $z = \frac{g}{f} = (a+\frac{1}{2}) + (b+\frac{1}{2})\sqrt{3}i$, $a, b \in \mathbb{Z}$ hat Abstand 1 zu allen Elementen von $\mathbb{Z}[\sqrt{3}i]$. Beweis scheitert für $R_{falsch}$.

Aber in diesem Fall ist $z \in R_{richtig}$ und deswegen hat es Abstand 0 zu sich selbst. Beweis klappt nun .

□

## 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 $I(f) \sim 1$.

**Beispiel.** Sei $R = \mathbb{Z}$. Dann ist $I(2x+2) \sim 2$ und $3x+2$ ist primitiv.

**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.*

*Beweis.* Sei $f = \sum_{i=0}^n \underbrace{a_i}_{\in K} x^i \in K[x] \setminus \{0\}$ und $a_i = \frac{b_i}{c_i}$ für $b_i, c_i \in R, c_i \neq 0$ für $i = 0, \dots, n$. Wir definieren

$$g = \left(\prod_{i=0}^n c_i\right) f \in R[x]$$

Sei $\underbrace{d}_{\in R} \sim I(g)$ ein ggT der Koeffizienten von $g$. Dann ist $g = d' g^*$ für ein primitives $g^* \in R[x]$.

$$\Rightarrow f = \underbrace{\frac{d'}{\prod_{i=0}^n c_i}}_{d} \underbrace{g^*}_{f^*} \quad \text{mit} \quad d \in K^\times, f^* \in R[x] \text{ primitiv.}$$

Wir erhalten die Existenzaussage im Lemma.

Sei nun $f = d_1 f_1^* = d_2 f_2^*$. Wir schreiben $\frac{d_1}{d_2} = \frac{a_1}{a_2}$ mit $a_1, a_2 \in R$ coprim.

$$f_2^* = \frac{d_1}{d_2} f_1^* = \frac{a_1}{a_2} f_1^* \Rightarrow a_1 f_1^* = a_2 f_2^* \Rightarrow a_1 \sim I(a_1 f_1^*) \sim I(a_2 f_2^*) \sim a_2.$$

Aus $a_1, a_2$ coprim folgt nun $a_1 \sim 1 \sim a_2$.

Wir haben also $\frac{d_1}{d_2} \in R^\times$ gezeigt was genau $d_1 \sim_R d_2$ und $f_1^* \sim_R f_2^*$ 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 $\Phi(X) = X$).

*Beweis.* Wir zeigen zuerst die zweite Aussage der Proposition. Seien also $f, g \in R[x]$ primitive Polynome. Sei $p \in R$ ein Primelement. Dann gilt $f \mod p \neq 0$ und $g \mod p \neq 0$. Da $p$ ein Primelement ist, ist $R/(p)$ ein Integritätsbereich. Daraus folgt, dass $R/(p)[x]$ auch ein Integritätsbereich ist. Daher ist also

$$(fg) \mod p = f \mod p \, g \mod p \neq 0.$$

Anders formuliert, sind also nicht alle Koeffizienten von $fg$ durch $p$ teilbar. Da $p \in R$ ein beliebiges Primelement war, sehen wir, dass $fg$ ein primitives Polynom ist.

Seien nun $f, g \in K[x] \setminus \{0\}$ beliebig. Dann gilt $f = af^*, g = bg^*$ für $a \sim I(f), b \sim I(g)$, $f^*, g^* \in R[x]$ primitiv.

$$\Rightarrow fg = ab \underbrace{f^* g^*}_{\in R[x]}$$

ist primitiv. Aus der Eindeutigkeit im Lemma folgt nun $I(fg) \sim_R ab \sim_R I(f)I(g)$ □

**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 $K[x]$.*

*Beweis.* Wir zeigen zuerst, dass die beiden Typen von Primelementen im Satz tatsächlich Primelemente von $R[x]$ sind.

- Sei $p \in R$ ein Primelement. Dann ist

  $$R[x]/(p)_{R[x]} \cong R/(p)_R[x]. \qquad (*)$$

  Warum: $\Phi : R[x] \to R/(p)_R[x], f \mapsto f \mod p$ ist ein Ringhomomorphismus. Der Kern von $\Phi$ besteht aus allen $f \in R[x]$ so dass $p$ alle Koeffizienten teilt - oder aus $\mathrm{Ker}(\Phi) = (p)_{R[x]}$. Also folgt $(*)$ aus dem ersten Isomorphiesatz.
  Da $R/(p)_R[x]$ ein Integritätsbereich ist, folgt, dass $p \in R[x]$ ein Primelement ist.
- Sei $f \in R[x]$ primitiv und als Element von $K[x]$ irreduzibel. Wir wollen zeigen, dass $f$ ein Primelement in $R[x]$ ist.
  Angenommen $f \mid gh$ in $R[x]$ für $g, h \in R[x]$. Folgt $f \mid gh$ in $K[x]$, da $gh = qf$ für $q \in R[x] \subseteq K[x]$. Da $f \in K[x]$ irreduzibel/prim ist, folgt $f \mid g$ oder $f \mid h$. O.B.d.A. nehmen wir an $f \mid g$. Dann existiert ein $q \in K[x]$ mit $g = qf$. Aus der Proposition folgt

  $$I(q) \sim_R I(q) \underbrace{I(f)}_{\sim_R 1} \sim_R I(qf) \sim_R I(g) \in R$$

  also auch $I(q) \in R$. Da $q \sim I(q)q^*$ folgt also $q \in R[x]$. Wir sehen also $f \mid g$ in $R[x]$.
  Also sehen wir, dass $f$ ein Primelement von $R[x]$ ist.

Als nächstes wollen wir zeigen, dass jedes irreduzible Element $f \in R[x]$ ein Element vom Typ 1 oder Typ 2 wie im Satz ist. Da diese Elemente bereits als Primelemente in $R[x]$ bekannt sind, folgt daraus insbesondere dass alle irreduziblen Elemente in $R[x]$ auch Primelemente sind.

Sei also $f \in R[x]$ irreduzibel.

- Falls $\deg(f) = 0$ ist, so ist $f \in R$ irreduzibel ($R[x]^\times = R^\times$). Also ist $f \in R$ prim nach Annahme an $R$ und $f$ ist vom Typ 1 und prim in $R[x]$.
- Sei nun $\deg(f) > 0$. Daraus folgt $f$ ist primitiv. Wir müssen zeigen, dass $f$ als Element von $K[x]$ irreduzibel ist. Dann ist $f$ vom Typ 2 und prim in $R[x]$.
  Angenommen $f = gh$ für $g, h \in K[x]$. Nach einem früheren Lemma gilt $g = cg^*, h = dh^*$ $c, d \in K, g^*, h^* \in R[x]$ primitiv. $\Rightarrow f = (cd)g^*h^*$, wobei $g^*, h^*$ primitiv ist (siehe frühere Proposition). $I(f) \sim 1 \sim cd$, womit $cd \in R^\times$. Also ist $f = (cdg^*)h^*$ eine Zerlegung von $f$ als Produkt von $cdg^* \in R[x]$ und $h^* \in R[x]$. Da $f$ in $R[x]$ irreduzibel ist, ist $cdg^*$ oder $h^*$ eine Einheit in $R[x]$. Dies zeigt, dass $f$ in $K[x]$ irreduzibel ist.

Es bleibt zu zeigen, dass jedes $f \in R[x] \setminus \{0\}$ ein endliches Produkt von endlich vielen Primelementen von $R[x]$ ist. Auf Grund des früheren Lemmas gilt $f = df^*$, wobei $d \in R \setminus \{0\}$ und $f^* \in R[x]$ primitiv ist. $d \in R \setminus \{0\}$ ist dabei ein endliches Produkt von Primelementen in $R$ (welche Primelemente in $R[x]$ vom Typ I sind und einer Einheit) - weil $R$ faktoriell ist. $f^* \in R[x]$ ist ein endliches Produkt von Primelementen vom Typ II und einer Einheit - wir können dies mittels Induktion nachdem Grad beweisen.
$\deg(f^*) = 0 \Rightarrow f^* \in R^*$ (Produkt ohne Primfaktoren)
$\deg(f^*) = 1 \Rightarrow f^*$ ist selbst irreduzibel, da $f^*$ primitiv ist und als Element von $K[x]$ irreduzibel ist.

Falls die Aussage für alle primitiven Elemente vom Grad kleiner als $\deg(f^*)$ von bekannt ist, so unterscheiden wir die Fälle

- $f^*$ ist irreduzibel ✓.
- $f^* = gh$ für $g, h \in R[x]$ (automatisch primitiv) beide nicht Einheiten.

Nach Induktionsannahme sind daher sowohl $g$ als auch $h$ endliche Produkte von Primelementen, womit dies auch für $f^*$ gilt. □

**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*

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

*Beweis.* $\Leftarrow$: Falls $\deg(f) \in \{2, 3\}$ und $f = gh$, $g, h \notin K[x]^\times$, dann gilt $\deg(f) = \deg(g) + \deg(h)$ und daher ist mindestens ein Faktor von Grad 1. Falls $\deg(g) = 1$ ist, so hat $g$ eine Nullstelle und $f(x) = g(x)h(x)$ ebenso.

$\Rightarrow$: Falls $f$ irreduzibel ist, so kann $f$ wegen dem Lemma keine Nullstelle haben. □

**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.*

*Beweis.* Wir müssen $\Rightarrow$ beweisen. Nach obigem Satz gibt es für jedes $f \in \mathbb{R}[x]$ mit $\deg(f) > 0$ eine Nullstelle $z \in \mathbb{C}$. Falls $z = a \in R$ ist, so folgt $(x-a)|f(x)$ also $f(x) \sim (x-a)$. Falls $z \notin \mathbb{R}$ ist, so folgt $0 = \overline{0} = \overline{f(z)} = f(\overline{z})$. Daher hat $f(x)$ in $\mathbb{C}[x]$ die Teiler $x - z$ und $x - \overline{z}$.

$$\Rightarrow (x-z)(x-\overline{z}) = (x^2 - (\underbrace{z+\overline{z}}_{2\operatorname{Re}(z)})x + \underbrace{\overline{z}z}_{|z|^2}) \mid f(x) \text{ in } \mathbb{C}[x]$$

und auch in $\mathbb{R}[x]$ z.B. wegen der Polynomdivision. Daher gilt $f(x) \sim (x^2 - (2\operatorname{Re}(z)x + |z|^2)$ und $\deg(f) = 2$, $f$ hat keine reellen Nullstellen. ☐

**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* $f$*.*

*Beweis.* Wir nehmen an $f(\frac{a}{b}) = 0$ an. Also gilt $(x - \frac{a}{b}) \mid f(x)$ in $K[x]$. Und auch $(bx - a) \mid f(x)$ in $K[x]$. Dann gilt sogar $(bx - a) \mid f(x)$ in $R[x]$.

Denn: Angenommen $f(x) = (bx - a)h(x)$ für $h(x) \in K[x]$. Für den Inhalt der Polynome gilt daher $I(f) \in R$.

$$I(f) = I((bx-a)h(x)) \sim I(bx-a)I(h) \sim I(h) \in R(h = ch^*, c \sim I(h)).$$

Also folgt $h(x) \in R[x]$ und daher $(bx - a) \mid f(x)$ in $R[x]$.

Also $f(x) = (bx-a)h(x)$ für $h(x) \in R[x]$. $\Rightarrow$ führende Koeffizient von $f = b\cdot$(führender Koeffizient von $h$). Und Konstanter Term von $f = -a \cdot$ (konstanter Term von $h$). ☐

**Beispiel.** Für welche $a \in \mathbb{Z}$ ist $f_a(x) = x^2 + ax + 1 \in \mathbb{Z}[x]$ irreduzibel?
Wegen der Proposition ist eine Nullstelle von $f_a(x)$ in $\mathbb{Q}$ automatisch $\pm 1$ ($f_a(\frac{p}{q}) = 0 \Rightarrow p \mid 1, q \mid 1 \Rightarrow \frac{p}{q} = \pm 1$ ).

$$f_a(1) = 2 + a1 = 0 \Leftrightarrow a = -2 \qquad f_a(-1) = 2 - a = 0 \Leftrightarrow a = 2.$$

Hier ist $f_a$ reduzibel. Für $a \in \mathbb{Z} \setminus \{\pm 2\}$ ist $f_a \in \mathbb{Z}[x]$ irreduzibel ($f_a$ ist primitiv und $f_a \in \mathbb{Q}[x]$ ist irreduzibel da $f_a$ keine Nullstellen hat).

**Beispiel.** Sei $K$ ein Körper. Dann ist $f(x,y) = y^3 - x^5 \in K[x,y]$ irreduzibel. In diesem Fall wollen wir das Diskutierte für $R = K[x]$ verwenden und den Polynomring $R[y]$. Wir bemerken zuerst, dass $f \in R[y]$ primitiv ist (da $f$ als Polynom in $y$ normiert ist und Koeffizienten in $K[x]$ besitzt). Daher (Korollar von Satz von Gauss) ist $f \in R[y]$ irreduzibel gdw. $f$ als Element von $\underbrace{\operatorname{Quot}(R)}_{K[x]}[y]$ irreduzibel ist.

Wir nehmen an, $f$ ist nicht irreduzibel als Element von $K(x)[y]$. Also muss $f$ eine Nullstelle in $K(x)$ besitzen. Seien $p, q \in K[x]$ coprim, $q \neq 0$ mit $f(\frac{p}{q}) = 0$. Folgt $q \mid 1$. Also o.B.d.A. $q = 1$ und $f(p) = 0$, $f(y) = y^3 - x^5 \Rightarrow p(x)^3 = x^5$ in $K[x]$. Insbesondere $p(x) \mid x^5$, also $p(x) = ax^k \Rightarrow p(x)^3 = a^3x^{3k} = x^5$ ist unmöglich. Dieser Widerspruch zeigt, dass $f(y)$ keine Nullstelle in $K(x)$ hat. Folgt $f(y)$ ist irreduzibel als Element von $K(x)[y]$ und primitiv in $(K[x])[y]$ und daher irreduzibel in $K[x,y]$.

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

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

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

*Beweis.* Angenommen $f = gh$ für $g, h \in R[x]$. Dann ist auch $f \mod p = g \mod p h \mod p$ in $R/(p)[x]$. Da $f \mod p$ irreduzibel ist, folgt nun, dass $g \mod p$ oder $h \mod p$ eine Einheit in $R/(p)[x]$ sein muss. Also insbesondere gilt $\deg(g \mod p) = 0$ oder $\deg(h \mod p) = 0$. O.B.d.A. ist $\deg(g \mod p) = 0$. Also $g \equiv a \mod p$ für ein $a \in R$. Wir behaupten, dass dies $\deg(g) = 0$ impliziert. Dies impliziert, dass $g \mid I(f) \sim 1$ womit $g \in R^\times = R[x]^\times$ ist. Da dies für beliebige Zerlegungen von $f$ gilt, folgt daraus, dass $f$ irreduzibel ist. Da $R[x]$ faktoriell ist, ist $f$ also auch ein Primelement.

*Beweis der Behauptung.* Zu zeigen $g \equiv a \mod p \Rightarrow \deg(g) = 0$ mit $a \in R$
Angenommen dies stimmt nicht. Dann ist der führende Koeffizient von $g$ durch $p$ teilbar. Aber dann ist auch der führende Koeffizient von $f$ (gleich dem Produkt der führenden Koeffizienten von $g$ und $h$ ) durch $p$ teilbar. Dies widerspricht der Annahme, dass $\deg(f) = \deg(f \mod p)$ ist. □

□

**Beispiel.** Sei $f(x) = x^4 + 3x^3 - x^2 + 1 \in \mathbb{Z}[x]$. Wir wählen $p = 5$ und wollen zeigen, dass $f$ alle Voraussetzungen der Proposition erfüllt $\Rightarrow f$ ist irreduzibel in $\mathbb{Z}[x]$.

- primitiv ✓
- $\deg(f \mod 5) = 4 = \deg(f)$ ✓

Wir müssen noch zeigen, dass $f \mod 5 \in \mathbb{F}_5[x]$ irreduzibel ist.

Linearfaktoren als Teiler ? Dies tritt genau dann ein wenn $f \mod 5$ in $\mathbb{F}_5$ eine Nullstelle hat.

$$f(0) = 1 \neq 0 \text{ in } \mathbb{F}_5 \quad f(1) = 4 \neq 0 \text{ in } \mathbb{F}_5 \quad \dots.$$

Insbesondere folgt daraus, dass es keine Zerlegung der Form linear mal kubisch in $\mathbb{F}_5[x]$ gibt.

Wir müssen noch überprüfen, dass es keine Zerlegung der Form quadratisch mal quadratisch gibt. Überprüfe dies mit Sage oder per Hand.

Eine alternative Beweismethode für die Irreduzibilität von $f(x) = x^4 + 3x^3 - x^2 + 1 \in \mathbb{Z}[x]$.

- $p = 2$: $x^4 + 3x^3 - x^2 + 1 = x^4 + x^3 + x^2 + 1 \mod 2 = (x+1)(x^3 + x + 1)$ beide Faktoren irreduzibel.
- $p = 3$: $x^4 + 3x^3 - x^2 + 1 = x^4 + 2x^2 + 1 \mod 3 = (x^2 + 1)^2$ ist irreduzibel.

*Behauptung.* Aus der Rechnung oben für $p = 2$ und $p = 3$ folgt, dass $f(x) \in \mathbb{Z}[x]$ irreduzibel ist.

Falls $f = gh$, $g, h \in \mathbb{Z}[x]$, keine Einheit, führende Koeffizienten $\pm 1$, wäre, so wäre $f \mod 2 = g \mod 2 h \mod 2 \Rightarrow g \mod 2 = \begin{cases} x + 1 \\ x^3 + x + 1 \end{cases}$. Und somit $\deg(g) \in \{1, 3\}$. Mittels $p = 3$ folgt analog $\deg(g) = 2$. ↯

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

*Beweis.* Angenommen $f = gh$ für $g, h \in R[x]$ beide keine Einheiten. Da $f$ primitiv ist, gilt dies auch für $g$ und $h$, womit $k := \deg(g) > 0$ und $l := \deg(h) > 0$ ist und $k + l = n$ Modulo $p$ folgt

$$f \mod p = a_n x^n = g \mod p h \mod p.$$

Wir betrachten diese Gleichung als Faktorisierung in $\mathrm{Quot}(R/(p))[x]$, wo $a_n \neq 0$ eine Einheit und $x$ ein Primfaktor ist. Es folgt, dass $g \mod p = bx^{k'}, k' < k, b \neq 0$ und $h \mod p = cx^{l'}, l' < l, c \neq 0$. Des Weiteren gilt $k' + l' = n$, also $k' = k > 0$ und $l' = l > 0$. Daraus folgt nun, dass $p$ den konstanten Term von $g$ und auch den konstanten Term von $h$ teilt. Für $f = gh$ folgt daraus, dass der konstante Term

$$a_0 = (\text{konstanter Term von } g)(\text{konstanter Term von } h)$$

durch $p^2$ teilbar ist. Dies widerspricht unserer Annahme an $f$ und wir erhalten, dass $f$ irreduzibel ist. $\square$

**Beispiel.** Das Polynom $x^n - 2 \in \mathbb{Z}[x]$ ist für jedes $n \geq 1$ irreduzibel. Dies folgt aus dem Eisensteinkriterium für $p = 2$.

**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.*

*Beweis.* Wir wollen das Eisenstein-Kriterium für

$$f(y) = \frac{(y+1)^p - 1}{y} = y^{-1}\left(\sum_{k=0}^{p}\binom{p}{k}y^k - 1\right) = \sum_{k=1}^{p}\binom{p}{k}y^{k-1}$$

anwenden. Für $k = p$ ist $\binom{p}{p} = 1$ also ist $f$ normiert und primitiv. Des Weiteren wissen wir $p \mid \binom{p}{k}$ für $k = 1, \ldots, p-1$. Der konstante Term von $f$ entspricht $k = 1$ und ist daher durch $\binom{p}{1} = p$ gegeben. Dieser ist nicht durch $p^2$ teilbar, womit $f \in \mathbb{Z}[y]$ irreduzibel ist.

Wir wollen „$x = y + 1$“ verwenden: Die Ringe

$$\Psi : \mathbb{Z}[y] \xrightarrow{\sim} \mathbb{Z}[x],$$

sind isomorph, wobei wir jeweils den Auswertungshomomorphismus verwenden um beide Abbildungen zu definieren:

$$\Psi(\underbrace{f(y)}_{\in \mathbb{Z}[y]}) = f(x-1) \in \mathbb{Z}[x] \qquad \widetilde{\Psi}(\underbrace{g(x)}_{\in \mathbb{Z}[x]}) = g(y+1) \in \mathbb{Z}[y].$$

Da $f \in \mathbb{Z}[y]$ irreduzibel ist und $\Phi_p(x)$ das Bild von $f$ unter diesem Isomorphismus ist, folgt die Irreduzibilität von $\Phi_p(x)$. $\square$

**Beispiel.** Für jedes $n \geq 1$ ist

$$f(x, y, z) = x^n + y^n - z^n \in \mathbb{C}[x, y, z]$$

irreduzibel. Wir setzen $R = \mathbb{C}[y, z]$ und $p = y - z \in R$. Als Element von $R[x]$ ist $f$ normiert und daher primitiv. Da es abgesehen vom führenden Koeffizienten von $f$ nur noch den konstanten Term gibt müssen wir $p \mid y^n - z^n$ und $p^2 \nmid y^n - z^n$ zeigen:

$$y^n - z^n = (y - z)(y^{n-1} + y^{n-2}z + \ldots + yz^{n-2} + z^{n-1})$$

also $p \mid y^n - z^n$.

*Behauptung.* $(y - z)$ teilt $(y^{n-1} + y^{n-2}z + \ldots + yz^{n-2} + z^{n-1})$ *nicht.*

$(y^{n-1} + y^{n-2}z + \ldots + yz^{n-2} + z^{n-1})$ modulo $y - z$ ist gleich $nz^{n-1}$, was nicht durch $y - z$ teilbar ist.

*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 $e = e_G = 1 = 1_G$.

*Beweis.* Angenommen $f \in G$ erfüllt $f \cdot a = a$ für alle $a \in G$ und $e \in G$ erfüllt Axiom 2). Dann gilt $f \overset{2)}{=} f \cdot e = e$.

Angenommen $f \in G$ erfüllt $f \cdot f = f$. Wir multiplizieren mit $f^{-1}$ wie in Axiom 3) und erhalten

$$f = f \cdot \underbrace{(f \cdot f^{-1})}_{e} = (f \cdot f) \cdot f^{-1} = f \cdot f^{-1} = e.$$

Angenommen $a \cdot y = e$ und $x$ ist wie in Axiom 3). Dann gilt

$$x \cdot (a \cdot y) = x \cdot e = x \Leftrightarrow \underbrace{(x \cdot a)}_{e} \cdot y = x \Leftrightarrow x = y.$$

□

**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 $(ab)^k = a^k b^k$.*

*Beweis.* Für $k,l \geq 0$ mittels Induktion nach $l$ :

1. IA: $a^k a^0 = a^{k+0}$
   IS: $a^k a^{l+1} = a^k a^l a = a^{k+l} a = a^{k+l+1}$ per rekursiver Definition
2. IA: $(a^k)^0 = e = a^{k \cdot 0}$
   IS: $(a^k)^{l+1} = (a^k)^l a^k = a^{kl} a^k \overset{a)}{=} a^{k(l+1)}$
3. IA: $ab^0 = b^0 a$
   IS: $ab^{l+1} = ab^l b = b^l ab = b^l ba = b^{l+1} a$ also $a$ kommutiert mit $b^l$.
   IA: $(ab)^0 = e = a^0 b^0$
   IS: $(ab)^{k+1} = (ab)^k (ab) = a^k b^k ab = a^{k+1} b^{k+1}$

Beweis für negative Potenzen analog. □

**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 $a = b \Leftrightarrow ac = bc \Leftrightarrow ca = cb$.*

*Beweis.* Angenommen $ax = b$, dann gilt $\underbrace{a^{-1}a}_{e} x = a^{-1}b \Rightarrow x = a^{-1}b$. Und in der Tat gilt $a(a^{-1}b) = b$.

$\Rightarrow$ trivial
$\Leftarrow$: Angenommen $ac = bc$, dann gilt $(ac)c^{-1} = (bc)c^{-1} \Rightarrow ae = be \Rightarrow a = b$. □

**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* $\mathrm{Ker}(\varphi) = \varphi^{-1}\{e_{G_2}\} = \{a \in G \mid \varphi(a) = e_{G_2}\}$ und das *Bild* $\mathrm{Im}(\varphi) = \varphi(G_1) = \{b \in G_2 \mid \exists a \in G \text{ mit } \varphi(a) = b\}$. Falls $\varphi$ 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 $a, b \in H \Rightarrow ab \in H$.

**Beispiel.** Für einen Homomorphismus $\varphi : G_1 \to G_2$ ist $\mathrm{Ker}(\varphi)$ eine Untergruppe von $G_1$ und $\mathrm{Im}(\varphi)$ eine Untergruppe von $G_2$.

**Beispiel.** 1. $\{1\}$
2. Addition in Ringen (und Körper) und Vektorräume.
3. Die Gruppe $R^\times$ der Einheiten in einem Ring. Insbesondere $K^\times = K \setminus \{0\}$ für einen Körper. Also $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ bzw $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.
4. Sei $M$ eine nichtleere Menge. Dann ist $\mathrm{Bij}(M) = \{\varphi : M \to M \text{ bijektiv}\}$ eine Gruppe (bzgl. Verknüpfung der Abbildungen). Falls $M = \{1, \ldots, n\}$ für ein $n \geq 1$, so nennen wir $\mathrm{Sym}_n = S_n = \mathrm{Bij}(\{1, \ldots, b\})$ auch die *symmetrische Gruppe*.
5. Sei $M$ eine nichtleere Menge mit „einer Struktur“. Dann ist

$$\mathrm{Aut}(M) = \{\varphi : M \to M \text{ bijektiv \& „strukturerhaltend“ }\}$$

oft eine Gruppe.

| $M$ & Struktur auf $M$ | $\mathrm{Aut}(M)$ |
|---|---|
| $M$ & ohne Struktur | $\mathrm{Bij}(M)$ |
| $V$ Vektorraum über einem Körper | $\mathrm{GL}(V)$ |
| $K \supseteq \mathbb{Q}$ ein Körper | $\mathrm{Gal}(K:\mathbb{Q}) = \{\varphi : K \to K : \mathbb{Q}$-linear, bijektiv und $\varphi(ab) = \varphi(a)\varphi(b)\}$ (Galois-Gruppe von $K$) |
| $G$ eine Gruppe | $\mathrm{Aut}(G) = \{\varphi : G \to G \underbrace{\text{ Isomorphismus von } G \text{ nach } G}_{\text{Automorphismus von } G}\}$ |
| Affine reelle Ebene | $\mathrm{GL}_2(\mathbb{R}) \ltimes \mathbb{R}^2$ |
| Euklidische reelle Ebene | $O_2(\mathbb{R}) \ltimes \mathbb{R}^2$ |
| Sphärische Geometrie | $O_3(\mathbb{R})$ |
| Hyperbolische Ebene | $\mathrm{SO}_{2,1}(\mathbb{R}), P\,\mathrm{GL}_2(\mathbb{R})$ ($P$ für Projektiv, also, dass man das Zentrum rausfaktorisiert) |
| $\vdots$ | |
| Topologischer-Raum $X$ | $\mathrm{Hom\ddot{o}o}(X) = \{\varphi : X \to X$ bijektiv, stetig, $\varphi^{-1}$ stetig$\}$ |
| Mannigfaltigkeit $M$ | $\mathrm{Diffeo}^\infty(M) = \{\varphi : M \to M$ bijektiv, stetig, glatt und ebenso $\varphi^{-1}\}$ |
| $M =$ regelmäßiges Polygon in $\mathbb{R}^2$ | Diedergruppe $D_n = \{$ lineare Abb. in $\mathrm{GL}_2(\mathbb{R})$, die $M$ auf sich abbilden $\}$ |
| $M =$ Platonische Körper im $\mathbb{R}^3$ | |
| $M =$ Zauberwürfel Rubik's Cube | Bewegungen des Zauberwürfels |

6. Sei $K$ ein Körper. Dann ist

$$\mathrm{GL}_n(K) = \{A \in \mathrm{Mat}_{nn}(K) : A \text{ invertierbar}\}$$

ein Gruppe. Falls $V$ ein $n$-dimensionaler Vektorraum über $K$ ist, so ist $\mathrm{GL}(V)$ isomorph zu $\mathrm{GL}_n(K)$ - dies ist mit der Auswahl einer Basis von $V$ gleichzusetzen. Des Weiteren ist

$$\det : \mathrm{GL}_n(K) \to K^\times.$$

ein Gruppenhomomorphismus und $\mathrm{Ker}(\det) = \mathrm{SL}_n(K)$.

7. .

$(0, \infty) < R^\times$ ist eine Untergruppe.

$\exp : \mathbb{R} \to \mathbb{R}^\times$ ist ein Homomorphismus.

$S^1 = \{z \in \mathbb{C} \mid |z| = 1\} = \mathrm{Ker}(|\cdot|) < \mathbb{C}^\times$ ist eine Untergruppe.

$\exp : \mathbb{C} \to \mathbb{C}^\times$ ist ein Homomorphismus. $\mathrm{Ker}(\exp) = 2\pi i\mathbb{Z}$

8. $G_1 \times G_2$ ist eine Gruppe (komponentenweisen Operationen) falls $G_1, G_2$ Gruppen sind.

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

**Definition.** Falls $\varphi$ 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.

*Beweis.* $\varphi : n \mapsto a^n$ ist ein Homomorphismus wegen dem zweiten Lemma von heute.

*Bemerkung.* $I = \mathrm{Ker}(\varphi)$ ist ein Ideal in $\mathbb{Z}$ und eine Untergruppe. Angenommen $k \in I$ und $n \in \mathbb{Z}$. Dann gilt $\varphi(n^k) = a^{nk} = (a^k)^n = e$ und daher $nk \in I$. Entweder $I = (0)$ oder $I = (n_0)$ für $n_0 > 0$:
$I = (0)$ dann ist $\varphi$ injektiv: Angenommen $\varphi(m) = \varphi(n) \Leftrightarrow \varphi(m-n) = e \Leftrightarrow m - n \in I = (0) \Rightarrow m = n$.

□

**Beispiel.** z.B. hat $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ unendliche Ordnung und $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ hat Ordnung 4.

## 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 $\Phi$ ist das Zentrum $Z_G = \{g \in G \mid gx = xg \; \forall x \in G\}$.*

*Beweis.* Für $g, x, y \in G$ gilt

$$\gamma_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \gamma_g(x)\gamma_g(y).$$

Also ist $\gamma_g$ ein Homomorphismus $G \to G$. Für $g, h, x \in G$ gilt

$$\gamma_g(\gamma_h(x) = g(\gamma_h(x))g^{-1} = g(hxh^{-1})g = (gh)x(gh)^{-1} = \gamma_{gh}(x).$$

Insbesondere gilt

$$\gamma_g \cdot \gamma_{g^{-1}}(x) = \gamma_{gg^{-1}}(x) = \gamma_e(x) = \mathrm{id}(x).$$

und daher $\gamma_g\gamma_{g^{-1}} = \mathrm{id} = \gamma_{g^{-1}}\gamma_g$. Also ist $\gamma_g$ ein Automorphismus und a) ist bewiesen.
Für b) haben wir bereits gezeigt, dass $\Phi : G \to \mathrm{Aut}(G)$ ein Homomorphismus ist:

$$\Phi(gh) = \gamma_{gh} = \gamma_g \cdot \gamma_h = \Phi(g)\Phi(h).$$

Des Weiteren gilt

$$\mathrm{Ker}(\Phi) = \{g \in G \mid \gamma_g = \mathrm{id}\} = \{g \in G \mid \underbrace{gxg^{-1} = x}_{gx=xg} \text{ für alle } x \in G\}.$$

□

**Definition.** Sei $G$ ein Gruppe und $g \in G$. Dann ist die Menge der Fixpunkte $\gamma_g$ 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.*

*Beweis.* Übung □

**Beispiel.** a) Sei $G = \mathrm{GL}_n(\mathbb{C})$. Zwei Matrizen $A, B$ sind konjugiert falls es ein $g \in \mathrm{GL}_n(\mathbb{C})$ gibt mit $gAg^{-1} = B$. Dies gilt genau dann, wenn $A$ und $B$ dieselbe Jordan-Normalform hat.
b) Sei $G = \mathrm{U}_n(\mathbb{C}) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid A^*A = AA^* = I\}$. Jedes $g \in G$ ist mittels einem Element von $G$ diagonalisierbar. $\Rightarrow$ Konjugationsklassen für $G$ können wir durch Elemente von $(S^1)^n$ modulo Vertauschung der Koordinaten beschreiben.

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

**Beispiel.** $\mathrm{Sym}_n = S_n$ hat $n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$ Elemente (Sterling-Formel). Die Anzahl der Konjugationsklassen ist hingegen ungefähr $\frac{1}{4\sqrt{3}n} e^{2\pi\sqrt{\frac{n}{6}}}$ (Hardy-Ramanujan 1918).

**Beispiel.** 1) Das Zentrum von $S_n$ für $n \geq 3$ ist $\{1\}$. (Übung)

2) Das Zentrum von $\mathrm{GL}_n(K)$ ist $\{A \in \mathrm{GL}_n(K) \mid A$ ist Diagonal mit Diagonaleintrag $t \in K^\times\}$ :

$$\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

3) Das Zentrum von $\mathrm{SL}_n(K)$ ist $\{A \in \mathrm{GL}_n(K) \mid A$ ist Diagonal mit Diagonaleintrag $t \in K^\times, t^n = 1\}$

## 3.3 Untergruppen und Erzeuger

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

**Beispiel.** Sei $G = \mathbb{Z}$. Dann ist jede Untergruppe $H < \mathbb{Z}$ ein Ideal und damit von der Form $H = (n_0)$ für ein $n_0 \in \mathbb{N}$. Denn: Für $n \in H$ und $k \in \mathbb{Z}$ gilt

$$k \cdot n = \begin{cases} \underbrace{n + \ldots + n}_{k-\text{mal}} \in H & \text{für } k > 0 \\ 0 \in H & \text{für } k = 0 \\ \underbrace{-n - \ldots - n}_{|k|-\text{mal}} \in H & \text{für } k < 0 \end{cases}$$

**Beispiel.** Sei $n \geq 2$ eine natürliche Zahl. Dann definieren wir die *Diedergruppe* $D_{2n}$ mittels $\zeta = e^{\frac{2\pi i}{n}}$ und $\mathbb{R}$-lineare Transformationen auf $\mathbb{C}$ :

$$D_{2n} = \underbrace{\{z \mapsto \zeta^k z \mid k = 0, 1, \ldots, n-1\}}_{C_n \cong \mathbb{Z}/(n)} \cup \{\underbrace{z \mapsto \zeta^k \overline{z}}_{\sigma_k} \mid k = 0, 1, \ldots, n-1\}.$$

und es gilt $\sigma_k(\sigma_k(z)) = \sigma_k(\zeta^k \overline{z}) = \zeta^k \overline{(\zeta^k \overline{z})} = z$, also definiert $\sigma_k$ eine Spiegelung des regelmäßigen $n$-Ecks. $C_n$ definiert die Drehungen.

**Untergruppen:** $\{\mathrm{id}\}, D_{2n}, C_n, \{\mathrm{id}, \sigma_k\}$ für $k = 0, \ldots, n-1$, für $k \mid n$ gibt es auch eine Untergruppe von $C_n$ isomorph zu $\mathbb{Z}/(n)$ und von $D_{2n}$ isomorph zu $D_{2k}$. $D_{2\cdot 2}$ hat noch eine weitere Untergruppe.

**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 $\langle X\rangle = \{x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n} \mid n \in \mathbb{N}, x_1,\dots,x_n \in X, \varepsilon_1,\dots,\varepsilon_n \in \{\pm 1\}\}$.*

*Beweis.* Sei $H_0$ die Menge rechts im Lemma. Dann gilt $X \subseteq H_0$ und $H_0 < G$. Daher tritt $H_0$ als eine der Untergruppen in der Definition von $\langle X\rangle$ auf und wir erhalten $\langle X\rangle \subseteq H_0$. Falls $H < G$ und $X \subseteq H$, dann enthält $H$ auch jeden Ausdruck der Form $x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n}$. Daher gilt $H_0 \subseteq H$. Da dies für alle derartigen $H$'s gilt, folgt $H_0 \subseteq \langle X\rangle$. $\square$

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

*Beweis.* Wir definieren $\varphi : n \in \mathbb{Z} \mapsto a^n \in G$. Dies ist ein Homomorphismus und $\operatorname{Ker}(\varphi) = I = (n_0)$ für ein $n_0 \in \mathbb{N}$. Nun definieren wir $\Phi : \mathbb{Z}/(n_0) \to \langle a\rangle, k + (n_0) \mapsto a^k$. Dies ist wohldefiniert und injektiv wegen

$$k + (n_0) = l + (n_0) \Leftrightarrow k - l \in (n_0) = \operatorname{Ker}(\varphi) \Leftrightarrow a^{k-l} = e \Leftrightarrow a^k = a^l.$$

$\square$

**Beispiel.** $S_n$ (mit $n!$ Elementen verschiedenster Natur) ist durch zwei Elemente erzeugt:

$$\tau_{1,2} = \text{ Vertauschung von 1 und 2: } \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \\ \quad\vdots \\ n \mapsto n \end{cases} \quad \text{(Ordnung 2)}$$

$$\sigma = \text{zyklische Vertauschung aller Zahlen: } \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 4 \\ \quad\vdots \\ n \mapsto 1 \end{cases} \quad \text{(Ordnung } n\text{)}$$

Zum Beispiel $\sigma\tau_{1,2}\sigma^{-1} = \begin{cases} 1 \mapsto n \mapsto n \mapsto 1 \\ 2 \mapsto 1 \mapsto 2 \mapsto 3 \\ 2 \mapsto 2 \mapsto 1 \mapsto 2 \\ \qquad\vdots \end{cases} = \tau_{2,3}$. Alle $\tau_{i,i+1} \in \langle \tau_{1,2}, \sigma\rangle$. Diese Vertauschungen erzeugen ganz $S_n$. Sei $\rho \in S_n$ beliebig. Durch Linksmultiplikation von $\rho$ mit Vertauschungen $\tau_{i,i+1}$ können wir $\rho$ schrittweise vereinfachen und erhalten nach endlich vielen Schritten die Identität $\tau_{i_k,i_k+1}\dots\tau_{i_n,i_n+1}\rho = \mathrm{id}$.

*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 ${}_H{\sim}$*

*Beweis.*
- $a \sim_H a$ denn $a^{-1}a = e \in H$.
- $a \sim_H b \Rightarrow b^{-1}a \in H \Rightarrow (b^{-1}a)^{-1} = a^{-1}b \in H \Rightarrow b \sim_H a$.
- $a \sim_H b$ und $b \sim_H c \Rightarrow b^{-1}a, c^{-1}b \in H \Rightarrow c^{-1}a = (c^{-1}b)(b^{-1}a) \in H \Rightarrow a \sim_H c$.

Also ist $\sim_H$ eine Äquivalenzrelation. Des Weiteren gilt:

$$[a]_{\sim_H} = \{b \mid b \sim_H a\} = \{b \mid b^{-1}a \in H\} = aH \quad (b^{-1}a = h \in H \Rightarrow a = bh \text{ für } h \in H).$$

□

**Beispiel.** $S_3 > H = \langle \tau_{12} \rangle = \{e, \tau_{12}\}$. Sei $\sigma$ die zyklische Vertauschung von $1, 2, 3$. Dann ist $\sigma H \neq H\sigma$, da $\{\sigma, \sigma\tau_{12}\} \neq \{\sigma, \tau_{12}\sigma\}$.

$$\sigma\tau_{12} : 1 \to 2 \to 3 \qquad \tau_{12}\sigma : 1 \to 2 \to 1.$$

**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.

*Beweis.* Wir definieren $\varphi : {}^{G}\!/\!_{H} \to {}^{H}\!/\!_{G}$ und $\psi : {}^{H}\!/\!_{G} \to {}^{G}\!/\!_{H}$ durch

$$aH \mapsto (aH)^{-1} = \{g^{-1} : g \in aH\} = Ha^{-1} \qquad Ha \mapsto (Ha)^{-1} = a^{-1}H.$$

Wir sehen auch $\psi(\varphi(aH)) = \psi(Ha^{-1}) = aH$ und analog $\psi \circ \varphi = \mathrm{id}$. Also folgt $|{}^{H}\!/\!_{G}| = |{}^{G}\!/\!_{H}|$ wie in (1) behauptet.

Für (2) wählen wir aus jeder Linksnebenklasse $aH$ für $a \in G$ genau einen Linksrepräsentanten $x \in aH$ aus. Die Menge der ausgewählten Linksrepräsentanten bezeichnen wir mit $X$. Es gilt $|{}^{G}\!/\!_{H}| = |X|$.

*Behauptung.*

$$|G| \stackrel{!}{=} |X \times H| = |X||H| = |{}^{G}/{}_{H}| \cdot |H|$$

$\psi : X \times H \to G$ mit $(x, h) \mapsto xh$

$\psi$ ist *surjektiv*: Sei $g \in G$, dann ist $gH \in {}^{G}/{}_{H}$ und wir haben in der Konstruktion von $X$ aus $gH$ ein $x \in X \cap gH$ ausgewählt. Insbesondere gibt es ein $h \in H$ (weil $g \sim_H x$) mit $g = xh = \psi(x, h)$. Also ist $\psi$ surjektiv.

$\psi$ ist *injektiv*: Angenommen $\psi(x_1, h_1) = \psi(x_2, h_2)$ also $x_1h_1 = x_2h_2$ für $(x_1, h_1), (x_2, h_2) \in X \times G$. Insbesondere gilt $x_1H = x_2H$ in der Konstruktion von $X$ nur einen Linksrepräsentanten ausgewählt haben, gilt also $x_1 = x_2$. Daher gilt $x_1h_1 = x_1h_2$ und auch $h_1 = h_2$. Wir haben also $(x_1, h_1) = (x_2, h_2)$ überprüft. Da dies für alle Paare $(x_1, h_1), (x_2, h_2)$ gilt, ist also $\psi$ injektiv. □

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

*Beweis.* Sei $m = |G|$ und $n = |\langle g \rangle| =$ Ordnung von $g$. Dann gilt $n \mid m$ wegen des Satzes von Lagrange. Sei $k = \frac{m}{n}$. Dan gilt

$$g^{|G|} = g^m = g^{nk} = (g^n)^k = e^k = e.$$

□

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

*Beweis.* $G = \mathbb{F}_p^\times$ hat Ordnung $p - 1$. □

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

*Beweis.* Sei $g \in G \setminus \{e\}$. Dann ist $n = \operatorname{Ord}(g) = \langle g \rangle = 1$ und ein Teiler von $p$. Also ist $n = p$ und $\langle g \rangle = G$. □

$\Rightarrow$ 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 $H = \operatorname{Ker}(\varphi)$.*
*(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.*

*Beweis.* $(5) \Rightarrow (3) : \operatorname{Ker}(\varphi) = \{g \mid gH = eH\} = H$
$(3) \Rightarrow (2)$ : Sei $x \in G, h \in H = \operatorname{Ker}(\varphi)$. Dann gilt $\varphi(xhx^{-1}) = \varphi(x)\underbrace{\varphi(h)}_{=e}\varphi(x)^{-1} = e$ also $xhx^{-1} \in H = \operatorname{Ker}(\varphi)$. $\Rightarrow xHx^{-1} \subseteq H, x^{-1}Hx \subseteq H \Rightarrow H \subseteq xHx^{-1}$. Somit folgt $xHx^{-1} = H$
$(2) \Leftrightarrow (1)$ : Rechtsmultiplikation mit $x^{-1}$ oder $x$.

(1) $\Rightarrow$ (4) : Seien $x, y \in G$. Dann gilt $(xH)(yH) = (Hx)(yH) = (Hxy)H = xyHH = xyH$.
(4) $\Rightarrow$ (5) : Nach Annahme in 4 ist die Abbildung

$$^G/_H \times {}^G/_H \to {}^G/_H \qquad (xh) \times (yH) \mapsto (xH)(yH) = (xy)H$$

wohldefiniert. Nun folgen die Gruppenaxiome in $^G/_H$ direkt aus den Gruppenaxiome in $G$.

$$((xH)(yH))(zH) = ((xy)H)(zH) = ((xy)z)H = (x(yz)H) = \ldots = (xH)((yH)(zH)).$$

also ist $a$ in $^G/_H$ assoziativ.

$$(xH)(eH) = (eH)(xH) = xH$$
$$(xH)(x^{-1}H) = (x^{-1}H)(xH) = eH.$$

$\square$

**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.

**Beispiel.** Eine abelsche Gruppe ist genau dann einfach wenn $G \cong {}^{\mathbb{Z}}/_{(p)}$ für eine Primzahl $p \in \mathbb{N}$.

**Beispiel.** Auf $S_n$ gibt es den Homomorphismus $\mathrm{sgn} : S_n \to \{\pm 1\}$. Der Kern $A_n = \mathrm{Ker}(\mathrm{sgn})$ wird die *alternierende Gruppe* genannt. Für $n \geq 5$ ist $A_n$ eine nicht abelsche einfache Gruppe.

**Satz** (Erster Isomorphiesatz). *Sei $\varphi : G \to H$ eine Homomorphismus zwischen zwei Gruppen $G$ und $H$. Dann induziert $\varphi$ 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 $\pi$ als der kanonischen Projektion und $\iota$ der Einbettung. Also gilt $\varphi = \iota \circ \overline{\varphi} \circ \pi$.*

*Beweis.* Wir zeigen, dass $\overline{\varphi}(x \,\mathrm{Ker}(\varphi)) = \varphi(x)$ auf $^G/_{\mathrm{Ker}(\varphi)}$ wohldefiniert und injektiv ist:
Seien $x, y \in G$, dann gilt

$$\varphi(x) = \varphi(y) \Leftrightarrow \varphi(y)^{-1}\varphi(x) = e \Leftrightarrow \varphi(y^{-1}x) = e \Leftrightarrow y^{-1}x \in \mathrm{Ker}(\varphi) \Leftrightarrow x \,\mathrm{Ker}(\varphi) = y \,\mathrm{Ker}(\varphi)$$

$\Rightarrow$ wohldefiniert. $\Leftarrow$ injektiv.
Auch gilt $\mathrm{Im}(\overline{\varphi}) = \mathrm{Im}(\varphi)$ womit $\overline{\varphi} : {}^G/_{\mathrm{Ker}(\varphi)} \to \mathrm{Im}(\varphi)$ ein Isomorphismus ist. Für $g \in G$ gilt $\iota(\overline{\varphi}(\pi(g))) = \iota(\overline{\varphi}(g \,\mathrm{Ker}(\varphi))) = \iota(\varphi(g)) = \varphi(g)$. $\square$

**Beispiel.** Sei $p$ prim. Dann ist $|\mathrm{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p)$ und $\det : \mathrm{GL}_2(\mathbb{F}_p) \to \mathbb{F}_p^\times$ ist surjektiv z.B. wegen $\det \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} = t$.

Weiters gilt $\mathrm{SL}_2(\mathbb{F}_p) = \mathrm{Ker}(\det)$. Aus dem Satz von Lagrange und dem ersten Isomorphiesatz folgt

$$|\mathrm{SL}_2(\mathbb{F}_p)| \cdot (p-1) = |\mathrm{GL}_2(\mathbb{F}_p)|$$

wobei Index $= |{}^{G}/_{\mathrm{Ker}(\det)}| = |\mathrm{Im}(\det)| = p-1$.

$$\Rightarrow |\mathrm{SL}_2(\mathbb{F}_p)| = \frac{(p^2-1)(p^2-p)}{p-1} = p(p^2-1).$$

**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 $x \in K$*

*Beweis.* Für $k \in K$ gilt $kH = Hk$. Für die Vereinigung über alle $k \in K$ gilt daher $KH = HK$. Des Weiteren gilt für $k_1, k_2 \in K, h_1, h_2 \in H$ dass

$$\begin{aligned}(k_1h_1)(k_2h_2) &\in \underbrace{KH}_{HK}KH = \underbrace{HK}_{KH}H = K\\ (k_1h_1)^{-1} &= h_1^{-1}k_1^{-1} \in KH = HK\end{aligned}$$

Folgt $KH < G$.

Des Weiteren ist $H \lhd KH$ weil $H < KH$ und für $x \in KH \subseteq G$ gilt $xH = Hx$.

Wir definieren den Gruppenhomomorphismus

$$\begin{tikzcd} K \arrow[r, hook] \arrow[rr, bend right, "\varphi"'] & KH \arrow[r] & KH/_H \end{tikzcd}.$$

Es gilt $\mathrm{Ker}(\varphi) = \{k \in K \mid \underbrace{kH = eH}_{k \in H}\} = K \cap H \lhd K$ und $K/_{K \cap H} \cong \mathrm{Im}(\varphi) = \{kH \mid k \in K\} = KH/_K$ $\square$

**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 $(xK)\, H/_K \mathrel{\hat{=}} xH$ einander im Isomorphismus entsprechen.*

*Beweis.* Wir definieren $\varphi : G/_K \to G/_H, gK \mapsto gH$. Dies ist wohldefiniert, da $K \subseteq H$ und wir einfach $gK$ rechts mit $H$ multiplizieren: $\varphi(gK) = (gK)H = gH$. Da die Gruppenstrukturen in $G/_K$ und $G/_H$ durch Multiplikation der Repräsentanten definiert ist, ist $\varphi$ auch ein Gruppenhomomorphismus

$$\varphi((g_1K)(g_2K)) = \varphi((g_1g_2)K) = (g_1g_2)H = (g_1H)(g_2H) = \varphi(g_1K)\varphi(g_2K).$$

$\varphi$ ist surjektiv. Daher gilt $G/K/_{\mathrm{Ker}(\varphi)} \cong G/_H$ und $\mathrm{Ker}(\varphi) = \{gK \mid gH = eH\} = \{hK \mid h \in H\} = H/_K$ $\square$

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

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

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

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

**Beispiel.**
- $C_n \lhd D_{2n}$ denn für eine Relation $R \in C_n$ und eine Reflexion $T \in D_{2n}$ gilt
$$TRT^{-1} = R^{-1} \in C_n.$$
(und jede Untergruppe $H < C_n$ ist auch ein Normalteiler von $D_{2n}$ )
- Zentrum und Kommutatorgruppe sind immer normal.
- Affine Gruppe $G = \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in K^\times, b \in K\}$ für einen Körper $K$.
$$H_1 = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in K\} \lhd G \qquad H_2 = \{\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in K^\times\} < G$$
aber nicht normal wenn $|K^\times| > 1$.

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

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

## 3.5 Gruppenwirkungen

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

**Beispiel.**
0) Sei $T$ eine Menge und $G$ eine Gruppe. Dann ist die triviale Gruppenwirkung $g \cdot t = t$ für alle $g \in G, t \in T$ eine Gruppenwirkung.
1) $G = S_n$ wirkt auf $T = \{1, \dots, n\}$ durch $\sigma \cdot t = \sigma(t)$ für $\sigma \in S_n, t \in \{1, \dots, n\}$
2) $G = \mathrm{GL}(V)$ wirkt auf $V$, ein Vektorraum über $K$ durch $\varphi \cdot v = \varphi(v)$ für $\varphi \in \mathrm{GL}(V)$ und $v \in V$.
3) Sei $G$ eine Gruppe und $H < G$. Wir definieren $T = G/H$ und $g \cdot (xH) = gxH$ für $g \in G$ und $xH \in G/H$. Dies definiert eine Gruppenwirkung:
   - $e \cdot (xH) = exH = xH$ für $xH \in G/H$
   - $g_1 \cdot (g_2 \cdot (xH)) = g_1 \cdot (g_2 xH) = (g_1 g_2) xH = (g_1 g_2) \cdot (xH)$ für $g_1 g_2, x \in G$.

   ⚠ **Achtung.** Wir können auch eine Gruppenwirkung auf $H/G$ definieren, müssen dies aber mittels der Formel $g \cdot (Hx) = Hxg^{-1}$ machen.
4) Sei $G$ eine Gruppe und $T = G$. Dann können wir Konjugation als eine Gruppenwirkung betrachten: $g \cdot x = gxg^{-1}$ für $g \in G$ und $x \in T = G$.
5) Sei $G$ eine Gruppe und $T = \mathcal{P}(G) = \{A \subseteq G\}$. Für $g \in G$ und $A \in T$ definieren wir $g \cdot A = gA = \{ga | a \in A\}$.

6) Sei $G$ eine Gruppe und $T = \{H < G\}$. Für $g \in G$ und $H \in T$ definieren wir $g \cdot H = gHg^{-1}$.

**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 $\mathrm{Fix}_{\mathrm{G}}(T) = \{t_0 \in T \mid t_0 \text{ ist ein Fixpunkt}\}$ 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.*

*Beweis.*
- Reflexivität: $t \sim t$ da $\underbrace{e}_{\in G} \cdot t = t$.
- Symmetrie: Angenommen $t_1 \sim t_2$, dann existiert ein $g \in G$ mit $g \cdot t_1 = t_2$. Wir wenden auf diesen Punkt $g^{-1}$ an und erhalten $g^{-1} \cdot (g \cdot t_1) = g^{-1} \cdot t_2$ und $t_1 = e \cdot t_1 = g^{-1} t_2$ und damit $t_2 \sim t_1$.
- Transitivität: Angenommen $t_1 \sim t_2, t_2 \sim t_3$ : Dann existieren $g_1, g_2 \in G$ mit $g_1 \cdot t_1 = t_2$, $g_2 \cdot t_2 = t_3$. $(\underbrace{g_2 g_1}_{\in G}) \cdot t_1 = g_2 \cdot (\underbrace{g_1 t_1}_{t_2}) = t_3 \Rightarrow t_1 \sim t_3$.

Des Weiteren $[t]_{\sim_G} = \{t_2 \sim t\} = \{g \cdot t : g \in G\} = G \cdot t$ und ${}^{T}/_{\sim} = \{[t]_\sim : t \in T\} = G \setminus T$. $\square$

**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.*

*Beweis.* Seien $h_1, h_2 \in H = \mathrm{Stab}_G(t_0)$. Dann gilt $(h_1 h_2) \cdot t_0 = h_1 \cdot (\underbrace{h_2 \cdot t_0}_{t_0}) = t_0$ und $h_1 h_2 \in H$.

Außerdem $h_1 \cdot t_0 = t_0 \Rightarrow t_0 = h_1^{-1} \cdot t_0$ und $h_1^{-1} \in H$. Folgt $H < G$ (da auch $e \in H$ ).

Angenommen $g \in G$ und $g' \cdot t_0 \in T_0 = G \cdot t_0$. Dann ist $g \cdot (g' \cdot t_0) = (gg') \cdot t_0 \in T_0 = G \cdot t_0$.

Angenommen $g_1, g_2 \in G$. Dann gilt $g_1 \cdot t_0 = g_2 \cdot t_0 \Leftrightarrow (g_2^{-1} g_1) \cdot t_0 = t_0 \Leftrightarrow g_2^{-1} g_1 \in H \Leftrightarrow g_1 H = g_2 H$. Dies zeigt ($\Leftarrow$), dass $f$ wohldefiniert ist und ($\Rightarrow$) injektiv ist.

$T_0 = G \cdot t_0 = \{g \cdot t_0\} = f(G)$ und $f : {}^{G}/_{H} \to T_0$ ist surjektiv.

Sei nun $g_1, g_2 \in G$. Dann gilt

$$f(g_1 \cdot (g_2H)) = f((g_1g_2)H) = (g_1g_2) \cdot t_0 = g_1 \cdot (g_2 \cdot to) = g_1 \cdot f(g_2H).$$

Also ist $f$ ein $G$-Isomorphismus. $\square$

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

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

*Beweis.* Nach dem Satz gilt $G \cdot t_0 \cong {}^{G}/_{\mathrm{Stab}_G(t_0)}$, d.h. $|G \cdot t_0| = [G : \mathrm{Stab}_G(t_0)]$ und das Korollar folgt aus dem Satz von Lagrange $\square$

**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.*

*Beweis.* Nach einem Lemma vom letzten Mal ist die Menge der Bahnen eine Partition von $T$.

$$T = \bigsqcup_{\text{alle Bahnen}} G \cdot t = \mathrm{Fix}_G(T) \sqcup \bigsqcup_{|G \cdot t|>1} G \cdot t.$$

Des Weiteren gilt für eine Bahn $|G \cdot t| = [G : \mathrm{Stab}_G(t)]$ womit das Korollar folgt. $\square$

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

*Beweis.* Sei $T = G$ und $g_1 \cdot g_2$ für $g_1 \in G$ und $g_2 \in T = G$ durch Gruppenmultiplikation definiert. Äquivalent dazu definiert dies einen Homomorphismus $\alpha : G \to \mathrm{Bij}(G), g \mapsto (\alpha_{g_1} : g_2 \mapsto g_1g_2)$. Es gilt

$$\mathrm{Ker}(\alpha) = \{g \in G \mid \alpha_g = \mathrm{id}\} \subseteq \{g \in G \mid \alpha_g(e) = e\} = \{g \in G \mid ge = e\} = \{e\}$$

also ist $\alpha$ injektiv. Nach Annahme ist $|G| = n \in \mathbb{N}$ und $\mathrm{Bij}(G) \cong S_n$. $\square$

*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.

**Beispiel.** Sei $R$ ein Ring. dann ist die Heisenberggruppe

$$H_R = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in R \right\}$$

nilpotent mit Nilpotenzgrad 2. Hierfür muss man zeugen:

$$Z_{H_R} = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid b \in R \right\}$$

und ${}^{H_R}/_{Z_{H_R}} \cong R^2$.

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

*Beweis.* Auf Grund des Korollars vom Anfang der Stunde wissen wir

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

Da $|G| = p^k$ ist, ist $[G : \mathrm{Stab}_G(t)] = p^l$ für $l \geq 1$ wenn $t \notin \mathrm{Fix}_G(T)$. Daher gilt $p \mid \sum_{|G \cdot t|>1} [G : \mathrm{Stab}_G(t)]$. □

**Satz.** *Eine $p$-Gruppe ist nilpotent.*

*Beweis.* Angenommen $p$ ist eine Primzahl und $G$ ist eine $p$-Gruppe. Wir definieren $T = G$ und machen $G$ zu einer $G$-Menge mittels Konjugation. Dann gilt

$$\mathrm{Fix}_G(T) = \{t \in G \mid gtg^{-1} = t \; \forall g \in G\} = Z_G.$$

Wegen obigem Lemma gilt also

$$|\mathrm{Fix}_G(T)| = |Z_G| = \equiv |T| = |G| = p^k = 0 \mod p.$$

Da $e \in Z_G$ gilt $|T_G| \geq 1$, also $|Za| \geq p$. Insbesondere ist $Z_G$ eine nichttriviale Untergruppe, und ${}^{G}/_{Z_G}$ ist eine kleinere $p$-Gruppe.

Falls $|G| = p$ ist, so ist $G = Z_G$ zyklisch, also abelsch, also nilpotent mit Nilpotenzgrad 1.

Ansonsten: Mittels Induktion nach $G$ dürfen wir bereits annehmen, dass ${}^{G}/_{Z_G}$ nilpotent mit Nilpotenzgrad $e$ ist. Demnach ist also $G$ nilpotent mit Nilpotenzgrad $l + 1$. □

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

*Beweis.* Aus dem Satz erhalten wir, dass $Z_G$ eine nichttriviale Untergruppe ($|Z_G| > 1$) ist. Falls $Z_G = G$ ist, so folgt das Korollar. Angenommen dem ist nicht so, dann ist $|Z_G| = p$. Dann ist aber ${}^{G}/_{Z_G}$ eine Gruppe der Ordnung $p$ und damit zyklisch. Also existiert ein $g \in G$ so dass ${}^{G}/_{Z_G} = \langle gZ_G \rangle = \{g^k Z_p \mid k = 0, \ldots, p-1\}$. Insbesondere gilt also

$$G = \{g^k z \mid k = 0, \ldots, p-1, z \in Z_G\}.$$

Damit gilt aber für $g^{k_1} z_1, g^{k_2} z_2 \in G$, dass $g^{k_1} z_1 g^{k_2} z_2 = g^{k_1+k_2} \underbrace{z_1 z_1}_{=z_2 z_1} = g^{k_2} z_2 g^{k_1} z_1$. Dies widerspricht der Annahme, dass $Z_G \subsetneq G$. □

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

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

jede Untergruppe in der nächsten normal ist.

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

**Beispiel.**
1. Diedergruppe $D_{2\cdot n}$ ist auflösbar.
2. Affine Gruppe $A_R = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in R^\times, b \in R \right\}$ ist auflösbar und ist nicht nilpotent falls $|R^\times| > 1$.

**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 $\varphi$ induziert einen Gruppenhomomorphismus $\overline{\varphi} : G/[G,G] \to H$. In diesem Sinne ist $G/[G,G]$ die größte abelsche Faktorgruppe von $G$.*

*Beweis.* In der Tat ist $[G,G]$ eine charakteristische Untergruppe (siehe Übung) und damit auch normal. Seien $a,b \in G$. Dann gilt $[a[G,G], b[G,G]] = [a,b][G,G] = [G,G]$, aber dies bedeutet genau, dass die Elemente $a[G,G]$ und $b[G,G]$ in $G/[G,G]$ kommutieren. Da $a,b \in G$ beliebig waren, ist also $G/[G,G]$ abelsch.

Sei nun $H$ abelsch und $\varphi : G \to H$ ein Homomorphismus. Für $a,b \in G$ gilt dann

$$\varphi([a,b]) = [\varphi(a), \varphi(b)] = e_H$$

Da dies für alle $a,b \in G$ gilt und $[G,G]$ von diesen Elementen erzeugt wird, erhalten wir daraus $\varphi([G,G]) = \{e_H\}$. Auf Grund eines Korollars zum ersten Isomorphiesatz gibt es damit einen Homomorphismus

$$\begin{tikzcd} G/[G,G] \arrow[r, "\overline{\varphi}"] & H \\ G \arrow[u, "\pi"] \arrow[ur, "\varphi"'] & \end{tikzcd}$$

mit $\varphi = \overline{\varphi} \circ \pi$. $\square$

**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:*

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

*Beweis.* Angenommen $G^{(n+1)} = \{e\}$ für ein $n \in \mathbb{N}$. Dann ist

$$\{e\} = G^{(n+1)} \lhd G^{(n)} \lhd G^{(n-1)} \lhd \ldots \lhd G^{(1)} \lhd G^{(0)}$$

eine Subnormalreihe für $G$ (mit umgekehrter Index-Reihenfolge). Des Weiteren sind die Quotienten $G^{(k)}/G^{(k+1)}$ auf Grund der letzten Proposition abelsch. Also ist $G$ auflösbar.

Sei nun umgekehrt $G$ auflösbar und $\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ eine Subnormalreihe mit abelschen Faktorgruppen. Da $G/G_{n-1} = G_n/G_{n-1}$ abelsch ist, gilt $[G,G] = G^{(1)} < G_{n-1}$. Mittels Induktion können wir analog $G^{(k)} < G_{n-k}$. Für $k = n$ erhalten wir also $G^{(n)} < G_0 = \{e\}$. $\square$

## 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.*

*Beweis.* Sei $S = \mathbb{Z}/(p^k) \times \{1, \ldots, m\}, G = \mathbb{Z}/(p^k)$, und definiere eine Wirkung von $G$ auf $S$ durch Addition in der ersten Komponente: $g \cdot (a, j) = (a + g, j)$. Wir bemerken dass die $G$-Bahnen in $S$ genau die Mengen der Form $G \times \{i\}$ für ein $j \in \{1, \ldots, m\}$ sind.

Wir definieren $T = \{A \subseteq S : \text{Teilmenge mit } |A| = p^k\}$ und lassen $G$ auf $A \in T$ mittels $g \cdot A = \{g \cdot (a, j) \mid (a, j) \in A\}$ wirken. Damit ist $T$ eine $G$-Menge.

Da $G$ eine $p$-Gruppe ist, können wir das frühere Lemma über $p$-Gruppen und Fixpunkte verwenden:

$$\binom{n}{p^k} = |T| = |\mathrm{Fix}_G(T)| = m \not\equiv 0 \mod px.$$

nach Annahme im Lemma.

$$\begin{aligned} A \in \mathrm{Fix}_G(T) &\Leftrightarrow A \subseteq S, |A| = p^k \text{ und } g \cdot A = A \text{ für alle } g \in G \\ &\Leftrightarrow A \subseteq S, |A| = p^k \text{ und } A \text{ ist eine Vereinigung von } G\text{-Bahnen} \\ &\Leftrightarrow A \subseteq S \text{ ist eine } G\text{-Bahn} \\ &\Leftrightarrow A = G \times \{j\} \text{ für ein } j \in \{1, \ldots, m\}. \end{aligned}$$

**Beispiel** (Sylow-Untergruppe)**.** Sei $G = \mathrm{SL}_2(\mathbb{F}_p)$ mit Ordnung $p(p^2 - 1)$. Dann ist $H_p = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_p\} \cong \mathbb{F}_p$ eine Sylow $p$-Untergruppe.

$\square$

*Beweis von 1) Satz.* Sei $T = \{A \subseteq G : |A| = p^k\}$. Dann ist $T$ eine $G$-Menge mittels Linksmultiplikation ($A \in T, g \in G, g \cdot A = \{g \cdot a \mid a \in A\}$) mit $|T| = \binom{n}{p^k} \not\equiv 0 \mod p$. Auf Grund eines Korollars zu dem Satz über Bahn und Stabilisator gilt

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

Falls $n = p^k$ ist, so ist $H_p = G$ selbst die gesuchte Sylow $p$-Untergruppe. Ansonsten ist $p^k < n$ und es gibt keine $G$-invariante Teilmenge $A \subseteq G$ mit $|A| = p^k$. Also ist $\mathrm{Fix}_G(T) = \{\}$. Da $|T| \not\equiv 0 \mod p$, folgt aus $(*)$, dass es ein $A \in T$ gibt, so dass $[G : \mathrm{Stab}(A)] \not\equiv 0 \mod p$ ist.

*Bemerkung.* $H_p = \mathrm{Stab}_G(A_0)$ ist eine Sylow $p$-Untergruppe mit $|H_p| = p^k$.

Da $|G| = |H_p|[G : H_p] = p^k m$ und $p \notin [G : H_p]$, folgt $p^k \mid |H_p|$. Des Weiteren wissen wir $H_p \cdot A_0 = A_0$. Sei $a_0 \in A_0$ beliebig, dann gilt also $h \cdot a_0 \in H_p \cdot A_0 = A_0$ für alle $h \in H_p$. Also gilt $H_p = a_0 \subseteq A_0$ und $|H_p| = |H_p \cdot a_0| \leq |A_0| = p^k$. Dies beweist die Behauptung und damit 1) im Satz. $\square$

*Beweis von 2).* Sei $H$ eine beliebige $p$-Untergruppe und $H_p$ eine beliebige Sylow $p$-Untergruppe. Wir definieren $T = {}^{G}/_{H_p}$ und lassen $H$ mittels Linksmultiplikation auf $T$ wirken. Wegen dem Lemma über Fixpunkte von $p$-Gruppen gilt

$$|\mathrm{Fix}_H(T)| \equiv |T| = [G : H_p] = \frac{n}{p_k} = m \not\equiv 0 \mod p.$$

Insbesondere gibt es einen Fixpunkt $gH_p \in T$ (für die Wirkung von $H$ ). D.h.

$$\begin{aligned}
&hgH_p = gH_p \text{ für alle } h \in H \\
&\Rightarrow hg \in gH_p \in \text{ für alle } h \in H \\
&\Rightarrow h \in gH_pg^{-1} \text{ für alle } h \in H \\
&\Rightarrow H < gH_pg^{-1} \;\&\; gH_pg^{-1} \text{ ist eine Sylow } p\text{-Untergruppe}
\end{aligned}$$

□

*Beweis von 3).* Angenommen $H, H_p$ sind zwei Sylow $p$-Untergruppen. Dann ist $H$ eine $p$-Untergruppe und obiger Beweis von 2) zeigt, dass es ein $g \in G$ mit $H < gH_pg^{-1}$ gibt. Da aber $|H| = |H_p| = p^k$ ist, gilt $H = gH_pg^{-1}$. □

## 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 $\tau_{ij}$ *für $i \neq j$ das Vorzeichen $-1$ mit*

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

**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.

*Beweis.* Siehe lineare Algebra. Alternative Beweis-Skizze: Für $F \in \mathbb{Z}[X_1, \ldots, X_n]$ definieren wir ${}^{\sigma}F = F(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. Dies definiert eine Gruppenwirkung von $S_n$ auf $\mathbb{Z}[X_1, \ldots, X_n]$ mittels Ringhomomorphismen. Wir definieren $P = \prod_{1 \leq i < j \leq n}(X_i - X_j)$ und erhalten

$${}^{\sigma}P = \prod_{1 \leq i < j \leq n} (X_{\sigma(i)} - X_{\sigma(j)} = \mathrm{sgn}(\sigma)P.$$

kann als Definition von $\mathrm{sgn}(\sigma)$ verwendet werden. □

*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 $\sigma$ sind, so nennen wir $\sigma$ einen *(k-)Zyklus* und schreiben

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

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

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

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

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

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

**Beispiel.** $n = 5$

$$(3,2,5) = (2,5,3) = \sigma : \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 5 \\ 3 \mapsto 2 \\ 4 \mapsto 4 \\ 5 \mapsto 3 \end{cases} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}.$$

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

**Beispiel.** $n = 5 : (2,5,3)$ und $(1,2,3)$ sind konjugiert.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} \in S_n$$

$$\sigma(1,2,3)\sigma^{-1} = \begin{cases} 1 \mapsto 4 \mapsto 4 \mapsto 1 \\ 2 \mapsto 1 \mapsto 2 \mapsto 5 \\ 3 \mapsto 3 \mapsto 1 \mapsto 2 \\ 4 \mapsto 5 \mapsto 5 \mapsto 4 \\ 5 \mapsto 2 \mapsto 3 \mapsto 3 \end{cases} = (2,5,3)$$

*Beweis-Skizze (Seite 122).* Sei $\sigma \in S_n$ beliebig und $(i_1, \dots, i_k)$ ein Zyklus. Dann ist

$$\sigma(i_1, \dots, i_k)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \dots, \sigma(i_k))$$

mit einer kleinen Rechnung wie im Beispiel.

Dies gilt analog auch für Produkte von Zyklen für zwei Permutationen mit demselben Zyklentyp kann man $\sigma$ finden:

$$\begin{aligned} \tau_1 &= (i_{1,1}, \dots, i_{1,k_1})(i_{2,1}, \dots, i_{2,k_2}) \dots (i_{r,1}, \dots, i_{r,k_r}) \overbrace{(i_{r+1}) \dots (i_s)}^{\text{Fixpunkte von } \tau_1} \\ \tau_2 &= (j_{1,1}, \dots, j_{1,k_1})(j_{2,1}, \dots, j_{2,k_2}) \dots (j_{r,1}, \dots, j_{r,k_r}) \underbrace{(j_{r+1}) \dots (j_s)}_{\text{Fixpunkte von } \tau_2}. \end{aligned}$$

wobei in beiden Zeilen jede Zahl von $1, \dots, n$ einmal auftritt. Definiere man nun $\sigma$ mittels $\sigma(i_*) = j_*$. □

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

*Beweis für $n \leq 4$ .* $A_1 \cong A_2 \cong \{e\}$
$A_3 \cong \mathbb{Z}/(3)$ ist abelsch.
$A_4$ : $V_4 = \langle(1,2)(3,4),(1,3)(2,4)\rangle = \{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$ (Kleinsche Vierergruppe) ist eine Untergruppe (wo jedes nichttriviale Element Ordnung 2 hat). Dies bedarf einer kleinen Nebenrechnung, z.B.

$$(1,2)(3,4)\cdot(1,3)(2,4) = \begin{cases} 1 \mapsto 3 \mapsto 4 \\ 4 \mapsto 2 \mapsto 1 \\ 2 \mapsto 4 \mapsto 3 \\ \quad \dots \end{cases} = (1,4)(2,3)$$

insbesondere ist $V_4 \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

$V_4$ enthält neben $e$ genau die Elemente vom Zyklentyp $2,2$. $\Rightarrow V_4 \lhd A_4$.

$$|A_4| = \frac{4!}{2} = 4\cdot 3 = 12, |V_4| = 4 \Rightarrow |A_4/V_4| = 3 \quad \& \quad A_4/V_4 \cong \mathbb{Z}/(3).$$

Folgt $A_4$ ist auflösbar. Weiters ist $S_4/A_4 \cong \mathbb{Z}/(2)$ also auch $S_4$ auflösbar. □

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

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

*Beweis.* $(1,2,3) \in A_n$ bildet 1 auf 2 ab. Für $i \geq 3$ bildet $(1,i,2) \in A_n$ die 1 auf $i$ ab. Also ist in beiden Fällen die Bahn von 1 ganz $\{1,\dots,n\}$. □

**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.*

*Beweis.* Sei $\sigma \in H$ und $\tau \in A_n$. Dann gilt $[\tau,\sigma] = \tau\sigma\tau^{-1}\sigma^{-1} \in H$, da $\tau\sigma\tau^{-1}\sigma^{-1} \in H$. Angenommen $\sigma \in H\setminus\{e\}$. Falls $\sigma$ einen Fixpunkt hat, so gilt das Lemma in diesem Fall. Wir nehmen also an, dass $\sigma$ keinen Fixpunkt hat und werden je nach Zyklentyp von $\sigma$ immer ein $\sigma' \in H\setminus\{e\}$ finden, dass ein Fixpunkt besitzt (Meist $\sigma' = [\tau,\sigma]$ für ein geeignetes $\tau \in A_n$).

- $\sigma$ enthält ein Zyklus der Länge $k \geq 4$. Sei $\sigma = (i_1,i_2,i_3,\dots,i_k)\dots$ und $\tau = (i_1,i_2,i_3) \in A_n$. Folgt

$$\sigma' = [\tau,\sigma] = (i_1,i_2,i_3)\sigma(i_1,i_2,i_3)^{-1}\sigma^{-1} : \begin{cases} i_1 \overset{\sigma^{-1}}{\mapsto} i_k \mapsto\overset{\tau^{-1}}{\mapsto} i_k \overset{\sigma}{\mapsto} i_1 \overset{\tau}{\mapsto} i_2 \\ i_3 \overset{\sigma^{-1}}{\mapsto} i_2 \mapsto\overset{\tau^{-1}}{\mapsto} i_1 \overset{\sigma}{\mapsto} i_2 \overset{\tau}{\mapsto} i_3 \end{cases}$$

  Nichttrivial (wegen $k \geq 4$), ein Fixpunkt.
- $\sigma$ enthält sowohl Zyklen der Länge 2 als auch Zyklen der Länge 3. $\sigma' = \sigma^2 \in H$ hat Zyklen der Länge 3 und Fixpunkte.
- $\sigma$ enthält nur Zyklen der Länge 3 (mind. 2 wegen $n \geq 5$ ) Sei $\sigma = (i_1,i_2,i_3)(i_4,i_5,i_6)\dots$ und $\tau = (i_1,i_2,i_4)$. Folgt

$$\sigma' = [\tau,\sigma] = (i_1,i_2,i_4)\sigma(i_1,i_2,i_4)^{-1}\sigma^{-1} : \begin{cases} i_1 \overset{\sigma^{-1}}{\mapsto} i_3 \mapsto\overset{\tau^{-1}}{\mapsto} i_3 \overset{\sigma}{\mapsto} i_1 \overset{\tau}{\mapsto} i_2 \\ i_6 \overset{\sigma^{-1}}{\mapsto} i_5 \mapsto\overset{\tau^{-1}}{\mapsto} i_5 \overset{\sigma}{\mapsto} i_6 \overset{\tau}{\mapsto} i_6 \end{cases}$$

  Nichttrivial, ein Fixpunkt.

- $\sigma$ enthält nur Zyklen der Länge 2 (mind. wegen $N \geq 5$ ) Sei $\sigma = (i_1, i_2)(i_3, i_4)(i_5, i_6)\dots$ und $\tau = (i_1, i_2, i_3)$. Folgt

$$\sigma' = [\tau, \sigma] = (i_1, i_2, i_3)\sigma(i_1, i_2, i_3)^{-1}\sigma^{-1} : \begin{cases} i_1 \overset{\sigma^{-1}}{\mapsto} i_2 \mapsto \overset{\tau^{-1}}{\mapsto} i_1 \overset{\sigma}{\mapsto} i_2 \overset{\tau}{\mapsto} i_3 \\ i_5 \overset{\sigma^{-1}}{\mapsto} i_6 \mapsto \overset{\tau^{-1}}{\mapsto} i_6 \overset{\sigma}{\mapsto} i_5 \overset{\tau}{\mapsto} i_5 \end{cases}$$

  Nichttrivial (wegen $k \geq 4$). Es existiert Fixpunkt.

Dies deckt alle Fälle ab. $\square$

*Beweis, dass $A_5$ einfach ist.* Sei $\{e\} \neq H \lhd A_5$ und $\sigma \in H \setminus \{e\}$ eine Permutation mit einem Fixpunkt wie im Lemma. Insbesondere ist $\sigma$ kein 5-Zyklus und wegen $\sigma \in H$ auch kein 4-Zyklus. Also ist $\sigma$ entweder ein 3-Zyklus oder mit Zyklentyp $2, 2$. Angenommen $\sigma = (i_1, i_2)(i_3, i_4)$ und $\tau = (i_1, i_2, i_3)$ für $i_5 \neq i_1, i_2, i_3, i_4$. Dann ist $\tau\sigma\tau^{-1} = (i_2, i_5)(i_3, i_4)$ und

$$\underbrace{\sigma}_{\in H}\underbrace{\tau\sigma\tau^{-1}}_{\in H} = (i_1, i_2)(i_3, i_4)(i_2, i_5)(i_3, i_4) = \begin{cases} i_1 \mapsto i_1 \mapsto i_1 \mapsto i_1 \mapsto i_2 \\ i_2 \mapsto i_2 \mapsto i_5 \mapsto i_5 \mapsto i_5 \\ i_5 \mapsto i_5 \mapsto i_2 \mapsto i_2 \mapsto i_1 \\ i_3 \mapsto i_4 \mapsto i_4 \mapsto i_3 \mapsto i_3 \\ \dots \end{cases} = (i_1, i_2, i_5) \in H.$$

Also enthält $H$ auch einen 3-Zyklus.

*Behauptung.* Alle 3-Zyklen sind in $A_5$ konjugiert. Also enthält die normale Untergruppe $H$ alle 3-Zyklen. Sei $\sigma = (i_1, i_2, i_3)$ für beliebige verschiedene $i_1, i_2, i_3 \in \{1, \dots, 5\}$. Wir definieren $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_2 & i_2 & i_3 & * & \diamond \end{pmatrix}$, wobei wir die verbleibenden Eintragungen $* \neq \diamond$ in $\{1, \dots, 5\} \setminus \{i_1, i_2, i_3\}$ wählen. Falls $\operatorname{sgn}(\tau) = -1$ vertauschen wir $*$ und $\diamond$ und erhalten $\tau \in A_n$. Damit gilt dann $\tau(1, 2, 3)\tau^{-1} = (i_1, i_2, i_3)$, was die Behauptung beweist. Wir berechnen

$$(i_1, i_2, i_3)(i_2, i_3, i_4) = (i_1, i_2)(i_3, i_4) \quad \text{und} \quad \underbrace{(i_1, i_2, i_3)(i_3, i_4, i_5)}_{\in H} = (i_1, i_2, i_3, i_4, i_5)$$

für eine beliebige Aufzählung $i_1, \dots, i_5$ von $1, \dots, 5$. Folgt $H = A_5$ enthält alle 5-Zyklen und alle Elemente vom Zyklentyp $2, 2$.

$\square$

*Beweis für $n > 5$ mittels Induktion.* Angenommen $\{e\} \neq H \lhd A_n$ und $\sigma \in H \setminus \{e\}$ hat einen Fixpunkt. Wegen dem ersten Lemma dürfen wir auch ohne Beschränkung annehmen, dass $\sigma(n) = n$.

$$\Rightarrow \{e\} \neq H \cap A_{n-1} \lhd A_{n-1}.$$

Nach Induktionsannahme gilt also $H \cap A_{n-1} = A_{n-1}$. Wegen dem ersten Lemma folgt, dass jedes Element von $A_n$ mit einem Fixpunkt zu einem Element von $A_{n-1}$ konjugiert ist. Zusammengenommen erhalten wir, dass $H$ jedes Element mit einem Fixpunkt enthält.

Sei $\sigma \in A_n$ beliebig.

- Falls $\sigma$ einen Fixpunkt hat so ist $\sigma \in H$.
- Ansonsten schreiben wir $\sigma = (1, \sigma(1), i)((1, \sigma(1), i)^{-1}\sigma)$ wobei $i \in \{1, \dots, n\} \setminus \{1, \sigma(1)\}$ und der erste Zyklus $n - 3$ Punkte fixiert und der zweite einen fixiert und daher beide in $H$ sind.

Es folgt also $\sigma \in H$.

Da $\sigma \in A_n$ beliebig war, gilt $H = A_n$. □

## 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 $G$.*

*Beweis.* Seien $N \lhd G$ und ${}^{G}/_{N}$ auflösbar. Dann existieren Subnormalreihen

$$\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_l = N \qquad (*_1)$$

$$\{eN\} = H_0 \lhd H_1 \lhd \ldots \lhd H_m = {}^{G}/_{N} \qquad (*_2)$$

mit abelschen Faktorgruppen. Sei $\pi : G \to {}^{G}/_{N}$ die kanonische Projektion. Wir definieren

$$G'_j = \pi^{-1}(H_i) < G$$

und erhalten

$$G_l = N = \pi^{-1}(eN) = G'_0 < G'_1 < \ldots < G'_m = G.$$

*Behauptung.* $G'_{j-1} \lhd G'_j$ und ${}^{G'_j}/_{G'_{j-1}} \cong {}^{H_j}/_{H_{j-1}}$ für $j = 1, \ldots, m$.

Gemeinsam mit $(*_1)$ beweist die Behauptung die Proposition, da damit die Subnormalreihe

$$\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_l = N = G'_0 \lhd \ldots \lhd G'_m = G$$

alle Eigenschaften wie in der Definition erfüllt.

Seien $h \in G$ □

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 $j = 1, \ldots, n$.*

*Beweis Idee.* Verwende $\phi(m) = \phi(\sum_{j=1}^n m_j b_j) = \sum_{j=1}^n m_j \phi(b_j) = \sum_{j=1}^n m_j a_j$ □

**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 $F_n$** : $F_n = \{$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

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

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 $N = \langle g w g^{-1} \mid g \in F_n, w \in W \rangle$ der von $W$ erzeugte Normalteiler von $F_n$. Dann heißt $F_n/N$ die *Gruppe mit Erzeugenden* $b_1, \ldots, b_n$ und Relationen $w \in W$ und wird mit $\langle b_1, \ldots, b_n \mid w = e \text{ für } w \in W \rangle$ bezeichnet.

**Beispiel.**
- $\mathbb{Z}^2 \cong \langle a, b \mid ab = ba \rangle = \langle a, b \mid aba^{-1}b^{-1} = c \rangle$
- $D_6 \cong \langle D, R \mid D^3 = R^3 = e, RDR = D^{-1} \rangle$

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

*Beweis.* Übung ☐

**Beispiel.**
0. Falls $R = K$ ein Körper ist, so reden wir genau über *Vektorräume über $K$*.
1. $M = R$ ist ein $R$-Modul und Ideale $I < R$ sind genau die Untermoduln von $R$.
2. Angenommen $M, N$ sind $R$-Moduln. Dann ist auch

$$\mathrm{Hom}_R(M, N) = \{f : M \to N \mid f \text{ ist } R\text{-linear}\}$$

   ein $R$-Modul: $(f_1 + f_2)(m) = f_1(m) + f_2(m)$ und $(a \cdot f)(m) = a \cdot f(m)$.
3. Sei $R = \mathbb{Z}$. Dann ist jede abelsche Gruppe $M$ auch ein $\mathbb{Z}$-Modul. Falls wir $\mathbb{Z}$-Modul klassifizieren können, so erhalten wir eine Klassifikation von abelschen Gruppen. Dies ist eines der *Hauptziele des Kapitels.*

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

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

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

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

*Beweis.* Übung □

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

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

*Beweis.* Übung □

**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* $f = \sum_k a_k X^k \in K[X]$ | $\longleftarrow$ | $\varphi$ |

*Beweis.* Angenommen $\cdot : K[X] \times M \to M$ definiert eine Modulstruktur auf $M$ über $K[X]$. Dann ist $\varphi(m) = X \cdot m$ für $m \in M$ eine $K$-lineare Abbildung auf $M$.

$$\begin{cases} \varphi(m_1 + m_2) = X \cdot (m_1 + m_2) = Xm \cdot_1 + X \cdot m_2 = \varphi(m_1) + \varphi(m_2) \\ \varphi(a \cdot m) = X \cdot (a \cdot m) = (aX) \cdot m = a \cdot \varphi(m) \end{cases}.$$

Angenommen $\varphi : M \to M$ ist $K$-linear. Dann definiert $f = \sum_k a_k X^k \in K[X] \mapsto f(\varphi) = \sum_k a_k \varphi^k \in \mathrm{Hom}_K(M,M)$ einen Ringhomomorphismus. Wir verwenden dies um $f \cdot m = (f(\varphi))(m)$ für $f \in K[X]$ und $m \in M$ zu definieren. Dies erfüllt die Axiome eines $K[X]$-Moduls:
Z.B. gilt für $f_1, f_2 \in K[X], m \in M$

$$f_1 \cdot (f_2 \cdot m) = f_1(\varphi)(f_2(\varphi)m) = \underbrace{(f_1(\varphi) \cdot f_2(\varphi))}_{=(f_1 \cdot f_2)(\varphi)} = (f_1 \cdot f_2) \cdot m.$$

wobei $(f_1 \cdot f_2)(\varphi)$ die Auswertung ein Ringhomomorphismus ist. Diese beiden Abbildungen sind invers zueinander.

$$\cdot \mapsto \begin{cases} \varphi(m) = X \cdot m \\ \varphi^2(m) = X^2 \cdot m \\ \quad \vdots \end{cases} \mapsto f(X) \cdot m = \sum_k a_k (\underbrace{X^k \cdot m}_{=\varphi^k(m)}) = f \cdot m$$

$$\varphi \mapsto \begin{cases} \cdot \text{ definiert durch} \\ f \cdot m = f(\varphi)m \end{cases} \mapsto X \cdot m = \varphi(m).$$

Wobei $*$ die neue Skalarmultiplikation und $\cdot$ die alte Skalarmultiplikation ist. Und außerdem $X \cdot m$ die neue lineare Abbildung und $\varphi(m)$ die alte lineare Abbildung ist. □

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.*

*Beweis.* Sei $J_{\max} \subseteq R$ ein Maximalideal (welches auf Grund eines Satzes aus dem Kapitel über Ringe existiert). Sei $M$ ein freier $R$-Modul. Dann ist

$$J_{\max} \cdot M = \{\sum_k a_k m_k \mid a_k \in J_{\max}, m_k \in M\}$$

ist ein Untermodul. Sei $I$ eine Menge mit $M \cong R^{(I)}$. Dann gilt

$$J_{\max} \cdot M \quad \text{wird auf} \quad \{\sum_{i \in I} a_i e_i \mid a_i \in J_{\max}, a_i = 0 \text{ für alle bis auf endlich viele } i \in I\}$$

abgebildet. Daraus folgt, dass

$$M/_{J_{\max} \cdot M} \cong (R/_{J_{\max}})^{(I)}$$

ein Vektorraum über $R/_{J_{\max}}$ der Dimension $|I|$ ist. Das Lemma folgt nun aus der Linearen Algebra. □

*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.*

*Beweis.* 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.

**Beispiel.**
- Sei $R = \mathbb{Z}$ und $M = G$ eine additiv geschriebene endliche abelsche Gruppe. Dann ist $M$ ein Torsionsmodul. Jedes $g \in M$ hat endliche Ordnung $n < \infty$ womit $n \cdot g = 0$ ist.
- Sei $R = \mathbb{Z}$. Dann ist $M = \mathbb{Q}/\mathbb{Z}$ ein Torsionsmodul.
- Sei $V$ ein endlich-dimensionaler Vektorraum über einem Körper $K$, und $A : V \to V$ $K$-linear. Wir verwenden $A$ um $V$ zu einem $K[X]$-Modul zu machen. Dann ist $V$ ein Torsionsmodul über $K[X]$. Sei $v \in V \setminus \{0\}$. Dann ist die Abbildung $f \in K[X] \mapsto f \cdot v \in V$ nicht injektiv (wegen $\dim(V) < \infty = \dim(K[X])$ ). Also gibt es ein $f \in K[X] \setminus \{0\}$ mit $f \cdot v = 0$.
- Falls $R$ ein Integritätsbereich ist in $M$ ein freier $R$-Modul ist, so ist $M$ torsionsfrei.

## 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.*

**Beispiel.** Für $R = K[X_1, X_2, \ldots]$ ist der Untermodul $I = \langle X_1, X_2, \ldots \rangle$ nicht endlich erzeugt.

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

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

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

*und $n$ ist der Rang von $M/M_{\text{tors}}$. 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 $\leq n$.*

*Beweis.* Sei $e_i$ für $i = 1, \ldots, n$ die Standardbasis von $R^n$. Wir definieren die Untermoduln

$$M_i = M \cap \langle e_1, e_2, \ldots, e_i \rangle \quad \text{für} \quad i = 1, \ldots, n.$$

Dann gilt $M_n = M$.

*Behauptung.* $M_i$ ist ein freier Modul mit Rang $\leq i$. Wir beweisen die Behauptung mittels Induktion nach $i$.

**Induktionsanfang:** Für $i = 1$ ist $M_1 = M \cap \langle e_1 \rangle \cong J \subseteq R$. Dies zeigt, dass $M_1$ isomorph zu einem Ideal $J$ in $R$. Da $R$ ein Hauptidealring ist, folgt entweder $J = (0)$ und $M_i = \{0\}$ hat Rang 0 oder $J = (d_1)$ für $d_1 \in R \setminus \{0\}$ und $M_1 \cong (d_1) \cong \underbrace{R}_{\in a \mapsto ad_1}$ hat Rang 1.

**Induktionsschritt:** Angenommen $M_{i-1}$ ist frei mit Rang $\leq i-1$. Wir betrachten die Abbildung $\phi : M_i \to R, (x_1, \ldots, x_i, 0, \ldots, 0) \mapsto x_i$. Das Bild $\mathrm{Im}(\phi)$ ist ein Untermodul von $R$ also entweder $\mathrm{Im}(\phi) = \{0\}$, und $M_i = M_{i-1}$ ist frei mit Rang $\leq i-1 < i$. Oder $\mathrm{Im}(\phi) = (d_i)$ und es gibt ein $m_i \in M_i$ mit $\phi(m_i) = d_i$. In diesem Fall definieren wir

$$\psi : M_{i-1} \times R \to M_i \qquad (m', a) \mapsto m' + am_i \in M_i.$$

Wir zeigen, dass $\psi$ ein Isomorphismus ist. Dies impliziert dann, dass $M_i$ frei ist und der Rang von $M_i$ eins höher ist als der Rang von $M_{i-1}$.

**Injektivität von $\psi$:** $\psi(m', a) = 0 = m' + am \underset{\phi(m')=0}{\overset{\phi}{\mapsto}} ad_i$ und $m' = 0$.

**Surjektivität von $\psi$:** Sei $m \in M_i$ beliebig, dann ist $\phi(m) \in \mathrm{Im}(\phi) = (d_i)$ und es existiert ein $a \in R$ mit $\phi(m) = ad_i$. Damit ist aber $m' = m - am_i \in M_{i-1}$ und $m = m' + am_i \in \mathrm{Im}(\phi)$.

Dies schließt den Induktionsschritt und damit den Beweis. $\square$

*Beweis des ersten Teils vom Klassifikationssatz.*

- $M_{\mathrm{tors}}$ ist ein Untermodul, z.B. $a_1 m_1 = 0 = a_2 m_2$, $m_1, m_2 \in M_{\mathrm{tors}}$ für $a_1, a_2 \in R \setminus \{0\}$ Impliziert $a_1 a_2 (m_1 + m_2) = a_2 \underbrace{a_1 m_1}_{=0} + a_1 \underbrace{a_2 m_2}_{=0} = 0$.
- Da $R$ ein Integritätsbereich ist, hat ein freier Modul ($\cong R^l$ ) keine nichttrivialen Torsionselemente. Also gilt $M$ frei $\Rightarrow M_{\mathrm{tors}} = \{0\}$.
- Wir zeigen nun die Umkehrung dieser Aussage, also $M_{\mathrm{tors}} = \{0\} \Rightarrow M$ ist frei.
  Seien $x_1, \ldots, x_n \in M$ eine Erzeugendenmenge von $M$. Wir wählen aus dieser Liste eine maximale l.u. Teilmenge $y_1 \ldots, y_k$ aus. Dies impliziert $N = \langle y_1, \ldots, y_k \rangle \cong R^k$.

  *Behauptung.* Für alle $x_i$ in der Erzeugendenmenge gibt es ein $a_i \in R \setminus \{0\}$ mit $a_i x_i \in N$. Falls $x_i = y_i$ ein Erzeuger von $N$ ist, so setzen wir $a_i = 1$.

  *Beweis von $M$ ist frei mittels der Behauptung.* Für $a = a_1 \cdot a_2 \cdot \ldots \cdot a_n$ gilt auf Grund der Behauptung $aM \subseteq N \cong R^k$. Also ist $aM$ isomorph zu einem Untermodul von $R^k$ und wegen der Proposition selbst frei. Des Weiteren ist $a\cdot : M \to aM$ ein Isomorphismus und daher ist auch $M$ frei, weil $\mathrm{Ker}(a\cdot) = \{m \in M \mid am = 0\} \subseteq M_{\mathrm{tors}} = \{0\}$ $\square$

  *Beweis der Behauptung.* Sei $x_i$ ein Erzeuger von $M$ ungleich $y_1, \ldots, y_k$. Wir definieren $\varphi : R \times N \to M, (a, m) \mapsto ax_i + m$. Dann kann $\varphi$ nicht injektiv sein. Denn wenn $\varphi$ injektiv wäre, so wäre $\mathrm{Im}(\varphi)$ frei mit Rang $k+1$ und $y_1, \ldots, y_k$ wäre nicht maximal gewesen. Es gibt also $(a, m) \neq 0$ mit $ax_i + m = 0$. Falls $a = 0$, so wäre auch $m = 0$. Also gilt $a + 0$ und $ax_i \in N$ und die Behauptung gilt. $\square$

  Dies beweist die Äquivalenz: $M$ ist frei $\Leftrightarrow M_{\mathrm{tors}} = \{0\}$.

Sei nun $M$ ein beliebiger endlich erzeugter $R$-Modul. Dann ist $M' = {}^{M}/_{M_{\mathrm{tors}}}$ ebenso endlich erzeugt. Des Weiteren ist $M'$ torsionsfrei (also frei wegen obiger Aussage). Sei $m + M_{\mathrm{tors}} \in M'$ ein Torsionselement und $a \in R \setminus \{0\}$ mit $a(m + M_{\mathrm{tors}}) = 0 + M_{\mathrm{tors}}$. Dies impliziert also $am \in M_{\mathrm{tors}}$. Also existiert ein $b \in R \setminus \{0\}$ mit $bam = 0$. Folgt $\underbrace{(ab)}_{\in R \setminus \{0\}} \cdot m = 0 \Rightarrow m \in M_{\mathrm{tors}}$ und $m + M_{\mathrm{tors}} = 0 + M_{\mathrm{tors}}$.

Wir erhalten also für einen beliebigen endlich erzeugten Modul $M$, dass ${}^{M}/_{M_{\mathrm{tors}}} \cong R^n$ ein freier Modul ist.

Angenommen $x_1 + M_{\mathrm{tors}}, \ldots, x_n + M_{\mathrm{tors}} \in {}^{m}/_{M_{\mathrm{tors}}}$ sind freie Erzeuger von ${}^{M}/_{M_{\mathrm{tors}}}$. Dann sind auch $x_1, \ldots, x_n$ in $M$ frei (): Falls $\sum_{i=1}^{n} a_i x_i = 0$ in $M$ ist, so ist

$$\sum_{i=1}^{n} a_i (x_i + M_{\mathrm{tors}}) = 0 \Rightarrow a_1 = a_2 = \ldots = 0.$$

Wir definieren $\psi : (a, m') \in R^n x M_{\text{tors}} \mapsto \sum_{i=1}^n a_i x_i + m' \in M$ und behaupten, dass $\psi$ ein Isomorphismus zwischen $R^n \times M_{\text{tors}}$ und $M$ darstellt.

**Injektiv:** Angenommen $\psi(a, m') = \sum_{i=1}^n a_i x_i + m' = 0 \Rightarrow \sum_{i=1}^n a_i(x_i + M_{\text{tors}}) = 0 \Rightarrow a = 0$ & $m' = 0$ Also ist $\psi$ injektiv.

**Surjektiv:** Sei $m \in M$ beliebig. Dann gibt es ein $a \in R^n$ mit $m + M_{\text{tors}} = \sum_{i=1}^n a_i(x_i + M_{\text{tors}})$. Also ist $m - \sum_{i=1}^n a_i x_i = m' \in M_{\text{tors}}$ und $\psi(a, m') = m$. Damit ist $\psi$ auch surjektiv. $\square$

**Satz** (Klassifikationssatz (2. Teil))**.** *Sei $R$ ein Hauptidealring und $M_{\text{tors}}$ 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*

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

**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 $A$.

*Beweis für Euklidische Ringe.* Wir beweisen den Satz mittels doppelter Induktion und zuerst nach $\max(k, l)$.

- Falls $\max(k, l) = 1$ ist, so ist $k = l = 1$ und $A = (0)$ oder $A = (d_1)$ für $d_1 \in R \setminus \{0\}$.
- Wir können annehmen, dass $\max(k, l) > 1$ ist und der Satz für „kleinere“ Matrizen bereits gilt.
  Falls $A = 0$ ist, so gibt es nichts zu beweisen.
  Also können wir annehmen, dass $A \neq 0$. Wir definieren die „Norm von $A$“ durch

  $$N = \min_{A_{ii} \neq 0} \phi(A_{ii}) \in \mathbb{N},$$

  wobei $\phi : R \setminus \{0\}$ die Euklidische Normfunktion von $R$ bezeichnet.
  Durch Vertauschung von Zeilen und Spalten können wir annehmen, dass

  $$d_1 = A_{11} \neq 0 \quad \text{und} \quad \phi(d_1) = N.$$

Wir verwenden Division durch $d_1$ mit Rest und erhalten

$$A_{1j} = a_j d_1 + r_j \quad \text{für} \quad i = 2, \dots, l \quad \text{mit} \quad r_1 = 0 \quad \text{oder} \quad \phi(r_j) < \phi(d_1).$$

Wir ziehen das $a_j$-fache der 1. Spalte von der $j$-ten Spalte für $j = 2, \dots, l$ ab und erhalten die Matrix

$$A' = \begin{pmatrix} d_1 & r_2 & r_3 & \dots & r_l \\ A_{21} & & & & \\ \vdots & & * & & \\ A_{k_1} & & & & \end{pmatrix}.$$

Falls $r_j \neq 0$ für ein $j \in \{2, \dots, l\}$, so ist $N' = \min_{A'_{ij} \neq 0} \phi(A'_{ij} < N$ und wir können per Induktion annehmen, dass $A'$ (und damit auch $A$ ) eine Smith Normalform hat. Also können wir annehmen, dass $r_2 = r_3 = \dots = r_l = 0$ ist.
Analog können wir dieses Argument nun auch für die erste Spalte wiederholen. Damit erhalten wir den verbleibenden Fall

$$A'' = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}.$$

Falls $\min(k, l) = 1$, dann ist $A''$ bereits die Smith Normalform von $A$. Falls $B = 0$, dann ist $A''$ bereits die Smith Normalform von $A$.
Ansonsten hat $B$ Dimension $k-1$ & $l-1$. Also hat nach Induktionsannahme $B$ eine Smith Normalform. Also können wir nach weiteren Zeilen- und Spaltenoperationen eine Matrix der Form

$$A''' = \begin{pmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_n & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}$$

erreichen.
Falls $d_1 \mid d_2$ (und ebenso $d_2 \mid d_3 \mid \dots \mid d_n$ nach Induktionsannahme), dann ist $A'''$ die Smith Normalform von $A$.
Falls $d_1 \nmid d_2$, so addieren wir die zweite Zeile zur ersten, verwenden Division mit Rest und erhalten eine Matrix mit kleinerem Minimum.

$$A''' \longmapsto \begin{pmatrix} d_1 & d_2 & & & \\ & \ddots & & & \\ & & d_n & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix} \mapsto \underbrace{\begin{pmatrix} d_1 & r & & & \\ & \ddots & & & \\ & & d_n & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}}_{\text{Matrix mit kleinerer Norm}} \underset{i.A.}{\longmapsto} A''''$$

wobei $A''''$ in Smith Normalform und $r$ der Rest bei Division durch $d_1$ ist.

Dies schließt die Induktion(en) und den Beweis. □

*Beweis beider Teile des Klassifikationssatzes.* Sei $M$ ein endlich erzeugter $R$-Modul und $R$ ein

Euklidischer Ring. Angenommen $x_1, \dots, x_k \in M$ erzeugen $M$. Dann ist

$$\phi : a \in R^k \mapsto \sum_{i=1}^{k} a_i x_i \in M$$

surjektiv. Sei $N = \operatorname{Ker}(\phi) \subseteq R^k$- ein Untermodul. Nach einer früheren Proposition wissen wir, dass $N$ selbst auch ein freier Modul ist - sei $N = \langle r_1, \dots, r_l \rangle$. Damit ist $M \cong {}^{R^k}/_{N}$ (induziert von $\phi$ ).

Wir definieren die Matrix

$$A = (r_1, \dots, r_l) \in \operatorname{Mat}_{kl}(R)$$

und wenden den Satz über die Smith Normalform an: Es existieren Matrizen $g \in \mathrm{GL}_k(R)$ und $h \in \mathrm{GL}_l(R)$ so dass

$$B = gAh^{-1} = \begin{pmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_n & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix} \qquad d_1 \mid d_2 \mid \dots \mid d_n \quad \text{in} \quad R \setminus \{0\}.$$

Da wir $A$ mit einer $R$-linearen Abbildungen $R^l \to R^k$ identifizieren können erhalten wir

$$\begin{aligned} &N = \operatorname{Im}(A) = A(R^l) \\ &\operatorname{Im}(B) = B(R^l) = ga\,\underbrace{h^{-1}(R^l)}_{R^l} = g\operatorname{Im}(A) = gN. \end{aligned}$$

Des Weiteren erhalten wir

$$R^k \xrightarrow{\sim g} R^k$$
$$N = \operatorname{Im}(A) \xrightarrow{\sim g} gN = \operatorname{Im}(B).$$

Verwende man den Isomorphiesatz indem man die Abbildung

$$\begin{tikzcd} R^k \arrow[r, "g"'] \arrow[rr, bend left, "\psi"] & R^k \arrow[r] & {}^{R^k}/_{gN} \end{tikzcd} .$$

betrachtet folgt ${}^{R^k}/_{\operatorname{Ker}(\psi)} \cong {}^{R^k}/_{gN}$ und $\operatorname{Ker}(\psi) = N$ da $g$ bijektiv ist.

$$M \cong {}^{R^k}/_{N} \xrightarrow{\sim} {}^{R^k}/_{gN} = {}^{R^k}/_{\operatorname{Im}(B)} \cong {}^{R}/_{(d_1)} \times \dots \times {}^{R}/_{(d_n)} \times R^{k-n}$$

und

$$\operatorname{Im}(B) = (d_1) \times (d_2) \times \dots \times (d_n) \times \{0\}^{k-n}.$$

wobei die erste Kongruenz von $\phi$ und die erste Abbildung von $g$ induziert ist. Außerdem gilt wegen dem Isomorphismus

$$\begin{aligned} &{}^{R \times R}/_{(d_1) \times (d_2)} \cong {}^{R}/_{(d_1)} \times {}^{R}/_{(d_2)} \\ &R \times R \xrightarrow{\psi} {}^{R}/_{(d_1)} \times {}^{R}/_{(d_2)} \\ &\operatorname{Ker}(\psi) = \{(a_1, a_2) \mid a_1 \in (d_1), a_2 \in (d_2)\} = (d_1) \times (d_2). \end{aligned}$$

$\square$

## 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*

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

*wobei $G_p$ die Sylow $p$-Untergruppe ist.*

*Beweis.* Folgt aus dem Klassifikationssatz $\square$

## 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 $\varphi$ 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 $\varphi$.*

*Beweis.* Da $V$ ein endlich-dimensional ist und $\mathbb{C}[X]$ unendlich-dimensional ist, muss $V$ ein Torsionsmodul über $\mathbb{C}[X]$ sein (wobei wir $\varphi$ verwenden um die Modulstruktur zu definieren). Ebenso ist $V$ als $\mathbb{C}[X]$-Modul endlich erzeugt weil $V$ endlich-dimensional ist.

Also können wir den Klassifikationssatz für Module anwenden und erhalten

$$V \cong \prod_{\substack{\text{endlich} \\ \text{viele } (\lambda,k)}} \mathbb{C}[X]/((X-\lambda)^k)$$

mit $V$ aufgefasst als $\mathbb{C}[X]$-Modul.

Wir beschreiben nun Multiplikation mit $X$ ($\cong$ Anwendung von $\varphi$ auf Teilräume von $V$ ) auf $\frac{\mathbb{C}[X]}{((X-\lambda)^k)} = M$. $M$ hat über $\mathbb{C}$ die Basis

$$1, (X-\lambda), (X-\lambda)^2, \ldots, (X-\lambda)^{k-1}.$$

und $X\cdot$ hat die folgende Matrixdarstellung bzgl. dieser (geordneten) Basis

$$\begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \end{pmatrix}$$

denn

$$
\begin{aligned}
&X \cdot 1 = X = (X-\lambda) + \lambda \cdot 1 \Rightarrow \text{ bestimmt die 1. Spalte} \\
&X \cdot (X-\lambda)^j = (X-\lambda)^{j+1} + \lambda (X-\lambda)^j \Rightarrow \text{ bestimmt die } (j+1)\text{. Spalte} \\
&\vdots \\
&X \cdot (X-\lambda)^{k-1} = (X-\lambda+\lambda)(X-\lambda)^{k-1} = \cancel{(X-\lambda)^k} + \lambda(X-\lambda)^{k-1} = 0 \text{ in } M.
\end{aligned}
$$

Nach Umordnung der Basisvektoren ($(X-\lambda)^{k-1}$ zuerst, 1 zuletzt) ergibt sich ein Jordanblock wie im Satz. □

# 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* $K$.

**Beispiel.**
- $\mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$
- $\mathbb{C} \mid \mathbb{R}$
- $\mathbb{Q}(\sqrt[3]{2}) \cong {}^{\mathbb{Q}[T]}/_{(T^3-2)} \mid \mathbb{Q}$

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

*Beweis.* Angenommen $[F : L] = m$ und $x_1, \dots, x_m \in F$ bilden eine Basis von $F$ über dem Körper $L$. Angenommen $[L : K] = n$ und $y_1, \dots, y_n \in L$ bilden eine Basis von $L$ über dem Körper $K$.

*Behauptung.* Die Produkte $x_i x_j$ für $\begin{cases} i = 1, \dots, m \\ j = 1, \dots, n \end{cases}$ bilden eine Basis von $F$ über dem Körper $K$.

Wir zeigen zuerst, dass diese Produkte l.u. sind. Angenommen $\alpha_{ij} \in K$ und $\sum_{i,j} \alpha_{ij} x_i x_j = 0$. $\Rightarrow \sum_{i=1}^m \left( \underbrace{\sum_{j=1}^n \alpha_{ij} y_j}_{\in L} \right) x_i = 0$ & auf Grund der ersten Annahme erhalten wir $\sum_{j=1}^n \alpha_{ij} y_j = 0$ (für jedes). Folgt $\alpha_{ij} = 0$ auf Grund der zweiten Annahme für $\begin{cases} i = 1, \dots, m \\ j = 1, \dots, n \end{cases}$, d.h. $x_i y_j$ für diese $i, j$ sind l.u. über $K$.

Angenommen $z \in F$. Aufgrund der ersten Annahme existieren dann Elemente $\beta_1, \dots, \beta_m \in L$ s.d. $z = \sum_{i=1}^m \beta_i x_i$, $\beta_i = \sum_{j=1}^n \alpha_{ij} y_j$. Auf Grund der zweiten Annahme für $\beta_i$ existieren auch Elemente $\alpha_{i1}, \dots, \alpha_{in} \in K$ s.d.

$$\Rightarrow z = \sum_{i,j} \underbrace{\alpha_{ij}}_{\in K} x_i y_j.$$

Daher gilt die Behauptung und auch der Satz. □

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

Falls $\varphi_x$ injektiv ist, so heißt $x$ *transzendent* über $K$

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

**Beispiel.**
- $e, \pi$ sind transzendent über $\mathbb{Q}$
- $\sqrt[3]{2}$ ist algebraisch über $\mathbb{Q}$, $\cos(20°)$ ist algebraisch

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

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

*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*

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

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

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

*Beweis.* Die Isomorphie ergibt sich aus dem ersten Isomorphiesatz. Angenommen $x$ ist transzendent. Dann ist

$$K(X) = \{\frac{f(x)}{g(x)} \mid f(T), g(T) \in K[T], g \neq 0\} \cong \{\frac{f(T)}{g(T)} \mid f, g \in K[T], g \neq 0\}.$$

Angenommen $x$ ist algebraisch. Dann ist $(m_x(T)) = \operatorname{Ker}(\varphi_x)$ ein Primideal. In einem Hauptidealring ist ein von $(0)$ verschiedenes Primideal ein Maximalideal $\Rightarrow {}^{K[T]}/_{(m_x(T))}$ ist ein Körper und damit ist $K[X]$ ein Unterkörper von $L$. In ${}^{K[T]}/_{(m_x(T)}$ ist

$$1 + (m_x(T)), T + (m_x(T)), \ldots, T^{\deg(m_x)-1} + (m_x(T))$$

eine Basis. $\square$

**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 ($p - 1 = 2^{2^n}$ ).*

*Beweis-Skizze.* Angenommen nach endlich vielen Konstruktionsschritten ausgehend von einer Einheitslänge und Anwendung von Gerade $\cap$ Gerade, Gerade $\cap$ Kreis, Kreis $\cap$ Kreis, erhalten wir die Länge auf der ersten Geraden, wobei $x = \sqrt[3]{2}$ oder $x = \cos(20°)$.

Wir definieren $L_0 = \mathbb{Q}$, $L_{n+1} = L_n$ falls im nächsten Konstruktionsschritt zwei Geraden geschnitten werden. $L_{n+1} = L_n$ oder eine quadratische Körpererweiterung von $L_n$, die die Koordinaten der Schnittpunkte Geraden $\cap$ Kreis enthält Kreis $\cap$ Kreis

$$\begin{cases} (x-x_0)st + (y-y_0)^2 = r^2 \\ ax+by=c \end{cases}.$$

$\Rightarrow$ quadratische Gleichung in $x$. Gleichung hat Nullstellen in $L_n$ Dann setze $L_{n+1} = L_n$ & Schnittpunkte haben Koordinaten in $L_n$.

Hat sie keine Nullstellen, dann setze $L_{n+1} = L_n$ ($x$-Koordinate eines Schnittpunkts).

$x \in L_n \mid Q$. Dann ist, da nur quadratische Körpererweiterungen auftreten $[L_n : \mathbb{Q}] = 2^k$. Aber $\mathbb{Q}[X] \mid \mathbb{Q}$ hat Grad 3. $\underbrace{L_N \mid \underbrace{K \mid \mathbb{Q}}_{3}}_{2^l}$

Da $[L_N : Q] = [L_N : K][K : \mathbb{Q}] = 2^l$ und $[K : \mathbb{Q}] = 3$, erhalten wir einen Widerspruch. □

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

**Lemma.** *Eine endliche Körpererweiterung ist algebraisch.*

*Beweis.* Für $[L : K] < \infty$ und $x \in L$ gilt $\varphi_x : K[T] \to L$ ( $K[T]$ unendlich-dim. über $K$, $L$ endlich-dim.) ist nicht injektiv. □

**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 $K$.*

*Beweis.* Nach Annahme gilt $[K(X) : K] < \infty$ und das Minimalpolynom $m_y(T) \in K[T]$ kann auch als Polynom in $K(X)[T]$ angesehen werden. Dies impliziert, dass $y$ auch algebraisch über $K(X)$ ist und daher gilt $[K(X)(Y) : K(X)] < \infty$. Aus dem Satz folgt also für $K(X,Y) = K(X)(Y)$, dass

$$[K(X,Y) : K] = [K(X,Y) : K(X)][K(X) : K] < \infty.$$

Also ist $K(X,Y)$ eine endliche Körpererweiterung und alle seine Elemente $x+y, x\cdot y, x^{17}y^2, \ldots . \in K(x,y)$ sind 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.

*Beweis.* $\Rightarrow$: überlassen wir als Übung

$\Leftarrow$: Angenommen $F \mid L$ und $L \mid K$ sind algebraische Körpererweiterungen. Sei $x \in L$. Dann existiert ein Minimalpolynom $m_x^L(T) \in L[T]$ von $x$ über $L$. Angenommen $y_1, \ldots, y_n \in L$ sind die Koeffizienten von $m_x^L(T)$. Wie im Beweis vom letzten Korollar können wir zeigen, dass

$$[K(y_1, \ldots, y_n) : K] < \infty.$$

Da $m_x^L(T)$ Koeffizienten in $K(y_1, \ldots, y_n)$ hat, ist $[K(y_1, \ldots, y_n, x) : K(y_1, \ldots, y_n)] < \deg(m_x^L) < \infty$. Daraus ergibt sich

$$[K(y_1, \ldots, y_n, x)] : K < \infty.$$

Da $x \in K(y_1, \ldots, y_n, x)$ und $K(y_1, \ldots, y_n, x) \mid K$ endlich ist, ist $x$ algebraisch auf Grund des Lemmas. □

**Beispiel.** $\sqrt{2}, \sqrt{3}$ sind algebraisch über $\mathbb{Q} \Rightarrow \sqrt{2} + \sqrt{3}$ ist algebraisch über $\mathbb{Q}$..

## 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*

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

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

*Beweis.* Wir können o.B.d.A. annehmen, dass $f$ einen Faktor $p(T)$. Wir definieren

$$K_1 := {}^{K[T_1]}/_{(p(T_1))}$$

und wir betrachten $K_1$ als Körpererweiterung von $K$. In $K_1$ gilt

$$p(T_1 + (p(T_1))) = p(t_1) + (p(T_1)) = 0 + (p(T_1))$$

also hat $f(T)$ eine Nullstelle in $K_1$, nämlich $T_1 + (p(T_1)) =: \alpha_1$. Wir schreiben $f(T) = (T - \alpha_1) f_1(T)$ für ein $f_1(T) \in K_1[T]$. Falls $f_1 = 1$, setzen wir $L = K_1$. Da $\deg(d_1) < \deg(f)$ gibt es aufgrund der Induktionsannahme eine Körpererweiterung $L|K_1$ mit $f_1(T) = \prod_{j=2}^{n} (T - \alpha_j), \alpha_j \in L$. □

**Beispiel.**
- $\mathbb{R}, f(T) = T^2 + 1$, $\mathbb{C} = \mathbb{R}[i]$
- $K = \mathbb{Q}, f(T) = T^3 - 2$, $L = \mathbb{Q}(\sqrt[3]{2}, \xi \sqrt[3]{2}, \xi^2 \sqrt[3]{2})$, wobei $\xi =$ dritte Einheitswurzel $= \frac{-1+\sqrt{3}i}{2}$ Minimalpolynom ist $T^2 + T + 1$ und nicht $T^3 - 1$ (nicht irreduzibel). Hat Grad 6 nach Multiplikativität.

**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 $K$.

**Beispiel.**
- $K = \mathbb{Q}, f(T) = T^2 + 1 \in \mathbb{Q}[T]$; die Nullstellen von $f$ sind $\pm i \Rightarrow f$ zerfällt über $\mathbb{C}$ aber $\mathbb{C}$ ist kein Zerfällungskörper von $f$ über $\mathbb{Q}$

*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.

**Beispiel.** $\mathbb{C}$ ist algebraisch abgeschlossen

*Bemerkung.* Ein algebraisch abgeschlossener Körper hat unendlich viele Elemente.

*Beweis Idee.* Angenommen $K = \{k_1, \dots, k_n\}$ ist algebraisch abgeschlossen. Betrachte das Polynom

$$f(T) = (T - k_1) \cdot \ldots \cdot (T - k_m) + 1 \lightning .$$

$\square$

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

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

*eine algebraisch abgeschlossene algebraische Körpererweiterung von $K$.*

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

*Beweis.* (1) $E$ ist ein Körper: Folgt aus einem Korollar vom letzten Mal [$x, y \in L$ algebraisch $\Rightarrow x + y, x \cdot y, \frac{1}{x}$ für $x \neq 0$ algebraisch].

(2) $E \mid K$ ist algebraisch per Definition

(3) $E$ ist algebraisch abgeschlossen: Sei $f \in E[T]$ mit $\deg(f) > 0$. Sei $E_1$ eine algebraische Erweiterung von $E$ so dass $f$ eine Nullstelle $\alpha$ in $E_1$ hat (Kronecker). Dann ist $E_1 \mid E$ algebraisch und $E \mid K$ algebraisch $\Rightarrow E_1 \mid K$ algebraisch. Nun ist $\alpha \in L$ ($L$ algebraisch abgeschlossen) und $\alpha$ ist algebraisch über $K \Rightarrow \alpha \in E$.

$\square$

*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).*

*Beweis.* Für jedes $f \in K[T]$, $\deg(f) > 0$, sei $T_g$ eine Unbestimmte. Wir betrachten den Polynomring (in $\infty$-vielen Unbestimmten)

$$R := K[(T_f)_f].$$

Sei $I \lhd R$ das Ideal, das von den Elementen $f(T_f)$ erzeugt wird. [$f(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_0 \rightsquigarrow f(T_f) = (T_f)^n + a_{n-1} + (T_f)^{n-1} + \ldots + a_0$ ]

*Behauptung.* $I \neq R$

*Beweis.* Angenommen $1 \in I, 1 = \sum_{i \in X} g_i f_i(T_{f_i}) \in I$, $g_i \in K[(T_f)_f]$, $X$ endlich. jedes $f_i$ eine Nullstelle in $\alpha_i$ in $E$ hat. Nun werten wir $f_i$ an $T_{f_i} = \alpha_i$ aus und erhalten

$$1 = \sum_{i \in X} \underbrace{g_i(\ldots)}_{\in E} \underbrace{f_i(\alpha_i)}_{=0} = 0 \lightning .$$

$\square$

Da $R \neq \{0\}$ existiert ein maximales Ideal $M$ in $R$, das $I$ enthält. Sei

$$L_1 := \frac{R}{M},$$

dann ist $L_1$ ein Körper und $K \to L_1$ ist ein injektiver Körperhomomorphismus. Wir identifizieren $K$ mit seinem Bild in $L_1$. ($K \hookrightarrow \underbrace{K[(T_f)_f]}_{=R} \to {}^{K[(T_f)_f]}/_{M} = L_1$)

*Behauptung.* Jedes $f \in K[T]$, $\deg(f) > 0$, hat eine Nullstelle in $L_1$ und $L_1 \mid K$ ist eine algebraische Körpererweiterung.

*Beweis.* Das Bild von $T_f$ in $L_1$ ist eine Nullstelle von $f \in L_1[T]$

$$f(T_f + M) = \underbrace{f(T_f)}_{\in I \subseteq M} + M = 0 + M \Rightarrow 1. \text{ Teil.}$$

Jedes $x \in L_1$ ist im Bild von $K[T_{f_1}, \ldots, T_{f_m}]$ für eine endliche Menge von Unbestimmten. Jedes $T_{f_i} \in L_1$ ist algebraisch über $K$, also auch $x \Rightarrow 2.$ Teil $\square$

Nun wiederholen wir die Konstruktion $L_0 = k \subseteq L_1 \subseteq L_2 \subseteq \ldots$, wobei jedes Polynom $f \in L_i[T]$, $\deg(f) > 0$, eine Nullstelle in $L_{i+1}$ hat und $L_{i+1} \mid L$ ist eine algebraische Körpererweiterung. Definiere

$$L := \bigcup_{n \geq 0} L_n.$$

Man rechnet nach, dass $L$ ein Körper ist und $K$ enthält (Übung). Außerdem ist $L$ algebraisch über $K$ (Übung).

Wir behaupten, dass $L$ algebraisch abgeschlossen ist: Sei $f \in L[T]$, $\deg(f) > 0$.

$$\begin{aligned}
&\Rightarrow \ \exists i : f \in L_i[T] \qquad (f \text{ hat nur endlich viele Koeffizienten})\\
&\Rightarrow \ \exists \alpha_1 \in L_{i+1} \mid f = (T - \alpha_1) f_1, \quad f_1 \in L_{i+1}[T],\\
&\Rightarrow \ \exists \alpha_2 \in L_{i+2} \mid f = (T - \alpha_2) f_2, \quad f_2 \in L_{i+2}[T],\\
&\Rightarrow \ \text{usw.} \ \Rightarrow f \text{ zerfällt in Linearfaktoren über } L.
\end{aligned}$$

$\square$

## 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.*

*Beweis.* Die Ableitung definieren wir mittels

$$D : f = \sum_{n=0}^{\infty} a_n T^n \mapsto f' = \sum_{n=1}^{\infty} n a_n T^{n-1}.$$

Dann ist $D$ $K$-linear und erfüllt die Produktregel

$$(fg)' = f'g + fg'. \tag{$*$}$$

Denn dies stimmt für $K = \mathbb{C}$ und $(*)$ ist eine polynomielle Gleichung über $\mathbb{Z}$ in den Koeffizienten von $f$ und von $g$. Insbesondere gilt also

$$((T-\alpha)^2 g(T))' = 2(T-\alpha)g(T) + (T-\alpha)^2 g'(T) = (T-\alpha)(2g(T) + (T-\alpha)g'(T)).$$

D.h. falls $f$ eine mehrfache Nullstelle hat, so ist diese auch eine Nullstelle von $f$. Dies gilt für $\alpha \in K$ aber auch für $\alpha \in L$ wenn $L \mid K$.

Angenommen $m(T) \& m'(T)$ sind in $K[T]$ coprim. Dann existieren $h_1, h_2 \in K[T]$ mit

$$1 = h_1(T)m(T) + h_2(T)m'(T).$$

Falls nun $L \mid K$ eine Körpererweiterung ist und $\alpha \in L$ eine Nullstelle von $m(T)$ ist, so ist $m'(T) \neq 0$. Auf Grund des oben gesagten ist also $\alpha$ eine einfache Nullstelle von $m(T)$. Falls $L$ algebraisch abgeschlossen ist, so gilt

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

und $\alpha_1, \dots, \alpha_n \in L$ sind paarweise verschieden.

Für $\mathrm{char}(K) = 0$ gilt $\deg(m'(T)) = \deg(m(T)) - 1$ falls nun $m(T) \in K[T]$ irreduzibel ist, so ist $m'(T)$ coprim zu $m(T)$ und obiges gilt. □

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

*Beweis von* 1) *im Satz.* Sei $m(T)$ das Minimalpolynom von $\alpha$ über $K$. Sei $\beta = \varphi(\alpha)$ für $K$-lineare Körpereinbettung $\sigma : E \to L$ so gilt $m(\beta) = m(\sigma(\alpha)) = 0$, da $m(T) = \sum_{n=0}^{\infty} a_n T^n$ mit Koeffizienten $a_n \in K$, $\sigma$ ist ein Ringhomomorphismus und $\sigma(a_n) = a_n$.

Des Weiteren gilt für ein $f(\alpha) \in K[\alpha]$ dass $\sigma(f(\alpha)) = f(\sigma(\alpha)) = f(\beta)$. Also ist $\beta = \sigma(\alpha)$ eine Nullstelle und $\sigma$ ist durch diese Nullstelle bereits eindeutig festgelegt. Folgt da $m(T)$ in $L$ höchstens $\deg(m(T)) = [E : K]$ viele verschiedene Nullstellen hat, gibt es höchstens so viele $K$-lineare Körpererweiterungen.

Sei nun umgekehrt $\beta \in L$ eine beliebige Nullstelle von $m(T)$ - Es gibt mindestens eine Nullstelle in $L$ und falls $\mathrm{char}(K) = 0$ so gibt es genau $\deg(m(T))$ viele verschiedene Nullstellen. Wir verwenden $\beta$ um eine $K$-lineare Körpererweiterung

$$\sigma = \sigma_\beta : E = K[\alpha] \to L$$

zu definieren. Wir betrachten das linke Diagramm Dann gilt $\mathrm{Ker}(\mathrm{ev}_\alpha) = (m(T))$. Und wegen $m(\beta) = 0$ folgt $(m(T)) \subseteq \mathrm{Ker}(\mathrm{ev}_\alpha)$ (Gleichheit, da $(m(T))$ ein Maximalideal ist). Daraus ergibt sich das rechte Diagramm und $\sigma = \overline{\mathrm{ev}_\beta} \circ (\overline{\mathrm{ev}_\alpha}^{-1}) : E \to L$ ist eine $K$-lineare Körpereinbettung.

$$
\begin{tikzcd}
 & f(\alpha) \in K[\alpha] = E \\
f(T) \in K[T] \arrow[ur, "\mathrm{ev}_\alpha"] \arrow[dr, "\mathrm{ev}_\beta"'] & \\
 & f(\beta) \in K[\beta] \subseteq L
\end{tikzcd}
\qquad
\begin{tikzcd}
 & f(\alpha) \in K[\alpha] = E \\
f(T) + (m(T)) \in {}^{K[T]}/_{(m(T))} \arrow[ur, "\mathrm{ev}_\alpha"] \arrow[dr, maps to, "\mathrm{ev}_\beta"'] & \\
 & f(\beta) \in K[\beta] \subseteq L
\end{tikzcd}
.
$$

Für zwei verschiedene Nullstellen $\beta_1 \neq \beta_2 \in L$ gilt

$$\sigma_{\beta_1}(\alpha) = \beta_1 \neq \beta_2 = \sigma_{\beta_2}(\alpha) \quad \text{also} \quad \sigma_{\beta_1} \neq \sigma_{\beta_2}.$$

Wir sehen also, dass es genauso viele Körpererweiterungen von $E = K[\alpha]$ nach $L$ gibt, wie es Nullstellen von $m(T)$ in $L$ gibt. $\square$

**Beispiel.** Sei $K = \mathbb{F}_p((X))$ und $m(T) = T^p - X$ (dies ist irreduzibel). Für $E = {}^{K[T]}/_{(m(T))}$ gibt es eine Nullstelle $T + (m(T)) = \alpha$ von $m(T)$. Hier gilt $m(T) = (T - \alpha)^p = T^p - \alpha^p = T^p - X$ und $m$ hat $\alpha$ als eine $p$-fache Nullstelle.

*Beweis von* 2) *im Satz (mittels dem Zorn'schen Lemma).* Wir definieren

$$\mathcal{O} = \{(F, \sigma) \mid F \text{ ein Körper mit } K \subseteq F \subseteq E, \sigma : F \to L \ K\text{-lineare Körpereinbettung}\}.$$

und die partielle Ordnung

$$(F_1, \sigma_1) \leq (F_2, \sigma_2) \Leftrightarrow \begin{cases} F_1 \subseteq F_2 \\ \sigma_2 \mid_{F_1} = \sigma_1 \end{cases}.$$

Dann gilt:

- $\mathcal{O} \neq \varnothing$ da $(K, \mathrm{id}) \in \mathcal{O}$.
- Angenommen $T \leq \mathcal{O}$ ist eine totalgeordnete Kette in $\mathcal{O}$. Wir definieren

$$F_T = \bigcup_{(F,\sigma) \in T} F \subseteq E.$$

  Dies ist ein Unterkörper von $E$. (kleine Übung)

Wir definieren

$$\sigma_T : F_T \to L$$
$$\begin{matrix} x \in F \\ \text{mit } (F, \sigma) \in T \end{matrix} \mapsto \sigma(x).$$

Dies ist wohldefiniert: Falls $\begin{matrix} x \in F_1 \\ (F_1, \sigma_1) \in T \end{matrix}$ und $\begin{matrix} x \in F_2 \\ (F_2, \sigma_2) \in T \end{matrix}$ ist, so können wir o.B.d.A. annehmen, dass $(F_1, \sigma_1) \leq (F_2, \sigma_2) \Rightarrow \sigma_2(x) = \sigma_2 \mid_{F_1} (x) = \sigma_1(x)$. Dies zeigt, dass $\sigma_T$ wohldefiniert ist. $\sigma_T$ ist auch eine Körpereinbettung: Für $x_1, x_2 \in F_T$ gibt es $\begin{matrix} (F_1, \sigma_1) \in T \\ (F_2, \sigma_2) \in T \end{matrix}$ mit $\begin{matrix} x_1 \in F_1 \\ x_2 \in F_2 \end{matrix}$.

O.B.d.A. sei $(F_1, \sigma_1) \leq (F_2, \sigma_2)$. Dann gilt

$$\sigma_T(x_1 + x_2) = \sigma_2(x_1 + x_2) = \sigma_2(x_1) + \sigma_2(x_2) = \sigma_T(x_1) + \sigma_T(x_1).$$

und analog für $x_1 \cdot x_2$ und $\frac{1}{x_1}$ falls $x_1 \neq 0$.

Folgt $(F_T, \sigma_T) \in \mathcal{O}$ ist eine obere Schranke con der total geordneten Kette $T$. Auf Grund des Zorn'schen Lemmas existiert also ein maximales Element

$$(F, \sigma) \in \mathcal{O}.$$

*Behauptung.* $F = E$ und $\sigma : F \to L$ ist die gesuchte $K$-lineare Körpereinbettung.

Falls $F \neq E$ ist, dann gibt es ein $\alpha \in E \setminus F$. In diesem Fall verwenden wir $\sigma : F \to L$ und die Elemente von $F$ mit den Elementen in $\sigma(F)$ zu identifizieren:

$$\begin{tikzcd} L \underset{\sigma}{\supseteq} & F \subseteq F[\alpha] \subseteq E \arrow[l, bend right, "\varphi"'] \end{tikzcd}.$$

Nach Teil 1 vom Satz gibt es eine $F$-lineare Körpereinbettung $\varphi : F[\alpha] \to L$. Da wir $\sigma$ verwendet haben um Elemente von $F$ mit Elementen von $\sigma(F)$ zu identifizieren, bedeutet dies gerade, dass $\varphi : F[\alpha] \to L$ die Abbildung $\sigma : F \to L$ erweitert.

Also gilt $(F, \sigma) \lneq (F[\alpha], \varphi)$ und dies widerspricht der Maximalität von $(F, \sigma)$. □

**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.*

*Beweis.* Angenommen $f(T) \in K[T]$ und $E_1, E_2$ sind zwei Zerfällungskörper von $f(T)$. Sei $L_2$ ein algebraischer Abschluss von $E_2$. Wir verwenden den 2. Teil vom Satz:

$$\begin{tikzcd} K \arrow[r] \arrow[dr] & E_1 \arrow[d, "\sigma"] \\ & E_2 \subseteq L_2 \end{tikzcd}.$$

Es folgt $f(T) = a\prod_{i=1}^{n}(T - \alpha_i)\sigma(f(T)) = a\prod_{i=1}^{n}(T - \sigma(\alpha_i - 1))$ für $\alpha_1, \ldots, \alpha_n \in E_1$. Da $E_1 = K(\alpha_1, \ldots, \alpha_n)$ und $E_2 = K[\sigma(\alpha_1), \ldots, \sigma(\alpha_n)]$, folgt, dass $\sigma : E_1 \to E_2$ ein Isomorphismus ist.

Angenommen $L_1$ & $L_2$ sind algebraische Abschlüsse von $K$.

Auf Grund vom 2. Teil vom Satz gibt es eine $K$-lineare Körpereinbettung $\sigma : L_1 \to L_2$. Damit ist $K \subseteq \sigma(L_1) \subseteq L_2$. Des Weiteren ist $L_2 \mid K$ algebraisch und $\sigma(L_1)$ ist algebraisch abgeschlossen. Daraus folgt

$$L_2 = \{\alpha \in L_2 \mid \ \exists f \in K[T] \setminus \{0\} \text{ mit } f(\alpha) = 0\} \subseteq \sigma(L_1) \subseteq L_2.$$

□

## 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*

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

*Beweis.* 1) Angenommen $|K| < \infty$. Dann ist $\mathbb{Z} \cdot 1_K \cong \mathbb{F}_p = {}^{\mathbb{Z}}/_{(p)}$ für eine Primzahl $p \in \mathbb{N}$. Damit ist $K$ ein endlich-dimensionaler Vektorraum über $\mathbb{F}_p$ und $K \cong \mathbb{F}_p^{[K:\mathbb{F}_p]} \Rightarrow |K| = p^{[K:\mathbb{F}_p]}$.

2) Sei $q = p^n$ wie in 2. Seien weiters

$$\begin{aligned}
&f(T) = T^q - T \in \mathbb{F}_p[T] \\
&L = \text{ Zerfällungskörper von } f \text{ (über } \mathbb{F}_p) \\
&E = \{x \in L \mid x_q = x\} = \{x \in L \mid f(x) = 0\} \\
&\phi : \begin{matrix} L \to L \\ x \mapsto x^p \end{matrix} \quad \text{Frobenius-Homomorphismus} \\
&\phi^n \begin{matrix} L \to L \\ x \mapsto x^{p^n} \end{matrix} \quad = x^q
\end{aligned}$$

wobei $L$ eine endliche Körpererweiterung von $\mathbb{F}_p$ und damit ein endlicher Körper und $\phi$ ist ein Automorphismus, da $\phi$ injektiv und $|L| < \infty$ ist.
Es folgt

$$E = \{x \in L \mid \underbrace{\phi^n(x) = x}_{\text{Körperautomorphismus}} \} = \{x \in L \mid f(x) = 0\}$$

ist ein Unterkörper von $L$, der alle Nullstellen von $f$ enthält. Also ist $E = L$. Daraus ergibt sich auch, dass $E = L$ als Zerfällungskörper bis auf Isomorphie eindeutig bestimmt ist.
Da $f'(T) = qT^{q-1} - 1 = -1$ ist, sind $f$ und $f'$ coprim. Daher hat $f$ keine mehrfachen Nullstellen in $L$ (wegen dem Lemma von früher). Es gibt also genau $q$ Nullstellen in $L$, also gilt

$$|L| = |E| = q = p^n.$$

Dies beweist die Existenz in 2.
Sei $F$ ein beliebiger Körper mit $p^n$ Elementen. Wie im Beweis von 1. wissen wir, dass $F \mid F_p$. Des Weiteren gilt $x \in F^\times$ dass $x^{p^n-1} = 1$ (weil $|\mathbb{F}^\times| = p^n - 1$ und $F^\times$ eine Gruppe ist). Also gilt $x^{p^n} = x$ für alle $x \in F$. D.h. $F$ enthält (besteht aus) den Nullstellen von $f(T) = T^q - T$, ist also der Zerfällungskörper von $f$. - Auf Grund des Korollars im letzten Abschnitt ist also $F$ isomorph zu $L$ von oben.

3) Sei $K$ ein algebraischer Abschluss von $\mathbb{F}_p$. Dan ist

$$\mathbb{F}_p = \{x \in K \mid x^{p^n} = x\} \subseteq K$$

ein Unterkörper. Wie in 2, sehen wir, dass $F_{p^n}$ der Zerfällungskörper von $T^{p^n} - T$ ist und auf Grund von dem oben bewiesenen, gilt $|\mathbb{F}_{p^n}| = p^n$.

4) Angenommen $m \mid n$ also $n = mk$

$$\phi^n = (\phi^n)^k \,.$$

Daraus folgt $\mathbb{F}_{p^n}\{x \mid \phi^n(x) = x\} \supseteq \{x \mid q^m(x) = x\} = \mathbb{F}_{p^m}$.
Angenommen $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. Dann ist $\mathbb{F}_{p^n} \mid \mathbb{F}_{p^m}$ und $\mathbb{F}_{p^n}$ ist ein Vektorraum über $\mathbb{F}_{p^m}$. Folgt $p^n = |\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^k = (p^m)^k = p^{mk}$ mit $k = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$.

□

**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 $p^n$.*

*Beweis.* Auf Grund der Klassifikation von endlich erzeugen abelschen Gruppen gilt

$$(G, \cdot) \cong (\mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_n), +) \,.$$

für gewisse natürliche $1 < d_1 \mid d_2 \mid \ldots \mid d_n$.
*Behauptung.* In $G$ gilt damit $x^{d_n} = 1$ für alle $x \in G$.

*Beweis.* Denn $d_n \cdot (a_1 + (d_1), \ldots, a_n + (d_n)) = (0 + (d_1), \ldots, 0 + (d_n))$ da $d_1 \mid d_n, d_2 \mid d_n, \ldots$. Dies zeigt die Behauptung wenn wir obigen Isomorphismus verwenden. □

Die Behauptung zeigt: jedes $x \in G$ ist eine Nullstelle von $T^{d_n} - 1$. Des Weiteren gilt $|G| = d_1 d_2 \cdot \ldots \cdot d_n$. Falls $n > 1$ wäre, so hätten wir $d_1 d_2 \cdots d_n > d_n = \deg(T^{d_n} - 1)$ viele Nullstellen von $f$ in $K$. Das ist unmöglich, also ist $n = 1$ und $G$ ist zyklisch. □

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

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

*Beweis-Idee.* $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)$ und in $\frac{\mathbb{Z}}{(p-1)}$ lässt sich die Aussage leichter bestätigen. □

# 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 $\sigma$ 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.* 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* $f$*.*

*Beweis.* Sei $\alpha \in R(f)$ d.h. $f(\alpha) = 0$ und $\sigma \in \mathrm{Gal}(E/K)$. Sei $f(X) = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0$ wobei $a_n, \ldots, a_0 \in K$.

$$0 = f(x) = \sigma(f(x)) = \sigma(a_n\alpha^n + \ldots + a_0) = \sigma(a_n)\sigma(\alpha)^n + \ldots + \sigma(a_0) = a_n\sigma(\alpha)^n + \ldots + a_0 = f(\sigma(\alpha))$$

Also folgt $\sigma(\alpha) \in R(f)$. $\sigma(R(f)) \subseteq R(f)$. Da $\sigma : E \to E$ injektiv und $|R(f)| < \deg(f) = n$ folgt $\sigma(R(f)) = R(f)$. □

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 $X = \{1, 2, \dots, n\}$ 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.*

*Beweis.* Aus Lemma II.4 folgt $\sigma(R(f)) = R(f)\ \forall \sigma \in \mathrm{Gal}(E/K)$. Homomorphismus: $(\sigma \circ \eta)\mid_{R(f)} = \sigma\mid_{R(f)} \circ \eta\mid_{R(f)}$
Injektivität: Sei $R(f) = \{\alpha_1, \dots, \alpha_n\}$ dann folgt aus Algebra I, dass $E = k[\alpha_1, \dots, \alpha_n$. Wobei $K[\alpha_1, \dots, \alpha_n]$ das Bild der Evaluationsabbildung $\begin{array}{c} K[X_1, \dots, X_n] \to E \\ P \mapsto P(\alpha_1, \dots, \alpha_n) \end{array}$. Sei $\sigma \in \mathrm{Gal}(E/K)$ mit $\sigma\mid_{R(f)} = \mathrm{id}_{R(f)}$. Das heißt $\sigma(\alpha_i) = \alpha_i\ \forall 1 \leq i \leq n$. Sei $\xi \in E$ und $P \in K[X_1, \dots, X_n]$ so dass $P(\alpha_1, \dots, \alpha_n] = \xi$. Also folgt: da $\sigma(x) = x\ \forall x \in K$ folgt

$$\sigma(P) = \sigma(P(\alpha_1, \dots, \alpha_n) = P(\sigma(\alpha), \dots, \sigma(\alpha_n)) = P(\alpha_1, \dots, \alpha_n) = P$$

folgt $\sigma = \mathrm{id}_E$. □

*Alternativer Beweis.*

$$E = K(\alpha_1, \dots, \alpha_n) = \left\{ \frac{P(\alpha_1, \dots, \alpha_n)}{Q(\alpha_1, \dots, \alpha_n} \mid P, Q \in K[X_1, \dots, X_n \text{ und } Q(\alpha_1, \dots, \alpha_n \neq 0 \right\}.$$

Dann analoger Beweis zu oben. □

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

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

**Beispiel.** $K = \mathbb{F}_p(t), f \in K[X], f = X^p - t$. Dann ist $f$ irreduzibel (Übung) und $|R(f)| = 1$. Sei $K \subseteq E$ ein Zerfällungskörper von $f$ und $\alpha \in R(f) : \alpha^p = t$. Da $E$ Charakteristik $p$ ist folgt $(X - \alpha)^p = X^p - \alpha^p = X^p - t^p = f$. Also $R(f) = \{\alpha\}$ und $|\mathrm{Gal}(E/K)| = 1$.

**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.*

*Beweis.* Sei $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$, $a_d \neq 0, \deg(f) = d$. Dann ist $f'(x) = a_d dx^{d-1} + a_{d-1}(d-1)x^{d-2} + \ldots + a_1$. Unter der Voraussetzung des Lemmas folgt $d \neq 0$ und somit $a_d d \neq 0$, also $\deg(f') = d-1$. Falls $p \in K[X]$ mit $p$ dividiert $f$ und $f' \Rightarrow \deg(p) \leq d-1$ aber $f$ ist irreduzibel $\deg(f) = d$. Folgt $\deg(p') = 0$ d.h. $p \in K$. Weiters folgt $\mathrm{ggT}(f, f') = 1$. Und somit mit dem Lemma folgt $f$ hat 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.

**Beispiel.** $X^4 + 1 \in Q[X]$ ist irreduzibel; da $\mathrm{char}(\mathbb{Q}) = 0$ folgt aus dem Lemma, dass $X^4 + 1$ separabel ist. Also ist auch $(X^4 + 1)^{15}$ separabel.

**Definition** (Wiederholung)**.** Sei $E/K$ eine Körpererweiterung und $\alpha \in E$ : $\begin{array}{c} \varphi_\alpha : K[X] \to E \\ P \mapsto P(\alpha) \end{array}$ 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 $\alpha$ transzendent über $K$.
(2) $\mathrm{Ker}(\varphi_\alpha) \neq (0)$ dann ist $\alpha$ algebraisch. Da $K[X]$ ein Hauptidealring ist gibt es genau ein unitäres Polynom $\mathrm{irr}(\alpha, K)$, das Minimalpolynom von $\alpha$ 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.** *$\varphi_\alpha$ 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 $\varphi_*$ 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 $\varphi$ erweitert und $\widehat{\varphi}(\alpha) = \alpha'$*

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

*Beweis.* Betrachte das linke Diagramm. Da $p$ irreduzibel und $p(\alpha) = 0$ folgt $\mathrm{Ker}(\varphi_\alpha) = p \cdot K[X]$. Gleiches gilt für $p_*$ : $\mathrm{Ker}(\varphi_{\alpha'}) = p_* K'[X]$. Da $\varphi_*(p) = p_*$ folgt $\varphi_*(\mathrm{Ker}(\varphi_\alpha)) = \mathrm{Ker}(\varphi_{\alpha'})$. Daraus folgt, dass $\varphi_*$ einen Ringisomorphismus $\overline{\varphi_*} : K[X]/\mathrm{Ker}(\varphi_\alpha) \xrightarrow{\sim} K'[X]/\mathrm{Ker}(\varphi_{\alpha'})$ induziert.
Betrachte das rechte Diagramm. Die gesuchte Erweiterung $\widehat{\varphi} = \overline{\varphi_{\alpha'}} \circ \overline{\varphi_*} \circ \overline{\varphi_\alpha}^{-1}$

$$\begin{tikzcd} E \arrow[r, "\varphi_*"] \arrow[d, "\varphi_\alpha"] & E_* \arrow[d, "\varphi_{\alpha'}"] \\ K(\alpha) \subset E & K'(\alpha') \end{tikzcd} \qquad \begin{tikzcd} K[X]/\mathrm{Ker}(\varphi_\alpha) \arrow[r, "\overline{\varphi_*}"] \arrow[d, "\overline{\varphi_\alpha}"] & K'[X]/\mathrm{Ker}(\varphi_{\alpha'}) \arrow[d, "\overline{\varphi_{\alpha'}}"] \\ K(\alpha) \arrow[r, "\widehat{\varphi}"] & K'(\alpha') \end{tikzcd}.$$

□

**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 $\varphi$ erweitern, d.h. $\Phi\,|_K = \varphi$*

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

*Beweis.* 1. (a) Wir hatten mittels $\varphi : K \to K'$ einen Ringhomomorphismus $\varphi_K : K[X] \to K'[X]$, nämlich $h = a_nX^n + \ldots + a_0 \in K[X]$. Dann ist $\varphi_*(h) = \varphi(a_n)X^n + \ldots + \varphi(a_0)$. Bemerke $\varphi_*(h_1 + h_2) = \varphi_*(h_1) + \varphi_*(h_2)$ und $\varphi_*(h_1h_2) = \varphi_*(h_1)\varphi_*(h_2), \varphi_*(\mathbb{1}) = \mathbb{1}$ und $\deg(\varphi_*(h)) = \deg(h)$. Aus diesen Eigenschaften folgt $\varphi_*(\mathrm{ggT}(h_1, h_2)) = \mathrm{ggT}(\varphi_*(h_1), \varphi_*(h_2))$. $f(X) = a_nX^n + \ldots + a_0$, $f'(X) = a_nnX^{n-1} + \ldots + a_1$. Allgemeine Eigenschaft $\varphi : K \to K'$: $\varphi(m\xi) = m\varphi(\xi)\ \forall m \in \mathbb{Z}$.

$$\begin{aligned} \varphi_*(f) &= \varphi(a_n)X^n + \ldots + \varphi(a_0) \\ \varphi_*(f) &= \varphi(a_nn)X^{n-1} + \ldots + \varphi(a_1) \\ &= \varphi(a_n)nX^{n-1} + \ldots + \varphi(a_1) = \varphi_*(f)'. \end{aligned}$$

Also folgt $\varphi_*(\mathrm{ggT}(f, f')) = \mathrm{ggT}(\varphi_*(f), \varphi_*(f)')$. Da $f$ separabel ist folgt $\mathrm{ggT}(f, f') = \mathbb{1} \Rightarrow \mathrm{ggT}(\varphi_*(f), \varphi_*(f)') = \mathbb{1}$. Und also $f_* = \varphi_*(f)$ separabel ist.

(b) $[E : K] = 1$ dann $R(f) \subseteq E = K$, $f$ zerfällt also in lineare Faktoren woraus folgt $f_* = \varphi_*(f)$ in $K'[X]$ auch in lineare Faktoren zerfällt $\Rightarrow E_* = K'$.

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

(c) $[E : K] > 1$ : Dann gibt es $p \in K[X]$ irreduzibel mit $\deg(p) > 1$ und $p$ dividiert $f$. Notation $d := \deg(f) > 1$. Sei $f = pg$ wobei $g \in K[X]$. Dann folgt $f_* = \varphi_*(f) = \underbrace{\varphi_*(p)}_{P_*}\underbrace{\varphi_*(g)}_{g_*} = f_*g_*$. Aus $f$ separabel folgt $f_*$ separabel.

Aus $p$ irreduzibel folgt $p_*$ irreduzibel: Also ist $p_*$ irreduzibel und separabel. Da $\deg(p_*) = \deg(p) = d$ hat $f_*$ in $E_*$ genau $d$ Nullstellen $\alpha_1^*, \ldots, \alpha_d^*$ alle in $E^*$ enthalten.

Sei $\alpha \in R(p) \subseteq E$. Aus Lemma 2.15 folgt, dass es für jedes $\alpha_i^*$ einen Isomorphismus

$$\widehat{\varphi_i} : K(\alpha) \to K'(\alpha_i^*) \subseteq E_* \quad \text{mit} \quad \widehat{\varphi_i}(\alpha) = \alpha_i^*$$

und erweitert $\varphi : K \to K'$.

Sei $\alpha_* = \alpha_i^*, \widehat{\varphi} = \widehat{\varphi_i}$.

$$\widehat{\varphi} : K(\alpha) \subseteq E \to K'(\alpha_*) \subseteq E_*.$$

*Bemerkung.* $f \in K(\alpha)[X]$ und $E$ ist Zerfällungskörper von $f \in K(\alpha)[X]$. $f_* \in K'(\alpha)[X]$ und $E_*$ ist Zerfällungskörper von $f_* \in K'(\alpha)[X]$. Es ist $(\widehat{\varphi})_* : K(\alpha)[X] \to K'(\alpha_*)[X]$ ein Isomorphismus. Da $\widehat{\varphi}\,|_K = \varphi$ folgt $(\widehat{\varphi})_*(f) = f_*$. $f$ und $f_*$ sind wieder separabel.

Da nun $[E : K(\alpha)] = \frac{[E:K]}{[K(\alpha):K]} = \frac{[E:K]}{d} < [E : K]$. Nach Induktionshypothese gibt es $[E : K(\alpha)]$ Erweiterungen von $\widehat{\varphi} : K(\alpha) \to K'(\alpha_*)$ auf $E \to E_*$. $\forall 1 \leq i \leq d$ hat $\widehat{\varphi_i} : K(\alpha) \to K'(\alpha_i^*)$ ist eine $[E : K(\alpha)]$-Erweiterung auf $E \to E_*$. Mit dieser Konstruktion erhalten wir also $d[E : K(\alpha)] = [K(\alpha) : K][E : K(\alpha)] = [E : K]$ Erweiterungen von $\varphi : K \to K'$.

*Bemerkung* (Einschub für weiter oben). $h$ hat keine mehrfachen Nullstellen genau dann wenn $\mathrm{ggT}(h, h') = 1$: Zu zeigen $f$ separabel $\Rightarrow f_*$ separabel. Sei $h$ ein irreduzibler Faktor von $f : f = h \cdot u$, dann ist $f_* = \varphi_*(h)\varphi_*(u) : \varphi_*(h)$ irreduzibel. $h$ hat keine mehrfachen Nullstellen $\Rightarrow \mathrm{ggT}(h, h') = 1 \Rightarrow \mathrm{ggT}(\varphi_*(h), \varphi_*(h)') = 1 \Rightarrow \varphi_*(h)$ keine mehrfachen Nullstellen.

2. Sei $E/K$ Zerfällungskörper eines separablen Polynoms: $|\mathrm{Gal}(E/K)| = [E : K]$. $\mathrm{Gal}(E/K) = \{\varphi : E \to E \text{ Isomorphismen die id} : K \to K\}$ erweitern.

$\square$

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

*Beweis.* Sei $\alpha \in R(f) \subseteq E$. Dann ist $K(\alpha) \subseteq E$ und da $f$ irreduzibel $[K(\alpha) : K] = n = \deg(f)$. Aus Satz 2.17: $|\mathrm{Gal}(E/K)| = [E : K] = [E : K(\alpha)][K(\alpha) : K] = [E : K(\alpha)] \cdot n$. $\square$

**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* $Fr : \begin{array}{c} \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \\ x \mapsto x^p \end{array}$

*Beweisidee.* 1. $\mathbb{F}_{p^n} : \left|\mathbb{F}_{p^n}^\times\right| = p^n - 1$ also ist $\mathbb{F}_{p^n}^\times$ genau die Menge der Nullstellen des Polynoms

$$x^{p^n - 1} - 1 \in \mathbb{F}_p[X].$$

Dieses Polynom hat keine mehrfachen Nullstellen $\Rightarrow$ separabel und mit Satz 2.17 folgt:

$$|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [F_{p^n} : F_p] = n.$$

Nun $Fr \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Für $k \geq 1, k \in \mathbb{N}$. $Fr^k(\xi) = (\xi)^{p^k}$. Sei $m$ die Ordnung von $Fr$ in $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) : Fr^m = \mathrm{id}_{\mathbb{F}_{p^n}} : \forall \xi \in F_{p^n} \xi^{p^m} = \xi$. Also ist $\mathbb{F}_{p^n}$ in der Menge der Nullstellen eines Polynoms von Grad $p^m$ enthalten $\Rightarrow p^n \leq p^m$. Folgt $n \geq m \Rightarrow n = m$. Folgt dass $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \{\mathrm{id}, Fr, \ldots, Fr^n\}$

$\square$

**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 $p$.*

*Beweis.* Sei $\Gamma_p = \{(g_1, \ldots, g_p) \in G^p : g_1 \cdot \ldots \cdot g_p = e\} \subseteq G^p$. Die Symmetrie Gruppe $S_p$ wirkt auf $G^p : \eta \in S_p$. $\eta_*(g_1, \ldots, g_p) = (g_{\eta(1)}, \ldots, g_{\eta(p)})$. Sei $\sigma = (1, 2, \ldots, p)$ der $p$-Zykel. Sei $(g_1, \ldots, g_p) \in \Gamma_p : g_1 \cdot \ldots \cdot g_p = e$.

$$\underbrace{g_1^{-1}(g_1 \cdot \ldots \cdot g_p)g_1}_{g_2 \cdot \ldots \cdot g_p g_1 = e} = g_1^{-1} e g_1 = e \quad \text{und} \quad g_{\sigma(1)} \cdot \ldots \cdot g_{\sigma(p)} = e.$$

Folglich lässt die durch $\sigma$ erzeugte zyklische Untergruppe von $S_p$

$$C_p = \{\mathrm{id}, \sigma, , \dots, \sigma^{p-1}\} \quad \Gamma_p \text{ invariant.}$$

Also ist $\Gamma_p$ = disjunkte Vereinigung der $C_p$-Bahnen in $\Gamma_p$. Da $p$ Primzahl hat so eine Bahn entweder Kardinalität 1 oder $p$. Sei $I$ = Menge der Bahnen mit Card 1, $J$ = Menge der Bahnen mit Card $p$. Dann ist $\Gamma_p = \bigsqcup_{i \in I} O_i \sqcup \bigsqcup_{j \in J} O_j$ und $O_1 = \{(e, \dots, e)\}$. Es ist dann $|G|^{p-1} = |\Gamma_p| = |I| \cdot 1 + |J| \cdot p$. Nun $p \mid |G|^{p-1}$. Folgt $p \mid |I| \Rightarrow |I| \geq_2$. $\square$

# Anhang A: Auswahlaxiom und das Zornsche Lemma

**Auswahlaxiom** (in der Mengenlehre)
Sei $I$ eine nichtleere Menge und seien $X_i$ für $i \in I$ nichtleere Mengen. Dann ist $\prod_{i \in I} X_i \neq \varnothing$, d.h. es existiert eine Funktion

$$f : I \to \bigcup_{i \in I} X_i$$

mit $f(i) \in X_i$ für alle $i \in I$.

*Bemerkung.*
- unabhängig von den anderen ZF-Axiomen der Mengenlehre
- kritisiert wegen der Nichtkonstruktivität des Axioms und mancher scheinbar paradoxen Folgerung
- notwendig für einen großen Teil der Mathematik

Häufig wird nicht das Auswahlaiom sondern ein dazu äquivalentes Lemma, das Zornsche Lemma, verwendet. Für dieses benötigen wir etwas mehr Begriffe:

**Definition.** Sei $X$ eine Menge. Eine *Ordnung* auf $X$ ist eine Relation $\leq$ so dass

1) reflexivität: $x \leq x$
2) antisymmetrie: $x \leq y$ und $y \leq x$
3) transitivität: $x \leq y$ und $y \leq z \Rightarrow x \leq z$ für alle $x, y, z \in X$.

Die Ordnung heißt *total* oder *linear* falls zusätzlich

4) linearität: $x \leq y$ oder $y \leq x$

gilt. Ansonsten heißt sie *partiell.*

**Beispiel.**
- $\leq$ in $\mathbb{R}$ ist total
- $|$ in $\mathbb{Z}$ partiell, da $2 X 3$ und $3 X 2$.
- $\subseteq$ auf $\mathcal{P}(A) = \{B \subseteq A\}$

**Definition.** Sei $\leq$ eine Ordnung auf einer Menge $X$. Ein Element $x \in X$ heißt *maximal* falls für alle $y \in X$ gilt $x \leq y \Rightarrow x = y$. Ein Element $m \in X$ ein *Maximum* falls $x \leq m$ für alle $x \in X$ gilt.

**Definition.** Sei $\leq$ eine Ordnung auf einer Menge $X$ und sei $A \subseteq X$. Ein Element $x \in X$ heißt eine *obere Schranke von $A$* falls $a \leq x$ für alle $a \in A$. Analog definiert man *untere Schranke von $A$*.

**Definition.** Sei $\leq$ eine Ordnung auf einer Menge $X$. Eine Teilmenge $K \subseteq X$ heißt eine *Kette* falls für alle $x, y \in K$ gilt $x \leq y$ oder $y \leq x$. Wir sagen die Ordnung $\leq$ sei *induktiv* falls jede Kette in $X$ eine obere Schranke besitzt.

**Satz** (Zornsches Lemma)**.** *Sei $\leq$ eine induktive Ordnung auf einer Menge $X$. Dann existiert ein maximales Element in $X$.*

**Typische Anwendung:** Jeder Vektorraum über $K$ hat eine Hamel-Basis.

*Beweisidee.* Ausgehend von der leeren Menge (die eine Kette darstellt) wollen wir Elemente einer immer Länger werdenden Kette finden, wobei wir immer wieder eine obere Schranke hinzufügen wollen - sofern dies möglich ist.

...

$\Rightarrow$ eine Art Induktion

**Problem:** Die Vereinigung von Ketten muss keine Kette sein. $\square$

Vorerst einige Definitionen und Lemmata:

**Definition.** Für eine Teilmenge $C \subseteq X$ definieren wir

$$\widehat{C} = \{x \in X \setminus C \mid x \text{ ist eine obere Schranke}\}.$$

Um die Beweisidee umzusetzen verwenden wir eine *Auswahlfunktion* auf der Menge $\{\widehat{C} : C \subseteq X \text{ s.d. } \hat{C} \neq \varnothing\}$

**Definition.** Eine Teilkette $K \subseteq X$ heißt eine *f-Kette* falls für jede Teilmenge $C \subseteq K$ mit $\widehat{C} \cap K \neq \varnothing$ das Element $f(\widehat{C})$ zu $K$ gehört und eine minimale obere Schranke von $C$ in $K$ ist, also $f(\widehat{C}) \leq y$ für alle $y \in \widehat{C} \cap K$ gilt. Dies vermeidet „unnötige Zwischenschritte", die zu Problemen bei einer Vereinigung von Ketten führen würde.

**Beispiel.** $K_{min} = \varnothing, \widehat{K_{min}} = X$ ist eine $f$-Kette, die in jeder anderen $f$-Kette enthalten ist.
$K_1 = \{f(\widehat{K_{min}}\} = K_{min} \cup \{f(\widehat{K_{min}})\}$ ist eine weitere $f$-Kette, die in jeder anderen nichtleeren $f$-Kette enthalten ist.

- $\widehat{\varnothing} = X \Rightarrow f(x) \in X$ ist definiert
- $K_{min}$ ist eine $f$-Kette: $C = \varnothing$ und $f(\widehat{\varnothing}) \in K_{min}$ ist minimal $C = K_{min}$ erfüllt $\widehat{C} \cap K_{min} = \varnothing$
- Falls $K$ eine $f$-Kette ist, so können wir $C = \varnothing$ in der Definition verwenden und erhalten $f(\widehat{\varnothing}) \in K$, also $K_{min} \subseteq K_1 \subseteq K$.

**Lemma** (Verlängerung)**.** *Falls $K$ eine $f$-Kette ist und $\widehat{K} \neq \varnothing$ ist, so ist $K_{neu} = K \cup \{f(\widehat{K})\}$ wieder eine $f$-Kette.*

*Beweis.* Sei $C \subseteq K_{neu}$.

- Falls $\widehat{C} \cap K \neq \varnothing$ ist, so gilt $C \subseteq K$, $f(\widehat{C}) \in K$ und $f(\widehat{C})$ ist eine minimales Element von $\widehat{C} \cap K$ (da $K$ eine $f$-Kette ist). Damit ist aber auch $f(\widehat{C}) \in K_{neu}$ und $f(\widehat{C})$ ist ein minimales Element von $\widehat{C} \cap K_{neu}$ (da $f(\widehat{K})$ eine obere Schranke von $K$ ist).
- Falls $C \subseteq K$ und $\widehat{C} \cap K = \varnothing$, dann ist $\widehat{C} = \widehat{K}$, da $K$ eine Kette ist gilt $\widehat{C} \supseteq \widehat{K}$. Sei $x \in \widehat{C}, k \in K \Rightarrow k \neq \widehat{C}$, also existiert ein $c \in C$ mit $k \leq c \leq x \Rightarrow x$ ist eine obere Schranke von $K$ und $x \notin K$ also $x \in \widehat{K}$ und somit $\widehat{C} \in \widehat{K}$.
  Folglich isst $f(\widehat{C}) = f(\widehat{K}) \in K_{neu}$ eine minimale obere Schranke von $C$ in $K_{neu}$.
- Falls $f(\widehat{K}) \in C$, so ist $\widehat{C} \cap K_{neu} = \varnothing$ und es gibt nichts zu beweisen.

$\square$

**Lemma** (Zwei $f$-Ketten)**.** *Angenommen $K, K'$ sind zwei $f$-Ketten und $K' \setminus K \neq \varnothing$. Dann ist $K \subseteq K'$ und es gilt $x \leq x'$ für alle $x \in K$ und $x' \in K' \setminus K$.*
*Informell: „$K$ ist eine Anfangsabschrift von $K'$".*

*Beweis.* Sei $x' \in K' \setminus K$. Wir definieren

$$C = \{x \in K \cap K' : x \leq x'\} \subseteq K' \cap K$$

und verwenden, dass $K'$ eine $f$-Kette ist. Da $x' \in \widehat{C} \cap K'$ ist, folgt $f(\widehat{C}) \in K'$ und $f(\widehat{C}) \leq x'$.
Falls $\widehat{C} \cap K \neq \varnothing$ wäre, so wäre $f(\widehat{C}) \in K$ (da $K$ eine $f$-Kette ist) womit aber $f(\widehat{C}) \in C \cap \widehat{C}$ der Definition von $\widehat{C}$ widerspricht.
Also ist $\widehat{C} \cap K = \varnothing$. In anderen Worten bedeutet dies, dass es zu jedem $x \in K$ ein $c \in C$ mit

$x \leq c$ geben muss. Nach Definition von $C$ folgt daher $x \leq c \leq x'$. Also $x \leq x'$ für alle $x \in K$. Unsere Annahmen an $K$ und $K'$ war bloss, dass es $x' \in K' \setminus K$ gibt. Daraus folgt nun auch $K \subseteq K'$, denn ansonsten könnten wir die Rollen von $K$ und $K'$ vertauschen. $\square$

**Lemma** (Vereinigung)**.** *Wir definieren* $K_{max} = \bigcup_{\substack{K \text{ ist eine} \\ f-Kette}} K$. *Dann ist* $K_{max}$ *eine* $f$*-Kette.*

*Beweis.* Da für je zwei Ketten $K, K'$ $K \subseteq K'$ oder $K' \subseteq K$ gilt, sehen wir, dass $K_{max}$ wieder eine Kette ist. Wir müssen noch zeigen, dass $K_{max}$ eine $f$-Kette ist und nehmen hierzu eine Teilmenge $C \subseteq K_{max}$ mit $\widehat{C} \cap K_{max} \neq \varnothing$. Sei $x' \in \widehat{C} \cap K_{max}$ und sei $K'$ eine $f$-Kette mit $x' \in K'$.

**Behauptung:** $C \subseteq K'$.
Sei also $x \in C$, dann existiert eine $f$-Kette $K$ mit $x \in K$. Nach obigem Lemma gilt $K \subseteq K'$ ($\Rightarrow x \in K' \checkmark$) oder $K' \subseteq K$. Woraus folgt $K'$ enthält wegen obigem Lemma alle Elemente von $K$ unterhalbt von $x'$. Da $x' \in \widehat{C}$ und $x \in C$ folgt $x \leq x'$ und $x \in K'$.

Da $C \subseteq K', c \in \widehat{C} \cap K'$ und da $K'$ eine $f$-Kette ist, folgt nun $f(\widehat{C}) \in K' \subseteq K_{max}$ und $f(\widehat{C}) \leq x'$. Da $x' \in \widehat{C} \cap K_{max}$ beliebig war, sehen wir, dass $f(\widehat{C}) \in K_{max}$ ein minimales Element von $\widehat{C} \cap K_{max}$ ist. Dies zeigt aber, dass $K_{max}$ eine $f$-Kette ist. $\square$

*Beweis vom Zornschen Lemma.* $K_{max}$ ist nach Definition eine größte $f$-Kette in $X$. Insbesondere ist also das erste Lemma nicht anwendbar, d.h. $\widehat{K_{max}} = \varnothing$.

Des Weiteren ist aber $K_{max}$ eine Teilkette, die nach Annahme an $\leq$ eine obere Schranke $x_{max}$ besitzen muss. Es folgt also $x_{max} \in K_{max}$ ist ein Maximum von $K_{max}$ und auch, dass $x_{max}$ ein maximales Element von $X$ ist. $\square$