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.

$$(a+b)+c = a+(b+c)$$
$$0+a = a$$
$$(-a)+a = 0$$
$$a+b = b+a$$

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 + punkteweise 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. □

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 $ab = ac \Rightarrow ab - ac = 0, a(b-c) = 0 \Rightarrow b = c$. □

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 Integritätbereich?

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 $a \neq 0, b, c \in R$.

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

□

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 $d = \mathrm{ggT}(m, a)$. Nahc Definition ist $d \geq 1$ ein Teiler von m. Falls $d = m$ wäre, dann folgt $m|a \Rightarrow \overline{a} = \overline{0}$ $\lightning$. 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 ι 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 $\iota(ab) = \frac{a \cdot b}{1 \cdot 1} = \iota(a)\iota(b)$ □

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:

$$0 \in \mathbb{F}_2 \mapsto 0^2 + 0 = 0$$
$$1 \in \mathbb{F}_2 \mapsto 1^2 + 1 = 1 + 1 = 0$$

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 überlsassen 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

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

   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 · 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 widerum $i \leq I, j \leq J$ und damit $n = i + j \leq I + J$ impliziert. □

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

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

Allgemeiner: Sei a ein Polynom, dann ist

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

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

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

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

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

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.

Angenommmen $p \mid q$, 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

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

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

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

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

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

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

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

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 φ und $x = \Phi(X)$ benötigt.

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

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

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

•

$$\Phi(a \cdot b) = \Phi(\sum_{n=0}^{\infty}(\sum_{i+j=n} a_i b_j)X^n) = \sum_{n=0}^{\infty} \underbrace{\varphi(\sum_{i+j=n} a_i b_j)}_{\sum_{i+j=n}\varphi(a_i\varphi(b_j)} x^n$$

$$= \sum_{i,j} \varphi(a_i)\varphi(b_j)x^{i+j} = (\sum_i \varphi(a_i)x^i)(\sum_j \varphi(b_j)x^j) = \Phi(a)\Phi(b).$$

Also ist Φ 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:

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

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 Ψ 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*

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

3. *Mit diesen Abbildungen, $0_{R/I} = [0]_\sim, 1_{R/I} = [1]_\sim$ ist ${}^{R}/_{I}$ ein Ring und die kanoische 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 Def 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. „⇐“: 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 and, 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 Äuivalent modulo I gleich

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

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

1. *Dann induziert φ einen Ringisomorphismus*

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

   so dass $\varphi = \overline{\varphi} \circ p$ wobei $p : R \to {}^{R}/_{\mathrm{Ker}(\varphi)}$ die kanonische Projektion ist (Diagramm links).
2. *Sei $I \subseteq \mathrm{Ker}(\varphi)$ ein Ideal in R. Dann induziert φ einen Ringhomomorpismus $\overline{\varphi} : {}^{R}/_{I} \to S$ mit $\varphi = \overline{\varphi} \circ p_I$ (Diagramm rechts). Des weiteren gilt $\mathrm{Ker}(\overline{\varphi}) = {}^{\mathrm{Ker}(\varphi)}/_{I}$ und $\mathrm{Im}(\overline{\varphi}) = \mathrm{Im}(\varphi)$*

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 φ ein Ringhomomorphismus ist, gilt

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

$\varphi = \overline{\varphi} \circ p_I$ 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.

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

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 $\mathrm{Ker}(\overline{\varphi}) = {}^{\mathrm{Ker}(\varphi)}/_{\mathrm{Ker}(\varphi)} = \{0 + \mathrm{Ker}(\varphi)\}$, also ist $\overline{\varphi}$ injektiv. Daher ist $\overline{\varphi}$ ein Ringhomomorphismus von ${}^{R}/_{\mathrm{Ker}(\varphi)}$ nach $\mathrm{Im}(\varphi)$ 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.

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

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

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* $\mathrm{Ker}(\varphi) = I_1 \cap \ldots \cap I_n$.
Dies induziert einen Ringisomorphismus ${}^{R}/_{I_1 \cap \ldots \cap I_n} \to {}^{R}/_{I_1} \times \ldots \times {}^{R}/_{I_n}$.

Beweis. Dass der Kern $\mathrm{Ker}(\varphi)$ genau $I_1 \cap \ldots \cap I_n$ ist, ergibt sich aus den Definitionen. Wir zeigen, dass φ 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 Definiton 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

$$\varphi(a_1x_1 + \ldots + a_nx_n) = (a_1x_1 + \ldots + a_nx_n + I_1, \ldots, a_1x_1 + \ldots + a_nx_n + I_n) = (a_1 + I_1, a_2 + I_2, \ldots, a_n + I_n).$$

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

Lemma. *Sei $I \subseteq \mathbb{Z}$ ein Ideal. Dann gilt $I = (m)$ für ein $m \in \mathbb{N}$. Der Quotient ist ein Integritätsbreich 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: $\text{Ker}(f) \subseteq K$ ist ein Ideal $\Rightarrow \text{Ker}(F) = \{0\}$ 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 Integritätsbreich 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 $a_1, \ldots, a_n \in K$. Wir definieren dass Ideal

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $a_1, \ldots, a_n \in R$. Wir definieren

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

genannt „s-adjungiert $a_1, \ldots, a_n$".

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

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

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

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

□

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

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

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

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

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

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. □

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 $N(a + \sqrt{2}b) = \left|a^2 - 2b^2\right|$ 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 $g = g_m X^m + \ldots$, $f = f_n X^n + \ldots$. 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)**.** $g = x^6 + x^4 + 4x^3 + 2$, $f = x^2 + 5$

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

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 ϕ ein Ringhomomorphismus. In der Tat ist ϕ 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 filt $N(f) \geq 1$ 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

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

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 $J_0 \subseteq J_1 \subseteq J_2 \subseteq \ldots$ eine austeigende 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 $m \geq n$.

□

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. □

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 $N(v) = 1$ ($v \in \mathbb{Z}[i]^\times$). □

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 $w \in \mathbb{Z}[i]^\times$. □

Beispiel. Im Ring der Poynome $K[x]$ 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 Primelemente 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 $p_1, \ldots p_m$ 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

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

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 Primfaktorzerlegug 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 Definitin von faktoriellen Ringen. Zu jedem p_j gibt es ein eindeutig bestimmtes $p \in P$ mit $p_j \sim p$. Damit erhalten wird

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

wobei $n_p = \#j$ mit $p_j \sim p$. □

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 $\sum_{p\in P} n'_p$. □

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. „⇒“: $b = ac$ 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 $p \in P$.

„⇐“: 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 $a \mid b$. □

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 $t \mid d$. □

Wir können analog den ggT von mehreren Elementen $a_1, \dots, a_l \in R$ definneren 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

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

□

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:
$1 \pm i\sqrt{5} = zw \Rightarrow N(1 \pm i\sqrt{5}) = 6 = N(z)N(w) \Rightarrow N(z)N(w) \in \{1, \cancel{2}, \cancel{3}, 6\}$ 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:

$$\begin{array}{ccccc} K & \xrightarrow{\varphi_+} & \mathbb{Q}[x]/(x^2 - d) & \xrightarrow{\varphi_-} & K \\ & \searrow & & \nearrow_{\tau} & \\ \sqrt{d} & \longmapsto & X + (x^2 + d) & \longmapsto & -\sqrt{d} \end{array}$$

Wobei der Isomorphismus φ_+ Auswertungen bei $\sqrt{d}$ verwendet und analog dazu der Isomorphismus φ_- 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 dasss $N : K \to \mathbb{Q}$ 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

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

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 iin 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 $u^{-1} = \pm\tau(u)$. □

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 $\underbrace{w = \pm 1}_{w\in R^\times}$. □

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 $N(v) = \pm p^2$). □

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

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

verwenden. Diese Menge P enthält

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

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

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 $(*)$. □

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 $\zeta = \frac{1+\sqrt{3}i}{2}$ funktionert 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 $\mathbb{Z}[x_1, \ldots, x_n]$ und der Ring $K[x_1, \ldots, x_n]$ 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 primitv.

Beobachtungen

- Jedes normierte Polynom is 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 $f > 0 \Rightarrow f = af^*, a \in R, f^*$ primitv. 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 $f = d_1 f_1^* = d_2 f_2^*$, $d_1, d_2 \in K^\times$, $f_1^*, f_2^* \in R[x]$ primitv, 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 $i = 0, \ldots, n$. 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 $g^* \in R[x]$.

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

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 $f \in R[x] \mapsto f \bmod p \in {}^R\!/_{(p)}[x], \sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n (a_i + (p)) X^i$. Dies folgt aus dem Satz von 4. VO (wobei $\varphi(a) = a + (p)$ und $\Phi(X) = X$).

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 Φ 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 ± 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*
- *$\deg(f) = \deg(f \bmod p)$ mit $f \bmod p \in {}^{R}/_{(p)}[x]$*
- *$f \bmod p \in \frac{R}{(p)}[x]$ ist irreduzibel*

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

Beweis. Angeonmmen $f = gh$ 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 telbar. 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 Vorraussetzungen 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.

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

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

Beweis. Angenomenn $f = gh$ 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 dauch den konstanten Ter 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. □

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 $\Phi_p(x)$. □

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 primitv. 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 φ bijektiv ist, so sprechen wir auch von einem *Isomorphismus* der Gruppen und sagen G_1 und G_2 sind *isomorph* .

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

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

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

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

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

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 $\mathbb{R}^x = \mathbb{R} \setminus \{0\}$ 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 *symmtrische Gruppe.*
5. Sei M eine nichtleere Menge mit „einer Struktur“. Dann ist

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

   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	$\mathrm{Gal}(K:\mathbb{Q}) = \{\varphi : K \to K : \mathbb{Q}\text{-linear, bijektiv und } \varphi(ab) = \varphi(a)\varphi(b)\}$ (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 reele 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	$\mathrm{SO}_{2,1}(\mathbb{R}), P\,\mathrm{GL}_2(\mathbb{R})$
$\vdots$	
Topologischer-Raum X	$\mathrm{Homöo}(X) = \{\varphi : X \to X \text{ bijektiv, stetig, } \varphi^{-1} \text{ stetig}\}$
Mannigfaltigkeit M	$\mathrm{Diffeo}^\infty(M) = \{\varphi : M \to M \text{ bijektiv, stetig, glatt und ebenso } \varphi^{-1}\}$
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 $\mathrm{Ker}(\det) = (\,SL)_n(K)$.

7. .

$(0,\infty) < R^\times$ ist eine Untergruppe.	$S^1 = \{z \in \mathbb{C} \mid \lvert z\rvert = 1\} = \mathrm{Ker}(\lvert\cdot\rvert) < \mathbb{C}^\times$ ist eine Untergruppe.
$\exp : \mathbb{R} \to \mathbb{R}^\times$ ist ein Homomorphismus.	$\exp : \mathbb{C} \to \mathbb{C}^\times$ ist ein Homomorphismus. $\mathrm{Ker}(\exp) = 2\pi i\mathbb{Z}$

8. $G_1 \times G_2$ ist eine Gruppe (komponenetenweisen 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 φ injektiv oder es gibt ein $n_0 > 0$ mit* $\mathrm{Ker}(\varphi) = (n_0) = \mathbb{Z}n_0$.

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

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 φ 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 Grupee.*

a) Für jedes $g \in G$ ist $\gamma_g : G \to G, x \mapsto gxg^{-1}$ ein Automorphismus von G, welche ein innerer Automorphismus *genannt wird.*

b) Die Abbildung $g \in G \mapsto \gamma_g \in \mathrm{Aut}(G)$ ist ein Homomorphismus. Der Kern von Φ ist das Zentrum $Z_G = \{g \in G \mid$ für alle $x \in G$ gilt $gx = xg\}$.

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 γ_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 γ_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 γ_g gleich dem Zentralisator von g :

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

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

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

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 $G = U_n(\mathbb{C}) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid A^*A = AA^* = I\}$. Jedes $g \in G$ ist mittels einem Element von G diagonalisierbar. ⇒ Konjugationsklassen für G können wir durch Elemente von $(S^1)^n$ modulo Vertauschung der Koordinaten beschreiben.

Manchmal ist G sehr kompliziert und unüberschaubar aber Konjugationsklassen 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 $\{1\}$. (Ü)

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

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

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

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 $\mathbb{C}$:

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

und es gilt $\sigma_k(\sigma_k(z)) = \sigma_k(\zeta^k \overline{z}) = \zeta^k \overline{(\zeta^k \overline{z})} = z$, also definiert σ_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 $\frac{\mathbb{Z}}{(n)}$ 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 nenne 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 $H_0 \subseteq \langle X\rangle$. □

Lemma. *Sei G eine Gruppe und $a \in G$. Dann gilt $\langle a\rangle \approx \mathbb{Z}/(n_0)$ 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 $\mathrm{Ker}(\varphi) = I = (n_0)$ 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

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

□

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 ρ mit Vertauschungen $\tau_{i,i+1}$ können wir ρ 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 Diemensionsbegriff“: Denn is 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

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

Lemma. *Sei G eine Gruppe und $H < G$. Dann ist $\sim_H$ eine Äquivalentrelation 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 σ 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 Grupee und $H < G$.*

(1) G/H und $H\backslash G$ 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 $\varphi : G/H \to H\backslash G$ und $\psi : H\backslash G \to G/H$ 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 $|H\backslash G| = |G/H|$ 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 $(x, h) \mapsto xh$

ψ 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. Insebsondere gibt es ein $h \in H$ (weil $g \sim_H x$) mit $g = xh = \psi(x, h)$. Also ist ψ surjektiv.

ψ 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 ψ 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 $k = \frac{m}{n}$. Dann 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 $n = \mathrm{Ord}(g) = \langle g \rangle = 1$ und ein Teiler von p. Also ist $n = p$ und $\langle g \rangle = G$. □

⇒ Es gibt bis auf Isomorphie nur eine Gruppe der Ordnung $2, 3, 5, 7, \ldots$.

Im Allgemeinen haben ${}^{G}/_{H}$ uund ${}^{H}/_{G}$ 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 Gruppenhomomorphimus $\varphi : G \to G_1$ mit $H = \mathrm{Ker}(\varphi)$.
(4) Für alle $x, y \in G$ gilt $(xH)(yH) = (xy)H$.
(5) ${}^{G}/_{H}$ ist (auf natürliche Weise) eine Gruppe so dass $\varphi : G \to {}^{G}/_{H}, g \mapsto gH$ ein Gruppenhomomorphismus ist.

Beweis. (5) ⇒ (3) : $\mathrm{Ker}(\varphi) = \{g \mid gH = eH\} = H$
(3) ⇒ (2) : Sei $x \in G, h \in H = \mathrm{Ker}(\varphi)$. Dann gilt $\varphi(xhx^{-1}) = \varphi(x)\underbrace{\varphi(h)}_{=e}\varphi(x)^{-1} = e$ also $xhx^{-1} \in H = \mathrm{Ker}(\varphi)$. ⇒ $xHx^{-1} \subseteq H, x^{-1}Hx \subseteq H \Rightarrow H \subseteq xHx^{-1}$. Somit folgt $xHx^{-1} = H$
(2) ⇔ (1) : Rechtsmultiplikation mit x^{-1} oder x.
(1) ⇒ (4) : Seien $x, yinG$. Dann gilt $(xH)(yH) = (Hx)(yH) = (Hxy)H = xyHH = xyH$.
(4) ⇒ (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.

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

□

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 $G \simeq \frac{\mathbb{Z}}{(p)}$ für eine Primzahl $p \in \mathbb{N}$.

Beispiel. Auf S_n gibt es den Homomorphismus $\text{sgn} : S_n \to \{\pm 1\}$. Der Kern $A_n = \text{Ker}(\text{sgn})$ 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 φ einen Isomorphismus $|\varphi| : G/\text{Ker}(\varphi) \to \text{Im}(\varphi)$ so dass folgendes Diagram komutiert*

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

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

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

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

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

Beispiel. Sei p prim. $|\text{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p)$ $\det : \text{GL}_2(\mathbb{F}_p) \to \mathbb{F}_p^\times$ ist surjektiv z.B. wegen $\det \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} = t$
$\text{SL}_2(\mathbb{F}_2) = \text{Ker}(\det)$. Es folgt aus dem Satz von Lagrange und dem ersten Isomorphiesatz

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

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

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

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*

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

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

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

Folht $KH < G$.

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

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 $2X3$ und $3X2$.
- $\subseteq$ 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. □

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.

□

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. □

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. □

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. □