Primfaktorzerlegung

13.15 Def.: R Integritätsring.

Ein Element $p \in R \setminus (R^\times \cup \{0\})$ ist...

... **irreduzibel**, falls für $a, b \in R$ gilt:

$$p = a \cdot b \Rightarrow (\underset{\Downarrow\ p \sim b}{a \in R^\times} \text{ oder } \underset{\Downarrow\ p \sim a}{b \in R^\times})$$

... **prim**, falls für $a, b \in R$ gilt:

$$p \mid a \cdot b \Rightarrow p \mid b \text{ oder } p \mid a$$

13.16 Satz:

① Jedes Primelement (in einem Integritätsring) ist irreduzibel.

② In einem euklidischen Ring sind die Primelemente genau die irreduziblen Elemente.

Beweis:

(prim $\Rightarrow$ irred.) Sei p prim, $p = a \cdot b$.

Nach Voraussetzung folgt: $p \mid b$ oder $p \mid a$.

Falls $p \mid b$: $b = c \cdot p$ für ein $c \in R$, also

$$p = a \cdot c \cdot p.$$

Nach Kürzungsregel 13.3: $1 = a \cdot c$ ($= c \cdot a$ da R kommutativ)

Somit $a \in R^\times$.

Falls $p \mid a$: analog $b \in R^\times$.

(prim $\Leftarrow$ irred. im euklidischen Fall):

Sei p irred., $p \mid ab$.

Angenommen $p \nmid a$. (Zu zeigen: $p \mid b$.)

Nach Satz 13.12 $\exists$ $\mathrm{dvggT}(a, p)$.

Nach Konstruktion $p = \tilde{p} \cdot d$ für ein $\tilde{p} \in R \setminus R^*$.
(Falls $\tilde{p} \in R^*$, folgt $p \sim d$, also $p \sim ggT(a,p)$, also insbesondere $p \mid a$ ↯).
Da p irreduzibel, folgt $d \in R^*$, also a und p teilerfremd. Nach Korollar 13.14 $\exists x,y \in R$ mit $xp + ya = 1$.

Demnach: $p \mid (1-ya)$.

Erst recht: $p \mid (b - yab)$.

Nach Annahme gilt $p \mid yab$. Also folgt $p \mid b$. $\square$

13.17 Notiz: Jedes Polynom von Grad 1 über einem Körper ist irreduzibel.

(Falls $P = A \cdot B$, folgt nach Gradformel
$\deg A = 0$ oder $\deg B = 0$,
also $A \in K$ oder $B \in K$.
Da $P \neq 0$, folgt ferner $A \neq 0$ und $B \neq 0$, also
$A \in K^\times = (K[X])^\times$ oder $B \in K^\times = (K[X])^\times$.)

13.18 Beispiel:

Die irreduziblen Polynome in $\mathbb{C}[X]$ sind genau die Polynome von Grad 1.

Beweis:

Ist $\deg P = 0$, so ist $P \in \mathbb{C}[X]^+ \cup \{0\} = \mathbb{C}$.
Ist $\deg P = 1$, so ist P irreduzibel nach 13.17.
Ist $\deg P > 1$, so liefert jede Nullstelle a von P eine Zerlegung $P = (X-a)\cdot Q$ (Satz 3.19).
Und über $\mathbb{C}$ hat jedes Polynom von Grad ≥ 1 eine Nullstelle nach 3.21.

13.19 Beispiel:

Die irreduziblen Polynome in $\mathbb{R}[X]$ sind die Polynome von Grad 1 und die Polynome ohne reelle Nullstelle von Grad 2.

Beweis:

Ist $\deg P = 0$, so ist $P \in \mathbb{R}[X]^+ \cup \{0\} = \mathbb{R}$.
Ist $\deg P = 1$, so ist P irreduzibel nach 13.17.
Ist $\deg P = 2$, so gilt:

$$\begin{aligned} P \text{ irreduzibel} &\iff P \text{ hat keinen Faktor von Grad 1} \\ &\iff P \text{ hat keine Nullstelle} \end{aligned}$$

Sei nun $\deg P > 2$.
Falls P reelle NS besitzt, ist P nicht irreduzibel.
Falls P keine reelle NS besitzt, besitzt P zumindest eine komplexe Nullstelle $a \in \mathbb{C} \setminus \mathbb{R}$.
Da P reell ist, ist dann auch $\bar{a} \neq a$ eine NS von P: $\quad P(\bar{a}) = \overline{P(a)} = \bar{0} = 0$.

Sei $\quad A := (X-a)(X-\bar{a})$
$$= X^2 - (a+\bar{a})X + a\bar{a}$$
$$= X^2 - 2\,\mathrm{Re}(a)X + \|a\|^2 \in \mathbb{R}[X].$$
Nach Konstruktion $A \mid P$ in $\mathbb{C}[X]$, aber wir brauchen: $\quad A \mid P$ in $\mathbb{R}[X]$.
Führe dazu Division mit Rest durch:
$$P = Q \cdot A + R \qquad (*)$$
mit $Q, R \in \mathbb{R}[X]$ und $\deg R \leq 1$.
Betrachte vorübergehend R als komplexes Polynom.
Falls $R \neq 0$, hat R nach Korollar 3.20 höchstens eine komplexe Nullstelle. Aber Auswertung von $(*)$ an a & $\bar{a}$ ergibt:
$$R(a) = R(\bar{a}) = 0 \qquad (\text{mit } a \neq \bar{a})$$
Also $R = 0$, und somit $P = \underbrace{Q}_{\text{Grad} \geq 1} \cdot \underbrace{A}_{\text{Grad } 2}$ in $\mathbb{R}[X]$.

$\square$

13.20 Def.: Eine *Primfaktorzerlegung* von $a \in R$ ist eine Darstellung von a als Produkt
$$a = p_1 \cdot \ldots \cdot p_r$$
mit $p_i \in R$ prim. Ein Integritätsring R ist *faktoriell*, wenn jedes $a \in R \setminus (R^* \cup \{0\})$ eine Primfaktorzerlegung besitzt.

13.21 Satz: Primfaktorzerlegungen in Integritätsringen sind (wenn sie existieren) eindeutig bis auf Reihenfolge der Faktoren und Assoziiertheit.

Genauer: Ist R Integritätsring und

$$p_1 \cdots\cdots p_r = q_1 \cdots\cdots q_s$$

für gewisse Primelement $p_i \in R$ und gewisse irreduzible Elemente $q_i \in R$, so ist $r = s$ und nach Umnummerierung der q_i gilt $p_i \sim q_i \ \forall i$.

Beweis: Induktion über r.

IA: $r = 0$ Ist $1 = q_1 \cdots\cdots q_s$, so ist jedes q_i eine Einheit, im Widerspruch zur Definition irreduzibler Elemente. Also $s = 0$.

IV: Aussage gilt für r Primfaktoren.

IS: Sei $p_1 \cdots\cdots p_{r+1} = q_1 \cdots\cdots q_s$.

Dann gilt insbesondere:

$$p_1 \mid q_1 \cdots\cdots q_s.$$

Da p_1 prim, folgt: $p_1 \mid q_i$ für ein i.

Nach Umnummerierung: $p_1 \mid q_1$, also $q_1 = u \cdot p_1$.

Da q_1 irreduzibel und $p_1 \notin R^*$ folgt $u \in R^*$.

Also $p_1 \sim q_1$, und nach Kürzungsregel 13.3

$$p_2 \cdots\cdots p_{r+1} = u \cdot q_2 \cdots\cdots q_s.$$

Da q_2 irreduzibel ist ist auch $(u \cdot q_2)$ irreduzibel.

Also können wir die IV anwenden und erhalten: $s = r+1$, $p_i \sim q_i \ \forall i$. $\square$

13.22 Satz: $\mathbb{Z}$ ist faktoriell.

Beweis:

Es reicht zu zeigen, dass jedes $n \geq 2$ eine Primfaktorzerlegung besitzt.

IA: $n = 2$ ✓

IV: Zerlegung existiert für jedes a mit $2 \leq a < n$.

IS: Falls n irreduzibel ist, ist n prim (13.16 ②).
Andernfalls ist $n = a \cdot b$ mit $2 \leq a, b < n$.
Also existiert nach IV Primfaktorzerlegung für a und b, und somit auch für n. □

13.23 Satz: Für jeden Körper K ist $K[X]$ faktoriell.

Beweis:

Wir müssen zu $P \in K[X]$ mit $\deg P \geq 1$ eine Primfaktorzerlegung finden. Induktion über $\deg P$.

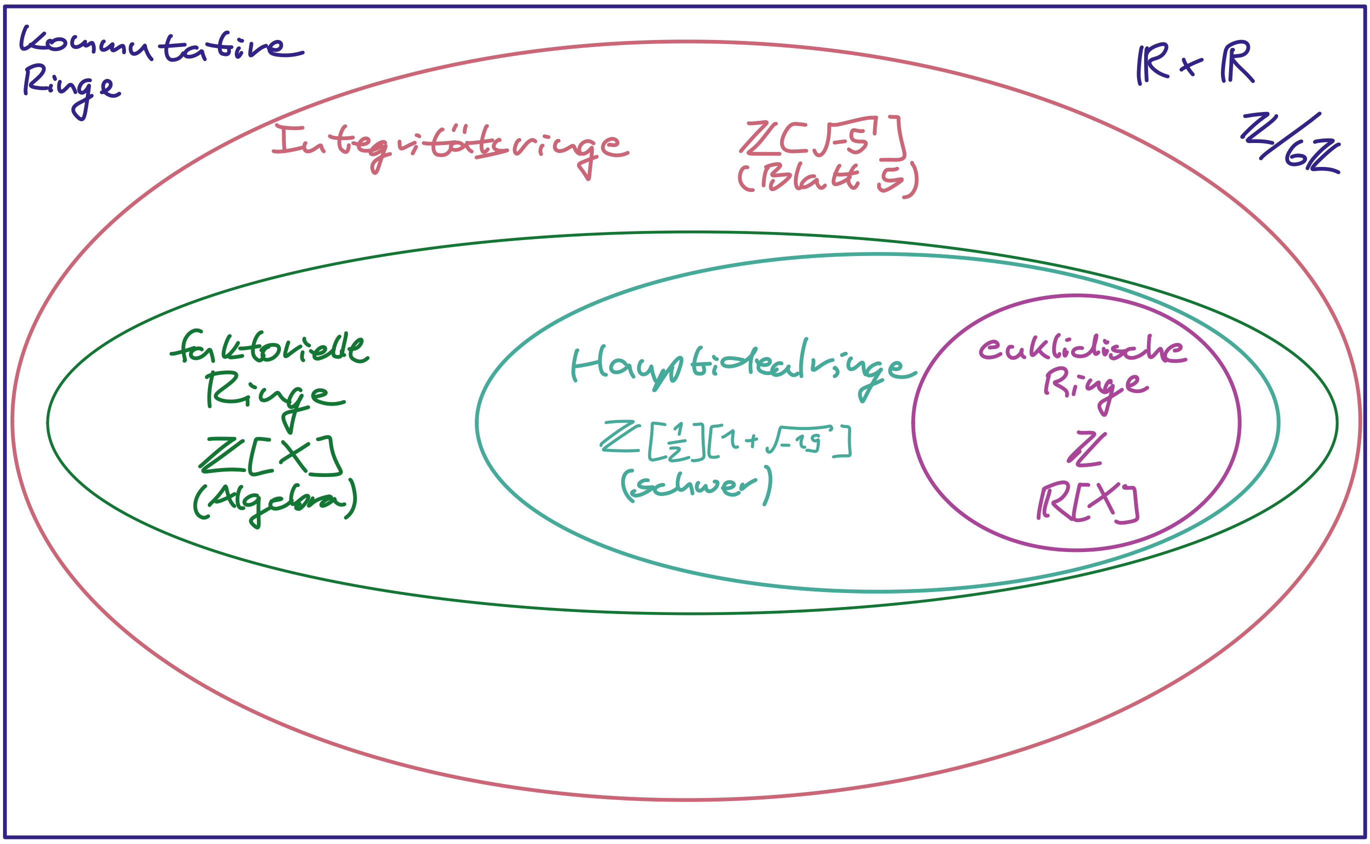
IA: $\deg P = 1$: siehe Notiz 13.17.

IV: Zerlegung existiert für alle $A \in K[X]$ mit $1 \leq \deg A < \deg P$.

IS: Falls P irreduzibel, P prim. ✓
Andernfalls $P = A \cdot B$ mit
$1 \leq \deg A, \deg B < \deg P$.
Nach IV existieren Primfaktorzerlegungen für A und B, und somit auch für P. □

13.24 Ausblick:

Alle euklidischen Ringe sind faktoriell.
Das folgt aber nicht so einfach wie für $\mathbb{Z}$ und $K[X]$, denn δ ist im Allgemeinen nicht mit Multiplikation „verträglich".
(Beweis zu 13.19 benutzt $|a \cdot b| = |a| \cdot |b|$;
Beweis zu 13.20 benutzt $\deg(A \cdot B) = \deg A + \deg B$.)
Stattdessen nutzt man, das euklidische Ring „Hauptidealringe" sind.



13.2.5 Bemerkung: ggT & kgV in faktoriellen Ringen

Sei R faktoriell,

$R^\times$ Einheiten von R,

$\mathbb{P}$ eine Menge von Primelementen von derart, dass jedes Primelement aus R zu genau einem Primelement aus assoziiert ist.

z.B.: $R = \mathbb{Z}$

$R = \{\pm 1\}$

$\mathbb{P} = \{p \in \mathbb{Z} \mid p \text{ prim und } p > 0\}$

z.B.: $R = \mathbb{C}[X]$ $\qquad (X-1)^2 = X^2 - 2X + 1$

$R^\times = \mathbb{C} \setminus \{0\}$

$\mathbb{P} = \{ P \in \mathbb{C}[X] \mid P \text{ irreduzibel und normiert} \}$

$= \{ X - c \mid c \in \mathbb{C} \}$

z.B.: $R = \mathbb{R}[X]$

$R^\times = \mathbb{R} \setminus \{0\}$

$\mathbb{P} = \{ P \in \mathbb{R}[X] \mid P \text{ irreduzibel und normiert} \}$

$= \{ X - r \mid r \in \mathbb{R} \} \,\dot\cup\, \{ X^2 - pX + q \mid p, q \in \mathbb{R}, \frac{p^2}{4} - q < 0 \}$

Dann hat jedes Element $a \in R$ eine bis auf Reihenfolge eindeutige Darstellung der Form

$$a = u \cdot \prod_{p \in \mathbb{P}} p^{\nu_p(a)}$$

mit $u \in R^\times$, $\nu_p(a) \in \mathbb{N}_0$, $\nu_p(a) = 0$ für fast alle $p \in \mathbb{P}$

z.B.: $$-18 = \underbrace{(-1)}_{u} \cdot 2 \cdot 3^{\overset{\nu_3(-18)}{2}} \in \mathbb{Z}$$

z.B.: $$2X^2 - 4X + 2 = \underbrace{2}_{u} \cdot (X-1)^{\overset{\nu_{X-1}(2X^2-4X+2)}{2}} \in \mathbb{R}[X]$$

Sind nun

$$a = u \cdot \prod_{p \in \mathbb{P}} p^{\nu_p(a)} \quad \text{und} \quad b = u' \cdot \prod_{p \in \mathbb{P}} p^{\nu_p(b)}$$

zwei solche Darstellungen, so ist

$$\operatorname{ggT}(a,b) \sim \prod_{p \in \mathbb{P}} p^{\min(\nu_p(a), \nu_p(b))}$$

$$\operatorname{kgV}(a,b) \sim \prod_{p \in \mathbb{P}} p^{\max(\nu_p(a), \nu_p(b))}$$

Kleine Anwendung:

13.26 Satz: Jedes reelle Polynom von **ungeradem** Grad hat eine Nullstelle.

Beweis:

Primfaktorzerlegung von $P \neq 0$ hat die Form

$$P = u \cdot (X - a_1) \cdot \ldots \cdot (X - a_k) \cdot Q_1 \cdot \ldots \cdot Q_\ell$$

für gewisse $u \in \mathbb{R}^\times$, $a_i \in \mathbb{R}$, $Q_i \in \mathbb{R}[X]$ ohne reelle NS mit $\deg Q_i = 2$ (siehe Beispiel 13.18).

Nach Voraussetzung ist

$\deg P = k + 2\ell$ ungerade,

also ist $k \neq 0$. $\square$