13. Faktorielle Ringe

Zur Primfaktorzerlegung in $\mathbb{Z}$

- Seien $a, b \in \mathbb{Z} \setminus \{0\}$ mit $(a,b) = 1$.
  Dann finden wir mit dem verallg. euklidischen Alg. Zahlen $k, \ell \in \mathbb{Z}$ mit $k \cdot a + \ell \cdot b = 1$.

- Seien $a, b, c \in \mathbb{Z} \setminus \{0\}$ mit $a \mid b \cdot c$ und $(a,b) = 1$, dann gilt $a \mid c$:
  - $a \mid b \cdot c \Rightarrow a \cdot s = b \cdot c$
  - Seien $k, \ell \in \mathbb{Z}$ mit $k \cdot a + \ell \cdot b = 1$.
  - $c = c \cdot 1 = c \cdot (k \cdot a + \ell \cdot b) = k \cdot a \cdot c + \ell \cdot b \cdot c$
    $= k \cdot a \cdot c + \ell \cdot a \cdot s = a \cdot (\underbrace{k \cdot c + \ell \cdot s}_{=t}) = a \cdot t$

  d.h. $a \mid c$.

- Sind $p_1, \dots, p_n$ und $q_1, \dots, q_m$ Primzahlen und gilt $p_1 \cdot \dots \cdot p_n = q_1 \cdot \dots \cdot q_m$, so ist $n = m$ und $\{p_1, \dots, p_n\} = \{q_1, \dots, q_m\}$ (sogar als Multimengen):
  Aus $p_1 \mid q_1 \cdot \dots \cdot q_m$ und $p_1 \neq q_1$ folgt $(p_1, q_1) = 1$,
  also gilt $p_1 \mid q_2 \cdot \dots \cdot q_m$; etc.

- Somit ist die Primfaktorzerlegung in $\mathbb{Z}$ bis auf die Reihenfolge der Faktoren eindeutig; die Einheiten in $\mathbb{Z}$ (also 1 und -1) sind keine Primzahlen.

[Wir übertragen nun dieses Konzept auf Integritätsringe]

[Fragen: Ist z.B. -3 auch eine Primzahl in $\mathbb{Z}$? → eindeutige Primfaktorzerl.?]

I $(a,b) = d \Rightarrow ka + \ell b = d$; II $a \mid b \cdot c \wedge (a,b) = 1 \rightarrow a \mid c$; III Primfaktorzerleg.

Def. Sei R ein Integritätsring.

- Ein Element $r \in R$ heisst <u>irreduzibel</u> (unzerlegbar) in R falls $r \neq 0$, $r \notin R^*$, und aus $r = a \cdot b$ mit $a, b \in R$ folgt: $a \in R^*$ oder $b \in R^*$.
- Ein Element $p \in R$ heisst <u>Primelement</u>, falls $p \neq 0$, $p \notin R^*$ und aus $p \mid a \cdot b$ folgt: $p \mid a$ oder $p \mid b$.
- Zwei Elemente $a, b \in R$ heissen <u>assoziiert</u>, falls eine Einheit $r \in R^*$ existiert mit $a = r \cdot b$.

Bsp: In $\mathbb{Z}$ sind die Primzahlen (sowie deren add. Inverse) irreduzibel und Primelemente, und zwei Zahlen $a, b \in \mathbb{Z}$ sind genau dann assoziiert wenn $a = b$ oder $a = -b$.

Lemma 13.1 Sei R ein Integritätsring. Dann gilt:

(a) Primelemente sind irreduzibel (in R).

(b) Ein Element $p \in R$, $p \neq 0$ ist genau dann Primelement, wenn (p) ein Primideal ist.

Beweis: (a) Sei $p \in R$ Primelement und $p = a \cdot b$ mit $a, b \in R$.

zu zeigen: $a \in R^*$ oder $b \in R^*$

- Da $p = p \cdot 1$ gilt $p \mid p$, also $p \mid a \cdot b$, und weil p Primelement ist, folgt $p \mid a \vee p \mid b$.
- OBdA $p \mid a$, also $p \cdot r = a$ für ein $r \in R$.
- Es gilt nun $p = \underbrace{a \cdot b}_{\text{Voraussetzung}} = \underbrace{p \cdot r}_{= a} \cdot b$, also $p = p \cdot r \cdot b = 0$ $\Rightarrow p \cdot (1 - r \cdot b) = 0$
- Da R ein Integritätsring ist und $p \neq 0$, muss gelten $1 - r \cdot b = 0$, d.h. $1 = r \cdot b$ und somit ist $b \in R^*$.

hier brauchen wir, dass R ein Integritätsring ist

(b) ($\Rightarrow$) Sei $p \in R$ ein Primelement.

zu zeigen: (p) ist Primideal.

- $(p) \neq R$, da sonst $1 \in (p)$, d.h. $1 = r \cdot p$ und damit wäre $p \in R^*$.
- Seien $a, b \in R$ mit $a \cdot b \in (p)$.
  Dann ist $a \cdot b = r \cdot p$ für ein $r \in R$.
  D.h. $p \mid a \cdot b$ und weil p Primelement ist, gilt $p \mid a \vee p \mid b$; also $a \in (p) \vee b \in (p)$.

($\Leftarrow$) Sei $(p) \neq (0)$ ein Primideal. (Erinnerung: $p \neq 0$)

zu zeigen: p ist Primelement

- Da $(p) \neq R$ ist $1 \notin (p)$, d.h. es ex. kein $r \in R$ mit $r \cdot p = 1$ und somit ist $p \notin R^*$.
- Gilt nun $p \mid a \cdot b$, so ex. $r \in R$ mit $p \cdot r = a \cdot b$, d.h. $a \cdot b \in (p)$, und weil (p) ein Primideal ist, haben wir $a \in (p) \vee b \in (p)$; also $p \mid a \vee p \mid b$.

⊣

Bemerkungen

(1) Die Umkehrung von Lemma 13.1(a) gilt im Allg. nicht: [Betrachte Beträge $|z|$]
$R = \mathbb{Z}[i\sqrt{5}] \subseteq \mathbb{C}$ ist Integritätsring; $2 \in R$ ist irreduzibel;
$2 \mid (1+i\sqrt{5}) \cdot (1-i\sqrt{5}) = 6$, d.h. 2 ist kein Primelement.

(2) Ist R kein Integritätsring, so gilt Lem. 13.1(a) im Allg. nicht:
$R = \mathbb{Z}/6\mathbb{Z}$; $p = 2$, $2 \mid a \cdot b \Rightarrow$ a oder b gerade $\Rightarrow 2 \mid a \vee 2 \mid b$
also 2 ist Primelement in R; $2 \mid 2 \cdot 4$ aber $2 \notin R^* \wedge 4 \notin R^*$.
$\Rightarrow$ 2 ist reduzibel

Def. Sei R ein Ring und $r \in R$. Wir sagen r lässt sich **endlich in irreduzible Faktoren zerlegen** wenn gilt:

(a) es ex. irreduzible Elemente $u_1, \dots, u_n \in R$ und eine Einheit $a \in R^*$ mit $r = a \cdot u_1 \cdot \dots \cdot u_n$ (für $n = 0$ erhalten wir $r = a$);

(b) sind $r = a \cdot u_1 \cdot \ldots \cdot u_n$ und $r = b \cdot v_1 \cdot \ldots \cdot v_m$ zwei solche Zerlegungen, so ist $n = m$ und nach geeigneter Umnummerierung ist für alle $1 \le i \le n$, u_i assoziiert zu v_i (d.h. $u_i = c_i \cdot v_i$ für $c_i \in R^*$).

Bsp. $R = \mathbb{Z}$; $6 = \underbrace{1 \cdot 2 \cdot 3}_{a \cdot u_1 \cdot u_2} = \underbrace{(-1) \cdot (-2) \cdot 3}_{b \cdot v_1 \cdot v_2} = \underbrace{1 \cdot (-2) \cdot (-3)}_{c \cdot w_1 \cdot w_2} = \ldots$

$a, b, c \in \mathbb{Z}^*$; u_1, v_1, w_1 und u_2, v_2, w_2 paarweise assoz.

Def. Ein Ring R heisst faktoriell wenn gilt:

(a) R ist Integritätsring;

(b) jedes Element $r \neq 0$ in R besitzt eindeutige Zerlegung in irreduzible Faktoren.

[Bem. In der Literatur heissen faktorielle Ringe manchmal auch ZPE-Ringe; Zerlegung in Primfaktoren eindeutig.]

Faktum 13.2 In einem faktoriellen Ring ist jedes irreduzible Element ein Primelement.

[Bew. Aufgabe 77]

Bem. Mit Lem. 13.1 folgt: Ist R faktoriell, dann ist p Primelement $\iff$ p irreduzibel.

Def. Sei R ein Integritätsring und seien $a, b \in R \setminus \{0\}$. Dann heisst $d \in R$ grösster gemeinsamer Teiler von a und b wenn gilt: $d \mid a$, $d \mid b$ und aus $c \mid a \wedge c \mid b$ folgt $c \mid d$.

Faktum 13.3 Der ggT von a und b ist bis auf Einheiten eindeutig bestimmt.

Beweis: $a, b \in R \setminus \{0\}$; $d, \tilde{d}$ ggT von a & b. Dann gilt $d \mid \tilde{d}$ und $\tilde{d} \mid d$, d.h. $d \cdot r = \tilde{d}$ und $\tilde{d} \cdot \tilde{r} = d \Rightarrow d \cdot r \cdot \tilde{r} = d$. Also $d \cdot (r \cdot \tilde{r} - 1) = 0$, und mit $d \neq 0$ und R Integritätsring ist $r \cdot \tilde{r} = 1$, also d & $\tilde{d}$ assoz. ⌟

Lemma 13.4 Sei R ein Hauptidealring und $a, b \in R \setminus \{0\}$.
Ist d ein ggT von a und b, so gilt:

$$(d) = (a, b)$$ [(a,b) ist das von a & b erz. Ideal]

Beweis:
- Weil R ein Hauptidealring ist, ex. $c \in R$ mit $(a,b) = (c)$, und weil $a, b \in (a,b) = (c)$ gilt $c \mid a \wedge c \mid b$, also $c \mid d \Rightarrow (d) \subseteq (c)$.
- Andererseits gilt $d \mid a \wedge d \mid b$, also $a, b \in (d)$ $\Rightarrow (a,b) = (c) \subseteq (d)$.

⊣

Korollar 13.5 In einem Hauptidealring ist jedes irreduzible Element ein Primelement.

Beweis: Sei $p \in R$ irred., $a, b \in R \setminus \{0\}$ und $p \mid a \cdot b$.
Annahme: $p \nmid a$ (sonst sind wir fertig)
- Sei $(p, a) = (d)$ mit d ein ggT von p und a, d.h. $d \mid p$ und $d \mid a$.
- p irred. und $d \mid p \Rightarrow$ $d \in R^*$ oder $d = p \cdot e^{-1}$ ($e \in R^*$) ($d \cdot e = p$)
  und mit $d \mid a$ folgt $p \mid a$ ↯
- Weil $(p,a) = (d)$ ex. $s, t \in R$ sodass $s \cdot p + t \cdot a = d$, und für $\bar{d} := d^{-1}$ gilt: $(s \cdot \bar{d}) \cdot p + (t \cdot \bar{d}) \cdot a = 1$.
- Somit gilt $p \cdot (s \cdot \bar{d}) \cdot b + \underbrace{a \cdot b}_{= p \cdot r \text{ weil } p \mid a \cdot b} (t \cdot \bar{d}) = b$

$$\Rightarrow p \cdot (s \cdot \bar{d} \cdot b + t \cdot \bar{d} \cdot r) = b \Rightarrow p \mid b.$$

⊣

Theorem 13.6 Jeder Hauptidealring ist faktoriell.

Bem. Ist K ein Körper, so folgt mit Thm. 12.8, dass $K[X]$ faktoriell ist.

Beweis: Sei R ein Hauptidealring.

Zuerst zeigen wir, dass jedes Element aus R in irred. Faktoren zerlegbar ist:

- Sei $\tilde{R} := \{r \in R : r \neq 0 \text{ und } r \text{ ist } \underline{\text{nicht}} \text{ in irred. Faktoren zerlegbar}\}$.
  Wir führen die Annahme $\tilde{R} \neq \emptyset$ zu einem Widerspruch.
- Sei $r_0 \in \tilde{R}$. Dann ist $r_0 \neq 0$ und r_0 ist nicht irred., d.h. es ex. r_1, r_1' mit $r_1 \notin R^*$, $r_1' \notin R^*$ und $r = r_1 \cdot r_1'$, und weil $r_0 \in \tilde{R}$, ist mindestens einer der Faktoren r_1, r_1' in $\tilde{R}$ (denn wenn $r_1, r_1' \notin \tilde{R}$, dann sind r_1 und r_1' beide in irred. Faktoren zerlegbar, somit auch $r_0 = r_1 \cdot r_1'$).
- OBdA sei $r_1 \in \tilde{R}$. Dann gilt $(r_0) \subsetneq (r_1)$:
  - Weil $r_0 \in (r_1)$ gilt $(r_0) \subseteq (r_1)$.
  - Ist $(r_0) = (r_1)$, dann ist $r_1 = r_0 \cdot s$, d.h. $r_0 = r_1 \cdot r_1' = r_0 \cdot s \cdot r_1'$
    $\Rightarrow r_0(1 - s r_1') = 0 \Rightarrow 1 = s \cdot r_1' \Rightarrow r_1' \in R^*$ ↯ zu $r_1' \notin R^*$
- Weil $r_1 \in \tilde{R}$ gilt analog, dass ein $r_2 \in \tilde{R}$ ex. mit $(r_1) \subsetneq (r_2)$.
- So weiter gefahren, erhalten wir aus $\tilde{R} \neq \emptyset$ eine unendliche Kette $(r_0) \subsetneq (r_1) \subsetneq \dots \subsetneq (r_n) \subsetneq \dots$ von Idealen in R.
- Sei $I := \bigcup_{n \in \mathbb{N}} (r_n) \subseteq R$. Dann ist I ein Ideal in R:
  - $a, b \in I$, dann ex. $m \in \mathbb{N}$ mit $a, b \in (r_m)$ und es ist $a + b \in (r_m) \subseteq I$ und $s \cdot a \in (r_m) \subseteq I$ (für alle $s \in R$).
- Weil R ein Hauptidealring ist, ex. $a \in R$ mit $I = (a)$, und weil $a \in I$ ex. $n_0 \in \mathbb{N}$ mit $a \in (r_{n_0}) \subsetneq (r_{n_0+1}) \subsetneq I = (a)$ ↯ zu $(a) \subseteq (r_{n_0})$
- Somit muss die Kette $(r_0) \subsetneq \dots$ abbrechen ↯ zu $\tilde{R} \neq \emptyset$

Nun zeigen wir, dass die Zerlegung eindeutig ist:

- Sei $r \in R$ mit $r = a \cdot u_1 \cdot \dots \cdot u_n = b \cdot v_1 \cdot \dots \cdot v_m$ wobei $a, b \in R^*$ und u_i, v_j irreduzibel sind.
- Mit Kor. 13.5 sind u_i, v_j Primelemente, d.h. $v_j \mid a \cdot u_1 \cdot \dots \cdot u_n$
  $\Rightarrow v_j$ teilt einen Faktor. ∘ $v_j \mid a \Rightarrow v_j \cdot s = a \Rightarrow v_j \cdot (s a^{-1}) = 1 \Rightarrow v_j \in R^*$ ↯
  ∘ $v_j \mid u_i \Rightarrow u_i = s \cdot v_j$ und weil u_i, v_j irred., ist $s \in R^*$, d.h. u_i, v_j assoz. ∎

Def. Sei R ein faktorieller Ring und $q \in R[X]$ mit $q \neq 0$. Dann heisst q **primitiv**, falls ein ggT der Koeffizienten von q gleich 1 ist. [Erinnerung: der ggT ist bis auf Einh. eind.]

Lemma 13.7 (Gauss) Sei R ein faktorieller Ring und $q \in R[X]$ primitiv. Weiter sei $Q := \mathrm{Quot}(R)$ der Quotientenkörper von R. Dann gilt:

$$q \text{ irreduzibel in } R[X] \iff q \text{ irreduzibel in } Q[X]$$

Beweis: Mit Kontraposition. (2-mal)

($\Rightarrow$) Wir nehmen an, dass q zerlegbar in $Q[X]$ ist.

- Sei $q = s \cdot t$ mit $s, t \notin Q[X]^* = Q^* = Q \setminus \{0\}$ (Prp. 12.5(b)).
- Weil $q \neq 0$ ist $s \neq 0 \neq t$, somit $s, t \notin Q$, aber $s, t \in Q[X]$.
- Sei $s = a_0 + a_1 X + \ldots + a_n X^n$ mit $a_i \in Q$, $a_n \neq 0$, $n \geq 1$. Dann ist $a_i = \frac{c_i}{d_i}$ mit $c_i, d_i \in R$, $d_i \neq 0$, und für den Hauptnenner $a := d_0 \cdot \ldots \cdot d_n$ ist dann $a \in R$ und $a \cdot s \in R[X]$.
- Analog finden wir $b \in R$ mit $b \cdot t \in R[X]$.
- Somit ist $(a \cdot s) \cdot (b \cdot t) = (a \cdot b) \cdot (s \cdot t) = (a \cdot b) \cdot q$ mit $a \cdot b \in R$.
- Weil R faktoriell ist gilt $a \cdot b = e \cdot u_1 \cdot \ldots \cdot u_k$ mit $e \in R^*$ und u_i irreduzibel in R, also u_i Primelement in R (Faktum 13.2).
- Es gilt somit $(a \cdot s) \cdot (b \cdot t) = (e \cdot u_1 \cdot \ldots \cdot u_k) \cdot q$
- Weil alle u_i's Primelemente sind und für alle u_i gilt $u_i \mid a \cdot b$, folgt für alle u_i: $u_i \mid a$ oder $u_i \mid b$. D.h. wir können alle u_i's kürzen und erhalten

$$(e_s \cdot s) \cdot (e_t \cdot t) = e \cdot q \quad \text{wobei } e_s, e_t, e \in R^*.$$

Somit ist $\underbrace{(e^{-1} \cdot e_s \cdot s)}_{\in R[X]} \cdot \underbrace{(e_t \cdot t)}_{\in R[X]} = q$ und q ist zerlegbar in $R[X]$.

($\Leftarrow$) Wir nehmen an, dass q zerlegbar in $R[X]$ ist.

- Sei $q = s \cdot t$ mit $s, t \in R[X]$ und $s, t \notin R[X]^* = R^*$.
- Ist $s \in R \setminus R^*$ oder $t \in R \setminus R^*$, so ist q nicht primitiv $\lightning$ zur Voraussetzung
- Also $s, t \notin R$, und weil $s, t \in R[X]$, ist $\operatorname{grad}(s), \operatorname{grad}(t) \geq 1$.
- D.h. $s, t \in Q[X] \setminus Q$ und $q = s \cdot t$ ist zerlegbar in $Q[X]$. $\dashv$

[Bem. $q = \underbrace{4X^5 - 12X^3 + 18X^2 - 30}_{2 \cdot (2X^5 - 6X^3 + 9X^2 - 15)}$ ist zerlegbar in $\mathbb{Z}[X]$ aber irreduzibel in $Q[X]$]

Kriterium von Schönemann-Eisenstein 13.9

Sei R ein faktorieller Ring, $q \in R[X]$, q primitiv, $\operatorname{grad}(q) = n \geq 1$,

$$q = a_0 + a_1 X + \ldots + a_n X^n, \quad a_n \neq 0.$$

Existiert ein Primelement $p \in R$ mit

- $p \mid a_i$ für $0 \leq i < n$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

dann ist q irreduzibel in $R[X]$ (und mit Gauss' Lemma auch in $Q[X]$).

Beweis: Seien $s, t \in R[X]$ mit $q = s \cdot t$.

zu zeigen: $s \in R^*$ oder $t \in R^*$, wobei $R^* = R[X]^*$.

- Seien $s = b_0 + \ldots + b_k X^k$, $t = c_0 + \ldots + c_\ell X^\ell$ mit $k, \ell \leq n$ und $b_k, c_\ell \neq 0$.
- Dann ist $q = s \cdot t = \underbrace{b_0 \cdot c_0}_{= a_0} + \underbrace{(b_0 \cdot c_1 + b_1 \cdot c_0)}_{a_1} \cdot X + \ldots + b_k c_\ell X^{k+\ell}$ mit $n = k + \ell$.
- p Primelement $\left.\begin{array}{l} p \mid b_0 \cdot c_0 \Rightarrow p \mid b_0 \vee p \mid c_0 \\ p^2 \nmid b_0 \cdot c_0 \Rightarrow \neg(p \mid b_0 \wedge p \mid c_0) \end{array}\right\}$ entweder $p \mid b_0$ oder $p \mid c_0$

- OBdA $p \mid b_0 \wedge p \nmid c_0$.
- $p \nmid \underbrace{a_n}_{= b_k \cdot c_\ell} \Rightarrow p \nmid b_k \wedge p \nmid c_\ell$
- Weil $p \mid b_0$ und $p \nmid b_k$ ex. kleinstes $j \leq k$ mit $p \mid b_i$ für $0 \leq i < j$ und $p \nmid b_j$.
- Für a_j gilt dann $a_j = \underbrace{b_0 c_j}_{p \text{ teilt}} + \underbrace{b_1 c_{j-1}}_{p \text{ teilt}} + \ldots + \underbrace{b_{j-1} \cdot c_1}_{p \text{ teilt}} + \underbrace{b_j c_0}_{p \text{ teilt nicht}}$

  und $p \mid a_i$ mit $i < j$ $\Rightarrow p \nmid a_j \Rightarrow j = n = k + \ell \Rightarrow j = k = n \wedge \ell = 0$.
- Somit ist $\operatorname{grad}(t) = 0$, also $t \in R$, und weil $q = s \cdot t$ und q primitiv ist, ist $t \in R^*$.
- Unter der Annahme $p \nmid b_0 \wedge p \mid c_0$ folgt analog $s \in R^*$.
- Somit folgt aus $q = s \cdot t$, dass $s \in R^*$ oder $t \in R^*$, d.h. q ist irreduzibel in $R[X]$.

⊣

Beispiel: $q = 2X^5 - 6X^3 + 9X^2 - 15 \in \mathbb{Z}[X]$

- q ist primitiv
- Für $p = 3$ gilt: $p \mid \overbrace{15}^{a_0}$, $p \mid \overbrace{0}^{a_1}$, $p \mid \overbrace{9}^{a_2}$, $p \mid \overbrace{6}^{a_3}$, $p \mid \overbrace{0}^{a_4}$

  $p \nmid \overbrace{2}^{a_5}$

  $p^2 \nmid \overbrace{15}^{a_0}$

Somit ist q irred. in $\mathbb{Z}[X]$ und weil $\mathbb{Q} = \operatorname{Quot}(\mathbb{Z})$ ist q auch irred. in $\mathbb{Q}[X]$.