2. Ringe

Vorwissen:

nullteilerfreie Ringe

$K[x,y,z,w]/(2xy-zw)$

$\mathbb{Z}[\sqrt{-3}]$

Noethersch, nicht faktoriell: $\mathbb{Z}[i\sqrt{5}]$

Faktoriell, nicht noethersch: $K[x_1, x_2, \ldots]$

Faktorielle Ringe

$K[x_1, \ldots, x_n]$

$\mathbb{Z}[x]$

($\langle 2, x \rangle$ ist kein Hauptideal)

(ohne Beweis: Satz von Gauß: R faktoriell $\Rightarrow$ R[x] faktoriell)

Noethersche Ringe

$K[x_1, \ldots, x_n]$

Hauptidealringe

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

(ohne Beweis)

euklidische Ringe

$\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$

Vorwissen:

Faktorielle Ringe,
Primelemente, irreduzible Elemente,
Einheiten,
Primfaktorzerlegung,
ggT und kgV
Quotientenkörper

Polynomringe
K-Algebra

in Kapitel 3 auch:
euklidische Ringe
Ideale
Noethersche Ringe
chinesischer Restsatz

in Kapitel 4 auch:
maximale Ideale

Notation: R bezeichnet einen kommutativen Ring mit 1.

Der Satz von Gauß und allgemeine Polynomringe

2.1 Satz (Satz von Gauß)

R faktoriell $\Rightarrow$ $R[X]$ faktoriell.

2.2 Def

Sei R nullteilerfrei,

$0 \neq f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ein Polynom. f heißt primitiv, falls

$1 = ggT(a_0, \dots, a_n)$.

2.3 Lemma

Sei R faktoriell.

1) Ist $f \in R[X]$ primitiv und $c \in Quot(R)$ mit $c \cdot f \in R[X]$, so ist $c \in R$.

2) Für $f \in Quot(R)[X]$ $\exists$ $0 \neq c \in Quot(R)$ und $g \in R[X]$ primitiv mit $f = c \cdot g$.

Beweis:

1) Sei $f = \sum_{i=0}^{n} a_i x^i$, $c = \frac{a}{b}$ mit $a, b \in R$ teilerfremd. Da $cf \in R[x] \Rightarrow$

$\frac{a a_i}{b} \in R \quad \forall i = 0, \dots, n.$

Sei $p \in R$ prim mit $p \mid b$.

Da $p \nmid a$ folgt aus $\frac{a a_i}{b} \in R$

$p \mid a_i \quad \forall i = 0, \dots, n$

$\Rightarrow p \mid ggT(a_0, \dots, a_n)$

$\Rightarrow ggT(a_0, \dots, a_n) \neq 1 \Rightarrow f$ nicht primitiv

$\Rightarrow \nexists$ solches p

$\Rightarrow b \in R^* \Rightarrow c = \frac{a}{b} \in R.$

2) Sei $f = \sum_{i=0}^{n} \frac{a_i}{b_i} \cdot x^i$ mit

$a_i \in R$, $b_i \in R \setminus \{0\}$.

$\Rightarrow b_0 \cdots b_n \cdot f \in R[x]$ und für $d = ggT(\text{Koeffizienten von } b_0 \cdots b_n f)$ gilt

$g := \frac{b_0 \cdots b_n \cdot f}{d} \in R[x]$ ist

primitiv und $c \cdot g = f$ mit

$c = \frac{d}{b_0 \cdots b_n} \in \mathrm{Quot}(R)$. □

Bsp:

Sei $f = x^3 - 3x + \frac{1}{4} \in \mathbb{Q}[x]$,

dann ist $g = 4x^3 - 12x + 1 \in \mathbb{Z}[x]$

primitiv und für $c = \frac{1}{4} \in \mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$

gilt $c \cdot g = f$.

2.4 Lemma Sei R nullteilerfrei, $p \in R$

prim $\Rightarrow$ p ist prim in $R[x]$.

Beweis: Seien $f = \sum_{i=0}^{n} a_i x^i$ und

$g = \sum_{j=0}^{m} b_j x^j \in R[x]$ mit

$p \mid f \cdot g = \sum_{k=0}^{m+n} c_k x^k$ mit

$$c_k = \sum_{l=0}^{k} a_l b_{k-l}.$$

$\Rightarrow \quad p \mid c_k \quad \forall k \quad (*)$

Angenommen, $p \nmid f$ und $p \nmid g$.

Dann $\exists \; i_0, j_0 : p \nmid a_{i_0}, \; p \nmid b_{j_0}$.

Wähle i_0, j_0 minimal.

Dann gilt

$$a_{i_0} b_{j_0} = c_{i_0+j_0} - \sum_{\ell=0}^{i_0-1} a_\ell \, b_{i_0+j_0-\ell} - \sum_{\ell=i_0+1}^{i_0+j_0} a_\ell \, b_{i_0+j_0-\ell}$$

und p teilt jeden Summanden auf der rechten Seite:

- $c_{i_0+j_0}$ wegen $(*)$
- $a_\ell \, b_{i_0+j_0-\ell}$ für $\ell < i_0 - 1$, da dann a_ℓ von p geteilt wird, da i_0 minimal mit $p \nmid a_{i_0}$
- $a_\ell \, b_{i_0+j_0-\ell}$ für $\ell > i_0 + 1$, da dann $b_{i_0+j_0-\ell}$ von p geteilt wird

da j_0 minimal mit $p \nmid b_{j_0}$.

$\Rightarrow \quad p \mid a_{i_0} b_{j_0}$

p prim $\Rightarrow \quad p \mid a_{i_0}$ oder $p \mid b_{j_0}$ $\lightning$

zur Wahl von a_{i_0}, b_{j_0} □

2.5 Lemma

Sei R faktoriell, $f, g \in R[x]$ primitiv, dann ist auch $f \cdot g$ primitiv.

Beweis: Angenommen, $f \cdot g$ ist nicht primitiv $\Rightarrow \exists$ Primelement $p \in R$, das jeden Koeffizienten von $f \cdot g$ teilt

$\Rightarrow p \mid f \cdot g \overset{2.4}{\Rightarrow} p \mid f$ oder $p \mid g$, da p auch in $R[x]$ prim ist

↯ zu f, g primitiv. □

2.6 Lemma

Sei R faktoriell, $f \in R[x]$ primitiv, f prim in $\mathrm{Quot}(R)[x]$. Dann ist f prim in $R[x]$.

Beweis: Da f primitiv ist, ist $f \neq 0$.

Da $f \in \mathrm{Quot}(R)[x]$ prim ist, ist $f \notin R^* = (R[x])^*$, also keine Einheit

in $R[x]$.

Seien $g, h \in R[x]$ mit $f \mid g \cdot h$ in $R[x]$.

Dann gilt auch $f \mid g \cdot h$ in $\mathrm{Quot}(R)[x]$,

und da f dort prim ist, folgt $\in$

$f \mid g$ in $\mathrm{Quot}(R)[x] \Rightarrow \exists\, q \in \mathrm{Quot}(R)[x]$:

$$f \cdot q = g.$$

Wie in 2.3 schreiben wir q als

$q = c \cdot \tilde{q}$ mit $\tilde{q} \in R[x]$ primitiv

und $c \in \mathrm{Quot}(R)$.

Dann gilt $g = f \cdot q = c \cdot f \cdot \tilde{q}$.

Wegen $f, \tilde{q}$ primitiv in $R[x]$ folgt

mit 2.5 : $f \cdot \tilde{q}$ primitiv in $R[x]$.

Damit folgt aus 2.3.1) $c \in R$

$\Rightarrow q \in R[x] \Rightarrow f \mid g$ in $R[x]$

□

Beweis von Satz 2.1 (Gauß):

Sei $0 \neq f \in R[x]$, $f \notin (R[x])^* \cup \{0\}$.

Zu zeigen: f besitzt eine Darstellung

als Produkt von Primelementen.

Ist $f \in R$, so folgt dies aus der Tatsache, daß R faktoriell ist, und Lemma 2.4.

Sei $\deg(f) \geq 1$.

Da $\mathrm{Quot}(R)$ ein Körper ist, ist $\mathrm{Quot}(R)[X]$ euklidisch, daher Hauptidealring, daher faktoriell.

In $\mathrm{Quot}(R)[X]$ können wir f also schreiben als

$f = q_1 \cdots q_k$ mit $q_i \in \mathrm{Quot}(R)[X]$ prim.

Wie in 2.3. 2) schreiben wir

$q_i = c_i \cdot p_i$ mit $c_i \in \mathrm{Quot}(R)$ und $p_i \in R[X]$ primitiv.

p_i und q_i sind assoziiert in $\mathrm{Quot}(R)[X]$ (da $c_i \in \mathrm{Quot}(R)$ Einheit, da $c_i \neq 0$ und $\mathrm{Quot}(R)$ Körper),

also ist mit q_i auch p_i prim in $\mathrm{Quot}(R)[X]$.

Wegen 2.6 ist p_i prim in $R[X]$.

Wegen 2.5 ist

$$p := p_1 \cdots p_k \in R[X]$$

primitiv.

Da $f = c \cdot p \in R[X]$ mit $c := c_1 \cdots c_k \in \mathrm{Quot}(R)$ und p primitiv folgt aus 2.3 1) $c \in R$.

Da R faktoriell ist, können wir $c = b_1 \cdots b_e$ in Primfaktoren b_i zerlegen, die wegen 2.4 prim in $R[X]$ sind.

Damit ist $f = b_1 \cdots b_e \cdot p_1 \cdots p_k$ eine Zerlegung in Primfaktoren in $R[X]$.

Die Eindeutigkeit der Zerlegung

bis auf Anordnung und Einheiten folgt per Induktion über die Anzahl der Faktoren und der definierenden Eigenschaft der Primelemente. □

Bsp

1) $\mathbb{Z}[x]$ ist faktoriell.
2) Ist K ein Körper, so ist $K[x_1, \dots, x_n]$ faktoriell.

2.7 Def

Sei I eine beliebige Menge.

$$R[x_i \mid i \in I] = \left\{ \sum_{\alpha = (\alpha_1, \dots, \alpha_k) \in \mathbb{N}^k} a_\alpha \, x_{i_1}^{\alpha_1} \cdots x_{i_k}^{\alpha_k} \;\middle|\; k \in \mathbb{N},\ \{i_1, \dots, i_k\} \subset I,\ a_\alpha \in R,\ \text{nur endlich viele } a_\alpha \neq 0 \right\}$$

ist der Polynomring in den Variablen x_i mit $i \in I$.

Für $|I| < \infty$, o.E. $I = \{1, \dots, n\}$ ist es $R[x_1, \dots, x_n]$.

Multiindexnotation:

Für $(i_1, \dots, i_k)$ fest und $\alpha \in \mathbb{N}^k$ schreiben wir

$$X^\alpha := X_{i_1}^{\alpha_1} \cdots X_{i_k}^{\alpha_k}.$$

Für $f \in R[X_i, i \in I]$ ist die Menge der vorkommenden Variablen (i.e. ij: $\exists \alpha : a_\alpha \neq 0, \alpha_j \neq 0$) $\{i_1, \dots, i_k\}$ der <u>Support</u> von f, $\mathrm{supp}(f)$.

Durch Hinzufügen von Nullen als Exponenten können wir ein Polynom immer bezüglich einer größeren Variablenmenge darstellen.
Durch Hinzufügen von Nullen als Koeffizienten können wir auch die Exponentenmenge erweitern.

Für $f, g \in R[X_i \mid i \in I]$ schreiben wir f und g bezüglich derselben Variablenmenge $(\mathrm{supp}(f) \cup \mathrm{supp}(g))$ sowie derselben Exponentenmenge,

$$f = \sum_\alpha a_\alpha X^\alpha, \quad g = \sum_\alpha b_\alpha X^\alpha$$

und definieren

$$f+g = \sum_{\alpha} (a_\alpha + b_\alpha) x^\alpha \quad \text{und}$$

$$f \cdot g = \sum_{\beta} \left(\sum_{\alpha+\alpha'=\beta} a_\alpha b_{\alpha'} \right) x^\beta$$

wobei die zweite Summe über alle β geht, die als Summen von Exponenten in f und g vorkommen.

Durch diese Verknüpfungen wird $R[x_i \mid i \in I]$ ein kommutativer Ring mit 1.

2.8 Lemma

Sei R nullteilerfrei, I eine Menge, $J \subset I$ eine endliche Teilmenge.

1) $(R[x_i \mid i \in I])^* = R^*$

2) Sei $p \neq 0$, $p \in R[x_j \mid j \in J] \setminus R^*$.

p prim in $R[x_j \mid j \in J] \iff$
p prim in $R[x_i \mid i \in I]$.

Beweis: Sei $f \in (R[x_i \mid i \in I])^*$

$\Rightarrow \exists\, g \in R[x_i \mid i \in I] : f \cdot g = 1.$

In f und g kommen nur endlich viele Variablen x_j mit $j \in J$ vor, daher gilt $f \cdot g = 1$ in $R[x_j \mid j \in J]$

$\Rightarrow f \in R^*$.

2) „$\Rightarrow$" Sei p prim in $R[x_j \mid j \in J]$.

Seien $f, g \in R[x_i \mid i \in I]$ mit $p \mid f \cdot g$. Es gibt eine endliche Menge $J' \supset J$, die alle Variablen von p, f und g enthält ($J' = J \cup \operatorname{supp} f \cup \operatorname{supp} g$)

$\Rightarrow p \mid f \cdot g$ in $R[x_j \mid j \in J']$

Durch Induktion folgt mit 2.4, daß p prim in $R[x_j \mid j \in J']$ ist

$\Rightarrow \; p \mid f$.

$\Rightarrow p$ prim in $R[x_i \mid i \in I]$.

„$\Leftarrow$" Sei p prim in $R[x_i \mid i \in I]$.

Seien $f, g \in R[x_j \mid j \in J]$ mit

$p \mid f \cdot g \Rightarrow p \mid f \cdot g$ in $R[x_i \mid i \in I]$

$\overset{p \text{ prim}}{\Rightarrow} \; p \mid f$ in $R[x_i \mid i \in I] \Rightarrow$

$\exists\ q \in R[x_i \mid i \in I]$:

$q \cdot p = f$.

Da $p, f \in R[x_j \mid j \in J]$ kann q keine Variable x_i mit $i \notin J$ enthalten, also folgt $q \in R[x_j \mid j \in J]$ und $p \mid f$ in $R[x_j \mid j \in J] \Rightarrow$ p prim in $R[x_j \mid j \in J]$. □

2.9 Proposition

Sei I eine Menge. Sei R faktoriell. $R[x_i \mid i \in I]$ ist faktoriell.

Beweis:

Sei $0 \neq f \in R[x_i \mid i \in I] \setminus R^*$.

Dann ist $J = \mathrm{supp}(f)$ endlich und $f \in R[x_j \mid j \in J]$. In diesem Ring hat f durch Induktion und den Satz von Gauß eine eindeutige Primfaktorzerlegung, die wegen 2.8 2) eine Primfaktorzerlegung in $R[x_i \mid i \in I]$ ist. □

2.10 Satz (Universelle Eigenschaft von Polynomringen)

Sei I eine Menge, A eine R-Algebra, $a_i \in A \quad \forall i \in I$.

Dann $\exists!$ R-Algebrenhomomorphismus

$\varphi: R[X_i \mid i \in I] \longrightarrow A$ mit $X_i \longmapsto a_i$,

der Einsetzehomomorphismus.

Das Bild von φ heißt die von den a_i erzeugte Unteralgebra $\langle a_i \mid i \in I \rangle \subset A$.

Man schreibt auch $\langle a_i \mid i \in I \rangle_R$ oder $R[a_i \mid i \in I]$ für $\mathrm{Im}(\varphi)$, also für die von den a_i erzeugte Unter(-R-)Algebra von A.

Beweis: Durch

$$\varphi\Big(\sum_{\alpha} b_\alpha X_{i_1}^{\alpha_1} \cdots X_{i_k}^{\alpha_k}\Big) = \sum_{\alpha} b_\alpha a_{i_1}^{\alpha_1} \cdots a_{i_k}^{\alpha_k}$$

ist der eindeutige Homomorphismus gegeben. □