Definition der Polynomringe

Definition (11.22)

Sei R ein Ring. Ein Erweiterungsring S von R wird Polynomring über R genannt, wenn es ein ausgezeichnetes Element $x \in S$ gibt mit der Eigenschaft, dass für jedes Element $f \in S \setminus \{0_R\}$ ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte $a_0, ..., a_n \in R$ existieren, so dass $a_n \neq 0$ ist und f in der Form

$$f = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$$

dargestellt werden kann.

Der Polynomring über R mit der Variablen x wird mit $R[x]$ bezeichnet.

Universelle Eigenschaft des Polynomrings

Satz (11.23)

Für jeden Ringhomomorphismus $\phi : R \to S$ und jedes $a \in S$ gibt es einen eindeutig bestimmten Ringhomomorphismus $\hat{\phi} : R[x] \to S$ mit $\hat{\phi}|_R = \phi$ und $\hat{\phi}(x) = a$.

Ist $S = R$ oder ein Erweiterungsring von R, dann bezeichnet man den eindeutig bestimmten Homorphismus $\hat{\phi}$ aus Satz 11.23 als den Auswertungshomomorphismus an der Stelle a.

Folgerung (11.24)

Je zwei Polynomringe über einem Ring R sind isomorph.

Beweis von Satz 11.23

Bem. Jedes Element $f \in R[x]$ kann durch eine Folge $(a_n)_{n \in \mathbb{N}_0}$ mit $a_n = 0_R$ für alle bis auf endlich viele $n \in \mathbb{N}_0$ beschrieben werden, indem man

(*) $\quad f = \sum_{n \in \mathbb{N}_0} a_n x^n$ schreibt.

geg: Ringhom $\phi : R \to S$, $a \in S$

zzg: Es existiert ein eind. bestimmter Ringhom.

$\hat{\phi} : R[x] \to R$ mit $\hat{\phi}|_R = \phi$ und $\hat{\phi}(x) = a$

Existenz: Für ein beliebiges $f \in K[x]$ geg. in der Form (*)

definiere $\hat{\phi}(f) = \sum_{n \in \mathbb{N}_0} \phi(a_n)\, a^n$

Dann gilt $\hat{\phi}(x) = a$ und $\hat{\phi}(b) = \phi(b) \;\forall\, b \in R$.

zu überprüfen: $\hat{\phi}$ ist Ringhom.

Es gilt $\hat{\phi}(1_R) = \phi(1_R) = 1_S$
($1_R \in R$; ϕ Ringhom)

Seien nun $f, g \in R[x]$, $m, n \in \mathbb{N}_0$ mit $\operatorname{grad}(f) = m$ oder $f = 0_R$ und $\operatorname{grad}(g) = n$ oder $g = 0_R$ und $f = \sum_{k \in \mathbb{N}_0} a_k x^k$, $g = \sum_{k \in \mathbb{N}_0} b_k x^k$

$\Rightarrow f + g = \sum_{k \in \mathbb{N}_0} (a_k + b_k) x^k$, $fg = \sum_{k=0}^{m+n} c_k x^k$ mit $c_k = \sum_{j=0}^{k} a_{k-j} b_j$ $\Rightarrow \hat{\phi}(f+g) = \sum_{k \in \mathbb{N}_0} \phi(a_k + b_k)\, a^k \overset{\phi \text{ Ringhom}}{=} \sum_{k \in \mathbb{N}_0} \left(\phi(a_k) + \phi(b_k)\right) a^k$

$$= \sum_{k \in \mathbb{N}_0} \phi(a_k)\, a^k + \sum_{k \in \mathbb{N}_0} \phi(b_k)\, a^k = \hat{\phi}(f) + \hat{\phi}(g)$$

und $\hat{\phi}(fg) = \sum_{k=0}^{m+n} \phi(c_k)\, a^k =$

$$\sum_{k=0}^{m+n} \left(\sum_{j=0}^{k} \phi(a_{k-j})\, \phi(b_k) \right) a^k = \left(\sum_{j=0}^{m} \phi(a_j)\, a^j \right) \cdot$$

$$\left(\sum_{i=0}^{n} \phi(b_i)\, a^i \right) = \hat{\phi}(f) \cdot \hat{\phi}(g)$$

<u>Eindeutigkeit</u>: Sei $\psi : R[x] \to S$ ein weiterer Hom. mit den angeg. Eigenschaften und $f \in R[x]$, $f = \sum_{k \in \mathbb{N}_0} a_k x^k$

$$\hat{\phi}(f) = \sum_{k \in \mathbb{N}_0} \hat{\phi}(a_k)\,\hat{\phi}(x)^k = \sum_{k \in \mathbb{N}_0} \phi(a_k)\,a^k$$

↑ $\hat{\phi}$ Ringhom

↑ $\hat{\phi}|_{\mathbb{R}} = \phi$, $\hat{\phi}(x) = a$

$$= \sum_{k \in \mathbb{N}_0} \psi(a_k)\,\psi(x)^k = \psi(f)$$

↑ $\psi|_{\mathbb{R}} = \phi$, $\psi(x) = a$

↑ ψ Hom.

□

(g)

Beweis von Folgerung 11.24:

Sei R ein Ring. $R[x]$ ein Polynomring über R und S ein weiterer Polynom über R, mit der Variablen $y \in S$. Beh.: Es gibt einen Isom. $\hat{\phi}: R[x] \to S$ mit $\hat{\phi}|_R = id_R$

Wende Satz 11.23 an auf den Hom. $\phi: R \to S$, $r \mapsto r$ und das Element $a = y$. $\Rightarrow$ erhalte einen (eind. best.) Ringhom. $\hat{\phi}: R[x] \to S$ mit $\hat{\phi}(x) = y$ und $\hat{\phi}(r) = \phi(r) = r \quad \forall r \in R$

Wende Satz 11.23 an auf den Hom. $\phi_1: R \to R[x]$, $r \mapsto r$ und das Element $a = x$. $\Rightarrow$ erhalte einen

(eind. best.) Ringhom. $\hat{\phi}_1 : S \to R[x]$ mit $\hat{\phi}_1(y) = x$ und $\hat{\phi}_1(r) = \phi_1(r) = r \quad \forall r \in R$

Es gilt dann $(\hat{\phi}_1 \circ \hat{\phi})(x) = \hat{\phi}_1(y) = x$ und $(\hat{\phi}_1 \circ \hat{\phi})(r) = r \quad \forall r \in R$. $(\hat{\phi}_1 \circ \hat{\phi})|_R = id_R$

Der Ringhom $id_{R[x]}$ hat dieselben Eigenschaften.

Eindeutigkeit (Satz 11.23) $\Rightarrow \hat{\phi}_1 \circ \hat{\phi} = id_{R[x]}$

Genauso zeigt man $\hat{\phi} \circ \hat{\phi}_1 = id_S$

Also ist $\hat{\phi}$ und $\hat{\phi}_1$ zueinander inverse Isomorphismen.

□

Eigenschaften der Polynomringe

Proposition (11.29)

Sei R ein Ring und $R[x]$ ein Polynomring über R.

(i) Sind $0_R \neq f, g \in R[x]$ und gilt auch $f + g \neq 0_R$ und $fg \neq 0_R$, dann folgt

$$\operatorname{grad}(f+g) \leq \max\{\operatorname{grad}(f), \operatorname{grad}(g)\}$$

und

$$\operatorname{grad}(fg) \leq \operatorname{grad}(f) + \operatorname{grad}(g).$$

(ii) Ist R ein Integritätsbereich, dann gilt dasselbe auch für den Ring $R[x]$. In diesem Fall gilt sogar

$$\operatorname{grad}(fg) \quad = \quad \operatorname{grad}(f) + \operatorname{grad}(g)$$

für alle $f, g \in R[x]$ mit $f, g \neq 0_R$.

Die Einheitengruppen der Polynomringe

Folgerung (11.30)

Sei R ein Integritätsbereich. Dann gilt $R[x]^\times = R^\times$, d.h. die Einheitengruppe des Polynomrings $R[x]$ stimmt mit der Einheitengruppe des Grundrings R überein.

Beweis von Folgerung 11.30.

geg. Integritätsbereich R. z.zg.: $(R[x])^\times = R^\times$

„$\supseteq$" Sei $a \in R^\times$. $\Rightarrow \exists b \in R$ mit $a \cdot b = 1_R$

Da R Teilring von $R[x]$ ist und somit $1_R = 1_{R[x]}$ gilt, zeigt die Gleichung, dass a in $(R[x])^\times$ liegt.

„$\subseteq$" Sei $f \in (R[x])^\times$. $\Rightarrow \exists g \in R[x]$ mit $f \cdot g = 1_R$

$1_R \neq 0_R$ in R $\Rightarrow f \cdot g \neq 0_R \Rightarrow \operatorname{grad}(f) + \operatorname{grad}(g) =$

$\operatorname{grad}(fg) = \operatorname{grad}(1_R) = 0$ $\xrightarrow{\operatorname{grad}(f),\ \operatorname{grad}(g) \geq 0}$ $\operatorname{grad}(f) =$ (Prop. 11.29)

$\operatorname{grad}(g) = 0 \Rightarrow f, g \in R$ $\xrightarrow{f \cdot g = 1_R}$ $f \in R^\times$ □

$f \in R$ □

Bem. Ist R kein Integritätsbereich, dann gibt es in $R[x]$ möglicherweise Einheiten außerhalb von $R^\times$.

Bsp.: $R = \mathbb{Z}/4\mathbb{Z}$, $f = \bar{1} + \bar{2}x \in R[x]$ $(\Rightarrow \operatorname{grad}(f) = 1)$

$$f \cdot f = \bar{1} + \bar{4}x + \bar{4}x^2 = \bar{1} = 1_{R[x]} \quad \Rightarrow f \in (R[x])^\times$$

$\uparrow\ \bar{4} = \bar{0}$

□

Rückblick: Ringtheorie

- Definition der Ringe (additive abelsche Gruppe, multiplikatives abelsches Monoid, Distributivgesetz)
- Grundbegriffe: Ringhomomorphismus, Einheit, Nulteiler, Charakteristik, Integritätsbereich, Körper
- Definition der Teilringe (Ringeigenschaft), von einer Teilmenge $A \subseteq \tilde{R}$ über R erzeugter Teilring $R[A]$
- Ideale und ihre Erzeugendensysteme (Nullideal, Einheitsideal, Hauptideal, Primideal, maximales Ideal)
- Teilbarkeitsbegriff und Beziehung zur Idealtheorie
- Definition der Faktorringe R/I
  (für einen Ring R und ein Ideal $I \subseteq R$)
- Konstruktion von Ringerweiterungen durch Monomorphismen (Anwendungen: komplexe Zahlen, Quotientenkörper, Polynomringe)

Definition (12.1)

Die Normfunktion $N : \mathbb{C} \to \mathbb{R}_+$ ist definiert durch

$$N(z) \quad = \quad z\bar{z} \quad = \quad |z|^2 \quad \text{für alle} \quad z \in \mathbb{C}.$$

Die wichtigste Eigenschaft der Normfunktion ist die Multiplikativität: Für alle $z, w \in \mathbb{C}$ gilt $N(zw) = N(z)N(w)$.

Die Normfunktion auf den quadratischen Teilringen

Lemma (12.2)

Sei $d \in \mathbb{N}$. Schränkt man die Normfunktion auf die Elemente des Rings $\mathbb{Z}[\sqrt{-d}]$ bzw. $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})]$ ein, so erhält man ausschließlich Werte in $\mathbb{N}_0$. Genauer gilt:

(i) Ist $\alpha \in \mathbb{Z}[\sqrt{-d}]$, $\alpha = a + b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$, dann ist

$$N(\alpha) = a^2 + db^2.$$

(ii) Gilt $(-d) \equiv 1 \mod 4$, $R = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})]$ und ist $\alpha = \frac{1}{2} + \frac{1}{2}b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$, $a \equiv b \mod 2$, dann ist

$$N(\alpha) = \tfrac{1}{4}a^2 + \tfrac{1}{4}db^2.$$

Sind α, β im Fall (i) oder (ii) jeweils Elemente des Rings R und gilt $\alpha \mid \beta$, dann ist $N(\alpha)$ ein Teiler von $N(\beta)$ im Ring $\mathbb{Z}$.

Definition der euklidischen Ringe

Definition (12.3)

Eine Höhenfunktion auf einem Integritätsbereich R ist eine Abbildung $h : R \setminus \{0_R\} \to \mathbb{N}$ mit der folgenden Eigenschaft: Sind $a, b \in R$, $b \neq 0_R$, dann gibt es Elemente $q, r \in R$, so dass die Gleichung

$$a \quad = \quad qb + r$$

erfüllt ist und außerdem entweder $r = 0_R$ oder $h(r) < h(b)$ gilt. Ein euklidischer Ring ist ein Integritätsbereich, auf dem eine Höhenfunktion existiert.

Beispiele für euklidische Ringe

Proposition (12.4)

(i) Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein euklidischer Ring, denn die Abbildung $h : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ gegeben durch $h(a) = |a|$ ist eine Höhenfunktion auf diesem Ring.

(ii) Sei K ein Körper. Dann ist der Polynomring $K[x]$ ein euklidischer Ring mit der Höhenfunktion gegeben durch die Gradabbildung, also $h(f) = \mathrm{grad}(f)$ für alle $f \in K[x] \setminus \{0_K\}$.

(iii) Der Ring $\mathbb{Z}[i]$ ist ein euklidischer Ring, wobei eine Höhenfunktion durch die auf $\mathbb{Z}[i] \setminus \{0\}$ eingeschränkte Normfunktion gegeben ist.

wichtiger Hinweis:
Die meisten quadratischen Zahlringe sind keine euklidischen Ringe, zum Beispiel $\mathbb{Z}[\sqrt{-3}]$ und $\mathbb{Z}[\sqrt{-5}]$ nicht.

Beweis von Proposition 12.4

zu ii) z.Zg.: $h : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$, $a \mapsto |a|$ ist eine Höhenfunktion auf $\mathbb{Z}$

Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$.

1. Fall: $b > 0$ Setze $q = \lfloor \frac{a}{b} \rfloor = \max\{s \in \mathbb{Z} \mid s \leq \frac{a}{b}\}$

Dann gilt $q \leq \frac{a}{b} < q+1$ (*). Setze $r = a - qb$.

Dann ist $a = qb + r$ erfüllt. Ang., $r \neq 0$

Aus (*) folgt $qb \leq a < (q+1)b \Rightarrow 0 \leq r < (q+1)b - qb$

$\Rightarrow 0 \leq r < b \Rightarrow h(r) = |r| = r < b = h(b)$

Aus (*) folgt $qb \leq a < (q+1)b \Rightarrow 0 \leq r < (q+1)b - qb$

2. Fall: $b < 0$ Setze $b_1 := -b \in \mathbb{N}$ s.o. $\Rightarrow$

$\exists\, q_1, r_1 \in \mathbb{Z}$ mit $a = q_1 b_1 + r_1$ mit $r_1 = 0$ oder $|r_1| < |b_1|$

$\Rightarrow a = qb + r$ mit $q := -q_1$, $r := r_1$, $r = 0$ oder $h(r) = |r|$

$= |r_1| < |b_1| = |b| = h(b)$

zu (ii) siehe Skript

zu (iii) Sei $R = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, $N : \mathbb{Z}[i] \to \mathbb{N}_0$,
$a + ib \mapsto a^2 + b^2$ (ist multiplikativ)

Seien $\alpha, \beta \in R$ mit $\beta \neq 0$ z.zg.: $\exists\, \gamma, \rho \in \mathbb{Z}[i]$ mit
$\alpha = \gamma\beta + \rho$ und $\rho = 0$ oder $N(\rho) < N(\beta)$

Seien $a, b, c, d \in \mathbb{Z}$ mit $\alpha = a + ib$, $\beta = c + id$ $(\beta \neq 0 \Rightarrow (c,d) \neq (0,0))$ $\Rightarrow \frac{\alpha}{\beta} = \frac{a+ib}{c+id} = \frac{(a+ib)(c-id)}{(c+id)(c-id)} =$

$$\frac{(ac+bd)+i(bc-ad)}{c^2+d^2} = r+si \quad \text{mit } r,s \in \mathbb{Q}.$$

$$r = \frac{ac+bd}{c^2+d^2}, \quad s = \frac{bc-ad}{c^2+d^2}$$ zu jedem $t \in \mathbb{R}$

gibt es ein $t_0 \in \mathbb{Z}$ mit $|t-t_0| \leq \frac{1}{2}$.

$\Rightarrow$ können $r_0, s_0 \in \mathbb{Z}$ wählen mit $|r-r_0| \leq \frac{1}{2}$,

$|s-s_0| \leq \frac{1}{2}$. Setze $\gamma = r_0 + s_0 i \in R$

und $\rho = \alpha - \gamma\beta$. $\Rightarrow \alpha = \gamma\beta + \rho$

Ang. $\rho \neq 0$. z.zg.: $N(\rho) < N(\beta)$

$$N\left(\frac{\rho}{\beta}\right) = N\left(\frac{\alpha-\gamma\beta}{\beta}\right) = N\left(\frac{\alpha}{\beta}-\gamma\right) =$$

$$N\left((r+is)-(r_0+is_0)\right) = (r-r_0)^2 + (s-s_0)^2$$

$\leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \Rightarrow N(\rho) = N\left(\frac{\rho}{\beta} \cdot \beta\right) =$

$|r - r_0| \leq \frac{1}{2}$

$|s - s_0| \leq \frac{1}{2}$

$N\left(\frac{\rho}{\beta}\right) N(\beta) \leq \frac{1}{2} N(\beta) < N(\beta)$ □