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 $f \in R[x] \setminus \{0_R\}$ 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.

Existenz und Eindeutigkeit bis auf Isomorphie

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 $\hat{\phi}(x) = a$.

Folgerung (11.24)

Je zwei Polynomringe über einem Ring R sind isomorph.

Satz (11.28)

Zu jedem Ring R existiert ein Polynomring über R.

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

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

und

$$\deg(fg) \leq \deg(f) + \deg(g).$$

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

$$\deg(fg) \quad = \quad \deg(f) + \deg(g)$$

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

Bem. Ist R kein Integritätsbereich, dann ist die Gleichung $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$ im Allgemeinen nicht erfüllt. Gegenbeispiel: $R = \mathbb{Z}/4\mathbb{Z}$.

$f = \bar{2}x + \bar{1}$, $g = \bar{2}x^2 + \bar{1}$. $\Rightarrow fg = (\bar{2}x+1)\cdot(\bar{2}x^2+\bar{1})$

$= \bar{4}x^3 + \bar{2}x^2 + \bar{2}x + \bar{1} = \bar{2}x^2 + \bar{2}x + \bar{1}$

$\Rightarrow \operatorname{grad}(f) + \operatorname{grad}(g) = 3$, $\operatorname{grad}(fg) = 2$

Beweis von Prop. 11.29 (nur teilweise)

geg.: Ring R, $f, g \in R[x]$ mit $fg \neq 0_R$

$(\Rightarrow f, g \neq 0_R)$

Schreibe f, g in der Form $f = \sum_{k=0}^{m} a_k x^k$,

$g = \sum_{l=0}^{n} b_l x^l$ mit $a_0, \dots, a_m \in R$, $b_0, \dots, b_n \in R$, $a_m \neq 0_R$,

$b_n \neq 0$ ($\rightarrow m = \operatorname{grad}(f)$, $n = \operatorname{grad}(g)$)

$\Rightarrow fg = \sum_{j=0}^{m+n} c_j x^j$ mit $c_j = \sum_{l=0}^{j} a_{j-l} b_l$

Sei $r = \max\{ j \mid 0 \leq j \leq m+n, c_j \neq 0_R \}$. Dann ist $r = \operatorname{grad}(fg)$, nach Def. des Grades. $\rightarrow \operatorname{grad}(fg) = r \leq m+n$

Setze nun voraus, dass R ein Integritätsbereich ist.

$a_m \neq 0_R$, $b_n \neq 0_R$ $\overset{R \text{ Int. B.}}{\Rightarrow}$ $c_{m+n} = a_m b_n \neq 0_R$

$\rightarrow r = m+n \rightarrow \operatorname{grad}(fg) = r = m+n = \operatorname{grad}(f) + \operatorname{grad}(g)$ □

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:

Sei R ein Integritätsbereich

Beh.: $R^\times = (R[x])^\times$

„$\subseteq$" Sei $c \in R^\times \Rightarrow \exists d \in R$ mit $c \cdot d = 1_R$

Wegen $R \subseteq R[x]$ liegen c, d beide auch in $R[x]$, und $c \cdot d = 1_R = 1_{R[x]} \Rightarrow c \in (R[x])^\times$

„$\supseteq$" Sei $f \in (R[x])^\times \Rightarrow \exists g \in R[x]$

mit $f \cdot g = 1_{R[x]} = 1_R$ R Int.-bereich

$\Rightarrow \operatorname{grad}(f) + \operatorname{grad}(g) = \operatorname{grad}(f \cdot g) =$

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

weg. $f, g \neq 0_R$

$\deg(f) = \deg(g) = 0 \Rightarrow f, g \in R$

$f \cdot g = 1_R \Rightarrow f \in R^\times$ □

Bem: Ist R kein Integritätsbereich ist, dann es in $R[x]$ nicht-konstante Einheiten geben

Bsp: $\bar{1} + \bar{2}x \in (\mathbb{Z}/4\mathbb{Z})[x]$

$(\bar{1} + \bar{2}x) \cdot (\bar{1} + \bar{2}x) = \bar{1} + \bar{4}x + \bar{4}x^2$

$= \bar{1} = 1_{(\mathbb{Z}/4\mathbb{Z})[x]}$

$\Rightarrow \bar{1} + \bar{2}x \in ((\mathbb{Z}/4\mathbb{Z})[x])^\times$

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 Prop. 12.4:

zu ii) Beh.: $h : \mathbb{Z} \setminus \{0\} \to \mathbb{N}, a \mapsto |a|$

ist eine Höhenfunktion auf dem Int.-b. $\mathbb{Z}$.

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

1. Fall: $b > 0$

(Erinnerung: untere Gaußklammer

$\lfloor r \rfloor = \max\{k \in \mathbb{Z} \mid k \leq r\}, r \in \mathbb{R}$)

Sei $q = \lfloor \frac{a}{b} \rfloor$ und $r = a - qb$.

$\Rightarrow a = qb + r$, außerdem: $q \leq \frac{a}{b} < q+1$

$\Rightarrow qb \leq a < qb + b \Rightarrow 0 \leq a - qb < b$

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

2 Fall: $b < 0$ Sei $b_1 = -b$. $(\Rightarrow b_1 > 0)$

s.o. $\Rightarrow \exists\, q_1, r_1 \in \mathbb{Z}$ mit $a = q_1 b_1 + r_1$

und $0 \leq r_1 < b_1$ Setze $q = -q_1$, $r = r_1$

$\Rightarrow a = (-q)\cdot(-b) + r = qb + r$

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

- Beweis von Prop 12.4 (Forts.)

zu (ii) siehe Skript

zu (iii) Beh: $h: \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}, \alpha \mapsto \alpha\bar{\alpha}$
ist eine Höhenfunktion auf $\mathbb{Z}[i]$

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

$\alpha, \beta \in \mathbb{Z}[i] \Rightarrow \exists a, b, c, d \in \mathbb{Z}$ mit $\alpha = a + ib$, $\beta = c + id$
wobei $(c, d) \neq (0, 0)$ wegen $\beta \neq 0$

$$\frac{\alpha}{\beta} = \frac{a+ib}{c+id} = \frac{(a+ib)(c-id)}{(c+id)(c-id)} = \frac{(ac+bd)+i(bc-ad)}{c^2+d^2}$$

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

Wähle $r_0, s_0 \in \mathbb{Z}$ so, dass $|r - r_0|, |s - s_0| \leq \frac{1}{2}$. Definiere dann $\gamma = r_0 + is_0 \in \mathbb{Z}[i]$ und $\rho = \alpha - \gamma\beta$. Es gilt dann $\alpha = \gamma\beta + \rho$, außerdem:

$$N\left(\frac{\rho}{\beta}\right) = N\left(\frac{\alpha}{\beta} - \gamma\right) = N(r + is - r_0 - is_0) = N\big((r - r_0) + i(s - s_0)\big) = (r - r_0)^2 + (s - s_0)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$$

Nehme jetzt an, dass $\rho \neq 0$ ist. Dann gilt

$$h(\rho) = N(\rho) = N\left(\frac{\rho}{\beta}\beta\right) = N\left(\frac{\rho}{\beta}\right) \cdot N(\beta) < N(\beta) = h(\beta)$$

($\uparrow$ $N\left(\frac{\rho}{\beta}\right) < 1$)

Anwendung: Nullstellen von Polynomen

Folgerung (12.5)

Sei K ein Körper und $0 \neq f \in K[x]$.

(i) Ist $a \in K$ eine Nullstelle von f, dann gilt $f = (x - a)g$ für ein Polynom $g \in K[x]$.

(ii) Ist $\mathrm{grad}(f) = n$ mit $n \in \mathbb{N}_0$, dann hat f höchstens n Nullstellen in K.

Wichtige Rechenregel für den ggT

Lemma (12.6)

Sei R ein Ring, und seien $a, b, q \in R$ mit $b \neq 0$. Dann gilt die Gleichung $\mathrm{ggT}(a, b) = \mathrm{ggT}(a - qb, b)$. Genauer ausformuliert bedeutet das: Ein Ringelement d ist genau dann ein größter gemeinsamer Teiler von a und b, wenn d ein größter gemeinsamer Teiler von $a - qb$ und b ist.

Der euklidische Algorithmus

Eingabe: ein euklidischer Ring R mit Höhenfunktion h
Elemente $a, b \in R$ mit $b \neq 0$

Ausgabe: Elemente $d, x, y \in R$ mit $d = \mathrm{ggT}(a, b)$ und $d = xa + yb$

Ablauf: (1) definiere $(a_1, x_1, y_1) = (a, 1, 0)$ und $(a_2, x_2, y_2) = (b, 0, 1)$
(2) Sei das Tupel (a_n, x_n, y_n) bereits definiert.
Wenn $a_n = 0$ ist,
dann setze $d = a_{n-1}$, $x = x_{n-1}$, $y = y_{n-1}$ und gib d, x, y als Ergebnis aus. (STOP)
Ansonsten
bestimme $q, r \in R$ mit
$a_{n-1} = qa_n + r$ und $r = 0$ oder $h(r) < h(a_n)$.
Definere $(a_{n+1}, x_{n+1}, y_{n+1}) = (r, x_{n-1} - qx_n, y_{n-1} - qy_n)$.
Wiederhole Schritt 2.

Beispiel für die Anwendung des Euklidischen Algorithmus

ggT: ggT(a, b) für $a = 98$, $b = 47$

q	a_n	x_n	y_n
–	98	1	0
–	47	0	1
2	4	1	−2
11	3	−11	23
1	1	12	−25
3	0	–	–

$98 - 2 \cdot 47 = 4$

$1 - q \cdot 0 = 1$

$0 - q \cdot 1 = -2$

Ergebnis:

$ggT(98, 47) = 1$

$= 12 \cdot 98 - 25 \cdot 47$

$1176 - 1175$

Korrektheit des euklidischen Algorithmus

Satz (12.7)

Sei R ein euklidischer Ring mit Höhenfunktion h. Der euklidische Algorithmus hält für jedes Paar (a, b) mit $a, b \in R$ und $b \neq 0$ nach einer endlichen Zahl von Wiederholungen. Er liefert als Ausgabe tatsächlich $d = \mathrm{ggT}(a, b)$ und Ringelemente $x, y \in R$ mit $d = xa + yb$.

- Wenn die Schleife im Algorithmus unendlich oft durchlaufen würde, dann wäre $h(a_1) > h(a_2) > h(a_3) > \ldots$ eine unendliche absteigende Folge in $\mathbb{N}$. Aber eine solche Folge gibt es nicht.

Korrektheit des euklidischen Algorithmus (Forts.)

- Mit Hilfe von Lemma 12.6 ist leicht zu sehen, dass $\mathrm{ggT}(a, b) = \mathrm{ggT}(a_1, a_2) = \mathrm{ggT}(a_2, a_3) = \ldots = \mathrm{ggT}(a_{n-1}, a_n) = \mathrm{ggT}(a_{n-1}, 0_R) = a_{n-1}$ gilt, dass im n-ten Schritt die Abbruchbedingung $a_n = 0_R$ erfüllt ist. Dies zeigt, dass der korrekte ggT ausgegeben wird.

- Durch vollständige Induktion zeigt man leicht, dass $a_k = x_k a + y_k b$ für $1 \leq k \leq n-1$ gilt. Insbesondere ist damit $d = a_{n-1} = x_{n-1} a + y_{n-1} b = xa + yb$ erfüllt.

Euklidische Ringe sind Hauptidealringe

Erinnerung:
Ein Hauptidealring ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.

Satz (12.8)

Jeder euklidische Ring R ist ein Hauptidealring.

Also sind insbesondere $\mathbb{Z}$, $\mathbb{Z}[i]$ und Polynomringe über Körpern Hauptidealringe.

Beweis von Satz 12.8:

geg.: euklidischer Ring R mit Höhenfkt. h

z.zg.: R ist Hauptidealring

Nach Def. ist R ein Integritätsbereich.

noch z.zg.: Jedes Ideal in R ist ein Hauptideal.

Sei also I ein Ideal in R, o.B.d.A. $I \neq (0)$.

Wähle $a \in I \setminus \{0\}$ so, dass $h(a) \in \mathbb{N}$ unter all diesen Elementen minimal ist.

Beh: $I = (a)$ ($\Rightarrow I$ ist Hauptideal)

„$\supseteq$" Aus $a \in I$ folgt $(a) \subseteq I$.

Sei $b \in I$. Ang. $b \notin (a)$. Division von b durch a mit Rest liefert $q, r \in R$ mit $b = qa + r$, wobei $r = 0$ oder $h(r) < h(a)$ gilt.

1. Fall: $r = 0 \Rightarrow b = qa \in (a)$ ↯ zur Annahme

2. Fall: $r \neq 0$, $h(r) < h(a)$

Es ist $r = b - qa \overset{\substack{b \in I \\ a \subset I}}{\Rightarrow} r \in I$

also: $r \in I \setminus \{0\}$, $h(r) < h(a)$ ↯ zur Minimalität von $h(a)$

□