Übertragung von Verknüpfungen

Lemma (11.14)

Seien X und Y Mengen, $\phi : Y \to X$ eine Bijektion und $\cdot$ eine Verknüpfung auf X. Wir definieren auf Y eine Vernüpfung $\odot$, indem wir $a \odot b = \phi^{-1}(\phi(a) \cdot \phi(b))$ für alle $a, b \in Y$ definieren. Die neue Verknüpfung $\odot$ hängt dann mit $\cdot$ auf folgende Weise zusammen.

(i) Ist die Verknüpfung $\cdot$ auf X assoziativ bzw. kommutativ, dann gilt dasselbe jeweils für die Verknüpfung $\odot$ auf Y.

(ii) Ist $e_X \in X$ ein Neutralelement in X bezüglich $\cdot$, dann ist $e_Y = \phi^{-1}(e_X)$ ein Neutralelement in Y bezüglich $\odot$.

(iii) Seien e_X und e_Y wie in (ii) und $a, b \in X$. Ist b ein Inverses von a bezüglich $\cdot$, dann ist $\phi^{-1}(b)$ ein Inverses von $\phi^{-1}(a)$ bezüglich $\odot$.

Übertragung einer Ringstruktur

Satz (11.15)

Sei $(R, +, \cdot)$ ein Ring, S eine Menge und $\phi : S \to R$ eine bijektive Abbildung. Seien die Verknüpfungen $\oplus$ und $\odot$ auf S definiert durch

$$a \oplus b = \phi^{-1}(\phi(a) + \phi(b)) \qquad \text{und} \qquad a \odot b = \phi^{-1}(\phi(a) \cdot \phi(b)).$$

Dann ist $(S, \oplus, \odot)$ ein Ring, und ϕ ist ein Isomorphismus von Ringen.

Konstruktion von Ringerweiterungen

Satz (11.16)

Sei $\phi : R \to S$ ein Monomorphismus von Ringen. Dann gibt es einen Erweiterungsring $\hat{R} \supseteq R$ und einen Isomorphismus $\hat{\phi} : \hat{R} \to S$ mit $\hat{\phi}|_R = \phi$.

Anwendung:

Konstruktion des Körpers $\mathbb{C}$ der komplexen Zahlen

Konstruktion der komplexen Zahlen

$f = x^2 + 1 \in \mathbb{R}[x]$, $I = (f)$, $\mathbb{C} = \mathbb{R}[x]/I$

$i = x + I$ Erinnerung: $i^2 = -1_{\mathbb{C}}$

Beh: $\phi : \mathbb{R} \to \mathbb{C}$, $a \mapsto a + I$ ist ein Monomorphismus von Ringen

Homomorphismus-Eigenschaft: liegt vor, denn ϕ ist die Komposition des Einbettungshom. $\mathbb{R} \to \mathbb{R}[x]$, $a \mapsto a$ und des kan. Epimorphismus $\pi : \mathbb{R}[x] \to \mathbb{R}[x]/I = \mathbb{C}$, $g \mapsto g + I$

Injektivität: Sei $a \in \ker(\phi) \Rightarrow \phi(a) = 0_{\mathbb{C}} \Rightarrow$

Homomorphismus-Eigenschaft: liegt vor, denn ϕ ist

$$a + I = 0 + I \Rightarrow a \in I \Rightarrow a \in (f) \Rightarrow f \mid a$$

Da f vom Grad 2 und a konstant ist, ist das nur für $a = 0$ möglich ($\Rightarrow$ Beh.)

Satz 11.16 $\Rightarrow$ Es gibt einen Erw.-ring $\mathbb{C} \supseteq \mathbb{R}$ und einen Isomorphismus $\hat{\phi} : \mathbb{C} \xrightarrow{\sim} \underline{C}$ mit $\hat{\phi}|_{\mathbb{R}} = \phi$.

Sei $i = \hat{\phi}^{-1}(\underline{i})$. Es gilt $i^2 = -1$, denn:

$$\hat{\phi}(i^2) = \hat{\phi}(i)^2 = \underline{i}^2 = -1_{\underline{C}} = -1 + I = \phi(-1) \overset{\hat{\phi}|_{\mathbb{R}} = \phi}{=} \hat{\phi}(-1)$$

Da $\hat{\phi}$ injektiv ist, folgt $i^2 = -1$.

Jedes $z \in \mathbb{C}$ besitzt eine Darstellung $a + ib$ mit $a, b \in \mathbb{R}$, denn:

$\hat{\phi}(z) \in \underline{C}$, $\underline{C} = \mathbb{R}[x]/I \Rightarrow \exists\, a, b \in \mathbb{R}$ mit $\hat{\phi}(z) = a + bx + I$

$= \phi(a) + \phi(b)(x + I) = \hat{\phi}(a) + \hat{\phi}(b)\,\underline{i} = \hat{\phi}(a) + \hat{\phi}(b)\,\hat{\phi}(i)$

$= \hat{\phi}(a + ib)$ $\quad \hat{\phi}$ injektiv $\Rightarrow z = a + ib$ $\quad \square$

Definition der Quotientenkörper

Definition (11.17)

Sei R ein Integritätsbereich. Ein Erweiterungsring $K \supseteq R$ wird Quotientenkörper von R genannt, wenn K ein Körper ist und

$$K = \{ab^{-1} \mid a, b \in R\ ,\ \ b \neq 0_R\} \qquad \text{gilt.}$$

Beispielsweise ist $\mathbb{Q}$ ein Quotientenkörper von $\mathbb{Z}$.

Rechenregeln für Brüche

$$\frac{a}{b} = \frac{c}{d} \quad (a, c \in \mathbb{Z},\ b, d \in \mathbb{Z} \setminus \{0\}) \iff ad = bc$$

Addition: $\frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad + bc}{bd}$

Multiplikation: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

Negative: $-\frac{a}{b} = \frac{(-a)}{b}$

Konstruktion des Quotientenkörpers

Wir definieren auf der Menge $X_R = R \times (R \setminus \{0_R\})$ eine Relation $\sim$ durch die Festlegung

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc$$

für alle $(a, b), (c, d) \in X_R$.

Lemma (11.18)

Die Relation $\sim$ ist eine Äquivalenzrelation auf $R \times (R \setminus \{0_R\})$.

Konstruktion des Quotientenkörpers (Forts.)

Proposition (11.19)

Auf der Menge $\hat{R} = X_R/\sim$ gibt es eindeutig bestimmte Verknüpfungen $\oplus$ und $\odot$ mit

$$[a,b] \oplus [c,d] = [ad + bc, bd] \qquad \text{und} \qquad [a,b] \odot [c,d] = [ac, bd]$$

für alle $(a,b),(c,d) \in X_R$, und $\hat{R}$ bildet mit diesen Verknüpfungen einen Körper.

Existenz und Eindeutigkeit des Quotientenkörpers

Satz (11.20)

Zu jedem Integritätsbereich existiert ein Quotientenkörper.

Satz (11.21)

Sei R ein Integritätsbereich, und seien K und L beides Quotientenkörper von R. Dann existiert ein Isomorphismus $\psi : K \to L$ von Körper mit $\psi|_R = \mathrm{id}_R$.

Beweis von Satz 11.20

geg. Integritätsbereich R, z.zg.:

Es existiert ein Quotientenkörper $K \supseteq R$.

Sei $\hat{R} = P_R / \sim$ mit $P_R = R \times (R \setminus \{0_R\})$

und $(a,b) \sim (c,d) \Leftrightarrow ad = bc$,

und seien $\oplus$ und $\odot$ die Verknüpfungen

aus Prop. 11.19. dort gezeigt:

$(\hat{R}, \oplus, \odot)$ ist ein Ring

<u>Beh.</u>: $\phi : R \to \hat{R}$, $a \mapsto [a, 1_R]$

ist ein Monomorphismus von Ringen

Homomorphismus-Eig.: $\phi(1_R) = [1_R, 1_R] = 1_{\hat{R}}$

Seien $a, b \in R$. $\phi(a+b) = [a+b, 1_R]$, andererseits $\phi(a) \oplus \phi(b) = [a, 1_R] \oplus [b, 1_R] =$

$[a \cdot 1_R + 1_R \cdot b, 1_R \cdot 1_R] = [a+b, 1_R]$.

$\Rightarrow \phi(a+b) = \phi(a) \oplus \phi(b)$

$\phi(ab) = [ab, 1_R] = [ab, 1_R \cdot 1_R] = [a, 1_R] \odot [b, 1_R]$

$= \phi(a) \odot \phi(b)$

Injektivität: Sei $a \in \ker(\phi) \Rightarrow \phi(a) = 0_{\hat{R}}$

$\Rightarrow [a, 1_R] = [0_R, 1_R] \Rightarrow (a, 1_R) \sim (0_R, 1_R)$

$\Rightarrow a \cdot 1_R = 1_R \cdot 0_R \Rightarrow a = 0_R$ $\quad$ ($\Rightarrow$ Beh.)

Satz 11.16 $\Rightarrow$ Es gibt einen Erweiterungsring $K \supseteq R$ und einen Isom. $\hat{\phi}: K \to \hat{R}$ von Ringen

R.

${}_R\})$

en

gen

mit $\hat{\phi}|_R = \phi$. Da $\hat{R}$ ein Körper und $\hat{\phi}$ ein Isomorphismus von Ringen ist, ist auch K ein Körper. Noch z.zg.: $K = \{a \cdot b^{-1} \mid a \in R, b \in R \setminus \{0\}\}$

„$\supseteq$" offensichtlich, da R Teilring von K

„$\subseteq$" Sei $\alpha \in K$. $\Rightarrow \hat{\phi}(\alpha) \in R \Rightarrow \exists a \in R$ und $b \in R \setminus \{0\}$ mit $\hat{\phi}(\alpha) = [a, b] =$

$[a, 1_R] \odot [1_R, b] = [a, 1_R] \odot [b, 1_R]^{-1} =$

$\phi(a) \cdot \phi(b)^{-1} = \hat{\phi}(a) \cdot \hat{\phi}(b)^{-1} = \hat{\phi}(a b^{-1})$

Injektivität $\Rightarrow \alpha = a b^{-1}$. $\square$

Beweis von Satz 11.21 (Skizze)

geg.: Integritätsbereich R, K, L beides Quotientenkörper von R

Beh.: $\exists$ Isom. $\psi : K \to L$ mit $\psi|_R = id_R$

überprüfe: $\exists$ Abb. $\varphi : \hat{R} \to K$ mit

$\varphi([a,b]) = a \cdot b^{-1}$ in K

ebenso: $\exists$ Abb. $\varphi_1 : \hat{R} \to L$ mit

$\varphi_1([a,b]) = a \cdot b^{-1}$ in L

Man kann zeigen, dass K und L Ringisomorphismen sind. Sei $\psi : K \to L$ geg. durch $\psi = \varphi_1 \circ \varphi^{-1}$. Für alle $a \in R$ gilt $\psi(a) =$

$(\varphi_1 \circ \varphi^{-1})(a \cdot 1_R^{-1}) = \varphi_1([a, 1_R]) = a\, 1_R^{-1}$

$= a$. Damit ist $\psi|_R = \mathrm{id}_R$ nachgewiesen. $\square$

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.

Ergänzungen zur Definition

- Das ausgezeichnete Elemente x nennt man die Variable (oder Unbestimmte) des Polynomrings.
- Für einen Polynomring S über einem Ring R mit der Variablen x wird in der Regel die Bezeichnung $R[x]$ verwendet.
- Die Elemente von $R[x]$ heißen Polynome übe dem Ring R.
- Man bezeichnet die Zahl n in der Definition als den Grad $\deg(f)$ des Polynoms f.
- Das Polynom $a_n x^n$ ist der Leitterm, das Element $a_n \in R$ der Leitkoeffizient von f.

wichtiger Hinweis: Das Element x im Polynomring $R[x]$ ist kein Element des Rings R.

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

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

Beh.: Es gibt einen eindeutig bestimmten Ringhom. $\hat{\phi}$:
$R[x] \to S$ mit $\hat{\phi}(x) = a$ und $\hat{\phi}|_R = \phi$.

Existenz: Sei $f \in R[x]$. Ist $f = 0_R = 0_{R[x]}$, dann
definiere $\hat{\phi}(f) = 0_S$. Ansonsten gibt es eind. bestimmte
$n \in \mathbb{N}_0$, $a_0, \dots, a_n \in R$ mit $a_n \neq 0_R$ und $f = \sum_{k=0}^{n} a_k x^k$.
Definiere dann $\hat{\phi}(f) = \sum_{k=0}^{n} \phi(a_k) a^k$. Überprüfe nun:
$\hat{\phi}$ ist Ringhom mit $\hat{\phi}|_R = \phi$ und $\hat{\phi}(x) = a$. (siehe Skript)

Eindeutigkeit: Ang. $\psi : R[x]$ ist ein weiterer Ringhom
mit diesen Eigenschaften. Sei $f \in R[x]$. z.zg. $\hat{\phi}(f) = \psi(f)$

1. Fall: $f = 0_R$ Dann gilt $\psi(f) = \psi(0_R)$

$= 0_S = \hat{\phi}(0_R) = \hat{\phi}(f)$

$\uparrow$ ψ Ringhom.

2. Fall: $f \neq 0_R \Rightarrow \exists$ eindeutige $n \in \mathbb{N}_0$, $a_0, \dots, a_n$

$\in R$ mit $a_n \neq 0_R$ und $f = \sum_{k=0}^{n} a_k x^k \Rightarrow$

$$\psi(f) = \psi\left(\sum_{k=0}^{n} a_k x^k\right) \underset{\uparrow \psi \text{ Ringh.}}{=} \sum_{k=0}^{n} \psi(a_k x^k)$$

$$= \sum_{k=0}^{n} \psi(a_k)\psi(x)^k \underset{\substack{\uparrow \psi(x) = a \\ \psi|_R = \phi}}{=} \sum_{k=0}^{n} \phi(a_k) a^k$$

$$= \hat{\phi}(f) \qquad \square$$

Beweis von Satz 11.24:

geg: Ring R, S, S' seien Polynomringe über R mit Unbekannten $x \in S$, $x' \in S'$

z.zg.: S und S' sind isomorph

Satz 11.23 (universelle Eig.) $\Rightarrow$ Es gibt einen eind. best. Ringhom. $\phi : S \to S'$ mit $\phi|_R = id_R$ und $\phi(x) = x'$

ebenso: Es gibt einen eind. best. Ringhom $\psi : S' \to S$ mit $\psi|_R = id_R$ und $\psi(x') = x$

$\Rightarrow$ $\psi \circ \phi$ ist ein Ringhom. $S \to S$ mit $(\psi \circ \phi)(x) = \psi(x') = x$ Auf Grund der

Eindeutigkeit in Satz 11.23 folgt daraus

$\psi \circ \phi = \mathrm{id}_S$! ebenso: $\phi \circ \psi = \mathrm{id}_{S'}$

Also sind ϕ und ψ zueinander inverse Ringisomorphismen. $\square$

Rechnen mit Polynomen

geg.: Ring R, $f, g \in R[x]$,

$$f = \sum_{k=0}^{m} a_k x^k, \quad g = \sum_{l=0}^{n} b_l x^l$$

Setze $a_k = 0_R$ für $k > m$, $b_l = 0_R$ für $l > n$.

Addition: $f + g = \sum_{k \in \mathbb{N}_0} (a_k + b_k) x^k$

Multiplikation: $f \cdot g = \sum_{l=0}^{m+n} c_l x^l$ mit

$$c_l = \sum_{\substack{(i,j) \\ i+j=l}} a_i b_j = \sum_{j=0}^{l} a_{l-j} b_j$$

Konstruktion der Polynomringe

- Sei P_R die Menge aller Abbildungen $f : \mathbb{N}_0 \to R$ mit der Eigenschaft, dass $f(k) = 0_R$ für alle bis auf endlich viele $k \in \mathbb{N}_0$.
- Auf der Menge P_R definieren wir eine Verknüpfung $\oplus$ durch

  $$(f \oplus g)(n) \quad = \quad f(n) + g(n).$$

  Ebenso definieren wir eine Verknüpfung $\odot$ durch

  $$(f \odot g)(n) = \sum_{k=0}^{n} f(n-k)g(k) = \sum_{k+\ell=n} f(\ell)g(k).$$

- Für jedes $a \in R$ sei $\tilde{a} \in P_R$ das Element gegeben durch $\tilde{a}(0) = a$ und $\tilde{a}(n) = 0_R$ für alle $n \geq 1$.
- Außerdem definieren wir ein Element $\tilde{x} \in P_R$ durch $\tilde{x}(1) = 1_R$ und $\tilde{x}(n) = 0_R$ für $n \neq 1$.

Lemma (11.25)

Das Tripel $(P_R, \oplus, \odot)$ ist ein Ring, mit $\tilde{0}$ als Null- und $\tilde{1}$ als Einselement.

Lemma (11.26)

Sei $a \in R$ und $m \in \mathbb{N}_0$. Dann gilt $(\tilde{a} \odot \tilde{x}^m)(m) = a$, und $(\tilde{a} \odot \tilde{x}^m)(n) = 0_R$ für alle $n \in \mathbb{N}_0 \setminus \{m\}$.

Konstruktion der Polynomringe (Forts.)

Lemma (11.27)

Für jedes $f \in P_R \setminus \{\tilde{0}\}$ gibt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte $a_0, a_1, ..., a_n \in R$, so dass $a_n \neq 0_R$ und

$$f \quad = \quad (\tilde{a}_n \odot \tilde{x}^n) \oplus \; ... \; \oplus \tilde{(}a_1 \odot \tilde{x}) \oplus \tilde{a}_0 \qquad \text{gilt.}$$

Satz (11.28)

Zu jedem Ring R existiert ein Polynomring über R.