Übertragung einer Verknüpfung auf eine andere Menge

Lemma (6.1)

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 auf eine Menge

Satz (6.2)

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.

Die Konstruktion von Ringerweiterungen

Satz (6.3)

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 $\hat{\phi}|_R = \phi$.

Beweis von Satz 6.3:

geg: Monomorphismus $\phi : R \to S$ von Ringen

z.zg: 1 Ringerweiterung $\hat{R} \mid R$ und einen Isom. $\hat{\phi} : \hat{R} \to S$ mit $\hat{\phi}|_R = \phi$

Definiere $\hat{R} = R \cup (S \setminus \phi(R))$ $(\to \hat{R} \supseteq R)$

allgemein gilt: A, B, C, D Mengen mit $A \cap B = C \cap D = \emptyset$ und sind $\phi_1 : A \to C$, $\phi_2 : B \to D$ Bijektionen, dann ist $\psi : A \cup B \to C \cup D$, $x \mapsto \begin{cases} \phi_1(x) & \text{falls } x \in A \\ \phi_2(x) & \text{falls } x \in B \end{cases}$ ebenfalls eine Bijektion (Übung)

Wende dies an auf $R = A$, $B = D = S \setminus \phi(R)$, $C = \phi(R)$ sowie die Bij. $\phi_1 := \phi$, $\phi_2 = id_{S \setminus \phi(R)}$ an, um eine Bijektion $\hat{\phi} : \hat{R} \to S$ zu erhalten. Wende nun Satz 6.2 an, um auf $\hat{R}$ eine Ringstruktur zu definieren. Die Abb. $\hat{\phi}$ wird dann zu einem Ringisom.

Nach Def. von $\hat{\phi}$ gilt $\hat{\phi}|_R = \phi$. □

Anwendung von Satz 6.3:
Konstruktion der komplexen Zahlen

Erinnerung: Beispiel aus §5

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

gezeigt: (1) Das Element $i = x + I$ erfüllt $i^2 = -1_C$.

(2) Jedes Element aus C hat eine eind. Darstellung $[a] + i[b]$ mit $a, b \in \mathbb{R}$, wobei $[a] = a + I$, $[b] = b + I$

Anwendung von Satz 6.3 liefert eine Ring-
erweiterung $\mathbb{C} | \mathbb{R}$ und einen Isom. $\hat{\phi} : \mathbb{C} \to C$
mit $\hat{\phi}_{|\mathbb{R}} = \phi$, wobei $\phi : \mathbb{R} \to C, \ a \mapsto [a]$.
(leicht zu überprüfen: ϕ ist ein Monomorphismus von Ringen)

(Injektivität: Sei $a \in \mathbb{R}$ mit $\phi(a) = 0_C \Rightarrow$
$a + I = I \Rightarrow a \in I \Rightarrow a \in (x^2 + 1)$
$\Rightarrow x^2 + 1$ ist Teiler von a in $\mathbb{R}[x] \Rightarrow a = 0$)

Beh.: (1) Jedes $z \in \mathbb{C}$ hat eine eind. Darst.
$a + ib$ mit $a, b \in \mathbb{R}$, wobei $i = \hat{\phi}^{-1}(\underset{x+I}{\underset{\shortparallel}{i}})$

(2) $i^2 = -1$

zu (1) Sei $z \in \mathbb{C}$. Existenz:

$\hat{\phi}(z) \in \mathbb{C} \Rightarrow \exists a, b \in \mathbb{R}$ mit $\hat{\phi}(z) = [a] + i[b]$

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

$= \hat{\phi}(a + ib) \overset{\hat{\phi} \text{ Bij}}{\Longrightarrow} z = a + ib$

Eindeutigkeit: Seien $a, b, c, d \in \mathbb{R}$ mit

$a + ib = z = c + id \Rightarrow \hat{\phi}(a + ib) = \hat{\phi}(c + id)$

$\Rightarrow [a] + i[b] = [c] + i[d] \overset{\text{Eind. der Darst. in } \mathbb{C}}{\longrightarrow} a = c, b = d$

zu (2) $\hat{\phi}(i^2) = \hat{\phi}(i)^2 = i^2 = -1_{\mathbb{C}} =$

$\hat{\phi}(-1) \overset{\hat{\phi} \text{ Bij}}{\Longrightarrow} i^2 = -1$ □

Definition der Quotientenkörper

Definition (6.4)

Sei R ein Integritätsbereich. Ein Erweiterungsring $K \supseteq R$ wird Quotientenkörper von R genannt, wenn K ein Körper ist und $K = \{ab^{-1} \mid a, b \in R \ , \ b \neq 0_R\}$ gilt.

Beispiel:

Der Körper $\mathbb{Q}$ der rationalen Zahlen ein Quotientenkörper von $\mathbb{Z}$.

Erinnerung. Def. des rationalen Zahlen

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0 \right\}$$

$$\frac{a}{b} = \frac{c}{d} \longleftrightarrow ad = bc$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Konstruktion der Quotientenkörper

Notation:

- Sei R ein Integritätsbereich.
- $X_R = R \times (R \setminus \{0_R\})$
- Definition einer Relation $\sim$ auf X_R durch

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

Lemma (6.5)

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

Konstruktion der Quotientenkörper (Forts.)

Proposition (6.6)

Auf der Menge $\hat{R} = X_R/\sim$ der Äquivalenzklassen der Relation $\sim$ auf X_R 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.

Satz (6.7)

Zu jedem Integritätsbereich existiert ein Quotientenkörper.

Eindeutigkeit der Quotientenkörper

Satz (6.8)

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

Definition der Polynomringe

Definition (6.9)

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.

Polynome über einem Ring R

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

mit $a_0, a_1, \dots, a_{n-1}, a_n \in R \quad (x \notin R)$

Idee: Betrachte das Pol. f als Abbildung

$$\mathbb{N}_0 \to R, \; k \mapsto \begin{cases} a_k & \text{falls } 0 \le k \le n \\ 0_R & \text{sonst} \end{cases}$$

Addition von Polynomen

$$\sum_{r \in \mathbb{N}_0} a_r x^r + \sum_{r \in \mathbb{N}_0} b_r x^r = \sum_{r \in \mathbb{N}_0} (a_r + b_r) x^r$$

Multiplikation von Polynomen

$$\left(\sum_{r=0}^{m} a_r x^r\right) \cdot \left(\sum_{s=0}^{n} b_s x^s\right) = \sum_{r \in \mathbb{N}_0} \left(\sum_{\substack{(k,l) \\ k+l=r}} a_k b_l\right) x^r$$

$$= \sum_{r \in \mathbb{N}_0} \left(\sum_{k=0}^{r} a_{r-k} b_k\right) x^r$$

Universelle Eigenschaft des Polynomrings

Satz (6.10)

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 6.10 als den Auswertungshomomorphismus an der Stelle a.

Folgerung (6.11)

Je zwei Polynomringe über einem Ring R sind isomorph.

Beweis von Satz 6.10 (nur Skizze)

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

z.zg.: $\exists!\, \hat{\phi} : R[x] \to S$ mit

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

Existenz. Sei $f \in R[x]$.

1. Fall: $f = 0_R$ $\to$ setze $\hat{\phi}(0_R) = 0_S$

2. Fall: $f \neq 0_R$ $\to$ $\exists$ eind. Darst.

$f = \sum_{k=0}^{n} a_k x^k$ mit $n \in \mathbb{N}_0$, $a_0, \ldots, a_n \in R$

und $a_n \neq 0_R \Rightarrow$ Setze

$$\hat{\phi}(f) = \sum_{k=0}^{n} \phi(a_k)\, a^k$$

Überprüfe, dass die so definierte Abb. $\hat{\phi}$: $R[x] \to S$ ein Ringhom. mit $\hat{\phi}|_R = \phi$ und $\hat{\phi}(x) = a$ ist.

<u>Eindeutigkeit</u>: Sei $\Psi : R[x] \to S$ mit den angeg. Eigenschaften. Sei $f \in R[x]$.

z.zg: $\Psi(f) = \hat{\phi}(f)$

<u>1. Fall</u>: $f = 0_R \to \Psi(0_R) = 0_S = \hat{\phi}(0_R)$

↑ Ψ Ringhom

zze)

$a \in S$

ut

.

$0_R) = 0_S$

Dass.

$a_0, \dots, a_n \in R$

2. Fall. $f \neq 0_R$. $f = \sum_{k=0}^{n} a_k x^k$ wie oben.

$$\psi(f) = \psi\left(\sum_{k=0}^{n} a_k x^k\right) = \sum_{k=0}^{n} \psi(a_k x^k)$$

$$= \sum_{k=0}^{n} \psi(a_k)\psi(x)^k = \sum_{k=0}^{n} \phi(a_k) a^k = \hat{\phi}(f) \quad \square$$

$\psi|_R = \phi$

$\psi(x) = a$

Konstruktion der Polynomringe

Notation:

- P_R = Menge der Abbildungen $f : \mathbb{N}_0 \to R$ mit $f(k) = 0_R$ für alle bis auf endlich viele $k \in \mathbb{N}_0$
- Definition der Addition auf P_R

$$(f \oplus g)(n) \;=\; f(n) + g(n)$$

- Definition der Multiplikation auf P_R

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

- Für jedes $a \in R$ definiere $\tilde{a} \in P_R$ durch $\tilde{a}(0) = a$ und $\tilde{a}(n) = 0_R$ für alle $n \geq 1$.
- Definiere $\tilde{x} \in P_R$ durch $\tilde{x}(1) = 1_R$ und $\tilde{x}(n) = 0_R$ für $n \neq 1$.

Konstruktion der Polynomringe (Forts.)

Lemma (6.12)

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

Lemma (6.13)

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 $n \in \mathbb{N}_0 \setminus \{m\}$.

Lemma (6.14)

Für jedes $f \in P_R \setminus \{\tilde{0}\}$ gilt 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

$$f = (\tilde{a}_n \odot \tilde{x}^n) \oplus \ ... \ \oplus (\tilde{a}_1 \odot \tilde{x}) \oplus \tilde{a}_0 \qquad \text{gilt.}$$

Existenz der Polynomringe

Satz (6.15)

Zu jedem Ring R existiert ein Polynomring über R.

Rechenregeln für den Polynomgrad

Proposition (6.16)

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

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

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

Anmerkung zu Prop. 6.16:

Ist R kein Integritätsbereich, dann gilt im Allg. nur $\operatorname{grad}(fg) \leq \operatorname{grad}(f) + \operatorname{grad}(g)$, keine Gleichheit!

Bsp: $R = \mathbb{Z}/4\mathbb{Z}$, $f = \bar{2}x + \bar{1}$, $g = \bar{2}x^2 + \bar{1}$ $\in \mathbb{Z}/4\mathbb{Z}[x]$ $\Rightarrow$

$$f \cdot g = (\bar{2}x + \bar{1}) \cdot (\bar{2}x^2 + \bar{1}) = \bar{2}x \cdot (\bar{2}x^2 + \bar{1}) + \bar{1} \cdot \bar{2}x^2 + \bar{1} = \bar{4}x^3 + \bar{2}x + \bar{2}x^2 + \bar{1}$$

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

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

Die Einheitengruppe der Polynomringe

Folgerung (6.17)

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 6.17

geg.: Integritätsbereich R

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

„$\supseteq$" Sei $r \in R^\times \Rightarrow r \in R[x]$

$r \in R^\times \Rightarrow \exists\, s \in R^\times$ mit $r\,s = 1_R \overset{s \in R[x]}{\Longrightarrow}$

$\exists\, s \in R[x]$ mit $r \cdot s = 1_R = 1_{R[x]} \Rightarrow r \in (R[x])^\times$

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

$f \cdot g = 1_{R[x]} = 1_R \Rightarrow \operatorname{grad}(f \cdot g) = \operatorname{grad}(1_R) = 0$

R Int-b $\Rightarrow$ $\operatorname{grad}(f) + \operatorname{grad}(g) = 0 \Rightarrow \operatorname{grad}(f) = 0$

$\operatorname{grad}(g), \operatorname{grad}(f) \geq 0$

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

Anmerkung: Ist R kein Integritätsbereich, dann kann es in $R[x]$ nicht-konstante Einheiten geben.

Bsp: $R = \mathbb{Z}/4\mathbb{Z}$ $f = \bar{2}x + \bar{1}$

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

$\Rightarrow f \in (\mathbb{Z}/4\mathbb{Z}[x])^\times$