

Wiederholung. $(R, 0, 1, +, \cdot)$ ist ein **Ring** $\iff (R, 0, +)$ ist eine Gruppe, $(R, 1, \cdot)$ ist ein Monoid und es gelten die Distributivgesetze.

$$R^\times = \{r \in R \mid \exists s \in R : rs = sr = 1\}$$

ist die Einheitengruppe von R

Beispiel. (Übung) $\mathbb{Z}_n^\times = \{\bar{a} \mid \text{ggT}(a, n) = 1\}$, wobei $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(n)$

Definition 0.1 (Ringhomomorphismus). Seien R, R' Ringe, eine Abbildung $\varphi : R \rightarrow R'$ heißt Ringhomomorphismus wenn:

- $\varphi : (R, 0, +) \rightarrow (R', 0', +')$ ist ein Gruppenhomomorphismus.
- $\varphi : (R, 1, \cdot) \rightarrow (R', 1', \cdot')$ ist ein Monoidhomomorphismus.

φ ist ein Ringisomorphismus $\iff \varphi$ ist bijektiver Ringhomomorphismus $\xLeftrightarrow{\text{Übung}}$

$\exists \varphi' : R' \xrightarrow{\text{Ringhom.}} R$, sodass $\varphi \circ \varphi' = \text{id}_{R'}$ und $\varphi' \circ \varphi = \text{id}_R$. In diesem Fall schreibe $R \cong R'$ (R isomorph zu R').

Beispiel. R heißt Nullring $\iff 0_R = 1_R \xLeftrightarrow{\text{Übung}} R = \{0_R\}$ (alle Nullringe sind isomorph.)

Beispiel. (Übung) Sei R beliebig $\implies \exists!$ Ringhomomorphismus $\varphi : \mathbb{Z} \rightarrow R$ nämlich

$$\varphi : \mathbb{Z} \rightarrow R, n \mapsto \varphi(n) = n \cdot 1_R$$

(wegen $\varphi(1) = 1_R$)

Definition 0.2 (Unterring). $S \subseteq R$ heißt Unterring, falls

- $1 \in S$
- $S - S = \{s_1 - s_2 \mid s_1, s_2 \in S\} \subseteq S$
- $S + S = \{s_1 + s_2 \mid s_1, s_2 \in S\} \subseteq S$

Definition (Produkt von Ringen). Seien R_1, R_2 Ringe, dann ist $(R_1 \times R_2, (0, 0), (1, 1), +, \cdot)$ ein Ring mit komponentenweiser Addition und Multiplikation.

$$+ : (R_1 \times R_2)^2 \rightarrow R_1 \times R_2, (r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$$

$$\cdot : (R_1 \times R_2)^2 \rightarrow R_1 \times R_2, (r_1, r_2) \cdot (s_1, s_2) = (r_1 \cdot s_1, r_2 \cdot s_2)$$

Bemerkung (Übung).

(a) Sei R ein kommutativer Ring, $S \subseteq R$ ein Unterring, dann ist S kommutativ.

(b) Seien R_1, R_2 kommutative Ringe, so ist auch $R_1 \times R_2$ kommutativ.

Wiederholung. Seien I, X Mengen. Eine Folge/Familie in X über (Indexmenge) I , geschrieben $(x_i)_{i \in I}$ ist eine Abbildung $x : I \rightarrow X, i \mapsto x - i$. Schreibe X^I für die Menge aller Folgen in X über I ($= \text{Abb}(I, X)$)

Beispiel 0.3 (Monoidring). Sei $R = (R, 0, 1, +, \cdot)$ ein kommutativer Ring und $M = (M, e, \circ)$ ein Monoid. Definiere

(i) $R[M] := \{(a_m)_{m \in M} \in R^M \mid (E) : \#\{m \in M : a_m \neq 0\} < \infty\}$

(ii) $\underline{0}$ = die Abbildung $M \rightarrow \{0\} \subseteq R$

(iii) $\underline{1}$ = die Folge $(\delta_{em})_{m \in M}$ mit $\delta_{em} = \begin{cases} 1, & m = e, \\ 0, & m \neq e. \end{cases}$

(iv) Verknüpfungen $+, \cdot : R[M] \times R[M] \rightarrow R[M]$ durch:

$$(a_m)_{m \in M} + (b_m)_{m \in M} := (a_m + b_m)_{m \in M}$$

und

$$(a_m)_{m \in M} \cdot (b_m)_{m \in M} := (c_m)_{m \in M}$$

mit (Übung)

$$c_m := \sum_{\substack{(m', m'') \in M \times M \\ m' \cdot m'' = m}} a_{m'} \cdot b_{m''}$$

die Summe ist endlich wegen (E) und wegen (E) gilt: $\#\{m \mid c_m \neq 0\} < \infty$

Notation.

$$\sum_{m \in M} a_m \cdot m \text{ für } (a_m)_{m \in M} \in R[M]$$

Übung 0.4.

- $(R[M], \underline{0}, \underline{1}, +, \cdot)$ ist ein Ring, $(R[M]$ heißt **Monoidring** zu M über R)
- Ist M abelsch, so ist $R[M]$ kommutativ.
- Ist $\varphi : R \rightarrow S$ ein Ringhomomorphismus und $\sigma : M \rightarrow (S, 1, \cdot)$ ein Monoidhomomorphismus, so $\exists!$ Ringhomomorphismus $\psi : R[M] \rightarrow S$ mit $\psi|_R = \varphi$ und $\psi_M = \sigma$. (dabei wir identifizieren R mit $R \cdot e = R \cdot 1$ (1-Folge) und M mit $1_R \cdot M$), nämlich:

$$\psi \left(\underbrace{\sum a_m \cdot m}_{\text{in } R[M]} \right) = \underbrace{\sum \varphi(a_m) \cdot \sigma(m)}_{\text{in } S}$$

Konvention. Ab nun seien alle Ringe R, R', S, R_i kommutativ, (und es Seien in §3 stets Ringe)

0.1 Polynomringe

Beispiel 0.5. Die folgenden Strukturen sind abelsche Monoide:

(i) $(\mathbb{N}_0, 0, +) = \mathbb{N}_0$

(ii) $(\mathbb{N}_0^n, (0, \dots, 0), +) = \times_{i \in \{1, \dots, n\}} \mathbb{N}_0$ (Komponentenweise Addition)

(iii) Für I eine beliebige Menge: $(\mathbb{N}_0^{(I)}, \underline{0}, \pm)$ mit

$$\mathbb{N}_0^{(I)} = \{(a_i)_{i \in I} \in \mathbb{N}_0 \text{ Folgen über } I \mid \#\{i \in I : a_i \neq 0\} < \infty\}$$

$\underline{0}$ = 0-Folge und \pm komponentenweise Addition in $\mathbb{N}_0^{(I)}$.

Facts 0.6 (Übung).

(i) $\mathbb{N}_0^n \cong \mathbb{N}_0^{\{1, \dots, n\}}$, $(a_i)_{i \in \{1, \dots, n\}} \mapsto (a_i)_{i \in \{1, \dots, n\}}$

(ii) Für $i \in I$ sei $e_i \in \mathbb{N}_0^{(I)}$ die Folge mit $e_i(j) = \begin{cases} 1, & j = i, \\ 0 & j \neq i. \end{cases}$

(betrachte $e_i : I \rightarrow \mathbb{N}_0$ als Abbildung) Damit ist jede Folge $\underline{a} = (a_i)_{i \in I} \in \mathbb{N}_0^{(I)}$ eindeutige Linearkombination mit Koeffizienten in \mathbb{N}_0 , nämlich:

$$\underline{a} = \sum_{i \in I} a_i \cdot e_i = \sum_{i \in I, a_i \neq 0} a_i \cdot e_i$$

Beachte: $\mathbb{N}_0^{(I)} \subseteq \mathbb{Q}^{(I)}$ (analog definiert, Folgen in \mathbb{Q} über I) mit Endlichkeitsbedingung (E). Und $(e_i)_{i \in I}$ ist eine Basis von $\mathbb{Q}^{(I)}$ als \mathbb{Q} -Vektorraum. Man sagt auch $\mathbb{N}_0^{(I)}$ ist freies abelsches Monoid über der Basis $(e_i)_{i \in I}$.

(iii) Ist M ein abelsches Monoid und $(m_i)_{i \in I}$ eine Folge in M , so $\exists!$ Monoidhomomorphismus

$$\varphi : \mathbb{N}_0^{(I)} \rightarrow M, \varphi(e_i) = m_i$$

Wiederholung. $R[X]$ ist der Polynomring über R in Variablen X . Elemente sind $\sum_{n \geq 0} a_n X^n$, ($a_n \in R$) nur endlich viele $a_n \neq 0$. $+$, \cdot auf $R[X]$ sind definiert durch

$$\begin{aligned} \sum a_i X^i + \sum b_i X^i &= \sum (a_i + b_i) X^i \\ \left(\sum a_i X^i \right) \left(\sum b_i X^i \right) &= \sum_i \left(\sum_{j=0}^i a_j b_{i-j} \right) X^i \end{aligned}$$

Proposition 0.7. Die folgende Abbildung ist ein Ringisomorphismus.

$$\psi : R[\mathbb{N}_0] \rightarrow R[X], \sum_{i \in \mathbb{N}_0} r_i i \mapsto \sum_{i \in \mathbb{N}_0} r_i X^i$$

Beweis.

- ψ wohldefiniert und bijektiv:

$$R[\mathbb{N}_0] = \text{Folgen } (r_i)_{i \in \mathbb{N}_0} \text{ mit } \#\{i \mid r_i \neq 0\} < \infty$$

$$R[X] = \text{analog}$$

- Ringstruktur:

– Addition (Übung)

– Multiplikation

$$\begin{aligned}
& \underbrace{\left(\sum_{i \in \mathbb{N}_0} r_i \cdot i \right)}_{f \in R[\mathbb{N}_0]} \underbrace{\left(\sum_{j \in \mathbb{N}_0} s_j \cdot j \right)}_g \stackrel{\text{Nach Def.}}{=} \sum_{k \in \mathbb{N}_0} s_k \cdot k, \quad s_k \\
& = \sum_{0 \leq i, j, i+j=k} r_i s_j = \sum_{j=0}^k r_j s_{k-j} \\
& \implies \psi(f \cdot g) = \psi \left(\sum_k s_k \cdot k \right) = \sum_k g_k X^k \\
& = \sum_i a_i \cdot \sum_j b_j X^j = \psi(f) \psi(g). \quad \square
\end{aligned}$$

Formal: $\{0, 1, \dots\} \rightarrow \{X^i \mid i \in \mathbb{N}_0\}$.

Proposition 0.8 (Universelle Eigenschaft von $K[X] \cong R[\mathbb{N}_0]$). $\forall \psi : R \rightarrow S$ Ringhomomorphismen und $\forall s \in S \exists!$ Ringhomomorphismus $\hat{\psi} : R[X] \rightarrow S$ mit $\hat{\psi}|_R = \psi$ und $\hat{\psi}(X) = s$

1. *Beweis.* Definiere $\hat{\psi}(\sum_{i \geq 0} r_i X^i) := \sum_{i \geq 0} \underbrace{\psi(r_i)}_{\in S} s^i$. Dann die Behauptung nachprüfen. \square

2. *Beweis.* Facts 6(iii) $\exists!$ Monoidhomomorphismus $\sigma : \mathbb{N}_0 \rightarrow (S, 1, \cdot)$ mit $\sigma(1) = s$ und Übung 4(c) (universelle Eigenschaft des Monoidrings) $\exists!$ Ringhomomorphismus $\hat{\psi} : R[\mathbb{N}_0] \rightarrow S$ mit $\hat{\psi}|_R = \psi$ und $\hat{\psi}|_{\mathbb{N}_0} = \sigma$. Dieser erfüllt die Aussagen in Prop 8, denn $\hat{\psi}(X) = \hat{\psi}(1) = s$, X entspricht $1 \in \mathbb{N}_0$ (Unter Isomorphismus von Proposition 7). Für $n \geq 1$ Variable: ($n \in \mathbb{N}$)

$$R[X_1, \dots, X_n] := (R[X_1, \dots, X_{n-1}])[X_n] = \dots = (\dots((R[X_1])[X_2])\dots)[X_n]$$

\square

Satz 0.9. Sei $\varphi : \mathbb{N}_0^n \rightarrow (R[X_1, \dots, X_n], 1, \cdot)$ der eindeutige Monoidhomomorphismus mit $\varphi(e_i) = X_i$, wobei $e_i = (\delta_{i,j})_j = (0, \dots, 1, \dots, 0)$ für $i \in \{1, \dots, n\}$. Dann ist (nach 4(c) eindeutige) Ringhomomorphismus $\hat{\psi} : R[\mathbb{N}_0^n] \rightarrow R[X_1, \dots, X_n]$ mit $\hat{\psi}|_R = \text{id}_R$ und $\hat{\psi}|_{\mathbb{N}_0^n} = \varphi$ ein Ringisomorphismus.

Beweis. (Übung) Hierbei wird $m = (m_1, \dots, m_n) \in \mathbb{N}_0^n$ identifiziert (unter $\hat{\psi}$) mit $X_1^{m_1} \cdot \dots \cdot X_n^{m_n}$ \square

Definition 0.10 (Polynomring). Der **Polynomring** in den Variablen $(X_i)_{i \in I}$ (I beliebige Menge) ist definiert als

$$R[X_i \mid i \in I] := R[\mathbb{N}_0^{(I)}]$$

Elemente in diesem Ring sind

$$\sum_{a \in \mathbb{N}_0^{(I)}} r_a \cdot a$$

mit $r_a \in R$ und es gilt $\{a \in \mathbb{N}_0^{(I)} \mid r_a \neq 0\} \leq \infty$.

Notation. Andere Notation: Für $a \in \mathbb{N}_0^{(I)}$ schreibe für a

$$X^a \text{ oder } \prod_{i \in I, a_i \neq 0} X_i^{a_i}$$

Insbesondere ist $X^{e_i} = X_i$, wobei e_i die Folge in $\mathbb{N}_0^{(I)}$ mit $e_i(j) = \delta_{i,j}$ ist. Monoidaddition $a + b$ entspricht

$$X^a \cdot X^b = X^{a+b}$$

(bilden $a + b$ in $(\mathbb{N}_0^{(I)}, 0, +)$ und $(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i +_{\mathbb{N}_0} b_i)_{i \in I}$) Also $+$ ist nicht die Addition im Ring.

Definition (Primitives Monom). Die Elemente in $R[\mathbb{N}_0^{(I)}]$ sind Summen

$$\sum_{a \in \mathbb{N}_0^{(I)}} r_a \cdot X^a$$

(Polynome wie gewohnt.) Die Elemente $X^a, a \in \mathbb{N}_0^{(I)}$ heißen **primitive Monome**. Jedes Element in $R[X_i \mid i \in I]$ ist eine eindeutige Linearkombination in den Monomen $X^a, a \in \mathbb{N}_0^{(I)}$, mit Koeffizienten r_a aus R , sodass $\#a \in \mathbb{N}_0^{(I)} \mid r_a \neq 0 \leq \infty$, d.h. als R -Modul ist $R[X_i \mid i \in I]$ frei über R mit Basis $X^a, a \in \mathbb{N}_0^{(I)}$

Beispiel. $(2, 5, 3) \in \mathbb{N}_0^3$ entspricht $X_1^2 X_2^5 X_3^3$

Satz 0.11 (Universelle Eigenschaft von $R[X_i \mid i \in I]$). Zu Ringhomomorphismus $\psi : R \rightarrow S$ und einer Folge $(s_i)_{i \in I}$ aus S über I $\exists!$ Ringhomomorphismus $\hat{\psi} : R[X_i \mid i \in I] \rightarrow S$ mit $\hat{\psi}|_R = \psi$ und $\hat{\psi}(X_i) = s_i$

Facts.

- (a) Für $J \subseteq I$ existiert eindeutiger Monoidhomomorphismus $\mathbb{N}_0^{(J)} \rightarrow \mathbb{N}_0^{(I)}$ mit $e_j \mapsto e_j$ und ein induzierter Ringhomomorphismus (für $j \in J$)

$$\hat{\psi} : R[\mathbb{N}_0^{(J)}] = R[X_j \mid j \in J] \rightarrow R[\mathbb{N}_0^{(I)}] = R[X_i \mid i \in I]$$

mit $\hat{\psi}|_R = \text{id}_R$ und $\hat{\psi}(X_j) = X_j$ ($j \in J$). Die Abbildung $\hat{\psi}$ ist injektiv deswegen betrachten wir $R[X_j \mid j \in J]$ als Unterring von $R[X_i \mid i \in I]$

- (b) Es gilt:

$$R[X_i \mid i \in I] = \bigcup_{J \subseteq I \text{ endl.}} R[X_j \mid j \in J]$$

d.h. jedes Polynom im Ring ist Polynom in nur endlich vielen Variablen.

Definition 0.12.

(a) $\text{Grad} : R[X] \rightarrow \mathbb{N}_0 \cup \{-\infty\}$ ist die eindeutige Abbildung mit

$$\text{Grad}(f) = \text{Grad} \left(\sum_{i \geq 0} r_i X^i \right) = \begin{cases} -\infty, & f = 0, \\ \max\{i \in \mathbb{N}_0 \mid r_i \neq 0\}, & f \neq 0 \end{cases}$$

(b) Der **Leitkoeffizient** von $f \neq 0$ ist $a_{\text{Grad}(f)}$.

(c) $f \neq 0$ heißt **normiert** $\iff a_{\text{Grad}(f)} = 1$.

(d) Ist $R = K$ ein Körper, so gelten außerdem

$$\text{Grad}(fg) = \text{Grad}(f) + \text{Grad}(g)$$

wobei $-\infty + n = n + -\infty = -\infty + (-\infty) = -\infty$ für $n \in \mathbb{N}_0$. Genügt: R ist Integritätsbereich.

(e) Falls R ein Körper (oder Integritätsbereich), so gilt

$$\begin{aligned} (R[X])^\times &= \{f \in R[X] \mid \exists g \in R[X] : fg = 1\} \\ &\stackrel{\text{Übung}}{=} \{f \in R[X] \mid \text{Grad}(f) = 0, \exists g \in R[X] : \text{Grad } g = 0 : fg = 1\} \\ &= \{f \in R \mid \exists g \in R : fg = 1\} = R^\times \end{aligned}$$

0.2 Symmetrische Polynome

Sei R ein kommutativer Ring, $n \in \mathbb{N}$ fest.

Bezeichnung. (a) Ein Monom in $R[X_1, \dots, X_n]$ ist ein Polynom der Form $aX^m = aX_1^{m_1} \cdots X_n^{m_n}$ für $a \in R \setminus \{0\}$ und $m = (m_i)_{i \in \{1, \dots, n\}} \in \mathbb{N}_0^n$ und X^m (falls $a = 1$) heißt primitives Monom.

(b) Der (Total-)Grad des Monoms aX^m für $a \in R \setminus \{0\}$ und $m = (m_i)$ ist $|m| := \sum_i m_i$. Der (Total-)Grad von $f = \sum a_m X^m$ ist $\text{Grad}(f) = \max\{|m| : a_m \neq 0\}$. ($\max(\emptyset) := -\infty$)

(c) $f \in R[X_1, \dots, X_n]$ heißt homogen vom Grad $t \iff f$ ist Summe von Monomen aX^m , die alle vom Grad $|m| = t$ sind.

Beispiel. (a) $f = X_1^3 X_2^2 X_3$ ist primitiver Monom mit $\text{Grad}(f) = 11$

(b) $g = X_1^3 X_2^2 + X_1 X_2^4$ ist homogen vom Grad 5

Lemma 0.13. (a) $\forall \sigma \in S_n \exists!$ Ringhomomorphismus $\tilde{\sigma} : R[X_1, \dots, X_n] \rightarrow R[X_1, \dots, X_n]$ mit $\tilde{s}|_R = \text{id}_R$ und $\tilde{\sigma}(X_i) = X_{\sigma(i)}$ für $i \in \{1, \dots, n\}$

(b) $\tilde{\text{id}} = \text{id}_{R[X_1, \dots, X_n]}$ (für $\text{id} \in S_n$ die Eins).

(c) $\forall \sigma, \tau \in S_n : \widetilde{\sigma \circ \tau} = \tilde{\sigma} \circ \tau$ Ringhomomorphismen.

Beweis. (a) $\tilde{\sigma}$ existiert und ist eindeutig nach universeller Eigenschaft (Satz 10) für $R[X_1, \dots, X_n]$.

(b) $\alpha := \text{id}_{R[X_1, \dots, X_n]}$ ist ein Ringhomomorphismus $R[X_1, \dots, X_n] \rightarrow R[X_1, \dots, X_n]$ mit $\alpha|_R = \text{id}_R$ und $\alpha(X_i) = X_i \xrightarrow{(a)} \alpha = \text{id}$.

(c) Wende universelle Eigenschaft von $R[X_1, \dots, X_n]$ an. Wir haben:

$$\widetilde{\sigma \circ \tau}|_R \stackrel{\text{Def. in (a)}}{=} \text{id}_R = \text{id}_R \circ \text{id}_R = \widetilde{\sigma}|_R \circ \widetilde{\tau}|_R = \widetilde{\sigma \circ \tau}|_R$$

und

$$\widetilde{\sigma \circ \tau}(X_i) = X_{\sigma \circ \tau(i)} = X_{\sigma(\tau(i))} = \widetilde{\sigma}(X_{\tau(i)}) = \widetilde{\sigma}(\widetilde{\tau}(X_i)) = (\widetilde{\sigma} \circ \widetilde{\tau})(X_i)$$

$$\xrightarrow[\text{in (a)}]{\text{Eindeutigkeit}} \widetilde{\sigma \circ \tau} = \widetilde{\sigma} \circ \widetilde{\tau}. \quad \square$$

Bemerkung (Übung). Ist $\alpha : R \rightarrow R$ ein Ringhomomorphismus, so ist $R^\alpha := \{r \in R \mid \alpha(r) = r\}$ ein Unterring von R .

Korollar 0.14. $R[X_1, \dots, X_n]^{S_n} := \{f \in R[X_1, \dots, X_n] \mid \widetilde{\sigma}(f) = f, \forall \sigma \in S_n\} = \bigcap_{\sigma \in S_n} R[X_1, \dots, X_n]^{\widetilde{\sigma}}$ ist ein Unterring von $R[X_1, \dots, X_n]$.

Definition 0.15 (Symmetrische Polynom). Die Elemente in $R[X_1, \dots, X_n]^{S_n}$ heißen symmetrische Polynome.

Korollar 0.16. Die Abbildung

$$\widetilde{\cdot} : S_n \rightarrow \text{Aut}(R[X_1, \dots, X_n]), \sigma \mapsto \widetilde{\sigma}$$

ist wohl-definiert und ein injektiver Gruppenhomomorphismus.

Beweis.

1) $\widetilde{\cdot}$ wohl-definiert: Zu zeigen $\widetilde{\sigma}$ ist Automorphismus (bijektiver Ringhomomorphismus). Dazu beachte

$$\widetilde{\sigma \circ \sigma^{-1}} \stackrel{12}{=} \widetilde{\sigma \circ \sigma^{-1}} = \widetilde{\text{id}} = \text{id}_{R[X_1, \dots, X_n]} = \dots = \widetilde{\sigma^{-1}} \circ \widetilde{\sigma}$$

folglich: $\widetilde{\sigma}$ ist Ringautomorphismus.

2) Gruppenhomomorphismus: folgt aus 12(c)

3) $\sigma \mapsto \widetilde{\sigma}$ injektiv: Denn verschiedene σ, τ wirken unterschiedlich auf $\{X_1, \dots, X_n\}$ \square

Bemerkung (Ziel von diesem Abschnitt). Explizite Beschreibung von $R[X_1, \dots, X_n]^{S_n}$

0.3 Elementar symmetrische Polynome

Proposition. Zu $\sigma \in S_n$ erweitern $\widetilde{\sigma}$ zu σ' Ringautomorphismus von $R[X_1, \dots, X_n][X]$ durch

$$\sigma'|_R = \text{id}_R, \sigma'(X_i) = X_{\sigma(i)} \text{ und } \sigma'(X) := X$$

Behauptung: $g := \prod_{i=1}^n (X - X_i) \stackrel{!}{\in} R[X_1, \dots, X_n]^{S_n} \stackrel{\text{Übung}}{=} R[X_1, \dots, X_n]^{S_n}[X].$

Beweis. $\sigma'(g) = \prod_{i=1}^n (\sigma'(X) - \sigma'(X_i)) = \prod_{i=1}^n (X - X_{\sigma(i)}) = \prod_{i=1}^n (X - X_i) = g$
da $\tilde{\sigma}$ eine Bijektion auf $\{X_1, \dots, X_n\}$ definiert. \square

Bemerkung. Schreibe g als Polynom in X mit Koeffizienten s_i in

$$R[X_1, \dots, X_n] \implies g = \sum_{i=0}^n (-1)^{n-i} X^i s_{n-i}(X_1, \dots, X_n)$$

$$= X^n - s_1(X_1, \dots, X_n) X^{n-1} + s_2(X_1, \dots, X_n) X^{n-2} \mp \dots + (-1)^n s_n(X_1, \dots, X_n)$$

Das definiert $s_1, \dots, s_n \in R[X_1, \dots, X_n]^{S_n}$

Insbesondere:

- (i) $s_1, \dots, s_n \in R[X_1, \dots, X_n]^{S_n}$
- (ii) s_i ist homogen vom Grad i , denn g ist homogen vom Grad $n \implies$ Koeffizient von X^{n-i} in g ist homogen vom Grad i .

Übung 0.17. Es gelten:

$$s_1 = \sum_{i=1}^n X_i, \quad s_n = \prod_{i=1}^n X_i$$

$$s_i(X_1, \dots, X_n) = \sum_{1 \leq j_1 < j_2 < \dots < j_i \leq n} X_{j_1} X_{j_2} \dots X_{j_i}$$

$$(n=3, i=2 \rightsquigarrow s_2 = X_1 X_2 + X_1 X_3 + X_2 X_3)$$

Definition 0.18. Die Polynome $s_1, \dots, s_n \in R[X_1, \dots, X_n]^{S_n}$ sind die elementar symmetrischen Polynome in X_1, \dots, X_n (homogen vom Grad $1, 2, \dots, n$) ($s_i = i$ -tes elementar symmetrisches Polynom)

Satz 0.19. Sei $\psi : R[Y_1, \dots, Y_n] \rightarrow R[X_1, \dots, X_n]$ der Ringhomomorphismus

$$h(Y_1, \dots, Y_n) \mapsto h(s_1, \dots, s_n)$$

Dann gilt

(a) ψ ist Ringhomomorphismus mit $\psi|_R = \text{id}_R$ und $\psi(Y_i) = s_i$ und $\text{Kern}(\psi) \subseteq R[X_1, \dots, X_n]^{S_n}$

(b) ψ definiert einen Ringisomorphismus

$$R[Y_1, \dots, Y_n] \rightarrow R[X_1, \dots, X_n]^{S_n}$$

Beispiel. $n=4, f = X_1^2 + X_2^2 + X_3^2 + X_4^2$

$$\underbrace{(X_1 + \dots + X_4)^2}_{s_1} - 2 \underbrace{(X_1 X_2 + X_1 X_3 + X_2 X_3 + X_1 X_4 + X_2 X_4 + X_3 X_4)}_{s_2}$$

$$= s_1^2 - 2s_2 = h(s_1, s_2), h = Y_1^2 - 2Y_2$$

Wiederholung.

(a) $R[X_1, \dots, X_n] \subseteq R[X_1, \dots, X_n]^{S_n}$ symmetrische Polynome.

(b) Elementar symmetrische Polynome $s_1, \dots, s_n \in K[X_1, \dots, X_n]^{S_n}$ mit

$$s_i(X_1, \dots, X_n) = \sum_{1 \leq j_1 < \dots < j_i \leq n} \prod_{1 \leq k \leq i} X_{j_k} = \sum_{1 \leq j_1 < \dots < j_i \leq n} X_{j_1} \cdot \dots \cdot X_{j_i}$$

Beweis. (zu Satz 3.19)

Teil (a) Klar

$$\text{Kern}(\psi) = \left\{ \sum_{m \in \mathbb{N}_0} \underbrace{a_m}_{\in R} \cdot \underbrace{s_1^{m_1} \cdot \dots \cdot s_n^{m_n}}_{\text{symm. Pol.}} \right\}$$

Teil (b) benötigt Vorbereitungen.

□

Bemerkung. Sei $R = K$ ein Körper, $\alpha_1, \dots, \alpha_n$ die Nullstellen von $f = X^n - \alpha_1 X^{n-1} + a_2 X^{n-2} \mp \dots + (-1)^n a_n \in K[X]$, dann gilt $\alpha_i = s_i(\alpha_1, \dots, \alpha_n)$, denn: $f = (X - \alpha_1) \cdot \dots \cdot (X - \alpha_n)$. (hatten s_i erhalten als die Koeffizienten von $(-1)^i X^{n-i}$ in $(X - X_1) \cdot \dots \cdot (X - X_n)$)

Definition 0.20 (Lex-Ordnung).

(a) Definiere auf \mathbb{N}_0^n die Relation \leq durch $\ell = (\ell_1, \dots, \ell_n) \leq m = (m_1, \dots, m_n) :$
 $\iff \ell = m$ oder $\exists i \in \{1, \dots, n\}$ mit $\ell_1 = m_1, \dots, \ell_{i-1} = m_{i-1}, \ell_i < m_i$. Dies definiert eine Totalordnung auf \mathbb{N}_0^n , die lexikographische Ordnung. Schreibe $\ell < m$ für $\ell \leq m$ und $\ell \neq m$. Für primitive Monome schreibe

$$X^\ell \leq X^m \iff \ell \leq m$$

(b) Der Leitgrad von $f = \sum_{m \in \mathbb{N}_0^n} a_m X^m$ ist $\text{in}(f) := \max\{m \in \mathbb{N}_0^n \mid a_m \neq 0\} \in \mathbb{N}_0^n \cup \{-\infty\}$ (mit der Konvention $\text{in}(0) = -\infty$) der Leitkoeffizient von $f \neq 0$ ist $a_{\text{in}(f)}$.

Beispiel. $\text{in}(\underbrace{X_1^3 X_2^2 + X_1^4 X_3}_{\in R[X_1, X_2, X_3]}) = (4, 0, 1) \in \mathbb{N}_0^3$

Proposition 0.21. Seien $f = \sum_{\ell \in \mathbb{N}_0^n} a_\ell X^\ell, g = \sum_{m \in \mathbb{N}_0^n} b_m X^m, \ell_0 = \text{in}(f), m_0 = \text{in}(g)$. Dann:

(a) Für $m, \ell, m', \ell' \in \mathbb{N}_0^n$ gilt

$$m \geq \ell, m' \geq \ell' \implies m + m' \geq \ell + \ell'$$

(gilt dabei $m \neq \ell$ oder $m' \neq \ell'$, so folgt $m + m' > \ell + \ell'$)

(b) $\text{in}(f \cdot g) \leq \ell_0 + m_0$ und es gilt $\text{in}(f \cdot g) = \ell_0 + m_0$ falls die Leitkoeffizienten $a_{\ell_0} \cdot b_{m_0} \neq 0$.

(c) $\text{in}(f \cdot g) \leq \max(\text{in}(f), \text{in}(g))$ und es gilt Gleichheit falls $\text{in}(f) \neq \text{in}(g)$.

(d) $\text{in}(s_i) = (\underbrace{1, \dots, 1}_i, \underbrace{0, \dots, 0}_{n-i}) =: \xi_i \in \mathbb{N}_0^n$ für $i \in \{1, \dots, n\}$.

- (e) ξ_1, \dots, ξ_n sind linear unabhängig als Elemente von \mathbb{Q}^n , und also ist $\varphi_i : \mathbb{N}_0^n \rightarrow \mathbb{N}_0^n, (a_i) \mapsto \sum a_i \xi_i$ injektiv und φ^{-1} ist durch die Formel (für Elemente im Bild)

$$(b_i) \mapsto (b_1 - b_2, b_2 - b_3, \dots, b_{n-1} - b_n, b_n)$$

Beweis. (a) (Übung) Es genügt zu zeigen $m \geq \ell \implies m + m' \geq \ell + m'$ (mit $> \implies >$) genügt mit Induktion zu zeigen: $m \geq \ell \implies m + e_j \geq \ell + e_j$, ($e_j = (0, \dots, 0, 1, 0, \dots, 0)$)

- (b) $f \cdot g = (\sum a_\ell X^\ell)(\sum b_m X^m) = \sum_{\ell, m} a_\ell b_m X^{\ell+m}$ falls $a_\ell b_m \neq 0$ (nur solche Terme tragen zu $f \cdot g$ bei), so folgt $\ell \leq \ell_0$ und $m \leq m_0$, ℓ_0, m_0 die Leitkoeffizienten. $\implies \ell + m \geq \ell_0 + m_0 \implies \text{in}(f \cdot g) \leq \ell_0 + m_0$.
(a)

Außerdem: (Koeffizient von $X^{\ell_0+m_0} = ?$) gilt $\ell + m = \ell_0 = m_0$, so muss wegen (a) $\ell = \ell_0$ und $m = m_0$ gelten, falls $a_\ell \neq 0$ und $b_m \neq 0 \implies$ Koeffizient von $X^{\ell_0+m_0}$ ist $a_{\ell_0} \cdot b_{m_0}$. Also $\text{in}(fg) = m_0 + \ell_0$, falls $a_{\ell_0} b_{m_0} \neq 0$.

- (c) $f + g = \sum_m (a_m + b_m) X^m$: Im Fall $a_m + b_m \neq 0$, so folgt $a_m \neq 0$ oder $b_m \neq 0 \implies m \leq \ell_0$ oder $m \leq m_0 \implies m \leq \max\{\ell_0, m_0\}$.

Für Zusatz: Gelte o.E. $\ell_0 < m_0$, dann ist der Koeffizient von X^{m_0} gleich $a_{m_0} + b_{m_0} \neq 0$, wobei $a_{m_0} = 0$ wegen $m_0 \geq \text{in}(f)$, und $b_{m_0} \neq 0$, da $m_0 = \text{in}(f)$. Also folgt $\text{in}(f + g) = \max\{\ell_0, m_0\}$.

- (d) $s_i = \sum_{i \leq j_1 < j_2 < \dots < j_i \leq n} X_{j_1} \cdot \dots \cdot X_{j_i}$ größtes Monom (mit Koeffizient $\neq 0$) in der Summe ist $X_1 \cdot \dots \cdot X_i \implies \text{in}(s_i) = (1, \dots, 1, 0, \dots, 0) = (\delta_{j \leq i})_{1 \leq j \leq n}$.

- (e) (Übung) zur linearen Algebra, φ hat Darstellungsmatrix

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 1 \end{pmatrix}$$

und φ^{-1}

$$\begin{pmatrix} 1 & -1 & & & \\ & 1 & -1 & & \\ & & \ddots & \ddots & \\ & & & 1 & -1 \\ & & & & 1 \end{pmatrix} : \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_{n-1} \\ t_n \end{pmatrix} \mapsto \begin{pmatrix} t_1 - t_2 \\ t_2 - t_3 \\ \vdots \\ t_{n-1} - t_n \\ t_n \end{pmatrix}. \quad \square$$

Beweis von Satz 3.19. \square

Definition 0.22. Die Diskriminante von $f(X) = X^n - a_1 X^{n-1} + a_2 X^{n-2} \mp \dots + (-1)^n a_n \in R[T]$ ist $D(f) := d_n(a_1, \dots, a_n)$ Polynom in n -Variablen über R .

Bedeutung. Sei R ein Körper und seien $\alpha_1, \dots, \alpha_n$ die Nullstellen von f , so dass $\alpha_i = s_i(\alpha_1, \dots, \alpha_n)$, dann folgt:

$$D(f) = d_n(s_1(\alpha_1, \dots, \alpha_n), \dots, s_n(\alpha_1, \dots, \alpha_n))$$

$$= D_n(\alpha_1, \dots, \alpha_n) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

d.h. $D(f)$ erkennt ob mehrfache Nullstelle vorliegt. Jedes symmetrische Polynom in den Nullstellen von f lässt sich schreiben als ein Polynom in den Koeffizienten von f .

Wiederholung 0.23. Sei R ein kommutativer Ring (im Weiteren), $I \subseteq R$ ist ein Ideal von R , falls $RI \subseteq I, I + I \subseteq I$.

Notation. Für $a \in R$ sei $(a) = Ra$ das Hauptideal in R , Erzeuger a . Für $a_1, \dots, a_n \in R$ sei $(a_1, \dots, a_n) = Ra_1 + Ra_2 + \dots + Ra_n \subseteq R$ Ideal.

Bemerkung (Übung). Für $I \subseteq R$ ein Ideal: $1 \in I \iff I = R$, für $S \subseteq R$ Unterring: $S = R \iff RS \subseteq S$.

Proposition 0.24. Sei $\varphi : R \rightarrow R'$ ein Ringhomomorphismus, dann gelten:

(i) Ist $I' \subseteq R'$ ein Ideal, so ist $\varphi^{-1}(I') \subseteq R$ ein Ideal.

(ii) Kern $\varphi = \varphi^{-1}(\{0\}) \subseteq R$ ist ein Ideal.

(iii) Kern $(\varphi) = \{\varphi(r) \mid r \in R\} \subseteq R'$ ist ein Unterring.

(iv) Ist φ surjektiv und $I \subseteq R$ ein Ideal, so ist $\varphi(I) \subseteq R'$ ein Ideal.

Beweis. nur (iv)

(iv)

$$\varphi(I) + \varphi(I) = \underbrace{\{\varphi(a) + \varphi(b) \mid a, b \in I\}}_{\varphi(a+b)} = \varphi(I + I) \underset{I+I \subseteq I}{\subseteq} \varphi(I)$$

(benötigt nicht, dass φ surjektiv)

$$R' \cdot \varphi(I) \underset{\varphi \text{ surj.}}{=} \varphi(R)\varphi(I) = \{\varphi(r)\varphi(a) \mid r \in R, a \in I\} = \varphi(RI) \underset{RI \subseteq I}{\subseteq} \varphi(I)$$

Also $\varphi(I) \subseteq R'$ ist ein Ideal. \square

Definition 0.25 (Charakteristik). Die Charakteristik von R ist

$$\text{char}(R) := \begin{cases} 0, & n \cdot 1_R \neq 0_R, \forall n \in \mathbb{N} \\ \min\{n \in \mathbb{N} \mid n \cdot 1_R = 0_R\}, & \exists n \in \mathbb{N} : n \cdot 1_R = 0_R \end{cases}$$

Beispiel.

$$\text{char}(\mathbb{Z}) = 0, \text{char}(\mathbb{Z}/n\mathbb{Z}) = n, n \in \mathbb{N}$$

Bemerkung (Übung). (a) Sei $\text{ord}(1_R)$ die Ordnung von 1_R in $(R, 0_R, +)$, dann

$$\text{char}(R) = \begin{cases} \text{ord}(1_R), & \text{ord}(1_R) \neq \infty \\ 0, & \text{ord}(1_R) = \infty \end{cases}$$

(b) Sei $\varphi : \mathbb{Z} \rightarrow R$ der eindeutige Ringhomomorphismus

$$\varphi(1_{\mathbb{Z}}) := 1_R \implies \varphi(n_{\mathbb{Z}}) = n \cdot 1_R, \forall n \in \mathbb{Z}$$

Dann gilt: $\text{char}(R)$ ist der (eindeutige) Erzeuger in \mathbb{N} von $\text{Kern}(\varphi) \subseteq \mathbb{Z}$ (ein Ideal) (“Grund für die Definition von $\text{char}(R)$ ”)

Proposition 0.26. *Ist K ein Körper, so ist $\text{char } K$ Null oder eine Primzahl.*

Beweis. Annahme: $\text{char } K \in \mathbb{N}$ und ist keine Primzahl $\implies \exists n, m \in \mathbb{N}$ mit $n > 1, m > 1$, sodass $\text{char } K = n \cdot m > \max\{n, m\}$

Definition der Charakteristik gibt:

$$n \cdot m \cdot 1_K = 0_K \implies \underbrace{n \cdot 1_K}_{\neq 0 (*)} \cdot \underbrace{m \cdot 1_K}_{\neq 0 (*)} = 0$$

(*) da $n, m < n \cdot m = \text{char } K$. Da K ein Körper $\implies K$ ist nullteilerfrei $\implies n \cdot 1_K = 0$ oder $m \cdot 1_K = 0$. Widerspruch zu (*). \square

Beispiel (Übung). Sei R ein Ring mit $\text{char}(R) = p$ eine Primzahl, dann gelten:

(a) $\varphi_R : R \rightarrow R, a \mapsto a^p$ ist ein Ringhomomorphismus.

(b) Es gilt $\varphi_{\mathbb{F}_p} = \text{id}_{\mathbb{F}_p}$, wobei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, d.h. $\forall a \in \mathbb{F}_p$ gilt $a^p = a$.

Wiederholung. Für $I \subseteq R$ ein Ideal, hatten Faktoring R/I und Faktorabbildung $\pi : R \rightarrow R/I, r \mapsto r + I$ (vgl. Satz 1.49)

Satz 0.27 (Homomorphiesatz für Ringe). *Sei $\varphi : R \rightarrow R'$ ein Ringhomomorphismus und $I \subseteq \text{Kern}(\varphi)$ ein Ideal von R , dann:*

(a) $\exists!$ Ringhomomorphismus $\bar{\varphi} : R/I \rightarrow R'$ mit $\bar{\varphi}(r + I) = \varphi(r)$, d.h. folgendes Diagramm kommutiert:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ \pi \downarrow & \nearrow \bar{\varphi} & \\ R/I & & \end{array}$$

(b) Ist $I = \text{Kern}(\varphi)$, so definiert $\bar{\varphi}$ aus (a) einen Ringisomorphismus

$$R/\text{Kern}(\varphi) \rightarrow \text{Kern}(\varphi) \subseteq R', r + \text{Kern}(\varphi) \mapsto \varphi(r)$$

Beweis. (Übung) analog zum Beweis vom Homomorphiesatz für Gruppen (Satz 1.45). \square

Satz 0.28 (Isomorphiesatz für Ringe). *Sei $\varphi : R \rightarrow R'$ ein surjektiver Ringhomomorphismus $(R' \cong R/\text{Kern}(\varphi))$, seien $X = \{I \subseteq R \text{ Ideal} \mid \text{Kern}(\varphi) \subseteq I\}$, $X' = \{I' \subseteq R' \mid I' \text{ Ideal}\}$. Dann gelten:*

(a) Die Abbildung $X' \rightarrow X, I' \mapsto \varphi^{-1}(I')$ ist eine Bijektion mit Umkehrabbildung $X \rightarrow X', I \mapsto \varphi(I)$.

(b) Für $I \subseteq R'$ ein Ideal und $I = \varphi^{-1}(I')$ ist die Abbildung

$$R/I \rightarrow R'/I', r + I \mapsto \varphi(r) + I'$$

ein Ringisomorphismus.

Beweis. (Übung) analog zum Beweis vom 2. Isomorphiesatz für Gruppen (Satz 1.51). \square

Notation. Für $I, J \subseteq R$ sei $I \cdot J = \{\sum_i a_i b_i \mid a_i \in I, b_i \in J\}$, d.h. (Übung) $I \cdot J$ ist das kleinste Ideal in R , das $\{a \cdot b \mid a \in I, b \in J\}$ enthält.

Satz 0.29 (Chinesischer Restsatz). *Seien $I_1, \dots, I_t \subseteq R$ Ideale, die "paarweise Koprime" sind, d.h. $I_i + I_j = R$ für $i \neq j \in \{1, \dots, t\}$. Dann gelten:*

(a) I_i und $\prod_{j \neq i \in \{1, \dots, t\}} I_j$ sind Koprime.

(b) $I_1 \cdot \dots \cdot I_t = \bigcap_{i \in \{1, \dots, t\}} I_i$.

(c) Die Abbildung

$$R / \prod_{i \in \{1, \dots, t\}} I_i = R / I_1 \cdot \dots \cdot I_t \xrightarrow{\cong} \prod_{i \in \{1, \dots, t\}} R / I_i = R / I_1 \times \dots \times R / I_t$$

$$r + I_1 \cdot \dots \cdot I_t \mapsto (r + I_1, \dots, r + I_t)$$

ist wohl-definiert und ein Ringisomorphismus. Also gilt

$$R / \prod_{i \in \{1, \dots, t\}} I_i \cong \prod_{i \in \{1, \dots, t\}} R / I_i$$

Beweis. In der LA2 für R ein Hauptidealring, allgemein: siehe Jantzen-Schwermer, Satz III.3.10 \square

0.4 Ringe von Brüchen/Lokalisierung

Definition 0.30. Eine Teilmenge $S \subseteq R$ heißt multiplikativ abgeschlossen \iff S ist ein Untermonoid von $(R, 1, \cdot)$.

Beispiel. (i) $S = \mathbb{Z} \setminus \{0\} \subseteq \mathbb{Z}$ ist multiplikativ abgeschlossen.

(ii) $S^p = \mathbb{Z} \setminus p\mathbb{Z} \subseteq \mathbb{Z}$ ist multiplikativ abgeschlossen.

(iii) $S_p = \{p^n \mid n \in \mathbb{N}_0\} \subseteq \mathbb{Z}$ ist multiplikativ abgeschlossen.

Es gilt $S = S^P \cdot S_p$

Definition 0.31. Definiere eine Äquivalenzrelation auf $R \times S$ ($S \subseteq R$ multiplikativ abgeschlossen) durch

$$(r, s) \sim (r', s') : \iff \exists t \in S : t(rs' - r's)$$

Denn:

\sim reflexiv: $(r, s) \sim r, s$, da $1 \cdot (rs - rs) = 0$.

\sim symmetrisch: Gelte $(r, s) \sim (r', s')$, d.h. $\exists t \in S : t(rs' - r's) = 0 \implies t(r's - rs') = 0 \implies (r', s') \sim (r, s)$.

\sim transitiv: Gelte $(r, s) \sim (r', s')$ und $(r', s') \sim (r'', s'')$, d.h. $\exists t, t' \in S : t(rs' - r's) = 0$ und $t'(r's'' - r''s') = 0$. Gemeinsamer Nenner $tt'ss's''$

$$\implies tt's''(rs' - r's) = 0, tt's(r's'' - r''s) = 0$$

$$\implies tt's''rs' - tt'sr''s' = 0 = tt's'(rs'' - r''s) \implies (r, s) \sim (r'', s'')$$

Schreibe: $\frac{r}{s}$ für die Äquivalenzklasse von (r, s) und $S^{-1}R$ für $R \times S / \sim$.

Beachte: $\frac{r}{s} = \frac{r'}{s'} \iff \exists t \in S : \frac{ts'r}{ts's'} = \frac{tsr'}{tss'}$ gilt $ts'r = tsr'$, beachte zudem $\frac{r}{s} = \frac{tr}{ts}$, für $t \in S$.

Übung

Satz 0.32. Sei $S \subseteq R$ multiplikativ abgeschlossen, dann:

(a) Die Verknüpfungen $+, \cdot$ auf $S^{-1}R$ definiert durch

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}, \quad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$$

sind wohl-definiert.

(b) $S^{-1}R = (S^{-1}R, \frac{0}{1}, \frac{1}{1}, +, \cdot)$ ist ein kommutativer Ring.

(c) Die Lokalisierung von R an S

$$\varphi : R \rightarrow S^{-1}R, r \mapsto \frac{r}{1}$$

ist ein Ringhomomorphismus. (Klar aus dem Definition von $+$ und \cdot)

(d) (Universelle Eigenschaft) Ist $\psi : R \rightarrow R'$ ein Ringhomomorphismus, so dass $\psi(S) \leq (R')^\times$, so existiert ein eindeutiger Ringhomomorphismus $\hat{\psi} : S^{-1}R \rightarrow R'$ mit $\hat{\psi}|_R = \psi$, nämlich $\hat{\psi}(\frac{r}{s}) = \psi(r) \cdot \psi(s)^{-1}$.

Beispiel. $(\mathbb{Z} \setminus \{0\})^{-1}\mathbb{Z} = \mathbb{Q}, \mathbb{Z}^{-1}\mathbb{Z} = 0\text{-Ring}$.

Beweis.

(a) $+$ und \cdot sind wohldefiniert: Gelte $\frac{r}{s} = \frac{a}{b}$ und $\frac{r'}{s'} = \frac{a'}{b'}$ mit $r, r', a, a' \in R, s, s', b, b' \in S$, zu zeigen ist:

$$\frac{rs' + r's}{ss'} = \frac{ab' + a'b}{bb'}$$

Voraussetzung: $\exists t, t' \in S : t(rb - as) = 0, t'(r'b' - a's') = 0$. Gemeinsamer Nenner: $ss'bb'tt'$, also

$$tt'b's'(rb - as) = 0, \quad tt'sb(r'b' - a's) = 0$$

$$\implies tt'b's'rb - tt'b's'as + tt'sbr'b' - tt'sba's' = 0$$

$$= tt'b'b(rs' + r's) - tt'ss'(ab' - a'b) \implies \frac{rs' + r's}{ss'} = \frac{ab' + a'b}{bb'}$$

(b) - (d) Siehe Jantzen Schwermer III.4.2 oder Übung.

□

Definition 0.33 (Nullteiler). (a) $x \in R$ heißt Nullteiler $\iff \exists y \in R \setminus \{0\}$ mit $xy = 0$

(b) R heißt Integritätsbereich (IB) $\iff 0_R \neq 1_R$ und 0_R ist der einzige Nullteiler.

Bemerkung 0.34. R ist Integritätsbereich \iff man darf in R kürzen und $0_R \neq 1_R$

$$\iff \forall a, b, c \in R : a \neq 0 : a \cdot b = a \cdot c \implies b = c$$

Übung

Denn $ab = ac \iff a(b - c) = 0$

Beispiel. (i) Jeder Körper ist ein Integritätsbereich.

(ii) $\mathbb{Z}, K[X]$ sind Integritätsbereich.

(iii) Jeder Unterring eines Körpers ist ein Integritätsbereich.

(iv) Jeder Unterring eines Integritätsbereichs ist ein Integritätsbereich.

Lemma 0.35. Sei $S \subseteq R$ multiplikativ abgeschlossen, dann gilt: enthält S keine Nullteiler, so ist

$$\varphi : R \hookrightarrow S^{-1}R, r \mapsto \frac{r}{1}$$

injektiv.

Beweis. Für $r \in R : \varphi(r) = 0 \iff \frac{r}{1} = \frac{0}{1} \iff \exists t \in S : t(r \cdot 1 - 0 \cdot 1) = 0 = tr$, da S nullteilerfrei $\iff r = 0$. □

Korollar 0.36. Sei R ein Integritätsbereich, dann:

(a) $S = R \setminus \{0\}$ multiplikativ abgeschlossen.

(b) $S^{-1}R$ ist ein Körper.

(c) $R \rightarrow S^{-1}R$ ist injektiv (also ist R Unterring des Körpers $S^{-1}R$)

Beweis. (a) Klar, $a, b \neq 0 \implies a \cdot b \neq 0$ (a, b keine Nullteiler)

(b) Sei $\frac{r}{s} \in S^{-1}R \setminus \{\frac{0}{1}\}$, Behauptung: $r \neq 0$ (also $r \in S$) $\implies \frac{s}{r}$ ist Inverses von $\frac{r}{s}$
Beweis der Behauptung: Angenommen $r = 0 \implies \frac{0}{s} \neq \frac{0}{1}$, Widerspruch,
da $\frac{0}{1} = \frac{0}{1} (1 \cdot (0 \cdot 1 - 0 \cdot s) = 0)$

(c) Folgt aus Lemma 3.35. □

Definition 0.37 (Quotientenkörper). $S^{-1}R = \text{Quot}(R)$ heißt Quotientenkörper von R .

Bemerkung 0.38. Jeder Integritätsbereich ist Unterring eines Körpers (seinem Quotientenkörper).

0.5 Spezielle Ideale

Definition 0.39. Sei $I \subseteq R$ ein echtes Ideal (d.h. $I \subsetneq R$), dann

(a) I ist **Primideal** $\iff \forall a, b \in R$ gilt:

$$a \cdot b \in I \implies a \in I \vee b \in I$$

(b) I heißt **maximales Ideal** $\iff \forall J \subsetneq R$ Ideale mit $I \subseteq J$ gilt $I = J$

Proposition 0.40. Seien $P, M \subseteq R$ Ideale, dann:

(a) P ist ein Primideal $\iff R/P$ ist ein Integritätsbereich.

(b) R ist ein Körper $\iff \{0\}$ und R sind die einzigen Ideale von R und $0_R \neq 1_R$.

(c) M ist ein maximales Ideal $\iff R/M$ ist ein Körper.

(d) Jedes maximale Ideal ist ein Primideal.

Beweis.

(a) P Primideal $\implies P \subsetneq R$ und $\forall a, b \in R : a \cdot b \in P \implies a \in P \vee b \in P \implies R/P \neq 0\text{-Ring}$ und $\forall a, b \in R :$

$$(a + P)(b + P) \subseteq P \implies a + P = P \vee b + P = P$$

$$\implies R/P \neq 0\text{-Ring} \text{ und } \forall \bar{a}, \bar{b} \in R/P :$$

$$\bar{a} \cdot \bar{b} = 0 \implies \bar{a} = 0 \vee \bar{b} = 0$$

$\implies R/P$ ist ein Integritätsbereich. Man kann auch "rückwärts laufen"
 \implies die Äquivalenz in (a).

(b) Übung.

(c) Folgt aus (b) und dem Isomorphiesatz für Ringe. (der postuliert Bijektion
 $: \{\text{Ideale } J \subseteq R \mid M \subseteq J \subseteq R\} \text{ und } \{\text{Ideale } \bar{J} \subseteq R/M \mid \{\bar{0}\} \subseteq \bar{J} \subseteq R/M\}$).

(d) Folgt aus (c) und (a), da Körper Integritätsbereiche sind. \square

Beispiel 0.41. (a) Ist R ein Integritätsbereich und kein Körper, so ist $\{0\}$ ein Primideal, aber nicht maximal.

(b) In $R = K[X, Y]$ sind $\{0\} \subsetneq X \subsetneq (X, Y) \subsetneq K$ Primideal.

Wiederholung (Grundlagen). Eine Relation \leq auf einer Menge M heißt [Halbordnung]
 $\iff \leq$ ist reflexiv, transitiv und antisymmetrisch. (\leq antisymmetrisch bedeutet: $x \leq y \wedge y \leq x \implies x = y$). Eine Halbordnung heißt **Totalordnung**
 $\iff \forall x, y \in M : x \leq y \vee y \leq x$.

Definition 0.42. Sei (M, \leq) eine halbgeordnete Menge.

(a) Eine Teilmenge $N \subseteq M$ heißt **Kette** $\iff (N, \leq|_{N \times N})$ ist eine Totalordnung.

(b) Eine Teilmenge $P \subseteq M$ besitzt eine obere Schranke (in M) $\iff \exists m \in M$, sodass $\forall p \in P : p \leq m$.

(c) $m \in M$ heißt maximales Element $\iff \nexists m' \in M : m' > m$

Beispiel. (a) Ist M eine beliebige Menge und $\mathcal{P}(M)$ eine Potenzmenge, so ist $(\mathcal{P}(M), \subseteq)$ eine Halbordnung. M ist obere Schranke für jede Teilmenge von $\mathcal{P}(M)$.

(b) \mathbb{N}_0 besitzt keine obere Schranke.

Wir betrachten nun die folgenden beiden Axiome der axiomatischen Mengenlehre:

Axiom (Zorn's Lemma). Sei (M, \leq) eine Halbordnung ($M \neq \emptyset$). Besitzt jede Kette in M eine obere Schranke, so besitzt M ein maximales Element. Dies nehmen wir als Axiom an.

Axiom (Auswahlaxiom). Ist I eine Menge und $(A_i)_{i \in I}$ eine Familie von nichtleeren Mengen (indiziert mit I), so \exists Funktion $f : I \rightarrow \bigcup_{i \in I} A_i$, mit $f(i) \in A_i$.

Satz (Halmos, Naive Set Theory, 62-65). Zorn's Lemma $(\forall(M, \leq))$ und das Auswahlaxiom $(\forall I, \forall(A_i)_{i \in I})$ sind äquivalent.

Satz 0.43. Sei $I \subseteq R$ ein echtes Ideal, dann \exists maximales Ideal $M \subsetneq R$ mit $I \subseteq M$. Insbesondere hat R maximale Ideale (Satz für $I = (0)$)

Beweis. Sei X die Menge aller Ideale $J \subsetneq R$ mit $I \subseteq J$. Wegen $I \in X$ gilt $X \neq \emptyset$. (X, \subseteq) ist halbgeordnete Menge.

Behauptung: Zorn's Lemma ist anwendbar.

Denn: Sei $X_0 \subseteq X$ eine Kette (o.E. $X_0 \neq \emptyset$). Definiere $J_\infty := \bigcup_{J \in X_0} J$.

Zu zeigen: $J_\infty \in X \implies J_\infty$ ist obere Schranke von X_0 . Klar ist $I \subseteq J_\infty$ und $1 \notin J_\infty (\implies J_\infty \subsetneq R)$

Zu zeigen: J_∞ ist ein Ideal. Seien $a, b \in J_\infty$ und $r \in R$. Nach Definition von $J_\infty \exists J, J' \in X_0$ mit $a \in J, b \in J'$. Nun ist aber X_0 totalgeordnet unter \subseteq . D.h. $J \subseteq J'$ oder $J' \subseteq J$. o.E. $J' \subseteq J \implies a, b \in J \implies a + b, r \cdot a \in J \implies a + b, ra \in J_\infty$, da $J \subseteq J_\infty$, damit ist die Behauptung gezeigt.

Sei M ein maximales Element von X . Dann ist M ein maximales Ideal von R (mit $I \subseteq M$) sonst $\exists J'' \subsetneq R$ ideal mit $M \subsetneq J''$, Widerspruch zu M maximales Element in X . \square

Übung. (Plenarübung 3) Zorn's Lemma \implies jeder Vektorraum hat eine Basis.

0.6 Teilbarkeit in Integritätsbereichen

Definition 0.44. Sei bis auf Weiteres R ein Integritätsbereich, $a, b \in R$.

(a) a ist Teiler von b (a teilt b , $a \mid b$): $\iff \exists c \in R : a \cdot c = b$.

(b) a, b sind assoziiert ($a \simeq b$): $\iff \exists c \in R^\times : a \cdot c = b$.

(c) a heißt irreduzibel (bzw. unzerlegbar) : $\iff a \in R \setminus (R^\times \cup \{0\})$ und $\forall c \in R : c \mid a \implies c \simeq a \vee c \simeq 1$.

(d) a heißt Primelement : $\iff a \in R \setminus (R^\times \cup \{0\})$ und $\forall b, c \in R : a \mid bc \implies a \mid b \vee a \mid c$.

Bemerkung 0.45 (Übung).

(a) $a \mid b \iff (b) \subseteq (a)$.

(b) $a \simeq b \iff a \mid b \wedge b \mid a \iff (a) = (b)$ und \simeq ist eine Äquivalenzrelation. (“denn:” $(R^\times, 1, \cdot)$ ist eine Gruppe).

(c) $Ra = (a) = (0) \iff a = 0$. $Ra = (1) \iff a \in R^\times \iff a \simeq 1$

(d) a Primelement $\iff (a)$ ist ein Primideal.

(e) a ist irreduzibel $\iff (0) \subsetneq (a) \subsetneq R$ und $\nexists b \in R : (a) \subsetneq (b) \subsetneq R$. (d.h. (a) ist maximal unter den Hauptidealen) und $a \in R \setminus (R^\times \cup \{0\})$ ist reduzibel $\iff \exists b, c \in R \setminus (R^\times \cup \{0\}) : a = b \cdot c \iff \exists b, c \in R : a = b \cdot c$ und $(a) \subsetneq (b), (c) \subsetneq R$.

(f) a Primelement $\implies a$ ist irreduzibel.

Beweis zu (f). Annahme: a ist reduzibel. Nach letzte Formulierung von (c) $\exists b, c \in R : a = b \cdot c \wedge (a) \subsetneq (b), (c) \subsetneq R \implies$ in $R_{/(a)}$ gilt $\bar{0} = \bar{a} = \bar{b} \cdot \bar{c}$ und $\bar{0} \neq \bar{b}, \bar{c} \implies R_{/(a)}$ kein Integritätsbereich $\implies (a)$ kein Primideal, Widerspruch zu (d), da a Primelement. \square

Definition 0.46 (Hauptidealring). Ein Integritätsbereich heißt **Hauptidealring** (HI-Ring), wenn jedes Ideal ein Hauptideal ist.

Definition 0.47. Ein Integritätsbereich R heißt **euklidischer Ring**, wenn $\exists \lambda : R \setminus \{0\} \rightarrow \mathbb{N}_0$, sodass gilt:

$$\forall a, b \in R \exists q, r \in R : a = qb + r, (r = 0 \vee \lambda(r) < \lambda(b)) \quad (*)$$

Bezeichnung.

(a) $(*)$ heißt Division mit Rest.

(b) λ heißt euklidische Funktion.

Beispiel 0.48. (a) \mathbb{Z} ist ein euklidischer Ring mit

$$\lambda : \cdot : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}_0, n \mapsto |n|$$

(b) $K[X]$ ist ein euklidischer Ring mit

$$\lambda = \text{Grad} : K[X] \setminus \{0\} \rightarrow \mathbb{N}_0, f \mapsto \text{Grad } f$$

Proposition 0.49. Ist R ein euklidischer Ring $\implies R$ ist ein Hauptidealring.

Beweis. Sei $I \neq \{0\}$ ein Ideal. Sei $a \in I \setminus \{0\}$ ein Element, sodass

$$\lambda(a) = \min\{\lambda(b) \mid b \in I \setminus \{0\}\} \subsetneq \mathbb{N}_0$$

Behauptung: $I = (a)$ ($I \supseteq$ klar, da $a \in I$).

Dazu: Sei $b \in I$ beliebig. Wende Division mit Rest an

$$b = qa + r, \quad r = 0 \vee \lambda(r) < \lambda(a)$$

$$\implies r = b - qa \in I - I \subseteq I \implies b = qa \in (a). \quad \square$$

Proposition 0.50. Sei R ein Hauptidealring und $a \in R \setminus (R^\times \cup \{0\})$, dann sind äquivalent:

- (i) a irreduzibel.
- (ii) a Primelement.
- (iii) (a) ist Primideal.
- (iv) (a) ist maximales Ideal.
- (v) $R/(a)$ ist ein Körper.

Beweis. • (iv) \iff (v) folgt aus Bemerkung 40(c)

- (i) \implies (iv) folgt aus Bemerkung 45(e) (a irreduzibel $\implies (a)$ ist maximal unter Hauptidealen)
- (iv) \implies (iii) folgt aus Bemerkung 40(d)
- (iii) \implies (ii) folgt aus Bemerkung 45(d)
- (ii) \implies (i) folgt aus Bemerkung 45(f)

\square

Definition 0.51. Seien $a, b \in R$

- (a) $d \in R$ heißt ggT (**größter gemeinsamer Teiler**) von a, b , wenn $d \mid a, d \mid b$ und $\forall c \in R : c \mid a, c \mid b \implies c \mid d$.
- (b) $d \in R$ heißt kgV (**kleinstes gemeinsames Vielfaches**) von a, b , wenn $a \mid d, b \mid d$ und $\forall c \in R : a \mid c, b \mid c \implies d \mid c$.
- (c) a, b heißen **teilerfremd**, wenn $\text{ggT}(a, b) \simeq 1$.

Bemerkung (Übung). ggT und kgV sind (sofern sie existieren) eindeutig bis auf Assoziiertheit.

Notation. $d \simeq \text{ggT}(a, b)$ bedeutet d ist ggT von a, b . $d \simeq \text{kgV}(a, b)$ bedeutet d ist kgV von a, b .

Konvention 0.52. Sei $K[X]_+ = \{f \in K[X] \setminus \{0\} \mid f \text{ normiert}\} \cup \{0\}$. In $\left\{ \begin{smallmatrix} \mathbb{Z} \\ K[X] \end{smallmatrix} \right\}$ ist jedes Element zu einem eindeutigen Element in $\left\{ \begin{smallmatrix} \mathbb{N}_0 \\ K[X]_+ \end{smallmatrix} \right\}$ assoziiert. Für $f, g \in \left\{ \begin{smallmatrix} \mathbb{Z} \\ K[X] \end{smallmatrix} \right\}$ schreibe $d = \text{ggT}(f, g)$ bzw. $d = \text{kgV}(f, g)$ $\iff d \simeq \text{ggT}(f, g)$ bzw. $d \simeq \text{kgV}(f, g)$ und $d \in \left\{ \begin{smallmatrix} \mathbb{N}_0 \\ K[X]_+ \end{smallmatrix} \right\}$.

Satz 0.53. Sei R ein Hauptidealring, dann gelten für $a, b, c \in R$:

$$(a) \quad (i) \quad c \simeq \text{ggT}(a, b) \iff (ii) \quad (c) = (a) + (b)$$

$$(b) \quad (i) \quad c = \text{kgV}(a, b) \iff (ii) \quad (c) = (a) \cap (b)$$

$$(c) \quad \text{ggT}(a, b) \text{ und } \text{kgV}(a, b) \text{ existieren } \forall a, b \in R$$

$$(d) \text{ Es sind \u00c4quivalent: } (i) \quad \text{ggT}(a, b) \simeq 1 \text{ (} a, b \text{ teilerfremd) } \iff (ii) \quad (a) + (b) = R \iff (iii) \quad \exists \alpha, \beta \in R : \alpha a + \beta b = 1$$

Beweis. (\"Ubung)

□

Bemerkung. (a) Hauptidealringe haben die Bezout-Eigenschaft, d.h. zu $a, b \in R$ $\exists \alpha, \beta \in R : \alpha a + \beta b \simeq \text{ggT}(a, b)$.

(b) In euklidischen Ringen kann man den ggT mit dem euklidischen Algorithmus berechnen und α, β wie in (a) mit dem erweiterten euklidischen Algorithmus.