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) $\mathbb{Z}_n^\times = \{\overline{a} \mid \mathrm{ggT}(a, n) = 1\}$, wobei $\mathbb{Z}_n = \mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}/_{(n)}$

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

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

φ ist ein Ringisomorphismus $\iff$ φ ist bijektiver Ringhomomorphismus $\underset{\text{Übung}}{\iff}$ $\exists \varphi' : R' \xrightarrow{\text{Ringhom.}} R$, sodass $\varphi \circ \varphi' = \mathrm{id}_{R'}$ und $\varphi' \circ \varphi = \mathrm{id}_R$. In diesem Fall schreibe $R \cong R'$ (R isomorph zu R').

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

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

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

(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.

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

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

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 $x : I \to X, i \mapsto x - I$. Schreibe X^I für die Menge aller Folgen in X über I ($= \mathrm{Abb}(I, X)$)

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 $M \to \{0\} \subseteq R$

(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 $+, \cdot : R[M] \times R[M] \to R[M]$ 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.

a) $(R[M], \underline{0}, \underline{1}, +, \cdot)$ ist ein Ring, ($R[M]$ heißt **Monoidring** zu M über R)

b) Ist M abelsch, so ist $R[M]$ kommutativ.

c) Ist $\varphi : R \to S$ ein Ringhomomorphismus und $\sigma : M \to (S, 1, \cdot)$ ein Monoidhomomorphismus, so $\exists!$ Ringhomomorphismus $\psi : R[M] \to S$ 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:

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

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

(iii) Für I eine beliebige Menge: $(\mathbb{N}_0^{(I)}, \underline{0}, \underline{+})$ 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 $\underline{+}$ komponentenweise Addition in $\mathbb{N}_0^{(I)}$.

Facts 0.6 (Übung)**.**

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

(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 $e_i : I \to \mathbb{N}_0$ 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

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

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

$$\sum a_i X^i + \sum b_i x^i = \sum (a_i + b_i) X^i$$

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

Proposition 0.7. *Die folgende Abbildung ist ein Ringisomorphismus.*

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

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

$$\underbrace{\left(\sum_{i\in\mathbb{N}_0} r_i\cdot i\right)}_{f\in R[\mathbb{N}_0]}\underbrace{\left(\sum_{j\in\mathbb{N}_0} s_j\cdot j\right)}_{g}\underset{\text{Nach Def.}}{=}\sum_{k\in\mathbb{N}_0} s_k\cdot k,\quad s_k$$

$$=\sum_{0\le i,j,i+j=k} r_is_j=\sum_{j=0}^{k} r_js_{k-j}$$

$$\implies \psi(f\cdot g)=\psi\left(\sum_k s_k\cdot k\right)=\sum_k g_kX^k$$

$$=\sum_i a_i\cdot\sum_j b_jX^j=\psi(f)\psi(g).\qquad\square$$

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

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

1. Beweis. Definiere $\widehat{\psi}(\sum_{i\ge0} r_iX^i):=\sum_{i\ge0}\underbrace{\psi(r_i)}_{\in S}s^i$. Dann die Behauptung nachprüfen. $\square$

2. Beweis. Facts 6(iii) $\exists!$ Monoidhomomorphismus $\sigma:\mathbb{N}_0\to(S,1,\cdot)$ mit $\sigma(1)=s$ und Übung 4(c) (universelle Eigenschaft des Monoidrings) $\exists!$ Ringhomomorphismus $\widehat{\psi}: R[\mathbb{N}_0]\to S$ mit $\widehat{\psi}|_R=\psi$ und $\widehat{\psi}|_{\mathbb{N}_0}=0$. Dieser erfüllt die Aussagen in Prop 8, denn $\widehat{\psi}(X)=\widehat{\psi}(1)=s$, X entspricht $1\in\mathbb{N}_0$ (Unter Isomorphismus von Proposition 7). Für $n\ge1$ Variable: $(n\in\mathbb{N})$

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

$\square$

Satz 0.9. *Sei* $\varphi:\mathbb{N}_0^n\to(R[X_1,\dots X_n],1,\cdot)$ *der eindeutige Monoidhomomorphismus mit* $\varphi(e_i)=X_i$*, wobei* $e_i=(\delta_{i,j})_j=(0,\cdots,1,\cdots0)$ *für* $i\in\{1,\dots,n\}$*. Dann ist (nach 4(c) eindeutige) Ringhomomorphismus* $\widehat{\psi}: R[\mathbb{N}_0^n]\to R[X_1,\dots,X_n]$ *mit* $\widehat{\psi}|_R=\mathrm{id}_R$ *und* $\widehat{\psi}|_{\mathbb{N}_0^n}=\varphi$ *ein Ringisomorphismus.*

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

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 $(\mathbb{N}_0^{(I)}, \underline{0}, +)$ 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 Elemete 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 $\psi : R \to S$ und einer Folge $(s_i)_{i\in I}$ aus S über I $\exists!$ Ringhomomorphismus $\widehat{\psi} : T[X_i \mid i \in I] \to S$ mit $\widehat{\psi}|_R = \psi$ und $\widehat{\psi}(X_i) = s_i$*

Facts.

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

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

mit $\widehat{\psi}|_R = \mathrm{id}_R$ und $\widehat{\psi}(X_j) = X_j$ $(j \in J)$. Die Abbildung $\widehat{\psi}$ 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) $\operatorname{Grad}: R[X] \to \mathbb{N}_0 \cup \{-\infty\}$ ist die eindeutige Abbildung mit

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

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

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

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

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

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

$$(R[X])^\times = \{f \in R[X] \mid \exists g \in R[X] : fg = 1\}$$

$$\underset{\text{Übung}}{=} \{f \in R[X] \mid \operatorname{Grad}(f) = 0, \exists g \in R[X] : \operatorname{Grad} g = 0 : fg = 1\}$$

$$= \{f \in R \mid \exists g \in R : fg = 1\} = R^\times$$

0.2 Symmetrische Polynome

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

Bezeichnung. (a) Ein Monom in $R[X_1, ..., X_n]$ ist ein Polynom der Form $aX^m = aX_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$ für $a \in R \setminus \{0\}$ und $m = (m_i)_{i \in \{1,\ldots,n\}} \in \mathbb{N}_0^n$ 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 $\operatorname{Grad}(f) = \max\{|m| : a_m \neq 0\}$. ($\max(\emptyset) := -\infty$)

(c) $f \in R[X_1, \ldots X_n]$ 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 $\operatorname{Grad}(f) = 11$

(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* $\widetilde{\sigma} : R[X_1, \ldots, X_n] \to R[X_1, \ldots, X_n]$ *mit* $\widetilde{s}|_R = \mathrm{id}_R$ *und* $\widetilde{\sigma}(X_i) = X_{\sigma(i)}$ *für* $i \in \{1, \ldots, n\}$

(b) $\widetilde{\mathrm{id}} = \mathrm{id}_{R[X_1,\ldots,X_n]}$ *(für* $\mathrm{id} \in S_n$ *die Eins).*

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

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

(b) $\alpha := \mathrm{id}_{R[X_1,\dots,X_n]}$ ist ein Ringhomomorphismus $R[X_1,\dots,X_n] \to R[X_1,\dots,X_n]$ mit $\alpha|_R = \mathrm{id}_R$ und $\alpha(X_i) = X_i \overset{(a)}{\Longrightarrow} \alpha = \widetilde{\mathrm{id}}$.

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

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

und

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

$$\underset{\text{in (a)}}{\overset{\text{Eindeutigkeit}}{\Longrightarrow}} \widetilde{\sigma \circ \tau} = \widetilde{\sigma} \circ \widetilde{\tau}.$$ □

Bemerkung (Übung)**.** Ist $\alpha : R \to R$ 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*

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

ist wohl-definiert und ein injektiver Gruppenhomomorphismus.

Beweis.

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

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

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

2) Gruppenhomomorphismus: folgt aus 12(c)

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

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*

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

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

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 $\widetilde{\sigma}$ eine Bijektion auf $\{X_1, ..., X_n\}$ definiert. $\square$

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

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

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

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

Insbesondere:

(i) $s_1, ..., s_n \in R[X_1, \ldots, X_n]^{S_n}$

(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:

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

$$s_i(X_1, ..., X_n) = \sum_{1 \le j_1 < j_2 < \cdots < j_i \le n} X_{j_1} X_{j_2} \cdots X_{j_i}$$

$(n = 3, i = 2 \rightsquigarrow s_2 = X_1X_2 + X_1X_3 + X_2X_3)$

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

Satz 0.19. *Sei* $\psi : R[Y_1, \ldots, Y_n] \to R[X_1, \ldots, X_n]$ *der Ringhomomorphismus*

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

Dann gilt

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

(b) ψ *definiert einen Ringisomorphismus*

$$R[Y_1, \ldots, Y_n] \to R[X_1, \ldots, X_n]^{S_n}$$

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

$$(\underbrace{X_1 + \cdots + X_4}_{s_1})^2 - 2(\underbrace{X_1X_2 + X_1X_3 + X_2X_3 + X_1X_4 + X_2X_4 + X_3X_4}_{s_2})$$

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

Wiederholung.

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

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

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

Beweis. (zu Satz 3.19)

Teil (a) Klar

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

Teil (b) benötigt Vorbereitungen.

□

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

Definition 0.20 (Lex-Ordnung)**.**

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

$$X^\ell \le X^m \iff \ell \le m$$

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

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

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

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

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

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

(b) $\mathrm{in}(f \cdot g) \le \ell_0 + m_0$ *und es gilt* $\mathrm{in}(f \cdot g) = \ell_0 + m_0$ *falls die Leitkoeffizienten* $a_{\ell_0} \cdot b_{m_0} \ne 0$.

(c) $\mathrm{in}(f \cdot g) \le \max \mathrm{in}(f), \mathrm{in}(g)$ *und es gilt Gleichheit falls* $\mathrm{in}(f) \ne \mathrm{in}(g)$.

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

(e) *$\xi_1, \dots, \xi_n$ sind linear unabhängig als Elemente von $\mathbb{Q}^n$, und also ist φ_i : $\mathbb{N}_0^n \to \mathbb{N}_0^n, (a_i) \mapsto \sum a_i\xi_i$ 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. $\underset{(a)}{\implies} \ell + m \geq \ell_0 + m_0 \implies \mathrm{in}(f \cdot g) \leq \ell_0 + m_0$.

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 $\mathrm{in}(fg) = m_0 + \ell_0$, 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 $m_0 \geq \mathrm{in}(f)$, und $b_{m_0} \neq 0$, da $m_0 = \mathrm{in}(f)$. Also folgt $\mathrm{in}(f + g) = \max\{\ell_0, m_0\}$.

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

(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}

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

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:

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

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

d.h. $D(f)$ erkennt ob merhfache 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 $\varphi : R \to R'$ 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)
$$\varphi(I) + \varphi(I) = \{\underbrace{\varphi(a) + \varphi(b)}_{\varphi(a+b)} \mid a, b \in I\} = \varphi(I + I) \underset{I+I\subseteq I}{\subseteq} \varphi(I)$$

(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. □

Definition 0.25 (Charakteristik)**.** Die Charakteristik von R ist

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

Beispiel.
$\mathrm{char}(\mathbb{Z}) = 0, \mathrm{char}({}^{Z}\!/_{nZ}) = n, n \in \mathbb{N}$

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

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

(b) Sei $\varphi : \mathbb{Z} \to R$ 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: $\mathrm{char}(R)$ ist der (eindeutige) Erzeuger in $\mathbb{N}$ von $\mathrm{Kern}(\varphi) \subseteq \mathbb{Z}$ (ein Ideal) ("Grund für die Definition von $\mathrm{char}(R)$")

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

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

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 $n, m < n \cdot m = \operatorname{char} K$. 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 $\operatorname{char}(R) = p$ eine Primzahl, dann gelten:

(a) $\varphi_R = R \to R, a \mapsto a^p$ ist ein Ringhomomorphismus.

(b) Es gilt $\varphi_{\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}$, 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 Faktorring R/I und Faktorabbildung $\pi : R \to R/I, r \mapsto r + I$ (vgl. Satz 1.49)

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

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

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & R' \\
R/I \arrow[ur, "\overline{\varphi}"'] &
\end{tikzcd}$$

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

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

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

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

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

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

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

ein Ringisomorphismus.

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

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 $I_1, \ldots, I_t \subseteq R$ Ideale, die "paarweise Koprim" sind, d.h. $I_i + I_j = R$ für $i \neq j \in \{1, \ldots, t\}$. Dann gelten:*

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

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

(c) Die Abbildung

$$R \big/ \textstyle\prod_{i \in \{1,\ldots,t\}} I_i = R \big/ I_1 \cdot \ldots \cdot I_t \xrightarrow{\cong} \displaystyle\bigtimes_{i \in \{1,\ldots,t\}} R \big/ I_i = R \big/ I_1 \times \cdots \times R \big/ I_t$$

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

ist wohl-definiert und ein Ringisomorphismus. Also gilt

$$R \big/ \textstyle\prod_{i \in \{1,\ldots,t\}} I_i \cong \displaystyle\bigtimes_{i \in \{1,\ldots,t\}} R \big/ I_i$$

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

0.4 Ringe von Brüchen/Lokalisierung

Definition 0.30. Eine Teilmenge $S \subseteq R$ heißt multiplikativ abgeschlossen $\Longleftrightarrow$ 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

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

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 $tt'ss's''$

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

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

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

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

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

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

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

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

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

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

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

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

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

$\square$

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 Itdentitätsbereich $\iff$ man darf in R kürzen und $0_R \neq 1_R$

$$\underset{\text{Übung}}{\iff} \forall a, b, c \in R : a \neq 0 : a \cdot b = a \cdot c \implies b = c$$

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) $R \to S^{-1}R$ 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 $\frac{r}{s} \in S^{-1}R \backslash \{\frac{0}{1}\}$, 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)**.** $S^{-1}R = \mathrm{Quot}(R)$ heißt Quotientenkörper von R.

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

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-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-Ring und $\forall \overline{a}, \overline{b} \in {}^{R}\!/_{P} :$

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

$\implies {}^{R}\!/_{P}$ ist ein Integritätsbereich. Man kann auch "rückwarts laufen" $\implies$ die Äquivalenz in (a).

(b) Übung.

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

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

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 $f : I \to \bigcup_{i\in I} A_i$, 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. $X_0 \neq 0$). 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 $\forall c \in R : c \mid a \implies c \simeq a \lor c \simeq 1$.

(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 $\overline{0} = \overline{a} = \overline{b} \cdot \overline{c}$ und $\overline{0} \neq \overline{b}, \overline{c} \implies {}^{R}\!/\!_{(a)}$ kein Integritätsbereich $\implies (a)$ kein Primideal, Widerspruch zu (d), da a Primelement. □

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 $\exists \lambda : R \setminus \{0\} \to \mathbb{N}_0$, 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

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

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

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

Proposition 0.49. *Ist R ein euklidischer Ringe $\implies$ 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

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

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

□

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)

□

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 $\mathrm{ggT}(a, b) \simeq 1$.

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

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

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

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

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

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

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

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

Beweis. (Übung) □

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

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

Satz/Definition 0.54. *Für einen Integritätsbereich R sind äquivalent:*

(i) $\forall a \in R \backslash (R^\times \cup \{0\}) \exists t \in \mathbb{N} \exists$ *Primelemente* $p_1, \ldots, p_t \in R$ *mit* $a \simeq p_1 \cdot \ldots \cdot p_t$

(ii) $\forall a \in R \setminus (R^\times \cup \{0\}) \exists t \in \mathbb{N} \exists$ *irreduzible Elemente* $p_1, \ldots, p_t \in R$ *mit* $a \simeq p_1 \cdot \ldots \cdot p_t$ *und diese Darstellung ist eindeutig bis auf Indexpermutation und Assoziiertheit, d.h. gilt* $a \simeq q_1 \cdot \ldots \cdot q_s$ *mit* $q_1, \ldots, q_s$ *irred., so gilt* $s = t$ *und nach Indexpermutation* $q_i \simeq p_i$ *für* $i = 1, \ldots, t$.

Ein Integritätsbereich, der (i) und (ii) erfüllt heißt faktorieller Ring (oder EPZ-Ring: Ring mit eindeutiger Primfaktorzerlgung)

Bemerkung.

(a) (i) $\implies$ irred. Elemente in R sind Primelemente. Denn: Sei q irred. in R, schreibe Faktorisierung wie in (i) für q, d.h. $q \simeq p_1 \cdot \ldots \cdot p_t \underset{q \text{ irred.}}{\implies} t = 1$ also $q \simeq p_1$. Primelement.

(b) In (b) ist R beliebiger Integritätsbereich (so zwigt man mit Induktion) Ist p ein Primelement in R und ein Teiler von $a_1 \cdot \ldots \cdot a_t$ (mit $a_i \in R$), so $\exists i \in \{1, \ldots, t\}$ mit $p | a_i$.

(c) Für R wie in 54 ist R faktoriell, so ist die Länge r einer Primfaktorzerlgung $r \simeq p_1 \cdot \ldots \cdot p_t$ (p_i prim) von $r \in R \setminus \{0\}$ unabhängig von der Faktorisierung (vgl (ii)). Schreibe $r(r) \in \mathbb{N}_0$ für diese Länge.

Beweis. (von Satz 54)

(i) $\implies$ (ii): Existenz der Faktorisierung in (ii) ist klar nach (i), da Primelemente irreduzibel sind.

Eindeutigkeit: Gelte $p_1 \cdot \ldots \cdot p_t \overset{(*)}{\simeq} q_1 \cdot \ldots \cdot q_t, s \in \mathbb{N}, p_i$ prim, q_i irred. Zeige mit Induktion über t: $s = t$ und nach Indexpermutation $q_i \simeq p_i$

- $t = 1$: $p_1 \simeq q_1 \cdot \ldots \cdot q_s \implies s = 1$ (p_1 prim, also irred.)

- $t-1 \to t$: $(*)$ und Bemerkung (b) $\Longrightarrow \exists j \in \{1,\dots,s\}$ mit $p_t \mid q_j$, o.E. $j = s$ (Umindizieren) und also $p_t \simeq q_s$ (q_s irreduzibel). teile beide Seiten durch p_t

$$p_1 \cdot \ldots \cdot p_{t-1} \simeq q_1 \cdot \ldots \cdot q_{s-1} \underbrace{u}_{\in R^\times} \simeq q_1 \cdot \ldots \cdot q_{s-1}$$

  Nun: wende Induktionsvoraussetzung an. $\Longrightarrow s-1 = t-1$ (also $s = t$) und nach Indexpermutation: $q_i \simeq p_i$ für $i = \{1,\dots,t-1\}$

(ii) $\Longrightarrow$ (i): Zeige irred. Elemente in R sind Primelemente. Sei also $q \in R$ irreduzibel. Seien weiter $a, b \in R$, sodass $q \mid ab$.

Zu zeigen: $q \mid a$ oder $q \mid b$: o.E. $a, b \neq 0$ (sonst $q \mid a \vee q \mid b$), o.E. $a, b \notin R^\times$, ist z.B. $a \in R^\times$, so folgt aus $q \mid ab$ direkt $q \mid b$. Sei $c \in R$ mit $qc = ab$. Schreibe c, a, b einer Faktorisierung wie in (ii) geg.

$$a \simeq p_1 \cdot \ldots \cdot p_t, \quad b \simeq q_1 \cdot \ldots \cdot q_s, \quad c \simeq r_1 \cdot \ldots \cdot r_u$$

(p_i, q_j, r_k irred. $t, s \in \mathbb{N}, u \in \mathbb{N}_0$)

$$qr_1 \cdot \ldots \cdot r_u \simeq p_1 \cdot \ldots \cdot p_t \cdot q_1 \cdot \ldots \cdot q_s$$

Wende Eindeutigkeitsaussage von (ii), um zu folgen:
$q \simeq p_i, i \in \{1,\dots,t\}$ oder $q \simeq q_j, j \in \{1,\dots,s\} \Longrightarrow q \mid a$ oder $q \mid b$. $\square$

Korollar 0.55 (Übung)**.** *Sei R ein faktorieller Ring und sei $\mathbb{P}$ ein Repräsentantensystem der Primelemente von R modulo Assoziiertheit, dann gelten:*

(a) $\forall p \in \mathbb{P}$ ist die Abbildung $v_p : R \setminus \{0\} \to \mathbb{N}_0, r \mapsto \max\{n \in \mathbb{N}_0 : p^n \mid r\}$ wohldefiniert (genauer $v_p(r) \leq t(r)$) und v_p ist ein Monoidhomomorphismus (für $(R, 1, \cdot)$)

(b) $\forall r \in R \setminus \{0\}$ gilt $\#\{p \in \mathbb{P} : p \mid r\} \leq t(r) < \infty$

(c) $\forall r \in R \setminus \{0\} \exists! u \in R^\times$:

$$r = u \prod_{p \in \mathbb{P}} p^{v_p(r)} = u \prod_{p \in P, v_p > 0} p^{v_p(r)}$$

(Primfaktorzerlgung von r)

(d) Für $r, s \in R \setminus \{0\}$ gilt:

$$r \mid s \iff \bigforall_{p \in \mathbb{P}} r_p(r) \leq v_p(s)$$

(e) Für $r, s \in R \setminus \{0\}$ gelten:

$$\mathrm{ggT}(r, s) \simeq \prod_{p \in \mathbb{P}} p^{\min(v_p(r), v_p(s))}, \quad \mathrm{kgV}(r, s) \simeq \prod_{p \in \mathbb{P}} p^{\max(v_p(r), v_p(s))}$$

(ggT und kgV existieren also in faktoriellen Ringen)

(f) Sei $K = \mathrm{Quot}(R)$, dann $\exists!$ Fortsetzung $v_p : K^\times \to \mathbb{Z}$ (ein Gruppenhomomorphismus, der den Monoidhomomorphismus $v_p : R \setminus \{0\} \to \mathbb{N}_0$ fortsetzt) und $\forall r \in K^\times \exists! u \in R^\times$:

$$r = u \prod_{p \in \mathbb{P}} p^{v_p(r)}$$

(dabei $\#\{p : v_p(r) \neq 0\}$ endlich.)

Übung 0.56 (vgl. LA2)**.** Für einen (beliebigen kommutativen) Ring R sind äquivalent:

(a) Jede aufsteigende Kette von Idealen

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots \subseteq R$$

($\mathbb{N}_0$ indiziert) wird stationär, d.h. $\exists n_0 : \forall n \in n_0 : I_n = I_{n_0}$

(b) Jede nichtleere Teilmenge $\mathscr{M}$ von Idealen enthält ein bzgl. der Inklusion maximales Element.

(c) Jedes Ideal $I \subseteq R$ ist endlich erzeugt, d.h. $\exists n \in \mathbb{N} \exists a_1, \ldots, a_n \in R$ mit $I = (a_1, \ldots, a_n)$

Definition (Noetherscher Ring)**.** Gelten (a)-(c) für R, so heißt R **noethersch**

Bemerkung. R noethersch $\underset{\text{ohne Zorn's Lemma}}{\Longrightarrow}$ $\forall$ echte Ideal $I \subsetneq R \exists$ maximales Ideal mit $I \subseteq \mathscr{M}$ denn ein solches findet sich in $\mathscr{M} = \{J \subsetneq R \mid I \subseteq J\}$

Korollar 0.57. *Ist R ein HI-Ring, so gelten:*

(a) R ist noethersch.

(b) $\forall r \in R \setminus (R^\times \cup \{0\}) \exists t \in \mathbb{N} \exists$ Primelemente $p_1, \ldots, p_t \in R$, sodass $r \simeq p_1 \cdot \ldots \cdot p_t$

(c) R ist faktoriell.

Beweis. (a) folgt aus 56, da jedes Ideal von R ein Hauptideal ist.

(b) folgt aus (b).

(c) Bei HI-Ringen, wissen schon Primelemente sind irred. und umgekehrt. (Prop. 50). Zu zeigen: Sei $r \in R \setminus (R^\times \cup \{0\})$, dann existiert eine Faktorisierung wie in (b). Definiere:

$$\mathscr{M}_a := \{(b) \subseteq R \mid \exists t \in \mathbb{N}_0 \exists \underbrace{q_1, \ldots, q_t}_{\text{irred.}} \in R : bq_1 \cdot \ldots \cdot q_t \simeq a\}$$

$\mathscr{M}_a \neq \emptyset$: denn $(a) \in \mathscr{M}_a$ für $t = 0$. Sei nun $(b) \in \mathscr{M}_a$ ein maximales Element (bzgl. $\subseteq$). Behauptung: $(b) = R$ (Dann $b \simeq 1 \implies q_1 \cdot \ldots \cdot q_t \simeq a$ für Faktorisierung in Definition von $\mathscr{M}_a$ zu b). Dazu: Nehme an: $(b) \subsetneq R$, dann ist wegen R noethersch $\exists$ maximales Ideal $M \subsetneq R$ mit $(b) \subseteq M$, da R HI-Ring ist $M = (p)$ für p ein Primelement (Proposition 50) und aus $(b) \subseteq (p)$ folgt $p \mid b$ und $({}^{b}\!/_{p}) \supsetneq (b)$ (p keine Einheit) und $({}^{b}\!/_{p}) \in \mathscr{M}_a$, da ${}^{b}\!/_{p} \cdot p \cdot q_1 \cdot \ldots \cdot q_t \simeq a$. Widerspruch zur Maximalität von (b).

$\square$

Bemerkung. Nächstes Ziel R faktoriell $\implies R[X]$ faktoriell.

Proposition 0.58 (Übung)**.**

(a) Für einen kommutativen Ring R sind äquivalent:

(i) R ist ein Integritätsbereich.

(ii) $R[X]$ ist ein Integritätsbereich

(iii) $\forall f, g \in R[X]$ gilt: $\operatorname{Grad}(fg) = \operatorname{Grad} f + \operatorname{Grad} g$

(b) Ist R ein Integritätsbereich, so gilt $(R[X])^\times = R^\times$

Beweis. (a) Zeige (i) $\implies$ (iii) $\implies$ (ii) $\implies$ (i)

(b) $u \in R[X]^\times \implies \exists r : vu = 1$, dann Grad Identität anwenden... $\square$

Beispiel. $\mathbb{Z}[X]^\times = \mathbb{Z}^\times = \{\pm 1\}, K[X_1, X_2]^\times = K^\times$.

Definition 0.59. Sei bis auf Widerruf R ein faktorieller Ring mit Quotientenkörper $K = \operatorname{Quot}(R) \supseteq R$, $f = \sum_{i=0}^n a_i X^i \in KX \setminus \{0\}$ heißt primitiv wenn:

(a) $f \in R[X]$ (alle $a_i \in R$)

(b) $\operatorname{ggT}(a_0, \dots, a_n) \simeq 1$

Lemma 0.60. *Sei $f = \sum_{i=0}^n a_i X^i \in K[X] \setminus \{0\}$, dann:*

(a) $\exists c \in K^\times \exists g \in K[X] \setminus \{0\}$ primitiv, so dass $f = cg$

(b) Gelte $cg = c'g'$ mit $c, c' \in R^\times, g, g' \in K[X] \setminus \{0\}$ primitive Polynome, so folgt $\frac{c}{c} \in R^\times$, d.h. c in (a) ist eindeutig bis auf Faktor in $R^\times$

Proof. Beweis

(a) Schreibe $a_i = \frac{b_i}{d_i}$ it $b_i \in R, d_i \in R \setminus \{0\}$ als gekürzten Bruch (d.h. $\operatorname{ggT}(b_i, d_i) \simeq 1$ geht R faktoriell.)
Sei $d = \operatorname{kgV}(d_0, \dots, d_n)$ (Hauptnenner), $b = \operatorname{ggT}(b_0, \dots, b_n)$. Es folgt $g := f \cdot \frac{a}{b} = \sum_{i=0}^n \left(\frac{b_i}{b} \cdot \frac{d}{d_i} \right) X^i \in R[X] (\setminus \{0\})$.
Behauptung: g ist primitiv. $\left(\implies c = \frac{b}{d} = \frac{\operatorname{ggT}(b_0, \dots, b_n)}{\operatorname{kgV}(d_0, \dots, d_n)} \right)$.
Annahme: g ist nicht primitiv. Dann $\exists$ Primelement $p \in R$, sodass $p \mid \frac{b_i}{b} \cdot \frac{d}{d_i}, \forall i$. Nach der Wahl von b gilt $\frac{b_0}{b}, \dots, \frac{b_n}{b}$ sind insgesamt teilerfremd $\implies \exists i : p \not| \frac{b_i}{b} \implies \exists i : p \mid \frac{d}{d_i} \implies p \mid d$. Sei $k = v_p(d)$, d.h. p^k teilt $d, p^{k+1} \not| d \underset{d = \operatorname{kgV}(\dots)}{\implies} \exists i : p^k \mid d_i, p^{k+1} \not| d_j, j \in \{0, \dots, n\}$, sei dieses i_0.
Insbesondere ist $p \mid d_{i_0}$.
Beachte: $\frac{b_{i_0}}{d_{i_0}}$ gekürzter Bruch $\implies p \not| b_{i_0}$, aber nach Voraussetsung (g nicht primitiv) p teilt $\frac{b_{i_0}}{b} \cdot \frac{d}{d_{i_0}}$. Widerspruch, da p kein Teiler von b oder d_{i_0} ist.

(b) Haben $c \cdot g = c' \cdot g'$ für $c, c' \in K^\times, g, g'$ primitiv. Schreibe $u = \frac{c'}{c}$ als gekürzter Bruch $u = \frac{d'}{d} \implies d \cdot h = d' \cdot g' = d \cdot \sum b_i X^i = d' \cdot \sum b_i' X^i$. g, g' primitiv heißt $\implies d = \operatorname{ggT}(b_0 d, \dots, b_n d) = \operatorname{ggT}(b_0' d', \dots, b_n' d') = d' \implies \frac{d'}{d} \in R^\times$ und $\frac{c'}{c} = \frac{d'}{d}$.

$\square$