0.1 Ringe

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 $(S_{em})_{m\in M}$ mit $S_{em} = \begin{cases} 1, & m = e, \\ 0, & m \neq e. \end{cases}$

(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)

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

(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

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

$$= \sum_{0\leq i,j,i+j=k} r_i s_j = \sum_{j=0}^{k} r_j s_{k-j}$$

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

$$= \sum_i a_i \cdot \sum_j b_j X^j = \psi(f)\psi(g).$$

□

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 $\widehat{\psi}(\sum_{i\geq 0} r_i X^i) := \sum_{i\geq 0} \underbrace{\psi(r_i)}_{\in S} s^i$. Dann die Behauptung nachprüfen. □

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 $n \geq 1$ Variable: $(n \in \mathbb{N})$

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

□

Satz 0.9. *Sei* $\varphi : \mathbb{N}_0^n \to (R[X_1, \ldots X_n], 1, \cdot)$ *der eindeutige Monoidhomomorphismus mit* $\varphi(e_i) = X_i$*, wobei* $e_i = (\delta_{i,j})_j = (0, \cdots, 1, \cdots 0)$ *für* $i \in \{1, \ldots, n\}$*. Dann ist (nach 4(c) eindeutige) Ringhomomorphismus* $\widehat{\psi} : R[\mathbb{N}_0^n] \to R[X_1, \ldots, X_n]$ *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 $X_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$ □

Definition 0.10. 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 (Primitive Monomen)**.** 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) Grad : $R[X] \to \mathbb{N}_0 \cup \{-\infty\}$ ist die eindeutige Abbildung mit

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

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

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

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

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

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

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

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

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

0.3 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 $\mathrm{Grad}(f) = \max\{|m| : a_m \neq 0\}$. ($\max(\emptyset) := -\infty$)

(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 $\mathrm{Grad}(f) = 11$

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

(c) Wende universelle Eigenschaft von $R[X_1,\ldots,X_n]$ 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. *$R[X_1,\ldots,X_n]^{S_n} := \{f \in R[X_1,\ldots,X_n] \mid \widetilde{\sigma}(f) = f, \forall \sigma \in S_n\} = \bigcap_{\sigma\in S_n} R[X_1,\ldots,X_n]^{\widetilde{\sigma}}$ ist ein Unterring von $R[X_1,\ldots,X_n]$.*

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

Korollar 0.16. *Die Abbildung*

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

ist wohl-definiert und ein injektiver Gruppenhomomorphismus.

Beweis.

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

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

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

2) Gruppenhomomorphismus: folgt aus 12(c)

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

□

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

0.4 Elementar symmetrische Polynome

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

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

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

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:

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

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

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

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 ist

(a) ψ *ist Ringhomomorphismus mit* $\operatorname{Kern}(\psi) \subseteq R[X_1, ..., X_n]^{S_n}$

(b) ψ *ist ein Ringisomorphismus.*

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

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

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