Definition

2.5.4 Proposition: *(Universelle Eigenschaft)* Für jeden Ring S, jeden Ringhomomorphismus $\varphi\colon R \to S$, und jedes System $\underline{x} = (x_\nu)_\nu \in S^n$ existiert genau ein Ringhomomorphismus $\varphi_{\underline{x}}\colon R[\underline{X}] \to S$ mit $\varphi_{\underline{x}} \circ \iota = \varphi$ und $\varphi_{\underline{x}}(X_\nu) = x_\nu$ für alle $1 \leqslant \nu \leqslant n$, das heisst, so dass das folgende Diagramm kommutiert:

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, "\iota"'] & S & \ni & x_\nu \\
R[\underline{X}] \arrow[ur, dotted, "\varphi_{\underline{x}}"'] & \ni & X_\nu \arrow[ur, mapsto] &
\end{tikzcd}$$

$\underline{X}^{\underline{i}} = \prod_{\nu=1}^{n} X_\nu^{i_\nu} \longmapsto \prod_{\nu=1}^{n} x_\nu^{i_\nu} = \underline{x}^{\underline{i}}$

Genauer ist $\varphi_{\underline{x}}$ die *Auswertungsabbildung*

$$R[\underline{X}] \to S,\ \ F(\underline{X}) = \sideset{}{'}\sum_{\underline{i} \in I_n} a_{\underline{i}} \underline{X}^{\underline{i}} \mapsto \boxed{F(\underline{x}) :=} \sideset{}{'}\sum_{\underline{i} \in I_n} \varphi(a_{\underline{i}}) \underline{x}^{\underline{i}}.$$

Wir nennen $F(\underline{x})$ den *Wert von F an der Stelle $\underline{x}$*. Jedes Polynom F induziert somit für jedes $\varphi\colon R \to S$ eine *Polynomfunktion*

$$S^n \to S,\ \underline{x} \mapsto F(\underline{x}).$$

Bew.: Eindeutigkeit ✓

Diese Formel definiert einen Ringhomo mit den gewünschten Eigenschaften.

2.5.5 Vorsicht: Ist R endlich, so können verschiedene Polynome über R dieselbe Polynomfunktion $R \to R$ induzieren, z.B. die beiden Polynome 0 und $\prod_{x \in R}(X - x)$. Ein Polynom ist also etwas grundsätzlich Anderes als eine Polynomfunktion. Dagegen gilt:

2.5.6 Proposition: Sei K ein unendlicher Körper. Dann ist jedes Polynom f über K durch die induzierte Polynomfunktion $K^n \to K$ eindeutig bestimmt.

Bew.: $n=0 \Rightarrow K[\underline{X}] = K \ni f \mapsto K^n = \{0\} \to K,\ 0 \mapsto f$. ✓

$n=1 \Rightarrow 0 \neq f \in K[X]$ hat höchstens endlich viele Nullstellen $\Rightarrow$ induzierte Funktion $\neq 0$.

$\Rightarrow \operatorname{Kern}\big(K[X] \to \operatorname{Abb}(K,K),\ f \mapsto (x \mapsto f(x))\big) = 0 \Rightarrow$ diese Abb. ist injektiv,

$n \mapsto n+1$: Schreibe $f = \sum_{j \geq 0} f_j \cdot X_{n+1}^j$ mit $f_j \in K[X_1,\ldots,X_n]$. Für alle $\xi_1,\ldots,\xi_n \in K$ betrachte $f(\xi_1,\ldots,\xi_n,X_{n+1}) \in K[X_{n+1}]$. Dies ist durch die Polynomfunktion bestimmt $\Rightarrow f_j(\xi_1,\ldots,\xi_n) \in K$ ist bestimmt für jedes j. IA $\Rightarrow f_j$ bestimmt $\Rightarrow f$ bestimmt. qed.

2.5.7 Bemerkung: Alternativ könnte man $R[\underline{X}]$ durch die universelle Eigenschaft abstrakt definieren und zeigen, dass er dadurch bis auf eindeutige Isomorphie bestimmt ist.

2.5.8 Proposition: Für alle $0 \leqslant m \leqslant n$ existiert ein natürlicher Isomorphismus

$$R[X_1,\ldots,X_n] \;\cong\; R[X_1,\ldots,X_m][X_{m+1},\ldots,X_n].$$

Bew.: Idee:

$$\sum_{\underline{i} \in (\mathbb{Z}^{\geq 0})^n} a_{\underline{i}} \cdot X_1^{i_1} \cdots X_n^{i_n} = \sum_{i_{m+1},\ldots,i_n \in \mathbb{Z}^{\geq 0}} \Big(\sum_{i_1,\ldots,i_m \geq 0} a_{(i_1,\ldots,i_n)} X_1^{i_1} \cdots X_m^{i_m} \Big) \cdot X_{m+1}^{i_{m+1}} \cdots X_n^{i_n}$$

qed.

2.5.9 Proposition: *(Funktorialität)* Jeder Ringhomomorphismus $\varphi\colon R \to S$ induziert einen eindeutigen Ringhomomorphismus $\tilde{\varphi}\colon R[\underline{X}] \to S[\underline{X}]$ mit $\tilde{\varphi}|_R = \varphi$ und $\tilde{\varphi}(X_\nu) = X_\nu$, nämlich

$$\boxed{\sideset{}{'}\sum_{\underline{i}\in I_n} a_{\underline{i}}\underline{X}^{\underline{i}} \mapsto \sideset{}{'}\sum_{\underline{i}\in I_n} \varphi(a_{\underline{i}})\underline{X}^{\underline{i}}.}$$

2.5.10 Proposition: Seien K ein Körper und V ein K-Vektorraum mit Basis $\underline{X} = (X_\nu)_{\nu=1}^n$. Dann existiert ein natürlicher Isomorphismus auf die symmetrische Algebra

$$K[\underline{X}] \xrightarrow{\sim} SV := \bigoplus_{r\geqslant 0} S^r V, \quad \boxed{\sideset{}{'}\sum_{\underline{i}\in I_n} a_{\underline{i}}\underline{X}^{\underline{i}} \mapsto \sideset{}{'}\sum_{\underline{i}\in I_n} a_{\underline{i}}\underline{X}^{\underline{i}}.}$$

Erinn.: $\forall r \geq 0$: $\left\{ X_1^{i_1} \cdots X_n^{i_n} = \underline{X}^{\underline{i}} \;\middle|\; \begin{array}{l} i_1, \dots, i_n \geq 0 \\ i_1 + \dots + i_n = r \end{array} \right\}$ Basis von $S^r V$.

$\Rightarrow$ $\{ \underline{X}^{\underline{i}} \mid i_1, \dots, i_n \geq 0 \}$ Basis von SV.

Vektorraum-Iso., Ringhomom.

qed.

2.5.11 Variante: Für $\underline{X} = (X_1, \ldots, X_n)$ sei $R[[\underline{X}]]$ die Menge aller Abbildungen $(\mathbb{Z}^{\geqslant 0})^n \to R$, $\underline{i} \mapsto a_{\underline{i}}$, ohne Endlichkeitsbedingungen. Definiere Summe und Produkt zweier Elemente von $R[[\underline{X}]]$ sowie die Inklusion $\iota\colon R \hookrightarrow R[[\underline{X}]]$ durch die gleichen Formeln wie oben.

2.5.12 Proposition: $(R[[\underline{X}]], +, \cdot, 0, 1)$ ist ein Ring und ι ein injektiver Ringhomomorphismus.

Wieder identifizieren wir R mit seinem Bild unter ι. Ein Element von $R[[\underline{X}]]$ schreiben wir in der Form

$$(a_{\underline{i}})_{\underline{i}} = \sum_{\underline{i} \in I_n} a_{\underline{i}} \underline{X}^{\underline{i}},$$

was aber nur als Notation und nicht als irgendeine Art von unendlicher Summe oder Reihe zu verstehen ist. Einen solchen Ausdruck nennen wir eine *formale Potenzreihe in den Variablen $X_1, \ldots, X_n$ über R.* Mit dieser Notation unterliegen alle Rechnungen denselben Regeln wie für Potenzreihen in der Analysis.

2.5.13 Bemerkung: Wir haben natürliche Einbettungen $R \subset R[\underline{X}] \subset R[[\underline{X}]]$.

2.5.14 Variante: Sei N eine beliebige, möglicherweise unendliche, Menge. Dann konstruieren wir den *Polynomring $R[\underline{X}]$ über R in den Variablen X_ν für alle $\nu \in N$* wie folgt.

Sei I_N die Menge aller Abbildungen $\underline{i}\colon N \to \mathbb{Z}^{\geqslant 0}$, $\nu \mapsto i_\nu$ mit endlichem Träger, das heisst, mit $i_\nu = 0$ für fast alle ν. Sei $R[\underline{X}]$ die Menge aller Abbildungen $I_N \to R$, $\underline{i} \mapsto a_{\underline{i}}$ mit endlichem Träger, das heisst, mit $a_{\underline{i}} = 0$ für fast alle $\underline{i} \in I_N$. Die Summe und das Produkt zweier Elemente von $R[\underline{X}]$, sowie die Abbildung $\iota\colon R \to R[\underline{X}]$, die Elemente $0, 1 \in R[\underline{X}]$ und die Elemente $X_\nu \in R[\underline{X}]$ für alle $\nu \in N$ sind definiert wie oben. Dann ist wieder $(R[\underline{X}], +, \cdot, 0, 1)$ ein Ring und ι ein injektiver Ringhomomorphismus, und jedes Element von $R[\underline{X}]$ ist eine endliche Summe

$$(a_{\underline{i}})_{\underline{i}} = \sum_{\underline{i} \in I_N}{}' a_{\underline{i}} \underline{X}^{\underline{i}}$$

mit eindeutigen Koeffizienten $a_{\underline{i}} \in R$.

$$\underline{X}^{\underline{i}} = \prod_{\nu \in N}{}' X_\nu^{i_\nu}$$

$i_\nu \in \mathbb{Z}^{\geq 0}$
fast alle $= 0$.

2.6 Matrizen

Für alle natürlichen Zahlen m, n bezeichnet $\mathrm{Mat}_{m\times n}(R)$ die Menge aller $m \times n$-Matrizen mit Koeffizienten in R. Summe und Produkt von Matrizen über R sind durch dieselben Formeln definiert wie über einem Körper.

2.6.1 Meta-Proposition: Jede Rechenregel für Matrizen und Skalare über $\mathbb{Q}$, die nur die Operationen $+$ und $-$ und $\cdot$ sowie die Konstanten 0 und 1 beinhaltet, gilt auch für Matrizen und Skalare über einem beliebigen Ring.

Bew.: Die Rechenregel sei ein Ausdruck in Matrizen $A_1, \ldots, A_r$ und Skalaren $b_1, \ldots, b_s$. Der sei identisch Null über $\mathbb{Q}$. Nimm unabhängige Variable X_{ijk} und Y_i. Setze $A_i := (X_{ijk})_{j,k}$ und $b_i := Y_i$ in der Rechenregel $\Rightarrow$ Matrix mit Koeffizienten $F_{\mu\nu} \in R := \mathbb{Z}[X_{ijk}|_{i,j,k}, Y_i|_i]$. Also sind die von den $F_{\mu\nu}$ induzierten Polynomfunktionen $\mathbb{Q}^N \to \mathbb{Q}$ identisch Null. $2.5.6 \Rightarrow \forall \mu,\nu: F_{\mu\nu} = 0$ in R.

Für jeden Ring S und alle $x_{ijk}, y_i \in S$ ist dann auch $F_{\mu\nu}(x_{ijk}|_{ijk}, y_i|_i) = 0$.

Also gilt die Rechenregel über S. qed.

2.6.2 Beispiel: Für alle Matrizen passender Grössen über einem beliebigen Ring gilt:

(a) $A(BC) = (AB)C$.

(b) $I_m A = A I_n = A$.

(c) $\det(AB) = \det(A)\det(B)$.

(d) $A\tilde{A} = \tilde{A}A = \det(A) \cdot I_n$ für die Adjunkte $\tilde{A} := \big((-1)^{i+j} \cdot \det(A_{ji})\big)_{i,j}$ von A.

(e) $\mathrm{char}_A(A) = 0$ für das charakteristische Polynom $\mathrm{char}_A(X) := \det(X \cdot I_n - A)$.

Cayley – Hamilton

2.6.3 Proposition-Definition: Für jede Matrix $A \in \mathrm{Mat}_{n\times n}(R)$ sind äquivalent:

(a) Es existiert $A' \in \mathrm{Mat}_{n\times n}(R)$ mit $AA' = A'A = I_n$. Dann heisst A *invertierbar*.

(b) Es existiert $A' \in \mathrm{Mat}_{n\times n}(R)$ mit $AA' = I_n$.

(c) Es existiert $A' \in \mathrm{Mat}_{n\times n}(R)$ mit $A'A = I_n$.

(d) Es gilt $\det(A) \in R^\times$.

Die Matrix A' ist durch (b) oder (c) eindeutig bestimmt und heisst die *Inverse* A^{-1}.

Bew.: $AA' = I_n \Rightarrow \det(A)\cdot\det(A') = \det(AA') = \det(I_n) = 1 \Rightarrow \det(A) \in R^\times$.

$A'A = I_n \Rightarrow$ - - - analog.

Also gilt (a) $\Rightarrow$ (b) $\Rightarrow$ (d), (a) $\Rightarrow$ (c) $\Rightarrow$ (d)

(d) Setze $a := \det(A)^{-1}$. $\Rightarrow$

$(a\tilde{A})A = a\tilde{A}A = aA\tilde{A} = A(a\tilde{A}) = \underbrace{a\cdot\det(A)}_{1}\cdot I_n = I_n$

$\Rightarrow a\tilde{A}$ beidseitiges Inverses von A, $\Rightarrow$ (a). qed.

2.6.4 Proposition-Definition: Die Menge $\mathrm{GL}_n(R)$ aller invertierbaren $n\times n$-Matrizen über R ist eine Gruppe mit der Matrixmultiplikation und dem neutralen Element I_n. Sie heisst die *allgemeine lineare Gruppe vom Grad n über R.*

Bsp.: $GL_n(\mathbb{Z}) = \{A \in \mathrm{Mat}_{n\times n}(\mathbb{Z}) \mid \det(A) = \pm 1\}$, da $\mathbb{Z}^\times = \{\pm 1\}$ ist.

$SL_n(\mathbb{Z}) = \{$ - - - - $\mid \det(A) = 1\} = \mathrm{Ker}(\det: GL_n(\mathbb{Z}) \to \mathbb{Z}^\times)$.

$SL_n(\mathbb{Z}) \triangleleft GL_n(\mathbb{Z})$, Index $= \begin{cases} 2 & n \geq 1 \\ 1 & n = 0 \end{cases}$.