

UNTERLAGEN ZU RINGERWEITERUNGEN

VORLESUNG "KOMMUTATIVE ALGEBRA", SOMMERSEMESTER 2008

1. GANZE ERWEITERUNGEN

Seien A, B kommutative Ringe mit Eins. Wir schreiben $A \leq B$, wenn A ein Unterring von B (mit dem gleichen Einselement) ist.

Definition 1.1. Seien A, B kommutative Ringe mit Eins mit $A \leq B$, und sei $S = \langle s_i \mid i \in I \rangle$ eine Folge von Elementen von B . Dann ist $A[[S]]$ der Durchschnitt aller Unterringe R von B mit $A \cup \{s_i \mid i \in I\} \subseteq R$.

Definition 1.2. Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$, und sei $x \in B$. Das Element x ist *ganz über* A , wenn x Nullstelle eines Polynoms in $A[t]$ mit führendem Koeffizienten 1 ist.

Definition 1.3. Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$. B ist *ganz über* A , wenn alle $b \in B$ ganz über A sind.

Satz 1.4. Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$. Wenn x ganz über B ist, so gibt es $n \in \mathbb{N}$ und $b_0, \dots, b_{n-1} \in \mathbb{N}$ mit $b_0 = 1$, sodass

$$A[[x]] = A \cdot 1 + A \cdot b_1 + \dots + A \cdot b_{n-1}.$$

Beweisskizze: Sei n der Grad eines Polynoms mit führendem Koeffizienten 1, das x als Nullstelle hat, und sei $b_i := x^i$.

Satz 1.5. Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$. Sei $x \in B$ so, dass es $n \in \mathbb{N}$ und $b_0, \dots, b_{n-1} \in B$ gibt, sodass

- (1) $b_0 = 1$,
- (2) $\sum_{i=0}^{n-1} A \cdot b_i$ ist abgeschlossen unter $\cdot$,
- (3) $x \in \sum_{i=0}^{n-1} A \cdot b_i$.

Dann ist x ganz über A .

Satz 1.6. Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$. Sei $x \in B$ so, dass x ganz über A ist. Dann ist $A[[x]]$ ganz über A .

Date: April 24, 2008.

Erhard Aichinger, Institut für Algebra, Johannes Kepler Universität Linz, Austria,
erhard@algebra.uni-linz.ac.at.

Satz 1.7. Seien A, B kommutative Ringe mit Eins, sodass $A \leq B$, und seien $x, y \in B$. Wenn x ganz über A ist, und y ganz über $A[[x]]$ ist, so ist y ganz über A .

Satz 1.8. Seien A, B, C kommutative Ringe mit Eins, sodass $A \leq B \leq C$. Wenn B ganz über A , und C ganz über B ist, so ist C ganz über A .

2. ALGEBRAISCHE ERWEITERUNGEN

Definition 2.1. Seien A, B kommutative Ringe mit Eins mit $A \leq B$, und sei $e \in B$. Das Element e ist *algebraisch* über A , wenn es ein $p \in A[t]$ mit $p \neq 0$ gibt, sodass $\bar{p}(e) = 0$. B ist *algebraisch* über A , wenn alle $b \in B$ algebraisch über A sind.

Definition 2.2. Seien A, B kommutative Ringe mit Eins mit $A \leq B$. Eine Folge $S = \langle s_i \mid i \in I \rangle$ von Elementen aus B ist *algebraisch unabhängig* über A , wenn für alle $n \in \mathbb{N}$, für alle $p \in A[t_1, \dots, t_n] \setminus \{0\}$ und für alle paarweise verschiedenen $i_1, \dots, i_n \in I$ gilt:

$$\bar{p}(s_{i_1}, \dots, s_{i_n}) \neq 0.$$

Lemma 2.3. Seien A, B Integritätsbereiche mit $A \leq B$. Dann sind äquivalent:

- (1) B ist algebraisch über A .
- (2) $Q(B)$ ist algebraisch über $Q(A)$.

Beweis: (1) $\Rightarrow$ (2): Seien $p, q \in B$ mit $q \neq 0$. Wir zeigen, dass $\frac{p}{q}$ algebraisch über $Q(A)$ ist. Da q algebraisch über A ist, gibt es ein Polynom $f \in A[t]$ vom Grad $n \geq 1$, sodass

$$\bar{f}(q) = 0.$$

Für $g(x) := x^n \cdot f(\frac{1}{x})$ gilt $\bar{g}(\frac{1}{q}) = 0$. Also ist $\frac{1}{q}$ algebraisch über A , und somit ganz über $Q(A)$. Das Element p ist ganz über $Q(A)$, also auch über $Q(A)[\frac{1}{q}]$. Also ist $Q(A)[\frac{1}{q}][p]$ ganz über $Q(A)$. Da $\frac{p}{q} \in Q(A)[\frac{1}{q}][p]$, ist $\frac{p}{q}$ ganz über $Q(A)$. (2) $\Rightarrow$ (1): Sei $b \in B$. Dann ist b Nullstelle eines Polynoms f in $Q(A)[t] \setminus \{0\}$, und nach Multiplikation mit den Nennern der Koeffizienten von f auch eines Polynoms $g \in A[t] \setminus \{0\}$. $\square$

Proposition 2.4. Seien A, B, C Integritätsbereiche mit $A \leq B \leq C$. Wenn B algebraisch über A und C algebraisch über B ist, so ist C algebraisch über A .

Beweis: Nach Lemma 2.3 ist $Q(B)$ algebraisch, also ganz, über $Q(A)$, und $Q(C)$ ganz über $Q(B)$. Also ist $Q(C)$ ganz über $Q(A)$, und somit ist C algebraisch über A . $\square$

Definition 2.5. Seien A, B kommutative Ringe mit Eins mit $A \leq B$, und sei S eine Folge von Elementen aus B . S ist eine *Transzendenzbasis* von B über A , wenn S maximal unter den algebraisch unabhängigen Folgen aus B ist.

Proposition 2.6. *Seien A, B kommutative Ringe mit Eins mit $A \leq B$. Dann besitzt B eine Transzendenzbasis über A .*

Beweis: Sei $\mathcal{S}$ eine Kette über A algebraisch unabhängiger Folgen, und sei $S := \bigcup \mathcal{S}$.

Wenn $S = \langle s_i \mid i \in I \rangle$ algebraisch abhängig ist, gibt es $i_1, \dots, i_n \in I$, und $p \in A[t_1, \dots, t_n]$ mit $p \neq 0$, sodass $\overline{p}(s_{i_1}, \dots, s_{i_n}) = 0$. Es gibt nun ein Element $S' \in \mathcal{S}$, das $\langle s_{i_k} \mid k \in \{1, \dots, n\} \rangle$ enthält. Daher ist S' algebraisch abhängig.

Also ist S algebraisch unabhängig. Somit liefert das Zornsche Lemma eine Transzendenzbasis von B . $\square$

Satz 2.7. *Seien A, B kommutative Ringe mit Eins mit $A \leq B$, und sei $S = \langle s_i \mid i \in I \rangle$ eine über A algebraisch unabhängige Teilfolge von B . Sei $e \in B$, und sei $j \notin I$. Sei $S' := S \cup \{(j, e)\}$. Dann sind äquivalent:*

- (1) S' ist algebraisch abhängig über A .
- (2) e ist algebraisch über $A[[S]]$.

Beweis: (1) $\Rightarrow$ (2): Seien $n \in \mathbb{N}_0$, $i_1, \dots, i_n$ paarweise verschiedene Elemente aus I und $f \in A[t_1, \dots, t_{n+1}]$ so, dass $f \neq 0$ und $\overline{f}(s_{i_1}, \dots, s_{i_n}, e) = 0$. Sei nun

$$f(t_1, \dots, t_{n+1}) = \sum_{j=0}^m u_j(t_1, \dots, t_n) t_{n+1}^j.$$

Dann gilt

$$\sum_{j=0}^m \overline{u_j}(s_{i_1}, \dots, s_{i_n}) e^j = 0.$$

Das Polynom $g := \sum_{j=0}^m \overline{u_j}(s_{i_1}, \dots, s_{i_n}) t^j \in A[[S]][t]$ erfüllt $g \neq 0$ und $\overline{g}(e) = 0$. Somit ist e algebraisch über A .

(2) $\Rightarrow$ (1): Sei $g \in A[[S]][t]$ so, dass $g \neq 0$ und $\overline{g}(e) = 0$. Jedes Element in $A[[S]]$ lässt sich in der Form $\overline{u}(s_{i_1}, \dots, s_{i_m})$ mit $n \in \mathbb{N}$ und $u \in A[t_1, \dots, t_n]$ schreiben. Also lässt sich das Polynom g schreiben als

$$g = \sum_{k=0}^{\deg(g)} \overline{u_k}(s_{i_1}, \dots, s_{i_m}) t^k.$$

wobei $m \in \mathbb{N}$ und die i_j paarweise verschieden sind. Wir betrachten nun das Polynom $g' \in A[t_1, \dots, t_{m+1}]$, das durch

$$g'(t_1, \dots, t_{m+1}) = \sum_{k=0}^{\deg(g)} u_k(t_1, \dots, t_m) t_{m+1}^k$$

definiert ist. Es gilt $g' \neq 0$ und $\overline{g'}(s_{i_1}, \dots, s_{i_m}, e) = 0$. Folglich ist $S \cup \{(j, e)\}$ algebraisch abhängig über A . $\square$

Satz 2.8. Seien A, B Integritätsbereiche mit $A \leq B$, sei $(x_1, \dots, x_m)$ eine Transzendenzbasis von B über A , sei $r \in \mathbb{N}$, und sei $(w_1, \dots, w_r)$ eine über A algebraisch unabhängige Folge von Elementen aus B . Dann gibt es für alle $i \in \{0, 1, \dots, \min(r, m)\}$ eine injektive Abbildung $\pi : \{i+1, \dots, m\} \rightarrow \{1, \dots, m\}$, sodass B algebraisch über

$$A[w_1, \dots, w_i, x_{\pi(i+1)}, \dots, x_{\pi(m)}]$$

ist.

Beweis: Induktion nach i . Für $i = 0$ setzen wir $\pi := \text{id}_{\{1, \dots, m\}}$. Da $(x_1, \dots, x_m)$ eine Transzendenzbasis von B über A ist, gilt für jedes $e \in B$, dass $(x_1, \dots, x_m, e)$ algebraisch abhängig über A ist. Dann ist e nach Satz 2.7 algebraisch über $A[x_1, \dots, x_m]$.

Sei nun $i \geq 1$. Wir nehmen an, dass

$$(2.1) \quad B \text{ algebraisch über } A[w_1, \dots, w_{i-1}, x_{\pi(i)}, \dots, x_{\pi(m)}]$$

ist. Wir wollen nun eines der $x_{\pi(j)}$ durch w_i ersetzen. Dazu wählen wir eine Menge $K = \{k_1, \dots, k_l\}$ als eine Teilmenge von $\{i, i+1, \dots, m\}$, die maximal bezüglich $\subseteq$ mit der Eigenschaft ist, dass

$$(w_1, \dots, w_{i-1}, w_i, x_{\pi(k_1)}, \dots, x_{\pi(k_l)}) \text{ algebraisch unabhängig}$$

ist; da $(w_1, \dots, w_i)$ algebraisch unabhängig ist, gibt es ein solches K .

Falls $K = \{i, i+1, \dots, m\}$, so ist

$$(w_1, \dots, w_i, x_{\pi(i)}, \dots, x_{\pi(m)})$$

algebraisch unabhängig. Wegen (2.1) ist w_i algebraisch über

$A[w_1, \dots, w_{i-1}, x_{\pi(i)}, \dots, x_{\pi(m)}]$. Nach Satz 2.7 ist dann $(w_1, \dots, w_i, x_{\pi(i)}, \dots, x_{\pi(m)})$ algebraisch abhängig über A .

Daher gibt es ein $j \in \{i, i+1, \dots, m\}$, sodass $j \notin K$. Wegen der Maximalität von K gilt also

$$\begin{aligned} (w_1, \dots, w_i, x_{\pi(k_1)}, \dots, x_{\pi(k_l)}) &\text{ ist algebraisch unabhängig über } A, \text{ und} \\ (w_1, \dots, w_i, x_{\pi(k_1)}, \dots, x_{\pi(k_l)}, x_{\pi(j)}) &\text{ ist algebraisch abhängig über } A. \end{aligned}$$

Daher ist nach Satz 2.7 $x_{\pi(j)}$ algebraisch über $A[w_1, \dots, w_i, x_{\pi(k_1)}, \dots, x_{\pi(k_l)}]$, folglich über $A[w_1, \dots, w_i, x_{\pi(i)}, \dots, x_{\pi(j-1)}, x_{\pi(j+1)}, \dots, x_{\pi(m)}]$. Wir definieren nun

$$\sigma : \{i, \dots, m\} \rightarrow \{1, \dots, m\}$$

durch $\sigma(j) := \pi(i)$, $\sigma(i) := \pi(j)$, und $\sigma(r) = \pi(r)$ für $r \in \{i, \dots, m\} \setminus \{i, j\}$. Nun ist also $x_{\sigma(i)}$ algebraisch über

$$C := A[w_1, \dots, w_i, x_{\sigma(i+1)}, \dots, x_{\sigma(m)}].$$

Wegen (2.1) ist B algebraisch über $A[w_1, \dots, w_{i-1}, x_{\sigma(i+1)}, \dots, x_{\sigma(m)}][x_{\sigma(i)}]$, und daher erst recht über $A[w_1, \dots, w_{i-1}, w_i, x_{\sigma(i+1)}, \dots, x_{\sigma(m)}][x_{\sigma(i)}] = C[x_{\sigma(i)}]$. Da

$C[x_{\sigma(i)}]$ algebraisch über C ist, folgt nach Proposition 2.4, dass B algebraisch über C ist. Somit leistet $\sigma|_{\{i+1, \dots, m\}}$ das Gewünschte. $\square$

Korollar 2.9. *Seien A, B Integritätsbereiche mit $A \leq B$, und sei $(x_1, \dots, x_m)$ eine Transzendenzbasis von B über A . Sei $(w_1, \dots, w_r)$ eine über A algebraisch unabhängige Folge von Elementen aus B . Dann gilt $r \leq m$.*

Beweis: Wir nehmen an $r > m$. Aus dem Austauschsatz (Satz 2.8) erhalten wir, dass B algebraisch über $A[w_1, \dots, w_m]$ ist. Also ist w_{m+1} algebraisch über $A[w_1, \dots, w_m]$. Nach Satz 2.7 ist $(w_1, \dots, w_m, w_{m+1})$ dann algebraisch abhängig. $\square$

Definition 2.10. Seien A, B Integritätsbereiche mit $A \leq B$. Wenn B eine endliche Transzendenzbasis über A besitzt, so ist der *Transzendenzgrad* von B über A die Anzahl der Elemente dieser Basis. Andernfalls ist der Transzendenzgrad ∞ .

3. NOETHERSCHE NORMALISIERUNG

Lemma 3.1. *Sei k ein unendlicher Körper, $n \in \mathbb{N}$, und sei $p \in k[t_1, \dots, t_n]$ mit $p \neq 0$. Dann gibt es ein $\mathbf{v} \in k^n$ mit $\bar{p}(\mathbf{v}) \neq 0$.*

Beweisskizze: Induktion nach n .

Lemma 3.2. *Sei k ein Körper, und sei B ein kommutativer Ring mit Eins mit $k \leq B$. Sei $n \in \mathbb{N}$, $\mathbf{x} = (x_1, \dots, x_n)$ eine Folge von Elementen aus B , und sei $p \in k[t_1, \dots, t_n]$ so, dass*

$$\bar{p}(x_1, \dots, x_n) = 0$$

und $p \neq 0$. Dann gibt es Polynome $f_2, \dots, f_n \in k[t_1, \dots, t_n]$ und $g_1, \dots, g_n \in k[t_1, \dots, t_n]$, sodass folgendes gilt:

- (1) x_1 ist ganz über $k[\bar{f}_2(\mathbf{x}), \dots, \bar{f}_n(\mathbf{x})]$,
- (2) Für alle $j \in \{1, \dots, n\}$ gilt

$$t_j = g_j(t_1, f_2(t_1, \dots, t_n), \dots, f_n(t_1, \dots, t_n)).$$

(Das bedeutet, dass $k[\bar{f}_2(\mathbf{x}), \dots, \bar{f}_n(\mathbf{x}), x_1] = B$.)

Wenn k unendlich ist, so kann man alle f_i linear wählen.

Beweis: Wir betrachten zunächst den Fall, dass k unendlich ist. Sei I eine endliche Teilmenge von $\mathbb{N}_0^n$, und sei $\langle c_i \mid i \in I \rangle : I \rightarrow k$ so, dass

$$p = \sum_{(i_1, \dots, i_n) \in I} c(i_1, \dots, i_n) t_1^{i_1} \cdots t_n^{i_n}.$$

Für ein passendes $(\alpha_2, \dots, \alpha_n) \in k^{n-1}$ gilt nun, dass das Polynom

$$q(t_1, \dots, t_n) := p(t_1, t_2 + \alpha_2 t_1, \dots, t_n + \alpha_n t_1)$$

von der Form $b_N t_1^N + \sum_{i=0}^{N-1} b_i(t_2, \dots, t_n) t_1^i$ mit $b_N \in k$, $b_i \in k[t_2, \dots, t_n]$ ist. Um das zu zeigen, bilden wir ein Polynom q' in $k[t_1, \dots, t_n, a_2, \dots, a_n]$.

$$\begin{aligned} q' &:= p(t_1, t_2 + a_2 t_1, \dots, t_n + a_n t_1) \\ &= \sum_{(i_1, \dots, i_n) \in I} c(i_1, \dots, i_n) t_1^{i_1} (t_2 + a_2 t_1)^{i_2} \cdots (t_n + a_n t_1)^{i_n}. \end{aligned}$$

Sei N der totale Grad von p . Dann erhalten wir den Koeffizienten K von x^N in q' durch

$$K = \sum_{\substack{(i_1, \dots, i_n) \in I \\ i_1 + \dots + i_n = N}} c(i_1, \dots, i_n) a_2^{i_2} a_3^{i_3} \cdots a_n^{i_n}.$$

Das Polynom $K \in k[a_2, \dots, a_n]$ ist nicht das Nullpolynom, also gibt es nach Lemma 3.1 ein $(\alpha_2, \dots, \alpha_n) \in k^{n-1}$, sodass $\overline{K}(\alpha_2, \dots, \alpha_n) \neq 0$.

Es gilt

$$\overline{q}(x_1, x_2 - \alpha_2 x_1, \dots, x_n - \alpha_n x_1) = 0.$$

Also ist x_1 ganz über $k[x_2 - \alpha_2 x_1, \dots, x_n - \alpha_n x_1]$. Somit leisten $f_j := x_j - \alpha_j x_1$ und $g_1 := t_1$, $g_j := x_j + \alpha_j x_1$ das Gewünschte.

Wenn k endlich ist, so kann man $g_j := t_j + t_1^{d^{j-1}}$ mit $d > \max\{i_j \mid i \in I, j \in \{1, \dots, n\}\}$ und $f_j := t_j - t_1^{d^{j-1}}$ wählen. $\square$

Satz 3.3 (Noethersche Normalisierung). *Sei k ein Körper, sei B ein kommutativer Ring mit Eins mit $k \leq B$, und seien $x_1, \dots, x_n \in B$ so, dass $k[x_1, \dots, x_n] = B$. Dann gibt es $r \in \{0, \dots, n\}$ und $f_1, \dots, f_r \in k[t_1, \dots, t_n]$, sodass für $y_j := \overline{f_j}(x_1, \dots, x_n)$ gilt:*

- (1) $(y_1, \dots, y_r)$ ist algebraisch unabhängig über k ,
- (2) B ist ganz über $k[y_1, \dots, y_r]$.

Beweis: Induktion nach n . Wenn $(x_1, \dots, x_n)$ algebraisch unabhängig ist, so gilt für $r := n$ und $f_j := t_j$ ($j \in \{1, \dots, n\}$) das Gewünschte.

Wenn $\mathbf{x} = (x_1, \dots, x_n)$ algebraisch abhängig ist, so gibt es ein $p \in k[t_1, \dots, t_n]$ mit $p \neq 0$, sodass

$$\overline{p}(x_1, \dots, x_n) = 0.$$

Daher gibt es nach Lemma 3.2 $f_1, \dots, f_{n-1} \in k[t_1, \dots, t_n]$, sodass x_n ganz über $k[\overline{f_1}(x_1, \dots, x_n), \dots, \overline{f_{n-1}}(x_1, \dots, x_n)]$ ist, und

$$k[\overline{f_1}(\mathbf{x}), \dots, \overline{f_{n-1}}(\mathbf{x}), x_n] = B.$$

Nach Induktionsvoraussetzung gibt es nun $g_1, \dots, g_r \in k[t_1, \dots, t_{n-1}]$, sodass $k[\overline{f_1}(\mathbf{x}), \dots, \overline{f_{n-1}}(\mathbf{x})]$ ganz über

$$k[\overline{g_1}(\overline{f_1}(\mathbf{x}), \dots, \overline{f_{n-1}}(\mathbf{x})), \dots, \overline{g_r}(\overline{f_1}(\mathbf{x}), \dots, \overline{f_{n-1}}(\mathbf{x}))]$$

ist

Für $h_j := g_j(f_1, \dots, f_{n-1}) \in k[t_1, \dots, t_n]$ gilt also:

$$k[\overline{f_1}(\mathbf{x}), \dots, \overline{f_{n-1}}(\mathbf{x})] \text{ ist ganz über } k[\overline{h_1}(\mathbf{x}), \dots, \overline{h_r}(\mathbf{x})].$$

Da x_n ganz über

$$k[\overline{f_1}(\mathbf{x}), \dots, \overline{f_{n-1}}(\mathbf{x})]$$

ist, gilt:

$$k[\overline{f_1}(\mathbf{x}), \dots, \overline{f_{n-1}}(\mathbf{x})][x_n] \text{ ist ganz über } k[\overline{h_1}(\mathbf{x}), \dots, \overline{h_r}(\mathbf{x})].$$

Folglich ist B ganz über $k[\overline{h_1}(\mathbf{x}), \dots, \overline{h_r}(\mathbf{x})]$. $\square$

4. DER HILBERTSCHE NULLSTELLENSATZ

Satz 4.1 (Hilberts Nullstellensatz – Schwache Form). *Sei k ein Körper, und sei I ein Ideal von $k[t_1, \dots, t_n]$ mit $1 \notin I$. Dann gibt es eine algebraische Körpererweiterung K von k und $\mathbf{x} \in K^n$, sodass für alle $f \in I$ gilt: $\overline{f}(\mathbf{x}) = 0$.*

Beweis: Sei M ein maximales Ideal von $k[t_1, \dots, t_n]$ mit $I \subseteq M \neq k[t]$, und sei $K := k[t]/M$. K ist ein Körper, und $(x_1, \dots, x_m) := (t_1 + M, \dots, t_m + M)$ ist eine Nullstelle aller Polynome in I . Es bleibt zu zeigen, dass K algebraisch über k ist: Seien dazu $r \in \{0, \dots, n\}$ und $y_1, \dots, y_r \in K$ so, dass K ganz über $k[y_1, \dots, y_r]$ ist, und $(y_1, \dots, y_r)$ algebraisch unabhängig ist. Wenn $r = 0$, so ist K ganz über k , also algebraisch. Wenn $r \geq 1$, so gilt wegen der Unabhängigkeit der y_i , dass $y_1 \neq 0 + M$. Also gibt es ein $z_1 \in K$ mit $z_1 \cdot y_1 = 1 + M$. Da z_1 ganz über $k[y_1, \dots, y_r]$ ist, gibt es $m \in \mathbb{N}$ und $f_1, \dots, f_{m-1} \in k[t_1, \dots, t_r]$, sodass

$$z_1^m + \sum_{i=0}^{m-1} \overline{f_i}(y_1, \dots, y_r) z_1^i = 0 + M.$$

Durch Multiplikation mit y_1^m erhalten wir

$$1 + \sum_{i=0}^{m-1} \overline{f_i}(y_1, \dots, y_r) y_1^{m-i} = 0 + M.$$

Das Polynom $g \in k[t_1, \dots, t_r]$, das durch

$$g := 1 + \sum_{i=0}^{m-1} f_i(t_1, \dots, t_r) t_1^{m-i}$$

gegeben ist, erfüllt $g \neq 0$ und $\overline{g}(y_1, \dots, y_r) = 0$. Dann ist $(y_1, \dots, y_r)$ algebraisch abhängig. $\square$

Satz 4.2 (Grundlage des automatischen Beweisens geometrischer Sätze). *Sei k ein algebraisch abgeschlossener Körper, seien $n \in \mathbb{N}$, $r, s \in \mathbb{N}_0$, $f_1, \dots, f_s, h_1, \dots, h_r, g \in k[t_1, \dots, t_n]$. Dann sind äquivalent:*

(1) Für alle $\mathbf{x} \in k^n$ gilt:

$$(f_1(\mathbf{x}) = \dots = f_s(\mathbf{x}) = 0, h_1(\mathbf{x}) \neq 0, \dots, h_r(\mathbf{x}) \neq 0) \implies g(\mathbf{x}) = 0.$$

(2) 1 liegt in dem von

$$(f_1, \dots, f_s, h_1 \cdot u_1 - 1, \dots, h_r \cdot u_r - 1, g \cdot v - 1)$$

erzeugten Ideal von $k[t_1, \dots, t_n, u_1, \dots, u_r, v]$.

Satz 4.3 (Rabinowitschs Trick). Sei k ein Körper, $s, n \in \mathbb{N}$, und seien $f_1, \dots, f_s \in k[t_1, \dots, t_n]$. Dann sind äquivalent:

$$(1) g \in \sqrt{\langle f_1, \dots, f_s \rangle_{\text{Id } k[t]}}.$$

$$(2) 1 \in \langle f_1, \dots, f_s, g \cdot u - 1 \rangle_{\text{Id } k[t, u]}.$$

Beweis: (1) $\implies$ (2). Sei $I := \langle f_1, \dots, f_s, g \cdot u - 1 \rangle_{\text{Id } k[t, u]}$. Wegen (1) gibt es ein $r \in \mathbb{N}$, sodass $g^r \in I$. Folglich gilt auch $g^r \cdot u^r \in I$. Da $g \cdot u \equiv 1 \pmod{I}$, gilt auch $(g \cdot u)^r \equiv 1^r \pmod{I}$, und somit $1 \in I$. (2) $\implies$ (1) Wenn $g = 0$, so liegt g klarerweise im Radikal. Wenn $g \neq 0$, so gibt es Polynome $a_1, \dots, a_s, b \in k[t, u]$, sodass

$$\sum_{i=1}^s a_i(t_1, \dots, t_n, u) f_i(t_1, \dots, t_n) + b(t_1, \dots, t_n, u)(g(t_1, \dots, t_n) \cdot u - 1) = 1.$$

Wir werten jetzt beide Seiten im rationalen Funktionenkörper $Q(k[x_1, \dots, x_n])$ an der Stelle $(x_1, \dots, x_n, \frac{1}{g(x_1, \dots, x_n)})$ aus, und erhalten

$$\sum_{i=1}^s a_i(x_1, \dots, x_n, 1/g(x_1, \dots, x_n)) f_i(x_1, \dots, x_n) = 1.$$

Es gibt nun $r \in \mathbb{N}$ und $h_1, \dots, h_s \in k[x_1, \dots, x_n]$, sodass

$$a_i(x_1, \dots, x_n, 1/g(x_1, \dots, x_n)) = \frac{h_i(x_1, \dots, x_n)}{g(x_1, \dots, x_n)^r}.$$

Dann liegt g^r in dem von $(f_1, \dots, f_s)$ erzeugten Ideal von $k[t_1, \dots, t_n]$.

Satz 4.4 (Hilberts Nullstellensatz – Starke Form). Sei k ein algebraisch abgeschlossener Körper, sei $n \in \mathbb{N}$, und seien $f_1, \dots, f_s \in k[t_1, \dots, t_n]$. Wenn für alle $\mathbf{x} \in k^n$ mit $\overline{f_1}(\mathbf{x}) = \dots = \overline{f_s}(\mathbf{x}) = 0$ gilt, dass $g(\mathbf{x}) = 0$, so liegt g im Radikal von $\langle f_1, \dots, f_s \rangle_{\text{Id } k[t]}$.

Beweis: Sei u eine neue Variable. $f_1 = \dots = f_s = 0$, $g \cdot u = 1$ ist unlösbar, also gilt wegen der schwachen Form des Nullstellensatzes $1 \in \langle f_1, \dots, f_s, g \cdot u - 1 \rangle_{\text{Id } k[t, u]}$. Also liegt nach dem Satz von Rabinowitsch (Satz 4.3) g im Radikal von $\langle f_1, \dots, f_s \rangle_{\text{Id } k[t]}$. $\square$