Universität Konstanz
Fachbereich Mathematik und Statistik
Markus Schweighofer

§2.8 Endliche Varietäten

In diesem Abschnitt sei stets $C|K$ eine Körpererweiterung, C algebraisch abgeschlossen und $\leq$ eine Monomordnung auf $[\underline{X}]$.

Satz 2.8.1. *Sei $I \subseteq K[\underline{X}]$ ein Ideal. Dann sind äquivalent:*

(a) $\#V(I) < \infty$

(b) $\forall i \in \{1,\dots,n\} : I \cap K[X_i] \neq (0)$

(c) $\forall i \in \{1,\dots,n\} : L(I) \cap [X_i] \neq \emptyset$

(d) $\dim_K(K[\underline{X}]/I) < \infty$

(e) Jedes Primideal $\mathfrak{p}$ von $K[\underline{X}]$ mit $I \subseteq \mathfrak{p}$ ist maximal.

(f) Es gibt keine irreduziblen affinen K-Untervarietäten V und W von $V(I)$ mit $V \subset W$.

Beweis. (a) $\Longrightarrow$ (b) Œ $C = \overline{K}$. Gelte nun (a) und sei $i \in \{1,\dots,n\}$. Nach 2.7.2 definiert das Eliminationsideal $I \cap K[X_i]$ dann eine endliche affine K-Varietät $V(I \cap K[X_i])$ (denn der Zariski-Abschluss einer endlichen Menge in C ist endlich, da C algebraisch über K ist). Wäre $I \cap K[X_i] = (0)$, so wäre aber $V(I \cap K[X_i]) = C$ unendlich, da C algebraisch abgeschlossen ist [→1.2.10].

(b) $\Longrightarrow$ (c) ist trivial.

(c) $\Longrightarrow$ (d) Gelte (c). Wähle eine Gröbnerbasis G von I. Nach 2.4.7(i) sind die K-Vektorräume $\operatorname{red}(G)$ und $K[\underline{X}]/I$ isomorph. Nach 2.4.11 ist

$$\operatorname{redM}(G) = \{u \in [\underline{X}] \mid \nexists g \in G \setminus \{0\} : \operatorname{LM}(g)|u\}$$

eine Basis von $\operatorname{red}(G)$. Also ist zu zeigen, dass $\operatorname{redM}(G)$ endlich ist. Wegen $L(I) = (\{\operatorname{LM}(g) \mid g \in G \setminus \{0\}\})$ und (c) gibt es aber zu jedem $i \in \{1,\dots,n\}$ ein $g_i \in G \setminus \{0\}$ mit $\operatorname{LM}(g_i) \in [X_i]$. Daraus sieht man leicht $\#\operatorname{redM}(G) < \infty$.

(d) $\Longrightarrow$ (e) Gelte (d) und sei $\mathfrak{p} \subseteq K[\underline{X}]$ ein Primideal mit $I \subseteq \mathfrak{p}$. Da wir einen K-Vektorraumepimorphismus $K[X]/I \twoheadrightarrow K[\underline{X}]/\mathfrak{p}$ haben, gilt auch $\dim_K(K[\underline{X}]/\mathfrak{p}) < \infty$. Sei nun $\mathfrak{m} \subset K[\underline{X}]$ ein Ideal mit $\mathfrak{p} \subseteq \mathfrak{m}$. Zu zeigen: $\mathfrak{p} = \mathfrak{m}$. Sei $f \in \mathfrak{m}$. Da die Potenzen $\overline{f}^0, \overline{f}^1, \overline{f}^2, \dots$ linear abhängig in $K[\underline{X}]/\mathfrak{p}$ sind, gibt es $k \in \mathbb{N}_0$ und $a_0,\dots,a_{k-1} \in K$ mit $f^k + a_{k-1}f^{k-1} + \cdots + a_0 \in \mathfrak{p}$. Dann $k \geq 1$, da $1 \notin \mathfrak{p}$. Falls $k = 1$, so $f + a_0 \in \mathfrak{p} \subseteq \mathfrak{m}$ und daher $a_0 \in K \cap \mathfrak{m} = (0)$ und somit $f \in \mathfrak{p}$. Falls $k \geq 2$, so ebenfalls $a_0 \in K \cap \mathfrak{m} = (0)$

und somit $f(f^{k-1} + \cdots + a_1) \in \mathfrak{p}$, woraus $f \in \mathfrak{p}$ oder $f^{k-1} + \cdots + a_1 \in \mathfrak{p}$ folgt und so weiter...

(e) $\Longrightarrow$ (f) Man kann (e) offensichtlich auch so formulieren: Es gibt keine Primideale $\mathfrak{p}$ und $\mathfrak{q}$ von $K[\underline{X}]$ mit $\sqrt{I} \subseteq \mathfrak{p} \subset \mathfrak{q}$. Mit 1.3.10 und 1.4.22 entspricht dies genau (f).

(f) $\Longrightarrow$ (a) zeigen wir durch Kontraposition: Gelte $\#V(I) = \infty$. Da $V(I)$ nur endlich viele irreduzible Komponenten hat, gibt es dann eine irreduzible affine K-Untervarietät W von $V(I)$ mit $\#W = \infty$ [$\rightarrow$1.4.20]. Dann muss die Projektion von W auf eine der Koordinatenachsen, ohne Einschränkung auf die letzte, auch unendlich sein, woraus $I \cap K[X_n] = (0)$ folgt. Wendet man Satz 2.7.2 auf die Körpererweiterung $\overline{K}|K$ an, wobei $\overline{K}$ den algebraischen Abschluss von K bezeichnet, so folgt $\pi(W \cap \overline{K}^n) \neq \emptyset$ mit $\pi : \mathbb{A}^n \to \mathbb{A}$, $(x_1, \ldots, x_n) \mapsto x_n$. Wähle nun $a \in \pi(W \cap \overline{K}^n) \subseteq \overline{K}$. Wähle $f \in K[X_n] \setminus \{0\}$ mit $f(a) = 0$. Dann ist $W \cap V(f)$ eine nichtleere echte affine K-Untervarietät von W (nichtleer, da $a \in \pi(W)$ und $f(a) = 0$, und echt, da $\#\pi(W) = \infty$ und $\#\pi(W \cap V(f)) < \infty$). Wähle nun eine irreduzible Komponente V von $W \cap V(f)$. Dann $V \subset W \subseteq V(f)$ und V und W sind irreduzibel. □

Korollar 2.8.2. *Sei G eine Gröbnerbasis des Ideals $I \subseteq K[\underline{X}]$. Dann gilt genau dann $\#V(I) < \infty$, wenn es für jedes $i \in \{1, \ldots, n\}$ ein $g \in G \setminus \{0\}$ gibt mit* $\mathrm{LM}(g) \in [X_i]$.

Beweis. Benutze 2.8.1 und 2.4.2(j). □

Erinnerung 2.8.3. Ist $f \in C[X]$ und $a \in C$, so heißt a eine *mehrfache Nullstelle* von f, wenn $(X - a)^2 \mid f$ in $C[X]$ [$\rightarrow$A4.4.4, A4.4.10] oder äquivalent, wenn $f(a) = f'(a) = 0$ [$\rightarrow$A4.4.11]. Ein Polynom $f \in C[X]$ heißt *separabel*, wenn f in C keine mehrfachen Nullstellen hat [$\rightarrow$A4.5.1] oder äquivalent, wenn $V(f, f') = \emptyset$. Ist also $f \in K[X]$, so ist f separabel genau dann, wenn $(f, f') = (1) = K[X]$. Man nennt K *vollkommen*, wenn jedes irreduzible Polynom in $K[X]$ separabel ist [$\rightarrow$A4.5.20]. Körper der Charakteristik 0, endliche Körper und algebraisch abgeschlossene Körper sind vollkommen [$\rightarrow$A4.5.5(a), A4.5.22].

Übung 2.8.4. Seien A ein faktorieller Ring, $s \in \mathbb{N}_0$, $p_1, \ldots, p_s$ paarweise nicht assoziierte irreduzible Elemente von A und $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$. Dann ist das Hauptideal $(p_1^{\alpha_1} \cdots p_s^{\alpha_s})$ genau dann ein Radikalideal, wenn $\alpha_1 = \ldots = \alpha_s = 1$.

Lemma 2.8.5. *Sei $f \in K[X]$ und $I := (f) \subseteq K[X]$.*

(a) Ist f separabel, so ist I ein Radikalideal.

(b) Ist K vollkommen und I ein Radikalideal, so ist f separabel.

Beweis. (a) folgt sofort aus 2.8.4, ebenso (b), wenn man noch berücksichtigt, dass zwei nicht assoziierte irreduzible Polynome in $K[X]$ keine gemeinsame Nullstelle in C haben können. □

Beispiel 2.8.6. Nimmt man $K := \mathbb{F}_p(T)$ für eine Primzahl p, so ist $X^p - T$ nach dem Kriterium von Eisenstein [$\rightarrow$A2.6.3] prim und daher $(X^p - T) \subseteq K[X]$ ein Primideal und insbesondere ein Radikalideal. Aber $X^p - T$ ist nicht separabel, denn ist $a \in \overline{K}$ mit $a^p - T = 0$, so $X^p - T = (X - a)^p$ [$\rightarrow$A4.4.3].

Lemma 2.8.7. *Sei $I \subseteq K[\underline{X}]$ ein Ideal, $s \in \mathbb{N}$ und $p_1, \ldots, p_s \in K[X_1]$ mit $(p_i, p_j) = (1) = K[X_1]$ für alle $i, j \in \{1, \ldots, s\}$ mit $i \neq j$. Dann*

$$(I \cup \{p_1 \cdots p_s\}) = \bigcap_{i=1}^{s} (I \cup \{p_i\}).$$

Beweis. „$\subseteq$“ ist trivial

„$\supseteq$“ Sei $g \in \bigcap_{i=1}^{s}(I \cup \{p_i\})$. Zu zeigen: $g \in (I \cup \{p_1 \cdots p_s\})$. Wähle $q_i \in I$ und $r_i \in K[\underline{X}]$ mit $g = q_i + r_i p_i$ $(1 \leq i \leq s)$. Für

$$f_i := \prod_{\substack{j=1 \\ j \neq i}}^{s} p_j$$

gilt $f_i g \in (I \cup \{p_1 \cdots p_s\})$. Da $K[X_1]$ ein Hauptidealring ist, gilt ausserdem

$$(f_1, \ldots, f_s) = (1) = K[X_1].$$

Daher gibt es $h_1, \ldots, h_s \in K[X_1]$ mit $h_1 f_1 + \cdots + h_s f_s = 1$. Es folgt

$$g = 1g = (h_1 f_1 + \cdots + h_s f_s)g = h_1(f_1 g) + \ldots + h_s(f_s g) \in (I \cup \{p_1 \cdots p_s\}).$$

□

Satz 2.8.8. [Abraham Seidenberg *1916 †1988] *Sei $I \subseteq K[\underline{X}]$ ein Ideal. Für jedes $i \in \{1, \ldots, n\}$ enthalte das Eliminationsideal $I \cap K[X_i]$ ein separables Polynom. Dann ist I ein Radikalideal.*

Beweis. Induktion nach $n \in \mathbb{N}_0$.
$\underline{n = 0}$ trivial
$\underline{n = 1}$ mit 2.8.5(a)
$\underline{n - 1 \to n \ \ (n \geq 2)}$ Wähle ein separables Polynom $f \in I \cap K[X_1]$. Falls $f \in K^\times$, so sind wir fertig. Sei also $f \in K[X_1] \setminus K$. Schreibe dann $f = p_1 \cdots p_s$ mit $s \in \mathbb{N}$, $p_1, \ldots, p_s \in K[X_1]$ irreduzibel und $(p_i, p_j) = (1)$ für $i \neq j$. Nach 2.8.7 gilt dann $I = \bigcap_{i=1}^{s}(I \cup \{p_i\})$. Da ein Schnitt von Radikalidealen wieder ein Radikalideal ist, können wir daher Œ f als irreduzibel in $K[X_1]$ voraussetzen. Wähle eine Nullstelle $a \in C$ mit $f(a) = 0$, setze $L := K(a)$ und betrachte den K-Algebrenepimorphismus $\varphi\colon K[X_1, \ldots, X_n] \twoheadrightarrow L[X_2, \ldots, X_n]$ mit $\varphi(X_1) = a$ und $\varphi(X_i) = X_i$ für $i \in \{2, \ldots, n\}$. Man sieht dann leicht, dass der Kern von φ von f erzeugt wird, denn f ist assoziiert zum Minimalpolynom von a über K. Insbesondere gilt $\ker \varphi \subseteq I$. Da φ wegen $L = K[a]$ surjektiv ist, ist $J := \varphi(I)$ ein Ideal in $L[X_2, \ldots, X_n]$. Wegen $\ker \varphi \subseteq I$ gilt $\varphi^{-1}(J) = I$. Daher reicht es zu zeigen, dass J ein Radikalideal ist. Für jedes $i \in \{2, \ldots, n\}$ enthält aber mit $I \cap K[X_i]$ auch $J \supseteq I \cap K[X_i]$ ein separables Polynom. Nach Induktionsvoraussetzung ist also J ein Radikalideal wie gewünscht. □

Korollar 2.8.9. *Sei K ein vollkommener Körper und $I \subseteq K[\underline{X}]$ ein Ideal. Dann sind äquivalent:*

(a) I ist ein Radikalideal mit $\#V(I) < \infty$.

(b) *Für jedes $i \in \{1, \ldots, n\}$ enthält $I \cap K[X_i]$ ein separables Polynom.*

(c) *Für jedes $i \in \{1, \ldots, n\}$ wird das Eliminationsideal $I \cap K[X_i]$ von einem separablen Polynom erzeugt.*

Beweis. (c) $\Longrightarrow$ (b) ist trivial.

(b) $\Longrightarrow$ (a) folgt aus den Sätzen 2.8.8 und 2.8.1.

(a) $\Longrightarrow$ (c) folgt aus Satz 2.8.5(b). □

Proposition 2.8.10. *Gelte* $\operatorname{char} K = 0$. *Seien $f \in K[X] \setminus \{0\}$ und $g, h \in K[X]$ mit $(f, f') = (h)$ und $f = gh$. Dann gilt $\sqrt{(f)} = (g)$ und g ist separabel.*

Beweis. Œ f normiert. Wähle dann $m \in \mathbb{N}_0$, paarweise verschiedene $a_1, \ldots, a_d \in C$ und $\alpha_1, \ldots, \alpha_d \in \mathbb{N}$ mit $f = \prod_{i=1}^{d} (X - a_i)^{\alpha_i}$. Es folgt $f' = \sum_{i=1}^{d} \alpha_i (X - a_i)^{\alpha_i - 1} \prod_{j \neq i} (X - a_j)^{\alpha_j}$, woraus man wegen $\operatorname{char} K = 0$ sieht, dass das von f und f' in $C[X]$ erzeugte Ideal von $\prod_{i=1}^{d} (X - a_i)^{\alpha_i - 1}$ erzeugt wird. Da h laut Voraussetzung das von f und f' in $K[X]$ und damit auch in das davon in $C[X]$ erzeugte Ideal erzeugt, gilt

$$(h) = \left(\prod_{i=1}^{d} (X - a_i)^{\alpha_i - 1} \right) \subseteq C[X]$$

und daher Œ $h = \prod_{i=1}^{d} (X - a_i)^{\alpha_i - 1}$. Somit $g = (X - a_1) \cdots (X - a_n)$. Entweder mit dem Hilbertschen Nullstellensatz 1.3.9 oder mit linearer Algebra sieht man nun leicht $\sqrt{(f)} = (g)$. Dass g separabel ist, ist klar. □

Satz 2.8.11. *Gelte* $\operatorname{char} K = 0$ *und sei $I \subseteq K[\underline{X}]$ ein Ideal mit $\#V(I) < \infty$. Für jedes $i \in \{1, \ldots, n\}$ erzeuge $f_i \in K[X_i]$ das Eliminationsideal $I \cap K[X_i]$ und es seien $g_i, h_i \in K[X]$ mit $(f_i, f_i') = (h_i) \subseteq K[X_i]$ und $f_i = g_i h_i$. Dann*

$$\sqrt{I} = (I \cup \{g_1, \ldots, g_n\}).$$

Beweis. Nach 2.8.10 ist $g_i \in K[X_i]$ separabel mit $g_i \in \sqrt{I}$ für $i \in \{1, \ldots, n\}$. Nach 2.8.8 ist $(I \cup \{g_1, \ldots, g_n\})$ ein Radikalideal. □

Lemma 2.8.12 (Interpolation)**.** *Seien $\ell \in \mathbb{N}_0$, $x_1, \ldots, x_\ell \in K^n$ paarweise verschieden und $y_1, \ldots, y_\ell \in K$. Dann gibt es $f \in K[X_1, \ldots, X_n]$ mit $f(x_i) = y_i$ für $i \in \{1, \ldots, \ell\}$.*

Beweis. Œ $\ell \geq 1$, $y_1 = 1$ und $y_2 = \ldots = y_\ell = 0$. Induktion nach $n \in \mathbb{N}_0$:
$\underline{n = 0}$ Wegen $K^0 = \{0\}$ gilt $\ell = 1$. Setze also $f := 1 \in K$.

$\underline{n = 1}$ Setze

$$f := \frac{\prod_{i=2}^{\ell} (X_1 - x_i)}{\prod_{i=2}^{\ell} (x_1 - x_i)} \in K[X_1].$$

$\underline{n - 1 \to n \ \ (n \in \mathbb{N})}$ Schreibe $x_i = (x_i', x_i'')$ mit $x_i \in K^{n-1}$ und $x_i'' \in K$ für $i \in \{1, \ldots, \ell\}$.

Nach allfälligem Umnummerieren gibt es $k \in \{1, \ldots, \ell\}$ mit

$$x_1'' = \ldots = x_k'' \notin \{x_{k+1}'', \ldots, x_\ell''\}.$$

Nach dem schon bewiesenen Fall $n = 1$ gibt es $g \in K[X_n]$ mit $g(x_1'') = 1$ und $g(x_i'') = 0$ für alle $i \in \{k+1, \ldots, \ell\}$. Nach Induktionsvoraussetzung gibt es weiter $h \in K[X_1, \ldots, X_{n-1}]$ mit $h(x_1') = 1$ und $h(x_2') = \ldots = h(x_k') = 0$. Setze $f := gh$. □

Lemma 2.8.13. *Sei $I \subseteq C[\underline{X}]$ ein Ideal mit $\#V(I) < \infty$. Dann ist der C-Algebrenhomomorphismus*

$$\varphi\colon C[\underline{X}]/I \to C^{V(I)},\ \overline{p} \mapsto (p(x))_{x \in V(I)} \quad (p \in C[X])$$

surjektiv. Ist I ein Radikalideal, so ist φ sogar ein Isomorphismus.

Beweis. Die erste Aussage ist aus 2.8.12 klar. Sei nun I ein Radikalideal. Wegen $I = \sqrt{I} \overset{1.3.9}{=} I(V(I))$ gilt dann mit $K := C$ und $V := V(I)$, dass $K[V] = C[\underline{X}]/I$. Es ist dann φ nichts anderes als der K-Algebrenisomorphismus $K[V] \to \mathrm{Mor}_K(V, \mathbb{A})$ aus 1.5.8. □

Satz 2.8.14. *Sei $I \subseteq K[\underline{X}]$ ein Ideal mit $\#V(I) < \infty$.*

(a) $\#V(I) \leq \dim_K(K[\underline{X}]/I) < \infty$

(b) Ist K vollkommen und I ein Radikalideal, so $\#V(I) = \dim_K(K[\underline{X}]/I)$.

Beweis. Wähle eine Gröbnerbasis G von I und sei J das von G in $C[\underline{X}]$ erzeugte Ideal. Es gilt natürlich $V(I) = V(G) = V(J)$. Es ist $\mathrm{redM}(G)$ [→2.4.10] sowohl eine Basis für den K-Vektorraum der modulo G reduzierten Polynome aus $K[\underline{X}]$ als auch für den C-Vektorraum der modulo G reduzierten Polynome aus $C[\underline{X}]$ [→2.4.1(b)]. Wegen 2.4.7(i) gilt also $\dim_K(K[\underline{X}]/I) = \dim_C(C[\underline{X}]/J)$, denn G ist auch eine Gröbnerbasis von J nach dem Buchberger-Kriterium 2.5.4. Ist K vollkommen und I ein Radikalideal, so ist nach 2.8.9 auch J ein Radikalideal. Wir sehen also, dass wir Œ $K = C$ voraussetzen dürfen. Dann folgt alles aus 2.8.13 (und 2.8.1(d)). □

Korollar 2.8.15. *Sei G eine Gröbnerbasis des Ideals $I \subseteq K[\underline{X}]$ mit $\#V(I) < \infty$.*

(a) $\#V(I) \leq \#\,\mathrm{redM}(G) < \infty$

(b) Ist K vollkommen und I ein Radikalideal, so $\#V(I) = \#\,\mathrm{redM}(G)$.

Beweis. Nach 2.4.7(i) ist $\mathrm{red}(G) \to K[\underline{X}]/I$ ein K-Vektorraumisomorphismus. □

Bemerkung 2.8.16. (a) Ist G eine Gröbnerbasis des Ideals $I \subseteq K[\underline{X}]$, so kann man $\#\,\mathrm{redM}(G) \in \mathbb{N}_0 \cup \{\infty\}$ mit 2.4.11(a) leicht bestimmen.

(b) Gelte $\mathrm{char}\, K = 0$ und sei $F \subseteq K[\underline{X}]$ endlich. Dann kann man $\#V(F) \in \mathbb{N}_0 \cup \{\infty\}$ wie folgt bestimmen: Berechne mit dem Buchberger-Algorithmus 2.5.6 eine Gröbnerbasis G des Ideals $I := (F)$. Überprüfe mit 2.8.2 anhand von G, ob $\#V(I) = \infty$. Gelte nun $\#V(I) < \infty$. Berechne mit 2.8.11 ein endliches $F' \subseteq K[\underline{X}]$ mit $(F') = \sqrt{I}$. Berechne eine Gröbnerbasis G' von $\sqrt{I}$. Bestimme mit 2.4.11(a) $\#\,\mathrm{redM}(G')$. Nach 2.8.15(b) gilt $\#V(I) = \#V(\sqrt{I}) = \#\,\mathrm{redM}(G')$.