Einführung in die Algebra

Vorlesung im
Wintersemester 2006-2007
Technische Universität Berlin

gehalten von
Prof. Dr. M. Pohst

Contents

CHAPTER 6

Kurven

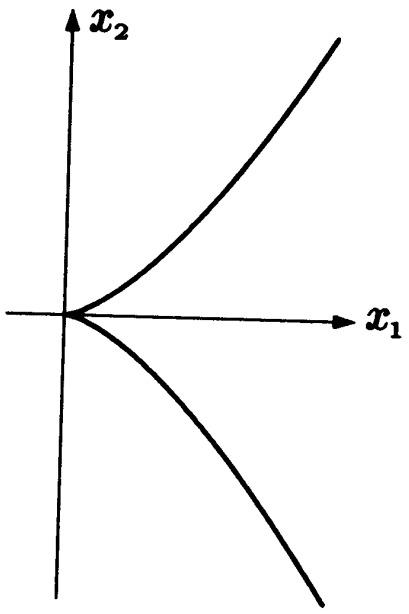
6.1. Einführende Beispiele

Der Einheitskreis im $\mathbb{R}^2$ hat die rationale Parametrisierung:

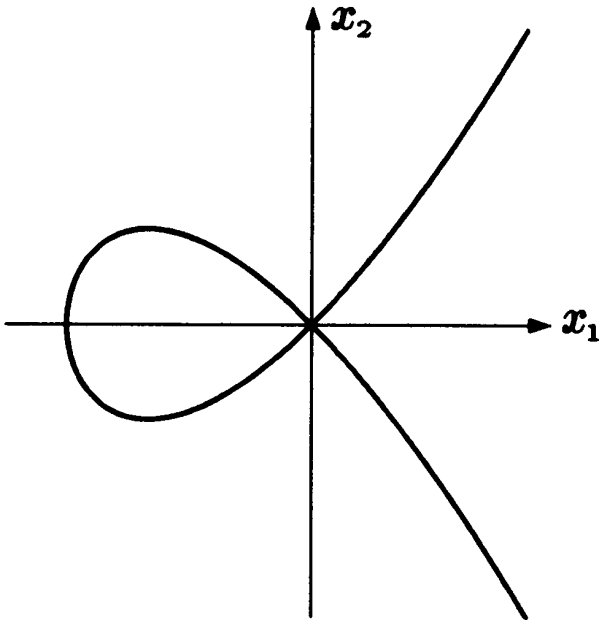
$$\varphi : \mathbb{R} \longrightarrow \mathbb{R}^2 : t \mapsto \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right).$$

Sie liefert $x^2 + y^2 = 1$ ohne $(0, 1)$.

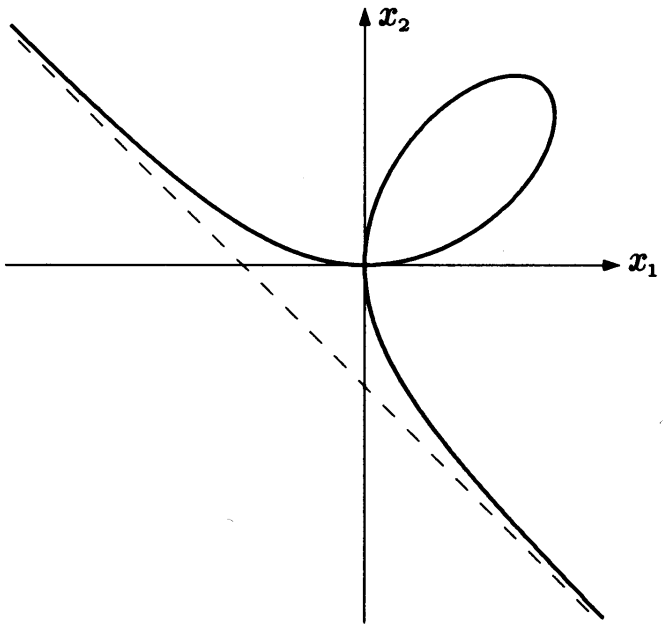
Die Neilsche Parabel: $x^3 - y^2 = 0$, $\varphi : \mathbb{R} \longrightarrow \mathbb{R}^2 : t \mapsto (t^2, t^3)$ hat Singularität in $(0, 0)$.



Newtonscher Knoten $y^2 = x^2(x + 1)$ hat die Parametrisierung $\varphi : \mathbb{R} \longrightarrow \mathbb{R}^2 : \quad t \mapsto (t^2 - 1, t - t^3)$.



Cartesisches Blatt : $x^3 + y^3 - 3xy = 0$



Blatt.png

Affin - algebraische Kurven

Es sei K ein Körper, i.a. algebraisch abgeschlossen, etwa $K = \mathbb{C}$.

6.2. Definition

Eine Teilmenge $C \subseteq K^2$ heißt affin-algebraische Kurve, wenn es $f \in K[x_1, x_2]$ gibt mit $\deg f \geq 1$ und $C = V(f) = \{(x_1, x_2) \in K^2 \mid$

$f(x_1, x_2) = 0\}$. $(V(f)$ heißt auch Varität von $f.)$

Beispiel

$$\begin{aligned}
(i) K = \mathbb{R}, \quad f = x_1^2 + x_2^2 - 1 \quad & C \text{ ist Kreis,} \\
x_1^2 + x_2^2 \quad & C \text{ ist Punkt,} \\
x_1^2 + x_2^2 + 1 \quad & C = \emptyset. \\
(ii) K = \mathbb{C} \quad f = x_1^2 + x_2^2 + 1 \quad & \text{hat} \\
V(f) = V(x_1 + ix_2) \cup V(x_1 - ix_2). &
\end{aligned}$$

Bemerkung $f \mid g \Longrightarrow V(f) \subseteq V(g)$.

6.3. Lemma (Study)

Es seien $f, g \in K[x_1, x_2]$, K algebraisch abgeschlossen. Ist f irreduzibel vom Grad ≥ 1 und $V(f) \subseteq V(g)$, so ist f ein Teiler von g.

Bemerkung Für $K = \mathbb{R}$ ist die Aussage falsch: $f = x_1^2 + x_2^2$, $g = x_1$.

Beweis Es seien $f = a_0 x_2^m + a_1 x_2^{m-1} + \ldots + a_m$, $g = b_0 x_2^n + b_1 x_2^{n-1} + \ldots + b_n \in K[x_1]\ [x_2]$ mit $a_0 b_0 \neq 0$. Vertauschen von x_1 und x_2, falls nötig, garantiert $m \geq 1$.

Wir schneiden die Mengen $V(f) \subseteq V(g)$ mit senkrechten Geraden $x_1 = \xi_1 \quad \forall \xi_1 \in K$. Es muss dann auch $n > 0$ gelten. Ansonsten wählt man ξ_1 mit $b_0(\xi_1) a_0(\xi_1) \neq 0$. Hiernach existiert $\xi_2 \in K$ mit $f(\xi_1, \xi_2) = 0 \neq g(\xi_1, \xi_2)$, also $V(f) \not\subseteq V(g)$.
Wir bilden nun die Resultante $\mathrm{Res}(f, g) \in K[x_1]$. Falls diese verschwindet, haben f und g einen gemeinsamen Teiler in $K[x_1]\ [x_2]$, also folgt (f irreduzibel!) $f \mid g$.
In jedem Fall ist $\mathrm{Res}(f, g)$ ein Polynom in $K[x_1]$. Also genügt der Nachweis, dass die Resultante für unendlich viele $\xi_1 \in K$ verschwindet. Es ist $a_0(\xi_1) \neq 0$ für fast alle $\xi_1 \in K$. Setzen wir nun $x_1 = \xi_1$ in f und g ein. so erhalten wir Polynome $f_{\xi_1}(x_2), g_{\xi_1}(x_2)$. In $K[x_2]$ gilt: $f_{\xi_1}(x_2) = \quad (x_2 - c_1)^{l_1} \cdot \ldots \cdot (x_2 - c_k)^{l_k}$. Dann sind gemäß $V(f) \subseteq V(g)$ auch $c_1, \ldots, c_k$ Nullstellen von g_{ξ_1}. Hiernach ist $(x_2 - c_1) \cdot \ldots \cdot (x_2 - c_k)$ ein gemeinsamer nicht konstanter Faktor von f_{ξ_1} und g_{ξ_1}. Es wird $\mathrm{Res}(f, g)(\xi_1) = \mathrm{Res}(f_{\xi_1}, g_{\xi_1}) \quad = 0$. $\square$

6.4. Korollar

Ist $f \in K[x_1, x_2]$ eine Nichteinheit, so ist $V(f) \neq \emptyset$.

Bemerkung Ist K algebraisch abgeschlossen, so enthält eine algebraische Kurve $C \subseteq K^2$ unendlich viele Punkte. Für $f = \prod_{i=1}^{r} f_i^{k_i}$ mit

irreduziblen nicht assoziierten f_i gilt

$$V(f) = \bigcup_{i=1}^{r} V(f_i).$$

6.5. Definition

Eine algebraische Kurve $C \subseteq K^2$ heißt reduzibel, wenn es algebraische Kurven $C_1 \neq C_2$ mit $C = C_1 \cup C_2$ gibt. C ist irreduzibel, falls aus einer Zerlegung $C = C_1 \cup C_2$ stets $C_1 = C_2$ folgt.

6.6. Lemma

Eine algebraische Kurve $C = V(f) \subseteq K^2$ ist genau dann irreduzibel, wenn es ein irreduzibles $g \in K[x_1, x_2]$ und $k \in \mathbb{N}$ mit $f = g^k$ gibt.

Beweis Ist C irreduzibel und $f = f_1 f_2$ mit teilerfremden f_i positiven Grades. Ist h irreduzibler Faktor von f_1, so folgt mit Study aus $V(h) \subseteq V(f_1) = V(f_2)$, dass h auch f_2 teilt.
Ist C dagegen reduzibel, also $V(f) = V(f_1) \cup V(f_2)$ mit $V(f_1) \neq V(f_2)$, so existieren nicht assoziierte irreduzible Faktoren h_i von f_i. Aus $V(h_i) \subseteq V(f)$ folgt mit Study, dass f mindestens zwei verschiedene Primfaktoren hat. □

6.7. Satz

Jede algebraische Kurve $C \subseteq K^2$ gestattet eine bis auf Reihenfolge eindeutige Darstellung
$C = C_1 \cup \ldots \cup C_r$ mit irreduziblen algebraischen Kurven $C_1, \ldots, C_r$.
(Die C_i heißen irreduzible Komponenten von C.)

Beweis Gemäß vorangehendem Lemma und der Primfaktorzerlegung von $f \in K[x_1, x_2]$ mit $C = V(f)$. Zur Eindeutigkeit: Für $C' \subseteq C$ irreduzibel ist $C' = V(f')$ mit f' irreduzibel. Nach Study gilt $f' \mid f$.
□

6.8. Korollar

Es sei $C = V(f)$ mit $f = f_1^{k_1} \cdot \ldots \cdot f_r^{k_r}$. Ist auch $C = V(g)$, so folgt $g = \lambda f_1^{l_1} \cdot \ldots \cdot f_r^{l_r}$ mit $\lambda \in K^\times$, $l_i \in \mathbb{N}$. Es ist folglich $\tilde{f} = f_1 \cdot \ldots \cdot f_r$ Minimalpolynom zur Kurve C.
$I(C) := \{h \in K[x_1, x_2] \mid \quad h \mid_C = 0\}$ ist Ideal in $K[x_1, x_2]$, das sogenannte Verschwindungsideal von C. ($I(C)$ ist Hauptideal, das vom Minimalpolynom erzeugt wird.)

Eine formale Summe $\sum_{i=1}^{r} k_i C_i$ mit irreduziblen C_i und $k_i \in \mathbb{Z}$ heißt Divisor. Sind alle $k_i \geq 0$, heißt der Divisor effektiv.

6.9. Definition

Ist $C = V(f)$ eine algebraische Kurve mit Minimalpolynom f, so heißt $\deg C := \deg f$ Grad der Kurve C.

Es sei L Gerade mit Parmetrisierung durch $\varphi : K \longrightarrow K^2 : t \mapsto (\varphi_1(t), \varphi_2(t))$ mit linearen Polynomen $\varphi_i(t) = \lambda_i t + \mu_i$. Zu $C = V(f)$ sei $g(t) = f(\varphi_1(t), \varphi_2(t))$. Die Nullstellen von g entsprechen Schnittpunkten von C mit L. Es ist $g = 0 \Longleftrightarrow L \subseteq C$.
Dann liefert $\deg g \leq \deg f$:

Bemerkung $\deg C = n$, $L \subset C$ Gerade $\Longrightarrow \sharp(C \cap L) \leq n$. (Für $f = f_0 + f_1 + \ldots + f_n$ mit $i = \deg f_i$ ist $f_n \neq 0$, f_n kann also höchstens für n verschiedene Steigungen λ_1/λ_2 von L verschwinden. Hindernisse: Ausnahmesteigung von L, mehrfache Nullstellen von g.)

6.10. Definition

Es sei $C = V(f)$ eine algebraische Kurve mit Minimalpolynom f. $P \in C$ heißt glatt, falls
$(\text{grad } f)\ (P) = \left(\frac{\partial f}{\partial x_1}(P), \frac{\partial f}{\partial x_2}(P)\right) \neq (0,0)$ ist. Ist C in P nicht glatt, heißt P singulärer Punkt.

Man mache sich die Bedeutung des Minimalpolynoms klar!

Projektive algebraische Kurven

Es sei $\mathbb{P}_2(K)$ die projektive Ebene über K. Sie besteht aus allen Geraden $K\underline{x} = K(\xi_0, \xi_1, \xi_2) \subseteq K^3$ durch den Ursprung.
Man schreibt $K\underline{x} = (\xi_0 : \xi_1 : \xi_2)$ ("homogene Koordinaten").
Beachte: $(\xi_0 : \xi_1 : \xi_2) = (\eta_0 : \eta_1 : \eta_2) \Longleftrightarrow \exists \lambda \in K^\times : (\xi_0, \xi_1, \xi_2) = \lambda(\eta_0, \eta_1, \eta_2)$.

Einbettung $\iota : K^2 \Longrightarrow \mathbb{P}_2(K) : (\xi_1, \xi_2) \mapsto (1 : \xi_1 : \xi_2)$. "Unendliche ferne Punkte":

$$\mathbb{P}_2(K) \backslash \iota(K^2) = \{(\xi_0 : \xi_1 : \xi_2) \in \mathbb{P}_2(K) \mid \xi_0 = 0\}.$$

Dies ist eine projektive Gerade $\mathbb{P}_1(K)$. (Es ist dim. $\mathbb{P}(V) = dimV - 1$.)

Wir betrachten die Fortsetzung einer affin-algebraischen Kurve $C \subseteq K^2$ zu einer projektiven Kurve $\tilde{C} \subseteq \mathbb{P}_2(K)$. Ist $F \in K[x_0, x_1, x_2]$ ein

homogenes Polynom, so heißt

$$V(F) := \{(\xi_0 : \xi_1 : \xi_2) \in \mathbb{P}_2(K) \mid F(\xi_0, \xi_1, \xi_2) = 0\}$$

.
Varietät von F; zu $f \in K[x_1, x_2]$ konstruiert man $F \in K[x_0, x_1, x_2]$ homogen (Homogenisierung von f) mittels:
$n = \deg f, \quad n_i = \deg f_i, \quad f = f_0 + f_1 + \ldots + f_n$, $F = \sum_{i=0}^{n} x_0^{n-i} f_i$.
Es ist $F = x_0^n f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right)$ sowie $f = F(1, x_1, x_2)$.

6.11. Definition

$\tilde{C} \subseteq \mathbb{P}_2(K)$ heißt projektiv-algebraische Kurve, falls es ein homogenes $F \in K[x_0, x_1, x_2]$ mit $\deg F \geq 1$ gibt, so dass $\tilde{C} = V(F)$ ist.
Ist $C = V(f) \subseteq K^2$ eine affin-algebraische Kurve und F die Homogenisierung von f, so heißt $\tilde{C} = V(F) \subseteq \mathbb{P}_2(K)$ der projektive Abschluss von C.

Beispiel
$f = x_1^3 - x_2^2$ hat $F = x_1^3 - x_0 x_2^2$.

6.12. Lemma

Es sei $f \in K[x_1, x_2]$ mit Homogenisierung $F \in K[x_0, x_1, x_2]$. Denn gilt: f irreduzibel $\iff$ F irreduzibel.

Beweis

(1) Sei f reduzibel, etwa $f = g \cdot h$. Wir haben dann

$$\begin{aligned}
f &= \sum_{i=0}^{m+n} f_i x_0^{m+n-i} \text{ mit } f_i \text{ homogen von Grad } i \text{ oder } f_i = 0,\\
g &= \sum_{j=0}^{m} g_j x_0^{m-j} \text{ mit } g_j \text{ homogen von Grad } j \text{ oder } g_j = 0,\\
h &= \sum_{k=0}^{n} h_k x_0^{n-k} \text{ mit } h_k \text{ homogen von Grad } k \text{ oder } h_k = 0,\\
gh &= \sum_{i=0}^{m+n} \Big(\sum_{j=0}^{i} g_j x_0^{m-j} h_{i-j} x_0^{n-(i-j)}\Big) = \sum_{i=0}^{m+n} f_i x_0^{m+n-i}.
\end{aligned}$$

(2) Es sei F reduzibel, etwa $F = G \cdot H$. Dann sind G, H homogen.

$$\begin{aligned}
G &= G_m + G_m + G_{m-1} + \ldots + G_0 \text{ mit } G_i = 0 \text{ oder } \deg G_i = i,\\
H &= H_n + H_{n-1} + \ldots + H_0 \text{ analog},\\
F &= F_{m+n}\\
GH &= G_m H_n + \ldots
\end{aligned}$$

Wäre oBdA G nicht homogen, so existiert $m > i_0$ minimal mit $G_{i_0} \neq 0$. Ferner sei $n \geq j_0$ minimal mit $H_{j_0} \neq 0$. Hierfür gilt $\deg(G_{i_0} H_{j_0}) = i_0 + j_0 < \deg(G_\mu H_\nu)$ für $\mu > i_0, \nu \geq j_0$ oder $\mu = i_0, \nu > j_0$. Demnach muss

$G_{i_0} \cdot H_{j_0} = 0$ gelten, also speziell $G_{i0} = 0$ im Widerspruch zur Annahme. Nunmehr erhalten wir $f = F(1, x_1, x_2) = G(1, x_1, x_2)H(1, x_1, x_2) = g \cdot h$ mit $\deg g = \deg G, \deg h = \deg H$, so dass f reduzibel ist. $\square$

Der Grad von $\tilde{C}$ wird als Grad eines zugeh. Minimalpolynoms F erklärt. Dieses ist homogen und erzeugt ein Ideal $I(\tilde{C}) = \{G \in K[x_0, x_1, x_2] \mid G(\xi_0, \xi_1, \xi_2) = 0 \quad \forall (\xi_0 : \xi_1 : \xi_2) \in \tilde{C}\}$.
Wir merken an, dass wir mittels $PGL(2, K) \cong GL(3, K)/\sim$, wobei $A \sim \tilde{A} :\Longleftrightarrow \exists \lambda \in K^\times : A = \lambda \tilde{A}$ ist, Koordinatentransformationen vornehmen können.

Aussagen über den Durchschnitt von Kurven

Es sei zunächst $C = V(F) \subseteq \mathbb{P}_2(K)$ mit $\deg C \geq 1$. Wir wählen die Koordinaten so, dass eine schneidende Gerade durch $x_2 = 0$ beschrieben wird. $C \cap L$ besteht folglich aus den Nullstellen von $G(t_0, t_1) := F(t_0, t_1, 0)$. Wir schreiben (für das Minimalpolynom F von C)

$$F(x_0, x_1, x_2) = F_0 x_2^n + F_1 x_2^{n-1} + \ldots + F_n$$

mit homogenen $F_i \in K[x_0, x_1]$ vom Grad i (für $F_i \neq 0$). Es ist folglich $G = F_n$. Ist $F_n = 0$, so wird F von x_2 geteilt, dass heißt es gilt $L \subseteq C$. Andernfalls ist $\deg G = n$ (nur im Projektiven!) und wir erhalten (K algebraisch abgeschlossen!)
$G = (b_1 t_0 - a_1 t_1)^{k_1} \cdot \ldots \cdot (b_m t_0 - a_m t_1)^{k_m}$ mit eind. best., paarweise verschiedenen Punkten $(a_\mu : b_\mu) \in \mathbb{P}_1(K)$, $\mu = 1, \ldots, m$, $k_\mu \in \mathbb{N}$.

(Die k_μ sind dabei nur von C und L, nicht aber von der Wahl der Koordinaten abhängig.)
Man erklärt folglich $mult_p(C \cap L) := k$ als Schnittmultiplizität von C und L, wobei $k = k_\mu$ für $P = (a_\mu : b_\mu : 0) \quad (1 \leq \mu \leq m)$ sowie $k = 0$ für die übrigen $P \in \mathbb{P}_2(K)$ gilt. Wegen $k_1 + \ldots + k_m = n$ folgt:

Bemerkung Ist $C \subseteq \mathbb{P}_2(K)$ eine Kurve vom Grad $n \geq 1$ und L eine nicht in C enthaltene Gerade, so ist die Gesamtzahl der Schnittpunkte von C und L, entsprechend den Multiplizitäten gezählt, gerade n. Für fast alle Geraden L sind die Schnittpunkte $C \cap L$ einfach, dass heißt es gibt genau n Schnittpunkte. Man vergleiche dazu nachfolgende Proposition.

6.13. Proposition

Es sei C ebene Kurve der Ordnung n, P Punkt, $P \notin C$. Dann gibt es unter der Geraden durch P höchstens $n(n-1)$ Geraden L_i, so dass jede Gerade $L \neq L_i$ die Kurve C in genau n verschiedenen Punkten schneidet.

Beweis Wähle homogene Koordinaten $(x_0 : x_1 : x_2)$ mit $P = (0 : 0 : 1)$. Es sei $F(x_1, x_2, x_3)$ das Minimalpolynom zu C. Es gibt eine Bijektion zwischen der Familie $\mathcal{L}$ aller Geraden durch P und einer festen projektiven Geraden G mit der Gleichung $x_2 = 0$, indem wir $L \in \mathcal{L}$ den Schnittpunkt $\lambda = (\lambda_0 : \lambda_1 : 0)$ mit G zuordnen. Die Gerade durch λ und P sei L_λ. Es ist $L_\lambda = aP + bQ$, also $(a, b \in K)$,

$$L_\lambda \backslash \{P\} = \{(\lambda_0 : \lambda_1 : t) \in \mathbb{P}_2(K) \mid t \in K\}.$$

Die Schnittpunkte von L_λ mit C werden durch $F(\lambda_0, \lambda_1, t) = 0$ gegeben. $F(\lambda_0, \lambda_1, t)$ verschwindet nicht identisch, weil kein L_λ Komponente von C ist. Wegen $P \notin C$ hat es den Grad n. (Die $F_i (i \geq 1)$ sind homogene Polynome in x_1, x_2 vom Grad i, verschwinden also in $(0 : 0 : 1)$.) Es besitzt mehrfache Nullstellen, genau dann, wenn seine Diskriminante verschwindet. Letztere ist $\mathrm{Res}(\lambda_0, \lambda_1) = \mathrm{Res}(F(\lambda_0, \lambda_1, t), \frac{\partial F}{\partial t}(\lambda_0, \lambda_1, t))$, also ein homogenes Polynom in λ_0, λ_1 vom Grad
$n(n-1)$; die Resultante besitzt also $n(n-1)$ Nullstellen $\lambda^{(i)}$. In $\mathcal{L}$ besitzen also höchstens die Geraden $L_i = L_{\lambda^{(i)}}$ mit der Kurve C Schnittpunkte höherer Multiplizität. □

Beispiel Es seien $C = V(x_0 x_2^2 - x_1^3), L : (t_0 : t_1) \mapsto (t_0 : \lambda_0 t_1 : \lambda_1 t_1) = x(t)$. L geht durch $P = (1 : 0 : 0)$; $(\lambda_0 : \lambda_1) \in \mathbb{P}_1(K)$ bestimmt die "Steigung" im Affinen. Es ist $F(x(t)) = G(t) = t_1^2 \ (\lambda_1^2 t_0 - \lambda_0^3 t_1)$. t_1^2 beschreibt den Schnittpunkt P, der 2. Faktor einen Schnittpunkt

$$Q = (\lambda_0^3 : \lambda_0 \lambda_1^2 : \lambda_1^3). \quad \text{(Mittels Einsetzen von } t_1 = \lambda_1^2, t_0 = \lambda_0^3 \text{ in } L.)$$

Ist die Gerade waagerecht, so wird $(\lambda_0 : \lambda_1) = (1 : 0)$, $P = Q$, $mult_P(C \cap L) = 3$.

Anzahl der Schnittpunkte zweier Kurven C und C'

Wir nehmen an, dass C und C' keine gemeinsame Komponente haben. Außerdem sei $\deg C = m$, $\deg C' = n$.
Dann wollen wir $\sharp C \cap C' < \infty$ zeigen.
Dazu wählt man einen Punkt $q \notin C \cup C'$ und eine Gerade L, die nicht durch q geht, und projiziert $\mathbb{P}_2(K) \backslash \{q\}$ von q auf L. Bei dieser Projektion π wird die Gerade L_c durch q und durch $c \in L$ auf c abgebildet.

Auf jeder solchen Geraden L_c liegen nach obiger Bemerkung nur endlich viele Punkte von $C \cap C'$. Es genügt also der Nachweis, dass nur für endlich viele $c_i \in L$ Schnittpunkte von $C \cap C'$ auf L_{c_i} liegen.
Zur Bestimmung der L_{c_i} verfährt man folgendermaßen. Wir wählen homogene Koordinaten $(x_0 : x_1 : x_2) \in \mathbb{P}_2(K)$, so dass $x_2 = 0$ die Gleichung von L ist und $q = (0 : 0 : 1)$ gilt. Danach sind $(x_0 : x_1)$ homogene Koordinaten von L und $\pi : \mathbb{P}_2(K)\backslash\{q\} \longrightarrow L : (x_0 : x_1 : x_2) \mapsto (x_0 : x_1)$. Bezüglich dieser Koordinaten seien $F(x_0, x_1, x_2) = 0$ und $F'(x_0, x_1, x_2)$ homogene Minimalpolynome für C, C' mit Graden m bzw. n. Wir schreiben sie als

$$F = A_0 x_2^m + A_1 x_2^{m-1} + \ldots + A_m \text{ bzw. } F' = B_0 x_2^n + B_1 x_2^{n-1} + \ldots + Bn.$$

Dabei sind die $A_i, B_j \in K[x_0, x_1]$ homogene Polynome vom Grad i bzw. j (falls sie nicht identisch verschwinden). Wegen $q \notin C \cup C'$ und $q = (0 : 0 : 1)$ muss $A_0 B_0 \neq 0$ sein (vgl. Beweis zu voriger Proposition). C, C' haben nach Voraussetzung keine gemeinsame Komponente, F und F' also keinen gemeinsamen Faktor, d. h. $0 \neq \mathrm{Res}_{x_2}(F, F')$ ist ein homogenes Polynom vom Grad mn. Es sei nun $p = (d_0 : d_1 : d_2)$ ein Schnittpunkt von C und C'.

Dann gilt $F(d_0, d_1, d_2) = F'(d_0, d_1, d_2) = 0$, es ist also d_2 eine gemeinsame Lösung von
$A_0(d_0, d_1)x_2^m + A_1(d_0, d_1)x_2^{m-1} + \ldots + A_m(d_0, d_1) = 0 = B_0(d_0, d_1)x_2^n + B_1(d_0, d_1)x_2^{n-1} + \ldots + B_n(d_0, d_1)$.
Demnach ist $\mathrm{Res}_{x_2}(F, F')(d_0, d_1) = 0$, und diese Bedingung ist für die Existenz einer Lösung
auch hinreichend.
Die Nullstellen von $\mathrm{Res}_{x_2}(F, F')$ sind also genau die $d \in L$, für die auf der Geraden L_d
ein Schnittpunkt von C und C' liegt.

6.14. Proposition

Es gilt $\sharp C \cap C' \leq m \cdot n$ unter den gemachten Voraussetzungen.

Beweis Annahme, es existieren $m \cdot n + 1$ Schnittpunkte $P_1, \ldots, P_{mn+1}$. Wir wählen nun q, L wie zuvor und q zudem so, dass es auf keiner Verbindungsgeraden von P_i nach P_j liegt $(i \neq j)$. Dann haben P_i und P_j für $i \neq j$ unter π verschiedene Bilder $c_i \neq c_j$ auf L. Dies liefert auf L mindestens $mn+1$ verschiedene Punkte $c_1, \ldots, c_{mn+1}$, die Nullstellen der Resultante $\mathrm{Res}_{x_2}(F, F')$ sind. Letztere war jedoch homogen vom Grad mn, so dass wir einen Widerspruch zu unserer Annahme erhalten. □

6.15. Definition

Es seien C, C' Kurven in $\mathbb{P}_2(K)$ ohne gemeinsame Komponente und P_i deren gemeinsame Schnitt-
punkte. Die Koordinaten $(x_0 : x_1 : x_2)$ seien so gewählt, dass $(0 : 0 : 1)$ auf keiner Verbindungsgeraden zweier Schnittpunkte liegt. Es seien $F(x_0, x_1, x_2)$, $F'(x_0, x_1, x_2)$ die Minimalpolynome zu C, C'. Es sei $P_i = (c_{oi} : c_{1i} : c_{2i})$ sowie $c_i := (c_{0i} : c_{1i})$. Dann wird die Schnittmultiplizität $\nu_{P_i}(C, C')$ als Multiplizität der Nullstelle c_i von $\mathrm{Res}_{x_2}(F, F')$ definiert.

6.16. Satz von Bezout

Für die Summe der Schnittmultiplizitäten von C und C' mit Graden m, n gilt: $\sum_{P \in C \cap C'} \nu_P(C, C') = m \cdot n$.

Bemerkung Dies gilt auch, falls F, F' nicht die Minimalpolynome sind, wenn die Vielfachheiten entsprechend gezählt werden.

Beispiele

(1) $C = V(x_2^3 - x_0x_1^2)$, $C' = V(x_2^3 + x_0x_1^2)$. $\mathrm{Res}_{x_2}(x_0, x_1) = -8x_0^3x_1^6$; Schnittpunkte sind demnach $q = (0 : 1 : 0)$ mit Multiplizität 3 sowie $p = (1 : 0 : 0)$ mit Multiplizität 6.
Dazu beachten wir die Resultantengesetze:
$\mathrm{Res}(a_0, B) = a_0^{\deg(B)}$, und für $A = QB + R$ (A, B normiert, Division mit Rest) gilt $\mathrm{Res}(A, B) = (-1)^{\deg B(\deg A - \deg R)}\mathrm{Res}(R, B)$.

(2) $C = V(x_0x_2^2 - x_1^3)$ Neilsche Parabel,
$C' = V(x_0x_2^2 - x_1^2(x_1 - x_0))$ Newton's Knoten;
es ist $A = 1 \cdot B + x_1^2x_0$, also $\mathrm{Res}(A, B) = -\mathrm{Res}(x_1^2x_0, B) = -x_1^6x_0^3$ analog zu (i).

(3) Newtons Knoten (siehe ii)) mit Krümmungskreis und Ellipse:

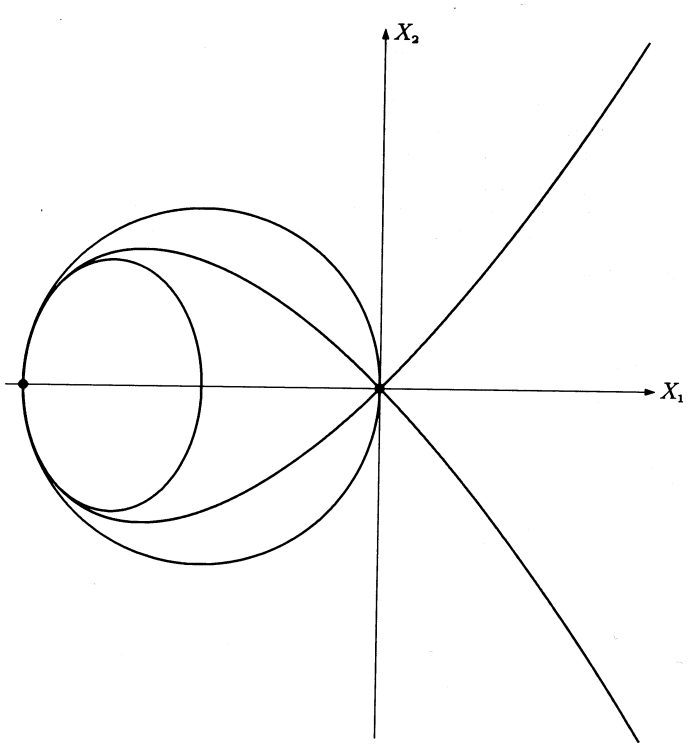
$$F = x_0x_2^2 - x_1^3 - x_1^2x_0.$$

Für den Krümmungskreis $F' = x_1^2 + x_2^2 + x_0x_1$ erhalten wir:
$F = x_0F' + R = x_0x_1^2 + x_0x_2^2 + x_0^2x_1 + (-2x_0x_1^2 - x_0^2x_1 - x_1^3)$, also

$$\begin{aligned} \mathrm{Res}(F, F') &= (2x_0x_1^2 + x_0^2x_1 + x_1^3)^2 \\ &= x_1^2(x_0^2 + 2x_0x_1 + x_1^2)^2 \\ &= x_1^2(x_0 + x_1)^4 \end{aligned}$$

und damit die Schnittpunkte $(1 : 0 : 0)$ mit Multiplizität 2 sowie $(1 : -1 : 0)$ mit Multiplizität 4.

Für die Ellipse $F' = x_0^2 + 2x_1^2 + x_2^2 + 3x_0x_1$ bekommt man
$F = x_0F' + R = x_0^3 + 2x_0x_1^2 + x_0x_2^2 + 3x_0^2x_1 - x_0^3 - 3x_0x_1^2 - 3x_0^2x_1 - x_1^3 = x_0F' - (x_0 + x_1)^3$, also
$\mathrm{Res}(F, F') = (x_0 + x_1)^6$ und damit den Schnittpunkt $(1 : -1 : 0)$ der Multiplizität 6.



Tangenten und Singularitäten

Ist eine Kurve C glatt im Punkt $P \in C$, das heißt $\operatorname{grad}_P(f) = \left(\frac{\partial f}{\partial x_1}(P), \frac{\partial f}{\partial x_2}(P)\right) \neq (0,0)$ für das Minimalpolynom f von C, so heißt die Gerade

$$T_p(C) = \{(x_1, x_2) \in K^2 \mid \frac{\partial f}{\partial x_1}(P)x_1 + \frac{\partial f}{\partial x_2}(P)x_2 = c\}$$

Tangente an C im Punkt P; dabei ist $c \in K$ so zu wählen, dass $P \in T_P(C)$ ist.

Bemerkung Jeder Schnittpunkt von (verschiedenen) Komponenten ist singulär. Dies zeigt man mit dem Satz über implizite Funktionen. Die Menge $\operatorname{Sing}(C) := \{P \in C \mid C \text{ singulär in } P\}$ heißt Singularitätenmenge von C.

Bemerkung Für eine algebraische Kurve $C \subseteq K^2$ ist $\operatorname{Sing}(C)$ endlich.

Beweis Für $C = V(f)$ setzen wir $C_i := V\left(\frac{\partial f}{\partial x_i}\right) \quad (i = 1, 2)$. Es ist $\operatorname{Sing}(C) = C \cap C_1 \cap C_2$! Da eine Gerade in jedem Punkt glatt ist, können wir oBdA $\deg C = \deg f \geq 2$ annehmen. Damit existiert $i \in \{1, 2\}$ mit $\deg\left(\frac{\partial f}{\partial x_i}\right) \geq 1$. OBdA sei $i = 1$. Dann ist C_1 eine algebraische Kurve, und es ist $\operatorname{Sing}(C) \subseteq C \cap C_1$. Also genügt der Nachweis, dass $C \cap C_1$ endlich ist. Dazu benutzen wir den Satz von Bezout, allerdings

für Divisoren, da $\frac{\partial f}{\partial x_1}$ nicht notwendig das Minimalpolynom von C_1 ist (etwa: $f = x_1x_2^2 + 1$). Es genügt demnach zu zeigen, dass C und C_1 keine gemeinsame Komponente besitzen. Wir nehmen daher an, dass f und $\frac{\partial f}{\partial x_1}$ einen gemeinsamen Primfaktor g besitzen. Es gilt sodann $f = gh$ und $gh_1 = \frac{\partial f}{\partial x_1} = h\frac{\partial g}{\partial x_1} + g\frac{\partial h}{\partial x_1}$. Hiernach teilt g auch $h\frac{\partial g}{\partial x_1}$. Ist $\frac{\partial g}{\partial x_1} \neq 0$, so muss g auch h teilen, damit $g^2 \mid f$ im Widerspruch dazu, dass f als Minimalpolynom gewählt war. Ist dagegen $\frac{\partial g}{\partial x_1} = 0$, so folgt $(\chi(K) = 0!) \quad g = x_2 - a$. Dies können wir aber ausschließen, indem wir die Koordinaten bereits anfangs so wählen, dass C keine achsenparallele Gerade enthält. □

Bemerkung Ist also $\deg C = n$, so hat C höchstens $n(n-1)$ singuläre Punkte.

Untersuchung der Art von Singularitäten

Es sei $f \in K[x_1, x_2]$ und $P = (p_1, p_2) \in K^2$ ein fester Punkt. Die Substitutionen $x_i = p_i + (x_i - p_i)$ führen zu einer Taglorentwicklung von f im Punkt P:

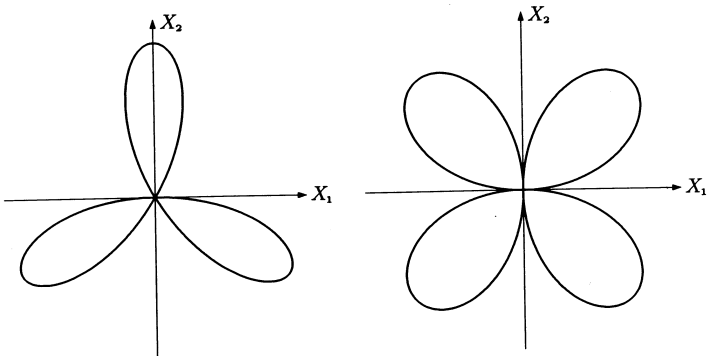
$$f(x_1, x_2) = \sum_k f_k \text{ mit } f_k = \sum_{\mu+\nu=k} a_{\mu\nu}(x_1-p_1)^\mu(x_2-p_2)^\nu \text{ mit } a_{\mu\nu} = \frac{1}{\mu!\nu!}\frac{\partial^{\mu+\nu} f}{\partial x_1^\mu \partial x_2^\nu}(P).$$

Damit lässt sich die Ordnung von f in P definieren als $\operatorname{ord}_P(f) := \min\{k \in \mathbb{Z}^{\geq 0} \mid f_k \neq 0\}$. Ist f Minimalpolynom von $C \subseteq K^2$, so ist $\operatorname{ord}_P(C) := \operatorname{ord}_P(f)$ die Ordnung von P auf C. Es gilt offenbar:

(1) $0 \leq \operatorname{ord}_P(C) \leq \deg C$,
(2) $P \in C \iff \operatorname{ord}_P(C) > O$,
(3) C glatt in $P \in C \iff \operatorname{ord}_P(C) = 1$,
(4) C singulär in $P \in C \iff \operatorname{ord}_P(C) > 1$.

Der Extremfall $\operatorname{ord}_P(C) = \deg C =: n$ tritt genau dann auf, wenn $f = f_n$ gilt. Demnach muss dann C aus n verschiedenen Geraden durch P bestehen. Folglich sind bei einer irreduziblen Kubik alle singulären Punkte von der Ordnung 2.

Beispiel Bei der Quartik $V((x_1^2 + x_2^2)^2 + 3x_1^2x_2 - x_2^3)$ (dreiblättriges Kleeblatt) hat der Ursprung die Ordnung 3, bei der Sextik $V((x_1^2 + x_2^2)^3 - 4x_1^2x_2^2)$ (vierblättriges Kleeblatt) die Ordnung 4.



6.17. Lemma

Eine Kurve $C \subseteq \mathbb{P}_2(K)$ ohne Gerade als Komponente und mit einem Punkt P der Ordnung $\mathrm{ord}_P(C) = \deg C - 1$ gestattet eine rationale Parametrisierung; das heißt es existiert $\varphi : \mathbb{P}_1(K) \longrightarrow C \subset \mathbb{P}_2(K) : t = (t_0 : t_1) \mapsto (\varphi_0(t) : \varphi_1(t) : \varphi_2(t))$ surjektiv, wobei $\varphi_i \in K[T_0, T_1]$ homogen vom Grad $\deg C$ sind.

Beweis Es sei $C = V(F)$ und $n = \deg F$. Wir nehmen $P = (0,0) \in K^2$ an. Danach ist $f(x_1, x_2) = F(1, x_1, x_2) = f_{n-1} + f_n$. Zu $(t_0 : t_1)$ betrachten wir die Gerade durch P mit dieser Steigung: $x_1 = \lambda t_0, x_2 = \lambda t_1$ mit $\lambda \in K$. Schneiden mit C liefert: $0 = f_{n-1}(\lambda t_0, \lambda t_1) + f_n(\lambda t_0, \lambda t_1) = \lambda^{n-1} f_{n-1}(t_0, t_1) + \lambda^n f_n(t_0, t_1) = \lambda^{n-1}(f_{n-1}(t_0, t_1) + \lambda f_n(t_0, t_1))$. Da C nach Voraussetzung keine Gerade enthält, gibt es nach Bezout neben dem Schnittpunkt P der Vielfachheit $n-1$ (zu $\lambda = 0$) einen weiteren zu $\lambda = -f_{n-1}(t_0, t_1)/f_n(t_0, t_1)$. Speziell haben f_{n-1} und f_n keine gemeinsame Nullstelle. Die gesuchte Parametrisierung ist demnach $(t_0 : t_1) \mapsto (f_n(t_0, t_1) : -t_0 f_{n-1}(t_0, t_1) : -t_1 f_{n-1}(t_0, t_1))$. □

Beispiel Dreiblättriges Kleeblatt.

Abhängigkeit der Schnittmultiplizitäten zweier Kurven von der Ordnung

Es sei $C = V(f)$ mit $f \in K[x_1, x_2]$, $f = \sum_{k=r}^{n} f_k$, $r = \mathrm{ord}_0(f)$, $n = \deg f$. (Entwicklung in $P = (0,0)$). Wir schneiden mit der Geraden L parametrisiert mittels
$\varphi(T) = (\lambda_1 T, \lambda_2 T)$, also $g(T) = f(\varphi(T)) = \sum_{k=r}^{n} f_k(\lambda_1, \lambda_2) T^k$. Hierfür ist die Schnittmultiplizität erklärt durch $\mathrm{mult}_P(C \cap L) = \mathrm{ord}_P(g)$ (vgl. vorigen Abschnitt). Es ist nun $\mathrm{ord}_P(g) > r$ genau im Fall $f_r(\lambda_1, \lambda_2) = 0$. Damit ist gezeigt:

Bemerkung Ist $C \subseteq K^2$ eine algebraische Kurve und L eine Gerade durch $P \in C$, so gilt

$\mathrm{ord}_P(C) \leq \mathrm{mult}_P(C \cap L)$. Dies ist für höchstens $\mathrm{ord}_P(C)$ Stück Geraden durch P eine echte Ungleichung.

Wir setzen noch $\mathrm{mult}_P(L \cap C) := \infty$ im Fall $P \in L \subset C$.

6.18. Definition

Unter den obigen Voraussetzungen heißt L Tangente an C in P, wenn $\mathrm{ord}_P(C) < \mathrm{mult}_P(C \cap L)$ gilt.

Bemerkung Falls C in P glatt ist, so stimmt diese Definition mit der früher gegebenen überein; es gibt genau eine Tangente. Im Fall $r = \mathrm{ord}_P(C)$ heißt P gewöhnlicher r-facher Punkt, wenn es r verschiedene Tangenten in P gibt, dass heißt wenn f_r (bei Entwicklung von f aus $C = V(f)$ in P) r verschiedene Nullstellen $(\lambda_1 : \lambda_2)$ in $\mathbb{P}_1(K)$ hat. Diese geben dann die Steigungen der Tangenten an.

Beispiele:

(1) Neilsche Parabel $x_1^3 - x_2^2 = 0$ in $P = (0,0)$: Wir haben $f = \quad f_2 + f_3 \quad$ mit $f_2 = -x_2^2, \quad f_3 = x_1^3$ und parametrisieren mit $\varphi(T) = \quad (\lambda_1 T, \lambda_2 T)$. Wir erhalten $g(T) = f(\varphi(T)) = f_2(\lambda_1, \lambda_2)T^2 + f_3(\lambda_1, \lambda_2)T^3$ und damit $\mathrm{ord}_P(C) = 2$. Für $\lambda_1 \neq 0$, $\lambda_2 = 0$ folgt $\mathrm{ord}_P(g) = 3$.

(2) $x_2^2 - x_1^3 - x_1$ ist glatt in 0. Wir haben $f = f_1 + f_2 + f_3$ mit $f_1 = -x_1$. Damit wird $g(T) = -\lambda_1 T + \lambda_2^2 T^2 - \lambda_1^3 T^3$, also $\mathrm{ord}_P(C) = 1$. Für $\lambda_1 = 0$ erhalten wir eine Tangente.

Aus der Taylorentwicklung folgt:

6.19. Lemma

Es sei $C = V(f) \subseteq K^2$ glatt in $P = (0,0)$ mit Tangente $T = V(x_2)$. Ist dann
$k := \mathrm{mult}_P(C \cap T) < \infty$, so ist $f(x_1, x_2) = x_1^k g(x_1) + x_2 h(x_1, x_2)$ mit $g(0) \neq 0$, $h(0,0) \neq 0$.

6.20. Definition

Die Tangente T in einem glatten Punkt $P \in C$ heißt einfach $:\Longleftrightarrow$ $\mathrm{mult}_P(C \cap T) = 2$, Wendetangente $:\Longleftrightarrow \mathrm{mult}_P(C \cap T) \geq 3$. Im letzten Fall heißt P Wendepunkt (unter Ausschluss von $\mathrm{mult}_P(C \cap T) = \infty$). Ein Wendepunkt heißt einfach im Fall $\mathrm{mult}_P(C \cap T) = 3$. T heißt Doppeltangente, falls sie Tangente in mindestens 2 verschiedenen glatten Punkten von C ist.

6.21. Satz

Es seien $C, C' \subset K^2$ algebraische Kurven ohne gemeinsame Komponente sowie $P \in C \cap C'$. Dann gilt: $\text{mult}_P(C \cap C') \geq \text{ord}_P(C)\text{ord}_P(C')$ mit Gleichheit genau dann, wenn C und C' in P keine gemeinsame Tangente haben.

Beweis Wir setzen $r = \nu_P(C)$ und $s = \nu_P(C')$. Dann wählen wir das Koordinatensystem, so dass $P = (1 : 0 : 0)$ gilt und $q = (0 : 0 : 1)$ weder auf $C \cup C'$ noch auf einer Verbindungsgeraden zweier Schnittpunkte von C und C', noch auf einer Tangente an C oder C' in P liegt. Es seien $f(x_1, x_2) = F(1, x_1, x_2)$, $f'(x_1, x_2) = F'(1, x_1, x_2)$ die zugehörigen Polynome mit Resultante $R := \text{Res}_{x_2}(f, g)$. Die Ordnung der Nullstelle $x_1 = 0$ von R ist gleich der Ordnung der Nullstelle $(1 : 0)$ von $\text{Res}_{x_2}(F, G)$, also gleich $\nu_p(C, C')$.

Wir untersuchen folglich R genauer. Aus $\nu_P(C) = r$ und $\nu_P(C') = s$ sowie $P = (1 : 0 : 0)$ folgt

$$f(x_1, x_2) = f_0 x_2^m + f_1 x_2^{m-1} + \ldots + f_{m-r} x_2^r + f_{m-r+1} x_2^{r-1} x_1 + \ldots + f_m x_1^r x_2^0,$$
$$g(x_1, x_2) = g_0 x_2^n + g_1 x_2^{n-1} + \ldots + g_{n-s} x_2^s + g_{n-s+1} x_1 x_2^{s-1} + \ldots + g_n x_1^s x_2^0$$

mit Koeffizienten $f_i, g_j \in K[x_1]$. Die Gleichungen der Tangenten in $P = (1 : 0 : 0)$ an C bzw. C' sind nun

$$T_1 := f_{m-r}(0) x_2^r + f_{m-r+1}(0) x_1 x_2^{r-1} + \ldots + f_m(0) x_1^r = 0;$$
$$T_2 := g_{n-s}(0) x_2^s + g_{n-s+1}(0) x_1 x_2^{s-1} + \ldots + g_n(0) x_1^s = 0.$$

Die Tangenten von C sind paarweise verschieden von denen von C', falls keine gemeinsamen nicht trivialen Lösungen existieren, das heißt $R_1 := \text{Res}_{x_2}(T_1(1, x_2), T_2(1, x_2)) \neq 0$ gilt. Die weitere Voraussetzung, dass auf der Verbindungsgeraden $x_1 = 0$ von P und q kein weiterer Schnittpunkt liegt, hat die Konsequenz, dass $f(0, x_2) = 0$ und $g(0, x_2) = 0$ nur $x_2 = 0$ als gemeinsame Lösung haben; es haben nämlich $f(0, x_2) = f_0(0) x_2^{m-r} + f_1(0) x_2^{m-r-1} + \ldots + f_{m-r}(0) = 0$ und $g(0, x_2) = g_0(0) x_2^{n-s} + g_1(0) x_2^{n-s-1} + \ldots + g_{n-s}(0) = 0$ keine gemeinsame Lösung wegen $f_{m-r}(0) \neq 0 \neq g_{n-s}(0)$, denn $x_1 = 0$ ist keine gemeinsame Tangente an C und C' in P. Dies bedingt nun $R_2 := \text{Res}_{x_2}(f(0, x_2), g(0, x_2)) \neq 0$.

Nunmehr betrachten wir R selbst.
Wir multiplizieren Zeile $(n - s + i)$ mit $x_1^i \quad (1 \leq i \leq s)$.
Wir multiplizieren Zeile $(n + m - r + j)$ mit $x_1^j \quad (1 \leq j \leq r)$.
Damit wird R zu $\tilde{R} = R x_1^{r(r+1)/2 + s(s+1)/2}$, die zugehörige Matrix sei

$M_{\tilde{R}}$. Jetzt teilen wir Spalte $(m+n-\mu)$ von $M_{\tilde{R}}$ durch x_1^{r+s} $(0 \le j \le r+s-1)$. Damit wird R zu $\hat{R} = \tilde{R}x_1^{-(r+s)(r+s+1)/2}$ sowie $\hat{R} = x_1^{-rs}R$ bzw.

$$R = x_1^{rs}\hat{R}, \tag{1}$$

wobei die Einträge in $\hat{R}$ Polynome in x_1 sind. Durch Entwicklung nach den ersten $n+m-r-s$ Spalten sieht man dann ein:

$$R(0) = R_1 \cdot R_2. \tag{2}$$

Die erste Behauptung folgt dann aus (6.1). Die Aussage über Gleichheit ist eine Konsequenz von

- (6.1) und (6.2),
- $R_2 \neq 0$ gemäß unserer Wahl des Koordinatensystems,
- $R_1 \neq 0$, falls die Tangenten in P von C und C' paarweise verschieden sind. □

Beispiele:

(1) Für $C = V(x_1)$, $C_n = V(x_2^n + x_0^{n-1}x_1)$, $P = (1:0:0)$ ist $\mathrm{mult}_P(C_1 \cap C_n) = n$. (Vgl. Resultanteneigenschaften in Beispiel (i) auf Seite 152.)

(2) Für $C = V(x_2^3 + x_0x_1^2)$ mit Spitzentangente $V(x_1)$ in P, C_n wie in (a) gilt
$\mathrm{mult}_P(C \cap C_n) = 3$.

(Beweis zu (b)) Es ist $\mathrm{Res}_{x_2}(F, F_n)$ - bis auf Vorzeichen - gleich dem Produkt $R := \prod_{i=1}^{n} F(y_i)$, wobei $y_1, \ldots, y_n$ die Nullstellen von F_n sind. Offenbar ist $y_i = \xi^i(-x_0^{n-1}x_1)^{1/n}$ mit einer primitiven n-ten Einheitswurzel ξ in einem geeigneten Erweiterungskörper von $K(x_0, x_1)$. Damit gilt:

$$\begin{aligned} K[x_0, x_1] \ni R &= \prod_{i=1}^{n}((\xi^i(-x_0^{n-1}x_1)^{1/n})^3 + x_0x_1^2) \\ &= \pm x_0^{3(n-1)}x_1^3 + x_1^4 g(x_0, x_1). \end{aligned}$$ □)

6.22. Formel von Euler

Es sei $F \in K[x_0, x_1, x_2]$ homogen vom Grad n, dann gilt:

$$x_0\frac{\partial F}{\partial x_0} + x_1\frac{\partial F}{\partial x_1} + x_2\frac{\partial F}{\partial x_2} = nF.$$

Beweis Durch Nachrechnen!

6.23. Lemma

Es sei $C = V(F) \subset \mathbb{P}_2(K)$ eine algebraische Kurve mit Minimalpolynom F. Für $P \in C$ gilt:

(1) C glatt in $P \iff \operatorname{grad}_P F = \left(\frac{\partial F}{\partial x_0}(P), \frac{\partial F}{\partial x_1}(P), \frac{\partial F}{\partial x_2}(P)\right) \neq (0,0,0)$.

(2) Ist C glatt in P, so lautet die Gleichung für die projektive Tangente
$T_P(C) : x_0 \frac{\partial F}{\partial x_0}(P) + x_1 \frac{\partial F}{\partial x_1}(p) + x_2 \frac{\partial F}{\partial x_2}(P) = 0$.

Beweis

(1) Es sei $P = (p_0 : p_1 : p_2)$ mit oBdA $p_0 \neq 0$. Ein affiner Teil von C mit $P \in C$ wird dann durch $f(x_1, x_2) = F(1, x_1, x_2)$ beschrieben. Hierfür gilt:
$\frac{\partial f}{\partial x_i}(x_1, x_2) = \frac{\partial F}{\partial x_i}(1, x_1, x_2)$ für $i = 1, 2$.
Ist daher $\operatorname{grad}_P(f) \neq 0$, so ist es auch $\operatorname{grad}_P(F)$. Ist andererseits $\operatorname{grad}_p(f) = 0$, so ergibt sich aus der Formel von Euler:

$$0 = nF(P) = p_0 \frac{\partial F}{\partial x_0}(P),$$

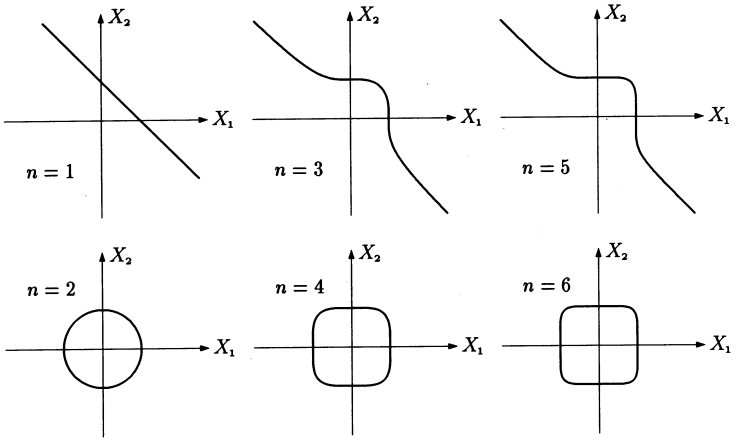
also auch $\operatorname{Grad}_P(F) = 0$.

(2) Die angegebene Gleichung besitzt die korrekte Steigung, gemäß Euler enthält sie den Punkt P. □

6.24. Korollar

Eine algebraische Kurve $C \subset \mathbb{P}_2(K)$ besitzt nur endlich viele Singularitäten.

Beispiel Die sogenannte Fermat-Kurve $V(x_0^n - x_1^n - x_2^n) \subset \mathbb{P}_2(K)$ ist für $n \geq 1$ irreduzibel (nach Eisenstein) und glatt. ($\chi(K)$ darf allerdings n nicht teilen!)



Anzahlaussagen über Singularitäten

Es sei $V_{k,n} \subseteq K[x_0, \ldots, x_k]$ der Vektoraum der homogenen Polynome vom Grad n in $k+1$ Variablen. Hierfür gilt: $\dim V_{k,n} = \binom{n+k}{n}$.

Beweis $k = 0$: Es gibt - bis auf skalare Vielfache - ein Polynom vom Grad n in der Variablen x_0.
$k \longrightarrow k+1$: Die Monome vom Grad n sind von der Gestalt (Monom in $x_0, \ldots, x_{k-1}$ vom Grad i) $* x_k^{n-i}$, die Gesamtzahl ist folglich $\sum_{i=0}^{n} \binom{i+k-1}{i} \overset{!}{=} \binom{n+k}{n}$. Letztere Gleichung zeigen wir nunmehr mittels Induktion nach n. Für $n = 0$ ist offenbar $\binom{k-1}{0} = \binom{k}{0}$. Induktionsschritt $n \longrightarrow n+1$:
Es ist

$$\begin{aligned}
\sum_{i=0}^{n+1} \binom{i+k-1}{i} &= \binom{n+k}{n} + \binom{n+k}{n+1} \qquad \text{(nach Ind. vor.)} \\
&= \tfrac{1}{n!} \left(\prod_{j=k+1}^{n+k} j + \tfrac{1}{n+1} \prod_{j=k}^{n+k+1} j \right) \\
&= \tfrac{1}{(n+1)!} \left(\prod_{j=k+1}^{n+k} j \right) (n+1+k) \\
&= \binom{n+1+k}{n+1}. \qquad \square
\end{aligned}$$

Zwei Polynome aus $V_{k,n}$ heißen äquivalent, falls sie sich nur um einen Faktor aus $K^\times$ unterscheiden. Die Menge dieser Äquivalenzklassen bildet dann einen projektiven Raum $\mathbb{P}_N(K)$ mit $N = \binom{n+k}{n} - 1$.
Wir betrachten nunmehr $F = \sum_{\nu_0+\nu_1+\nu_2=n} a_{\underline{\nu}} \underline{x}^{\underline{\nu}} \in K[x_0, x_1, x_2]$ sowie $P = (p_0 : p_1 : p_2) \in \mathbb{P}_2(K)$. $P \in V(F)$ liefert dann eine lineare Bedingung für die $N+1$ Koeffizienten $a_{\nu_0\nu_1\nu_2}$ von F. $P \in V(F)$ legt demnach eine Hyperebene in $\mathbb{P}_N(K)$ fest, und der Durchschnitt von N Hyperebenenen enthält mindestens einen Punkt in $\mathbb{P}_n(K)$.

Sprechweise: Punkte $P_1, \ldots, P_N \in \mathbb{P}_2(K)$ befinden sich bezüglich Kurven vom Grad n in allgemeiner Lage, wenn sich die zugehörigen Hyperebenen in $\mathbb{P}_N(K)$ in genau einem Punkt schneiden.

Da $\binom{n+2}{n} - 1 = \frac{(n+2)(n+1)}{1 \cdot 2} - 1 = \frac{1}{2}(n^2+3n) = \frac{1}{2}n(n+3)$ gilt, haben wir bewiesen:

6.25. Lemma

Durch $\frac{1}{2}n(n+3)$ Punkte in $\mathbb{P}_2(K)$ geht mindestens eine Kurve vom Grad $\leq n$.

6.26. Satz

Eine irreduzible algebraische Kurve $C \subset \mathbb{P}_2(K)$ vom Grad n hat höchstens
$\gamma(n) := \frac{1}{2}(n-1)(n-2)$ Singularitäten.

Beispiel $\gamma(1) = \gamma(2) = 0$, $\gamma(3) = 1$ (Spitze, Doppelpunkt), $\gamma(4) = 3$.

Beweis OBdA sei $n \geq 3$. Wir nehmen an, dass $\gamma(n) + 1$ Singularitäten auf C existieren. Wir nehmen zu diesen noch $n-3$ weitere Punkte auf C hinzu, haben dann $\frac{1}{2}(n-1)(n-2) + 1 + n - 3 = \frac{1}{2}(n-2)(n+1)$ Punkte. Gemäß dem Lemma (6.21) gibt es eine Kurve C' vom Grad $m \leq n-2$, die durch alle diese Punkte geht. Für jeden singulären Punkt P von C gilt $\mathrm{mult}_P(C \cap C') \geq 2$ (Satz 6.18), für jeden der weiteren $n-3$ Punkte $\mathrm{mult}_P(C \cap C') \geq 1$, insgesamt also

$$\sum_{P \in C \cap C'} \mathrm{mult}_P(C \cap C') \geq 2(\gamma(n)+1) + (n-3) = n^2 - 2n + 1.$$

C ist nach Voraussetzung irreduzibel, kann also wegen $\deg C' < n$ keine Komponente von C' sein. Damit liefert der Satz von Bezout:

$$\sum_{P \in C \cap C'} \mathrm{mult}_P(C \cap C') = n \cdot m \leq n(n-2) = n^2 - 2n.$$

Widerspruch! □

6.27. Korollar

Eine beliebige algebraische Kurve vom Grad n in $\mathbb{P}_2(K)$ hat höchstens $\frac{1}{2}n(n-1)$ Singularitäten.

Beweis Der Beweis erfolgt per Induktion über die Anzahl der Komponenten. Für $n = 1$ ist C irreduzibel. Die Behauptung sei für Kurven vom Grad $< n$ bereits bewiesen. Hat dann eine Kurve C vom Grad n Komponenten vom Grad $m < n$ und $n - m$, so folgt: $\sharp \mathrm{Sing} C \leq \frac{1}{2}m(m-1) + \frac{1}{2}(n-m)(n-m-1) = \frac{1}{2}n(n-1) + m(m-n) < \frac{1}{2}n(n-1)$. □

6.28. Definition

Eine glatte irreduzible Kurve $C \subset \mathbb{P}_2(K)$ vom Grad n hat das Geschlecht
$g = \frac{1}{2}(n-1)(n-2)$.

Elliptische Kurven

Diese Kurven besitzen eine Gleichung in allgemeiner Weierstraß Form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

wobei die Koeffizienten a_i einem vorgegebenen Körper K angehören. Ist die Charakteristik von K von zwei und drei verschieden, so sieht man leicht, dass sich jene Gleichung in die einfachere Form

$$y^2 = x^3 + ax + b$$

überführen lässt. Die zugehörige homogene Gleichung ist dann

$$y^2z - x^3 - axz^2 - bz^3 = 0 \ .$$

Wir zeigen, dass eine elliptische Kurve in dieser Form glatt in $\infty = (0 : 1 : 0)$ ist. Dazu bilden wir die partiellen Ableitungen und berechnen die Werte in ∞:

$$\begin{array}{lll} \frac{\partial}{\partial x} & : & -3x^3 + az^2 \qquad\quad 0 \\ \\ \frac{\partial}{\partial y} & : & 2yz \qquad\qquad\quad 0 \\ \\ \frac{\partial}{\partial z} & : & y^2 - 2axz - 3bz^2 \quad 1 \end{array}$$

Singularitäten in endlichen Punkten $P = (x_0, y_0)$ liegen vor, falls beide partiellen Ableitungen von $f(x, y) := y^2 - x^3 - ax - b$ verschwinden. Wegen

$$\frac{\partial f}{\partial y} = 2y \quad \frac{\partial f}{\partial x} = 3x^2 + a$$

erhalten wir die Bedingungen $0 = 2y_0 = 3x_0^2 + a$ und weiter – wegen $f(x_0, y_0) = 0$ – dann noch $0 = x_0^3 + ax_0 + b$. Also muss x_0 doppelte Nullstelle von $f(x, 0)$ sein, was gleichbedeutend damit ist, dass die Diskriminante $D := 4(-a)^3 - 27b^2$ von $f(x, 0)$ verschwindet. Die Kurve $f(x, y) = 0$ ist also genau dann nicht singulär, wenn die Diskriminante D nicht verschwindet.

Wir gehen jetzt wieder von der allgemeinen Weierstrass Form aus. Eine Gerade durch zwei verschiedene Punkte $P_1 = (x_1, y_1) \neq P_2 = (x_2, y_2)$ der Kurve beziehungsweise die Tangente an die Kurve im Punkte P_1 schneidet die Kurve eine weiteres Mal, etwa im Punkt $P_3 = (x_3, y_3)$, was zur Erklärung der Punktaddition auf einer elliptischen Kurve führt. Bezeichnen wir die Gerade G mit $y = mx + b$, so erhalten wir für deren Steigung m:

$$m \ = \ \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{G durch } P_1 \neq P_2 \\ \\ \frac{3x_1^2 + a_4 + 2a_2x_1 - a_1y_1}{2y_1 + a_1x_1 + a_3} & G \text{ Tangente in } P_1x_1 \end{cases} .$$

Wegen $P_1 \in G$ lässt sich damit b leicht berechnen:

$$b \ = \ \begin{cases} (y_1x_2 - y_2x_1) & / \quad (x_2 - x_1) \\ (-x_1^3 + a_4x_1 + 2a_6 - a_3y_1) & / \quad (2y_1 + a_1x_1 + a_3). \end{cases}$$

Ersetzen wir nun in der allgemeinen Weierstrass Gleichung y durch $mx + b$, so erhalten wir eine kubische Gleichung in x, die $x1, x2, x3$ als

Wurzeln besitzt. Folglich gilt in dieser Gleichung für den Koeffizienten von x^2, dass er gleich $-(x_1 + x_2 + x_3)$ ist (elementarsymmetrische Funktionen!). Wir bekommen so die x-Koordinate von P_3 als

$$x_3 = m^2 - x_1 - x_2 + a_1 m - a_2 \ .$$

Die Punktaddition auf der elliptischen Kurve wird nun folgendermaßen erklärt. Als neutrales Element O wählt man den unendlich fernen Punkt. Dann besitzt der Punkt $-P$ dieselbe x-Koordinate wie $P = (x, y)$ und gemäß der allgemeinen Weierstrassgleichung die y-Koordinate $-y - a_1 x - a_3$. Entsprechend wird die y-Koordinate y_3 von $P_1 + P_2$ beziehungsweise von $2P_1$ festgesetzt zu:

$$y_3 = -mx_3 - b - a_1 x_3 - a_3 \ .$$

Offenbar gilt das Kommutativgesetz: $P_1 + P_2 = P_2 + P_1$. Dagegen erweist sich der Nachweis des Assoziativgesetzes als aufwendig. Ein rein algebraische Nachrechnen ist aber mit Hilfe eines Computer Algebra Systems problemlos möglich.

Bespiel Wir betrachten die elliptische Kurve $y^2 + y = x^3 - x$ mit Parametern $a_1 = a_2 = a_6 = 0,\ a_3 = 1 = -a_4$. Sie hat offensichtlich den Punkt $P = (0, 0)$. Mit den obigen Formeln rechnetman leicht nach:

$$2P = (1, 0),\ 3P = (-1, -1),\ 4P = (2, -3),\ 5P = \left(\frac{1}{4}, -\frac{5}{8}\right),\ 6P = (6, 14),\ 7P = \left(-\frac{5}{9}, \frac{8}{27}\right),\ 8I$$

Bemerkung Die x-Koordinate von $2P = (x_2, y_2)$ aus der von $P = (x, y)$ leichter mit folgenden Formeln berechnen. Deren Herleitung wird als Übungsaufgabe empfohlen. Setzt man

$$b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1 a_3,\ b_6 = a_3^2 + 4a_6,\ b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \ ,$$

so gilt

$$x(2P) = (x^4 - b_4 x^2 - 2b_6 x - b_8)/(4x^3 + b_2 x^2 + 2b_4 x + b_6) \ .$$

6.29. Elliptische Kurven über endlichen Körpern

Es sei p eine Primzahl $\neq 2, 3$ sowie $y^2 = x^3 + ax + b$ mit $4a^3 + 27b^2 \not\equiv 0 \bmod p$. Es bezeichne $\sharp E_p$ die Anzahl der $(x, y) \in \{\infty\} \cup (\mathbb{Z}/_p\mathbb{Z})^2$, die auf der modulo p reduzierten Kurve liegen.

Offenbar gilt: $\sharp E_p \leq 2p + 1$.

6.30. Satz (Hasse)

$| p + 1 - \sharp E_p | < 2\sqrt{p}$.

Zum Beweis betrachtet man die Kurve

$$y^2 = \frac{X^3 + aX + b}{x^3 + ax + b} \text{ über } (\mathbb{Z}/_p\mathbb{Z})(x) \ . \tag{3}$$

Auf ihr liegen offenbar die Punkte $(X,Y) = (x,1)$ sowie $(X,Y) = (x^p, -(x^3+ax+b)^{(p-1)/2})$. Wir spezifizieren ∞ als Null. Dann bilden die projektiven Lösungen von (3) eine Gruppe. Wir setzen

$$Z_n \;=\; (x^p, -(x^3+ax+b)^{(p-1)/2}) + n(x,1) \quad (n \in \mathbb{Z}) \;. \tag{4}$$

In Abhängigkeit von Z_n bezeichnet d_n das Maximum der Grade von Zähler und Nenner der x-Koordinate X_n von Z_n; außerdem setzen wir $d_n = 0$ für $Z_n = \infty$.

Bemerkung Es gilt stets $d_n + d_{n+1} > 0$.

6.31. Lemma

Es gilt $d_{-1} - d_0 - 1 = \sharp E_p - p - 1$.

Beweis Aus (4) erhalten wir unmittelbar $d_0 = p$. Wir setzen $N_p = \sharp E_p - 1$ und müssen dann

$$d_{-1} = N_p + 1 \tag{5}$$

zeigen.
Wir erhalten

$$\begin{aligned} X_{-1} &= -x - x^p + \tfrac{(1+(x^3+ax+b)^{(p-1)/2})^2(x^3+ax+b)}{(x-x^p)^2} \\ &= \tfrac{-x^{3p}+x^{2p+1}+x^{p+2}-x^3+(x^3+ax+b)^p+2(x^3+ax+b)^{(p+1)/2}+(x^3+ax+b)}{(x-x^p)^2} \\ &= \tfrac{x^{2p+1}+R(x)}{(x-x^p)^2} \;. \end{aligned}$$

Dabei ist $R(x)$ ein Polynom vom Grad kleiner als $2p+1$, und bei der letzten Gleichung wurde benutzt, dass die Charakteristik des Konstantenkörpers p ist. Der Grad des Zählers ist also um 1 größer als der des Nenners. Nach Kürzen ist letzterer also $d_{-1} - 1$. Für den Nenner gilt – wiederum aufgrund der Charakteristik:

$$(x^p - x)^2 \;=\; \prod_{j=1}^{p} (x-j)^2 \;.$$

Bezüglich der Nullstellen des Zählers bemerken wir:

$$0 = 1+(j^3+aj+b)^{(p-1)/2} \iff -1 = \left(\frac{j^3+aj+b}{p}\right) = (j^3+aj+b)^{(p-1)/2} \;.$$

Diese Nullstellen des Zählers sind jeweils doppelte Nullstellen. Die restlichen Nullstellen sind einfach:

$$0 = j^3 + aj + b \iff (x-j) \mid (x^3+ax+b) \;.$$

Es verbleiben also im Nenner als Faktoren:

$$(x-j)^2 \quad \text{für} \quad \left(\tfrac{j^3+aj+b}{p}\right) = 1 \text{ sowie}$$

$$(x-j) \quad \text{für} \quad \left(\tfrac{j^3+aj+b}{p}\right) = 0\ .$$

Diese entsprechen aber genau den affinen Lösungen E_p, die ersteren mit 2 y-Werten, letztere mit $y=0$. Also haben wir $d_{-1}-1=N_p$ und damit (5) gezeigt. □

6.32. Lemma

Für $n \in \mathbb{Z}$ gilt: $d_{n-1}+d_{n+1}=2d_n+2$.

Bevor wir Lemma 6.30 beweisen, zeigen wir, wie dann der Beweis des Satzes von Hasse erfolgt.

(1) Per Induktion folgt zunächst $d_n = n^2-(d_{-1}-d_0-1)n+d_0$.

Als Induktionsanfang haben wir die Werte: $d_0=d_0$ und $d_{-1}=1+d_{-1}-d_0-1+d_0=d_{-1}$.

Der Induktionsschritt $n \longrightarrow n\pm 1$ verläuft wie folgt. Nach Lemma 6.30 gilt:

$$\begin{aligned} d_{n\pm1} &= 2d_n+2-d_{n\mp1} \\ &= 2(n^2-(d_{-1}-d_0-1)n+d_0)+2-((n\mp1)^2-(n\mp1)(d_{-1}-d_0-1)+d_0) \\ &= 2n^2-2n(d_{-1}-d_0-1)+2d_0+2-(n\mp1)^2+(n\mp1)(d_{-1}-d_0-1)-d_0 \\ &= n^2\pm 2n+1 \quad -(n\pm1)(d_{-1}-d_0-1)+d_0\ . \end{aligned}$$

(2) Für $a_p := p+1-\sharp E_p$ besagt Lemma 6.29 ($d_{-1}-d_0-1=-a_p$). Damit folgt aus (i): $d_n=n^2+a_pn+p$. Hierbei gilt $d_n \geq 0$, ja sogar $d_n+d_{n+1}>0$.

(3) Wegen $a_p \in \mathbb{Z}$ folgt $z^2+a_pz+p \geq 0$ für alle $z \in \mathbb{R}$. Also muss $a_p^2-4p \leq 0$ gelten, woraus der Satz von Hasse unmittelbar folgt.
(Falls $f(z)=z^2+a_pz+p$ zwei reelle Nullstellen hat, besitzen sie einen Abstand <1, also gilt $\sqrt{a_p^2-4p}<1$, was nur für $a_p^2=4p$ möglich ist.)

Beweis von Lemma 6.30

Wir nehmen zunächst an, dass (genau!) einer der drei Punkte Z_{n-1}, Z_n, Z_{n+1} gleich ∞ ist.

Für $Z_n = \infty$ ist $d_n = 0$, $Z_{n+1} = (x, 1)$, $Z_{n-1} = -(x, 1) = (x, 1)$. Es ist also $d_{n+1} = d_{n-1} = 1$, Lemma 6.30 daher erfüllt.
Für $Z_{n-1} = \infty$ ist $d_{n-1} = 0$, $Z_n = (x, 1)$. Wir erhalten dann mit der Formel für $X(2P)$:

$$Z_{n+1} = \left(\frac{(x^2 - a)^2 - 8bx}{4(x^3 + ax + b)}, Y_{n+1} \right) .$$

Hiernach ist $d_n = 1$, $d_{n+1} = 4$ und Lemma 6.30 ebenfalls erfüllt.
Für $Z_{n+1} = \infty$ gilt $Z_n = -(x, 1)$, $Z_{n-1} = -2(x, 1)$, und die Behauptung folgt analog.

Im folgenden können wir also annehmen, dass Z_{n-1}, Z_n, Z_{n+1} alle von ∞ verschieden sind. Wir schreiben dann die entsprechenden X-Koordinaten in gekürzter Form als

$$X_{n-1} = \frac{A}{B}, X_n = \frac{P}{Q}, X_{n+1} = \frac{C}{D} .$$

Mittels der Additionsformeln erhalten wir dann:

$$X_{n-1} = \frac{-(Qx + P)(Qx - P)^2 + (1 + Y_n)^2(x^3 + ax + b)Q^3}{Q(Qx - P)^2} ,$$

$$X_{n+1} = \frac{-(Qx + P)(Qx - P)^2 + (1 - y_n)^2(x^3 + ax + b)Q^3}{Q(Qx - P)^2} . \tag{6}$$

Addition dieser 2 Gleichungen ergibt unter Ausnutzung von (**??**):
$\frac{1}{2}(x_{n-1} + x_{n+1})$

$$\begin{aligned} \frac{1}{2}(X_{n-1} + X_{n+1}) &= \frac{-(Qx + P)(Qx - P)^2 + (x^3 + ax + b)Q^3 + ((P/Q)^3 + a(P/Q) + b)\, Q^3}{Q(Qx - P)^2} \\ &= \frac{PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ}{(Qx - P)^2} . \end{aligned} \tag{7}$$

Ebenso erhält man durch Multiplikation nebst einiger Umformungen:

$$X_{n-1}X_{n+1} = \frac{(Px - aQ)^2 - 4bQ(Qx + P)}{(Qx - P)^2} \stackrel{!}{=} \frac{AC}{BD} . \tag{8}$$

Wir behaupten $BD = (Qx - P)^2$ (bis auf einen Faktor aus $(\mathbb{Z}/p\mathbb{Z})^\times$).
Es bezeichne S den größten gemeinsamen Teiler von AC und BD.

Dann ergibt (8):

$$AC \;=\; S\left((Px - aQ)^2 - 4bQ(Qx + P)\right)\,,\; BD \;=\; S(Qx - P)^2\,.$$

Andererseits liefert der Zähler von (7):

$$AD + BC \;=\; 2S(PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ)\,.$$

Es sei nun F ein Primteiler von S.
Es folgt $F \mid (BD)$, und ohne Beschränkung der Allgemeinheit können wir $F \mid B$ annehmen. Wegen $\gcd(A, B) = 1$ folgt $F \not| A$. Wegen $F \mid (AC)$ muss daher $F \mid C$ gelten. Hiernach folgt $F \mid (AD)$, also $F \mid D$. Dies steht im Widerspruch zu $\gcd(C, D) = 1$, folglich muss S konstant sein.

Wir rufen in Erinnerung:

$$d_{n-1} \;=\; \max\{\deg A, \deg B\},\; d_{n+1} \;=\; \max\{\deg C, \deg D\},\; d_n \;=\; \max\{\deg P, \deg Q\}\,.$$

Der Beweis der Formel aus Lemma 6.30 wird jetzt in 4 Fälle unterteilt:

(1) $d_{n-1} = \deg A \wedge d_{n+1} = \deg C$;

(2) $d_{n-1} = \deg B \wedge d_{n+1} = \deg D$;

(3) $d_{n-1} = \deg A \wedge d_{n+1} = \deg D$, aber nicht $(i) \vee (ii)$;

(4) $d_{n-1} = \deg B \wedge d_{n+1} = \deg C$, aber nicht $(i) \vee (ii)$.

Ad(i):
Nach (8) (nebst Folgerungen) gilt

$$d_{n-1} + d_{n+1} \;=\; \deg(AC) \;=\; \deg((Px - aQ)^2 - 4bQ(Qx + P)) \;=:\; \lambda\,.$$

Im Fall $\deg P \geq \deg Q$ gilt $\lambda = \deg(P^2x^2) = 2d_n + 2$. Im Fall $\deg P < \deg Q$ erhalten wir aus (8): $\deg(BD) = 2\deg Q + 2$. Es folgt dann $\deg(AC) \leq \max\{2\deg P + 2, 2\deg Q + 1\} = 2\deg Q + 1 < \deg(BD)$, im Widerspruch zu unserer Annahme im Fall (i). Also ist Lemma 6.30 im Fall (i) bewiesen.

Ad(ii):
Analog zu (i) erhalten wir jetzt

$$d_{n-1} + d_{n+1} \;=\; \deg(BD) = \deg((Qx - P)^2) \;=:\; \lambda\,.$$

Für $\deg Q \geq \deg P$ folgt $\lambda = 2d_n + 2$, also die Aussage von Lemma 6.30. Wäre hingegen $\deg Q < \deg P$, so würde (vgl. (i)) gelten: $\deg(AC) = \deg(P^2x^2) > \deg(P^2) \geq \deg(BD)$; dies steht im Widerspruch zur Annahme im Fall (ii).

Ad(iii):
Nach Annahme gilt $\deg A > \deg B$ und $\deg D > \deg C$. Wir erhalten folglich:

$$(9) \qquad \deg(AD) \;>\; \max\{\deg(AC), \deg(BD), \deg(BC)\}\ ,$$

und somit

$$\deg(AD) \;=\; \deg(AD+BC) = \deg(PQx^2+P^2x+axQ^2+2bQ^2+aPQ) \;=:\; \lambda\ .$$

Für $\deg P \geq \deg Q$ wird $\lambda \leq \deg(P^2x^2) = \deg(AC)$, im Widerspruch zu (9). Für $\deg P < \deg Q$ wird $\lambda \leq \deg(Q^2x^2) = \deg(BD)$, ebenfalls ein Widerspruch zu (9). Fall (iii) ist also gar nicht möglich.

Ad(iv):
Dieser Fall ist symmetrisch zu (iii), er ist ebenfalls unmöglich.

Dies beendet den Beweis von Lemma 6.30 und damit auch den Beweis des Satzes von Hasse.

Moderne Beweise des Satzes von Hasse (und seiner Verallgemeinerung von Weil auf beliebige endliche Körper) erfordern wesentlich mehr technische Vorbereitungen, so dass wir sie im Rahmen dieser Vorlesung nur knapp skizzieren können.

6.33. Definition

Es sei A eine abelsche Gruppe. Eine Funktion $d : A \longrightarrow \mathbb{R}$ heißt quadratische Form, falls gilt:

(1) $d(\alpha) = d(-\alpha) \quad \forall \alpha \in A$,

(2) $L(\alpha, \beta) := d(\alpha+\beta) - d(\alpha) - d(\beta)$ ist (symmetrische) Bilinearform.

d heißt positiv definit, falls $d(A) \subseteq \mathbb{R}^{\geq 0}$ und $(d(\alpha) = 0 \iff \alpha = 0)$ erfüllt sind.

6.34. Lemma

Für eine positiv definite quadratische Form $d : A \longrightarrow \mathbb{Z}$ gilt: $| d(\alpha-\beta) - d(\alpha) - d(\beta) | \leq 2(d(\alpha)d(\beta))^{1/2}$.

Beweis $\tilde{L}(\alpha, \beta) := d(\alpha-\beta) - d(\alpha) - d(\beta)$ ist nach Voraussetzung (symmetrische) Bilinearform! Für $m, n \in \mathbb{Z}$ erhalten wir:

(1)

$$\begin{array}{lcl} 0 \leq d(m\alpha - n\beta) & = & \tilde{L}(m\alpha, m\beta) + d(m\alpha) + d(n\beta)\ . \\ (\text{Wegen } -L(\alpha,\alpha) & = & L(\alpha,-\alpha) = d(0) - d(\alpha) - d(\alpha) \\ \text{folgt } L(\alpha,\alpha) & = & 2d(\alpha) \text{ und damit für } n \in \mathbb{N} \\ d((n+1)\alpha) & = & L(n\alpha,\alpha) + d(n\alpha) + d(\alpha) \\ & = & nL(\alpha,\alpha) + n^2 d(\alpha) + d(\alpha) = (n+1)^2 d(\alpha)\ . \end{array}$$

Bei der vorletzten Gleichung geht dabei die Induktionsvoraussetzung ein. Wir erhalten insgesamt $d(k\alpha) = k^2 d(\alpha)$ wegen Definition 6.31 (i). Damit wird aus Lemma 6.32 (i):

(2) $0 \leq m^2 d(\alpha) + n^2 d(\beta) + mn\tilde{L}(\alpha,\beta)$. Wir setzen speziell $m = -\tilde{L}(\alpha,\beta), n = 2d(\alpha)$ und erhalten

(3)

$$\begin{array}{rcl} 0 & \leq & \tilde{L}(\alpha,\beta)^2 d(\alpha) + 4d(\alpha)^2 d(\beta) - 2d(\alpha)\tilde{L}(\alpha,\beta)^2 \\ & = & d(\alpha)(4d(\alpha)d(\beta) - \tilde{L}(\alpha,\beta)^2)\ . \end{array}$$

Dies liefert die Behauptung für $\alpha \neq 0$, für $\alpha = 0$ ist sie ohnehin trivial. □

6.35. Satz

Es sei $K = \mathbb{F}_q (q = p^n)$ und E eine elliptische Kurve mit Koeffizienten in K. Dann gilt für die Anzahl ihrer Punkte $\sharp E_k$: $\quad \mid \sharp E_K - q - 1 \mid \leq 2\sqrt{q}$.

Beweisskizze Ein Punkt $P = (x,y) \in \overline{K}^2$ liegt in K dann und nur dann, wenn er vom Frobenius-Isomorphismus $\phi : (x,y) \mapsto (x^q, y^q)$ auf sich abgebildet wird. Demnach gilt $E_K = \ker(id - \phi)$, also $\sharp E_K = \sharp \ker(id - \phi) = \deg(id - \phi)$. Die Gradabbildung ist dabei eine positiv definite quadratische Form mit $\deg \phi = q$. Die Behauptung folgt dann direkt aus dem vorangehenden Lemma.

Es sei wiederum $K = \mathbb{F}_q$ sowie K_n eine Erweiterung von K vom Grad n.

Es sei V/K eine projektive Varietät, das heißt Nullstellenmenge von einer vorangegebenen endlichen Menge von Polynomen $f_1(x_0, \ldots, x_N), \ldots, f_m(x_0, \ldots, x_N) \in K[x_0, \ldots, x_N]$. Mit $V(K_n)$ bezeichnen wir entsprechend die Nullstellenmenge mit Koordinaten aus K_n.

6.36. Definition

Die Potenzreihe

$$Z(V/K;T) := \exp\left(\sum_{n=1}^{\infty} (\sharp V(K_n)) \frac{T^n}{n}\right)$$

heißt Zetafunktion von V/K.

(Ist $F(T)$ eine Potenzreihe mit $F(0) = 0$, so ist $\exp(F(T)) := \sum_{i=0}^{\infty} F(T)^i/i!$.)

Bemerkung Ist die Zetafunktion einer Varietät bekannt, so lassen sich die Anzahlen $\sharp V(K_n)$ einfach berechnen mittels

$$\sharp V(K_n) = \frac{1}{(n-1)!}\left[\frac{d^n}{dT^n}\log Z(V/K;T)\right]_{T=0}.$$

Beispiel Es sei $V = \mathbb{P}^N$. Ein Punkt $V(K_n)$ wird durch homogene Koordinaten $(x_0 : x_1 : \ldots : x_N) \in \mathbb{P}_N(K_n)$ gegeben. Koordinatentupel bestimmen genau dann denselben Punkt, wenn sie sich um einen Faktor aus $K_n^\times$ unterscheiden. Also gilt:

$$\sharp V(K_n) = \frac{q^{n(N+1)}-1}{q^n-1} = \sum_{i=0}^{N} q^{ni}$$

und damit

$$\log Z(V/K;T) = \sum_{n=1}^{\infty}\left(\sum_{i=0}^{N} q^{ni}\right)\frac{T^n}{n} = \sum_{i=0}^{N} -\log(1-q^iT)$$

Es folgt unmittelbar:

$$Z(\mathbb{P}^N/K;T) = \frac{1}{(1-T)(1-qT)\cdots(-q^NT)}.$$

Die Zetafunktion liegt also in $\mathbb{Q}(T)$.

6.37. Weil - Vermutungen

Es sei $K = \mathbb{F}_q$ und V/K eine glatte projektive Varietät der Dimension n. Dann gelten:

(1) $Z(V/K;T) \in \mathbb{Q}(T)$;

(2) Es existiert $\varepsilon \in \mathbb{Z}$ (Euler-Charakteristik) mit $Z(V/K;q^{-n}T^{-1}) = \pm q^{n\varepsilon/2}T^{\varepsilon}Z(V/K_1T)$;

(3) Es besteht eine Faktorisierung $Z(V/K;T) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)P_2(T)\cdots P_{2n}(T)}$ mit $P_i(T) \in \mathbb{Z}[T]$, ferner gilt $P_0 = 1-T$, $P_{2n}(T) = 1-q^nT$ sowie $P_i(T) = \prod_j(1-\alpha_{ij}T)$ in $\mathbb{C}[T]$ mit $\mid \alpha_{ij} \mid = q^{i/2}$ $(1 \le i \le 2n-1)$.

($I(V)$ Primideal, $K[V] = \frac{K[x]}{I(V)}$, $K(V) = \mathcal{Q}(K[V])$, $\dim V$ = Transzendenzgrad von $\overline{K}(V)$ über $\overline{K}$.)

6.38. Satz

Es sei $K = \mathbb{F}_q$ und E/K eine elliptische Kurve. Dann existiert $a \in \mathbb{Z}$ mit $Z(E/K;T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}$. Ferner gilt $Z(E/K;q^{-1}T^{-1}) = Z(E/K;T)$ sowie $1-aT+qT^2 = (1-\alpha T)(1-\beta T)$ mit $\mid \alpha \mid = \mid \beta \mid = q^{1/2}$.

Beweisidee Ausgehend von $\sharp E_{K_n} = \deg(id - \phi^n) \stackrel{!}{=} 1 - \alpha^n - \beta^n + q^n$ mit $\alpha, \beta \in \mathbb{C}$, $\mid \alpha \mid = \mid \beta \mid = \sqrt{q}$, erhalten wir:

$$\begin{aligned} \log Z(E/K;T) &= \sum_{n=1}^{\infty} (\sharp E_{K_n}) \frac{T^n}{n} \\ &= \sum_{n=1}^{\infty} (1 - \alpha^n - \beta^n + q^n) T^n/n \\ &= -\log(1-T) + \log(1-\alpha T) + \log(1-\beta T) - \log(1-qT) \ , \end{aligned}$$

woraus man die Behauptung für $Z(E/K;T)$ sofort abliest. Die Funktionalgleichung ergibt sich leicht durch Nachrechnen.

6.39. Zusammenhang zur Riemannschen Vermutung

Dazu setzen wir $T = q^{-s}$ und bekommen

$$\zeta_{E_K}(s) := Z(E/K;q^{-s}) = \frac{1 - aq^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})} \ .$$

Dann wird die Funktionalgleichung zu $\zeta_{E_K}(1-s) = \zeta_{E_K}(s)$. ($T \mapsto 1/(qT)$ entspricht $s \mapsto 1-s$.) Die Nullstellen der Zetafunktion sind α, β vom Betrag $\mid q^s \mid = \sqrt{q}$, was $\mathrm{Re}s = 1/2$ entspricht.

Bibliography

[1] Bewersdorff, Jörg, *Algebra für Einsteiger*,Vieweg, 2002.
[2] Birkhoff, Bartee, *Modern Applied Algebra*.
[3] S. Bosch, *Algebra*, Springer, 1993.
[4] N. Bourbaki, *Algebre*, Hermann, Paris 1962.
[5] J. H. Davenport, Y. Siret, E. Tournier, *Computer algebra*, Acad. Press, 1989.
[6] I. N. Herstein, *Topics in Algebra*, Xerox Coll. Pub., 1964.
[7] Th. W. Hungerford, *Algebra*, 1974.
[8] N. Jacobson, *Lectures in Abstract Algebra*, Springer GTM, 1974.
[9] R. Kochendörffer, *Einführung in die Algebra*, Dt.Verl.d. Wissenschaften, 1974.
[10] S. Lang, *Algebra*, Addison-Wesley, 1971.
[11] A. Leutbecher, *Zahlentheorie*, Springer, 1996.
[12] F. Lorenz, *Algebra I, II*, BI Wissenschaftsverlag, 1987/90.
[13] K. Meyberg, *Algebra I, II*, Carl Hanser Verlag, 1975.
[14] Mignotte, *Mathematics for Computer Algebra*, Springer, 1992.
[15] E. Scholz, *Geschichte der Algebra*, BI Wissenschaftsverlag, 1990.
[16] G. Stroth, *Algebra*, de Gruyter, 1998.
[17] B. L. van der Waerden, *Algebra I, II*, Springer, 1966/87.
[18] Weber, *Lehrbuch der Algebra*, Vieweg, 1895.