Elliptische Kurven und Kryptographie

Serie 2

Resultante & Schnittpunkte algebraischer Kurven — Musterlösungen

---

6. Seien $f = a_0 + a_1 z + \ldots + a_m z^m$ und $g = b_0 + b_1 z + \ldots + b_n z^n$ Polynome über dem Ring $R[x, y]$, wobei R ein faktorieller Ring ist.

Zeige: Sind die Koeffizienten a_i $(0 \leq i \leq m)$ und b_j $(0 \leq j \leq n)$ homogene Polynome in x, y vom Grad $m - i$ bzw. $n - j$, dann ist die Resultante $R(f, g) \in R[x, y]$ ein Polynom in x, y und homogen vom Grad mn.

Beweis:

Seien r_{ij} die Einträge der Sylvester-Matrix von f und g, deren Determinante $R(f, g)$ ist. Dann gilt:

$$R(f,g) = \sum_{\sigma \in S_{m+n}} \operatorname{sign} \sigma \prod_{i=1}^{m+n} r_{i\sigma(i)} \,.$$

Also ist für fixes σ entweder $\prod_{i=1}^{m+n} r_{i\sigma(i)} = 0$ oder

$$\forall i = 1, \ldots, m+n \colon \operatorname{degr}(r_{i\sigma(i)}) = \operatorname{degr}(r_{ii}) - (\sigma(i) - i)$$

und somit

$$\operatorname{degr}\left(\prod_{i=1}^{m+n} r_{i\sigma(i)}\right) = \sum_{i=1}^{m+n} \operatorname{degr}(r_{ii}) - \underbrace{\sum_{i=1}^{m+n} (\sigma(i) - i)}_{=0} \,.$$

Nun haben wir in der Vorlesung gesehen, dass (wie gewünscht) $\sum_{i=1}^{m+n} \operatorname{degr}(r_{ii}) = mn$ ist. Enstprechend ist $R(f, g)$ eine Summe von Polynomen, die homogen vom Grad mn sind, also selbst homogen vom Grad mn.

7. (a) Finde alle komplexen Schnittpunkte sowie deren Vielfachheit der beiden Kurven

$$C_1 \colon\ y = 2z \qquad \text{und} \qquad C_2 \colon\ x^2 + y^2 = z^2 \,.$$

(b) Finde alle komplexen Schnittpunkte sowie deren Vielfachheit der beiden Kurven

$$C_1 \colon\ y = x + z \qquad \text{und} \qquad C_3 \colon\ y^2 z = x^3 - 2x^2 z + 5xz^2 \,.$$

Lösung:

(a) Durch Einsetzen erhalten wir

$$C_1 \text{ in } C_2\colon\ x^2 + 4z^2 = z^2 \ \Leftrightarrow\ x^2 = -3z^2 \ \Leftrightarrow\ x_{0,1} = \pm\sqrt{3}iz\,.$$

Wäre $z = 0$, so auch die beiden anderen Koordinaten, was keinen projektiven Punkt liefert. Also sind die Schnittpunkte

$$P_0 = (\sqrt{3}i, 2, 1) \qquad \text{und} \qquad P_1 = (-\sqrt{3}i, 2, 1)\,.$$

(b) Durch Einsetzen erhalten wir

$$C_1 \text{ in } C_3\colon\ x^2z + 2xz^2 + z^3 = x^3 - 2x^2z + 5xz^2\,.$$

Wäre $z = 0$, so auch die beiden anderen Koordinaten, was keinen projektiven Punkt liefert. Also können wir ohne Einschränkung $z = 1$ setzen und erhalten

$$x^2 + 2x + 1 = x^3 - 2x^2 + 5x \ \Leftrightarrow\ 1 - 3x + 3x^2 - x^3 = 0 \ \Leftrightarrow\ (1-x)^3 = 0\,.$$

Somit ist $P = (1, 2, 1)$ ein dreifacher Schnittpunkt.

8. (a) Schneidet eine Gerade eine cubische Kurve in genau 2 verschiedenen reellen Punkten, so ist die Gerade tangential an die Kurve.

(b) Schneidet eine Gerade eine rationale cubische Kurve in 3 verschiedenen reellen Punkten und sind 2 dieser Punkte rational, so ist auch der dritte Punkt rational.

(c) Sind C_m und C_n algebraische Kurven vom Grad m bzw. n und schneiden sich diese Kurven in mindestens $mn + 1$ komplexen Punkten (inklusive Vielfachheit), so haben C_m und C_n eine Kurve vom Grad ≥ 1 gemeinsam.

Beweis:

In (a) und (b) können wir jeweils ohne Einschränkung die Geradengleichung nach z auflösen und das Resultat in die Gleichung der kubischen Kurve einsetzen. Im entstehenden Polynom in x und y können wir ohne Einschränkung durch $y = 1$ homogenisieren. (Wenn nötig, müssen wir Koordinaten vertauschen.) Wir erhalten also ein Polynom p in der Variable x. Dieses zerfällt über $\mathbb{C}$: $p(x) = (x - x_0)(x - x_1)(x - x_2)$.

(a) Zwei verschiedene reelle Schnittpunkte entsprechen zwei verschiedenen reellen Nullstellen, z. B. x_0 und x_1. Da p reelle Koeffizienten besitzt, muss $-(x_0 + x_1 + x_2)$ reell sein, also auch x_2. Weil genau 2 reelle Schnittpunkte existieren, ist ohne Einschränkung $x_2 = x_0$.

Die doppelte Nullstelle x_0 ist nun auch eine Nullstelle von p'. Der Gradient der kubischen Kurve ist also 0 bei x_0, was bedeutet, dass die Gerade tangential an die Kurve ist.

(b) Da die Gerade durch zwei rationale Punkte geht, ist sie auch rational. Entsprechend besitzt p rationale Koeffizienten. Zwei verschiedene rationale Schnittpunkte entsprechen zwei verschiedenen rationalen Nullstellen, z. B. x_0 und x_1. Da p rationale Koeffizienten besitzt, muss insbesondere $-(x_0 + x_1 + x_2)$ rational sein, also auch x_2.

(c) Seien

$$C_m\colon\ f_{xy}(z) = 0 \qquad \text{und} \qquad C'_n\colon\ g_{xy}(z) = 0$$

mit Koeffizienten wie in Aufgabe **6**. Jeder Schnittpunkt (x_0, y_0, z_0) enspricht einer gemeinsamen Nullstelle z_0 von $f_{x_0\,y_0}$ und $g_{x_0\,y_0}$, also gilt für die Resultante

$$R(f_{x_0\,y_0}, g_{x_0\,y_0}) = 0\,.$$

Aber nach Aufgabe **6** ist $R(f_{xy}, g_{xy})$ höchstens vom Grad mn. Somit gilt auch

$$R(f_{xy}, g_{xy}) = 0\,.$$

D. h. bereits f_{xy} und g_{xy} haben einen Faktor vom Grad ≥ 1 gemeinsam.