Elliptische Kurven und Kryptographie

Serie 2

Resultante & Schnittpunkte algebraischer Kurven | Besprechung am 10. Oktober

---

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 $(0 \le i \le m)$ und b_j $(0 \le j \le n)$ homogene Polynome in x, y vom Grad $m - i$ bzw. $n - j$, dann ist die Resultante $R(f, g) \in R[x, y]$ ein homogenes Polynom in x, y vom Grad mn.

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

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

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

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

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.