Elliptische Kurven & Kryptologie Serie 6

Polynome mit mehreren Variablen Abgabe: 14. April

---

1. Gegeben seien folgende Polynome aus $\mathbb{Q}[x, y]$:

$$\begin{aligned} f(x,y) &= x^3 - 2xy - 3x^2y + 6y^2 \\ g_0(x,y) &= 2x - 6y - xy + 3y^2 \\ g_1(x,y) &= 2x - 5y - xy + 3y^2 \end{aligned}$$

(a) Schreibe $f(x,y), g_0(x,y), g_1(x,y)$ als Polynome $\tilde{f}(x), \tilde{g}_0(x), \tilde{g}_1(x)$ aus $\mathbb{Q}[y][x]$, *d.h.* als Polynome in x mit Koeffizienten aus $\mathbb{Q}[y]$.

(b) Zeige: $R(\tilde{f}, \tilde{g}_0) = 0$ und $R(\tilde{f}, \tilde{g}_1) \neq 0$.

(c) Verifiziere: $(-2+y, -2y, 0, 1)\big[R(\tilde{f}, \tilde{g}_0)\big] = (0,0,0,0)$.

(d) Finde nicht-triviale Lösungen $a(x)$ und $b(x)$ in $\mathbb{Q}[y][x]$ mit $\deg(a) < \deg(\tilde{g}_0)$ *bzw.* $\deg(b) < \deg(\tilde{f})$ für die Gleichung:

$$a(x) \cdot \tilde{f}(x) + b(x) \cdot \tilde{g}_0(x) = 0$$

(e) Berechne ggT $\big(f(x,y), g_0(x,y)\big)$.

2. Sei $\mathbb{F}$ ein Körper. Ferner sei R der Polynomring $\mathbb{F}[x_1, \ldots, x_n]$ und $H \subseteq \mathbb{F}[x_1, \ldots, x_n, z]$ die Menge der homogenen Polynome in den Variablen $x_1, \ldots, x_n, z$.

(a) Finde eine Injektion $i : R \to H$, so dass für alle $f, g \in R$ gilt:

- $i(f \cdot g) = i(f) \cdot i(g)$, und
- falls f irreduzibel ist, dann ist auch $i(f)$ irreduzibel.

(b) Bestimme $H \setminus \big\{i(f) \in H : f \in R\big\}$.

3. Gegeben seien folgende homogenen Polynome aus $\mathbb{Q}[X, Y, Z]$:

$$\begin{aligned} F(X,Y,Z) &= X^3 - 2XYZ - 3X^2Y + 6Y^2Z \\ G(X,Y,Z) &= 2XZ - 6YZ - XY + 3Y^2 \end{aligned}$$

(a) Finde Lösungen $A(X,Y,Z)$ und $B(X,Y,Z)$ in $\mathbb{Q}[X,Y,Z]$ mit $\deg(A) = 1$ *bzw.* $\deg(B) = 2$ für die Gleichung:

$$A(X,Y,Z) \cdot F(X,Y,Z) + B(X,Y,Z) \cdot G(X,Y,Z) = 0$$

(b) Berechne ggT $\big(F(X,Y,Z), G(X,Y,Z)\big)$.