Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Dr. Peter Ullrich

WS 2004/05
Übungsblatt 5
18. November 2004

Elliptische Kurven-Kryptosysteme

Besprechung in der Übungsstunde am 24.11.04

Aufgabe 1

Sei E/K eine algebraische Körpererweiterung, und sei $R \subset E$ ein Teilring mit $K \subset R$. Zeigen Sie, dass R ein Teilkörper von E ist.

Aufgabe 2

Zeigen Sie, dass $f(X) = X^2 - 3$ irreduzibel in $\mathbb{Q}(\sqrt{2})[X]$ ist.

Aufgabe 3

Sei R ein Integritätsring, $\mathrm{Quot}(R)$ der in der Vorlesung konstruierte Quotientenkörper von R und $\varphi : R \to \mathrm{Quot}(R)$, $a \mapsto \frac{a}{1}$ der kanonische Ringhomomorphismus. Zeigen Sie:

(a) Der Homomorphismus $\varphi : R \to \mathrm{Quot}(R)$ ist injektiv.

(b) (Universelle Eigenschaft des Quotientenkörpers). Jeder injektive Ringhomomorphismus $\psi : R \to E$ in einen Körper E setzt sich eindeutig zu einen Homomorphismus $\bar{\psi} : \mathrm{Quot}(R) \to E$ fort, d.h. es gibt genau einen (Ring-)Homomorphismus $\bar{\psi} : \mathrm{Quot}(R) \to E$ mit $\psi = \bar{\psi} \circ \varphi$.

(c) Sei $\lambda : R \to F$ ein weiterer injektiver Ringhomomorphismus in einen Körper F, der die universelle Eigenschaft aus (b) hat, d.h. zu jedem injektiven Ringhomomorphismus $\psi : R \to E$ in einen Körper E gebe es genau einen Homomorphismus $\bar{\psi} : F \to E$ mit $\bar{\psi} \circ \lambda = \psi$. Dann gibt es genau einen Isomorphismus $\chi : \mathrm{Quot}(R) \to F$ mit $\chi \circ \varphi = \lambda$. (Bem.: Der Quotientenkörper $\mathrm{Quot}(R)$ ist daher durch die universelle Eigenschaft aus (b) bis auf eindeutige Isomorphie eindeutig bestimmt.)

Aufgabe 4

Sei K ein Körper und C ein algebraischer Abschluß von K. Für $a = (a_1, \ldots, a_n) \in C^n$ setze $m_a = \{f \in K[X_1, \ldots, X_n] : f(a) = 0\}$. Zeigen Sie:

(a) Jedes m_a ($a \in C^n$) ist ein maximales Ideal von $K[X_1, \ldots, X_n]$. (Hinweis: Aufgabe 1).

(b) Ist $a \in K^n$, so wird m_a von den Polynomen $X_1 - a_1, \ldots, X_n - a_n$ erzeugt.

(c) Es sei nun speziell $C = \mathbb{C}$, $K = \mathbb{R}$ und $n = 1$. Für $z = a + ib \in \mathbb{C}$ sei $\bar{z} = a - ib$. Ist $z = a \in \mathbb{R}$, so gilt $m_z = (X - a)$ in $\mathbb{R}[X]$. Ist $z = a + ib \in \mathbb{C} \setminus \mathbb{R}$, so gilt $m_z = m_{\bar{z}} = ((X - a)^2 + b^2)$ in $\mathbb{R}[X]$.