Wolfgang K. Seiler
Tel. 2515

A5, C201

10. November 2015

9. Übungsblatt Algebra

Aufgabe 1: *(4 Punkte)*

Sie verwenden bei DSA versehentlich für die Unterschriften unter zwei verschiedene Nachrichten m_1, m_2 die gleiche Zufallszahl k. Die Unterschriften sind (r_1, s_1) und (r_2, s_2).

a) Woran erkennt jemand, der beide Unterschriften sieht, Ihren Fehler?

b) Wie kann er dann mit Hilfe der beiden Nachrichten und Unterschriften Ihren geheimen Schlüssel x finden?

Aufgabe 2: *(6 Punkte)*

a) Bestimmen Sie über $\mathbb{Q}$ Zerfällungskörper für die beiden Polynome $f = X^3 - 1 \in \mathbb{Q}[X]$ und $g = X^2 + 3 \in \mathbb{Q}[X]$, und zeigen Sie, daß diese isomorph sind!

b) Gibt es einen Ringisomorphismus $\mathbb{Q}[X]/(X^3 - 1) \to \mathbb{Q}[X]/(X^2 + 3)$?

c) Zeigen Sie, daß $\mathbb{Q}[X]/(X^2 + X + 1) \cong \mathbb{Q}[X]/(X^2 + 3)$ ist!

Aufgabe 3: *(6 Punkte)*

a) $K \subset \mathbb{C}$ sei ein Körper, der sowohl i als auch $\sqrt{2}$ enthält. Berechnen Sie das Polynom

$$f = (X - i - \sqrt{2})(X - i + \sqrt{2})(X + i - \sqrt{2})(X + i + \sqrt{2})$$

und überzeugen Sie sich, daß $f \in \mathbb{Q}[X]$!

b) Was ist der Zerfällungskörper von f über $\mathbb{Q}$?

Aufgabe 4: *(4 Punkte)*

K/k sei eine Körpererweiterung mit endlichem Grad $d = [K : k]$. Zeigen Sie, daß jedes Element $x \in K$ Nullstelle eines Polynoms $f \in k[X]$ vom Grad höchstens d ist! *(Hinweis: Betrachten Sie die Menge aller x-Potenzen!*