Wolfgang K. Seiler
Tel. 2515

A5, C201

3. November 2015

8. Übungsblatt Algebra

Aufgabe 1: *(5 Punkte)*

Geben Sie die Einheitengruppen der folgenden Ringe explizit an und entscheiden Sie, welche davon zyklisch sind:

a) $\mathbb{Z}$ *b)* $\{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ *c)* $\mathbb{Z}/30$ *d)* $\mathbb{Z}[X, Y]$ *e)* $\mathbb{R}[X, Y, Z]$

Aufgabe 2: *(5 Punkte)*

a) Zeigen Sie, daß die Abbildung

$$\varphi: \begin{cases} \mathbb{Z}/4 \oplus \mathbb{Z}/2 \to \left(\mathbb{Z}/16\right)^\times \\ (n, m) \mapsto 3^n \cdot 7^m \end{cases}$$

ein Gruppenhomomorphismus ist! *(Hinweis: Betrachten Sie die von 3 und 7 erzeugten Untergruppen von* $\left(\mathbb{Z}/16\right)^\times$*.)*

b) Folgern Sie, daß für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, 16) = 1$ gilt: $a^4 \equiv 1 \bmod 16$.

Aufgabe 3: *(5 Punkte)*

a) Finden Sie jeweils eine primitive Wurzel modulo fünf und eine modulo sieben!

b) Zeigen Sie, daß $\left(\mathbb{Z}/35\right)^\times \cong \mathbb{Z}/4 \oplus \mathbb{Z}/6$ ist!

c) Ist $\left(\mathbb{Z}/35\right)^\times$ zyklisch?

Aufgabe 4: *(5 Punkte)*

Ein Spielzeug-DSA-System verwendet die Primzahlen $p = 1033$ und $q = 43$ und die Basis $a = 5$. Ihr geheimer Schlüssel ist vier.

a) Welcher öffentliche Schlüssel gehört dazu?

b) Wählen Sie die „Zufallszahl“ fünf und unterschreiben Sie die Nachricht 17!

Abgabe bis zum Dienstag, dem 10. November 2015, um 15.30 Uhr