Wolfgang K. Seiler
*Tel.* 2515

A5, C201

*9. Oktober 2008*

# 5. Übungsblatt Computeralgebra

**Aufgabe 1:** (*5 Punkte)*

*a)* Bestimmen Sie die quadratfreie Zerlegung des Polynoms

$$f = x^9 - 2x^8 - 3x^7 + 7x^6 + 2x^5 - 5x^4 - 4x^3 + 8x - 4\,!$$

*b)* Zerlegen Sie $f$ in $\mathbb{Z}[x]$ in irreduzible Faktoren!

*c)* Bestimmen Sie alle reellen Nullstellen von $f$ !

**Aufgabe 2:** (*5 Punkte)*

$p$ sei eine Primzahl und $p \equiv 3 \bmod 4$. Zeigen Sie:

*a)* Falls es zu $a \in \mathbb{F}_p$ ein $b \in \mathbb{F}_p$ gibt mit $b^2 = a$, so ist $x = \pm a^{(p+1)/4}$ die beiden Lösungen der quadratischen Gleichung $x^2 = a$.
*Hinweis:* Wenden Sie den kleinen Satz von Fermat auf $b$ an!

*b)* Die Gleichung $x^2 = a$ ist in $\mathbb{F}_p$ genau dann lösbar, wenn $a^{(p-1)/2} = 1$ ist.

*c)* Lösen Sie im Körper $\mathbb{F}_{17}$ die quadratischen Gleichungen

$$x^2 = 2 \quad \text{und} \quad x^2 + 4x + 12 = 0\,!$$

**Aufgabe 3:** (*5 Punkte)*

Faktorisieren Sie das Polynom $f = x^5 + x^4 + 1 \in \mathbb{F}_2[x]$ nach dem Algorithmus von Berlekamp!

**Aufgabe 4:** (*5 Punkte)*

Das Polynom $f = x^7 + 11x^5 - 8x^4 - 21x^3 + x^2 + 72x - 35$ erfüllt die Kongruenz

$$f \equiv (x^4 + 20x^2 + 4x + 2)(x^3 + 3x + 22) \bmod 23\,.$$

*a)* Setzen sie diese Faktorisierung nach dem Henselschen Lemma fort zu einer Faktorisierung modulo $23^2$.

*b)* Versuchen Sie, daraus eine Faktorisierung von $f \in \mathbb{Z}[x]$ zu erraten und überprüfen Sie, ob diese korrekt ist!

*c)* Wie groß können die Koeffizienten eines irreduziblen Faktors von $f$ höchstens werden?

**Abgabe** bis zum Donnerstag, dem 16. Oktober 2008, um 15.30 Uhr