Technische Universität Berlin
Fakultät II – Institut für Mathematik
Prof. Stefan Felsner
Andreas Paffenholz

Diskrete MAFI
Sommersemester 2005

Wiebke Höhn
Raman Sanyal
Xiumei Wang

Diskrete und strukturelle Mathematik für Informatiker
6. Übungsblatt

Abgabe am 4. Juli 2005 **vor** der Vorlesung

Zum Erreichen der vollen Punktzahl muss bei jeder Aufgabe der Lösungsweg vollständig angegeben werden.

Aufgabe 1. — 2+2+2 Punkte

Wir betrachten die das Polynom

$$f(x) := x^4 + x^2 + 1 \quad \in \mathrm{K}[x]$$

Geben Sie eine Zerlegung von f in irreduzible Faktoren an (d. h. schreiben Sie f als Produkt von Polynomen, die sich jeweils nicht weiter in Polynome von kleinerem Grad zerlegen lassen, wenn es solche gibt), und zwar für jeden der drei Körper

$$(1)\ \ \mathrm{K} = \mathbb{Z}_2, \qquad (2)\ \ \mathrm{K} = \mathbb{Z}_5 \qquad (3)\ \ \mathrm{K} = \mathbb{R}.$$

Aufgabe 2. — 2+2 Punkte

Gegeben seien die beiden Polynome

$$f_1(x) = x^5 + x^4 + x^3 + x^2 + x + 1 \quad \text{und} \qquad f_2(x) = x^4 - x^2 + 1\ .$$

in einem Polynomring $K[x]$. Bestimmen Sie

(1) den größten gemeinsamen Teiler $g(x)$ der beiden Polynome und
(2) eine Linearkombination von g aus f_1 und f_2.

für die beiden Körper $K = \mathbb{Z}_2$ und $K = \mathbb{R}$.

Aufgabe 3. — 6 Punkte

Sei p eine ungerade Primzahl. Dann wissen wir, dass $\mathbb{Z}_p$ ein Körper ist. Mit $\mathbb{Z}_p^*$ bezeichnen wir im folgenden die multiplikative Gruppe des Körpers. Die folgenden vier Aussagen sind äquivalent.

(1) $x^2 + 1 \in \mathbb{Z}_p[x]$ ist reduzibel.
(2) $x^2 \equiv -1 \mod p$ hat eine Lösung in $\mathbb{Z}$.
(3) $\mathbb{Z}_p^*$ enhält ein Element der Ordnung 4.
(4) $p \equiv 1 \mod 4$.

Beweisen Sie mindestens drei der Äquivalenzen!

Aufgabe 4. — 4 Punkte

Das Polynom $f(z) = z^2 + 1 \in \mathbb{Z}_3[z]$ ist irreduzibel (Überprüfen Sie dies!).

Wieviele Elemente hat der Quotientenkörper $\mathbb{Z}_3(f)$? Bestimmen Sie die Multiplikationstabelle von $\mathbb{Z}_3(f)$.

Die folgenden beiden Aufgaben sind ***nicht*** *Teil der Hausaufgabe.*
Wenn Sie jedoch erwarten, dass Ihre bisher erreichten Punkte (zusammen mit den evtl. in diesen Hausaufgaben erzielten Punkten) nicht für die Teilnahme an der Klausur ausreichen, dann können Sie durch die Bearbeitung dieser Aufgaben versuchen, Ihren Punktestand zu verbessern und so trotzdem eine Zulassung zur Klausur erreichen.

Zusatzaufgabe 1. — 5 Punkte

Sei $R := \mathbb{Z}_2[x]$ der Polynomring in einer Variablen über $\mathbb{Z}_2$. Bestimmen Sie alle Polynome vom Grad höchstens 3 und untersuchen Sie, welche dieser Polynome irreduzibel sind. Geben Sie gegebenenfalls eine Zerlegung an!

Zusatzaufgabe 2. — 5 Punkte

Sei K ein Körper, und es gebe eine Zahl $n \in \mathbb{N}$ so dass

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ mal}} = 0.$$

Sei n die kleinste Zahl mit dieser Eigenschaft. Zeigen Sie, dass n eine Primzahl sein muss.