Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Ernst W. Mayr

WS 2003/04
Übungsblatt 7
5. Dezember 2003

Diskrete Strukturen I

Abgabe bis Donnerstag, 11. Dezember 2003, 12:15 Uhr (in Stellordner vor Raum 03.09.052)

Aufgabe 1

Sei $K[x]$ der Polynomring (K ein Körper) und sei $g \in K[x]$, $\text{grad}(g) \geq 1$ fest gewählt. Für jedes $f \in K[x]$ bezeiche $r(f)$ den Rest der Polynomdivision von f durch g. Zeigen Sie, dass für alle $f_1, f_2 \in K[x]$ gilt:

(i) $r(f_1 + f_2) = r(f_1) + r(f_2)$,

(ii) $r(f_1 \cdot f_2) = r(r(f_1) \cdot r(f_2))$.

Aufgabe 2

(i) Zeigen Sie, dass das Polynom $g(x) = x^3 + x + 1$ irreduzibel in $\text{GF}(2)[x]$ ist.

(ii) Nach (i) und Vorlesung (Kap. 4, Satz 18) ist $\text{GF}(8) := \text{GF}(2)[x]/(g)$ ein Körper. Erstellen Sie für diesen Körper GF(8) eine Multiplikationstabelle.

(iii) Bestimmen Sie a^{-1} für jedes Element $a \in \text{GF}(8)^*(= \text{GF}(8) \setminus \{0\})$.

(iv) Nach Vorlesung (Kap.4, Satz 4) ist $(\text{GF}(8)^*, \cdot)$ eine zyklische Gruppe. Welche Ordnung besitzt diese Gruppe? Finden Sie alle Generatoren von $\text{GF}(8)^*$, d.h. alle Elemente $a \in \text{GF}(8)^*$, so dass $\text{GF}(8)^* =< a > (= \{a^i : i \in \mathbb{Z}\})$ gilt. (Begründen Sie Ihre Antworten!)

Aufgabe 3

Sei $(K, +, \cdot)$ ein Körper mit Einselement 1_K (neutrales Element bzgl. Multiplikation).
Die *Charakteristik* von K (i.Z. $\text{char}(K)$) ist wie folgt definiert:
Gilt $\underbrace{1_K + \cdots + 1_K}_{n\text{-mal}} \neq 0$ für alle $n \geq 1$, so ist $\text{char}(K) = \infty$, andernfalls definiert man $\text{char}(K) = \min\{n \in \mathbb{N} : \underbrace{1_K + \cdots + 1_K}_{n\text{-mal}} = 0\}$. Zeigen Sie:

(i) Ist $\text{char}(K) < \infty$, so ist $\text{char}(K)$ eine Primzahl.

(ii) Sei $p = \text{char}(K) < \infty$. Dann ist die Abbildung

$$\Phi_p : K \to K,\ a \mapsto a^p$$

ein Ringhomomorphismus – er heißt der *Frobenius-Endomorphismus* von K.

(iii) Ist $p = \text{char}(K) < \infty$ und K ein endlicher Körper, so ist Φ_p in (ii) bijektiv.

Aufgabe 4

Sei K ein endlicher Körper, wobei $q = |K|$ ungerade ist, $K^* = K \setminus \{0\}$. Zeigen Sie:

(i) $x^{q-1} - 1 = \prod_{a \in K^*} (x - a)$ in $K[x]$,

(ii) $x^q - x = \prod_{a \in K} (x - a)$ in $K[x]$,

(iii) $\sum_{a \in K} a = 0$ (Hinweis: (ii)),

(iv) $\prod_{a \in K^*} a = -1$ (Hinweis: (i)),

(v) Für jede Primzahl p gilt: $(p-1)! \equiv -1 \mod p$ (Wilsonscher Satz).