Technische Universität München
Institut für Informatik
Lehrstuhl für Theoretische Informatik und
Grundlagen der Künstlichen Intelligenz
Prof. Dr. Dr. h.c. Wilfried Brauer

Wintersemester 2004/05
Diskrete Strukturen I
Übungsblatt 5
24. November 2004
Sebastian Wernicke

Diskrete Strukturen I

15. Ringrestregeln

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:

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

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

(Zur Erinnerung: Es gibt eindeutig bestimmte $q_i, r_i \in K[x]$ mit $f_i = q_i g + r_i$ und $\text{grad}(r_i) < \text{grad}(g)$; es ist dann $r_i = r(f_i)$ $(i = 1, 2)$)

16. Feldforschung

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

b) Nach *a)* und Vorlesung ist $\text{GF}(8) := \text{GF}(2)[x]/(g)$ ein Körper. Erstellen Sie für diesen Körper $\text{GF}(8)$ eine Multiplikationstabelle.

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

17. Körpercharakteristik

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:

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

b) 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.

18. Körpersätze

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

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

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

c) $\sum_{a \in K} a = 0$ (Hinweis: b) verwenden),

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

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