TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Mathematik und Naturwissenschaften Fachrichtung Mathematik, Institut für Algebra

Prof. U. Baumann, Dr. C. Zschalig

Algebra für Informationssystemtechniker (Modul ET - 01 04 04), Sommersemester 2015

13. Übungsblatt für die Übung am 7.7.2015

Endliche Körper

Ü73. Konstruieren Sie einen Körper mit 8 Elementen und geben Sie die Verknüpfungstafeln für Addition und Multiplikation an. Geben Sie zu jedem Element des Körpers sein multiplikatives Inverses und seine Ordnung in der additiven Gruppe und in der multiplikativen Gruppe an.

Hinweis: Da $8 = 2^3$ ist, benötigen Sie zur Konstruktion ein irreduzibles Polynom der Ordnung 3 über $\mathbb{Z}(2)[x]$.

Ü74. (a) Zeigen Sie, dass das Polynom $x^3 + x + 1$ irreduzibel im Polynomring $\mathrm{GF}(2)[x]$ ist.

(b) Bestimmen Sie alle irreduziblen Polynome vom Grad 3 in $\mathrm{GF}(2)[x]$.

(c) Geben Sie ein irreduzibles Polynom vom Grad 5 in $\mathrm{GF}(2)[x]$ an. Geben Sie ein Polynom vom Grad 5 in $\mathrm{GF}(2)[x]$ an, das nicht irreduzibel ist, aber keine Nullstellen besitzt.

Ü75. (a) Zeigen Sie: Ist $f(x)$ ein Polynom im Ring $R[x]$, dann gilt $(x-a)|f(x) \iff f(a) = 0$.

(b) Schlussfolgern Sie aus (a): Ist K ein Körper und $f(x)$ ein Polynom aus dem Polynomring $\mathrm{K}[x]$ vom Grad 2 oder 3, dann ist $f(x)$ genau dann irreduzibel, wenn $f(x)$ eine Nullstelle in K besitzt.

H76. (a) Zeigen Sie: das Polynom $p(X) = 2X^2 + 2X + 1$ ist irreduzibel in $\mathsf{GF}(3)[X]$.

(b) Bestimmen Sie zu allen Elementen aus $\mathsf{GF}(9) \cong \mathsf{GF}(3)[X]/p(X)$ die additiven und die multiplikativen Inversen.

(c) Berechnen Sie in $\mathsf{GF}(9) \cong \mathsf{GF}(3)[X]/p(X)$ mit $\alpha := X \pmod{p(X)}$:

$$(\alpha + 1)^{-2} \cdot \alpha^3 + 2(\alpha + 2)$$

H77. Beweisen Sie: Jedes irreduzible Polynom $p(x) \in \mathbb{Z}_2[x]$ vom Grad 5 ist primitiv.

Hinweis: Sie werden in der letzten Vorlesung primitive Polynome kennenlernen und erfahren, dass $p(x)$ genau dann primitiv ist, wenn das Element x die gesamte multiplikative Gruppe $(\mathbb{Z}_2[x]/p(x) \setminus \{0\}, \cdot)$ erzeugt.

W78. Gegeben ist der Graph $G = (V, E)$ mit der Knotenmenge $V = \{1, 2, 3, 4, 5, 6\}$ und der Kantenmenge
$E = \{\{1,2\}, \{1,3\}, \{1,5\}, \{1,6\}, \{2,3\}, \{2,4\}, \{2,5\}, \{3,4\}, \{3,6\}, \{4,5\}, \{4,6\}, \{5,6\}\}$.

(a) Wie viele Elemente enthält die Potenzmenge $\mathcal{P}(V)$?
Wie viele Elemente enthält die Potenzmenge $\mathcal{P}(E)$?
Geben Sie ein $X \in \mathcal{P}(E)$ mit $|X| = 2$ an.

(b) Der Graph G ist planar. Ermitteln Sie die Anzahl der Flächen in einem ebenen Graphendiagramm von G mit der Polyederformel von Euler. Zeichnen Sie ein ebenes Diagramm des Graphen G.

(c) Finden Sie zwei nichtisomorphe Bäume T_1 und T_2 mit der Knotenanzahl 6, die Untergraphen von G sind. Geben Sie für T_1 das Graphendiagramm und für T_2 den Prüfercode an.

(d) Ermitteln Sie $\mathcal{P}(V) \cap \mathcal{P}(E)$.

W79. (a) Berechnen Sie $\varphi(120)$.

(b) Wie viele Elemente $x \in \mathbb{Z}_{120}$ besitzen ein multiplikatives Inverses?

(c) Berechnen Sie die multiplikativen Inversen zu $a = 17$, $b = 117$ und $c = 49$ in $\mathbb{Z}_{120}$ (falls sie existieren) mit dem erweiterten Euklidischen Algorithmus.

(d) Geben Sie eine Lösung der Gleichung $117x = 111$ in $\mathbb{Z}_{120}$ an. Wie viele Lösungen hat diese Gleichung in $\mathbb{Z}_{120}$?

W80. Gegeben sind die Elemente $\alpha = (1\,2\,7\,6\,5\,4\,8\,3)$ und $\beta = (2\,3)(7\,8)(4\,6)$ der symmetrischen Gruppe S_8.

(a) Ermitteln Sie die Ordnung von α.
Geben Sie ein Element $\gamma \in S_8$ an, das die Ordnung 10 besitzt.

(b) Berechnen Sie $\alpha \circ \beta$, $\beta \circ \alpha$ und $\alpha^{83} \circ \beta \circ \alpha^4$.

(c) Ist die Gruppe $\langle \alpha, \beta \rangle$ abelsch?
Zeigen Sie, dass die Gruppe $\langle \alpha, \beta \rangle$ nicht zyklisch ist.

(d) Stellen Sie α als Produkt von Transpositionen dar und geben Sie das Signum von α an.