Übungsblatt 6

Aufgabe 21

(a) Zeigen Sie, dass es ein $n_0 \geq 0$ gibt, so dass für alle $n > n_0$ gilt: Die Anzahl der multilinearen Monome mit n Variablen vom Grad $\leq \frac{n}{2} + \frac{\sqrt{n}}{2}$ ist höchstens $\frac{9}{10} \cdot 2^n$.

(b) Seien $p \neq q$ prim. Zeigen Sie, dass es eine Zahl $k > 0$ gibt, so dass in $\mathrm{GF}(p^k)$ ein $\omega \neq 1$ existiert mit $\omega^q = 1$.

Aufgabe 22

(a) Bestimmen Sie in $\mathbb{Z}_5[x]/3x^2 + 1$ den Repräsentanten für die Restklasse, in der das Polynom $2x^5 + x^4 + 4x + 3$ enthalten ist.

(b) Bestimmen Sie alle irreduziblen Polynome $m(x)$ vom Grad 2 in $\mathbb{Z}_2[x]$. Stellen Sie jeweils die Additions- und Multiplikationstafeln für den Polynomrestklassenring $\mathbb{Z}_2[x]/m(x)$ auf.

(c) Sei $m(x) = x^2 + 2$. Stellen Sie die Additions- und Multiplikationstafeln für den Polynomrestklassenring $\mathbb{Z}_3[x]/m(x)$ auf. Ist $\mathbb{Z}_3[x]/m(x)$ ein Körper?

(d) Berechnen Sie das multiplikative Inverse von $g(x) = x^4 + x^2 + 2x$ in $\mathbb{Z}_3[x]/m(x)$, wobei $m(x) = 2x^6 + x^3 + x^2 + 2$ ist. Ist $m(x)$ irreduzibel über $\mathbb{Z}_3$?

Aufgabe 23

Seien a, b Elemente einer abelschen Gruppe G mit Ordnungen $\mathrm{ord}(a)$ und $\mathrm{ord}(b)$.

(a) Zeigen Sie, dass ab die Ordnung $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$ hat, falls $\mathrm{ord}(a)$ und $\mathrm{ord}(b)$ teilerfremd sind.

(b) Lässt sich die Aussage in Teilaufgabe (a) zu $\mathrm{ord}(ab) = \mathrm{kgV}(\mathrm{ord}(a), \mathrm{ord}(b))$ verallgemeinern?

Aufgabe 24

(a) Zeigen Sie, dass ein Polynom $p(x) \in \mathbb{F}[x]$ vom Grad $n \geq 1$ über einem Körper $\mathbb{F}$ höchstens n Nullstellen besitzt.

(b) Finden Sie ein Polynom $q(x) \in \mathbb{Z}_6[x]$ vom Grad 2 mit möglichst vielen Nullstellen.

Aufgabe 25

Zeigen Sie, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist.

Hinweis: Sei $h = \prod p_i^{e_i}$ die Primfaktorzerlegung der Gruppenordnung $h = \|\mathbb{F}^*\|$. Finden Sie Elemente $b_i \in \mathbb{F}^*$ der Form $b_i = a_i^{h/p_i^{e_i}}$ mit $\mathrm{ord}(b_i) = p_i^{e_i}$, indem Sie die Anzahl der Nullstellen des Polynoms $x^{h/p_i} - 1$ abschätzen, und verwenden Sie Aufgabe 23.