Goethe-Universität, Frankfurt am Main
Sommersemester 2008
Prof. Dr. C.P. Schnorr, Antoine Scemama

Diskrete Mathematik, Übung 7

Aufgabe 1. Sei G endliche, abelsche Gruppe, $a, b \in G$. Zeige:

1. $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$ impliziert $\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

2. $\mathrm{kgv}(\mathrm{ord}(a) \mid a \in G) = \max\{\mathrm{ord}(a) \mid a \in G\}$.

Hinweis: Lemma 17.3 Skript Theobald

Aufgabe 2.

1. Zeige: Ein Polynom $g \in K[x]$ vom Grad 2 oder 3 über einem Körper K ist genau dann irreduzibel über K, wenn es keine Nullstelle in K hat. Warum gilt das nicht für Polynome vom Grad ≥ 4 ?

2. Zähle alle irreduzible, normierte Polynome vom Grad ≤ 4 in $\mathbb{Z}_3[x]$ auf.

Die Ableitung f' von $f = \sum_i f_i x^i \in K[x]$ ist $f' = \sum_i i f_i x^{i-1}$.

Aufgabe 3. Sei K Körper $\mathbf{0} \neq f \in K[x]$, $a \in K$. Zeige:

1. $(x-a)^m \mid f \;\Leftrightarrow\; f(a) = f'(a) = \cdots = f^{(m-1)}(a) = 0$ für $m \geq 1$

2. $f \mid x^{p^m} - x$ und $f \in \mathbb{Z}_p[x]$ irreduzibel impliziert $f^2 \not| x^{p^m} - x$.

Aufgabe 4. Das Polynom $f = x^3 - x^2 + 1 \in \mathbb{Z}_3[x]$ ist irreduzibel. Konstruiere mit f den Körper $\mathbb{F}_{27}$ mit Basis über $\mathbb{Z}_3$ und ein primitives Element $\alpha \in \mathbb{F}_{27}^*$.

Abgabetermin dieses Blattes: Montag, der 5.Juni um 12.10 Uhr

Übungsblätter im Internet:
www.mi.informatik.uni-frankfurt.de:
Teaching, Diskrete Mathematik.