Prof. C. P. Schnorr Sommersemester 2006

# Diskrete Mathematik

Blatt 7, 02.06.2006, Abgabe 09.06.2006

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

1. $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$ impliziert $\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.
2. $\mathrm{kgV}\{\mathrm{ord}(a) \mid a \in G\} = \max\{\mathrm{ord}(a) \mid a \in G\}$.
3. Welche Ordnungen kommen in der additiven Gruppe $\mathbf{Z}_N$ mit $N \in \mathbf{N}$ vor?

*Hinweis:* 1. $\langle a \rangle \cap \langle b \rangle = \{1_G\}$. Skript Theobald, Lemma 12.3.

**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 $\geq 4$ ?
2. Zähle alle irreduzible, normierte Polynome vom Grad $\leq 4$ in $\mathbf{Z}_3[x]$ auf.

**Aufgabe 3.** Sei $K$ Körper $0 \neq f \in K[x]$, $a \in K$. 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 $f \in \mathbf{Z}_p[x]$ irreduzibel impliziert $f^2 \nmid x^{p^m} - x$.

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

**(6 Punkte pro Aufgabe)**