B. Külshammer
M. Müller

Ausgabe: 30.10.06
Abgabe: 06.11.06

Übungen zur Algebra I

Blatt 3

Aufgabe 10 (2+2+2+2+2+2+2)
Für ein Element a in einer Gruppe G nennt man

$$\operatorname{ord}(a) = \min\{n \in \mathbb{N} : a^n = 1\}$$

die **Ordnung** von a. Existiert das Minimum nicht, so sagt man, dass a unendliche Ordnung hat, und schreibt $\operatorname{ord}(a) = \infty$. Zeigen Sie:

(i) In einer endlichen Gruppe G hat jedes Element endliche Ordnung.

(ii) Hat a die Ordnung $n < \infty$, so sind die Elemente $1, a, a^2, \ldots, a^{n-1}$ paarweise verschieden.

(iii) Für $k, l \in \mathbb{Z}$ gilt in (ii): $a^k = a^l \Leftrightarrow k \equiv l \pmod{n}$.

(iv) Für $m \in \mathbb{Z}$ gilt in (ii): $a^m = 1 \Leftrightarrow n|m$.

(v) Für $i \in \mathbb{N}$ gilt in (ii): $\operatorname{ord}(a^i) = \frac{n}{\operatorname{ggT}(i,n)}$.

(vi) Sind $a, b \in G$ Elemente endlicher Ordnung mit $ab = ba$ und $\operatorname{ggT}(\operatorname{ord}(a), \operatorname{ord}(b)) = 1$, so ist $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$.

(vii) Berechnen Sie die Ordnungen der Elemente in $U(\mathbb{Z}/24\mathbb{Z})$.

Aufgabe 11 (2+2+2+2)
Beweisen Sie:

(i) $641|2^{2^5} + 1$.

(ii) $2 \neq p \in \mathbb{P} \Rightarrow \left(\frac{p-1}{2}!\right)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.

(iii) $2 \neq p \in \mathbb{P} \wedge n \in \mathbb{N} \Rightarrow (1+p)^{p^{n-1}} \equiv 1 + p^n \pmod{p^{n+1}}$.

(iv) $2 \leq n \in \mathbb{N} \Rightarrow 5^{2^{n-2}} \equiv 1 + 2^n \pmod{2^{n+1}}$.

Aufgabe 12 (2+2+2)
Zeigen Sie, dass für jeden Körper K und jede endliche Untergruppe G von $(K \setminus \{0\}, \cdot)$ gilt:

(i) Für $t \in \mathbb{N}$ enthält G entweder 0 oder $\varphi(t)$ Elemente der Ordnung t.

(ii) Für jeden (positiven) Teiler t von $|G|$ enthält G genau $\varphi(t)$ Elemente der Ordnung t.

(iii) Es existiert ein Element $a \in G$ mit $G = \{1, a, a^2, \ldots, a^{n-1}\}$ und $n = |G|$.