

### 3. Übung Algebra I

(Zyklische Gruppen, Normalteiler, Faktorgruppen, Homomorphiesätze)

---

#### 1. Aufgabe

Es sei  $G$  eine Gruppe. Beweisen oder widerlegen Sie die folgenden Aussagen:

- Es sei  $(G : 1) = 40$ . Dann existiert eine Untergruppe  $H$  von  $G$  mit 12 Elementen.
- Jede echte Untergruppe von  $G$  mit  $(G : 1) = p^2$  ist zyklisch, falls  $p$  eine Primzahl ist.
- $G$  ist nicht zyklisch, falls es keinen Homomorphismus von  $\mathbb{Z}$  nach  $G$  gibt.

(3 Punkte)

#### 2. Aufgabe

- Zeigen Sie, dass jedes Element der Gruppe  $\mathbb{Q}/\mathbb{Z}$  endliche Ordnung besitzt.
- Zeigen Sie, dass für jedes  $n \in \mathbb{N}$  und  $a \in \mathbb{Q}/\mathbb{Z}$  die Abbildung

$$\varphi : \mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z} : a \mapsto na,$$

ein Epimorphismus mit Kern  $\varphi = \mathbb{Z}/n\mathbb{Z}$  ist.

(4 Punkte)

#### 3. Aufgabe

- Es seien  $G$  eine Gruppe und  $V$  eine Teilmenge von  $G$ . Der **Normalisator**  $N(V)$  von der Menge  $V$  ist definiert durch

$$N(V) := \{g \in G \mid gV = Vg\}.$$

Zeigen Sie, dass  $N(V)$  eine Untergruppe von  $G$  ist.

- Es sei  $V$  eine Untergruppe von  $G$ . Zeigen Sie, dass  $V$  genau dann ein Normalteiler von  $G$  ist, falls  $N(V) = G$  gilt.
- Zeigen Sie, dass  $V$  ein Normalteiler von  $N(V)$  ist, falls  $V$  eine Untergruppe von  $G$  ist.

- (d) Es seien  $G$  eine Gruppe und  $U$  eine Untergruppe von  $G$ . Zeigen Sie, dass

$$N(U)/C(U) \cong \mathcal{T}$$

gilt, wobei  $N(U)$  Normalisator von  $U$ ,  $C(U) = \{a \in G \mid aua^{-1} = u \text{ für alle } u \in U\}$  und  $\mathcal{T}$  eine Untergruppe von  $\text{Aut}(U)$  sind.

- (e) Zeigen Sie, dass  $8\mathbb{Z}/56\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z}$  gilt.

(8 Punkte)

#### 4. Aufgabe

Es seien  $G$  und  $G'$  Gruppen und  $\phi : G \rightarrow G'$  ein Epimorphismus mit Kern  $\phi = N$ . Ferner seien

$$L := \{H \mid H \leq G \text{ mit } N \subseteq H\} \text{ und } L' := \{H' \mid H' \leq G'\}.$$

- (a) Zeigen Sie, dass die Abbildung

$$f : L \rightarrow L', H \mapsto \phi(H)$$

die Abbildung

$$g : L' \rightarrow L, H' \mapsto \phi^{-1}(H')$$

als Umkehrabbildung besitzt, wobei  $\phi^{-1} = \{g \in G \mid \phi(g) \in H'\}$  ist.

- (b) Zeigen Sie, dass eine Untergruppe  $V$  von  $G$  genau dann ein Normalteiler von  $G$  ist, falls  $\phi(V)$  ein Normalteiler von  $G'$  ist.
- (c) Es seien nun  $G = \langle g \rangle$  und  $G' = \langle g' \rangle$  mit  $g \in G$  und  $g' \in G'$ . Ferner seien  $\text{ord}(g) = 12$ ,  $\text{ord}(g') = 6$  und der Gruppenhomomorphismus

$$\phi : G \rightarrow G', g^i \mapsto g'^i$$

gegeben. Wie sehen die Mengen  $L$  und  $L'$  aus?

(5 Punkte)

#### 5. Aufgabe

Es sei  $G = \langle g \rangle$  eine zyklische Gruppe mit  $\text{ord}(g) = n \in \mathbb{N}$ , d. h. jedes Element  $a \in G$  lässt sich durch  $a = g^j$  mit  $j \in \{0, 1, \dots, n-1\}$  eindeutig darstellen. Die Exponent für ein Element  $a \in G$  mit  $a = g^j$  nennen wir den **diskreten Logarithmus** von  $a$  zur Basis  $g$ . Wir wollen zu gegebenem Element  $a \in G$  den diskreten Logarithmus  $j$  zur fest gewählten Basis  $g$  berechnen.

Auf der VL-Seite ist eine KASH-Datei **DiskretLog.k** vorgegeben. Dort finden Sie eine Gruppe  $G$  mit ihrem Erzeuger  $g$ , eine Funktion 'VerknuepfeElemente', welche beliebige Elemente von  $G$  verknüpft und eine Funktion 'ghochn', welche die Potenz  $g^n$  berechnet.

- (a) Implementieren Sie zuerst einen einfachen Algorithmus, der durch Ausprobieren den diskreten Logarithmus eines gegebenen Elements  $a \in G$  berechnet.

- (b) Es sei  $a = g^j$  mit  $j \in \{0, 1, \dots, n-1\}$  und  $0 < l < n-1$  gegeben. Mit  $j = t \cdot l + r$ ,  $t, r \in \mathbb{Z}$  mit  $l > r \geq 0$ , kann man nun  $g^j = g^{t \cdot l + r} = a$  schreiben. Es gilt dann  $g^{t \cdot l} = a \cdot g^{-r}$ . Der diskrete Logarithmus von  $a$  zur Basis  $g$  kann dadurch berechnet werden, in dem man versucht bei den Ausdrücken  $(g^l)^k$  und  $a \cdot g^{-s}$  mit  $0 \leq k \cdot l \leq n$  und  $0 \leq s < l$  eine Übereinstimmung zu finden. Dabei soll  $l$  natürlich geschickt gewählt werden. Diesen Algorithmus nennt man **Baby-Step-Giant-Step**. Implementieren Sie diesen Algorithmus, welcher als Eingabe ein  $g \in G$  der zyklischen Gruppe  $G$  und  $a \in G$  bekommt und als Ausgabe den diskreten Logarithmus von  $a$  zur Basis  $g$  in  $G$  berechnet.
- (c) Was lässt sich über den Aufwand der Ausprobier-Methode und der Baby-Step-Giant-Step Methode sagen?

(6 Punkte)

**Hinweis 1:** KANT/KASH ist frei erhältlich unter

[www.math.tu-berlin.de/~kant/download.html](http://www.math.tu-berlin.de/~kant/download.html).

Sie können natürlich auch KANT/KASH zuhause installieren. Eine kurze Einführung in KASH finden Sie auch unter der VL-Seite.

**Hinweis 2:** Sie können die 5. Aufgabe bis 15.05.2008 abgeben.