Universität Augsburg
Institut für Mathematik

Prof. Dr. Katrin Wendland
Dr. Katrin Leschke
WS 2006/2007

Lineare Algebra I, Lösung zur 3. und 4. Aufgabe

Aufgabe 3 (4 Punkte). Sei $(G, \circ)$ eine Gruppe und $A \subset G$. Sei

$$\hat{A} = \{a_1 \circ \ldots \circ a_n \mid n \in \mathbb{N} \text{ und } a_i \in A \text{ oder } a_i^{-1} \in A \text{ für alle } i = 1, \ldots, n\}.$$

Erst einmal ein Beispiel...

$G = (\mathbb{Z}, +)$, $A = \{3, 5\} \subset \mathbb{Z}$, A ist natürlich selbst keine Gruppe (kein neutrales Element der Addition). Was ist nun also $\hat{A}$?

$$\begin{aligned} 3 \in A, 5 \in A &\implies 3, 5 \in \hat{A}. \\ -(-3) = 3 \in A &\implies -3 \in \hat{A}. \\ 5 \in A, -(-3) \in A &\implies 2 = 5 + (-3) \in \hat{A}, 8 = 5 + 3 \in \hat{A}. \\ 3 \in A, -(-3) \in A &\implies 3 + (-3) \in \hat{A} \end{aligned}$$

Also überzeugt man sich: $\hat{A} = \mathbb{Z}$.

Zeigen Sie:

- **$\hat{A}$ ist eine Gruppe.** Es reicht zu zeigen, dass $\hat{A}$ eine Untergruppe von G ist, d.h., dass $\hat{A}$ abgeschlossen ist bezüglich der Verknüpfung $\circ$.
  - Seien $\hat{a}, \hat{b} \in \hat{A}$. Dann existieren $n, m \in \mathbb{N}$ und a_i, b_i mit $a_i \in A$ oder $a_i^{-1} \in A$ für $i = 1, \ldots, n$ und $b_j \in A$ oder $b_j^{-1} \in A$ für $j = 1, \ldots, m$, und

    $$\hat{a} = a_1 \circ \ldots \circ a_n, \quad \hat{b} = b_1 \circ \ldots \circ b_m \,.$$

    Also ist

    $$\hat{a} \circ \hat{b} = a_1 \circ \ldots \circ a_n \circ b_1 \circ \ldots \circ b_m \in \hat{A} \,,$$

    da $\hat{a} \circ \hat{b}$ die Verknüpfung von $n + m$ Elementen ist, die entweder selbst in A sind oder deren Inverse in A sind.
  - Sei $\hat{a} = a_1 \circ \ldots \circ a_n \in \hat{A}$. Dann ist

    $$\hat{a}^{-1} = a_n^{-1} \circ \ldots \circ a_1^{-1} \in \hat{A} \,,$$

    da $\hat{a}^{-1}$ die Verknüpfung von n Elementen ist, die entweder selbst in A sind oder deren Inverse in A sind.
  - Damit ist $\hat{A}$ abgeschlossen bezüglich der Verknüpfung $\circ$ und somit eine Untergruppe von G. Damit ist $\hat{A}$ eine Gruppe.
- **Ist $H \subset G$ eine Untergruppe von G mit $A \subset H$ dann gilt auch $\hat{A} \subset H$.**

  Z.z: Für alle $\hat{a} \in \hat{A}$ gilt $\hat{a} \in H$.

Sei also $\hat{a} = a_1 \circ \ldots \circ a_n \in \hat{A}$. Da $a_i \in A \subset H$ oder $a_i^{-1} \in A \subset H$, ist also $a_i \in H$ oder $a_i^{-1} \in H$. Da H eine Gruppe ist, ist mit $a_i \in H$ auch $a_i^{-1} \in H$ (bzw. mit $a_i^{-1} \in H$ ist auch $a_i = (a_i^{-1})^{-1} \in H$). Damit ist

$$\hat{a} = \underbrace{a_1}_{\in H} \circ \ldots \circ \underbrace{a_n}_{\in H} \in H\,.$$

Das heißt, $\hat{A}$ ist die kleinste Untergruppe von G, die A enthält. Man nennt $\hat{A}$ die von A erzeugte Untergruppe.

Wie sieht $\hat{A}$ aus, wenn A einelementig ist?
Sei $A = \{g\}$ mit $g \in G$. Da $\hat{A}$ alle Kompositionen von endlich vielen Elementen in A enthält, sind genau die Potenzen von g die Elemente von $\hat{A}$:

$$\hat{A} = \{g^n \mid n \in \mathbb{Z}\}\,.$$

(Spezialfälle: Wenn $g = e$, dann ist $\hat{A} = \{e\}$. Wenn $g^n \neq e$ für ale $n \in \mathbb{Z}$, dann ist $|\hat{A}| = \infty$, sonst erhält man eine endliche Gruppe. Aufgabe 4 zeigt: $\hat{A}$ ist isomorph zu einer zyklischen Gruppe).

Aufgabe 4 (4 Punkte). Sei G eine Gruppe und $A = \{g\}$ mit $g \in G$. Zeigen Sie: wird G von A erzeugt, d.h. $G = \hat{A}$, dann ist G isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/q\mathbb{Z}$ mit $q \in \mathbb{N}, q \geq 1$.

Zunächst erhält man mit Aufgabe 3: $G = \{g^n \mid n \in \mathbb{Z}\}$.

Fallunterscheidung:

1. Fall: $|G| = \infty$
Definiere $\varphi : \mathbb{Z} \to G, m \mapsto g^m \in G$. Dann ist φ Gruppenhomomorphismus, da

$$\varphi(m+n) = g^{m+n} = g^m \cdot g^n = \varphi(m) \cdot \varphi(n)\,.$$

Beh: φ ist injektiv:

$$\varphi(m) = \varphi(n) \implies g^m = g^n \overset{\text{Üb.}}{\implies} e = g^m \cdot g^{-n} = g^{m-n}$$

Wäre $k = m - n \neq 0$, dann entält die Gruppe G wegen $g^{l+k} = g^l \cdot g^k = g^l$ für alle $l \in \mathbb{Z}$ höchstens k Elemente. Widerspruch! Also ist $k = 0$, d.h. $m = n$, und damit ist φ injektiv.

Beh: φ ist surjektiv: Sei $h \in G$, d.h. es existiert $m \in \mathbb{Z}$ mit $h = g^m$. Für dieses gilt dann

$$\varphi(m) = g^m = h\,,$$

also ist φ surjektiv.
Da φ somit ein bijektiver Gruppenhomomorphismus ist, sind G und $\mathbb{Z}$ isomorph.

2. Fall: $|G| = q < \infty$
Dann ist q die kleinste natürliche Zahl mit $q \geq 1$ und $g^q = e$ und es gilt $h^q = e$ für alle $h \in G$ (vergl. Übungsgruppen).

Definiere $\varphi : \mathbb{Z}/q\mathbb{Z} \to G, [m] \mapsto g^m$. Diese Abbildung ist wohldefiniert, da für $[m] = [\tilde{m}]$ gilt, daß $m = \tilde{m} + qk$ mit $k \in \mathbb{Z}$ und daher

$$\varphi([m]) = g^m = g^{\tilde{m}+qk} = g^{\tilde{m}} \cdot (g^q)^k = g^{\tilde{m}} \cdot e^k = g^{\tilde{m}}\,.$$

φ ist Gruppenhomomorphismus, da

$$\varphi([m] + [n]) \overset{\text{Def von } + \text{ in } \mathbb{Z}/q\mathbb{Z}}{=} \varphi([m+n]) = g^{m+n} = g^m \cdot g^n = \varphi([m]) \cdot \varphi([n])\,.$$

Beh: φ ist injektiv: Seien $u, v \in \mathbb{Z}/q\mathbb{Z}$ mit $\varphi(u) = \varphi(v)$. Wähle Repräsentanten $m \in u$ und $n \in v$ so dass $0 \leq n \leq m \leq q-1$ (geht: siehe Vl.). Dann gilt $g^m = g^n$, und damit (s.o.) $g^{m-n} = e$. Da q die kleinste natürliche Zahl ≥ 1 ist, für die $g^q = e$ ist also $m - n = 0$. Damit ist φ injektiv.

Beh: φ ist surjektiv: Sei $h \in G$, d.h., es existiert $m \in \mathbb{Z}$ mit $h = g^m$. Dann gilt für $[m] \in \mathbb{Z}/q\mathbb{Z}$:

$$\varphi([m]) = g^m = h\,,$$

also ist φ surjektiv.
Da φ somit ein bijektiver Gruppenhomomorphismus ist, sind G und $\mathbb{Z}/q\mathbb{Z}$ isomorph.