Algebra I

Musterlösung 1

Zyklische Gruppen, Untergruppen, Ordnung eines Elements

---

6. (a) Sei G eine Gruppe und sei g ein Element endlicher Ordnung. Zeige, dass für jede ganze Zahl k gilt

$$\operatorname{ord}(g^k) = \frac{\operatorname{kgV}(k, \operatorname{ord}(g))}{k}.$$

(b) Sei G eine Gruppe und seien $g, h \in G$ zwei kommutierende Elemente endlicher teilerfremder Ordnung. Zeige: $\operatorname{ord}(gh) = \operatorname{ord}(g) \cdot \operatorname{ord}(h)$.

(c) Zeige, dass die Aussage aus (b) für nicht kommutierende Elemente im Algemeinen nicht stimmt.

Lösung: (a) Sei $l \in \mathbb{Z}$. Dann gilt die Äquivalenz $g^l = e \Leftrightarrow \operatorname{ord}(g)|l$. Daraus folgt

$$\begin{aligned}\operatorname{ord}(g^k) &= \min\{l \in \mathbb{Z}_+ : \operatorname{ord}(g)|lk\} \\ &= \frac{1}{k}\min\{l \in \mathbb{Z}_+ : \operatorname{ord}(g)|l \wedge k|l\} \\ &= \frac{\operatorname{kgV}(k, \operatorname{ord}(g))}{k}.\end{aligned}$$

(b) Da g und h kommutieren gilt

$$(gh)^{\operatorname{ord}(g)\operatorname{ord}(h)} = g^{\operatorname{ord}(g)\operatorname{ord}(h)} h^{\operatorname{ord}(g)\operatorname{ord}(h)} = e^{\operatorname{ord}(h)} e^{\operatorname{ord}(g)} = e.$$

Es folgt $\operatorname{ord}(gh)|\operatorname{ord}(g)\operatorname{ord}(h)$.

Sei umgekehrt $(gh)^k = e$. Dann folgt mit Kommutativität $g^k = h^{-k}$. Aus Teil (a) wissen wir

$$\frac{\operatorname{kgV}(k, \operatorname{ord}(g))}{k} = \operatorname{ord}(g^k) = \operatorname{ord}(h^{-k}) = \frac{\operatorname{kgV}(k, \operatorname{ord}(h))}{k},$$

also $\operatorname{kgV}(k, \operatorname{ord}(g)) = \operatorname{kgV}(k, \operatorname{ord}(h))$. Deshalb gilt $\operatorname{ord}(g)|\operatorname{kgV}(k, \operatorname{ord}(h))$. Da $\operatorname{ord}(g)$ und $\operatorname{ord}(h)$ jedoch teilerfremd sind, impliziert das $\operatorname{ord}(g)|k$. Genauso gilt $\operatorname{ord}(h)|k$. Wieder wegen Teilerfremdheit von $\operatorname{ord}(g)$ und $\operatorname{ord}(h)$ folgt $\operatorname{ord}(g)\operatorname{ord}(h)|k$ und mit $k = \operatorname{ord}(gh)$ wissen wir $\operatorname{ord}(g)\operatorname{ord}(h)|\operatorname{ord}(gh)$. Insgesamt heisst das $\operatorname{ord}(gh) = \operatorname{ord}(g)\operatorname{ord}(h)$.

(c) Sei $G = S_3$ und seien g die Permutation, die 1 und 2 vertauscht, und h die Permutation, die $1, 2, 3$ zyklisch vertauscht. Dann sind $\operatorname{ord}(g) = 2$ und $\operatorname{ord}(h) = 3$ teilerfremd. Deren Produkt gh vertauscht die Zahlen $2, 3$ zyklisch, hat also Ordnung $2 \neq 2 \cdot 3$.

7. Seien $m, n \geqslant 1$ natürliche Zahlen.

Zeige: Es gilt genau dann $C_m \times C_n \cong C_{n \cdot m}$, wenn $\operatorname{ggT}(m, n) = 1$ ist.

Lösung: Seien zuerst m und n nicht teilerfremd. Sei $(g, h) \in C_m \times C_n$. Dann gilt

$$(g, h)^{\operatorname{kgV}(\operatorname{ord}(g), \operatorname{ord}(h))} = (g^{\operatorname{kgV}(\operatorname{ord}(g), \operatorname{ord}(h))}, h^{\operatorname{kgV}(\operatorname{ord}(g), \operatorname{ord}(h))}) = e.$$

Das bedeutet $\operatorname{ord}((g,h))|\operatorname{kgV}(\operatorname{ord}(g),\operatorname{ord}(h))$ und weiter wissen wir wegen $\operatorname{ord}(g)|m$ und $\operatorname{ord}(h)|n$, dass $\operatorname{kgV}(\operatorname{ord}(g),\operatorname{ord}(h))|\operatorname{kgV}(m,n)$ gilt. Da m und n nicht teilerfremd sind, wissen wir $\operatorname{kgV}(m,n) < mn$, somit ist $\operatorname{ord}((g,h)) < mn$ und (g,h) kann $C_m \times C_n$ deshalb nicht erzeugen. Da (g,h) beliebig gewählt war, ist $C_m \times C_n$ nicht zyklisch.

Nimm nun an, dass $\operatorname{ggT}(m,n) = 1$ gilt. Sei g ein Erzeuger von C_m und h ein Erzeuger von C_n. Die Elemente $(g,0)$ und $(0,h)$ kommutieren in $C_m \times C_n$. Wegen der vorherigen Aufgabe gilt $\operatorname{ord}((g,h)) = mn$, somit ist $C_{m\cdot n}$ zyklisch von (g,h) erzeugt.

8. Zeige, dass C_4 und $C_2 \times C_2$ bis auf Isomorphie die einzigen Gruppen der Ordnung 4 sind.

Lösung: Sei G eine Gruppe der Ordnung 4. Betrachte $g \in G$ mit maximaler Ordnung. Wegen $\operatorname{ord}(g)|4$ gilt $\operatorname{ord}(g) = 2$ oder $\operatorname{ord}(g) = 4$. Im zweiten Fall ist G von g erzeugt, also zyklisch der Ordnung 4 und somit isomorph zu C_4.

Im ersten Fall haben alle nichttrivialen Elemente aus G Ordnung 2. Nun können wir wie in Aufgabe 5(b) die Gruppentafel ausfüllen und sehen, dass die Gruppe isomorph zu $C_2 \times C_2$ ist.

9. Sei $m \geqslant 1$ eine natürliche Zahl.

Zeige, dass alle Untergruppen von C_m zyklisch sind und folgere, dass die Abbildung

$$\begin{array}{ccc} \{H : H \leqslant C_m\} & \to & \{k \in \mathbb{N} : k \mid m\} \\ H & \mapsto & |H| \end{array}$$

wohldefiniert und bijektiv ist.

Sei g ein Erzeuger von C_m, also ist $C_m = \{e, g, g^2, \ldots, g^{m-1}\}$. Sei $H \leqslant G$ eine Untergruppe. Sei $n = \min\{1 \leqslant k \leqslant m-1 : g^k \in H\}$ und sei $h = g^n$. Offensichtlich erzeugt h eine Untergruppe von H, nämlich $\langle h\rangle = \{e, g^n, g^{2n}, \ldots, g^{(\frac{m}{n}-1)n}\}$. Wir wollen zeigen, dass $\langle h\rangle = H$ gilt. Nimm im Widerspruch dazu an, es gebe ein $l \in \{1, \ldots, m-1\}$ mit $g^l \in H \backslash \langle h\rangle$. Dann folgt $n \nmid l$. Betrachte das kleinste Vielfache n' von n, das grösser ist als l. Aus $g^{n'} \in H$ folgt $g^{n'}(g^l)^{-1} = g^{n'-l} \in H$. Wegen $n \nmid l$ gilt aber $0 < n' - l < n$, was einen Widerspruch zur Wahl von n darstellt. Also ist H zyklisch von h erzeugt.

Jede Untergruppe von C_m zyklisch ist, folgt, dass ihre Ordnung m teilt. Daher ist die Abbildung aus der Aufgabenstellung wohldefiniert. Sei nun $H \leqslant C_m$ eine Untergruppe. Wegen obiger Argumentation ist $H = \langle g^n\rangle$ für einen Teiler n von m. Daraus folgt Injektivität. Umgekehrt erzeugt für jeden Teiler n von m das Element g^n eine Untergruppe von C_m der Ordnung $\frac{m}{n}$.

10. (a) Sei p eine Primzahl.

Zeige: Es gibt bis auf Isomorphie genau eine Gruppe der Ordnung p, nämlich C_p.

(b) Sei G eine Gruppe mit genau einer nichttrivialen echten Untergruppe.

Zeige: Dann gilt $G \cong C_{p^2}$ für eine Primzahl p.

Lösung: (a) Sei G eine Gruppe der Ordnung p und $g \in G\backslash\{e\}$. Dann gilt $1 < \operatorname{ord}(g)|p$. Da p prim ist, folgt $\operatorname{ord}(g) = p$ und G ist zyklisch mit Erzeuger g.

(b) Es sei $H \subset G$ die einzige von $\{e\}$ und G verschiedene Untergruppe von G. Betrachte $x \in G\backslash H$ und die davon erzeugte Untergruppe $\langle x\rangle$. Da $x \neq e$ und $x \notin H$ ist, kann diese weder trivial noch gleich H sein. Sie ist daher gleich ganz G und G ist zyklisch.

Wäre G unendlich zyklisch, hätte G unendlich viele Untergruppen. Daher ist G eine endliche zyklische Gruppe der Ordnung $n \geqslant 1$. Die Untergruppen von G stehen nach der vorherigen Aufgabe in bijektiver Korrespondenz mit den Teilern von n. Nach Voraussetzung hat n darum genau einen von 1 und n verschiedenen Teiler. Daher kann n nur einen Faktor p in der Primfaktorzerlegung haben und es muss $n = p^2$ gelten.

11. Sei G eine Gruppe mit Untergruppen $H_1, H_2 \leqslant G$.

Zeige, $(H_1 \cup H_2) \leqslant G \iff H_1 \leqslant H_2 \vee H_2 \leqslant H_1$.

Lösung: Wir nehmen zuerst an, dass $H_1 \leqslant H_2$ (beziehungsweise $H_2 \leqslant H_1$) gilt. Dann ist $H_1 \cup H_2 = H_2$ (beziehungsweise $H_1 \cup H_2 = H_1$) und somit ist $H_1 \cup H_2$ eine Untergruppe von G.

Nun gelte umgekehrt weder $H_1 \leqslant H_2$ noch $H_2 \leqslant H_1$. Dann können wir also Elemente $h_1 \in H_1 \backslash H_2$ und $h_2 \in H_2 \backslash H_1$ wählen. Nehmen wir nun an, es wäre $h_1 h_2 \in H_1 \cup H_2$. Dann wäre $h_1 h_2$ in H_1 oder in H_2 enthalten; sei ohne Beschränkung der Allgemeinheit $h_1 h_2 \in H_1$. Wegen $h_1 \in H_1$ ist auch $h_1^{-1} \in H_1$, und somit $h_1^{-1}(h_1 h_2) = (h_1^{-1} h_1) h_2 = h_2 \in H_1$. Aber wir hatten $h_2 \in H_2 \backslash H_1$ gewählt; Widerspruch. Somit haben wir gezeigt, dass $h_1 h_2 \notin H_1 \cup H_2$. Aber es gilt $h_1, h_2 \in H_1 \cup H_2$. Also ist $H_1 \cup H_2$ keine Untergruppe von G.

12. Zeige, dass jede Untergruppe von $(\mathbb{Z}, +)$ von der Form $n\mathbb{Z}$ ist für ein $n \in \mathbb{N}$.

Lösung: Sei $H \leqslant \mathbb{Z}$ eine Untergrupe und $n = \min\{k > 0 : k \in H\}$. Dann gilt $n\mathbb{Z} \leqslant H$. Sei per Widerspruchsannahme $m \in H \backslash n\mathbb{Z}$. Betrachte das kleinste Vielfache n' von n, das grösser ist als m. Dann gilt $0 < n' - m < n$ und $n' - m \in H$, Widerspruch zur Wahl von n. Also ist $H = n\mathbb{Z}$.