

Musterlösung Serie 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

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

- (b) Sei G eine Gruppe und seien $g, h \in G$ zwei kommutierende Elemente endlicher teilerfremder Ordnung. Zeige: $\text{ord}(gh) = \text{ord}(g) \cdot \text{ord}(h)$.
(c) Zeige, dass die Aussage aus (b) für nicht kommutierende Elemente im Allgemeinen nicht stimmt.

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

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

- (b) Da g und h kommutieren gilt

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

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

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

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

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

(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 $\text{ord}(g) = 2$ und $\text{ord}(h) = 3$ teilerfremd. Deren Produkt gh vertauscht die Zahlen 2, 3 zyklisch, hat also Ordnung $2 \neq 2 \cdot 3$.

7. Sei G eine endliche Gruppe mit Neutralelement e und sei $x \in G$.

- (a) Zeige, dass gilt $\text{ord}(x) | \text{ord}(G)$.
(b) Zeige, dass gilt $x^{\text{ord}(G)} = e$.

Lösung:

- (a) Sei $H := \langle x \rangle$ die Untergruppe von G , welche durch x erzeugt wird. Die Ordnung von H ist die Ordnung von x , also folgt aus dem Satz von Lagrange $\text{ord}(x) \mid \text{ord}(G)$.
- (b) Nach Aufgabe a) existiert $n \in \mathbb{N}$ so dass $\text{ord}(x)n = \text{ord}(G)$. Die Potenzregeln implizieren nun

$$x^{\text{ord}(G)} = x^{\text{ord}(x)n} = (x^{\text{ord}(x)})^n = e^n = e.$$

8. Seien $m, n \geq 1$ natürliche Zahlen.

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

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

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

Das bedeutet $\text{ord}((g, h)) \mid \text{kgV}(\text{ord}(g), \text{ord}(h))$ und weiter wissen wir wegen $\text{ord}(g) \mid m$ und $\text{ord}(h) \mid n$, dass $\text{kgV}(\text{ord}(g), \text{ord}(h)) \mid \text{kgV}(m, n)$ gilt. Da m und n nicht teilerfremd sind, wissen wir $\text{kgV}(m, n) < mn$, somit ist $\text{ord}((g, h)) < mn$ 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 $\text{ggT}(m, n) = 1$ 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 $\text{ord}((g, h)) = mn$, somit ist $C_{m \cdot n}$ zyklisch von (g, h) erzeugt.

9. 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 $\text{ord}(g) \mid 4$ gilt $\text{ord}(g) = 2$ oder $\text{ord}(g) = 4$. 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.

10. Sei G eine zyklische Gruppe. Zeige:

- (a) Jede Untergruppe von G ist zyklisch.
- (b) Falls G eine endliche Gruppe der Ordnung $m \geq 1$ ist, so ist die Abbildung

$$\begin{aligned} \{H : H \leq G\} &\rightarrow \{k \in \mathbb{N} : k \mid m\} \\ H &\mapsto |H| \end{aligned}$$

wohldefiniert und bijektiv.

Lösung: (a) Sei g ein Erzeuger von G , also ist $G = \{g^k \mid k \in \mathbb{Z}\}$. Sei $H \leq G$ eine Untergruppe. Sei $n = \min\{1 \leq k \leq m-1 : g^k \in H\}$ und sei $h = g^n$. Offensichtlich erzeugt h eine Untergruppe von H , nämlich $\langle h \rangle = \{g^{kn} \mid k \in \mathbb{Z}\}$. Wir wollen zeigen, dass

$\langle h \rangle = H$ gilt. Nimm im Widerspruch dazu an, es gebe ein $l \in \{1, \dots, m-1\}$ mit $g^l \in H \setminus \langle h \rangle$. 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.

(b) Nun nehmen wir an, dass G endlich der Ordnung m ist. Da jede Untergruppe von G zyklisch ist, folgt, dass ihre Ordnung m teilt. Daher ist die Abbildung aus der Aufgabenstellung wohldefiniert. Sei nun $H \leq G$ 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 G der Ordnung $\frac{m}{n}$.

11. (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 $g \in G \setminus \{e\}$. Dann gilt $1 < \text{ord}(g) | p$. Da p prim ist, folgt $\text{ord}(g) = p$ und G ist zyklisch mit Erzeuger g .

(b) Es sei $H \subset G$ die einzige von $\{e\}$ und G verschiedene Untergruppe von G . Betrachte $x \in G \setminus H$ 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 $n \geq 1$. 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.

12. Sei G eine Gruppe mit Untergruppen $H_1, H_2 \leq G$.

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

Lösung: Wir nehmen zuerst an, dass $H_1 \leq H_2$ (beziehungsweise $H_2 \leq H_1$) 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 $H_1 \leq H_2$ noch $H_2 \leq H_1$. Dann können wir also Elemente $h_1 \in H_1 \setminus H_2$ und $h_2 \in H_2 \setminus H_1$ 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 $h_2 \in H_2 \setminus H_1$ 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 .

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

Lösung: Sei $H \leq \mathbb{Z}$ eine Untergruppe und $n = \min\{k > 0 : k \in H\}$. Dann gilt $n\mathbb{Z} \leq H$. Sei per Widerspruchsannahme $m \in H \setminus n\mathbb{Z}$. 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 $H = n\mathbb{Z}$.