Universität des Saarlandes
Fachbereich 9, Mathematik
Prof. Dr. R. Berger

Musterlösung zur 2. Übung der Linearen Algebra I, WS 1998/99

Lösung zur Aufgabe 10:

a) *Per definitionem* ist eine von einem Element erzeugte Gruppe zyklisch. Die Gruppe $(\mathbb{Z},+)$ wird von der '1' erzeugt, d.h. jedes Element $z \in \mathbb{Z}$ kann durch z-malige Addition oder $1-z$-malige Subtraktion der Eins erzeugt werden.

Allerdings gibt es keine Zahl $m \in \mathbb{N}$, so daß $m \cdot 1 = 0$ gilt, d.h. die zyklische Gruppe $\mathbb{Z}$ ist unendlich.

Der Erzeuger 1 von $\mathbb{Z}$ ist nicht eindeutig – der andere ist (-1).

b) Trivialerweise sind $\{0\}$ und $\mathbb{Z}$ Untergruppen von $\mathbb{Z}$.

Sei nun U eine weitere Untergruppe von $\mathbb{Z}$. Dann gibt es eine kleinste Zahl $n \in \mathbb{N}$, die in U liegt, da aus $a \in U$ bereits $(-a) \in U$ folgt, d.h.

$$n := \min \underbrace{\mathbb{N} \cap U}_{\neq \emptyset}.$$

<u>Beh.:</u> $n\mathbb{Z} = U$

<u>Bew.:</u> "$\subset$": $n\mathbb{Z} = \{n \cdot z | z \in \mathbb{Z}\}$ ist die von n erzeugte Untergruppe von $\mathbb{Z}$. Wegen $n \in U$ gilt $n\mathbb{Z} \subset U$.
"$\supset$": Sei $u \in U$ fest aber beliebig. Dann teilen wir jetzt mit Rest, d.h. es gibt eine Zerlegung

$$u = a \cdot n + r \text{ mit } a \in \mathbb{Z}, 0 \leq r < n.$$

(Dies ist eigentlich eine Vorwegnahme des Euklidschen Algorithmuses, aber in der Schule kam das sicher schon dran.) Formen wir dies um

$$r = \underbrace{u}_{\in U} - \underbrace{a \cdot n}_{\in U} \in U$$

Da n minimal gewählt war, muß $r = 0$ gelten, d.h. $u = a \cdot n \in n\mathbb{Z}$. □

Auch die trivialen Untergruppen $\{0\} = 0 \cdot \mathbb{Z}$ und $\mathbb{Z} = 1 \cdot \mathbb{Z}$ lassen sich in dieser Form schreiben.

Fazit: Die Untergruppen von Z haben genau die Form $n \cdot \mathbb{Z}$ für alle $n \in \mathbb{N}$.

c) Sei $\emptyset \neq U \leq \mathbb{Z}$. Dann gibt es ein minimales $n \in \mathbb{N} \setminus \{0\}$ mit $U = n\mathbb{Z}$.

<u>Beh.:</u> Die Abbildung $\varphi : \mathbb{Z} \to U : z \mapsto n \cdot z$ ist ein Isomorphismus.

<u>Bew.:</u> (i) $\forall a, b \in \mathbb{Z} : \varphi(a+b) = n(a+b) = na + nb = \varphi(a) + \varphi(b) \Rightarrow$ Gruppenhomomorphismus.

(ii) surjektiv ist evident.

(iii) $\ker(\varphi) = \{z \in \mathbb{Z} | \varphi(z) = 0\} = \{z \in \mathbb{Z} | n \cdot z = 0\} = \{0\}$, da $n \neq 0$. Also ist φ injektiv.

Fazit: φ ist ein injektiver, surjektiver Gruppenhomomorphismus, d.h. ein Gruppenisomorphismus.

d) Allgemein heißt eine Untergruppe ***normal***, wenn $\forall g \in G : gUg^{-1} = U$ gilt. Ist G abelsch, so gilt: $g \in G \Rightarrow gUg^{-1} = gg^{-1}U = eU = U$. Natürlich ist $\mathbb{Z}$ abelsch …

Lösung zur Aufgabe 11:

a) Sei $|G| = p \geq 2$ prim. Dann liegt in G ein Element $a \neq e$. Insbesondere erzeugt dieses Element eine Untergruppe $U := \langle a \rangle \leq G$ von G mit $\langle e \rangle < \langle a \rangle \leq G$. Es gilt also $|U| \geq 2$ und nach dem Satz von Lagrange (1.8.6) gilt $|U|$ teilt $|G|$, d.h. $|U|$ teilt p. Da p prim und $|U| \geq 2$ gilt, muß $|U| = |G|$ gelten. Somit ist $\langle a \rangle = G$ und G wird von a erzeugt, ist also zyklisch.

b) Sei $m = |G|$ die Ordnung der zyklischen Gruppe $(G, \cdot)$ und a ein Erzeuger von G.
Die Abbildung

$$\varphi : (\mathbb{Z}, +) \to (G, \cdot) : z \mapsto a^z$$

ist ein Epimorphismus:
(i) $\varphi(n + z) = a^{n+z} = a^n a^z = \varphi(n)\varphi(z)$
(ii) Sei $b \in G$ beliebig. Dann gibt es die Darstellung $b = a^n$ für ein geeignetes n mit $0 \leq n < m$. Damit gilt $\varphi(n) = b$ und φ ist surjektiv.

Der Kern dieses Epimorphismus ist $\ker \varphi = \{z \in \mathbb{Z} | a^z = e\} = \{z \in \mathbb{Z} | z = 0 \mod m\} = m\mathbb{Z}$. Wenden wir darauf den Homomorphiesatz 1.9.5 für den surjektiven Fall an, so ergibt sich das nachfolgende kommutative Diagramm.

$$\begin{tikzcd} \mathbb{Z} \arrow[d, "s"'] \arrow[dr, "\varphi"] & \\ \mathbb{Z}/m\mathbb{Z} \arrow[r, "\cong"'] & G \end{tikzcd}$$

Exakt analog verfährt man bei einer zweiten Gruppe, nennen wir sie H, der Ordnung m. Dadurch ergibt sich die Isomorphismenkette $G \simeq \mathbb{Z}/m\mathbb{Z} \simeq H$ und somit sind G und H zueinander isomorph.

Lösung zur Aufgabe 12:

a) Der Nachweis ist eine Mischung aus Lagrange und Kombinatorik: Im Wesentlichen nutzt man die Tatsache, daß die Ordnung einer Untergruppe die Gruppenordnung teilt. Da $\mathfrak{S}_3$ die Ordnung 6 hat, kann eine Untergruppe nur von Ordnung $1, 2, 3$ oder 6 sein.

Zum Ergebnis: $\mathfrak{S}_3$ hat genau

1 Untergruppe der Ordnung 1: $U_0 = \{e\}$ (Mehr kann es nicht geben!)

3 Untergruppe der Ordnung 2: Gruppen der Ordnung 2 sind nach Aufgabe 11 a) zyklisch, werden also von einem Element der Ordnung 2 erzeugt. Dies sind in $\mathfrak{S}_3$ gerade die Transpositionen: $U_i = \langle \tau_i \rangle$ für $i \in \{1, 2, 3\}$.

1 Untergruppe der Ordnung 3: Gruppen der Ordnung 3 sind nach Aufgabe 11 a) zyklisch, werden also von einem Element der Ordnung 3 erzeugt. Dies sind in $\mathfrak{S}_3$ gerade σ_1 und σ_2. Beide erzeugen dieselbe Gruppe: U_4 (in der Vorlesung $\mathfrak{A}_3$ genannt).

1 Untergruppe der Ordnung 6: $U_5 = \mathfrak{S}_3$ selbst!

b) U_0, U_1, U_2, U_3: Trivialerweise sind alle Untergruppen der Ordnung 1 und 2 abelsch.

U_4: Diese Untergruppe wird von etwa $\sigma := \sigma_1$ erzeugt und besteht aus $\{\sigma^0 = e, \sigma, \sigma^2\}$. Es gilt $\sigma^i \circ \sigma^j = \sigma^{i+j} = \sigma^j \circ \sigma^j$ für beliebige $i, j \in \mathbb{N}$. Also ist U_4 abelsch.

U_5: Die einzige nichtabelsche Gruppe ist die $\mathfrak{S}_3$ selber wie man der Gruppentafel entnimmt, denn jene Tafel ist nicht diagonalsymmetrisch.

c) Die inneren Automorphismen sind (vgl 1.7.13)

$\varphi_{\tau_1} : \mathfrak{S}_3 \to \mathfrak{S}_3 : a \mapsto \tau_1 \cdot a \cdot \tau_1$ $\qquad$ $\varphi_e : \mathfrak{S}_3 \to \mathfrak{S}_3 : a \mapsto e \cdot a \cdot e = a$
$\varphi_{\tau_2} : \mathfrak{S}_3 \to \mathfrak{S}_3 : a \mapsto \tau_2 \cdot a \cdot \tau_2$ $\qquad$ $\varphi_{\sigma_1} : \mathfrak{S}_3 \to \mathfrak{S}_3 : a \mapsto \sigma_1 \cdot a \cdot \sigma_2,$
$\varphi_{\tau_3} : \mathfrak{S}_3 \to \mathfrak{S}_3 : a \mapsto \tau_3 \cdot a \cdot \tau_3$ $\qquad$ $\varphi_{\sigma_2} : \mathfrak{S}_3 \to \mathfrak{S}_3 : a \mapsto \sigma_2 \cdot a \cdot \sigma_1,$

d) Eine Untergruppe $U \leq G$ heißt ***Normalteiler*** von G, wenn U invariant unter allen inneren Automorphismen von G ist, d.h. wenn $\varphi(U) \subset U$ für alle φ gilt. (vgl. 1.7.13 und 1.7.16)

Die Untergruppen U_0 und U_5 sind trivialerweise normal, doch auch U_4 ist normal! Bei letzterer reicht es, $\varphi_{\tau_i}(U_4)$ nachzurechnen.

Eine Untergruppen V heißt ***konjugiert*** zu einer Untergruppe U, falls es einen inneren Automorphismus φ mit $V = \varphi(U)$ gibt.

U_1, U_2, U_3 sind zueinander konjugiert

$U_1 : \varphi_{\tau_2}(\tau_1) = \tau_2 \circ \tau_1 \circ \tau_2 = \tau_3 \Rightarrow \varphi_{\tau_2}(U_1) = U_3 \quad (= \varphi_{\tau_1}(U_2))$
$U_1 : \varphi_{\tau_3}(\tau_1) = \tau_3 \circ \tau_1 \circ \tau_3 = \tau_2 \Rightarrow \varphi_{\tau_3}(U_1) = U_2 \quad (= \varphi_{\tau_1}(U_3))$
$U_2 : \varphi_{\tau_3}(\tau_2) = \tau_3 \circ \tau_2 \circ \tau_3 = \tau_1 \Rightarrow \varphi_{\tau_3}(U_2) = U_1 \quad (= \varphi_{\tau_2}(U_3))$

und damit keine Normalteiler.

Lösung zur Aufgabe 13:

Die Maplelösungen sind auf der Maplehomepage der Linearen Algebra zu finden.

Lösung von Teilaufgabe **c):** Angenommen, es gebe nur endlich viele Primzahlen. Dann gibt es eine Primzahl p, die größer als alle anderen ist. Bilde das Produkt alle Primzahlen $q = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p_r$. Dann ist $m = q + 1$ sicher größer als alle Primzahlen, also insbesondere keine Primzahl. Es gibt also eine Zerlegung von m in Primfaktoren. Sei p ein solcher Primfaktor. Angenommen, es gilt $p \in \{2, 3, \cdots, p_r\}$. Dann gilt $p|q$ und $p|m$, also auch $p|(m - q)$, was $p|1$ bedeutet. Da p aber als Primzahl vorausgesetzt war, also insbesondere größer als eins ist, haben wir einen Widerspruch. Damit war die Annahme falsch und $p \notin \{2, 3, \cdots, p_r\}$.

Nach Voraussetzung war p ein Primfaktor, als prim. Somit ist p eine weitere Primzahl und die Annahme, daß es nur endlich viele Primzahlen gibt war falsch!

Fazit: Es gibt unendlich viele Primzahlen. Insbesondere können mit dem Sieb des Eratosthenes nicht alle gefunden werden.