Einführung in die Algebra
Blatt 1

Jendrik Stelzner

6. November 2013

Aufgabe 1.1.

Bemerkung. Sei G eine Gruppe und $H \subset G$ ein Untergruppe mit $(G : H) = 2$. Dann ist H ein Normalteiler in G.

Beweis der Bemerkung. Da $(G : H) = 2$ zerfällt in G in zwei Links- bzw. Rechtsnebenklassen, nämlich je H und H^c. Für alle $g \in H$ ist damit $gH = H = Hg$ und für alle $g \in H^c$ ist $gH = H^c = Hg$. $\square$

Es ist $S_3 = \{\text{id}, \sigma, \sigma^2, \tau_{12}, \tau_{13}, \tau_{23}\}$, wobei in Zykelschreibweise $\sigma = (1, 2, 3)$, $\sigma^2 = (3, 2, 1)$, $\tau_{12} = (1, 2)$, $\tau_{13} = (1, 3)$ und $\tau_{23} = (2, 3)$.
Da $\operatorname{ord} S_3 = 3! = 6$ folgt aus dem Satz von Lagrange, dass $\operatorname{ord} H \in \{1, 2, 3, 6\}$ für jede Untergruppe $H \subseteq G$. Neben den beiden trivialen Untergruppen $\{\text{id}\}$ und S_3 kann S_3 also nur zwei- oder dreielementige Untergruppen enthalten.
Offenbar sind $\langle\tau_{12}\rangle = \{\text{id}, \tau_{12}\}$, $\langle\tau_{13}\rangle = \{\text{id}, \tau_{13}\}$ und $\langle\tau_{23}\rangle = \{\text{id}, \tau_{23}\}$ Untergruppen der Ordnung 2 . Dies sind auch die einzigen Untergruppen dieser Ordnung: Ist $H = \{\text{id}, a\}$ eine Untergruppe mit $\operatorname{ord} H = 2$, so muss $a^2 = \text{id}$, also a selbstinvers sein. Die einzigen selbstinversen Elemente in S_3 sind aber e, τ_{12}, τ_{13} und τ_{23} (da $\sigma\sigma^2 = \sigma^2\sigma = \sigma^3 = \text{id}$).
Offenbar ist $\langle\sigma\rangle = \{\text{id}, \sigma, \sigma^2\}$ eine Untergruppe der Ordnung 3. Es ist auch die einzige Untergruppe dieser Ordnung: Ist $H = \{\text{id}, a, b\}$ eine Untergruppe mit $\operatorname{ord} H = 3$, so ist, wie aus der Vorlesung bekannt, H zyklisch und von a und b erzeugt. Insbesondere muss daher $\operatorname{ord} a = \operatorname{ord} b = \operatorname{ord} H = 3$. Die einzigen beiden Elemente in S_3 mit Ordnung 3 sind jedoch σ und σ^2.
Die Untergruppen von S_3 sind also $\{\text{id}\}$, $\langle\tau_{12}\rangle$, $\langle\tau_{13}\rangle$, $\langle\tau 23\rangle$, $\langle\sigma\rangle$ und S_3.
$\{\text{id}\}$ und S_3 sind trivialerweise Nullteiler in S_3. Aus der Bemerkung folgt, dass auch $\langle\sigma\rangle$ ein Normalteiler in S_3 ist, da $(S_3 : \langle\sigma\rangle) = 2$. $\langle\tau_{12}\rangle$, $\langle\tau_{13}\rangle$ und $\langle\tau_{23}\rangle$ sind keine Normalteiler in S_3, denn

$$\begin{aligned}
\tau_{23}\{\text{id}, \tau_{12}\} &= \{\tau_{23}, \sigma^2\} \neq \{\tau_{23}, \sigma\} = \{\text{id}, \tau_{12}\}\tau_{23}, \\
\tau_{12}\{\text{id}, \tau_{13}\} &= \{\tau_{12}, \sigma^2\} \neq \{\tau_{12}, \sigma\} = \{\text{id}, \tau_{13}\}\tau_{12} \text{ und} \\
\tau_{12}\{\text{id}, \tau_{23}\} &= \{\tau_{12}, \sigma\} \neq \{\tau_{12}, \sigma^2\} = \{\text{id}, \tau_{23}\}\tau_{12}.
\end{aligned}$$

Aufgabe 1.2.

Im Folgenden sei $Q := \{E, -E, I, -I, J, -J, K, -K\}$, wobei für die multiplikative Struktur $(Q, \cdot)$ (die sich als Gruppe herausstellen wird), ebenfalls Q geschrieben wird.

(i)

Wie die Multiplikationstabelle verrät, ist für $A, B \in \{E, I, J, K\}$ auch $AB \in Q$, folglich ist sogar für alle $A, B \in Q$ auch $AB \in Q$, Q ist also abgeschlossen bezüglich der Multiplikation.

$\cdot$	E	I	J	K
E	E	I	J	K
I	I	$-E$	$-K$	J
J	J	K	$-E$	$-I$
K	K	$-J$	I	$-E$

Die Assoziativität der Multiplikation vererbt sich direkt von $M(2 \times 2, \mathbb{C})$ auf Q. Da $E \in Q$ die Einheitsmatrix ist, gibt es in Q ein neutrales Element. Wie mit Aufgabenteil **(ii)** folgt, ist $E^{-1} = E, (-E)^{-1} = -E, I^{-1} = -I, J^{-1} = -J$ und $K^{-1} = -K$, also gibt es für alle $A \in Q$ ein $A^{-1} \in Q$. Damit ist Q eine Gruppe.

(ii)

Stupides Nachrechnen ergibt, dass

$$\begin{aligned} I^2 &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -E, \\ J^2 &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -E, \\ K^2 &= \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -E, \end{aligned}$$

sowie, entgegen der falschen Angabe in der Aufgabenstellung,

$$\begin{aligned} IJK &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \\ &= -K^2 = E, \text{ dafür aber} \\ KJI &= \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= I^2 = -E. \end{aligned}$$

(iii)

Da $\operatorname{ord} Q = 8$ ist nach dem Satz von Lagrange $\operatorname{ord} H \in \{1, 2, 4, 8\}$ für jede Untergruppe $H \subseteq Q$. Neben den trivialen Untergruppen $\{E\}$ und Q kann Q also nur Untergruppen der Ordnung 2 und 4 haben.
Offenbar ist $\{E, -E\}$ eine Untergruppe der Ordnung 2 von Q; dies ist auch die einzige Untergruppe dieser Ordung: Ist $H = \{E, A\} \subseteq Q$ eine Untergruppe mit $\operatorname{ord} H = 2$, so muss $A^2 = E$, also A selbstinvers sein. Aus **Aufgabenteil (ii)** folgt jedoch, dass E und $-E$ die einzige selbstinverse Elemente in Q sind, weshalb $A = -E$ gelten muss.
Für alle $A \in \{I, J, K\}$ ist $\{E, -E, A, -A\}$ offenbar eine Untergruppe der Ordnung 4 von Q. Dies sind auch die einzigen Untergruppen dieser Ordung: Ist $H \subset Q$ eine Untergruppe mit $\operatorname{ord} H = 4$, so gibt es ein $A \in H$ mit $A \notin \{E, -E\}$. Es muss

dann auch $E \in H$, $-E = A^2 \in H$, und $A^{-1} = -A \in H$. Also muss bereits $H = \{E, -E, A, -A\}$.
Die Untergruppen von Q sind also $\{E\}$, $\{E, -E\}$, $\{E, -E, I, -I\}$, $\{E, -E, J, -J\}$, $\{E, -E, K, -K\}$ und Q. Diese Untergruppen sind sogar alle normal in Q: Für $\{E\}$ und Q ist dies offensichtlich, für die Untergruppen der Ordnung 4, und damit Index 2, folgt es aus der Bemerkung in **Aufgabe 1.1**, und für $\{E, -E\}$ folgt es daraus, dass $A\{E, -E\} = \{A, -A\} = \{E, -E\}A$ für alle $A \in Q$, da E und $-E$ mit allen Matrizen in $M(2 \times 2, \mathbb{C})$ kommutieren.

Aufgabe 1.3.

(i)

Wie aus der Vorlesung bekannt genügt es zu zeigen, dass $gHg^{-1} = H$ für alle $g \in G$. Sei hierzu $g \in G$ beliebig aber fest. Wie aus Lineare Algebra I bekannt ist $\operatorname{inn}_g : G \to G, h \mapsto ghg^{-1}$ ein Gruppenautomorphismus von G. Daher ist insbesondere $\operatorname{ord} H = \operatorname{ord} \operatorname{inn}_g(H)$. Da aber H nach Annahme die einzige Untergruppe von G mit Ordung $\operatorname{ord} H$ ist, muss $gHg^{-1} = \operatorname{inn}_g(H) = H$. Aus der Beliebigkeit von g folgt damit die zu zeigende Aussage.

(ii)

Bemerkung. Seien G und G' Gruppen, G endlich, und $\varphi : G \to G'$ ein Gruppenhomomorphismus. Dann ist $\operatorname{ord} G = \operatorname{ord} \operatorname{Ker} \varphi \cdot \operatorname{ord} \operatorname{Im} \varphi$.

Beweis der Bemerkung. Wie aus der Vorlesung bekannt ist $G/\operatorname{Ker} \varphi \cong \operatorname{Im} \varphi$, also insbesondere $(G : \operatorname{Ker} \varphi) = \operatorname{ord} G/\operatorname{Ker} \varphi = \operatorname{ord} \operatorname{Im} \varphi$. Nach dem Satz von Lagrange gilt $\operatorname{ord} G = \operatorname{ord} \operatorname{Ker} \varphi \cdot (G : \operatorname{Ker} \varphi)$. Einsetzen ergibt, dass $\operatorname{ord} G = \operatorname{ord} \operatorname{Ker} \varphi \cdot \operatorname{ord} \operatorname{Im} \varphi$. □

Sei F eine Untergruppe von G mit $\operatorname{ord} F = \operatorname{ord} H$. Es gilt zu zeigen, dass $F = H$. Hierzu betrachte man die kanonische Abbildung $\pi : G \to G/H$. Da F eine Untergruppe von G ist, ist $\pi(F)$ eine Untergruppe von $\pi(G) = G/H$, insbesondere ist nach dem Satz von Lagrange daher $\operatorname{ord} \pi(F)$ ein Teiler von $\operatorname{ord} G/H = (G : H)$. Betrachtet man die Komposition

$$\varphi : F \hookrightarrow G \xrightarrow{\pi} G/H$$

so ist diese ein Homomorphismus mit $\operatorname{Ker} \varphi = F \cap H$ und $\operatorname{Im} \varphi = \pi(F)$, nach der Bemerkung also

$$\operatorname{ord} H = \operatorname{ord} F = \operatorname{ord} F \cap H \cdot \operatorname{ord} \pi(F).$$

Es ist also $\operatorname{ord} \pi(F)$ auch ein Teiler von $\operatorname{ord} H$. Da $\operatorname{ord} H$ und $(G : H)$ teilerfremd sind, muss $\operatorname{ord} \pi(F) = 1$, also $\pi(F) = \{1\}$ und daher $F \subseteq \operatorname{Ker} \pi = H$. Da $\operatorname{ord} F = \operatorname{ord} H$ gilt schon $F = H$.

Aufgabe 1.4.

(i)

Da, wie aus der Vorlesung bekannt, $\langle g \rangle$ für alle $g \in G$ eine Untergruppe von G ist, ist nach dem Satz von Lagrange $\operatorname{ord} g = \operatorname{ord} \langle g \rangle$ für alle $g \in G$ ein Teiler von $\operatorname{ord} G$, und

somit ebenfalls ungerade.
Da $aba = b \Leftrightarrow b = a^{-1}ba^{-1}$ ist für alle $n \in \mathbb{N}$

$$b^{2n+1} = a(baa^{-1}ba^{-1}a)^n ba = ab^{2n+1}a.$$

Da $\operatorname{ord} b$ ungerade ist, ist damit insbesondere

$$e = b^{\operatorname{ord} b} = ab^{\operatorname{ord} b}a = aea = a^2,$$

also a selbstinvers. Da damit $\langle a \rangle = \{e, a\}$, aber $\operatorname{ord} a$ ungerade ist, muss $a = e$.

(ii)

Da $c = abcba$ ist $cb = abcbab = ab \cdot cb \cdot ab$, nach Aufgabenteil **(i)** also $ab = e$.

Aufgabe 1.5.

Es ist

$$U \cong U/\{1\} = U/(U \cap N) \cong UN/N,$$

wobei die letzte Isomorphie aus dem ersten Isomorphiesatz folgt. Analog ergibt sich, dass $V \cong VN/N$. Um zu zeigen, dass $U \cong V$ genügt es daher zu zeigen, dass $UN = VN = G$. Dies ergibt sich durch Fallunterscheidung:
Ist $N = \{1\}$, so ist $N \subset U$ und $N \subset V$, wegen der Maximalitätseigenschaft von N daher $U = V = G$ und damit insbesondere $UN = VN = G$.
Ist $N \neq \{1\}$, so ist gibt es wegen $U \cap N = \{1\}$ ein $u \in U$ mit $u \notin N$. Es ist dann $uN \subseteq UN$ aber $uN \cap N = \emptyset$, da $aN \in N \Leftrightarrow a \in N$ für alle $a \in G$. Daher ist $UN \neq N$, also $N \subset UN$ und damit $UN = G$. Analog ergibt sich, dass auch $VN = G$.