

Algebra I

Musterlösung 2

Untergruppen, Nebenklassen, Normalteiler

13. Seien $m = 12$ und $n = 21$ und sei g ein Erzeuger der zyklischen Gruppe C_{mn} . Weiter sei $x := g^{120}$.

- (a) Zeige: $\text{ord}(x) = n$.
 (b) Finde mehrere Elemente $y, z \in C_{mn}$ mit

$$C_{mn} \neq \langle z \rangle, \quad C_{mn} = \langle y \rangle \quad \text{und} \quad z^m = y^m = x.$$

Lösung: Wir verwenden Aufgabe 6a). Diese besagt $\text{ord}(g^k) = \frac{\text{kgV}(k, mn)}{k}$.

(a) Aus Aufgabe 6a) wissen wir

$$\text{ord}(x) = \frac{\text{kgV}(120, 12 \cdot 21)}{120} = 21.$$

(b) Sei $y = g^k$ mit $0 \leq k < nm = 252$. Wieder wegen Aufgabe 6a) muss k genau die Bedingungen

- $\frac{\text{kgV}(k, mn)}{k} = mn$ und
- $mk \in \{120 + amn : a \in \mathbb{Z}\} \cap \{0, 1, 2, \dots, mn - 1\}$

erfüllen. Die erste Bedingung ist äquivalent zu $\text{ggT}(k, mn) = 1$, was wiederum äquivalent ist dazu, dass k durch keine der Primzahlen 2, 3 oder 7 teilbar ist. Die zweite Bedingung ist äquivalent zu $k \in \{10 + an : a \in \mathbb{Z}\} \cap \{0, 1, 2, \dots, mn - 1\}$. Daraus folgt, dass die möglichen k genau $k = 31, 73, 115, 157, 199, 241$ sind.

Sei nun $z = g^l$ mit $0 \leq l < nm$. Wieder wegen Aufgabe 6a) muss l genau die Bedingungen

- $\frac{\text{kgV}(l, mn)}{l} < mn$ und
- $ml \in \{120, 120 + mn, 120 + 2mn, \dots\}$

erfüllen. Die erste Bedingung ist äquivalent zu $\text{ggT}(l, mn) > 1$, was wiederum äquivalent ist dazu, dass l durch mindestens eine der Primzahlen 2, 3 oder 7 teilbar ist. Die zweite Bedingung ist wieder äquivalent zu $l \in \{10, 10 + n, 10 + 2n, \dots\}$. Da $n = 3 \cdot 7$ ist, aber 10 weder durch 3, noch durch 7 teilbar ist, kann $10 + an$ für keine ganze Zahl a durch 3 oder 7 teilbar sein. Deshalb muss $10 + an$ durch 2 teilbar sein, also ist a gerade. Daraus folgt, dass die möglichen l genau $l = 10, 52, 94, 136, 178, 220$ sind.

14. Sei G eine Gruppe und $H \leq G$. Definiere folgende Relation auf G :

$$g \sim g' \Leftrightarrow g'^{-1}g \in H.$$

(a) Zeige, dass diese Relation eine Äquivalenzrelation ist.

- (b) Zeige, dass Äquivalenzklassen genau die Linksnebenklassen von H sind.
- (c) Nimm an, die Vorschrift $[g] \circ [g'] := [gg']$ definiere eine wohldefinierte binäre Operation auf G/H . Zeige, dass H ein Normalteiler von G ist. (*Bemerkung:* In der Vorlesung wurde die Umkehrung dieser Aussage gezeigt.)

Lösung: (a) Wir müssen Reflexivität, Symmetrie und Transitivität nachprüfen. Sei $g \in G$. Dann gilt $g^{-1}g = e \in H$, also ist $g \sim g$ und \sim ist reflexiv. Seien nun $g, h \in G$ mit $g \sim h$. Das bedeutet $h^{-1}g \in H$. Dann ist auch $(h^{-1}g)^{-1} = g^{-1}h \in H$. Also folgt $h \sim g$ und die Relation ist symmetrisch. Seien nun $g, h, k \in G$ mit $g \sim h$ und $h \sim k$. Das bedeutet $h^{-1}g \in H$ und $k^{-1}h \in H$. Dann ist auch $(k^{-1}h)(h^{-1}g) = k^{-1}g \in H$. Also folgt $g \sim k$ und die Relation ist transitiv.

(b) Sei $g \in G$. Wir müssen zeigen, dass $[g] = gH$ gilt. Sei also $g' \in [g]$, das heisst $g' \sim g$. Dann existiert ein $h \in H$ mit $g^{-1}g' = h$. Das ist äquivalent zu $g' = gh$, also folgt $g' \in gH$. Wir haben somit bewiesen, dass $[g] \subseteq gH$ ist. Sei nun $k \in gH$. Dann existiert ein $h \in H$ mit $k = gh$. Daraus folgt $g^{-1}k = h \in H$ und somit ist $k \sim g$. Wir haben somit $[g] \supseteq gH$ bewiesen und insgesamt folgt $[g] = gH$.

(c) Wir zeigen die Kontraposition. Sei H kein Normalteiler von G . Dann existieren $g \in G$ und $h \in H$ mit $g^{-1}hg \notin H$. Das ist äquivalent zu $hg \notin gH$. Wegen $e \in H$ gilt $[e] = [h]$. Weiter sehen wir $[e][g] = [g]$ und $[h][g] = [hg]$. Wegen $hg \notin gH = [g]$ folgt daraus $[h][g] \neq [e][g]$. Also ist $[g] \circ [g'] := [gg']$ keine wohldefinierte Operation.

15. Sei G eine Gruppe und seien U, V nichtleere Teilmengen von G . Wir definieren

$$UV := \{uv \mid u \in U, v \in V\}$$

$$U^{-1} := \{u^{-1} \mid u \in U\}.$$

- (a) Zeige, dass die folgenden Aussagen äquivalent sind:
- U ist eine Untergruppe von G .
 - $UU \subseteq U$ und $U^{-1} \subseteq U$.
 - $UU^{-1} \subseteq U$.
- (b) Falls U und V Untergruppen von G sind, dann ist UV genau dann eine Untergruppe von G , wenn $UV = VU$ gilt.
- (c) Ist U endlich, dann ist U bereits dann eine Untergruppe, wenn $UU \subseteq U$ gilt.

Lösung: (a) Wir zeigen zuerst i. \Leftrightarrow ii. Die Bedingung $UU \subseteq U$ ist äquivalent zu $\forall u, u' \in U: uu' \in U$. Die Bedingung $U^{-1} \subseteq U$ ist äquivalent zu $\forall u \in U: u^{-1} \in U$. Da U laut Voraussetzung nicht leer ist, ist das nach der Vorlesung äquivalent dazu, dass U eine Untergruppe ist.

Wir zeigen nun i. \Leftrightarrow iii. Die Bedingung $UU^{-1} \subseteq U$ ist äquivalent zu $\forall u, u' \in U: uu'^{-1} \in U$. Da U laut Voraussetzung nicht leer ist, entspricht das genau der Definition einer Untergruppe aus der Vorlesung.

- (b) Wir beobachten zuerst, dass für eine Untergruppe $H \leq G$ gilt

$$H^{-1} = \{h^{-1} : h \in H\} = H,$$

da die Abbildung $H \rightarrow H, h \mapsto h^{-1}$ bijektiv ist.

Sei $UV \leq G$. Nach obiger Beobachtung folgt $(UV)^{-1} \subseteq UV$. Andererseits folgt aus $U^{-1} = U$ und $V^{-1} = V$ die Gleichheit

$$(UV)^{-1} = \{uv : u \in U, v \in V\}^{-1} = \{v^{-1}u^{-1} : u \in U, v \in V\} = V^{-1}U^{-1} = VU,$$

also gilt $UV = VU$.

Sei nun $UV = VU$. Widerum gilt

$$(UV)^{-1} = \{uv : u \in U, v \in V\}^{-1} = \{v^{-1}u^{-1} : u \in U, v \in V\} = V^{-1}U^{-1} = VU,$$

also folgt $(UV)^{-1} = UV$. Ausserdem beobachten wir, dass sich das Assoziativgesetz auf Teilmengen von G übertragen lässt. Seien nämlich $A, B, C \subseteq G$ alle nicht leer. Dann gilt

$$(AB)C = \{ab : a \in A, b \in B\}C = \{abc : a \in A, b \in B, c \in C\} = A(BC).$$

Also ist

$$\begin{aligned}(UV)(UV) &= \{uvu'v' : u, u' \in U, v, v' \in V\} \\ &= (U(VU))V = (U(UV))V = (UU)(VV) \subseteq UV.\end{aligned}$$

Weiters ist wegen $U \neq \emptyset \neq V$ auch $UV \neq \emptyset$. Daher ist UV nach Teil (a) eine Untergruppe von G .

(c) Wir müssen nachprüfen, dass $U^{-1} \subseteq U$ gilt. Sei $u \in U$. Falls $u = e$ ist, dann gilt trivialerweise auch $u^{-1} = e \in U$. Sei nun $u \neq e$. Es gilt $u^{|U|} = 1$ oder äquivalenterweise $u^{-1} = u^{|U|-1}$. Wir definieren induktiv $U^1 := U$ und

$$U^n := UU^{n-1} = \{u_1u_2 \dots u_n : u_1, \dots, u_n \in U\}.$$

Also ist $u^{-1} \in U^{|U|-1} = (UU)U^{|U|-3} \subseteq UU^{|U|-3} = U^{|U|-2} \subseteq \dots \subseteq U$. Das beweist $U^{-1} \subseteq U$. Da U nach Voraussetzung nicht leer ist, ist es somit eine Untergruppe von G .

16. Sei $\mathbb{U} := \{z \in \mathbb{C} : |z| = 1\} \subseteq \mathbb{C}$.

- Zeige, dass \mathbb{U} ein Normalteiler von (\mathbb{C}^*, \cdot) ist.
- Beschreibe die Menge \mathbb{C}^*/\mathbb{U} .
- Finde eine Gruppe, die isomorph zur Faktorgruppe \mathbb{C}^*/\mathbb{U} ist.

Lösung: (a) Offensichtlich gilt $1 \in \mathbb{U}$. Ausserdem gilt für alle $w, z \in \mathbb{C}^*$ die Gleichheit $|w^{-1}z| = |w|^{-1}|z|$. Wenn $w, z \in \mathbb{U}$ sind, gilt also auch $|w^{-1}z| = 1$ und somit $w^{-1}z \in \mathbb{U}$. Deshalb ist \mathbb{U} eine Untergruppe von \mathbb{C}^* . Da komplexe Multiplikation kommutativ ist, ist \mathbb{U} damit automatisch ein Normalteiler.

(b) Jedes $z \in \mathbb{C}^*$ können wir in Polarkoordinaten als $z = re^{i\varphi}$ mit $r \in \mathbb{R}^+, \varphi \in \mathbb{R}$ schreiben. Ausserdem ist $\mathbb{U} = \{re^{i\vartheta} : \vartheta \in \mathbb{R}\}$. Damit sehen wir

$$z\mathbb{U} = \{re^{i(\varphi+\vartheta)} : \vartheta \in \mathbb{R}\} = \{re^{i\varphi} : \vartheta \in \mathbb{R}\}.$$

Die Menge $z\mathbb{U}$ ist somit der Kreis mit Mittelpunkt 0 und Radius $|z|$.

(c) Wir behaupten, dass die Abbildung

$$f: (\mathbb{R}^+, \cdot) \rightarrow \mathbb{C}^*/\mathbb{U}, r \mapsto r\mathbb{U}$$

ein Isomorphismus ist. Wir zeigen zuerst Injektivität. Seien $r, r' \in \mathbb{R}^+$ mit $f(r) = f(r')$. Das bedeutet es gibt ein $z \in \mathbb{U}$ mit $rz = r'$, also $\frac{r'}{r} = z$. Es folgt, dass $z \in \mathbb{R}^+$ sein muss. Da z ausserdem Betrag 1 hat, folgt $z = 1$. Also ist $r = r'$ und f ist injektiv. Als nächstes zeigen wir Surjektivität. Sei $z\mathbb{U}$ eine Nebenklasse. Dann ist wieder $z = re^{i\varphi}$ und für dieses r gilt $f(r) = z\mathbb{U}$. Zuletzt müssen wir zeigen, dass für alle $r, r' \in \mathbb{R}^+$ die Gleichheit $f(rr') = f(r)f(r')$ gilt. Da \mathbb{U} ein Normalteiler ist, folgt $f(rr') = rr'\mathbb{U} = r\mathbb{U}r'\mathbb{U} = f(r)f(r')$. Somit haben wir gezeigt, dass f ein Gruppenisomorphismus ist.

17. Finde alle Untergruppen von D_4 sowie alle Inklusionen zwischen diesen. Gib an, in welchen Fällen es sich um einen Normalteiler handelt und bestimme die entsprechende Faktorgruppe.

Lösung: Die Diedergruppe D_4 mit 8 Elementen ist die Symmetriegruppe des Quadrates und besteht aus der Identität, drei Rotationen T, T^2, T^3 (um $\frac{\pi}{2}$, um π und um $\frac{3\pi}{2}$) und 4 Spiegelungen S, ST, ST^2, ST^3 .

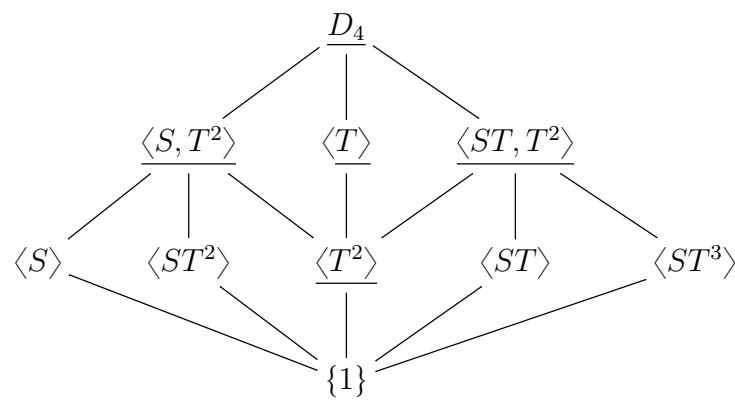
Sei H eine Untergruppe von D_4 . Wir unterscheiden vier Fälle:

- H ist die triviale Untergruppe $\{1\}$.
- H ist nicht trivial und besteht nur aus Rotationen. Dann gibt es zwei Möglichkeiten für H . Falls H nämlich T oder T^3 enthält, dann umfasst H auch alle anderen Rotationen (insbesondere die Identität!) und ist zyklisch von Ordnung 4, da sich alle Rotationen als Potenzen von T bzw. $T^3 = T^{-1}$ schreiben lassen. Andernfalls besteht H aus der Identität und der Rotation T^2 um π und ist zyklisch von Ordnung 2.
- H besteht aus der Identität und einer Spiegelung. Da $S'^2 = 1$ für jede Spiegelung S' gilt, bildet jede Spiegelung mit der Identität zusammen eine Untergruppe von D_4 . Somit gibt es in diesem Fall vier Möglichkeiten für H (alle zyklisch von Ordnung 2).
- H enthält die Identität, eine Spiegelung S' und mindestens ein weiteres Element. Dieses ist entweder eine Spiegelung ungleich S' oder eine nicht-triviale Rotation. Falls es eine Spiegelung ist, ist seine Verknüpfung mit S' eine nicht-triviale Rotation. Deshalb enthält H sicher eine nicht-triviale Rotation R .

Falls $R = T$ oder $R = T^3$ ist, umfasst H wie im zweiten Fall auch alle anderen Rotationen und auch alle 4 Spiegelungen, da $S', S'R, S'R^2, S'R^3$ paarweise verschiedene Spiegelungen sind. In diesem Fall ist also $H = D_4$.

Andernfalls ist $R = T^2$ eine Rotation um π und H enthält keine weiteren nicht-trivialen Rotationen. Dann ist $H = \{1, S', T^2, S'T^2\}$ eine Diedergruppe mit 4 Elementen, denn H enthält die beiden Spiegelungen $S'T$ und $S'T^3$ nicht, da T und T^3 keine Elemente von H sind. Es gibt genau zwei solche Möglichkeiten für H , denn $\{S', S'T^2\} = \{S, ST^2\}$ oder $\{S', S'T^2\} = \{ST, ST^3\}$. Die Untergruppe H enthält also entweder die Spiegelungen an den Diagonalen des Quadrates oder diejenigen an den zu den Quadratseiten parallelen Symmetrieachsen.

Insgesamt hat H somit 10 Untergruppen mit folgenden Inklusionen (bei den unterstrichenen Untergruppen handelt es sich um Normalteiler, siehe unten):



Wir überprüfen nun für je zwei Untergruppen H, H' von D_4 mit $H' \subseteq H$, ob $H' \triangleleft H$ gilt. Da jede Gruppe der Ordnung 1, 2 oder 4 abelsch ist und jede Untergruppe einer abelschen Gruppe normal ist, ist $H' \triangleleft H$ immer erfüllt, wenn $H \neq D_4$.

Offensichtlich sind $\{1\}$ und D_4 Normalteiler von D_4 . Durch explizites Einsetzen stellen wir fest, dass alle Untergruppen mit 4 Elementen, also $\langle T \rangle$, $\langle S, T^2 \rangle$ und $\langle ST, T^2 \rangle$, Normalteiler von D_4 sind (später wird dies aus einer allgemeineren Aussage über den Index folgen). Die Untergruppen $\langle S \rangle$, $\langle ST \rangle$, $\langle ST^2 \rangle$ und $\langle ST^3 \rangle$ sind keine Normalteiler von D_4 , denn sie sind nicht abgeschlossen unter Konjugation mit dem Element T . Schliesslich können wir wieder durch explizites Einsetzen überprüfen, dass $\langle T^2 \rangle$ ein Normalteiler von D_4 ist.

In allen Fällen, in denen $[H : H'] = 2$ gilt, ist die Faktorgruppe isomorph zu C_2 , da dies bis auf Isomorphie die einzige Gruppe der Ordnung 2 ist. Die einzigen übrigen Fälle sind $D_4/\langle T^2 \rangle$ und $\langle T \rangle/\{e\}$. Letzteres ist isomorph zu $\langle T \rangle \cong C_4$. Die Gruppe $D_4/\langle T^2 \rangle$ ist isomorph zu C_4 oder $C_2 \times C_2$. Da sowohl die Nebenklasse von T als auch die Nebenklasse von S Ordnung 2 haben, aber verschieden sind, hat $D_4/\langle T^2 \rangle$ mindestens zwei Elemente der Ordnung 2. Somit ist sie isomorph zu $C_2 \times C_2$.

Bemerkung: Es gilt zwar $\langle S \rangle \triangleleft \langle S, T^2 \rangle$ und $\langle S, T^2 \rangle \triangleleft D_4$, aber nicht $\langle S \rangle \triangleleft D_4$. Wir haben also an einem Gegenbeispiel gezeigt, dass für Untergruppen M, N, K einer Gruppe G

$$(M \triangleleft N \wedge N \triangleleft K) \not\Rightarrow M \triangleleft K.$$

18. Sei T die Symmetriegruppe des regulären Tetraeders.

- (a) Bestimme $|T|$.
- (b) Zeige, dass T nicht abelsch ist.
- (c) Bestimme alle Untergruppen von T .
- (d) Welche Untergruppen von T sind nichttriviale Normalteiler?

Lösung: (a) Ein Tetraeder hat vier Seitenflächen. Ein Element der Symmetriegruppe kann die Grundfläche F so auf jede der vier Seitenflächen abbilden, dass eine beliebige Ecke von F auf eine bestimmte der drei Ecken der Seitenfläche abgebildet wird. Dadurch ist die Bewegung des Tetraeders eindeutig bestimmt. Es gibt also insgesamt $4 \cdot 3 = 12$ Möglichkeiten, somit ist $|T| = 12$.

(b) Bezeichne mit A, B, C, D die Ecken des Tetraeders. Betrachte das nichttriviale Element $R_D \in T$ mit $\sigma(D) = D$, das A, B, C zyklisch vertauscht und das Element $R_A \in T$, das A fest lässt und B, C, D zyklisch vertauscht. Dann gilt $R_D \circ R_A(A) = B$, aber $R_A \circ R_D(A) = C$.

(c) Das Element R_A erzeugt die Untergruppe von T , die die Ecke A fest lassen. Diese ist isomorph zu C_3 , hat also keine weiteren Untergruppen mehr. Bezeichne analog R_B das Element, das C, D, A zyklisch vertauscht und R_C das Element, das D, A, B zyklisch vertauscht. Genauso erzeugen R_B, R_C und R_D Untergruppen isomorph zu C_3 , die eine Ecke fest lassen.

Sei nun $\sigma \in T$ mit $\sigma(A) = B$. Falls $\sigma(B) = A$ gilt, dann vertauscht σ auch B und C . Wir bezeichnen dieses Element σ mit $S_{AB} = S_{CD}$. Es erzeugt eine Untergruppe der Ordnung 2. Analog bekommen wir Elemente $S_{AC} = S_{BD}$ und S_{AD} , die Untergruppen der Ordnung 2 erzeugen.

Falls $\sigma(B) = C$ gilt, lässt σ das Dreieck A, B, C und daher die Ecke D invariant. Diesen Fall haben wir schon betrachtet.

Da $|T| = 12$ ist, gilt

$$T = \{e, R_A, R_A^2, R_B, R_B^2, R_C, R_C^2, R_D, R_D^2, S_{AB}, S_{AC}, S_{AD}\}.$$

Das Produkt von zwei verschiedenen Elementen aus der Menge $\{S_{AB}, S_{AC}, S_{AD}\}$ ergibt jeweils das dritte. Also ist $\{e, S_{AB}, S_{AC}, S_{AD}\} = \langle S_{AB}, S_{AC} \rangle \cong C_2 \times C_2$.

Wir wollen zeigen, dass die Liste $\{e\}, \langle R_A \rangle, \langle R_B \rangle, \langle R_C \rangle, \langle R_D \rangle, \langle S_{AB} \rangle, \langle S_{AC} \rangle, \langle S_{AD} \rangle, \langle S_{AB}, S_{AC} \rangle$ und T bereits alle Untergruppen umfasst.

Eine Untergruppe von T hat Ordnung 1, 2, 3, 4, 6 oder 12. Die Liste enthält sicher alle Untergruppen der Ordnungen 1 und 12, da nur die triviale Gruppe und die ganze Gruppe diese Ordnungen haben können. Weiter enthält die Liste offenbar alle zyklischen Untergruppen von T und deshalb sind bereits alle Untergruppen der Ordnung 2 und 3 vertreten. Eine Untergruppe der Ordnung 4 darf kein Element der Ordnung 3 enthalten, da die Ordnung jedes Elements die Gruppenordnung teilt. Es gibt in T aber nur vier Elemente, die nicht Ordnung 3 haben. Deshalb ist $\langle S_{AB}, S_{AC} \rangle$ die einzige Untergruppe der Ordnung 4.

Eine Untergruppe H der Ordnung 6 muss isomorph zu C_6 oder D_3 sein, da dies bis auf Isomorphie die einzigen Gruppen der Ordnung 6 sind. Ausserdem muss sie nach dem Satz von Lagrange Index 2 haben und deshalb ein Normalteiler sein. Da die Liste zwar alle zyklischen Untergruppen von T enthält, aber keine, die isomorph zu C_6 ist, muss $H \cong D_3$ gelten. Dann enthält H ein Element der Ordnung 2 und ein Element der Ordnung 3. Wegen Symmetrie können wir ohne Beschränkung der Allgemeinheit annehmen, dass $R_A \in H$ liegt, also $\langle R_A \rangle \leq H$. Es gilt $R_B^{-1} \circ R_A \circ R_B(D) = D$, also ist $R_B^{-1} \circ R_A \circ R_B \in \{R_D, R_D^2\}$. Wegen Normalität und wegen $R_D^2 = R_D^{-1}$ folgt $R_D \in H$, analog liegen ebenso $R_B, R_C \in H$ und natürlich auch deren Quadrate. Somit hat H bereits acht Elemente der Ordnung 3, was bei $|H| = 6$ nicht sein kann. Deshalb kann T keine Untergruppe der Ordnung 6 haben und obige Liste ist vollständig.

Wegen $R_B^{-1} \circ R_A \circ R_B \in \{R_D, R_D^{-1}\}$ sind die Gruppen $\langle R_A \rangle$ und $\langle R_D \rangle$ zueinander konjugiert. Analog sind diese Gruppen auch konjugiert zu $\langle R_B \rangle$ und $\langle R_C \rangle$. Insbesondere ist keine dieser Untergruppen normal in T .

Eine zu $\langle S_{AB}, S_{AC} \rangle$ konjugierte Untergruppe von T muss ebenfalls Ordnung 4 haben. Da $\langle S_{AB}, S_{AC} \rangle$ die einzige solche Untergruppe von T ist, ist sie somit normal.

Zuletzt rechnen wir $R_A^{-1} \circ S_{AB} \circ R_A(A) = D$ und $R_A^{-1} \circ S_{AB} \circ R_A(D) = A$, also gilt $R_A^{-1} \circ S_{AB} \circ R_A = S_{AD}$. Deshalb sind $\langle S_{AB} \rangle$ und $\langle S_{AD} \rangle$ zueinander konjugiert. Analog sehen wir, dass alle Untergruppen der Ordnung 2 zueinander konjugiert sind.