# Gruppentheorie I

Nils Gerding

WS 2008 / 2009

Proseminar Lineare Algebra - O. Bogopolski
Technische Universität Dortmund

# 1 Gruppen - Einführung

## 1.1 Definition: Die Gruppenaxiome

Eine Menge G heißt Gruppe, wenn es eine binäre Verknüpfung $\cdot : G \times G \to G$ gibt, so dass folgende Axiome gelten:

1. $(ab)c = a(bc)$
2. $\exists\, e \in G :\ ea = ae = e \quad \forall\, a \in G$
3. $\forall\, a \in G \ \ \exists\, b \in G :\ ab = ba = e.$

Eine Gruppe heißt kommunitiv oder abelsch, wenn gilt: $ab = ba\ \forall\, a, b \in G$.

Im weiteren Verlauf sein $G$ eine Gruppe mit der inneren Verknüpfung $\cdot$.

## 1.2 Definition: Potenzgesetze

Sei $a \in G$. Das Element $a^n,\ n \in \mathbb{Z}$, sei wie folgt definiert:

- Wenn $n > 0$, dann ist $a^n := \underbrace{a \cdot a \cdot ... \cdot a}_{n}$,
- wenn $n < 0$, dann ist $a^n := (a^{-1})^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdot ... \cdot a^{-1}}_{|n|}$,
- wenn $n = 0$, dann ist $a^0 := e$.

## 1.3 Satz

Sind $a, b \in G$ invertierbar, so ist auch $ab$ invertierbar und es gilt: $(ab)^{-1} = b^{-1}a^{-1}$.

*Beweis:* $ab(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})ab$ ■

Ein Beispiel aus dem Alltag zur Verdeutlichung: Sei $a$ eine Socke und $b$ ein Schuh, dann ergibt es Sinn, morgens erst die Socke und dann den Schuh anzuziehen (also $ab$). Will man dieses Vorgehen aber abends rückgängig machen (invertieren), dann sollte man sich zuerst des Schuhs und dann der Socke entledigen (also $b^{-1}a^{-1}$).

## 1.4 Definition: Untergruppe

Eine nichtleere Teilmenge $G_1 \subseteq G$ heißt Untergruppe (in Zeichen: $G_1 \leqslant G$), wenn

1. $\forall\, g_1, g_2 \in G_1$ gilt: $g_1 g_2 \in G_1$,
2. $\forall\, g \in G_1$ gilt: $g^{-1} \in G_1$.

$G_1$ ist selbst wieder eine Gruppe.

## 1.5 Beispiele

### 1.5.1 Symmetrien eines Quadrats

Wir betrachten die Gruppe von Symmetrien eines Quadrats. Sie besteht aus:

$Sym(\square) = \{r_0, r_{90}, r_{180}, r_{270}, s_1, s_2, s_3, s_4\}$,

wobei $r_i$ die Rotation um den jeweiligen Winkel $i$ und $r_j$ die Spiegelung an der entsprechenden Achse $j$ meint. Somit ist $|Sym(\square)| = 8$.

$Sym(\square)$ ist offensichtlich nicht kommunitiv, da z. B. $r_{90}s_2 \neq s_2r_{90}$, für eine Seitenhalbierende $s_2$.

Weiter sollen nun alle Untergruppen von $Sym(\square)$ bestimmt werden. Dazu stellt man zunächst das neutrale Element fest, da dies in jeder Untergruppe vorhanden sein muss, und sucht sich des Weiteren Elemente, die durch Verknüpfung mit anderen sich in dieser Untergruppe befindenden Elementen weiterhin in der Untergruppe liegen. So ergeben sich folgende Untergruppen:

$G_0 = Sym(\square)$
$G_1 = \{r_0\}$
$G_2 = \{r_0, r_{180}\}$
$G_3 = \{r_0, s_1\}$
$G_4 = \{r_0, s_2\}$
$G_5 = \{r_0, s_3\}$
$G_6 = \{r_0, s_4\}$
$G_7 = \{r_0, s_2, s_4, r_{180}\}$
$G_8 = \{r_0, r_{90}, r_{180}, r_{270}\}$

Dass dies alle Untergruppen von $Sym(\square)$ sind, ergibt sich schnell, wenn man versucht, andere Kombinationen der Elemente zu bilden sofort zu einer der genannten Untergruppen führt.

### 1.5.2 $n \times n$-Matrizen

Wir betrachten die Menge $GL_n(\mathbb{Z}) := \{\square_{n\times n} \in \mathbb{Z}^{n\times n} : \ det(\square_{n\times n}) = \pm 1\}$, auf der die Matrizenmultiplikation als binäre Verknüpfung definiert ist. Dass $GL_n(\mathbb{Z})$ eine Gruppe ist, lässt sich z. T. leicht überprüfen:

1. $(AB)C = A(BC)$
2. $\exists \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} := E$

3. $\forall\ A \in GL_n(\mathbb{Z})\ \ \exists\ A^{-1} \in GL_n(\mathbb{Z}) :\quad AA^{-1} = E$
   mit $A^{-1} = \frac{1}{detA} A_{adj}$.

   Zeige, dass $det(A^{-1}) = \pm 1$ und somit $A^{-1} \in GL_n(\mathbb{Z})$:
   $1 = det(E) = det(AA^{-1}) = \underbrace{det(A)}_{\pm 1} det(A^{-1}) \quad \Rightarrow \quad det(A^{-1}) = \pm 1$ ■

Offensichtlich ist z.B. $SL_n(\mathbb{Z}) := \{\square \in GL_n(\mathbb{Z}) \mid det(\square) = 1\}$ eine Untergruppe von $GL_n(\mathbb{Z})$. Weiterhin ist auch leicht nachvollziehbar, dass die Untermenge

$$D_O(\mathbb{Z}) = \begin{pmatrix} 1 & * & \cdots & * \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

aller Oberen-Dreiecksmatrizen eine Untergruppe von $SL_n(\mathbb{Z})$ (und natürlich auch von $GL_n(\mathbb{Z})$) ist, wenn man berücksichtigt, dass 1) und 2) gelten und die für 3) benötigte inverse Matrix sich mit $A^{-1} = \frac{1}{detA} A_{adj}$ berechnen lässt, wobei sich am Beispiel zeigt, dass sie wieder in $D_O(\mathbb{Z})$ liegt:

$$\begin{pmatrix} 1 & 2 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad \frac{1}{1} \begin{pmatrix} 1 & -2 & 2 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix} = A^{-1} \in D_O(\mathbb{Z})$$

### 1.5.3 Permutationsgruppen

Sei $\Sigma(S) = \{f : S \to S,\ f\ bijektiv\}$ die Permutationsgruppe von $S$, mit $S := \{1, 2, 3, 4, 5\}$. Es ist offensichtlich, dass $\Sigma(S)$ die Gruppenaxiome erfüllt: es gilt Assoziativität, es existier ein Neutralelement $f_e = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{smallmatrix}\right)$ und das Inverse lässt sich durch einfaches Vertauschen der Zeilen bestimmen, z.B. $f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{smallmatrix}\right) \Rightarrow f^{-1} = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{smallmatrix}\right)$.

## 1.6 Definition

Sei $H \leqslant G$ und $g \in G$. Dann heißt die durch Komplexmultiplikation entstehende Menge $gH$ bzw. $Hg$ Links- bzw. Rechtsnebenklasse von $H$.

## 1.7 Beispiel

Sei $G := \Sigma(\{1, 2, 3\}) = \{id, (12), (13), (23), (123), (132)\}$ und $H := \{(id), (12)\}$ eine Untergruppe von $G$.

Bildung der Nebenklassen von $H$ für $g = (13)$:

- linke Nebenklasse:
  $(13)H = \{(13), (12)(13)\} = \{(13), (123)\}$
- rechte Nebenklasse:
  $H(13) = \{(13), (13)(12)\} = \{(13), (132)\}$

*Bemerkung:*
Offensichtlich müssen Rechts- und Linksnebenklasse mit einem festem $g \in G$ nicht gleich sein.

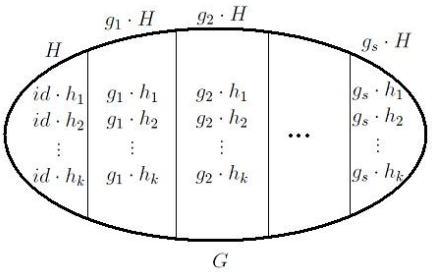
### 1.8 Satz von Lagrange

Sei $G$ eine endliche Gruppe und $H \leqslant G$. Dann gilt:

$|G| = |H| \cdot |G : H|$,

mit $|G : H|$ als der Anzahl von Nebenklassen, genannt Index von $H$ in $G$.

*Beweis*
Jede Nebenklasse von $H$ enthält genau so viele Elemente wie $H$ selbst, was leicht in folgendem Schaubild ersichtlich ist:




Dass die Vereinigung aller Nebenklassen tatsächlich eine disjungte Zerlegung von $G$ ist, folgt aus der Annahme, dass für ein $g_2 h_j \notin g_1 H$ gelte $g_1 h_i = g_2 h_j$. Dann folgt $g_2 = g_1 h_i h_j^{-1} \in g_1 H$ und somit ein Widerspruch.

Mit der Definition des Index ergibt sich die Behauptung ■

## 2 Zyklische Gruppen

### 2.1 Definition

Eine Gruppe $G$ heißt zyklisch, wenn $\exists\, g \in G : \quad G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

## 2.2 Satz

Wenn $G$ eine zyklische Gruppe ist, dann ist $G \cong \mathbb{Z}$ für $|G| = \infty$ bzw. $G \cong Z_n,\ n \in \{1, 2, 3, ..., n-1\}$ für eine endliche Gruppe.

*Beweis*
Behauptung folgt, wenn man betrachtet, dass $\mathbb{Z}$ bzw. $\mathbb{Z}_n$ durch 1 erzeugt wird. ■

## 2.3 Bemerkung

Betrachte $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.
Dann ist $\overline{2} + \overline{3} = \overline{1}$, aber $\overline{2} \cdot \overline{3} = \overline{2}$. Daraus ergibt sich, dass $(\mathbb{Z}, \cdot)$ keine Gruppe ist, jedoch $(\mathbb{Z}, +)$ durchaus.

## 2.4 Satz

$\Sigma_n$, die Gruppe aller Permutationen, wird erzeugt von $(12), (13), ..., (1n)$.

*Beweis*
Die Elemente von $\Sigma_n$ bestehen entweder aus mehreren Zyklen, die unterschiedlich lang sein können, aus einem Zyklus der Länge $n > 2$ oder aus einem Zweierzyklus. Ein Zweierzyklus lässt sich ausdrücken durch $(ij) = (1i)(1j)(1i)$. Da sich ein Zyklus der Länge $n > 2$ schreiben lässt als $(i_1 i_2 ... i_n) = (i_1 i_2)(i_2 i_3)...(i_{n-1} i_n)$, kann man auch diesen durch Elementarzyklen ausdrücken. Aus diesen beiden Arten von Elementen aus $\Sigma_n$ setzt sich die fehlende Art von Elementen $(i_1 i_2 ... i_k)(j_1 j_2 ... j_l)...(t_1 t_2 ... t_r) \in \Sigma_n$ zusammen, die sich folglich auch durch Elementarzyklen ausdrücken lässt. ■

## 2.5 Satz und Definition

Die Gruppe $Alt_n = \{\sigma \in \Sigma_n \mid sign\, \sigma = +1\}$ heißt alternierende Gruppe vom Grad $n$. Sie ist eine Untergruppe von $Sym_n$ und wird erzeugt von $(123), (124), ..., (12n)$. *(ohne Beweis)*

Außerdem gilt: $|\Sigma_n : Alt_n| = 2$, da $\underbrace{\Sigma_n = Alt_n}_{sign=+1} \cup \underbrace{(12)Alt_n}_{sign=-1}$

## 2.6 Satz von Cayley

Jede Gruppe ist isomorph zu einer Untergruppe der symmetrischen Gruppe.

*Beweis*
Wir zeigen, dass es eine Einbettung $\Pi: G \to \Sigma(G)$ gibt. Definieren wir $\Pi$ wie folgt: $\Pi(g) = \left(\begin{smallmatrix} g_1 & g_2 & \cdots \\ gg_1 & gg_2 & \cdots \end{smallmatrix}\right)$. Es ist klar, dass $\Pi(g)$ in $\Sigma(G)$ liegt. Man kann leicht nachprüfen, dass $\Pi(g_1 g_2) = \Pi(g_1) \cdot \Pi(g_2)$ gilt. Außerdem ist $\Pi$ injektiv, womit die Behauptung folgt. ■

# 3 Orbits

## 3.1 Definition

Sei $M$ eine Menge und $G$ eine Gruppe. Wir sagen $G$ operiert von rechts auf $M$ bzw. von links auf $M$ (in Zeichen: $M \circlearrowleft G$), wenn $\forall\ g \in G, \quad \forall\ m \in M$ ein Element $mg \in M$ definiert ist und folgende zwei Axiome gelten:

1. $(mg_1)g_2 = m(g_1g_2)$ bzw. $g_1(g_2m) = (g_1g_2)m$
2. $m \cdot 1 = m$ bzw. $1 \cdot m = m$.

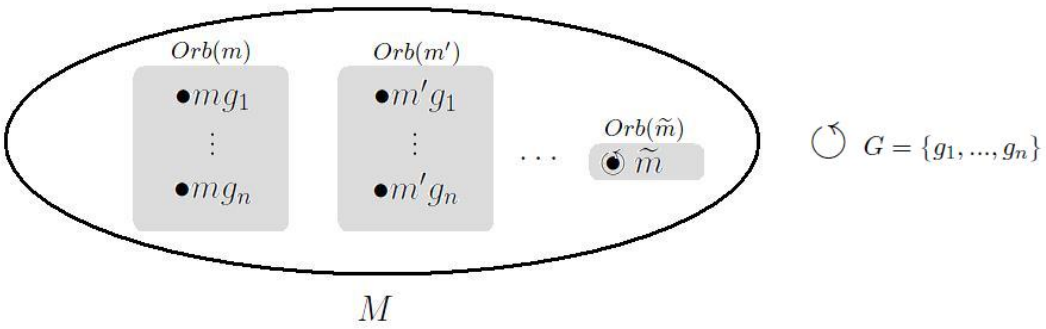
## 3.2 Beispiel: Abbildungsmatrizen

Sei $M := \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \mid \alpha_i \in \mathbb{R} \right\}$ und $G := GL_n(\mathbb{Z}) = \left\{ \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix} \mid c_{ij} \in \mathbb{R} \right\}$.

$M \circlearrowleft G$ lässt sich nun beispielhaft darstellen als: $\underbrace{\begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix}}_{\in G} \underbrace{\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}}_{\in M} = \underbrace{\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}}_{\in M}$

## 3.3 Definition

Die Menge $Orb(m) = \{mg \mid g \in G\}$, für $m \in M$, heißt der Orbit von $m$.




## 3.4 Satz und Definition

Sei $m \in M$. Die Menge $Stab(m) = \{g \in G \mid mg = m\}$ ist eine Untergruppe von $G$. Diese Menge nennt man auch Stabilisator von $m$.

*Beweis*

1. Abgeschlossen bzgl. $\cdot$ : Sind $g_1, g_2 \in Stab(m)$ : $m(g_1 g_2) = (mg_1)g_2 = mg_2 = m \Rightarrow g_1 g_2 \in Stab(m)$.
2. Existens eines Inversen: Sei $g \in Stab(m)$ : $mg = m \overset{\cdot g^{-1}}{\rightarrow} m(gg^{-1}) = mg^{-1} \Leftrightarrow m = mg^{-1}$

■

## 3.5 Satz

Sei $Orb(m)$ ein Orbit von $m \in G$ und $Stab(m)$ der Stabilisator von $m$. Dann gilt: $|Orb(m)| = |G : Stab(m)|$, mit $|G : Stab(m)|$ als Index von $Stab(m)$ in $G$.

*Beweis*

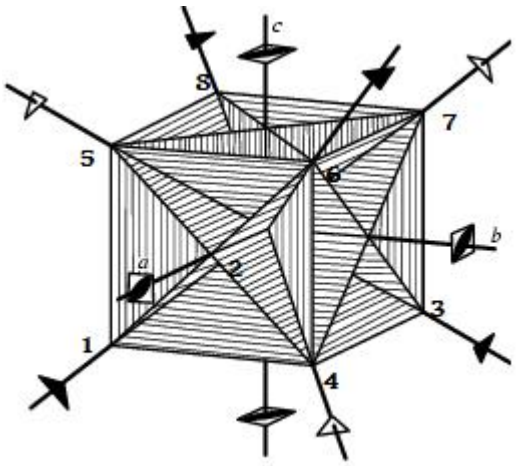
$|G : Stab(m)|$ ist laut der Definition die Anzahl von Nebenklassen. Betrachte nun

$$\eta : \underbrace{\{mg \mid g \in G\}}_{Orb(m)} \rightarrow \underbrace{\{Stab(m) \cdot g \mid g \in G\}}_{\text{Menge von rechten Nebenklassen von } Stab(m) \text{ in } G}, \; mg \longmapsto Stab(m) \cdot g.$$

Ist $\eta$ nun bijektiv, ist die Behauptung erfüllt.

1. *Injektivität:* Zu zeigen ist $mg_1 \neq mg_2 \Rightarrow Stab(m)g_1 \neq Stab(m)g_2$. Nehmen wir an: $Stab(m)g_1 = Stab(m)g_2$. Dann ist $g_1 g_2^{-1} \in Stab(m) \Rightarrow m(g_1 g_2^{-1}) = m \Rightarrow mg_1 = mg_2 \Rightarrow$ Behauptung
2. *Surjektivität:* Da $\eta(mg_1) = Stab(m)g_1$ laut Definition ist die Surjektivität offensichtlich ■

## 3.6 Beispiel: Symmetrieachsen eines Würfels




[1]

Sei $M := \{1, 2, ..., 8\}$ die Menge der Eckpunkte eines Würfels und $G$ die Gruppe von Rotationen im $\mathbb{R}^3$, die den Würfel in sich selbst abbilden. Für den Stabilisator gilt $Stab(m) = \left\{id, q_i^{120}, q_i^{240}\right\}$, wobei $q_i^{120}, q_i^{240}$ die Drehung um den jeweiligen Winkel um die Achse durch $m$ und den gegenüberliegenden Punkt, also z. B. 6 und 2, ist. Insbesondere ist $|Stab(6)| = 3$.

Für z.B. den Punkt 6 gilt $Orb(6) = \{1, 2, ..., 8\}$, da durch die Elemente von $G$ der Punkt 6 auf alle Punkte abgebildet werden kann. Somit ist $|Orb(6)| = 8$. Nach obigen Satz muss also auch $|G : Stab(6)| = 8$ sein. Mit dem *Satz von Lagrange* folgt weiterhin: $|G| = |Stab(6)| \cdot |G : Stab(6)| = 3 \cdot 8 = 24$.

Dies bestätigt sich durch geometrische Überlegungen zum Bestimmen der Elemente von $G$ zu

$$G := \left\{ \begin{array}{c} id, r'_{90}, r'_{180}, r'_{270}, r''_{90}, r''_{180}, r''_{270}, r'''_{90}, r'''_{180}, r'''_{270}, \\ l_1, l_2, l_3, l_4, l_5, l_6, \\ q_1^{120}, q_2^{120}, q_3^{120}, q_4^{120}, q_1^{240}, q_2^{240}, q_3^{240}, q_3^{240} \end{array} \right\},$$

wobei $r_i^{(j)}$ die Rotationen um die Achsen durch die gegenüberliegenden Seitenmitten, $l_i$ die um die Achse durch die gegenüberliegenden Kantenmitten und $q_i^j$ die um die Achse durch die gegenüberliegenden Eckpunkte sind.

## 3.7 Satz von Burnside

Sei $Orb(G) :=$ die Menge aller Orbits von $G$ auf $M$, $Stab(m) := \{g \in G \mid mg = m\} \subseteq G$, $Fix(g) := \{m \in M \mid mg = m\} \subseteq M$ und $M \circlearrowleft G$. Dann gilt:

[1] Quelle: http://tbookdtd.sourceforge.net/datb-no-mathml/f43m-web.png, 09.03.09. Enthält Anpassungen.

$|Orb(G)| = \frac{1}{|G|} \cdot \sum_{g \in G} |Fix(g)|$.

*Beweis*

Wir betrachten die Kapazität der folgenden Menge auf zwei unterschidlichen Wegen:

$$|\{(m,g) \mid m \in M,\ g \in G :\ mg = m\}|$$

$$\swarrow \qquad\qquad \searrow$$

$$\frac{1}{|G|} \cdot \sum_{g \in G} |Fix(g)| \qquad\qquad \frac{1}{|G|} \cdot \sum_{m \in M} |Stab(m)|$$

$$= \sum_{m \in M} \frac{|Stab(m)|}{|G|} = \sum_{m \in M} \frac{1}{\frac{|G|}{Stab(m)}}$$

$$\overset{Satz\ 3.5}{=} \sum_{m \in M} \frac{1}{|Orb(m)|} = \sum_{m \in Repr.\ v.\ Orb.} \frac{|Orb(m)|}{|Orb(m)|}$$

$$= \sum_{m \in Repr.\ v.\ Orb.} 1 = |Orb(G)|$$

■

## 3.8 Beispiele

### 3.8.1 Punkte auf Kreisrand

Sei $M := \{1,2,3,4,5\}$ eine Menge von Punkten auf einem Kreisrand, die jeweils gleichmäßig in einem Winkel von $72°$ auseinander liegen, und $G := \langle Rot_{72} \rangle = \{id, r_{72}, ..., r_{4 \cdot 72}\}$ die Menge der Rotationen um den Kreismittelpunkt.

Es ergibt sich mit obigen Definitionen:

$|Orb(G)| = 1, \quad |Fix(r_{k \cdot 72})| = 0$ für $0 < k \leq 4, \quad |Fix(id)| = |\{1,2,3,4,5\}| = 5.$

Anwendung der im vorrausgehenden Satz bewiesenen Gleichung ergibt:

$|Orb(G)| = \frac{1}{|G|} \cdot \sum_{g \in G} |Fix(g)| \quad \Rightarrow \quad 1 = \frac{1}{5} \cdot 5 = 1 \quad ☺$

### 3.8.2 Eckpunkte eines Würfels

Erneut wird der Würfen aus Beispiel 3.4.1 betrachtet und die gewählten Notationen übernommen.

Es lässt sich leicht feststellen, dass $|Orb(G) = 1$ ist, da ein beliebig gewählter Punkt mit $M \circlearrowleft G$ auf jeden anderen abgebildet wird und somit nur ein Orbit entstehen kann. Des Weiteren gilt $|G| = 24$. Für die einzelnen Summanden von $\sum_{g \in G} |Fix(g)|$ lassen sich folgende Aussagen treffen:

$|Fix(id)| = 8, \quad |Fix(r_i^{(j)})| = |Fix(l_i)| = 0, \quad |Fix(q_i^{120})| = |Fix(q_i^{240})| = 2$

$\Rightarrow \quad |Orb(G)| = \frac{1}{|G|} \cdot \sum_{g \in G} |Fix(g)| \quad \Rightarrow \quad 1 = \frac{1}{24} \cdot (8 + 2 \cdot 8) = 1 \quad ☺$