CHAPTER 7

Cosets and Lagrange's Theorem

Properties of Cosets

DEFINITION (Coset of H in G).

Let G be a group and $H \subseteq G$. For all $a \in G$, the set $\{ah|h \in H\}$ is denoted by aH. Analagously, $Ha = \{ha|h \in H\}$ and $aHa^{-1} = \{aha^{-1}|h \in H\}$. When $H \leq G$, aH is called the left coset of H in G containing a, and Ha is called the right coset of H in G containing a. In this case the element a is called the coset representative of aH or Ha. $|aH|$ and $|Ha|$ are used to denote the number of elements in aH and Ha, respectively.

EXAMPLE. Consider the left cosets of

$$H = \{(1), (1\ 2)(34), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \leq A_4$$

from the table below:

Table 5.1 The Alternating Group A_4 of Even Permutations of {1, 2, 3, 4}

(In this table, the permutations of A_4 are designated as $\alpha_1, \alpha_2, \ldots, \alpha_{12}$ and an entry k inside the table represents α_k. For example, $\alpha_3\alpha_8 = \alpha_6$.)

	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}
$(1) = \alpha_1$	1	2	3	4	5	6	7	8	9	10	11	12
$(12)(34) = \alpha_2$	2	1	4	3	6	5	8	7	10	9	12	11
$(13)(24) = \alpha_3$	3	4	1	2	7	8	5	6	11	12	9	10
$(14)(23) = \alpha_4$	4	3	2	1	8	7	6	5	12	11	10	9
$(123) = \alpha_5$	5	8	6	7	9	12	10	11	1	4	2	3
$(243) = \alpha_6$	6	7	5	8	10	11	9	12	2	3	1	4
$(142) = \alpha_7$	7	6	8	5	11	10	12	9	3	2	4	1
$(134) = \alpha_8$	8	5	7	6	12	9	11	10	4	1	3	2
$(132) = \alpha_9$	9	11	12	10	1	3	4	2	5	7	8	6
$(143) = \alpha_{10}$	10	12	11	9	2	4	3	1	6	8	7	5
$(234) = \alpha_{11}$	11	9	10	12	3	1	2	4	7	5	6	8
$(124) = \alpha_{12}$	12	10	9	11	4	2	1	3	8	6	5	7

$H = 1H = \alpha_1 H = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \alpha_2 H = \alpha_3 H = \alpha_4 H$

$\alpha_5 H = \{\alpha_5, \alpha_6, \alpha_7, \alpha_8\} = \alpha_6 H = \alpha_7 H = \alpha_8 H.$

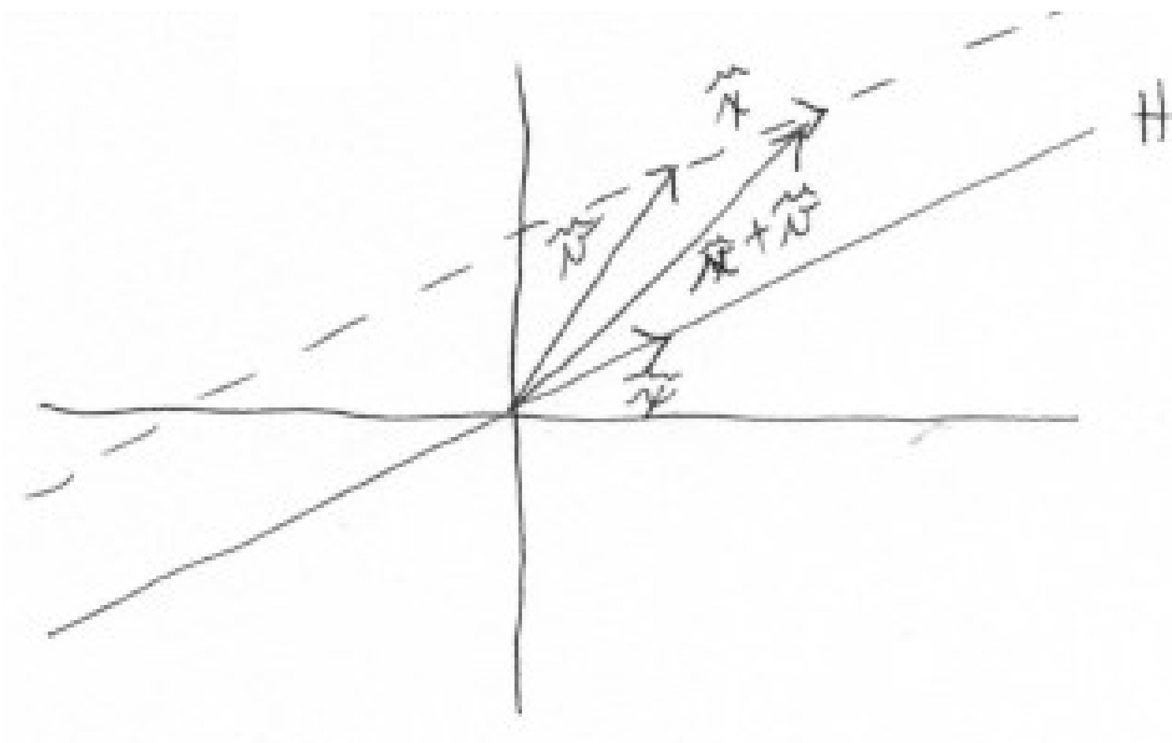
$\alpha_9 H = \{\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}\} = \alpha_{10} H, \alpha_{11} H, \alpha_{12} H.$

Also, for $k = 1, 2, \ldots, 12$, $\alpha_k H = H\alpha_k$.

When the group operation is addition, we use $a + H$ and $H + a$ instead of aH and Ha.

Example. Let G be the group of vectors in the plane with addition. Let H be a subgroup which is a line through the origin, i.e.,

$$H = \{t\mathbf{x} | \mathbf{t} \in \mathbb{R} \text{ and } \|\mathbf{x}\| = \mathbf{1}\}.$$



Then the left coset $\mathbf{v} + \mathrm{H} = \{\mathbf{v} + \mathbf{x} | \mathbf{x} \in \mathrm{H}\}$ and the right coset $H + \mathbf{v} = \{\mathbf{x} + \mathbf{v} | \mathbf{x} \in \mathrm{H}\}$ are the same line, and is parallel to H.

Lemma (Properties of Cosets). *Let $H \leq G$, and let $a, b \in G$. Then*

(1) $a \in aH$.

Proof. $a = ae \in aH$. □

(2) $aH = H \iff a \in H$.

Proof.

($\Longrightarrow$) Suppose $aH = H$. Then $a = ae \in aH = H$.

($\Longleftarrow$) Now assume $a \in H$. Since H is closed, $aH \subseteq H$. Next assume $h \in H$ also, so $a^{-1}h \in H$ since $H \leq G$. Then

$$h = eh = (aa^{-1})h = a(a^{-1}h) \in aH,$$

so $H \subseteq aH$. By mutual inclusion, $aH = H$. □

(3) $(ab)H = a(bH)$ *and* $H(ab) = (Ha)b$.

PROOF.

Follows from the associative property of group multiplication. □

(4) $aH = bH \iff a \in bH$.

PROOF.

($\Longrightarrow$) $aH = bH \Longrightarrow a = ae \in aH = bH$.

($\Longleftarrow$)$a \in bH \Longrightarrow a = bh$ where $h \in H \Longrightarrow aH = (bh)H = b(hH) = bH$ □

(5) $aH = bH$ *or* $aH \cap bH = \emptyset$.

PROOF.

Suppose $aH \cap bH \neq \emptyset$. Then $\exists\ x \in aH \cap bH \Longrightarrow \exists\ h_1, h_2 \in H \ni$ $x = ah_1$ and $x = bh_2$. Thus

$$a = xh_1^{-1} = bh_2h_1^{-1} \text{ and } aH = bh_2h_1^{-1}H = b(h_2h_1^{-1}H) = bH$$

by (2). □

(6) $aH = bH \iff a^{-1}b \in H$

PROOF.

$aH = bH \iff H = a^{-1}bH \overset{(2)}{\iff} a^{-1}b \in H$. □

(7) $|aH| = |bH|$.

PROOF.

[Find a map $\alpha : aH \to bH$ that is 1–1 and onto]

Consider $\alpha : aH \to bH$ defined by $\alpha(ah) = bh$. This is clearly onto bH. Suppose $\alpha(ah_1) = \alpha(ah_2)$. Then $bh_1 = bh_2 \Longrightarrow h_1 = h_2$ by left cancellation $\Longrightarrow ah_1 = ah_2$, so α is 1–1. Since α provides a 1-0-1 correspondence between aH and bH, $|aH| = |bH|$. □

(8) $aH = Ha \iff H = aHa^{-1}$.

PROOF.

$aH = Ha \iff (aH)a^{-1} = (Ha)a^{-1} = H(aa^{-1}) = H \iff aHa^{-1} = H$. □

(9) $aH \leq G \iff a \in H$.

PROOF.

($\Longrightarrow$) If $aH \leq G$, $e \in ah \Longrightarrow aH \cap eH \neq \emptyset \overset{(5)}{\Longrightarrow} aH = eH = H \overset{(2)}{\Longrightarrow} a \in H$.

($\Longleftarrow$) If $a \in H$, $aH = H$ by (2), so $aH \leq G$ since $H \leq G$. □

NOTE. Analagous results hold for right cosets.

NOTE. From(1), (5), and (7), the left (right) cosets of H partition G into equivalence classes under the relation

$$a \sim b \iff aH = bH \text{ (or } Ha = Hb).$$

Lagrange's Theorem and Consequences

THEOREM (7.1 — Lagrange's Theorem: $|H|$ Divides $|G|$). *If G is a finite group and $H \leq G$, then $|H| \big| |G|$. Moreover, the number of distinct left (right) cosets of H in G is $\frac{|G|}{|H|}$.*

PROOF.

Let $a_1H, a_2H, \ldots, a_rH$ denote the distinct left cosets of H in G. Then, for all $a \in G$, $aH = a_iH$ for some $i = 1, 2, \ldots, r$. By (1) of the Lemma, $a \in aH$. Thus

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH.$$

By (5) of the Lemma, this union is disjoint, so

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH| = r|H|$$

since $|a_iH| = |aH|$ for $i = 1, 2, \ldots r$. □

DEFINITION. The index of a subgroup H in G is the number of distinct left cosets of H in G, and is denoted by $|G : H|$.

COROLLARY (1 — $|G : H| = \frac{|G|}{|H|}$.). *If G is a finite group and $H \leq G$, then $|G : H| = \frac{|G|}{|H|}$.*

PROOF. Immediate consequence of Lagrange's Theorem. □

COROLLARY (2— $|a|$ Divides $|G|$). *In a finite group, the order of each element divides the order of the group.*

PROOF. For $a \in G$, $|a| = |\langle a \rangle|$, so $|a| \big| |G|$. □

COROLLARY (3 — Groups of Prime Order are Cyclic). *A group of prime order is cyclic.*

PROOF.

Suppose G has prime order. Let $a \in G$, $a \neq e$. The $|\langle a\rangle| \big| |G|$ and $|\langle a\rangle| \neq 1$, so $|\langle a\rangle| = |G| \Longrightarrow \langle a\rangle = G$. □

COROLLARY (4 — $a^{|G|} = e$.). *Let G be a finite group and $a \in G$. Then $a^{|G|} = e$.*

PROOF.

By Corollary 2, $|G| = |a|k$ for some $k \in \mathbb{N}$. Then

$$a^{|G|} = a^{|a|k} = (a^{|a|})^k = e^k = e.$$

□

COROLLARY (5 — Fermat's Little Theorem.). *For all $a \in \mathbb{Z}$ and every prime p,*

$$a^p \bmod p = a \bmod p.$$

PROOF.

By the division algorithm, $a = pm + r$ where $0 \leq r < p$. Thus $a \bmod p = r$, so we need only show $r^p \bmod p = r$. if $r = 0$, the result is clear, so

$$r \in U(p) = \{1, 2, \ldots, p-1\}.$$

Then, by Corollary 4, $r^{p-1} \bmod p = 1 \Longrightarrow r^p \bmod p = r$. □

EXAMPLE.

Table 5.1 The Alternating Group A_4 of Even Permutations of {1, 2, 3, 4}

(In this table, the permutations of A_4 are designated as $\alpha_1, \alpha_2, \ldots, \alpha_{12}$ and an entry k inside the table represents α_k. For example, $\alpha_3 \alpha_8 = \alpha_6$.)

	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}
$(1) = \alpha_1$	1	2	3	4	5	6	7	8	9	10	11	12
$(12)(34) = \alpha_2$	2	1	4	3	6	5	8	7	10	9	12	11
$(13)(24) = \alpha_3$	3	4	1	2	7	8	5	6	11	12	9	10
$(14)(23) = \alpha_4$	4	3	2	1	8	7	6	5	12	11	10	9
$(123) = \alpha_5$	5	8	6	7	9	12	10	11	1	4	2	3
$(243) = \alpha_6$	6	7	5	8	10	11	9	12	2	3	1	4
$(142) = \alpha_7$	7	6	8	5	11	10	12	9	3	2	4	1
$(134) = \alpha_8$	8	5	7	6	12	9	11	10	4	1	3	2
$(132) = \alpha_9$	9	11	12	10	1	3	4	2	5	7	8	6
$(143) = \alpha_{10}$	10	12	11	9	2	4	3	1	6	8	7	5
$(234) = \alpha_{11}$	11	9	10	12	3	1	2	4	7	5	6	8
$(124) = \alpha_{12}$	12	10	9	11	4	2	1	3	8	6	5	7

In A_4, there are 8 elements of order 3 (α_5–α_{12}). Suppose $H \leq A_4$ with $|H| = 6$. Let $a \in A_4$ with $|a| = 3$. Since $|A_4 : H| = 2$, at most two of H, aH, and a^2H are distinct. If $a \in H, H = aH = a^2H$, a contradiction.

If $a \notin H$, then $A_4 = H \cup aH \implies a^2 \in H$ or $a^2 \in aH$.

Now $a^2 \in H \implies (a^2)^2 = a^4 = a \in H$, again a contradiction.

If $a^2 \in aH$, $a^2 = ah$ for some $h \in H \implies a \in H$. Thus all 8 elemts of order 3 are in H, a group of order 6, a contradiction.

NOTE. This example means the converse of Lagrange's Theorem is not true.

THEOREM (7.2 — $|HK| = \dfrac{|H||K|}{|H \cap K|}$). *For two finite subgroups H and K of a group G, define the set $HK = \{hk \mid h \in H, k \in K\}$. Then* $|HK| = \dfrac{|H||K|}{|H \cap K|}$.

PROOF.

Although the set HK has $|H||K|$ products, all not need be distinct. That is, we may have $hk = h'k'$ where $h \neq h'$ and $k \neq k'$. To determine $|HK|$, we need to determine the extent to which this happens. For every $t \in H \cap K$, $hk = (ht)(t^{-1}k)$, so each group element in HK is represented by at least $|H \cap K|$ products in HK. But $hk = h'k' \Longrightarrow t = h^{-1}h' = kk'^{-1} \in H \cap K$, so $h' = ht$ and $k' = t^{-1}k$. Thus each element in HK is represented by exactly $|H \cap K|$ products, and so $|HK| = \dfrac{|H||K|}{|H \cap K|}$. □

PROBLEM (Page 158 # 41). Let G be a group of order 100 that has a subgroup H of order 25. Prove that every element of order 5 in G is in H.

SOLUTION.

Let $a \in G$ and $|a| = 5$. Then by Theorem 7.2 the set $\langle a \rangle H$ has exactly $\dfrac{5 \cdot |H|}{|\langle a \rangle \cap H|}$ elements and $|\langle a \rangle \cap H|$ divides $|\langle a \rangle| = 5 \Longrightarrow |\langle a \rangle \cap H| = 5 \Longrightarrow$ $\langle a \rangle \cap H = \langle a \rangle \Longrightarrow a \in H$. □

THEOREM (7.3 — Classification of Groups of Order $2p$.). *Let G be a group of order $2p$ where p is a prime greater than 2. Then $G \approx \mathbb{Z}_{2p}$ or $G \approx D_p$.*

PROOF.

Assume G has no element of order $2p$. [To show $G \approx D_p$.]

[Show G has an element of order p.] By Lagrange's Theorem, every nonidentity element must have order 2 or p. So assume every nonidentity element has order 2. Then, for all $a, b \in G$,

$$(ab) = (ab)^{-1} = b^{-1}a^{-1} = ba,$$

so G is Abelian. Thus, for $a, b \in G$, $a \neq e$, $b \neq e$, $\{e, a, b, ab\}$ is closed and so is a subgroup of G of order 4, contradicting Lagrange's Theorem. Thus G has an element of order p. Call it a.

[To show any element not in $\langle a\rangle$ has order 2.] Suppose $b \in G, b \notin \langle a\rangle$. By Lagrange's theorem and our assumption that G does not have an element of order of $2p$, $|b| = 2$ or $|b| = p$. Because $|\langle a\rangle \cap \langle b\rangle|$ divides $|\langle a\rangle| = p$ and $\langle a\rangle \neq \langle b\rangle$, $|\langle a\rangle \cap \langle b\rangle| = 1$. Now suppose $|b| \neq 2$. Then by Theorem 7.2 $|\langle a\rangle\langle b\rangle| = |\langle a\rangle||\langle b\rangle| = p^2 > 2p = |G|$, which is impossible. Thus $|b| = 2$.

Now $ab \notin \langle a\rangle \implies |ab| = 2$ by the same argument as above. Then

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1}.$$

This relation completely determines the multiplication table for G. [For example,

$$a^3ba^4 = a^2(ab)a^4 = a^2(ba^{-1})a^4 = a(ab)a^3 = a(ba^{-1})a^3 = (ab)a^2 = (ba^{-1})a^2 = ba.]$$

Thus all noncyclic groups of order $2p$ must be isomorphic to each other, and D_p is one such group. □

EXAMPLE. $S_3 \approx D_3$.

PROOF. $|S_3| = 6 = 2 \cdot 3$ and S_3 is not cyclic. □

An Application of Cosets to Permutation Groups

Definition (Stabilizer of a Point). Let G be a group of permutations of a set S. For each $i \in S$, let $\text{stab}_G(i) = \{\phi \in G | \phi(i) = i\}$. We call $\text{stab}_G(i)$ the stabilizer of i in G.

Corollary. $\text{stab}_G(i)$ *is a subgroup of* G.

Proof.

[Page 120 # 35] Let $\alpha, \beta \in \text{stab}_G(i)$. Then $\alpha(i) = i$ and $\beta(i) = i$, so

$$(\alpha\beta)(i) = \alpha\big(\beta(i)\big) = \alpha(i) = i,$$

so $\alpha\beta \in \text{stab}_G(i)$. Also,

$$\alpha^{-1}\big(a(i)\big) = \alpha^{-1}(i) \Longrightarrow i = \alpha^{-1}(i),$$

so $\alpha^{-1} \in \text{stab}_G(i)$.

Thus $\text{stab}_G(i) \leq G$ by the two-step test. □

Definition (Orbit of a Point). Let G be a group of permutations of a set S. For each $i \in S$, let $\text{orb}_G(s) = \{\phi(s) | \phi \in G\}$. The set $\text{orb}_G(s)$ is a subset of S called the orbit of s under G. We use $|\text{orb}_G(s)|$ to denote the number of elements in $\text{orb}_G(s)$.

Problem (Page 158 # 45).

Let

$$G = \{(1), (1\ 2)(3\ 4), (1\ 2\ 3\ 4)(5\ 6), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)(5\ 6), (5\ 6)(1\ 3), (1\ 4)(2\ 3), (2\ 4)(5\ 6)\}$$

Solution.

$\text{stab}_G(1) = \{(1), (2\ 4)(5\ 6)\}$.

$\text{stab}_G(3) = \{(1), (2\ 4)(5\ 6)\}$.

$\text{stab}_G(5) = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

$\text{orb}_G(1) = \{1, 2, 3, 4\}$.

$\text{orb}_G(3) = \{1, 2, 3, 4\}$.

$\text{orb}_G(5) = \{5, 6\}$.

□

THEOREM (7.4 — Orbit-Stabilizer Theorem). *Let G be a group of permutations of a set S. Then, for any $i \in S$, $|G| = |\text{orb}_G(i)| \cdot |\text{stab}_G(i)|$.*

PROOF.

By Lagange's Theorem, $\dfrac{|G|}{|\text{stab}_G(i)|}$ is the number of distinct left cosets of $\text{stab}_G(i)$ in G. [To show a 1–1 correspondence between these cosets and the elements of $\text{orb}_G(i)$.]

Define

$$T : \{\phi\,\text{stab}_G(i) | \phi \in G\} \to \text{orb}_G(i) \text{ by } T(\phi\,\text{stab}_G(i)) = \phi(i).$$

[To show T is well-defined, i.e., that $\alpha\,\text{stab}_G(i) = \beta\,\text{stab}_G(i) \implies \alpha(i) = \beta(i)$ or that the result of the mapping depends on the coset and not on a particular representation of it.] Now,

$$\alpha\,\text{stab}_G(i) = \beta\,\text{stab}_G(i) \iff \text{stab}_G(i) = \alpha^{-1}\beta\,\text{stab}_G(i) \iff \alpha^{-1}\beta \in \text{stab}_G(i) \iff \alpha^{-1}\beta(i) = i \iff \beta(i) = \alpha(i)$$

so T is well-defined and, from the reverse implications, T is 1–1.

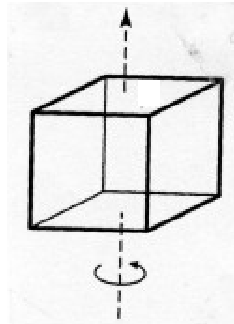
[To show T is onto.] Let $j \in \text{orb}_G(i)$. Then $\alpha(i) = j$ for some $\alpha \in G$, and $T(\alpha\,\text{stab}_G(i)) = \alpha(i) = j$, so T is onto.

Thus T is a 1–1 correspondence. □

The Rotation Group of a Cube

Let G be the rotation group of a cube. Label the faces 1–6. Since each rotation must carry each face to exactly one other face, G is a group of permutations on $\{1, 2, 3, 4, 5, 6\}$.There is a central horizontal or vertical permutation that carries face 1 to any other face, so $|\text{orb}_G(1)| = 6$. Also, there are 4 rotations ($0°, 90°, 180°, 270°$ about the line $\perp$ to the face and passing through its center), so $|\text{stab}_G(1)| = 4$. By Theorem 7.4,

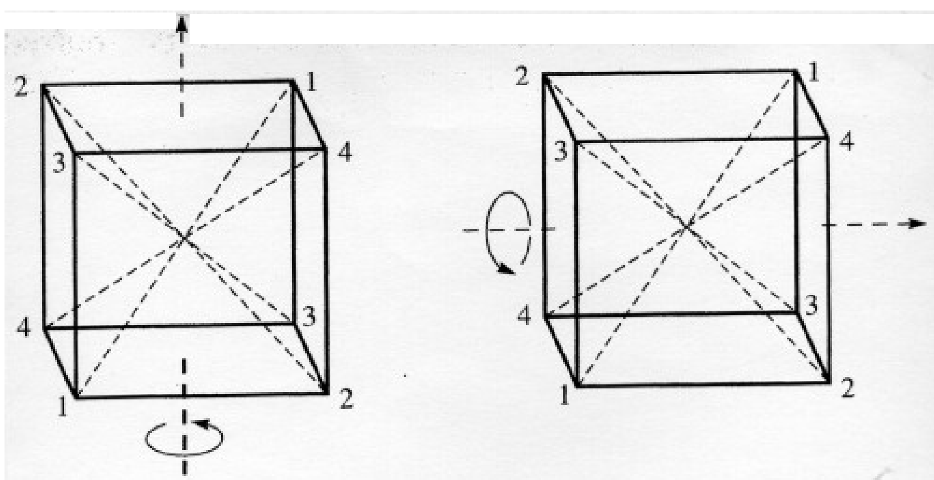
$$|G| = |\text{orb}_G(1)| \cdot |\text{stab}_G(1)| = 6 \cdot 4 = 24.$$



Theorem (The rotation Group of the Cube). *The group of rotations of a cube is isomorphic to* S_4.

Proof.

Since $|G| = |S_4|$, we need only show that G is isomorphic to a subgroup of S_4. Now a cube has 4 diagonals and any rotation induces a permutation of these diagonals. But we cannot just assume that different rotations correspond to different rotations.



$\alpha = (1\ 2\ 3\ 4)$ $\qquad\qquad$ $\beta = (1\ 4\ 3\ 2)$

We need to show all 24 permutations of the diagonals come from rotations. Numbering the diagonals as above, we see two perpendicular axes where 90° rotations give the permutations $\alpha = (1\ 2\ 3\ 4)$ and $\beta = (1\ 4\ 3\ 2)$. These induce an 8 element subgroup $\{\varepsilon, \alpha, \alpha^2, \alpha^3, \beta^2, \beta^2\alpha, \beta^2\alpha^2, \beta^2\alpha^3\}$ and the 3 element subgroup $\{\varepsilon, \alpha\beta, (\alpha\beta)^2\}$. Thus the rotations induce all 24 permutations since $24 = \text{lcm}(8, 3)$. □

PROBLEM (Page 158 # 46). Prove that a group G of order 12 must have an element of order 2.

PROOF.

Let $a \in G, a \neq e$. By Lagrange's theorem, $|a| = 12, 6, 4, 3$, or 2.

If $|a| = 12$, $|a^6| = 2$. If $|a| = 6$, $|a^3| = 2$. If $|a| = 4$, $|a^2| = 2$.

Suppose all non-identity elements of G have order 3. But such elements come in pairs, e.g., if $|a| = 3$, $|a^2| = 3$. But there are 11 non-identity elements, a contradiction. Thus G has an element of order 2. □

PROBLEM (Page 158 # 47). Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution.

PROOF.

Suppose y is a solution also, i.e., $y^2 = a \Longrightarrow x^2 = y^2$. Let $|G| = 2k+1$. Then

$$x = xe = xx^{2k+1} = x^{2k+2} = (x^2)^{k+1} = (y^2)^{k+1} = y^{2k+2} = yy^{2k+1} = ye = y.$$

□