MATH 343 · GROUP THEORY · CHAPTER 7

Cosets and Lagrange's Theorem

Properties of Cosets · Lagrange's Theorem and Consequences · Orbits and Stabilizers

Fahd M. Alshammari

Part 1 — Cosets

GOAL. Use a subgroup H to cut a group G into pieces of the same size, called cosets.

- Left and right cosets, and how to compute them
- Lemma 7.1: nine properties of cosets, with proofs
- The cosets of H partition G — the key to Lagrange's Theorem

Definition — Cosets

DEFINITION. Let G be a group, H a subgroup of G, and $a \in G$.

- The **left coset** of H containing a is $aH = \{ah \mid h \in H\}$
- The **right coset** of H containing a is $Ha = \{ha \mid h \in H\}$

The element a is called a **representative** of aH (or of Ha). We also write $aHa^{-1} = \{aha^{-1} \mid h \in H\}$, and $|aH|$ for the number of elements of aH.

NOTATION. When the operation is $+$, the left coset is written $a + H = \{a + h \mid h \in H\}$.

Left Cosets in S_3

EXAMPLE. In S_3, let $H = \{(1), (13)\}$. The left cosets of H are

$$(1)H = (13)H = H,$$

$$(12)H = \{(12), (12)(13)\} = \{(12), (132)\} = (132)H,$$

$$(23)H = \{(23), (23)(13)\} = \{(23), (123)\} = (123)H.$$

The right coset $H(12) = \{(12), (13)(12)\} = \{(12), (123)\}$ is different from $(12)H$.

Cosets in D_4 and in $\mathbb{Z}_9$

EXAMPLE. In D_4, let $K = \{R_0, R_{180}\}$. Then

$$R_0K = R_{180}K = K, \qquad R_{90}K = R_{270}K = \{R_{90}, R_{270}\},$$

$$HK = VK = \{H, V\}, \qquad DK = D'K = \{D, D'\}.$$

EXAMPLE. In $\mathbb{Z}_9$, let $H = \{0,3,6\}$. Then

$$0 + H = \{0,3,6\}, \qquad 1 + H = \{1,4,7\}, \qquad 2 + H = \{2,5,8\},$$

and $3 + H = 0 + H$, $4 + H = 1 + H$, $5 + H = 2 + H$, and so on.

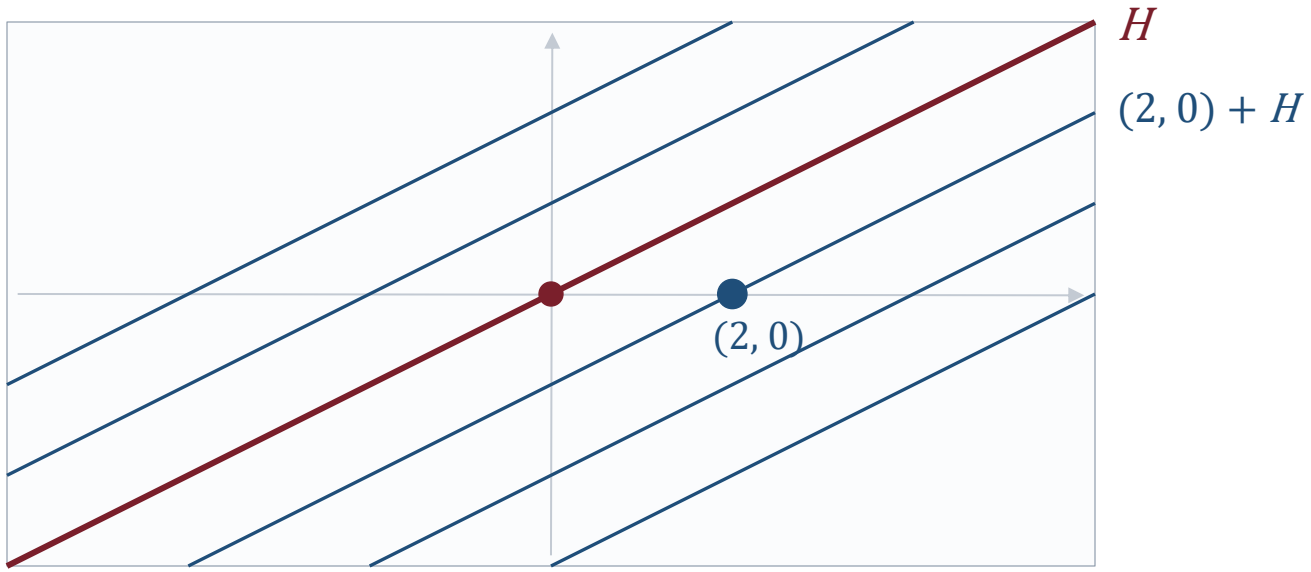
What the Examples Show

- Cosets are usually not subgroups: $(12)H = \{(12), (132)\}$ does not contain the identity
- $aH = bH$ can happen with $a \neq b$: $(12)H = (132)H$
- aH and Ha can be different: $(12)H \neq H(12)$
- But in every example the cosets cut the group into blocks of the same size, with no overlaps

When is $aH = bH$? Can two different cosets overlap? Which cosets are subgroups? Lemma 7.1 answers these questions.

Cosets of a Line in the Plane

EXAMPLE. In $\mathbb{R}^2$ under addition, let $H = \{(2t, t) \mid t \in \mathbb{R}\}$, a line through the origin. The coset $(a, b) + H$ is the line through (a, b) parallel to H.



Red: H. Blue: some of its cosets. Every point lies on exactly one line, and each line is H moved by a vector.

Lemma 7.1 — Properties of Cosets

LEMMA 7.1. Let H be a subgroup of G, and let $a, b \in G$. Then:

(1) $a \in aH$.

(2) $aH = H$ if and only if $a \in H$.

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

(4) $aH = bH$ if and only if $a \in bH$.

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

Lemma 7.1, Continued

LEMMA 7.1 (CONTINUED).

(6) $aH = bH$ if and only if $a^{-1}b \in H$.

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

(8) $aH = Ha$ if and only if $H = aHa^{-1}$.

(9) aH is a subgroup of G if and only if $a \in H$.

- Parts (1), (5) and (7) are the heart of the lemma: every element lies in a coset, different cosets do not overlap, and all cosets have the same size

Proof of Lemma 7.1 — Parts 1, 2 and 3

PROOF (1). $a = ae$ and $e \in H$, so $a \in aH$.

PROOF (2). If $aH = H$, then $a = ae \in aH = H$. Conversely, let $a \in H$. Then $aH \subseteq H$, since H is closed. And for every $h \in H$, $a^{-1}h \in H$ and $h = a\left(a^{-1}h\right) \in aH$; so $H \subseteq aH$. Hence $aH = H$.

PROOF (3). For every $h \in H$, $(ab)h = a(bh)$, so $(ab)H = a(bH)$. Likewise, $h(ab) = (ha)b$ gives $H(ab) = (Ha)b$.

Proof of Lemma 7.1 — Parts 4, 5 and 6

PROOF (4). If $aH = bH$, then $a \in aH = bH$ by (1). Conversely, if $a \in bH$, then $a = bh$ for some $h \in H$, and by (3) and (2), $aH = (bh)H = b(hH) = bH$.

PROOF (5). Suppose $aH \cap bH \neq \emptyset$, and let $c \in aH \cap bH$. By (4), $cH = aH$ and $cH = bH$. So $aH = bH$.

PROOF (6). Multiply on the left by a^{-1} (or back by a) and use (3) and (2):

$$aH = bH \Leftrightarrow H = \left(a^{-1}b\right)H \Leftrightarrow a^{-1}b \in H.$$

Proof of Lemma 7.1 — Part 7

PROOF (7). Define $\varphi: aH \to bH$ by $\varphi(ah) = bh$ for $h \in H$.

Step 1 (well defined). If $ah = ah'$, then $h = h'$ by cancellation. So each $x \in aH$ is ah for exactly one $h \in H$, and $\varphi(x) = bh$ is one element of bH.

Step 2 (one-to-one). If $\varphi(ah) = \varphi(ah')$, then $bh = bh'$, so $h = h'$ and $ah = ah'$.

Step 3 (onto). Every element bh of bH is $\varphi(ah)$.

So φ is a one-to-one correspondence, and $|aH| = |bH|$. With $b = e$: $|aH| = |H|$.

Proof of Lemma 7.1 — Parts 8 and 9

PROOF (8). Multiply on the right by a^{-1} (or back by a). Since $(aH)a^{-1} = aHa^{-1}$ and, by (3), $(Ha)a^{-1} = H\left(aa^{-1}\right) = H$,

$$aH = Ha \Leftrightarrow aHa^{-1} = H.$$

PROOF (9). If aH is a subgroup, then $e \in aH$. Also $e \in eH = H$, so $aH \cap eH \neq \emptyset$, and $aH = eH = H$ by (5). Then $a \in H$ by (2). Conversely, if $a \in H$, then $aH = H$ by (2), which is a subgroup.

The Cosets of H Partition G

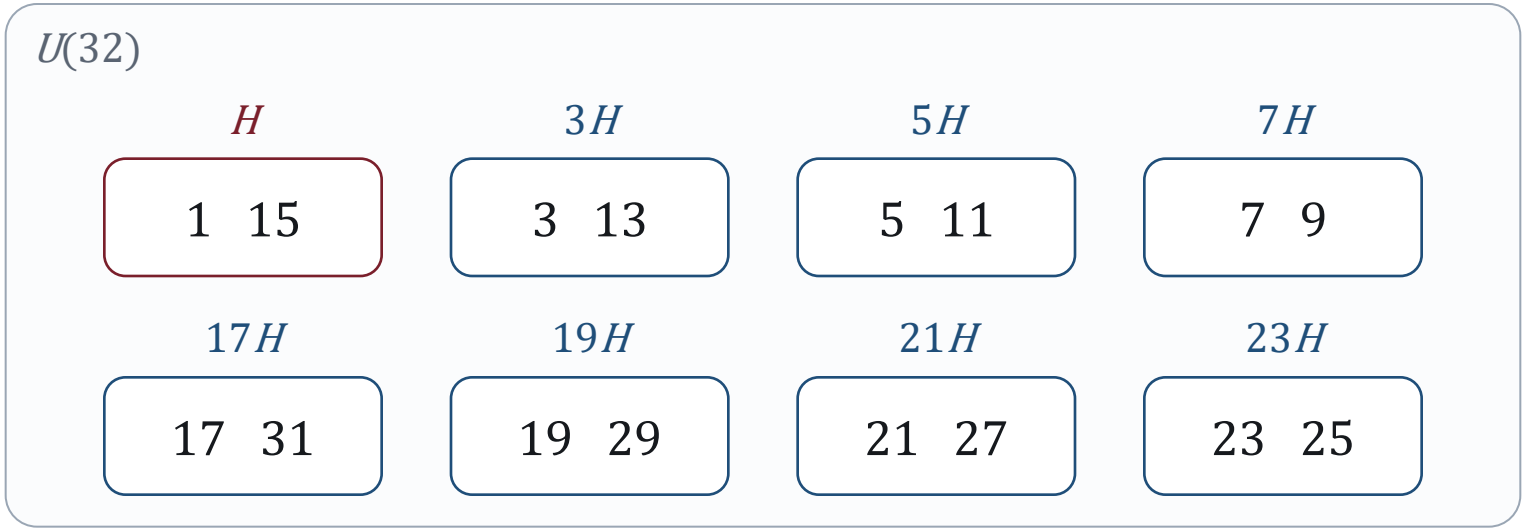
CONSEQUENCE. Let H be a subgroup of G. By Lemma 7.1:

- every $a \in G$ lies in a left coset of H, namely aH — part (1)
- two left cosets are equal or disjoint — part (5)
- every left coset has $|H|$ elements, since $|aH| = |eH| = |H|$ — part (7)

So the left cosets of H **partition** G into blocks of size $|H|$. They are the equivalence classes of the relation $a \sim b \Leftrightarrow aH = bH$ (Theorem 0.7).

All the Cosets of a Subgroup of U(32)

EXAMPLE. $U(32)$ has 16 elements. Let $H = \{1,15\}$. Choose a representative not used yet, and repeat: H, $3H = \{3,13\}$, $5H = \{5,11\}$, …, until every element appears.



8 cosets of 2 elements each, with no overlaps: 16 = 8 · 2.

Part 2 — Lagrange's Theorem

GOAL. Count with cosets: the order of a subgroup divides the order of the group.

- Lagrange's Theorem, the index, and five corollaries
- The converse is false: A_4 has no subgroup of order 6
- Counting products: $|HK| = |H||K|/|H \cap K|$
- Every group of order $2p$ is $\mathbb{Z}_{2p}$ or D_p

Theorem 7.1 — Lagrange's Theorem

THEOREM 7.1 (LAGRANGE). If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, H has exactly $|G|/|H|$ left cosets in G, and $|G|/|H|$ right cosets.

- Lagrange's Theorem lists the candidates: a group of order 12 can have subgroups only of order 1, 2, 3, 4, 6 or 12

WARNING. The converse is false: a divisor d of $|G|$ need not be the order of any subgroup. A_4 has order 12 and no subgroup of order 6.

Proof of Lagrange's Theorem

PROOF. Let $a_1H, a_2H, \ldots, a_rH$ be the distinct left cosets of H in G.

Step 1 (they cover G). For $a \in G$, $a \in aH$ by Lemma 7.1(1), and $aH = a_iH$ for some i. So $G = a_1H \cup a_2H \cup \cdots \cup a_rH$.

Step 2 (no overlaps). The cosets are disjoint, by Lemma 7.1(5). So

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH|.$$

Step 3 (equal sizes). $|a_iH| = |H|$ for each i, by Lemma 7.1(7). So $|G| = r\,|H|$.

Hence $|H|$ divides $|G|$, and $r = |G|/|H|$.

The Index of a Subgroup

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

COROLLARY 1. If G is a finite group and H is a subgroup of G, then $|G:H| = |G|/|H|$.

EXAMPLE. $|U(32):\{1,15\}| = 16/2 = 8$, and $|S_3:\{(1),(13)\}| = 6/2 = 3$, in agreement with the lists found earlier.

Corollary 2 — |a| Divides |G|

COROLLARY 2. In a finite group G, the order of every element divides $|G|$.

PROOF. Let $a \in G$. By Chapter 4 (Corollary 1 of Theorem 4.1), $|a| = |\langle a \rangle|$, and $\langle a \rangle$ is a subgroup of G. By Lagrange's Theorem, $|\langle a \rangle|$ divides $|G|$.

EXAMPLE. $|S_4| = 24$. The elements of S_4 have orders 1, 2, 3 and 4 — all divisors of 24. No element has order 6, 8, 12 or 24: divisors of $|G|$ need not occur as orders.

Corollary 3 — Groups of Prime Order Are Cyclic

COROLLARY 3. Every group of prime order p is cyclic, and isomorphic to $\mathbb{Z}_p$.

PROOF. Let $|G| = p$, and choose $a \in G$ with $a \neq e$. By Lagrange's Theorem, $|\langle a \rangle|$ divides p; and $|\langle a \rangle| \neq 1$, since $a \neq e$. So $|\langle a \rangle| = p$, that is, $\langle a \rangle = G$. By the Proposition of Chapter 6, $\varphi: G \to \mathbb{Z}_p$, $\varphi(a^k) = k \bmod p$, is an isomorphism.

- Up to isomorphism there is exactly one group of each prime order

Corollary 4 — The Power |G| Gives e

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

PROOF. By Corollary 2, $|G| = |a|\, k$ for some positive integer k. So

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

EXAMPLE. $U(13)$ has 12 elements, so $2^{12} \bmod 13 = 1$. Since $100 = 8 \cdot 12 + 4$,

$$2^{100} \bmod 13 = \left(\left(2^{12}\right)^8 \cdot 2^4\right) \bmod 13 = 16 \bmod 13 = 3.$$

Corollary 5 — Fermat's Little Theorem

COROLLARY 5 (FERMAT'S LITTLE THEOREM). For every integer a and every prime p, $a^p \bmod p = a \bmod p$.

PROOF. By the division algorithm, $a = pm + r$ with $0 \leq r < p$. Then $a \bmod p = r$ and $a \equiv r \pmod{p}$, so it is enough to show $r^p \bmod p = r$.

If $r = 0$, both sides are 0. If $r \neq 0$, then $r \in U(p) = \{1,2, \ldots, p-1\}$, a group of order $p - 1$. By Corollary 4, $r^{p-1} \bmod p = 1$, so $r^p \bmod p = r$.

The Converse of Lagrange's Theorem Is False

EXAMPLE. $|A_4| = 12$, but A_4 has no subgroup of order 6.

- The proof uses one fact from Chapter 5: A_4 has eight elements of order 3, the 3-cycles
  $(123), (132), (124), (142), (134), (143), (234), (243)$
- We show that a subgroup of order 6 would have to contain all eight of them, which is impossible
- So "d divides $|G|$" does not guarantee a subgroup of order d

Proof That A_4 Has No Subgroup of Order 6

PROOF. Suppose $H \leq A_4$ with $|H| = 6$. Let $a \in A_4$ with $|a| = 3$; we show that $a \in H$.

Suppose $a \notin H$. Then $aH \neq H$ (Lemma 7.1(2)), and H has only $12/6 = 2$ left cosets, so $A_4 = H \cup aH$. Hence $a^2 \in H$ or $a^2 \in aH$.

- If $a^2 \in H$, then $a = a^4 = \left(a^2\right)^2 \in H$
- If $a^2 \in aH$, then $a^2 = ah$ for some $h \in H$, so $a = h \in H$

Both cases contradict $a \notin H$. So H contains all eight elements of order 3, although $|H| = 6$ — a contradiction.

Theorem 7.2 — Counting the Products HK

DEFINITION. For subgroups H and K of a group, $HK = \{hk \mid h \in H,\ k \in K\}$.

THEOREM 7.2. If H and K are finite subgroups of a group, then

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

- There are $|H||K|$ products hk, but different products can be the same element; the theorem counts the repeats
- HK is a set of products, not the union $H \cup K$, and it need not be a subgroup

Proof of Theorem 7.2

PROOF. Define $f: H \times K \to HK$ by $f(h,k) = hk$. It is onto, by the definition of HK. We show that each $x \in HK$ is $f(h,k)$ for exactly $|H \cap K|$ pairs.

Let $x = hk$. For each $t \in H \cap K$, the pair $\left(ht,\ t^{-1}k\right)$ is in $H \times K$, and $(ht)\left(t^{-1}k\right) = hk = x$. Different t give different pairs.

Conversely, if $h'k' = hk$, put $t = h^{-1}h' = kk'^{-1}$. Then $t \in H \cap K$, $h' = ht$ and $k' = t^{-1}k$.

So $|H|\,|K| = |HK| \cdot |H \cap K|$.

Using Theorem 7.2

EXAMPLE. A group G of order 75 has at most one subgroup of order 25.

PROOF. Let H and K be subgroups of G with $|H| = |K| = 25$. $H \cap K$ is a subgroup of H, so $|H \cap K|$ is 1, 5 or 25, by Lagrange's Theorem.

If $|H \cap K| = 1$ or 5, Theorem 7.2 gives $|HK| = 625$ or 125; but $HK \subseteq G$ has at most 75 elements. So $|H \cap K| = 25$, and $H = H \cap K = K$.

Theorem 7.3 — Groups of Order 2p

THEOREM 7.3. Let $p > 2$ be a prime, and let G be a group of order $2p$. Then $G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$.

CONSEQUENCE. A non-Abelian group of order $2p$ is D_p in disguise. For example, $S_3 \cong D_3$, and $GL(2, \mathbb{Z}_2) \cong D_3$.

- $\mathbb{Z}_{2p}$ and D_p are not isomorphic: one is Abelian, the other is not
- The proof uses Corollary 2, Lagrange's Theorem and Theorem 7.2

Proof of Theorem 7.3 — An Element of Order p

PROOF. If G has an element of order $2p$, then G is cyclic and $G \cong \mathbb{Z}_{2p}$ (Chapter 6). So assume G has no element of order $2p$; we show $G \cong D_p$.

Claim 1. G has an element of order p. By Corollary 2, each $x \neq e$ has order 2 or p. Suppose every $x \neq e$ has order 2. Then $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$ for all x, y, so G is Abelian; and for distinct $x, y \neq e$, $\{e, x, y, xy\}$ is a subgroup of order 4. But 4 does not divide $2p$. So some $a \in G$ has $|a| = p$.

Proof of Theorem 7.3 — The Elements Outside ⟨a⟩

Claim 2. Every $b \notin \langle a \rangle$ has order 2. By Corollary 2, $|b| = 2$ or p. Suppose $|b| = p$. The subgroup $\langle a \rangle \cap \langle b \rangle$ of $\langle a \rangle$ has order 1 or p; if p, then $\langle a \rangle = \langle b \rangle$ and $b \in \langle a \rangle$. So $|\langle a \rangle \cap \langle b \rangle| = 1$, and by Theorem 7.2, $|\langle a \rangle\langle b \rangle| = p^2 > 2p = |G|$ — impossible.

Claim 3. Fix $b \notin \langle a \rangle$. The right cosets $\langle a \rangle$ and $\langle a \rangle b$ are different, and there are only $2p/p = 2$ of them, so

$$G = \{e, a, \ldots, a^{p-1}, b, ab, \ldots, a^{p-1}b\}.$$

Also $ab \notin \langle a \rangle$, so $|ab| = 2$ by Claim 2: $abab = e$, and $bab = a^{-1}$.

Proof of Theorem 7.3 — The Isomorphism with D_p

From $bab = a^{-1}$ and $b^2 = e$ we get $a^{-j} = (bab)^j = ba^jb$, so $ba^j = a^{-j}b$. Hence products in G follow four rules:

$$a^i a^j = a^{i+j}, \qquad a^i(a^j b) = a^{i+j}b,$$

$$(a^i b)a^j = a^{i-j}b, \qquad (a^i b)(a^j b) = a^{i-j}.$$

In D_p, let R be the rotation through $360°/p$ and F a reflection: $|R| = p$, $F^2 = R_0$, $FRF = R^{-1}$, so the same rules hold for R and F. Define $\varphi: D_p \to G$ by $\varphi(R^i) = a^i$ and $\varphi(R^iF) = a^ib$, for $0 \le i < p$.

Steps 1–3. φ matches the $2p$ elements of D_p one to one with those of G. **Step 4.** Both groups multiply by the same four rules. So $G \cong D_p$.

Part 3 — Orbits and Stabilizers

GOAL. Use cosets to count the symmetries of an object.

- Stabilizers and orbits of a group of permutations
- The Orbit-Stabilizer Theorem: $|G| = |\mathrm{orb}_G(i)|\,|\mathrm{stab}_G(i)|$
- The rotation groups of a cube (24 rotations, isomorphic to S_4) and of a soccer ball (60 rotations)

Definitions — Stabilizer and Orbit

DEFINITION. Let G be a group of permutations of a set S, and let $i \in S$.

- The **stabilizer** of i is $\mathrm{stab}_G(i) = \{\alpha \in G \mid \alpha(i) = i\}$
- The **orbit** of i is $\mathrm{orb}_G(i) = \{\alpha(i) \mid \alpha \in G\}$

So $\mathrm{stab}_G(i)$ is a set of permutations, a subset of G; $\mathrm{orb}_G(i)$ is a set of points, a subset of S.

EXAMPLE. If G is the group of rotations of the plane about a point P, the orbit of a point Q is the circle with centre P through Q — hence the name.

Stabilizers Are Subgroups

PROPOSITION. Let G be a group of permutations of a set S, and $i \in S$. Then $\text{stab}_G(i)$ is a subgroup of G.

PROOF. The identity ε fixes i, so $\text{stab}_G(i) \neq \emptyset$. Let $\alpha, \beta \in \text{stab}_G(i)$. From $\beta(i) = i$ we get $\beta^{-1}(i) = i$, so

$$\left(\alpha\beta^{-1}\right)(i) = \alpha\left(\beta^{-1}(i)\right) = \alpha(i) = i.$$

So $\alpha\beta^{-1} \in \text{stab}_G(i)$, and by the One-Step Subgroup Test (Theorem 3.1), $\text{stab}_G(i)$ is a subgroup of G.

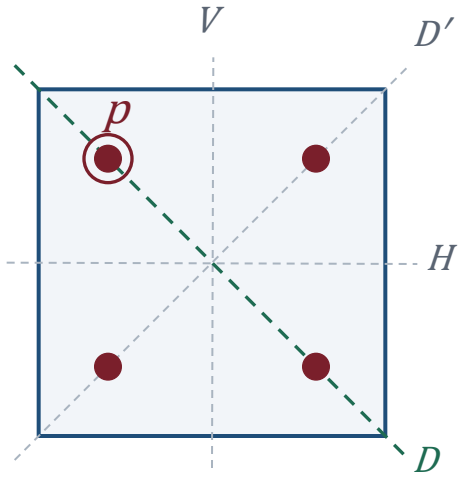
Orbits and Stabilizers in a Subgroup of S_8

EXAMPLE. $G = \{(1), (132)(465)(78), (132)(465), (123)(456), (123)(456)(78), (78)\}$, a subgroup of S_8 of order 6.

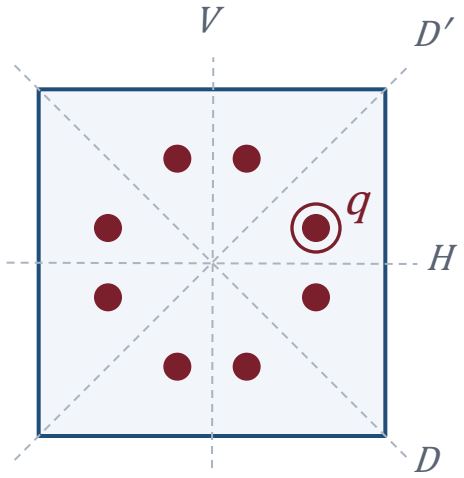
i	orbit of i	stabilizer of i	product
1	{1, 2, 3}	{(1), (78)}	3 · 2 = 6
4	{4, 5, 6}	{(1), (78)}	3 · 2 = 6
7	{7, 8}	{(1), (132)(465), (123)(456)}	2 · 3 = 6

D_4 Acting on the Square

EXAMPLE. D_4 moves the points of the square region. Below: the orbit and the stabilizer of a point p on the axis of D, and of a point q on no axis.



$\text{orb}(p)$: 4 points, $\text{stab}(p) = \{R_0, D\}$



$\text{orb}(q)$: 8 points, $\text{stab}(q) = \{R_0\}$

In both cases |orb| · |stab| = 8 = $|D_4|$. Ringed: the point; red dots: its orbit.

Theorem 7.4 — The Orbit-Stabilizer Theorem

THEOREM 7.4. Let G be a finite group of permutations of a set S. Then for every $i \in S$,

$$|G| = |\mathrm{orb}_G(i)|\,|\mathrm{stab}_G(i)|.$$

- Example 8: $3 \cdot 2 = 2 \cdot 3 = 6 = |G|$; the square: $4 \cdot 2 = 8 \cdot 1 = 8 = |D_4|$
- Idea of the proof: the points of the orbit match the left cosets of the stabilizer, one to one

Proof of the Orbit-Stabilizer Theorem

PROOF. Let $H = \text{stab}_G(i)$. By Lagrange's Theorem, H has $|G|/|H|$ left cosets, so it is enough to match them one to one with the points of $\text{orb}_G(i)$. Define $T(\alpha H) = \alpha(i)$ for $\alpha \in G$.

Step 1 (well defined). If $\alpha H = \beta H$, then $\alpha^{-1}\beta \in H$ by Lemma 7.1(6), so $(\alpha^{-1}\beta)(i) = i$, that is, $\beta(i) = \alpha(i)$.

Step 2 (one-to-one). If $\alpha(i) = \beta(i)$, then $(\alpha^{-1}\beta)(i) = i$, so $\alpha^{-1}\beta \in H$, and $\alpha H = \beta H$.

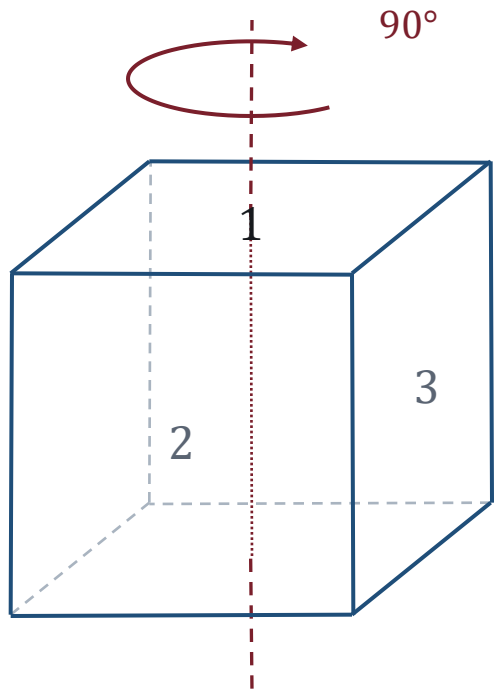
Step 3 (onto). If $j \in \text{orb}_G(i)$, then $j = \alpha(i) = T(\alpha H)$ for some $\alpha \in G$.

So $|G|/|H| = |\text{orb}_G(i)|$.

The Rotation Group of a Cube

EXAMPLE. Let G be the group of rotations of a cube, acting on its six faces. Some rotation carries face 1 to any other face, so $|\mathrm{orb}_G(1)| = 6$. The rotations keeping face 1 in place are the turns through $0°$, $90°$, $180°$ and $270°$ about the axis through its centre, so $|\mathrm{stab}_G(1)| = 4$. Hence

$$|G| = 6 \cdot 4 = 24.$$



Turns about this axis keep face 1 on top.

Theorem 7.5 — The Rotation Group of a Cube Is S_4

THEOREM 7.5. The group G of rotations of a cube is isomorphic to S_4.

- A cube has four diagonals, each joining a corner to the opposite corner
- Every rotation carries diagonals to diagonals, so it permutes the four diagonals
- The proof shows that this is an isomorphism from G to S_4, using $|G| = 24$ and Lagrange's Theorem

Proof of Theorem 7.5

PROOF. Number the diagonals 1, 2, 3, 4, and let $\varphi(r) \in S_4$ be the permutation of the diagonals made by the rotation r.

Step 4 (operation-preserving). Doing r_2 and then r_1 moves the diagonals by $\varphi(r_1)\varphi(r_2)$, so $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$. Hence $\varphi(G)$ is closed under products, so it is a subgroup of S_4 (Theorem 3.3).

Step 3 (onto). Two quarter turns give $\alpha = (1234)$ and $\beta = (1423)$ in $\varphi(G)$. Then α and $\beta^2 = (12)(34)$ generate a subgroup of order 8, and $\alpha\beta = (243)$ has order 3. So 8 and 3 divide $|\varphi(G)|$, and $\varphi(G) = S_4$.

Steps 1 and 2. Each rotation gives one permutation, and φ maps the 24 rotations onto the 24 elements of S_4; so it is one-to-one.

The Soccer Ball

EXAMPLE. A soccer ball has 12 pentagonal faces and 20 hexagonal faces. Let G be its rotation group, acting on the 12 pentagons. Any pentagon can be carried to any other, so $|\mathrm{orb}_G(P)| = 12$; the rotations keeping a pentagon P in place are the five turns through multiples of $72°$ about its centre. So

$$|G| = 12 \cdot 5 = 60.$$

- The rotation group of the soccer ball is isomorphic to A_5 (Gallian, without proof)
- The "buckyball", a molecule of 60 carbon atoms, has this shape (Nobel Prize in Chemistry, 1996)

What to Take Away

- The left cosets of a subgroup H partition G into blocks of size $|H|$, and $aH = bH \Leftrightarrow a^{-1}b \in H$
- Lagrange: $|H|$ divides $|G|$, and $|G:H| = |G|/|H|$; so $|a|$ divides $|G|$ and $a^{|G|} = e$
- The converse fails: A_4 has no subgroup of order 6
- Groups of prime order are cyclic; a group of order $2p$ is $\mathbb{Z}_{2p}$ or D_p
- Counting tools: $|HK| = |H||K|/|H \cap K|$ and $|G| = |\mathrm{orb}_G(i)||\mathrm{stab}_G(i)|$