



Figure 5.29: Transpositions in the motion group of a cube

Sage A permutation group is a very concrete representation of a group, and Sage support for permutations groups is very good — making Sage a natural place for beginners to learn about group theory.

5.3 Exercises

1. Write the following permutations in cycle notation.

(a)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$$

(c)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$$

(b)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$$

(d)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

2. Compute each of the following.

(a) $(1345)(234)$

(i) $(123)(45)(1254)^{-2}$

(b) $(12)(1253)$

(j) $(1254)^{100}$

(c) $(143)(23)(24)$

(k) $|(1254)|$

(d) $(1423)(34)(56)(1324)$

(l) $|(1254)^2|$

(e) $(1254)(13)(25)$

(m) $(12)^{-1}$

(f) $(1254)(13)(25)^2$

(n) $(12537)^{-1}$

(g) $(1254)^{-1}(123)(45)(1254)$

(o) $[(12)(34)(12)(47)]^{-1}$

(h) $(1254)^2(123)(45)$

(p) $[(1235)(467)]^{-1}$

3. Express the following permutations as products of transpositions and identify them as even or odd.

(a) (14356)

(d) $(17254)(1423)(154632)$

(b) $(156)(234)$

(e) (142637)

(c) $(1426)(142)$

4. Find $(a_1, a_2, \dots, a_n)^{-1}$.
5. List all of the subgroups of S_4 . Find each of the following sets:
 - (a) $\{\sigma \in S_4 : \sigma(1) = 3\}$
 - (b) $\{\sigma \in S_4 : \sigma(2) = 2\}$
 - (c) $\{\sigma \in S_4 : \sigma(1) = 3 \text{ and } \sigma(2) = 2\}$.

Are any of these sets subgroups of S_4 ?

6. Find all of the subgroups in A_4 . What is the order of each subgroup?
7. Find all possible orders of elements in S_7 and A_7 .
8. Show that A_{10} contains an element of order 15.
9. Does A_8 contain an element of order 26?
10. Find an element of largest order in S_n for $n = 3, \dots, 10$.
11. What are the possible cycle structures of elements of A_5 ? What about A_6 ?
12. Let $\sigma \in S_n$ have order n . Show that for all integers i and j , $\sigma^i = \sigma^j$ if and only if $i \equiv j \pmod{n}$.
13. Let $\sigma = \sigma_1 \cdots \sigma_m \in S_n$ be the product of disjoint cycles. Prove that the order of σ is the least common multiple of the lengths of the cycles $\sigma_1, \dots, \sigma_m$.
14. Using cycle notation, list the elements in D_5 . What are r and s ? Write every element as a product of r and s .
15. If the diagonals of a cube are labeled as Figure 5.26, to which motion of the cube does the permutation $(12)(34)$ correspond? What about the other permutations of the diagonals?
16. Find the group of rigid motions of a tetrahedron. Show that this is the same group as A_4 .
17. Prove that S_n is nonabelian for $n \geq 3$.
18. Show that A_n is nonabelian for $n \geq 4$.
19. Prove that D_n is nonabelian for $n \geq 3$.
20. Let $\sigma \in S_n$ be a cycle. Prove that σ can be written as the product of at most $n - 1$ transpositions.
21. Let $\sigma \in S_n$. If σ is not a cycle, prove that σ can be written as the product of at most $n - 2$ transpositions.
22. If σ can be expressed as an odd number of transpositions, show that any other product of transpositions equaling σ must also be odd.
23. If σ is a cycle of odd length, prove that σ^2 is also a cycle.
24. Show that a 3-cycle is an even permutation.
25. Prove that in A_n with $n \geq 3$, any permutation is a product of cycles of length 3.
26. Prove that any element in S_n can be written as a finite product of the following permutations.
 - (a) $(12), (13), \dots, (1n)$
 - (b) $(12), (23), \dots, (n-1, n)$
 - (c) $(12), (12 \dots n)$

27. Let G be a group and define a map $\lambda_g : G \rightarrow G$ by $\lambda_g(a) = ga$. Prove that λ_g is a permutation of G .
28. Prove that there exist $n!$ permutations of a set containing n elements.
29. Recall that the **center** of a group G is

$$Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}.$$

Find the center of D_8 . What about the center of D_{10} ? What is the center of D_n ?

30. Let $\tau = (a_1, a_2, \dots, a_k)$ be a cycle of length k .

(a) Prove that if σ is any permutation, then

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k))$$

is a cycle of length k .

(b) Let μ be a cycle of length k . Prove that there is a permutation σ such that $\sigma\tau\sigma^{-1} = \mu$.

31. For α and β in S_n , define $\alpha \sim \beta$ if there exists an $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$. Show that \sim is an equivalence relation on S_n .

32. Let $\sigma \in S_X$. If $\sigma^n(x) = y$, we will say that $x \sim y$.

(a) Show that \sim is an equivalence relation on X .

(b) If $\sigma \in A_n$ and $\tau \in S_n$, show that $\tau^{-1}\sigma\tau \in A_n$.

(c) Define the **orbit** of $x \in X$ under $\sigma \in S_X$ to be the set

$$\mathcal{O}_{x,\sigma} = \{y : x \sim y\}.$$

Compute the orbits of each of the following elements in S_5 :

$$\alpha = (1254)$$

$$\beta = (123)(45)$$

$$\gamma = (13)(25).$$

- (d) If $\mathcal{O}_{x,\sigma} \cap \mathcal{O}_{y,\sigma} \neq \emptyset$, prove that $\mathcal{O}_{x,\sigma} = \mathcal{O}_{y,\sigma}$. The orbits under a permutation σ are the equivalence classes corresponding to the equivalence relation \sim .
- (e) A subgroup H of S_X is **transitive** if for every $x, y \in X$, there exists a $\sigma \in H$ such that $\sigma(x) = y$. Prove that $\langle \sigma \rangle$ is transitive if and only if $\mathcal{O}_{x,\sigma} = X$ for some $x \in X$.
33. Let $\alpha \in S_n$ for $n \geq 3$. If $\alpha\beta = \beta\alpha$ for all $\beta \in S_n$, prove that α must be the identity permutation; hence, the center of S_n is the trivial subgroup.
34. If α is even, prove that α^{-1} is also even. Does a corresponding result hold if α is odd?
35. Show that $\alpha^{-1}\beta^{-1}\alpha\beta$ is even for $\alpha, \beta \in S_n$.
36. Let r and s be the elements in D_n described in Theorem 5.23

(a) Show that $srs = r^{-1}$.

(b) Show that $r^k s = sr^{-k}$ in D_n .

(c) Prove that the order of $r^k \in D_n$ is $n/\gcd(k, n)$.

Theorem 6.18 Euler’s Theorem. *Let a and n be integers such that $n > 0$ and $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

PROOF. By Theorem 6.17 the order of $U(n)$ is $\phi(n)$. Consequently, $a^{\phi(n)} = 1$ for all $a \in U(n)$; or $a^{\phi(n)} - 1$ is divisible by n . Therefore, $a^{\phi(n)} \equiv 1 \pmod{n}$. \square

If we consider the special case of Euler’s Theorem in which $n = p$ is prime and recall that $\phi(p) = p - 1$, we obtain the following result, due to Pierre de Fermat.

Theorem 6.19 Fermat’s Little Theorem. *Let p be any prime number and suppose that $p \nmid a$ (p does not divide a). Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for any integer b , $b^p \equiv b \pmod{p}$.

Sage Sage can create all the subgroups of a group, so long as the group is not too large. It can also create the cosets of a subgroup.

Historical Note

Joseph-Louis Lagrange (1736–1813), born in Turin, Italy, was of French and Italian descent. His talent for mathematics became apparent at an early age. Leonhard Euler recognized Lagrange’s abilities when Lagrange, who was only 19, communicated to Euler some work that he had done in the calculus of variations. That year he was also named a professor at the Royal Artillery School in Turin. At the age of 23 he joined the Berlin Academy. Frederick the Great had written to Lagrange proclaiming that the “greatest king in Europe” should have the “greatest mathematician in Europe” at his court. For 20 years Lagrange held the position vacated by his mentor, Euler. His works include contributions to number theory, group theory, physics and mechanics, the calculus of variations, the theory of equations, and differential equations. Along with Laplace and Lavoisier, Lagrange was one of the people responsible for designing the metric system. During his life Lagrange profoundly influenced the development of mathematics, leaving much to the next generation of mathematicians in the form of examples and new problems to be solved.

6.4 Exercises

1. Suppose that G is a finite group with an element g of order 5 and an element h of order 7. Why must $|G| \geq 35$?
2. Suppose that G is a finite group with 60 elements. What are the orders of possible subgroups of G ?
3. Prove or disprove: Every subgroup of the integers has finite index.
4. Prove or disprove: Every subgroup of the integers has finite order.
5. List the left and right cosets of the subgroups in each of the following.

(a) $\langle 8 \rangle$ in \mathbb{Z}_{24}	(e) A_n in S_n
(b) $\langle 3 \rangle$ in $U(8)$	(f) D_4 in S_4
(c) $3\mathbb{Z}$ in \mathbb{Z}	(g) \mathbb{T} in \mathbb{C}^*
(d) A_4 in S_4	(h) $H = \{(1), (123), (132)\}$ in S_4

6. Describe the left cosets of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$. What is the index of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$?
7. Verify Euler's Theorem for $n = 15$ and $a = 4$.
8. Use Fermat's Little Theorem to show that if $p = 4n + 3$ is prime, there is no solution to the equation $x^2 \equiv -1 \pmod{p}$.
9. Show that the integers have infinite index in the additive group of rational numbers.
10. Show that the additive group of real numbers has infinite index in the additive group of the complex numbers.
11. Let H be a subgroup of a group G and suppose that $g_1, g_2 \in G$. Prove that the following conditions are equivalent.

(a) $g_1H = g_2H$

(b) $Hg_1^{-1} = Hg_2^{-1}$

(c) $g_1H \subset g_2H$

(d) $g_2 \in g_1H$

(e) $g_1^{-1}g_2 \in H$

12. If $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$, show that right cosets are identical to left cosets. That is, show that $gH = Hg$ for all $g \in G$.
13. What fails in the proof of Theorem 6.8 if $\phi : \mathcal{L}_H \rightarrow \mathcal{R}_H$ is defined by $\phi(gH) = Hg$?
14. Suppose that $g^n = e$. Show that the order of g divides n .
15. Show that any two permutations $\alpha, \beta \in S_n$ have the same cycle structure if and only if there exists a permutation γ such that $\beta = \gamma\alpha\gamma^{-1}$. If $\beta = \gamma\alpha\gamma^{-1}$ for some $\gamma \in S_n$, then α and β are **conjugate**.
16. If $|G| = 2n$, prove that the number of elements of order 2 is odd. Use this result to show that G must contain a subgroup of order 2.
17. Suppose that $[G : H] = 2$. If a and b are not in H , show that $ab \in H$.
18. If $[G : H] = 2$, prove that $gH = Hg$.
19. Let H and K be subgroups of a group G . Prove that $gH \cap gK$ is a coset of $H \cap K$ in G .
20. Let H and K be subgroups of a group G . Define a relation \sim on G by $a \sim b$ if there exists an $h \in H$ and a $k \in K$ such that $hak = b$. Show that this relation is an equivalence relation. The corresponding equivalence classes are called **double cosets**. Compute the double cosets of $H = \{(1), (123), (132)\}$ in A_4 .
21. Let G be a cyclic group of order n . Show that there are exactly $\phi(n)$ generators for G .
22. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where p_1, p_2, \dots, p_k are distinct primes. Prove that

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

23. Show that

$$n = \sum_{d|n} \phi(d)$$

for all positive integers n .

$$\begin{aligned}
&= (h_1h_2, k_1k_2) \\
&= (h_1, k_1)(h_2, k_2) \\
&= \phi(g_1)\phi(g_2).
\end{aligned}$$

We will leave the proof that ϕ is one-to-one and onto as an exercise. \square

Example 9.28. The group \mathbb{Z}_6 is an internal direct product isomorphic to $\{0, 2, 4\} \times \{0, 3\}$.

We can extend the definition of an internal direct product of G to a collection of subgroups H_1, H_2, \dots, H_n of G , by requiring that

- $G = H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n : h_i \in H_i\}$;
- $H_i \cap \langle \cup_{j \neq i} H_j \rangle = \{e\}$;
- $h_ih_j = h_jh_i$ for all $h_i \in H_i$ and $h_j \in H_j$.

We will leave the proof of the following theorem as an exercise.

Theorem 9.29. Let G be the internal direct product of subgroups H_i , where $i = 1, 2, \dots, n$. Then G is isomorphic to $\prod_i H_i$.

Sage Sage can quickly determine if two permutation groups are isomorphic, even though this should, in theory, be a very difficult computation.

9.3 Exercises

1. Prove that $\mathbb{Z} \cong n\mathbb{Z}$ for $n \neq 0$.
2. Prove that \mathbb{C}^* is isomorphic to the subgroup of $GL_2(\mathbb{R})$ consisting of matrices of the form

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

3. Prove or disprove: $U(8) \cong \mathbb{Z}_4$.
4. Prove that $U(8)$ is isomorphic to the group of matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

5. Show that $U(5)$ is isomorphic to $U(10)$, but $U(12)$ is not.
6. Show that the n th roots of unity are isomorphic to \mathbb{Z}_n .
7. Show that any cyclic group of order n is isomorphic to \mathbb{Z}_n .
8. Prove that \mathbb{Q} is not isomorphic to \mathbb{Z} .
9. Let $G = \mathbb{R} \setminus \{-1\}$ and define a binary operation on G by

$$a * b = a + b + ab.$$

Prove that G is a group under this operation. Show that $(G, *)$ is isomorphic to the multiplicative group of nonzero real numbers.

10. Show that the matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

form a group. Find an isomorphism of G with a more familiar group of order 6.

11. Find five non-isomorphic groups of order 8.
12. Prove S_4 is not isomorphic to D_{12} .
13. Let $\omega = \text{cis}(2\pi/n)$ be a primitive n th root of unity. Prove that the matrices

$$A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

generate a multiplicative group isomorphic to D_n .

14. Show that the set of all matrices of the form

$$\begin{pmatrix} \pm 1 & k \\ 0 & 1 \end{pmatrix},$$

is a group isomorphic to D_n , where all entries in the matrix are in \mathbb{Z}_n .

15. List all of the elements of $\mathbb{Z}_4 \times \mathbb{Z}_2$.
16. Find the order of each of the following elements.
 - (a) $(3, 4)$ in $\mathbb{Z}_4 \times \mathbb{Z}_6$
 - (b) $(6, 15, 4)$ in $\mathbb{Z}_{30} \times \mathbb{Z}_{45} \times \mathbb{Z}_{24}$
 - (c) $(5, 10, 15)$ in $\mathbb{Z}_{25} \times \mathbb{Z}_{25} \times \mathbb{Z}_{25}$
 - (d) $(8, 8, 8)$ in $\mathbb{Z}_{10} \times \mathbb{Z}_{24} \times \mathbb{Z}_{80}$
17. Prove that D_4 cannot be the internal direct product of two of its proper subgroups.
18. Prove that the subgroup of \mathbb{Q}^* consisting of elements of the form $2^m 3^n$ for $m, n \in \mathbb{Z}$ is an internal direct product isomorphic to $\mathbb{Z} \times \mathbb{Z}$.
19. Prove that $S_3 \times \mathbb{Z}_2$ is isomorphic to D_6 . Can you make a conjecture about D_{2n} ? Prove your conjecture.
20. Prove or disprove: Every abelian group of order divisible by 3 contains a subgroup of order 3.
21. Prove or disprove: Every nonabelian group of order divisible by 6 contains a subgroup of order 6.
22. Let G be a group of order 20. If G has subgroups H and K of orders 4 and 5 respectively such that $hk = kh$ for all $h \in H$ and $k \in K$, prove that G is the internal direct product of H and K .
23. Prove or disprove the following assertion. Let G , H , and K be groups. If $G \times K \cong H \times K$, then $G \cong H$.
24. Prove or disprove: There is a noncyclic abelian group of order 51.
25. Prove or disprove: There is a noncyclic abelian group of order 52.
26. Let $\phi: G \rightarrow H$ be a group isomorphism. Show that $\phi(x) = e_H$ if and only if $x = e_G$, where e_G and e_H are the identities of G and H , respectively.
27. Let $G \cong H$. Show that if G is cyclic, then so is H .
28. Prove that any group G of order p , p prime, must be isomorphic to \mathbb{Z}_p .

29. Show that S_n is isomorphic to a subgroup of A_{n+2} .
30. Prove that D_n is isomorphic to a subgroup of S_n .
31. Let $\phi : G_1 \rightarrow G_2$ and $\psi : G_2 \rightarrow G_3$ be isomorphisms. Show that ϕ^{-1} and $\psi \circ \phi$ are both isomorphisms. Using these results, show that the isomorphism of groups determines an equivalence relation on the class of all groups.
32. Prove $U(5) \cong \mathbb{Z}_4$. Can you generalize this result for $U(p)$, where p is prime?
33. Write out the permutations associated with each element of S_3 in the proof of Cayley's Theorem.
34. An **automorphism** of a group G is an isomorphism with itself. Prove that complex conjugation is an automorphism of the additive group of complex numbers; that is, show that the map $\phi(a + bi) = a - bi$ is an isomorphism from \mathbb{C} to \mathbb{C} .
35. Prove that $a + ib \mapsto a - ib$ is an automorphism of \mathbb{C}^* .
36. Prove that $A \mapsto B^{-1}AB$ is an automorphism of $SL_2(\mathbb{R})$ for all B in $GL_2(\mathbb{R})$.
37. We will denote the set of all automorphisms of G by $\text{Aut}(G)$. Prove that $\text{Aut}(G)$ is a subgroup of S_G , the group of permutations of G .
38. Find $\text{Aut}(\mathbb{Z}_6)$.
39. Find $\text{Aut}(\mathbb{Z})$.
40. Find two nonisomorphic groups G and H such that $\text{Aut}(G) \cong \text{Aut}(H)$.
41. Let G be a group and $g \in G$. Define a map $i_g : G \rightarrow G$ by $i_g(x) = gxg^{-1}$. Prove that i_g defines an automorphism of G . Such an automorphism is called an **inner automorphism**. The set of all inner automorphisms is denoted by $\text{Inn}(G)$.
42. Prove that $\text{Inn}(G)$ is a subgroup of $\text{Aut}(G)$.
43. What are the inner automorphisms of the quaternion group Q_8 ? Is $\text{Inn}(G) = \text{Aut}(G)$ in this case?
44. Let G be a group and $g \in G$. Define maps $\lambda_g : G \rightarrow G$ and $\rho_g : G \rightarrow G$ by $\lambda_g(x) = gx$ and $\rho_g(x) = xg^{-1}$. Show that $i_g = \rho_g \circ \lambda_g$ is an automorphism of G . The isomorphism $g \mapsto \rho_g$ is called the **right regular representation** of G .
45. Let G be the internal direct product of subgroups H and K . Show that the map $\phi : G \rightarrow H \times K$ defined by $\phi(g) = (h, k)$ for $g = hk$, where $h \in H$ and $k \in K$, is one-to-one and onto.
46. Let G and H be isomorphic groups. If G has a subgroup of order n , prove that H must also have a subgroup of order n .
47. If $G \cong \overline{G}$ and $H \cong \overline{H}$, show that $G \times H \cong \overline{G} \times \overline{H}$.
48. Prove that $G \times H$ is isomorphic to $H \times G$.
49. Let n_1, \dots, n_k be positive integers. Show that

$$\prod_{i=1}^k \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 \cdots n_k}$$

if and only if $\gcd(n_i, n_j) = 1$ for $i \neq j$.

50. Prove that $A \times B$ is abelian if and only if A and B are abelian.
51. If G is the internal direct product of H_1, H_2, \dots, H_n , prove that G is isomorphic to $\prod_i H_i$.
52. Let H_1 and H_2 be subgroups of G_1 and G_2 , respectively. Prove that $H_1 \times H_2$ is a subgroup of $G_1 \times G_2$.