MTH 203: Introduction to Groups and Symmetry
Semester 1, 2022-23

November 4, 2022

Contents

1 Groups - An introduction

The presentation from the first lecture is available here.

1.1 Basic definitions and examples

(i) A group $(G,\cdot)$ is a nonempty set G with a binary operation $\cdot$ satisfying the properties:

(a) (Closure property) For any $a,b\in G$, we have $a\cdot b\in G$.

(b) (Associativity) For any $a,b,c\in G$, we have

$$a\cdot(b\cdot c)=(a\cdot b)\cdot c.$$

(c) (Existence of identity) There exists an element $e\in g$ called the *identity element* such that

$$a\cdot e=a=e\cdot a,$$

for any $a\in G$.

(d) (Existence of inverse) For each $a\in G$, there exists an $a^{-1}\in G$ such that

$$a\cdot a^{-1}=e=a^{-1}\cdot a.$$

(ii) In a group $(G,\cdot)$ as above, the following properties hold:

(a) (Right cancellation law) For $a,b,c\in G$, if $a\cdot c=b\cdot c$, then $a=b$.

(b) (Left cancellation law) For $a,b,c\in G$, if $c\cdot a=c\cdot b$, then $a=b$.

(c) The identity e is unique.

(d) Every element $a\in G$ has a unique inverse a^{-1}.

(iii) Examples of groups:

(a) For $n\geq 3$, the Dihedral group D_{2n} - the group of symmetries of a regular n-gon is a group comprising n reflections and and n rotations, where the operation is composition (See presentation at the beginning of Section 1).

(b) Additive groups: $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, and

$$M_n(X)=\{(a_{ij})_{n\times n}\,|\,a_{ij}\in X\},\text{ for }X=\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}.$$

(c) The group $C_n = \{e^{2\pi k/n} : 0 \leq k \leq n-1\}$ of complex n^{th} roots of unity. This is group can also be viewed as the group of rotations of a regular n-gon or the group of symmetries of a space of n equidistantly marked point on a circle.

(d) For a fixed $n \in \mathbb{N}$, define a relation $\sim$ on $\mathbb{Z}$ by

$$x \sim y \iff n \mid x - y.$$

Then $\sim$ defines an equivalence relation on $\mathbb{Z}$ whose equivalence classes are denoted by

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

The set $\mathbb{Z}_n$ forms a group under the operation

$$[x] + [y] = [x + y]$$

known as the *group of residue classes of integers modulo n*. This group is an additive version of the group described in (c).

(e) Multiplicative groups: $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, and the *general linear group*

$$\mathrm{GL}(n, X) = \{A = (a_{ij})_{n \times n} \mid a_{ij} \in X \text{ and } \det(A) \neq 0\}, \text{ for } X = \mathbb{Q}, \mathbb{R}, \mathbb{C}.$$

(f) The group of symmetries (or rigid motions) $\mathrm{Sym}(\mathbb{R}^2)$ of $\mathbb{R}^2$ has infinitely may elements, which fall into four broad types:

(a) Translation by a vector.

(b) Rotation about a point.

(c) Reflection about a line.

(d) Glide reflection about a line (i.e a reflection about a line followed by a translation by a vector parallel to the line).

Symmetries of type (a) and (b) are said to be *orientation-preserving*, as they do not flip the plane over), while symmetries of type (c) and (d) are called *orientation-reversing* symmetries (see Figure 1 below).

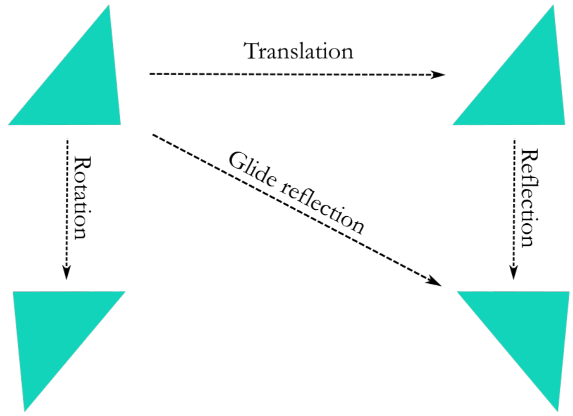


Figure 1: The symmetries of the plane.

(iv) Let $(G, \cdot)$ be a group. A subset $H \subset G$ is called a *subgroup* of G (written as $H < G$), if $(H, \cdot)$ is a group.

(v) Examples of subgroups.

(a) $n\mathbb{Z} < \mathbb{Z}$, for every $n \in \mathbb{Z}$.

(b) $M_n(k\mathbb{Z}) < M_n(\mathbb{Z})$, for every $n \in \mathbb{Z}$.

(c) Consider the *special linear group*

$$\mathrm{SL}(n, X) = \{A = (a_{ij})_{n\times n} \,|\, \det(A) = 1\}, \text{ for } X = \mathbb{Q}, \mathbb{R}, \mathbb{C}.$$

Then $\mathrm{SL}(n, X) < \mathrm{GL}(n, X)$.

(vi) Let G be a group. A subgroup $H < G$ is said to be *proper* if $H \neq \{1\}$ or G.

(vii) (The subgroup criterion). Let G be a group, and let $H \subset G$. Then $H < G$ if, and only if, for every pair of elements $g, h \in H$, the product $gh^{-1} \in H$. In particular, if $|G| < \infty$, then a subset $H \subset G$ is a subgroup if, and only if, H is closed under the operation in G.

(viii) A group G is said to be *abelian* if $ab = ba$, for all $a, b \in G$ (i.e. if the group operation is commutative).

(ix) Examples of abelian (and nonabelian) groups.

(a) All additive groups are abelian groups.

(b) A vector space is an abelian group with respect to vector addition.

(c) The multiplicative groups $(\mathbb{Q}^{\times}, \cdot)$, $(\mathbb{R}^{\times}, \cdot)$, and $(\mathbb{C}^{\times}, \cdot)$ are abelian groups.

(d) The group D_{2n}, for $n \geq 3$, is non-abelian, as a reflection never commutes with a rotation.

(e) The groups $\mathrm{GL}(n, F)$ and $\mathrm{SL}(n, F)$ are non-abelian groups, as matrix multiplication is non-commutative.

1.2 Order of an element

(i) A groups $(G, \cdot)$ is said to be *finite*, if G is a finite set. If G is not a finite group, then G said to be a *infinite group*.

(ii) The *order* of a finite group (denoted by $|G|$) is the number of elements in it.

(iii) Examples of finite and infinite groups.

  (a) The groups C_n and $\mathbb{Z}_n$ ($|C_n| = |\mathbb{Z}_n| = n$), and D_{2n} ($|D_{2n}| = 2n$) are finite groups.

  (b) The groups $\mathbb{Z}$, $\mathrm{GL}(n, F)$, the symmetries of a circle, and the symmetries of $\mathbb{R}^2$ are infinite groups.

(iv) The *order of an element* $g \in G$ (denoted by $o(g)$) is the smallest positive integer m such that $g^m = 1$. If such an n does not exist for a $g \in G$, then g is said to be of *infinite order*.

(v) In a finite group, every element has finite order. However, an infinite can have elements of finite order.

(vi) Let G be a group, and let $g \in G$ with $o(g) = n$. If $g^m = 1$, for some m. Then $n \mid m$.

(vii) Let G be a group, and let $g \in G$ with $o(g) = n$. Then

$$o(g^k) = \frac{n}{\gcd(k, n)}.$$

(viii) Examples of elements with finite and infinite orders.

(a) In any group of symmetries, a reflection will always have order 2. For example, in D_{2n}, $o(s) = 2$, and the same holds for the reflexive symmetries of $\mathbb{R}^2$.

(b) In D_{2n}, $o(r^k) = n/\gcd(k,n)$, for $0 \le k \le n-1$.

(c) In C_n (resp. $\mathbb{Z}_n$), $o(e^{i2\pi k/n})$(resp. $o([k]) = n/\gcd(k,n)$, for $0 \le k \le n-1$.

1.3 Generating set for a group

(i) Let G be group and $S \subset G$. Then S is a *generating set for G* (denoted by $G = \langle S \rangle$) if every element in G can be expressed as a finite product of powers of elements in S and their inverses.

(ii) Examples of generating sets for groups.

(a) The group $\mathbb{Z}$ is generated by the sets $\{-1,1\}$ and $\{1\}$.

(b) The group C_n is generated by $\{e^{i2\pi/n}\}$, while the group $\mathbb{Z}_n$ is generated by $\{[1]\}$.

(c) The group D_{2n} is generated by a rotation r (by $2\pi/n$) and a reflection s. In fact, the elements of the group may be enumerated as:

$$D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\},$$

where r and s satisfy the relation

$$sr^k = r^{n-k}s, \text{ for } 0 \le k \le n-1.$$

(d) The group symmetries of $\mathbb{R}^2$ is not finitely generated.

1.4 Cyclic groups

(i) A group G is said to be *cyclic*, if there exists a $g \in G$ such that $G = \langle \{g\} \rangle$. In other words, G is cyclic, if its generated by a single element in G.

(ii) Let $G = \langle g \rangle$ be a cyclic group.

(a) If G is of order n (also denoted by C_n), then

$$G = \{1, g, g^2, \dots, g^{n-1}\}.$$

This group is analogous (or isomorphic) to the groups $\mathbb{Z}_n$ and C_n via the association $g^i \mapsto [i]$.

(b) If G is of infinite order, then

$$G = \{1, g^{\pm 1}, g^{\pm 2}, \ldots\}.$$

This group is analogous (or isomorphic) to the group $\mathbb{Z}$ via the association $g^i \mapsto i$.

(iii) Every subgroup of a cyclic group is cyclic.

(iv) Let $G = \langle g \rangle$ be a cyclic group.

(a) If $o(g) = \infty$, then every proper subgroup of G is of the form $\langle g^k \rangle$, for $k \in \mathbb{Z}^+ \setminus \{1\}$.

(b) If $o(g) = n$, then every proper subgroup of G is of the form $\langle g^{n/d} \rangle$, where d is any proper divisor of n.

(v) Consider an element $[k] \in \mathbb{Z}_n$. Then the following statements are equivalent.

(a) $[k]$ generates $\mathbb{Z}_n$.

(b) $\gcd(k, n) = 1$.

(c) $o([k]) = n$.

2 Cosets and the Lagrange's Theorem

2.1 Cosets - Basic definitions and examples

(i) Let G be a group and $H \leq G$. Then a *left coset of H in G* is given by

$$gH = \{gh \mid h \in H\},$$

and a *right coset of H in G* is given by

$$Hg = \{hg \mid h \in H\}.$$

(ii) Let G be a group, and let $H < G$. Then for $x, y \in G$, the following statements are equivalent:

(a) $xH = yH$.

(b) $y^{-1}x \in H$.

(c) $y^{-1}xH = H$.

(iii) Let G be a group and $H \leq G$. Then the relation $\sim_H$ on G defined by

$$x \sim_H y \iff y^{-1}x \in H$$

is an equivalence relation. The set of equivalence classes $G/\sim_H$ under this relations are precisely the distinct left cosets of H in G. Hence, any two left cosets of H in G are either identical or totally disjoint.

(iv) The set of all distinct left (resp. right) cosets of H in G is denoted by G/H (resp. $H\backslash G$).

(v) Examples of cosets.

(a) $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$.

(b) $D_{2n}/\langle r\rangle = \{\langle r\rangle, D_{2n} - \langle r\rangle\}$.

2.2 The Lagrange's theorem

(i) There is bijective correspondence between any two distinct left cosets (or right cosets) of H in G.

(ii) For any $g \in G$, there is a bijective correspondence between the cosets gH and Hg^{-1}. Consequently, there is a bijective correspondence between the sets G/H and $H\backslash G$.

(iii) Let G be a finite group, and let $H < G$. Then the *index* $[G : H]$ *of* H *in* G is defined by

$$[G : H] := |G/H| = |H\backslash G|.$$

(iv) Lagrange's Theorem: Let G be a finite group, and let $H < G$. Then

$$|G| = |H|[G : H],$$

and consequently $|H| \mid |G|$.

2.3 Applications of the Lagrange's Theorem

(i) Every group of prime order is cyclic.

(ii) Let G be a finite group with $|G| = n$, and let $g \in G$. Then $o(g) \mid n$, and consequently $g^n = 1$.

(iii) The set $U_n = \{[k] \in \mathbb{Z}_n \,|\, \gcd(k,n) = 1\}$ forms an abelian group under the multiplication operation defined by $[a][b] = [ab]$ called the *multiplicative group of integers modulo n*.

(iv) Examples of multiplicative groups of integers.

   (a) The group $U_8 = \{[1],[3],[5],[7]\}$ is a noncyclic group of order 2, as every non-identity element is of order 2. In fact, every non-cyclic group of order 4 is analogous to U_8.

   (b) The groups U_5, U_7, and U_{11} are cyclic. (In fact, it is known U_n is cyclic if and only if $n = 2, 4, p^n$, or $2p^n$, for some odd prime p. The proof of this fact requires the Chinese Reminder Theorem.)

(v) The function $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ defined by $\phi(n) = |U_n|$ is called the *Euler totient function or the Euler ϕ-function.* In particular, for a prime p, $\phi(p) = p - 1$.

(vi) Euler's Theorem: If a and n are positive integers such that $\gcd(a,n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

(vii) Fermat's Little Theorem: If p is a prime number and a is a positive integer, then

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

3 Normal subgroups and homomorphisms

3.1 Normal subgroups

(i) Let G be a group and $N < G$. Then N is said to be a *normal subgroup of G* (denoted by $N \lhd G$) if $gNg^{-1} \subset N$, for all $g \in G$.

(ii) Examples of normal subgroups.

(a) Every subgroup of an abelian group is normal.

(1) $C_n \lhd \mathbb{C}^\times$, for $n \geq 2$.

(2) $m\mathbb{Z} \lhd \mathbb{Z}$, for all $m \in \mathbb{Z}$

(b) $\mathrm{SL}(n, F) \lhd \mathrm{GL}(n, F)$, for $n \geq 2$.

(iii) The G be a group, and $N < G$. Then the following statements are equivalent.

(a) $N \lhd G$.

(b) $gNg^{-1} = N$, for all $g \in G$.

(c) $gN = Ng$, for all $g \in G$.

(d) $(gN)(hN) = ghN$, for all $g, h \in G$.

(iv) The G be a group, and $N \lhd G$. Then G/N forms a group under the operation $(gN)(hN) = ghN$.

(v) Let G be a group. The *center Z(G) of G* is defined by

$$Z(G) = \{g \in G : gh = hg, \forall h \in H\}.$$

(vi) Let G be a group. Then $Z(G) \lhd G$.

3.2 Homomorphisms

(i) Let $(G, \cdot)$ and $(H, *)$ be groups. A function $\varphi : G \to H$ is said to be a *homomorphism* if

$$\varphi(g \cdot h) = \varphi(g) * \varphi(h),$$

for all $g, h \in G$.

(ii) Examples of homomorphisms:

(a) The *trivial homomophism* $e : G \to H$ given by $e(x) = 1$, for all $x \in G$.

(b) The *identity homomorphism* $i : G \to G$ given by $i(g) = g$, for all $g \in G$.

(c) The map $\alpha_n : \mathbb{Z} \to \mathbb{Z}$ defined by $\alpha_n(x) = nx$.

(d) The map $\beta_n : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\beta_n(x) = [x]$.

(e) The determinant map $\mathrm{Det} : \mathrm{GL}(n, \mathbb{C}) \to \mathbb{C}^\times$.

(f) The map $T : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ defined by $T(A) = A^\intercal$.

(g) The pair of maps $\gamma_\pm : M_n(\mathbb{R}) \to M_n(\mathbb{R})$ defined by

$$\gamma_\pm(A) = \frac{1}{2}(A \pm A^\intercal).$$

(h) The map $\psi : \mathbb{R} \to \mathbb{C}^\times$ defined by $\psi(x) = e^{ix}$.

(iii) Let $\varphi : G \to H$ be a homomorphism.

(a) If φ is injective, then it is called a *monomorphism* (denoted by $\varphi : G \hookrightarrow H$).

(b) If φ is surjective, then it is called an *epimorphism*.

(c) If φ is bijective, then it is called an *isomorphism*, and we say that *G is isomorphic to H*, denoted by $G \cong H$.

(iv) Let $\varphi : G \to H$ be a homomorphism. Then:

(a) $\varphi(1) = 1$.

(b) $\varphi(g^{-1}) = \varphi(g)^{-1}$, for all $g \in G$.

(v) Let $\varphi : G \to H$ be a homomorphism. Then:

(a) The set $\ker\varphi = \{g \in G : \varphi(g) = 1\}$ is called the *kernel of φ*.

(b) The set $\operatorname{Im}\varphi = \{\varphi(g) : g \in G\}$ is called the *image of φ*.

(vi) Let $\varphi : G \to H$ be a homomorphism. Then

(a) $\ker\varphi \lhd G$.

(b) $\operatorname{Im}\varphi < H$.

(vii) Let $\varphi : G \to H$ be a homomorphism. Then the following statements are equivalent:

(a) φ is a monomorphism.

(b) $G \cong \operatorname{Im}\varphi$.

(c) $\ker\varphi = \{1\}$.

If in addition we assume that G, H are finite, then the above statements are equivalent to φ being *order-preserving*, that is, $o(g) = o(\varphi(g))$, for all $g \in G$.

(viii) Let G be a group.

(a) An isomorphism $\varphi : G \to G$ is called an *automorphism* of G.

(b) The set
$$\mathrm{Aut}(G) := \{\varphi : G \to G \,|\, \varphi \text{ is an isomorphism}\}$$
forms a group under composition called the *automorphism group of* G.

(ix) $\mathrm{Aut}(\mathbb{Z}_n) \cong U_n$.

3.3 The Isomorphism Theorems

(i) Let G be a group, and $N \lhd G$. Then the quotient map $q : G \to G/N$ given by $q(g) = gN$ is an epimorphism.

(ii) First Isomorphism Theorem: Let G, H be groups, and $\varphi : G \to H$ is a homomorphism. Then
$$G/\ker\varphi \cong \mathrm{Im}\,\varphi.$$
In particular, if φ is onto, then
$$G/\ker\varphi \cong H.$$

(iii) Implications of First isomorphism theorem.

(a) The map $\mathrm{Det} : \mathrm{GL}(n, F) \to F^{\times}$ is an epimorphism whose kernel is given by
$$\ker(\mathrm{Det}) = \{A \in \mathrm{GL}(n, F) : \mathrm{Det}(A) = 1\} = \mathrm{SL}(n, F).$$
Therefore, the First isomorphism theorem implies that
$$\mathrm{GL}(n, F)/\mathrm{SL}(n, F) \cong F^{\times}.$$

(b) For $n \geq 2$, the map $\beta_n : \mathbb{Z} \to \mathbb{Z}_n$ is an epimorphism whose kernel is given by
$$\ker\beta_n = \{x \in \mathbb{Z} : \beta_n(x) = [x] = [0]\} = n\mathbb{Z}.$$
Therefore, the First isomorphism Theorem implies that
$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

(c) The map

$$\varphi : \mathbb{R} \to S^1 = \{z \in \mathbb{C} : |z| = 1\} : x \overset{\varphi}{\longmapsto} e^{i2\pi x}$$

is an epimorphism whose kernel is given by

$$\ker \varphi = \{x \in \mathbb{R} : \varphi(x) = \cos(2\pi x) + i \sin(2\pi x) = 1\} = \mathbb{Z}.$$

Therefore, the First isomorphism theorem implies that

$$\mathbb{R}/\mathbb{Z} \cong S^1.$$

(iv) Let G be a group, $H < G$, and $N \lhd G$. Then

(a) $H \cap N \lhd H$.

(b) $N \lhd HN$.

(v) Second Isomorphism Theorem: Let G be a group, $H < G$, and $N \lhd G$. Then

$$H/H \cap N \cong HN/N.$$

(vi) Third Isomorphism Theorem: Let G be group, and $H, K \lhd G$ such that $H < K$. Then

$$(G/H)/(K/H) \cong G/K.$$

(vii) Some applications of the Third isomorphism theorem.

(a) For positive integers ℓ, m, n such that $m \mid \ell$ and $n \mid m$, we know that

$$\ell\mathbb{Z} \lhd n\mathbb{Z}, m\mathbb{Z} \lhd n\mathbb{Z} \text{ and } \ell\mathbb{Z} < m\mathbb{Z}.$$

Therefore, the Third Isomorphism Theorem implies that

$$(n\mathbb{Z}/\ell\mathbb{Z})/(m\mathbb{Z}/\ell\mathbb{Z}) \cong n\mathbb{Z}/m\mathbb{Z},$$

or equivalently, we have

$$\mathbb{Z}_{\ell/n}/\mathbb{Z}_{\ell/m} \cong \mathbb{Z}_{m/n}.$$

(b) Consider the group D_{2n}, when n is even and $n \geq 4$. Then we know that

$$\langle r^{n/2} \rangle \lhd D_{2n}, \langle r \rangle \lhd D_{2n}, \text{ and } \langle r^{n/2} \rangle < \langle r \rangle.$$

Therefore, the Third isomorphism Theorem implies that

$$(D_{2n}/\langle r^{n/2} \rangle)/(\langle r \rangle/\langle r^{n/2} \rangle) \cong D_{2n}/\langle r \rangle.$$

4 Direct products of groups

4.1 Basic properties

(i) Given two groups G and H, consider the cartesian product $G \times H$ with a binary operation given by

$$(g_1, h_2)(g_2, h_2) = (g_1 g_2, h_1 h_2), \text{ for all } g_1, g_2 \in G \text{ and } h_1, h_2 \in H.$$

Under this operation, the set $G \times H$ forms a group with identity element $(1, 1)$ and the inverse of $(g, h) \in G \times H$ is given by (g^{-1}, h^{-1}). The group $G \times H$ is called the *external direct product (or the direct product)* of the groups G and H.

(ii) The notion of a direct product of two groups can be extended to define the direct product of n groups G_i, $1 \leq i \leq n$, denoted by

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \ldots \times G_n.$$

If in the product above each $G_i = G$, then the product is simply denoted by G^n.

(iii) The groups G and H inject into the $G \times H$, via the natural monomorphisms

$$G \hookrightarrow G \times H : g \mapsto (g, 1)$$
$$H \hookrightarrow G \times H : h \mapsto (1, h)$$

(iv) For any two groups G and H, the natural homomorphism

$$G \times H \to H \times G : (g, h) \mapsto (h, g)$$

is an isomorphism, and hence we have that

$$G \times H \cong H \times G.$$

In other words, up to isomorphism, the direct product of two groups is commutative.

(v) For any three groups G, H, and K, the natural homomorphism

$$(G \times H) \times K \to (G \times H) \times K : ((g, h), k) \mapsto (g, (h, k))$$

is an isomorphism, and hence we have that

$$G \times (H \times K) \cong (G \times H) \times K.$$

In other words, up to isomorphism, the direct product of three groups is associative.

4.2 Direct products of abelian groups

(i) A direct product $\prod_{i=1}^{n} G_i$ of groups is abelian, if and only if, each component group G_i is abelian.

(ii) Example of direct products that are abelian (or non-abelian).

(a) For any positive integer r, the group

$$\mathbb{Z}^r = \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{r\ times}$$

is an abelian group.

(b) For positive integers $n_1, \ldots n_k$, the group

$$\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$$

is an abelian group.

(c) The direct product of D_{2m}, for $m \geq 4$ with any abelian group will yield a non-abelian group.

(iii) Let $m, n \geq 2$ be positive integers. Then

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$$

if and only is $\gcd(m, n) = 1$.

(iv) Chinese Remainder Theorem: Let N be a positive integer such that $N = p_1^{r_1} \ldots p_k^{r_k}$, where the p_i are distinct primes and the r_i are positive integers. Then

$$\mathbb{Z}_N \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_k^{r_k}}.$$

(v) Examples of the Chinese Remainder Theorem.

   (a) $\mathbb{Z}_{120} \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_8$.
   (b) For positive integers $m, n \geq 2$, $\mathbb{Z}_{n^m} \ncong \mathbb{Z}_n^m$.

(vi) Classification of finitely generated abelian groups: Every finitely generated abelian group is isomorphic to a group of the form

$$\mathbb{Z}^r \times \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_k^{r_k}}, \qquad (*)$$

where r and the $r_i \geq 1$ are positive integers, and the p_i are (not necessarily distinct) primes.

(vii) Let G be a finitely generated abelian group which has a direct product decomposition of the form (*) above.

   (a) The component $\mathbb{Z}^r$ is the called *free part*, and the component $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_k^{r_k}}$ is called the *torsion* part of the direct product decomposition of G.
   (b) The integer r is called *rank* of G.

(viii) Examples of finitely generated abelian groups.

   (a) Up to isomorphism, there are three abelian groups of order 8, namely

$$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \text{ and } \mathbb{Z}_2^3.$$

   (b) Up to isomorphism, there is a unique abelian group of order 15, which is

$$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5.$$

   (c) In general, given distinct primes $p_1, \ldots, p_k$, there exists a unique abelian group of order $p_1 p_2 \ldots p_k$ up to isomorphism, which is $\mathbb{Z}_{p_1 p_2 \ldots p_k}$.

5 The symmetric group

5.1 Basic definitions and examples

(i) Let X be a nonempty set. Then the set of permutations (or self-bijections) of X defined by

$$S(X) := \{f : X \to X : f \text{ is a bijection}\}$$

forms a group under composition called the *symmetric group of X.*

(ii) When $|X| = n$, without loss of generality, we take $X = \{1,2,\ldots,n\}$, and we denote the group $S(X)$ simply by S_n. The group S_n, of order $n!$, is called the *symmetric group (or the permutation group) on n letters.*

(iii) Examples of symmetric groups.

(a) $S_2 \cong \mathbb{Z}_2$.

(b) Since each symmetry of a regular n-gon induces a permutation of its n vertices, we have $S_3 \cong D_6$ and in general, $D_{2n} < S_n$ for $n \geq 4$.

(c) For $n \geq 4$, S_n is a non-abelian group.

(d) For any group G, $\mathrm{Aut}(G) < S(G)$, since each automorphism is a bijective map.

(e) Given any group G and fixed $g \in G$, consider $\varphi_g : G \to G$ defined by $\varphi_g(h) = gh$, for all $h \in G$ (i.e., left multiplication by the element g). Then it is apparent that $\varphi_g \in S(G)$, and consequently, the map

$$\psi : G \to S(G) : g \overset{\psi}{\longmapsto} \varphi_g$$

is a monomorphism. In particular, if $|G| = n$, then G imbeds into S_n (i.e. $G \hookrightarrow S_n$).

(iv) A typical element $\sigma \in S_n$ is a bijection $\sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$, so we often denote such a σ by

$$\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

To further simplify notation for σ, we only list the values of σ on the subset $\{i \in \{1,2,\ldots,n\} : \sigma(i) \neq i\}$. For example, the permutation $\sigma \in S_5$ given by

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

is simply written as

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

(v) A product $\sigma_1\sigma_2$ of two permutations $\sigma_1, \sigma_2 \in S_n$ is defined as the permutation

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ (\sigma_1 \circ \sigma_2)(1) & (\sigma_1 \circ \sigma_2)(2) & \dots & (\sigma_1 \circ \sigma_2)(n-1) & (\sigma_1 \circ \sigma_2)(n) \end{pmatrix}.$$

(vi) The *support* of a permutation $\sigma \in S_n$ is defined by

$$\operatorname{supp}(\sigma) := \{i \in \{1, \dots, n\} : \sigma(i) \neq i\}.$$

(vii) Two permutations $\sigma_1, \sigma_2 \in S_n$ are said to be *disjoint* if

$$\operatorname{supp}(\sigma_1) \cap \operatorname{supp}(\sigma_2) = \emptyset.$$

(viii) Any two disjoint permutations in S_n commute.

5.2 k-cycles

(i) A *k-cycle* in S_n is a permutation of the form

$$\begin{pmatrix} i_1 & i_2 & \dots & i_{k-1} & i_k \\ i_2 & i_3 & \dots & i_k & i_1 \end{pmatrix},$$

where $1 \leq k \leq n$. A k-cycle as above is often denoted by

$$(i_1\, i_2 \dots i_k).$$

A 2-cycle in S_n is a called a *transposition (or an inversion).*

(ii) Consider the k-cycle $\sigma = (i_1\, i_2 \dots i_k)$ in S_n. Then we have:

(a)
$$\sigma = (i_1\ \sigma(i_1)\ \sigma^2(i_1) \dots \sigma^{k-1}(i_1)), \text{ and}$$

(b) $o(\sigma) = k$.

(iii) Example of k-cycles.

(a) The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \in S_5$$

is a 3-cycle given by $(1\,2\,3)$.

(b) The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \in S_4$$

is a 2-cycle (transposition) given by $(2\,3)$.

(iv) Two cycles $(i_1\, i_2 \dots i_k), (j_1\, j_2 \dots j_\ell) \in S_n$ commute if

$$\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_\ell\} = \emptyset.$$

(v) Every k-cycle is a product of no less than $k-1$ transpositions. In particular, for a k-cycle $(i_1\, i_2 \dots i_k) \in S_n$, we have

$$(i_1\, i_2 \dots i_k) = (i_1\, i_k)(i_1\, i_{k-1}) \dots (i_1\, i_2).$$

(vi) Every permutation $\sigma \in S_n$ can be expressed uniquely as a product of disjoint cycles. This is called the *unique cycle decomposition* of the permutation σ.

5.3 Parity of a permutation

(i) Suppose that the unique cycle decomposition of a permutation $\sigma \in S_n$ is given by

$$\sigma = \sigma_1 \sigma_2 \dots \sigma_{k_\sigma},$$

where each σ_i is an m_i-cycle. Then we define

$$N(\sigma) := \sum_{i=1}^{k_\sigma} (m_i - 1).$$

(ii) The *sign (or parity)* of a permutation $\sigma \in S_n$ is defined by

$$\operatorname{sgn}(\sigma) := (-1)^{N(\sigma)}.$$

(iii) A permutation $\sigma \in S_n$ is called an:

(a) *even permutation*, if $\operatorname{sgn}(\sigma) = 1$.

(b) *odd permutation*, if $\operatorname{sgn}(\sigma) = -1$.

(iv) Let $A_n = \{\sigma \in S_n : \text{sgn} = 1\}$. For $n \geq 2$, the map

$$\tau : S_n \to \{\pm 1\}(= \mathbb{Z}_2) : \sigma \overset{\tau}{\mapsto} \text{sgn}(\sigma)$$

is an epimorphism with $\ker \tau = A_n$. Thus, we have

$$S_n / A_n \cong \mathbb{Z}_2.$$

Consequently, $A_n \lhd S_n$ and $[S_n : A_n] = 2$. The group A_n consisting of the even permutations in S_n is called the *alternating group on n letters.*

5.4 Conjugacy classes of permutations

(i) Let G be a nontrivial group. Two elements $g, h \in G$ are said to be *conjugate in G* if there exists $x \in G$ such that $g = xhx^{-1}$.

(ii) The relation $\sim_c$ on G given by

$$g \sim_c h \iff g \text{ and } h \text{ are conjugate}$$

defines an equivalence relation on G. Each equivalence class (denoted by $[g]_c$) induced by the relation $\sim_c$ is called a *conjugacy class of G.*

(iii) A *partition of a positive integer n* is a way of writing n as a sum of positive integers, up to reordering of summands. For example, the partitions of 4 are:

(a) $1+1+1+1$,

(b) $2+1+1$,

(c) $3+1$,

(d) $2+2$, and

(e) 4.

(iv) Suppose that the unique cycle decomposition of a permutation $\sigma \in S_n$ is given by

$$\sigma = \sigma_1 \sigma_2 \ldots \sigma_{k_\sigma},$$

where each σ_i is an m_i-cycle. Then:

(a) $o(\sigma) = \text{lcm}(m_1, m_2, \ldots, m_{k_\sigma})$.

(b) As $\sum_{i=1}^{k_\sigma} m_i = n$, this decomposition induces a partition P_σ of the integer n.

(c) Given two permutations $\sigma_1, \sigma_2 \in S_n$,

$$[\sigma_1]_c = [\sigma_2]_c \iff P_{\sigma_1} = P_{\sigma_2}.$$

Consequently, the number of distinct conjugacy classes of S_n is precisely the number of partitions of n.

6 Groups of symmetries

6.1 Symmetries of polyhedra

(i) A *convex polyhedron* (pl. polyhedra) is a solid formed by enclosing a portion of 3-dimensional space with 4 or more plane polygons. For example, cube, prisms and pyramids are polyhedra.

(ii) A polyhedron whose faces are identical (or congruent) regular polygons is called a *regular polyhedron*. There are exactly five regular polyhedra, namely, the cube, the tetrahedron, octahedron, dodecahedron, and the icosahedron.

(iii) Two polyhedra are said to be *duals of each other* if the vertices of one correspond to the faces of the other (and vice versa) and the edges between pairs of vertices of one correspond to the edges between pairs of faces of the other (and vice versa).

(iv) The edges of the dual of a regular polyhedron are constructed by joining the centers of adjacent faces of the polyhedron. The cube and the octahedron, and the dodecahedron and the icosahedron, are duals of each other.

(v) The collection of rotational symmetries $\mathrm{Sym}(P)$ of a regular polyhedron P forms a group under composition.

(vi) The group of a rotational symmetries of a polyhedron and its dual are isomorphic.

(vii) **Rotational symmetries of the tetrahedron.** The *tetrahedron* T_4 has 4 vertices, 6 edges, and 4 faces (see Figure 2 below), each of which is a equilateral triangle.

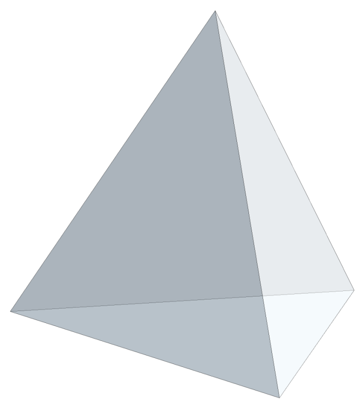


Figure 2: A tetrahedron.

The tetrahedron has exactly 12 rotational symmetries, which comprise:

- 1 trivial rotation or the identity symmetry,
- 8 non-trivial rotations (by $2\pi/3$ and $4\pi/3$ radians) about the 4 axes joining vertices to the centers of opposite faces, and
- 3 non-trivial rotations (by π radians) about the 3 axes joining the midpoints of opposite edges.

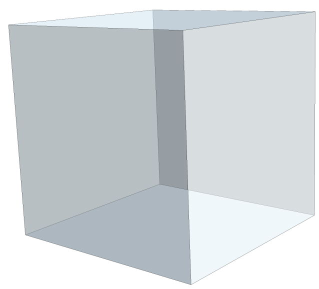
Labeling the vertices of T_4 with numbers 1-4, we see each rotational symmetry $r \in \mathrm{Sym}(T_4)$ induces a permutation of these vertices, and hence induces a bijection $\sigma_r \in S_4$ on the the set $\{1,2,3,4\}$. Moreover, we see that a order 3 rotation induces a 3-cycle in S_4, while a order 2 rotation induces a product of two disjoint transpositions in S_4. As every non-trivial rotation induces an even permutation, the association

$$\mathrm{Sym}(T_4) \to A_4 : r \mapsto \sigma_r$$

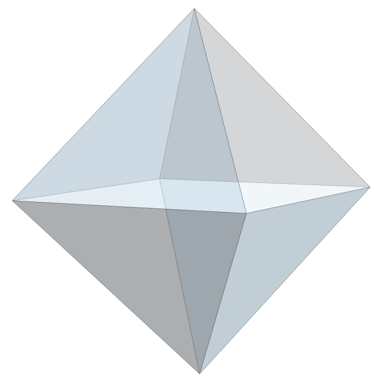
is an isomorphism, or in other words,

$$\mathrm{Sym}(T_4) \cong A_4.$$

(viii) **Rotational symmetries of the cube (and the octahedron.)** The *cube* C has 8 vertices, 12 edges, and 6 faces (see Figure 3 below), each of which is a square.



(a) A cube.



(b) An octahedron.

Figure 3: The cube and the octahedron are dual polyhedra.

The cube has exactly 24 rotational symmetries, which comprise:

- 1 trivial rotation or the identity symmetry,
- 9 non-trivial rotations (by $\pi/2$, π and $3\pi/2$ radians) about 3 axes joining the centers of opposite faces,
- 8 non-trivial rotations (by $2\pi/3$ and $4\pi/3$ radians) about the 4 great diagonals, and
- 6 non-trivial rotations (by π radians) about the 6 axes joining the midpoints of opposite edges.

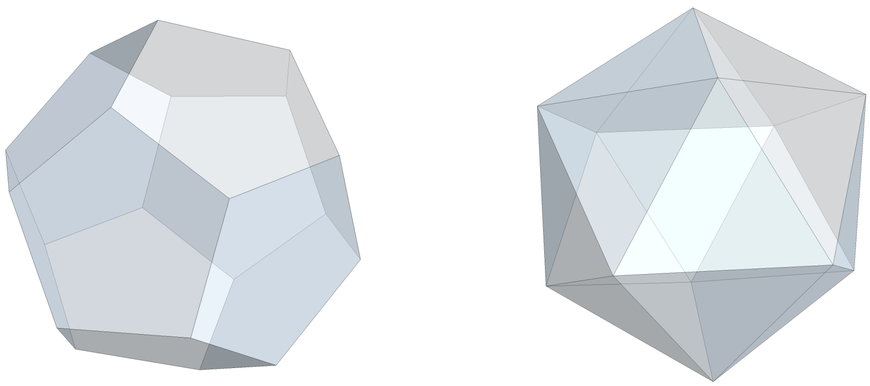
Any rotational symmetry of C maps a great diagonal to another great diagonal, and hence it induces a permutation of the set of great diagonals. So we label the four distinct pairs of diagonally opposite vertices of C with numbers 1-4. This labeling would the give the vertices in each face of C the labels 1-4. Fixing any face in C, we see that each rotational symmetry $r \in \mathrm{Sym}(C)$ induces a permutation of vertices of that face, and hence induces bijection $\sigma_r \in S_4$ on the set $\{1,2,3,4\}$. Consequently, the map

$$\mathrm{Sym}(C) \to S_4 : r \mapsto \sigma_r$$

is an isomorphism, that is,

$$\mathrm{Sym}(C) \cong S_4.$$

(ix) **Rotational symmetries of the dodecahedron (and the icosahedron.)** The *dodecahedron* $\mathscr{D}$ has 20 vertices, 30 edges, and 12 faces (see Figure 4 below), each of which is a regular pentagon.



(a) A dodechedron.

(b) An icosahedron.

Figure 4: The dodecahedron and the icoshedron are dual polyhedra.

The icosahedron has exactly 60 rotational symmetries, which comprise:

- 1 trivial rotation or the identity symmetry,
- 24 non-trivial rotations (by $2\pi k/5$ radians, for $k = 2, 3, 4, 5$) about the 6 axes joining the centers of opposite faces, and
- 20 non-trivial rotations (by $2\pi/3$ and $4\pi/3$ radians) about the 10 great diagonals, and
- 15 non-trivial rotations (by π radians) about the 15 axes joining the midpoints of opposite edges.

Each pentagonal face of $\mathscr{D}$ has five diagonals. Note that there are 5 distinct cubes (labeled 1-5) that can be inscribed in $\mathscr{D}$ such that:

- the vertices of the cube are also vertices of $\mathscr{D}$, and
- each cube intersects each face of $\mathscr{D}$ in exactly one diagonal (see Figure 5 below [1]).

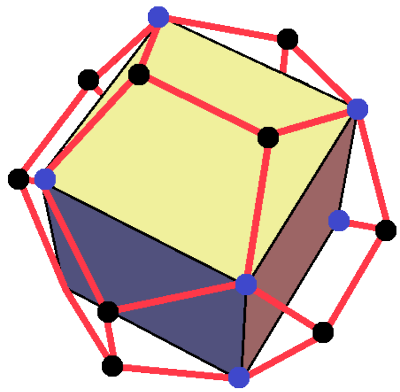


Figure 5: A cube inscribed in a dodecahedron.

Any rotational symmetry of $r \in \mathrm{Sym}(\mathscr{D})$ induces a permutation $\sigma_r \in S_5$ of these cubes. Further, we note that each permutation thus induced is an even permutation. Consequently, the map

$$\mathrm{Sym}(\mathscr{D}) \to A_5 : r \mapsto \sigma_r$$

is an isomorphism, that is,

$$\mathrm{Sym}(\mathscr{D}) \cong A_5.$$

6.2 Real orthogonal groups

(i) The *real orthogonal group in dimension n*, denoted by $\mathrm{O}(n,\mathbb{R})$ is defined by

$$\mathrm{O}(n,\mathbb{R}) := \{A \in \mathrm{GL}(n,\mathbb{R}) : AA^\intercal = A^\intercal A = I_n\}.$$

(ii) The determinant map

$$\mathrm{Det} : \mathrm{O}(n,\mathbb{R}) \to C_2 = \{\pm 1\} : A \xrightarrow{\mathrm{Det}} \mathrm{Det}(A)$$

is an epimorphism. Moreover,

$$\ker \mathrm{Det} = \{A \in \mathrm{O}(n,\mathbb{R}) : \mathrm{Det}(A) = 1\}$$

is a normal subgroup of index 2 called the *special real orthogonal group*, and is denoted by $\mathrm{SO}(n,\mathbb{R})$.

(iii) Any matrix in $\mathrm{SO}(2,\mathbb{R})$ has the form

$$A_\theta := \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}, \text{ where } \theta \in \mathbb{R}.$$

Consequently, the map

$$\mathrm{SO}(2,\mathbb{R}) \to S^1 : A_\theta \mapsto e^{i\theta}$$

is an isomorphism, and so we have

$$\mathrm{SO}(2,\mathbb{R}) \cong S^1.$$

(iv) Consider a matrix $A \in \mathrm{GL}(n,\mathbb{R})$. Then the following statements are equivalent.

(a) $A \in \mathrm{O}(n,\mathbb{R})$.

(b) A preserves dot product of vectors, that is,

$$AX \cdot AY = X \cdot Y, \forall X, Y \in \mathbb{R}^n.$$

(c) The columns of A form an orthonormal basis for $\mathbb{R}^n$.

(v) Let $f : \mathbb{R}^n \to \mathbb{R}^n$ be a bijective map (i.e. $f \in S(\mathbb{R}^n)$). Then f is said to be an *isometry (or a rigid motion)* of $\mathbb{R}^n$ if

$$\|X - Y\| = \|f(X) - f(Y)\|, \forall X, Y \in \mathbb{R}^n.$$

(vi) The group $\mathrm{Sym}(\mathbb{R}^n)$ of *isometries (or rigid motions) of* $\mathbb{R}^n$ is defined by

$$\mathrm{Sym}(\mathbb{R}^n) := \{f \in S(\mathbb{R}^n) : f \textit{ is an isometry.}\}.$$

(vii) Let $f \in S(\mathbb{R}^n)$ be a bijection. Then the following statements are equivalent.

(a) $f \in \mathrm{Sym}(\mathbb{R}^n)$ with $f(0) = 0$, where $0 \in \mathbb{R}^n$ denotes the zero vector.

(b) f preserves dot product of vectors, that is,

$$f(X) \cdot f(Y) = X \cdot Y, \forall X, Y \in \mathbb{R}^n.$$

(c) There exists $A \in \mathrm{O}(n,\mathbb{R})$ such that $f(X) = AX$, for all $X \in \mathbb{R}^n$.

(viii) Given $m \in \mathrm{Sym}(\mathbb{R}^n)$, there exists $A \in \mathrm{O}(n, \mathbb{R})$ and a vector $B \in \mathbb{R}^n$ such that

$$m(X) = AX + B, \forall X \in \mathbb{R}^n.$$

In other words, every rigid motion of $\mathbb{R}^n$ is the composition of a orthogonal linear operator with a translation.

(ix) The group of rotations of $\mathbb{R}^2$ (resp. $\mathbb{R}^3$) about the origin is isomorphic to $\mathrm{SO}(2, \mathbb{R})$ (resp. $\mathrm{SO}(3, \mathbb{R})$).

(x) A matrix $A \in \mathrm{O}(n, \mathbb{R})$ is said to be *orientation-preserving*, if $\mathrm{Det}(A) = 1$, and *orientation-reversing*, if $\mathrm{Det}(A) = -1$.

(xi) The rotations of $\mathbb{R}^2$ and $\mathbb{R}^3$ are orientation-preserving rigid motions which fix the origin.

(xii) Any finite subgroup of $\mathrm{SO}(2, \mathbb{R})$ is isomorphic to $\mathbb{Z}_n$, for $n \geq 1$, any finite subgroup of $\mathrm{O}(2, \mathbb{R})$ that is not contained in $\mathrm{SO}(2, \mathbb{R})$ is isomorphic to D_{2n}, for $n \geq 2$.

(xiii) Any finite subgroup of $\mathrm{SO}(3, \mathbb{R})$ is isomorphic to precisely one of the following groups.

  (a) C_n, $n \geq 1$, the group of rotational symmetries of an n-pyramid (see Figure 6 below).

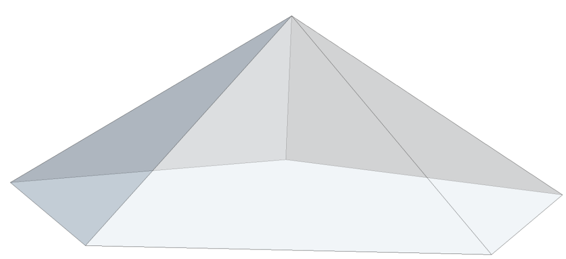


Figure 6: A pentagonal pyramid.

  (b) D_{2n}, $n \geq 1$ the group of rotational symmetries of an n-prism (see Figure 7 below).

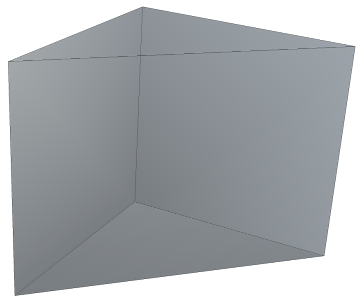


Figure 7: A 3-prism.

(c) A_4, the group of rotational symmetries of a tetrahedron.

(d) S_4, the group of symmetries of a cube or a octahedron.

(e) A_5, the group of symmetries of a dodecahedron or a icosahedron.

References

[1] Cube in a dodecahedron. https://lt.wikipedia.org/wiki/Vaizdas:Cube_in_dodecahedron.png. Accessed: November 14, 2018.