Examples and some basic properties of groups

1. **Definition (Group).** A *group* consists of a set G and a binary operation $\circ : G \times G \to G : (g, h) \mapsto g \circ h$ which satisfies the following properties.

   (a) **Associativity.** For all $g, h, k \in G$ we have
   $$(g \circ h) \circ k \;=\; g \circ (h \circ k)$$

   (b) **Identity.** There is an element $e \in G$ such that
   $$e \circ g \;=\; g \circ e \;=\; g$$
   for all $g \in G$.

   (c) **Inverses.** For every $g \in G$ there exists $g^{-1} \in G$ such that
   $$g \circ g^{-1} \;=\; g^{-1} \circ g \;=\; e$$

   Note that the *closure* property is included in the definition of a binary operation as being a function from $G \times G$ with values in G.

2. **Examples of groups.** Here are some examples and some non-examples.

   - The set $S_n = \text{Perm}(\{1, \ldots, n\})$ is a group under composition of functions $\circ$.
   - The set $\mathbb{Z}$ is a group under $+$. So also are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ under $+$.
   - The set $\mathbb{N}$ is not a group under $+$ (no inverses).
   - The set $\mathbb{R} - \{0\}$ is a group under $\times$. So also are $\mathbb{R}_{>0}$, $\mathbb{Q} - \{0\}$, $\mathbb{Q}_{>0}$, and $\mathbb{C} - \{0\}$ groups under $\times$.
   - The set $\mathbb{Z}_n$ is a group under $+_n$.
   - The set $\mathbb{Z}_p - \{0\}$ is a group under $\times_p$ where p is a prime.
   - The set D_n of *symmetries* of a regular n–gon in the euclidean plane is a group under composition of functions.
   - The set of symmetries of a regular polyhedron (e.g., a cube, an octahedron, a tetrahedron, an octahedron, an icosahedron, a dodecahedron) in euclidean 3-dimensional space is a group.
   - The set of symmetries of a wallpaper pattern in the euclidean plane is a group.

3. **Basic properties.** The following results are true for all groups.

   - The identity element is unique.
   - Inverses are unique.

4. **Isomorphic groups.** Two groups $(G_1, \circ_1)$ and $(G_2, \circ_2)$ are said to be *isomorphic* if there is a bijection $\varphi : G_1 \to G_2$ which respects multiplication. That is
   $$\varphi(g \circ_1 h) \;=\; \varphi(g) \circ_2 \varphi(h)$$
   for all $g, h \in G_1$.

   Intuitively, isomorphic groups are the same. They have the same number of elements and the elements (once paired up) multiply in the same way, You could think of it as translating a group from English into French. There is the same underlying group structure but different expressions for the elements and the operation.

   Examples of isomorphic groups include.

- D_3 and S_3.
- S_4 and the group of symmetries of a regular tetrahedron in 3–space.
- S_2 and $\mathbb{Z}_2$.
- A_3 and $\mathbb{Z}_3$.
- $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \times)$.
- $(\mathbb{Z}_p - \{0\}, \times_p)$ and $(\mathbb{Z}_{p-1}, +_{p-1})$ where $p \geq 3$ is a prime. You can learn proofs of this fact in an abstract algebra course. Meanwhile, find explicit isomorphisms in the cases $p = 3$, 5 , 7, and 11.
- $(\{\pm 1, \pm i\}, \times)$ and $(\mathbb{Z}_4, +_4)$.

5. **Subgroups.** A subset $H \subseteq G$ of a group G is said to be a subgroup if it is a group under the operation on G. That is H contains the identity of G, and is closed under taking inverses and products.

   Examples of subgroups include the following.

   - $m\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.
   - A_n the alternating group is a subgroup of S_n the symmetric group.
   - $\{\mathbb{I}, (12)\}$ is a subgroup of S_3.
   - $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$ which is a subgroup of $(\mathbb{R}, +)$ etc.
   - If $g \in G$ then the set
   $$\langle g \rangle \;=\; \{g^n \mid n \in \mathbb{Z}\}$$
   is a subgroup of G. It is called the *cyclic subgroup of G generated by g*.
   An element $g \in G$ has *finite order* if $g^m = e$ for some $m \in \mathbb{N}$. The smallest such m is called the order of g and is denoted by $\operatorname{ord}(g)$. If $\operatorname{ord}(g) = m$, then $\langle g \rangle$ has size m. Its elements are $g^1, g^2, \ldots, g^{m-1}, g^m = e$.
   For example
   $$\langle (123)(45) \rangle \;=\; \{(123)(45), (132), (45), (123), (132)(45), \mathbb{I}\}$$
   is a subgroup of size 6 in S_5.
   - The symmetries of a cube which send a given face to itself forms a subgroup of the group of symmetries of a cube. Similarly for the symmetries which send an edge to itself, or for the symmetries which fix a vertex.

6. **Cayley's Theorem.** Every group is isomorphic to a group of permutations of a set. In particular, the group G is isomorphic to a subgroup of $\operatorname{Perm}(G)$.

   Proof. Let $g \in G$. Consider the function $L_g : G \to G : x \mapsto L_g(x) = gx$ defined by *left multiplication by g*. Here are two cool properties of left multiplication.

   - If $e \in G$ is the identity element, then $L_e = \mathbb{I}_G$.
   Proof. By definition $L_e(x) = ex = x = \mathbb{I}_G(x)$ for all $x \in G$. Thus $L_e = \mathbb{I}_G$. □
   - If $g_1, g_2 \in G$, then $L_{g_1} \circ L_{g_2} = L_{g_1 g_2}$.
   Proof. Indeed for any $x \in G$ we have
   $$L_{g_1} \circ L_{g_2}(x) \;=\; L_{g_1}(L_{g_2}(x)) \;=\; L_{g_1}(g_2 x) \;=\; g_1(g_2 x) \;=\; (g_1 g_2)x \;=\; L_{g_1 g_2}(x)$$
   Thus $L_{g_1} \circ L_{g_2} = L_{g_1 g_2}$. □

From these properties we conclude that

$$L_g \circ L_{g^{-1}} \;=\; L_{gg^{-1}} \;=\; L_e \;=\; \mathbb{I}_G$$

and

$$L_g^{-1} \circ L_g \;=\; L_{g^{-1}g} \;=\; L_e \;=\; \mathbb{I}_G$$

The top equality implies that L_g is surjective, and the bottom equality implies that L_g is injective. Therefore L_g is a bijection (permutation of G) with inverse

$$L_g^{-1} \;=\; L_{g^{-1}}$$

Now, the facts that $\mathbb{I}_G = L_e$, that $L_g \circ L_h = L_{gh}$ and that $L_g^{-1} = L_{g^{-1}}$ imply that the subset

$$\{L_g \mid g \in G\} \;\subseteq\; \mathrm{Perm}(G)$$

is a subgroup.

Finally we verify that the assignment

$$G \;\to\; \{L_g \mid g \in G\} \;\subseteq\; \mathrm{Perm}(G)$$

sending g to L_g is an isomorphism of groups. It is clearly surjective (by definition of the set $\{L_g \mid g \in G\}$) and injectivity is readily established. If $L_g = L_h$, then $L_g(e) = L_h(e)$, and this implies $ge = he$ or $g = h$. Done! Finally, the equation $L_g \circ L_h = L_{gh}$ implies that the assignment respects group multiplications (multiplication gh on G on the one hand and composition of permutations $L_g \circ L_h$ on the other) and so is an isomorphism. □

Examples. Here are some examples of groups considered as subgroups of permutation groups according to the proof of Cayley's theorem.

- $(\mathbb{Z}_3, +_3)$ is isomorphic to the group $\{\mathbb{I}, (012), (021)\}$ of $\mathrm{Perm}(\mathbb{Z}_3)$.
- $(\mathbb{Z}_n, +_n)$ is isomorphic to the group $\{\mathbb{I}, (012\ldots n{-}1), (012\ldots n{-}1)^2, \ldots, (12\ldots n{-}1)^{n-1}\}$ of $\mathrm{Perm}(\mathbb{Z}_n)$.
- Given $m \in \mathbb{Z}$ let P_m denote the bijection of $\mathbb{Z}$ given by adding m (*plus* m)

$$P_m : \mathbb{Z} \to \mathbb{Z} : n \mapsto P_m(n) = m + n$$

  Cayley's theorem implies that the assignment

$$(\mathbb{Z}, +) \;\to\; (\mathrm{Perm}(\mathbb{Z}), \circ)$$

  sending m to P_m is an isomorphism of groups.

More efficient examples. We can often realize particular groups as being isomorphic to subgroups of permutation groups in more efficient ways than the method of Cayley's theorem.

- The dihedral group D_3 is isomorphic to a subgroup of S_3 where the 3 element set is the set of vertices of the triangle.
- Write out explicit isomorphisms for D_4, D_5, D_6 similar to the one above.
- The group of symmetries of a regular tetrahedron is isomorphic to S_4.

- The group of symmetries of a regular cube is isomorphic to a subgroup of S_8 (using vertices), and to a subgroup of S_{12} (using edges), and to a subgroup of S_6 (using faces).

7. **Lagrange's Theorem.** If G is a finite group and H is a subgroup of G, then $|H| \mid |G|$.

   Proof. We have already seen that left multiplication L_g by $g \in G$ is a bijective function. In particular

   $$L_g|_H : H \ \to \ L_g(H)$$

   is a bijection. This shows that each set $L_g(H)$ has the same number of elements as H.

   Some of these image sets are the same. For example, if $h \in H$ then $L_h(H) = H$. Likewise if $h \in H$ and $g \in G - H$ then $L_g(H) = L_g(L_h(H)) = L_{gh}(H)$.

   It is a wonderful fact that two such image sets are either the same or are disjoint. In other words, if $L_{g_1}(H) \cap L_{g_2}(H) \neq \emptyset$, then $L_{g_1}(H) = L_{g_2}(H)$. Indeed, if $x \in L_{g_1}(H) \cap L_{g_2}(H)$ then this means that $x = g_1 h_1$ for some $h_1 \in H$ and that $x = g_2 h_2$ for some $h_2 \in H$. But this means that

   $$g_1 h_1 \ = \ g_2 h_2$$

   Multiplying across on the left by g_2^{-1} and on the right by h_1^{-1} gives

   $$g_2^{-1} g_1 \ = \ h_2 h_1^{-1}$$

   Thus

   $$L_{g_2}^{-1} \circ L_{g_1}(H) \ = \ L_{g_2^{-1} g_1}(H) \ = \ L_{h_2 h_1^{-1}}(H) \ = \ H$$

   This means

   $$L_{g_2}^{-1}(L_{g_1}(H)) \ = \ H$$

   and so

   $$L_{g_2}(L_{g_2}^{-1}(L_{g_1}(H))) \ = \ L_{g_2}(H)$$

   In other words

   $$L_{g_1}(H) \ = \ L_{g_2}(H)$$

   Thus we have a partition of G into disjoint subsets of the form $L_g(H)$ each of which is bijective to H and so has the same cardinality as H. Since G is finite there are only finitely many (say that there are m) of these distinct subsets $L_g(H)$. But this means $m|H| = |G|$ and so $|H|$ divides $|G|$. □

   Examples. There are lots of examples of Lagrange's Theorem.

   - If G is a finite group and $g \in G$, then $\text{ord}(g) \mid |G|$.
   - $\langle(12)\rangle$, $(123)\langle(12)\rangle$ and $(132)\langle(12)\rangle$ form a partition of S_3.
   - $\langle(123)\rangle$ and $(12)\langle(123)\rangle$ form a partition of S_3.
   - A_n and $(12)A_n$ form a partition of S_n.
   - The set of symmetries of the cube which send a given face of the cube into itself forms a subgroup of the group of symmetries of the cube which is isomorphic to D_4. Thus the number of symmetries of the cube is a multiple of 8.
   - We know that for p prime $(\mathbb{Z}_p - \{0\}, \times)$ is a group under multiplication. Its order is $p - 1$. If $a \in \mathbb{Z}_p - \{0\}$ then the order of a (that is the power of a which yields the identity $1 \mod p$) divides $p - 1$ by Lagrange's theorem. This means

     $$a^{p-1} \ \equiv \ 1 \mod p$$

     This is the statement of Fermat's Little Theorem.