Group theory

Terry Wang

November 11, 2024

All * problems are the more difficult ones.

A slight note on notation, many of you may already be familiar with set builder notation, but since this notation often varies from place to place, for the sake of standardization, here is a quick definition. A **set** is just any collection of items, it can be numbers, shapes, objects, or something else (except a set cannot contain itself). If G, H are sets, and every element of H is also an element of G, then we write $H \subseteq G$ and say that H is a **subset** of G.

Sometimes, we will need additional notation to describe subsets. We will use $\{x \in G : x \text{ satisfies condition } P\}$ to describe the subset of G consisting of elements of G which satisfy a condition P. For instance:

$$\{x \in \mathbb{N} : x \text{ is even}\}$$

is the set of all positive even numbers.

1 Permutations

Definition 1.1 Let X be a set, a **permutation** of the set X is an one to one mapping of elements in X to elements in X. For instance, a permutation of letters (a, b, c) might be (b, a, c). In this case, we will write:

$$\sigma := \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$

To denote our permutation σ. In particular, in the first row, we will list out the elements, and the in the second row we will list out what each element gets mapped to:

Problem 1.2 Consider the permutation on the letters a through e that maps $\{a, b, c, d, e\} \to \{c, b, a, e, d\}$, write this in our standard notation.

Problem 1.3 Consider the permutation:

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

What does 2 get mapped to?

In general, it does not matter what symbols we use when we write out a permutation (letters, numbers, shapes, or something else). For the sake of standardization, we will use numbers from now on. It is possible to compose two permutations, for instance, given the following permutations:

$$\alpha := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \beta := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

We can write the product or composition, denoted $\alpha\beta$ as the permutation:

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Since:

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

In other words, $\alpha\beta$ is the permutation created by first applying β, then α. Here, when we write $\alpha\beta$, the order matters.

Problem 1.4 What is $\beta\alpha$, and is it the same as $\alpha\beta$?

Hence forth, given a set X, we will denote the set of its permutations as S_X, when X is the first n natural numbers, we will instead use S_n.

Problem 1.5 How many elements are in S_4, how about S_X with any set X having 4 elements. What about a set having 10 elements? Can you figure out the general formula?

Problem 1.6 Prove the following properties about S_n:

1. There exists a permutation, denoted 1 and called the **identity element** such that for any permutation α, $\alpha 1 = 1\alpha = \alpha$.
2. For every permutation α, there exists a corresponding unique permutation α^{-1}, called the **inverse**, such that $\alpha^{-1}\alpha = \alpha\alpha^{-1} = 1$.
3. The product of any two permutations is a permutation and $\alpha\beta\gamma = (\alpha\beta)\gamma = \alpha(\beta\gamma)$ for any three permutations. This is known as associativity.

Those of you who are reading ahead might recognize these three properties as the defining properties of a group.

Definition 1.7 We say that a permutation α **fixes** an element k if $\alpha(k) = k$. If $\alpha(k) \neq k$, then we say that α **moves** k.

Definition 1.8 Let $i_1, i_2, \ldots, i_n$ be distinct integers, then let α be the permutation such that:

$$\alpha(i_1) = i_2,\ \alpha(i_2) = i_3, \ldots,\ \alpha(i_n) = i_1$$

And $\alpha(k) = k$ for any k that isn't one of $i_1, \ldots, i_n$. Then α is known as a **cycle**. Specifically, a n-cycle.

Problem 1.9 Identify which of the following are cycles and which are not:

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 6 & 4 & 5 & 7 & 1 \end{pmatrix}$
2. $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 3 & 6 \end{pmatrix}$
4. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$

When a cycle is a 2-cycle, we also call it a **transposition**.

Definition 1.10 We call two permutations α, β **disjoint** if every element moved by β is fixed by α and every element moved by α is fixed by β.

Problem 1.11 Prove that $\alpha\beta = \beta\alpha$ if α, β are disjoint, that is to say that the two **commute**.

Problem 1.12* Prove that every permutation in S_n can be written as the product of pairwise disjoint cycles.

Problem 1.13* How many permutations in S_n satisfy $\alpha^2 = 1$, (by α^k, I mean $\alpha \dots \alpha$ a total of k times).

2 Groups and symmetry

To generalize the ideas that we have developed in the last section, we focus in on the ideas described in problem 1.6, namely:

Definition 2.1 We call a set G, together with a binary operation $*$ (an operation that combines two elements of G to return another element of G), a **group**, if this pair, $(G, *)$ obeys the following rules:

1. There exists an element 1, called the identity, such that $1 * a = a * 1 = a$ for any a in G.
2. For any element a in G, there exists an element, called the inverse, a^{-1} such that $a^{-1} * a = a * a^{-1} = 1$.
3. The binary operation $*$ is associative, meaning $a * b * c = (a * b) * c = a * (b * c)$ for any three elements of G.

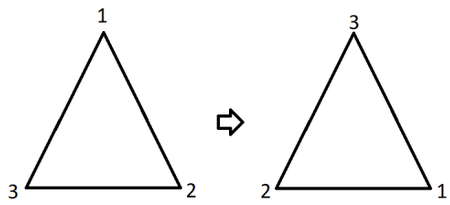
Sometimes, for the sake of notation, we will just drop the $*$ notation, in the sense that $a * b$ is the same as ab for elements in a group. Also for the sake of notation, a^k is $a * \cdots * a$ a total of k times, and a^{-k} is the same but with a^{-1}.

Problem 2.2 Consider the following, which one of these are groups and which are not?

1. $\mathbb{R}$, the set of all rational numbers, with the binary operation of multiplication.
2. The set of integers, $\mathbb{Z}$, with the operation of addition.
3. The set of odd numbers also with the operation of addition.
4. The set of permutations defined above S_X for some set X.
5. $\mathbb{Q}\backslash\{0\}$, the set of all nonzero rational numbers with the operation of multiplication.

Other examples can exist, but are a bit more nuanced. There are precisely 3 rotational symmetries of a triangle: 120, 240, and 360 clockwise rotations. If we number the vertices of the triangle, then we can write these in permutation notation, for instance:

$$120 \text{ clockwise rotation} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$



Problem 2.3 Write out the other two rotational symmetries in permutation notation, now do the same with the reflectional symmetries.

Formally speaking, a rotational symmetry of a regular n-gon is such that when written in permutation notation, it can be expressed as α^k for some integer k, where α is the n-cycle that maps each vertex to its clockwise direction neighbor. A reflectional symmetry is a symmetry β such that $\beta^2 = 1$.

Problem 2.4 Write out the reflectional symmetries of the square in permutation form.

Problem 2.5 Do the rotational symmetries form a group (with the binary operation here being composition of the permutations)? What about the reflectional symmetries?

Problem 2.6 Do the rotational symmetries of a square form a group? What about the reflectional symmetries of a square?

Notice from the above 4 problems that although S_X forms a group, we do not need all of the permutations in S_X to form a group. In particular, all of the symmetries above can be viewed as elements of the permutation group of the vertices of a square/triangle and form a group. As such, we have the following definition:

Definition 2.7 A **subgroup** of a group $(G, *)$, is a subset, $H \subseteq G$ such that H is a group in it of itself, still with the same binary operation $*$.

Here is another useful definition:

Definition 2.8 For elements of a group G, say a, b, if $ab = ba$, then we say that a and b **commute**. If all elements of a group commute with each other then we call that group **abelian**.

Problem 2.9 Show that for any two elements a, b of a group G, the inverse of ab, or $(ab)^{-1}$, is equal to $b^{-1}a^{-1}$.

Problem 2.10 For each of the three examples listed at the beginning of the section, categorize them as abelian or not.

Problem 2.11 Show that the identity element in a group is unique, similarly, also show that for any element in a group, its inverse is unique.

Problem 2.12* Suppose we have a finite abelian group G such that no element a satisfies $a^2 = 1$, compute the product of all of the elements of the group.

Problem 2.13* Prove Wilson's theorem, for any prime p:

$$(p-1)! \equiv -1 \mod p$$

Hint. The non-zero residue classes modulo any prime form an abelian group under multiplication, also try to use problem 2.11.

Problem 2.14* Suppose we have a finite group G such that every element a satisfies $a^2 = 1$, show that G is an abelian group.

3 Homomorphisms and equality between groups

Consider the following two groups. Define G as the group consisting of -1 and 1 (the numbers) with the binary operation of multiplication. Define H as the group of 0 and 1 with addition modulo two as the binary operation (ie. $1 + 1 = 0$). These two groups share a fairly similar structure:

$\times$	0	1
0	0	1
1	1	0

$+$	-1	1
-1	1	-1
1	-1	1

They share the exact same structure. In fact, in the above multiplication tables, if we swap $0 \to 1$ and $1 \to -1$ we get one from the other. Clearly, in some sense, these groups are the "same." Specifically, we can map one to another in some way that does not disturb the underlying binary operation structure.

Definition 3.1 A **homomorphism** is a function, f, from one group, $(G, *)$, to another group, $(H, \times)$, such that $f(a * b) = f(a) \times f(b)$ for any two elements a, b of G. An **isomorphism** is a homomorphism that is also one to one or bijective. When there exists an isomorphism between two groups, we say that the two groups are **isomorphic**.

As it turns out, this notion of isomorphic is what we want when we want to say that two groups G, H are the same. In the above example, the mapping described is a isomorphism that demonstrates groups G and H are isomorphic.

Problem 3.2 Verify that the following are homomorphisms:

1. $\mathbb{R} \to \mathbb{C} : f(x) = x$
2. $\mathbb{R}^{+,\times} \to \mathbb{R}^{+} : f(x) = \ln(x)$
3. Consider the mapping from the set of rotational symmetries of a square to the integers modulo 4, where we map: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \to 0,\ a := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \to 1,\ a^2 \to 2,\ a^3 \to 3$

Which one of the above are isomorphisms?

Problem 3.3* Construct an isomorphism between the following groups: $S_3 \to \{x, \frac{1}{x}, 1-x, \frac{1}{1-x}, \frac{x}{1-x}, \frac{x-1}{x}\}$, where the latter is a set of functions which forms a group under the composition of functions.

Problem 3.4 Prove that there are at most n^{n^2} possible groups of size n (meaning the group has n elements).

Problem 3.5 Prove the following facts about homomorphisms:

1. $f(1_G) = 1_H$
2. $f(a^{-1}) = f(a)^{-1}$ for any a in G
3. $f(a^k) = f(a)^k$ for any a in G

In the above $(G, *), (H, \times)$ are groups with identity elements 1_G and 1_H respectively and $f : G \to H$ is a homomorphism.

Problem 3.6* Prove that the group of all polynomials with integer coefficients equipped with the operation of polynomial addition is isomorphic to the group of all positive rationals equipped with the operation of multiplication.
Hint. Use the fundamental theorem of arithmetic.

As above, let $(G, *), (H, \times)$ be groups with identity elements 1_G and 1_H respectively and $f : G \to H$ is a homomorphism. It is not true that $f(x) = 1_H$ implies that x is the identity of G, however, elements which do satisfy this trait have a special name:

Definition 3.7 Let G, H be as above, then the set of elements of G that map to 1_H under f are known as the **kernel** of G, and the set of elements of H that are mapped to by some element of G are known as the **image** of f. Written in set builder notation:

$$\text{Ker}(f) = \{x \in G : f(x) = 1_H\},\ \text{Img}(f) = \{x \in H : f(y) = x \text{ for some } y \text{ in } G\}$$

Problem 3.8 Prove that the kernel and image of a homomorphism f which maps from $G \to H$ are subgroups of G and H respectively.

Problem 3.9 Let $H, K \subseteq G$ be two subgroups of a group G, first show that H, K must have at least 1 element in common (ie. $H \cap K \neq \emptyset$), then show that whatever this intersection is, it is in fact also a subgroup.

Definition 3.10 $^\otimes$ In light of the above problem, it is possible to define the *least* subgroup containing a given subset of a group. Specifically, if G is a group and S is a subset, then there exists a unique subgroup, that is contained in any other subgroup which contains the subset S:

Notice that S is contained in at least 1 subgroup, namely the whole group G itself, and if many different subgroups contain S, then we can take their intersection to get a single subgroup which is contained in all the other subgroups. This is the **subgroup generated by** S, denoted $< S >$.

Lemma 3.11 (One step subgroup test) In general, most subsets of a group are not in fact a subgroup, here is an useful criterion for distinguishing these situations: A subset S of a group $(G, *)$ containing the identity is a subgroup if and only if for any a, b in S we have that $a * b^{-1}$ is also in S.
Proof. We have to prove two directions here, first, assuming that S is a subgroup, we need to show that for any a, b in S we have that ab^{-1} is also in S (when we don't need to distinguish between group operations of two different groups we sometimes just drop the $*$ between elements). This isn't too hard to show, since S is closed under multiplication and taking inverses, so b^{-1} is in S and thus also ab^{-1} is in S.

Now to show the other direction, namely, if S satisfies the property listed in the statement of the theorem, that S is a subgroup. This is also not too hard to prove, we just need to verify the 4 criteria of a group:

1. S contains the identity, as per hypothesis
2. If a is in S, then so is a^{-1}, since 1 is in S and $a^{-1} = 1a^{-1}$ is in S by assumption
3. Obviously $*$ is still associative, it was associative for any elements of the larger group G and thus associative when restricted to only elements in S

Problem 3.12 Complete the above proof by showing that for any two elements of S, say a and b, we have that $ab \in S$.

4 Cosets and Lagrange's theorem

Sometimes, we will deal with sets that are *almost* subgroups, but just are slightly off. For instance, consider the following set:

$$\{k \in \mathbb{Z} : k = 3m + 1 \text{ for some integer } m\} = \{\dots, -2, 1, 4, 7, 10, \dots\}$$

If we could just subtract 1 from each one of the elements, we would end up with the subgroup of the integers consisting of all multiples of 3 (with the group operation of addition). Similarly, consider the group of rotational symmetries of the square:

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

Which we can also denote (let α be the first permutation in the above list):

$$\alpha, \alpha^2, \alpha^3, 1$$

Now, $1, \alpha^2$ is a subgroup, but α, α^3 is not. This leads us to the following definition:

Definition 4.1 For a subgroup H of a group $(G, *)$ and an element g of G, the **right coset** of H with **representative** g is the set:

$$Hg := \{hg : h \in H\}$$

Similarly, the **left coset** is:

$$gH := \{gh : h \in H\}$$

Problem 4.2 For each of the given groups, subgroups, and elements, write out the right coset with the given element as a representative in set builder notation:

1. The nonzero residue classes of the integers modulo 7 form a group under multiplication. The elements $2, 4, 1$ form a subgroup, find the coset of this subgroup with representative 3
2. The symmetries of a triangle can be written as follows:

$$\alpha = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \alpha^2,\ 1,\ b_1 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ b_2 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ b_3 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

   The elements b_2 and 1 form a subgroup, find the right coset with representative α.
3. The integers form a group under addition, multiples of 10 form a subgroup. Find the coset of this subgroup with representative 5.

Notice that I did not bother specifying left or right coset for the first. This is because that group is abelian, why does a group being abelian make its left and right cosets indistinguishable?

In practice, left and right cosets work the same in the sense that almost every theorem and lemma applicable to the former will apply to the latter: mathematics does not distinguish between left and right. As such, we will mostly stick to working with left cosets.

Problem 4.3 Prove that in a group G with elements a, b, g, if $ag = bg$ then $a = b$. From this, prove that if S is a subgroup, then the mapping $f(g) = tg$ is a bijection. Finally, conclude that any two cosets of the same subgroup must have the same size.

Problem 4.4 Prove that for a group G and cosets aS and bS (here a, b are representatives and S is a subgroup of G) that either they are disjoint from each other or they are the same set.

Definition 4.5 In light of the above two problems, we can make the following definition. The **order** of a group is just the number of elements of a group, the **index** of a subgroup S is the number of (left) cosets of S in the larger group G, this is denoted $[G : S]$ typically.

Problem 4.6 Prove Lagrange's theorem using 4.3 and 4.4, namely, that for a finite group G and a subgroup S, the number of (left) cosets of S is $|G|/|S|$ (here, $|A|$ of a set A is the number of elements in A).

Hint. First prove that every element of G is in a coset, now with 4.3 and 4.4, we know that every coset has the same size and they must have no overlap. What can you say now?

Problem 4.7* The **order** of an element a of a group G is $| < a > |$ (ie. take the subgroup generated by the single element a and then take its size). Prove that if G is a finite group, then the order of any element divides the size of G.

Problem 4.8* From the previous problem, prove Fermat's theorem that $a^p \equiv a \bmod p$ for any prime number p and any integer a.

Problem 4.9 Prove that $< a >$, the subgroup generated by a single element a of a group G has the form:

$$\{g \in G : g = a^k \text{ for some } k \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}$$

Thus prove that a group G such that $|G|$ is prime can be written in the form $\{1, a, \dots, a^{p-1}\}$ for some element a in G.

Problem 4.10 Let G be a finite group and let H be a subgroup of G and K be a subgroup of H (and thus also a subgroup of G), prove that $[H : K] \times [G : H] = [G : K]$

Problem 4.11 Let f be a homomorphism from the group G to the group H, both of which are groups which are finite in size, then show that the order of a in G divides the order of $f(a)$ in H.

Problem 4.12* Let G be a group and S be a non empty subset, define S^2 to be the subset of G such that:

$$S^2 := \{g \in G : g = rs \text{ for some } r, s \in S\}$$

Show that if S is a subgroup, then $S^2 = S$, conversely, show that if $S^2 = S$ and S is finite then S is also a subgroup. Why do we need to assume S is finite? Can you find a counterexample if S is infinite?

Problem 4.13* If G is a group and H is a subgroup with only two cosets (ie. of index 2), then prove that for any element a in G a^2 is an element of H.

Problem 4.14* Let G be a group with S, T two non empty subsets of G (they do not have to be distinct). Prove that either:

$$ST := \{g \in G : g = st \text{ for some } s \in S \text{ and } t \in T\}$$

Is equal to the whole set G, or $|G| \geq |S| + |T|$.