Group theory

Terry Wang

November 22, 2024

All * problems are the more difficult ones.

1 A slight review

We will be continuing with the concepts introduced our previous class. Recall that last time, we introduced the idea of a permutation.

Definition 1.1 A **permutation** on a set X is a set function $\sigma : X \to X$ that is bijective. We denote the set of all permutations on a set X as S_X. In the special case that X is the integers 1 through n, we instead write S_n.

Problem 1.2 Let σ be a permutation on numbers $1, 2, ..., n$ where n is an odd number. Show that the product

$$(1 - \sigma(1))(2 - \sigma(2))...(n - \sigma(n))$$

is even.

Furthermore, we were able to generalize the above structure to a type of object known as a group. Recall from last time the following definition:

Definition 1.3 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.
4. G is closed under $*$, specifically, for any two elements of G, say a and b, $a * b$ is also in G.

Continuing the content from last week, this will be the main character for the purposes of this packet.

Problem 1.4 Consider the following, which one of these are groups and which are not?

1. $\mathbb{Q}$, the set of all rational numbers, with the binary operation of multiplication.
2. The set of even numbers with the operation of addition.
3. The set of odd numbers also with the operation of addition.
4. The set of rotational symmetries of a hexagon (with composition of permutations as the binary operation, recall from last time that symmetries can be represented using the permutation notation).
5. $\mathbb{Q}\backslash\{0\}$, the set of all nonzero rational numbers with the operation of multiplication.

For each of the above which is a group, what is the identity element?

In the last packet, we also introduced this notion of a subgroup:

Definition 1.5 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 $*$.

Problem 1.6 Give an example of a subgroup to the group of integers with the group operation of addition and the group of rotational and reflectional symmetries of a square.

Problem 1.7 Give an example of a group G and a subset H such that H is closed under the group operation and contains the identity element but is not a subgroup.

2 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 2.1 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 2.2 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 2.3* 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 2.4 Prove that there are at most n^{n^2} possible groups of size n (meaning the group has n elements).

Problem 2.5 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 2.6* 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 2.7 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 2.8 Prove that the kernel and image of a homomorphism f which maps from $G \to H$ are subgroups of G and H respectively.

Problem 2.9 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 2.10 $^{\otimes}$ 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 2.11 (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 2.12 Complete the above proof by showing that for any two elements of S, say a and b, we have that $ab \in S$.

3 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 3.1 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 3.2 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 3.3 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 3.4 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 3.5 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 3.6 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 3.7* 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 3.8* 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 3.9 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 3.10 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 3.11 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 3.12* 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 3.13* 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 3.14* 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 $|G| \geq |S| + |T|$.

4 Burnside's lemma

Up until now, we have been working to increasingly abstractify the content we work with. Now, we are going to do the opposite and see if we can find some real world application for the theory we have found.

Definition 4.1 Let G be a group, we call a set X a **G-set** if for each element $g \in G$ we can associate to it a function from X to X (which we are also going to denote by g) which satisfies the following:

1. If g is the identity element, then $g(x) = x$ for every x in X
2. If g, h are both in G, then the function associated to their product, gh, is such that $(gh)(x) = g(h(x))$.

Problem 4.2 Identify which of the following sets are an example G-set with the given group:

1. $\mathbb{Z}$ as a group with operation addition acts on the real numbers by having each integer k be associated with the function $k(x) = k - x$.
2. Let $(G, *)$ be any group, it acts on itself by having each element g be associated with the function that maps $g(h) = g * h$.
3. The permutation group S_6 acts on the symbols $1, 2, 3, 4, 5, 6$ in the obvious way, namely by permuting their order as defined.
4. $\mathbb{Z}$ acts on itself by associating each integer k to the function that maps $k(x) = k \times x$.

Justify your answers to each of the above.

Definition 4.3 Let X be a G-set for a group G and let x be an element of X, the **stabilizer** of X is:

$$\mathcal{S}(x) := \{g \in G : g(x) = x\}$$

And the **orbit** of X is:

$$\mathcal{O}(x) := \{y \in X : y = g(x) \text{ for some } g \text{ in } G\}$$

Problem 4.4 Prove that the stabilizer of any x in a G-set X is in fact a subgroup of the group G.

Problem 4.5 Let X be a G-set, and let x be an element of X. First prove that if a, b are in G, then $ax = bx$ implies that the cosets $a\mathcal{S}(x) = b\mathcal{S}(x)$.

Problem 4.6 Let X be a G-set of a group G. Prove that the oribitals of any two elements x, y of X are either disjoint or equal.

Now define a function from $\mathcal{O}(x)$ to the set of cosets of $\mathcal{S}(x)$, which we will denote $G/\mathcal{S}(x)$ where the element ax (a is an element of G) gets mapped to $a\mathcal{S}(x)$:

$$f(ax) = a\mathcal{S}(x)$$

Problem 3.5 shows that this function is well defined.

Problem 4.7 Prove that this function is injective and surjective, and thus bijective. Thus prove the orbital-stabilizer theorem:

$$|\mathcal{O}(x)| = [G : \mathcal{S}(x)]$$

Hint. To show that f is injective, suppose $f(ax) = f(bx)$, then $a\mathcal{S}(x) = b\mathcal{S}(x)$, and so $ag = bh$ for some g, h in the stabilizer. In other words $a = bk$ where $k = hg^{-1}$ is an element of the stabilizer. What can you say about ax and bx now?

Problem 4.8 Prove that if X is a G-set, then for any x in X, the number of elements in $\mathcal{O}(x)$ is a divisor of $|G|$.

The point of the orbital stabilizer theorem is to show that orbitals and stabilizers are somewhat related in a way that investigating one uncovers information regarding the other. To understand why we may want to understand orbitals (and by extension, stabilizers) consider the following problem:

We can describe a black and white flag by a sequence of letters, for instance, the following flag:

By BWBW. But clearly, the flag described by WBWB is the same as the one above (just flip the flag 180 degrees). In a physical sense, a flag described by the sequence $a_1a_2a_3a_4$ is the same as the sequence $a_4a_3a_2a_1$.

We can describe this phenomenon with G-sets. Let $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$, then the identity permutation and a form a (2 element) group, call this group G. The set of 4 term B/W sequences thus form a G-set.

This is useful now because for any sequence $a_1a_2a_3a_4$, its orbital is just: $\{a_1a_2a_3a_4, a_4a_3a_2a_1\}$. As such, if we can count the number of orbitals, we can count the number of such flags.

Problem 4.9 The above situation is pretty simple to handle without group theoretic methods. How many distinct flags are there with four stripes? What about 5?

Problem 4.10* Prove that if X is a G-set for the group G (both of which are finite in size):

$$\sum_{x \in X} \mathcal{S}(x) = \sum_{g \in G} F(g)$$

In the above $F(g)$ is the number of elements in x such that $gx = x$.

Problem 4.11* Prove Burnside's Lemma:

$$\text{The number of orbitals in } X \ = \frac{1}{|G|} \sum_{g \in G} F(g)$$

Hint. The number of orbitals is equal to:

$$\sum_{x \in X} \frac{1}{|\mathcal{O}(x)|}$$

Now use 3.10, the orbital-stabilizer theorem, and Lagrange's theorem.

Problem 4.12 Using Burnside's lemma, check your answer to 3.9. What is the general formula for the number of distinct flags with n stripes?

Problem 4.13 Suppose we are coloring a chessboard (a 8×8 board) so that each square is one of three colors: black, white, and gray. How many distinct chessboards can be made? Remember that you can't really flip over a chessboard and get a different coloring (only one side is colored), but you can rotate it by a multiple of 90 degrees and get another coloring.

Problem 4.14 The sides of a rectangle (that is not a square) are to be colored by either red or blue. How many possible colorings are there, if two colorings that can be obtained from each other by rotation and/or reflection are considered identical?

Problem 4.15* Prove the following identity:

$$\frac{1}{k!} \sum_{\pi \in S_n} n^{\mathrm{cyc}(\pi)} = \binom{n+k-1}{k}.$$

Here, $n^{\mathrm{cyc}}(\pi)$ means the number of cycles in its decomposition into disjoint cycles.