A FRIENDLY INTRODUCTION TO GROUP THEORY

JAKE WELLENS

1. who cares?

You do, prefrosh. If you're a math major, then you probably want to pass Math 5. If you're a chemistry major, then you probably want to take that one chem class I heard involves representation theory. If you're a physics major, then at some point you might want to know what the Standard Model is. And I'll bet at least a few of you CS majors care at least a little bit about cryptography. Anyway, Wikipedia thinks it's useful to know some basic group theory, and I think I agree. It's also fun and I promise it isn't very difficult.

2. what is a group?

I'm about to tell you what a group is, so brace yourself for disappointment. It's bound to be a somewhat anticlimactic experience for both of us: I type out a bunch of unimpressive-looking properties, and a bunch of you sit there looking unimpressed. I hope I can convince you, however, that it is the simplicity and ordinariness of this definition that makes group theory so deep and fundamentally interesting.

Definition 1: *A* ***group*** $(G, *)$ *is a set* G *together with a binary operation* $* : G \times G \to G$ *satisfying the following three conditions:*
1. ***Associativity*** *- that is, for any* $x, y, z \in G$*, we have* $(x * y) * z = x * (y * z)$*.*
2. There is an ***identity element*** $e \in G$ *such that* $\forall g \in G$*, we have* $e * g = g * e = g$*.*
3. Each element has an ***inverse*** *- that is, for each* $g \in G$*, there is some* $h \in G$ *such that* $g * h = h * g = e$*.*

(Remark: we often just write G for $(G, *)$, and basically always call the operation 'multiplication' and suppress the $*$ symbol when we write out products - i.e. we write gh instead of $g * h$, and we write g^n for the n-fold product - even though this may not always be exponentiation in the usual sense!)

Using this Definition 1, it's usually pretty obvious when something is or isn't a group. For example, you should check in your head that $(\{1, -1\}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, and $(\{z \in \mathbb{C} : |z| = 1\}, \cdot)$ are all groups, while $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \div)$, and $(\{z \in \mathbb{C} : |z| = 1\}, +)$ are not groups. In fact, if you start thinking about all the sets and binary operations you've ever seen, it's likely that many of these are actually groups. What's not so obvious is that the conditions defining a group make up a *minimal* set of interesting conditions. That is to say that if you remove any non-empty subset of these conditions, the resulting class of algebraic objects is largely uninteresting. Getting rid of condition 3 gives you the category of *monoids*, which my TeX editor's spell check doesn't recognize. If we also get rid of condition 2, we get *semigroups*, which I know no one who cares about, and getting rid of 1, 2 and 3 (i.e. everything but the binary operation), we get an obscure class of objects called *magmas*, which I know no one cares about. If instead we add more conditions (such as commutativity of the operation, or multiple operations with distributive laws), we get very "well-behaved" classes of algebraic objects like rings, fields, and modules. (I'm not exactly sure what I mean by "well-behaved", but consider this: there exists a finite field of size q iff $q = p^n$ is power of a prime, in which case the field is essentially unique; on the other hand, there are always groups of size n, and often many more than one.)

Before we get to the really interesting stuff, you need to master some basic definitions and concepts which may seem a bit abstract at first. Take your time with this and make sure to attempt all the exercises - nothing will make sense unless you firmly grasp the material in this chapter.

Definition 2: *If $(G, *)$ is a group and $H \subset G$ is a subset such that $(H, *)$ satisfies the group axioms (Definition 1), then we call H a* ***subgroup*** *of G, which we write as $H \leq G$.*

Definition 3: *For any subset S of a group G, we define the* ***subgroup generated by*** *S to be the smallest subgroup of G containing S. We denote this subgroup by $\langle S \rangle$. Here, "smallest" means that if $S \subset H \leq G$, then $\langle S \rangle \leq H$.*

You should be wondering why a smallest such subgroup always exists. One way to see this is to note that given an arbitrary family $\{H_\alpha\}_{\alpha \in \Lambda}$ of subgroups of G, their intersection

$$\bigcap_{\alpha \in \Lambda} H_\alpha$$

is also a subgroup of G. Thus, to form $\langle S \rangle$, we simply intersect over the (non-empty) family $\{H : S \subset H \leq G\}$. You will prove an equivalent characterization of $\langle S \rangle$ in the exercises following this section.

Definition 4: *We denote by $|G|$ the size of a group G, and call this the* ***order*** *of G. The word order means something slightly different when used with particular group elements: the* ***order*** *of an element $g \in G$, written $o(g)$, is defined to be the smallest natural number such that $g^n = e$, if such an n exists. If not, we say g has infinite order.*

A good way to check your understanding of the above definitions is to make sure you understand why the following equation is correct:

$$|\langle g\rangle| = o(g). \tag{1}$$

Definition 5: *A group G is called* ***abelian*** *(or commutative) if $gh = hg$ for all $g, h \in G$. A group is called* ***cyclic*** *if it is generated by a single element, that is, $G = \langle g\rangle$ for some $g \in G$. In general, if $S \subset G$ and $\langle S\rangle = G$, we say that G is generated by S.*

Sometimes it's best to work with explicitly with certain groups, considering their elements as matrices, functions, numbers, congruence classes or whatever they are, but "pure" group theory is more often concerned with *structural* properties of groups. To define what this is precisely, I first need to introduce a really important concept.

Definition 6: *Let $G = (G, \cdot)$ and $G' = (G', *)$ be groups, and let $\phi : G \to G'$ be a map between them. We call ϕ a* ***homomorphism*** *if for every pair of elements $g, h \in G$, we have*

$$\phi(g \cdot h) = \phi(g) * \phi(h). \tag{2}$$

If ϕ is a bijective homomorphism we call it an ***isomorphism****, in which case we say the groups G and G' are* ***isomorphic****, which we write as $G \cong G'$.*

In the exercises, you will check that many things are preserved under isomorphism. Basically, if you can state a property using only group-theoretic language, then this property is isomorphism invariant. **This is important:** From a group-theoretic perspective, isomorphic groups are considered *the same group.* You should think of an isomorphism is just a way of *relabeling* group elements while leaving multiplication intact. For example, the two groups

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}, \quad \mathbb{Z}_2 = \{0, 1\} \tag{3}$$

(where the first operation is matrix multiplication, and the second operation is addition modulo 2) are isomorphic, via the map which sends I to 0 and $-I$ to 1. It's pretty clear in this example that the elements x and $\phi(x)$ play the same "role" in their respective groups, for each $x \in G$. (And if you think about it, *all* groups of order 2 must be isomorphic, by sending the identity element in one group to the identity element in the other, and the non-identity element in one group to the non-identity element in the other.) A slightly less obvious pair of isomorphic groups is

$$(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot) \tag{4}$$

via the isomorphism $x \mapsto e^x$. Of course all groups are isomorphic to themselves via the identity map, but this may not be the only such mapping - isomorphisms from a group G to itself are called **automorphisms**, and the set of all such maps is denoted $\mathrm{Aut}(G)$. For example, given any $g \in G$, the map π_g which sends

$$x \mapsto gxg^{-1} \tag{5}$$

defines an automorphism on G called **conjugation by** g. One last definition before you get to try your hand at some group theory problems.

Definition 7: *Given a homomorphism $\phi : G \to G'$, we define its **kernel** $\ker \phi$ to be the set of $g \in G$ that get mapped to the identity element in G' by ϕ. Its **image** $\phi(G) \subset G'$ is just its image as a map on the set G.*

The following fact is one tiny wheat germ on the "bread-and-butter" of group theory, and will be used everywhere:

Claim: *If $\phi : G \to G'$ is a group homomorphism, then $\ker \phi \leq G$ and $\phi(G) \leq G'$.*

Proof: We must show that if $g, h \in \ker \phi$, then gh and h^{-1} also belong to $\ker \phi$. (This would already imply that $e \in \ker \phi$, do you see why?) Directly from the definitions,

$$\phi(gh) = \phi(g)\phi(h) = e^2 = e, \tag{6}$$

and thus $gh \in \ker \phi$. Similarly, we obtain the general fact

$$\phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}) \implies \phi(g^{-1}) = \phi(g)^{-1}, \tag{7}$$

which certainly implies that $\ker \phi$ has inverses - thus it is a subgroup of G. Now let x' and y' be two elements of the image $\phi(G)$. Then for some $x, y \in G$, we have $x' = \phi(x)$ and $y' = \phi(y)$, so $x'y' = \phi(xy) \in \phi(G)$. Using the fact from (7) again, we see that $x'^{-1} = \phi(x)^{-1} = \phi(x^{-1}) \in \phi(G)$. □

Okay kid, time for you to go HAM.

EZ EXERCISES:

2.1: Show that $\langle S \rangle$ can be viewed as the set of all strings made up of elements of S and their inverses. That is, prove that for any $S \subset G$:

$$\langle S \rangle = \{s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n} : \forall i,\ s_i \in S,\ \epsilon_i \in \{\pm 1\}\} \tag{8}$$

2.2: Show that for $g, h \in G$, we have $\pi_g \circ \pi_h = \pi_{gh}$, and thus that the map $\pi : G \to \mathrm{Aut}(G)$ defined by

$$g \mapsto \pi_g \tag{9}$$

is a group homomorphism.

2.3: A property $\mathcal{P}$ is called an isomorphism (or structural) property if whenever G has $\mathcal{P}$, and $G \cong G'$, then G' also has $\mathcal{P}$. Prove that being abelian, being cyclic, having exactly 20 elements of order 3, and having exactly 100 automorphisms are all isomorphism properties.

2.4: Show that the set of permutations on the set $\{1, 2, \ldots, n\}$ form a group with function composition as the group operation. This group is called the **symmetric group on n letters**, and is denoted by S_n. Find the order of S_n and prove that for $n \geq 3$, S_n is non-abelian.

2.5: If $|G|$ is even, prove that G contains an element of order 2.

HARD MODE:

2.6: If $\mathrm{Aut}(G) = \{e\}$, show that G is abelian and that every non-identity element of G has order 2.

Define the **center** of a group G, denoted $Z(G)$, as the set of elements which commute with all other elements in G, that is

$$Z(G) := \{g \in G : gh = hg, \ \forall h \in G\}. \tag{10}$$

2.7: Prove that if $|Z(G)| = 1$, then $|\mathrm{Aut}(G)| \geq |G|$. (Hint: show that the map π defined in (9) is injective when G has trivial center.)

2.8: Suppose $S \subset G$ satisfies $2|S| > |G|$. Prove that every element of G can be written in the form $s_1 s_2$, for some elements $s_1, s_2 \in S$. As a corollary, conclude that if $H < G$ is a *proper* subgroup, then $|H| \leq |G|/2$.

2.9: Use the previous exercise to show that all groups of order 5 are isomorphic to $\mathbb{Z}_5$, the group of integers modulo 5.

2.10: Show that a finite group G can never be written as the union of two proper subgroups. (Hint: use (2.8))

3. Cosets, quotients and Lagrange's theorem

Now that you sort of know what a group is, we can prove our first sort of interesting theorem!

Lagrange's Theorem: *If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.*

The proof is rather quick, once we know a few things about *cosets*.

Definition 8: *Given a subgroup $H \leq G$ and an element $g \in G$, the corresponding **left coset** of H in G, written gH, is the set*

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

*Similarly we can define **right cosets**:*

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

Notice that since $e \in H$, we always have $g \in gH$, and thus

$$\bigcup_{g \in G} gH = G. \tag{11}$$

Before deriving the next fact we need about cosets, let's pause to look at an informative and familiar example. Consider the additive group of integers, $\mathbb{Z}$, and the subgroup $(n) := \{nk : k \in \mathbb{Z}\}$ consisting of integers divisible by n. (Notice that this is NOT the coset $n\mathbb{Z}$, because our group operation is addition!) What are the cosets of (n) in $\mathbb{Z}$? Well, by definition they are sets of the form

$$j + (n) := \{j + n \cdot k : k \in \mathbb{Z}\}. \tag{12}$$

You'll notice that some of these sets contain the same elements - in fact, $j + (n)$ is the set of integers congruent to j modulo n, and thus $0 + (n) \cup 1 + (n) \cup \cdots \cup n - 1 + (n)$ already contains every integer. So, when do two cosets $j + (n)$ and $m + (n)$ overlap? Evidently, it's precisely when $j \equiv m \mod n$, which we can rewrite suggestively as

$$j + (n) = m + (n) \iff jm^{-1} \in (n) \tag{13}$$

(remember what this notation means in our additive group!) Let's prove this useful fact in general:

Fact: *An element x belongs to a coset gH if and only if $g^{-1}x \in H$, which happens if and only if $gH = xH$. Thus, distinct cosets are disjoint.*

Proof: Note that $x \in gH \iff x = gh$ for some $h \in G \iff g^{-1}x \in H \iff x^{-1}g \in H \iff g \in xH$. If $x = gh$, then

$$xH = (gh)H = g(hH) = gH, \tag{14}$$

where the last equality follows from the fact that (left) multiplication by h is a bijection from H to itself. □

Thus, the distinct cosets of any subgroup form a *partition* of the whole group. We call the number of distinct cosets of H in G the **index** of H in G, written $|G : H|$. Now we can prove Lagrange's theorem!

Proof of Lagrange's theorem: Let $H \leq G$. Suppose $g_1H, \dots, g_nH$ are the distinct cosets of H in G. Note that

$$h \mapsto g_ih \tag{15}$$

is an invertible map from $H \to g_iH$, and so $|g_iH| = |H|$. Since the set of distinct cosets is a partition of G, we get

$$|G| = \left|\bigcup_{i=1}^{n} g_iH\right| = \sum_{i=1}^{n} |g_iH| = \sum_{i=1}^{n} |H| = n \cdot |H|, \tag{16}$$

and thus not only have we shown that $|H|$ divides $|G|$, but we have shown the formula

$$|G| = |G : H| \cdot |H|. \tag{17}$$

□

Feel free to take some time to play around with Lagrange's theorem and its consequences in this chapter's exercises before reading on. You have my permission.

Thus far, we've kind of neglected the right cosets. This is because we only introduced them to exploit some of their *combinatorial* properties (and because I'm left-handed). However, the most important subgroups in group theory are the **normal subgroups** - those for which the right and left cosets coincide.

Definition 9: *A subgroup $N \leq G$ is called* ***normal*** *(written $N \trianglelefteq G$) if for all $g \in G$, we have the equality of cosets*

$$gN = Ng, \tag{18}$$

which is often expressed equivalently as

$$gNg^{-1} = N. \tag{19}$$

Why do we care if right and left cosets coincide? The reason is that when this happens, we can actually *turn the set of cosets of a subgroup into a group itself*, in the natural way. That is, we want to define the composition of cosets

$$(gN)(hN) = (gh)N. \tag{20}$$

It may at first seem like we don't even need N to be normal - we're just sticking an "N" after everything in G and multiplying, right? The problem is, however, that we need this multiplication to give the same answer *regardless of which representative g of the coset gN we pick.* Remember, we're working with a set of cosets, which is NOT simply the elements of g with an N stuck on the end - that is just notation we use to identify which coset we mean, but we could choose any of the other $|N|-1$ elements of gN to stick in front of the N, and this would be the same coset. Thus, what we need for this group multiplication to be well defined is precisely the condition that

$$gN = g'N \text{ and } hN = h'N \implies (gh)N = (g'h')N \;\; (\iff (h^{-1}g^{-1}g'h')N = N) \tag{21}$$

But remember that characterization we proved about equality of cosets - the condition on the right side of (21) is equivalent to

$$h^{-1}g^{-1}g'h' \in N, \tag{22}$$

but writing $h' = nh$ and $g' = mg$ where $n, m \in N$, we can write condition (22) as

$$h^{-1}g^{-1}mgnh \in N. \tag{23}$$

But if N is normal, then $g^{-1}mg \in N$, and thus $g^{-1}mgn \in N$. Using normality (i.e. conjugation invariance) of N one last time, we see that (22) holds. Thus we have shown that normality of N is a sufficient condition to turn the cosets of N into a group in the canonical way, and in the exercises you will show that this condition is also necessary.

Definition 10: *If N is a normal subgroup of G, then we define the* ***quotient group*** *G/N (read G mod N) to be the set of cosets gN of N in G with the group law*

$$(gN)(hN) = (gh)N. \tag{24}$$

If $N \leq G$ is not normal, then G/N still denotes the set of cosets of N in G, although the above operation is no longer well-defined.

If we return to our motivating example where $G = \mathbb{Z}$ and $N = (n) = n\mathbb{Z}$,[1] we see that (n) is a normal subgroup (because $\mathbb{Z}$ is abelian), and so we can form the quotient group $G/N = \mathbb{Z}/n\mathbb{Z}$ of integers modulo n. In this quotient group, we have "lost some information" about the integers by "zooming out" to a coarser view: everything divisible by n becomes indistinguishable from 0, and consequently the only thing we know about the other integers is their remainder upon division by n. It's a little hard to grasp at first, but you'll get used to it.

Before setting you loose to sink your eager rabid-dog teeth into some exercises, there's one more important theorem I want to squeeze in.

[1] This notation is standard, although a bit confusing, because here $n\mathbb{Z}$ is not meant to be the additive coset $n + \mathbb{Z}$ (which would just be $\mathbb{Z}$), but rather the *multiplicative ideal* generated by n in $\mathbb{Z}$ considered as a *ring*.

The isomorphism theorem:[2] *If $\phi : G \to G'$ is a group homomorphism, then*

$$G/\ker\phi \cong \phi(G). \tag{25}$$

Before providing the proof, let's think about why this theorem makes sense. You've seen that $\ker\phi \leq G$, and you'll show in an exercise that $\ker\phi$ is actually *normal* in G - so the thing on the left side is actually a group. You already know the thing on the right is a group, but why should it be isomorphic to the quotient of G by $\ker\phi$? Intuitively, the image of G under ϕ is kind of like a "zoomed out" version of G, where the "less injective" ϕ is, the further we zoom out. The theorem is trivial if ϕ is injective, so we could try to "make" ϕ injective by identifying everything its kernel with the identity - formally, this is what it means to form a quotient group, and this is exactly how we construct the isomorphism in the isomorphism theorem.

Proof of the isomorphism theorem: Set $K := \ker\phi$ and define the map $\overline{\phi} : G/K \to \phi(G)$ as follows:

$$\overline{\phi}(gK) := \phi(g). \tag{26}$$

Is this map well defined? Well, suppose $gK = hK$. Then $g = hk$ for some $k \in \ker\phi$, and thus

$$\phi(g) = \phi(hk) = \phi(h)\phi(k) = \phi(h)e = \phi(h), \tag{27}$$

which means the map $\overline{\phi}$ is well defined. It is clear that $\overline{\phi}$ is a surjective homomorphism, but it is injective as well, since

$$\phi(g) = \phi(h) \iff \phi(gh^{-1}) = e \iff gh^{-1} \in K \iff gK = hK. \tag{28}$$

□

EXERCISES:

3.1: Show that the order of an element divides the order of a group. Conclude that groups of prime order are cyclic.

3.2: Use Lagrange's theorem to prove Fermat's little theorem: if p is a prime and a is an integer, then

$$a^p \equiv a \mod p. \tag{29}$$

3.3: Provide an example to show that the converse to Lagrange's theorem does not hold.

3.4: If H and K are subgroups of G such that $\gcd(|H|, |K|) = 1$, then $H \cap K = \{e\}$.

[2] If you know some linear algebra, then you might recognize the analogous statement for linear transformations on vector spaces: $V/\ker\phi \cong \phi(V)$. In particular, taking dimensions implies the *rank-nullity theorem.*

3.5: Show that

$$K \trianglelefteq G \iff \exists \text{ a group } G' \text{ and a homomorphism } \phi : G \to G' \text{ s.t. } \ker\phi = K$$

(Hint: for showing the forward direction, consider the map $G \to G/K$ sending $g \mapsto gK$.)

3.6: Show that the intersection of normal subgroups is a normal subgroup, and use this to define $\langle\langle S \rangle\rangle$, the *normal subgroup generated by* $S \subset G$.

3.7: Given $H \leq G$, prove that

$$\bigcap_{g \in G} gHg^{-1} \trianglelefteq G.$$

3.8: Define the **commutator** of two elements $a, b \in G$ as

$$[a, b] := aba^{-1}b^{-1}.$$

Show that the group $G/\langle\langle\{[a, b] : a, b \in G\}\rangle\rangle$ is abelian. (This group is called the *abelianization* of G.)

3.9: Let G be a group and $\mathrm{Aut}(G)$ its group of automorphisms. Show that the group of **inner automorphisms** of G,

$$\mathrm{Inn}(G) := \{\pi_g : g \in G\} \tag{30}$$

is a normal subgroup of $\mathrm{Aut}(G)$.

The following two exercises will make use of *direct products* and *exact sequences.*

Given two groups H and K, we define their **direct product** $H \times K$ to be the group of ordered pairs (h, k) with $h \in H$, $k \in K$ and multiplication defined by

$$(h, k) \cdot (h', k') := (hh', kk'). \tag{31}$$

Given groups A, B, C and homomorphisms $f : A \to B$ and $g : B \to C$, we say the sequence

$$A \xrightarrow{f} B \xrightarrow{g} C \tag{32}$$

is **exact** at B if $\ker g = \mathrm{im} f$.

3.10.1: If $N \trianglelefteq G$, construct homomorphisms f and g such that

$$N \xrightarrow{f} G \xrightarrow{g} G/N \tag{33}$$

is exact at G.

3.10.2: Let H and K be any two groups. Construct homomorphisms f and g such that

$$H \xrightarrow{f} H \times K \xrightarrow{g} K \tag{34}$$

is exact at $H \times K$.

4. Group actions and combinatorics

There's actually quite a lot that can be done using the simple concepts and theorems we've accumulated so far, and it was tough to decide which applications to include in this brief and *friendly* introduction to group theory. Armed with a solid understanding of the previous two chapters, you're prepared to study objects like rings, fields and vector spaces, and eventually take on more formidable topics such as Galois theory, representation theory, and category theory. But here, I'll conclude with a *friendly* introduction to group actions, and some *kawaii* applications to combinatorics.

A *group action* is a formalization of certain "external" properties we often associate to groups - for example, we think of the symmetric group S_n as the group of permutations of the set $\{1, \cdots, n\}$. But really, this is only how we *think* of S_n - as a group, it's just a set of elements with rules for composing them - there is no mention of "permutations" or of the external set $\{1, \ldots, n\}$ in the group axioms. Another example is the dihedral group D_{2n} of plane symmetries of the regular n-gon:

$$D_{2n} := \langle r, s \rangle, \tag{35}$$

where r is a rotation about the n-gon's center by an angle $2\pi/n$, and s is a mirror-flip about a diameter. (If you think about all the different symmetries you get by composing these generating operations, you'll see where the $2n$ comes from.) Again, D_{2n} is just a set with a binary operation, and the n-gon is only flipping around in our heads - that is, until we formally define the group action.

Definition 11: *Given a set X, let*

$$\mathrm{Sym}(X) := (\{f : X \to X : f \text{ is bijective}\}, \circ) = S_{|X|} \tag{36}$$

*then an **action** of a group G on X is a homomorphism*

$$\rho : G \to \mathrm{Sym}(X). \tag{37}$$

It is the homomorphism ρ that encodes all the geometry and combinatorial information we associate "in our heads" with certain groups. Let's write the action down explicitly for the dihedral group D_{10} of plane symmetries of a pentagon P. We label the five vertices 1, 2, 3, 4, 5 consecutively, and let $X = \{\text{vertices}\} = \{1, 2, 3, 4, 5\}$. Since the rotation r just shifts vertex i to vertex $i + 1 \mod 5$, we can write down

$\rho(r)$ as the 5-cycle[3] $(12345) \in S_5$. The flip symmetry s swaps vertices 2 and 5, and 3 and 4 while leaving 1 fixed, and thus $\rho(s) = (1)(25)(34) \in S_5$. Since these two elements generate D_{10}, we can get the value of ρ on the other elements by writing those elements in as products of powers of r and s, and using the homomorphism property. (This is common: to define a homomorphism, it always suffices to define it on a set of generators.)

All groups (not just groups "born" from specific actions like S_n and D_{2n}) have a few natural actions associated to them. One can check that left/right multiplication and conjugation define actions of a group G on itself. Multiplication is a special kind of action, called a **faithful** action, which means that the homomorphism $\rho : G \to \mathrm{Sym}(G)$ is injective. In fact, it satisfies a condition even stronger than injectivity: given any pair of elements $x, y \in G$ there is a *unique* element $g \in G$ such that $\rho(g)(x) = y$ (this is called *sharp transitivity*). Anyway, because we always have a faithful action of G on a set of size $|G|$, we get the following result:

Cayley's Theorem: *If $|G| = n$, then G is isomorphic to a subgroup of S_n.*

Note that $|S_n| = n!$, which grows very large very fast, and so it is often desirable to improve on the bound given by Cayley's Theorem. We have already seen that $D_{2n} \leq S_n$, which is better than Cayley's theorem guarantees. However, finding the minimal k such that a group G imbeds into S_k is generally a *really* hard problem.

I want to prove to you that group actions are not just useless formalism, so let's shift our view towards their combinatorial applications. First we look at a classic type of problem you've all seen before: in how many distinct ways can you arrange $k_1 + k_2 + \cdots + k_n$ objects, k_i (indistinguishable) objects of type i, in a line? Your intuition (or a distant memory of a formula from your MATHCOUNTS days) may tell you that the answer is

$$\frac{(k_1 + k_2 + \cdots + k_n)!}{k_1!k_2!\cdots k_n!}. \tag{38}$$

This is correct, but how do you prove it? Your reasoning might go something like this: there are $(k_1 + k_2 + \cdots + k_n)!$ different orderings of all the objects, but since the k_i objects of each type are indistinguishable, there are $k_i!$ permutations on *these* objects which *stabilize* the overall ordering, so we need to divide by $k_i!$ for each i. It turns out that we can make this kind of argument more rigorous in a more general setting, using group actions. The result is known as the *orbit-stabilizer lemma:*

[3] If you're not familiar with cycle notation for permutations, read it like this: each number gets mapped to the number on its right, except the last number before a parenthesis, which gets sent to the first number in that same set of parenthesis. For example, $(14)(23)(5)$ is the permutation which sends $1 \to 4$, $4 \to 1$, $2 \to 3$, $3 \to 2$ and $5 \to 5$.

Orbit-Stabilizer lemma: *Let G be a group acting on a set X via $\rho : G \to S_{|X|}$. For $x \in X$, we define the* ***orbit*** *and the* ***stabilizer*** *of x, respectively, to be the sets*

$$Gx := \{\rho(g)x : g \in G\}, \quad G_x := \{g \in G : \rho(g)x = x\} \leq G. \tag{39}$$

Then $|Gx| = |G|/|G_x|$.

Before proving the lemma, let's see what it says for our little example: letting $m = k_1 + k_2 + \cdots + k_n$, we see that $G := S_m$ acts naturally on the set X of arrangements in such a way that the orbit of any particular arrangement is the whole set of possible arrangements (this is called a **transitive** action). So we want to find $|Gx|$, for any $x \in X$. Using the lemma, it suffices to find the size of the stabilizer, $|G_x|$, which, after a little thought, we can write down as the set of all permutations π in the direct product $S_{k_1} \times \cdots \times S_{k_n} \leq G$, and so $|G_x| = k_1!k_2! \cdots k_n!$, implying formula (38). Anyway, now that we've made your seventh grade intuition rigorous, let's give a proof of the lemma.

Proof of orbit-stabilizer lemma: It may not be obvious that $G_x \leq G$, but this is always true and you will provide the easy proof in an exercise. Then by Lagrange's theorem, it suffices to find a bijection $\pi : Gx \to G/G_x$ (the set of cosets of the stabilizer G_x in G). Given $y \in G_x$, we can write $y = \rho(g)x$ for at least one $g \in G$. We define

$$\phi(y) := gG_x \in G/G_x, \tag{40}$$

which is well-defined because

$$y = \rho(g)x = \rho(h)x \iff \rho(gh^{-1})x = x \iff gh^{-1} \in G_x \iff gG_x = hG_x. \tag{41}$$

The above equivalences (used going right to left, this time) also prove that π is injective. Surjectivity is obvious since for any $gG_x \in G/G_x$, the element $gx \in Gx$ maps to gG_x under π. □

With a little extra work, we can derive a formula for the total number of orbits $|X/G|$ on a set X acted on by a group G.

Burnside's lemma: *If a finite group G acts (via ρ) on a set X, the total number of orbits in X (written $|X/G|$) is given by the formula*

$$\frac{1}{|G|}\sum_{g\in G}|X^g|, \tag{42}$$

where $X^g = \{x \in X : \rho(g)x = x\} = \{x \in X : g \in G_x\}$.

In words, Burnside's lemma says that the total number of orbits is equal to the average number of elements fixed by G. Let's prove it.

Proof of Burnside's lemma: Since the sum $\sum_{g \in G} |X^g|$ counts the number of times each g appears in a point stabilizer G_x, we have the equality

$$\sum_{g \in G} |X^g| = \sum_{x \in X} |G_x|. \tag{43}$$

Using orbit-stabilizer, we know

$$\sum_{x \in X} |G_x| = \sum_{x \in X} |G|/|Gx| = |G| \sum_{x \in X} \frac{1}{|Gx|}. \tag{44}$$

Now we need to make the observation that X is the *disjoint* union of its orbits (this follows from the fact that if $\rho(g)x = y$ and $\rho(h)y = z$, then $\rho(hg)x = z$), to conclude that

$$\sum_{x \in X} \frac{1}{|Gx|} = \sum_{O \in X/G} \sum_{x \in O} \frac{1}{|O|} = \sum_{O \in X/G} 1 = |X/G| \tag{45}$$

as desired. □

Well that's all for today. I hope this last set of exercises is enough to keep you busy for the remainder of your friendless, internship-less month at home. Class dismissed!

EXERCISES:

4.1: We used Lagrange's theorem to prove the orbit-stabilizer lemma, but now I want you to use the orbit-stabilizer lemma to give a different proof of Lagrange's theorem. (This type of relationship between theorems is usually called "equivalence," although this is somewhat meaningless because all true statements are logically equivalent.)

4.2: If $G \xrightarrow{\rho} \mathrm{Sym}(X)$ is a group action and $x \in X$, show that G_x is a subgroup of G.

4.3: If G has a sharply transitive action on a set X of size 20, what can we say about the size of G?

4.4: A group G with no non-trivial normal subgroups (the trivial ones are G and $\{e\}$) is called a **simple group**. Show that if G is a simple group of order 1000, then all proper subgroups of G have order < 200. (Hint: Consider G acting by left multiplication on the set of left cosets of a subgroup H. This gives a homomorphism of G into a certain symmetric group. What can you say about the kernel of this homomorphism?)

4.5: If we color each of the vertices of a regular pentagon with one of n colors, how many distinct (up to plane symmetry) colorings are possible? (Two colorings are distinct up to plane symmetry if there is no element of D_{10} that can turn one coloring into the other.)

Given an element $g \in G$, we call the set of elements in G that commute with g the **centralizer** of g, written

$$C_G(g) := \{h \in G : hg = gh\} = \{h \in G : hgh^{-1} = g\}. \tag{46}$$

We define the **conjugacy class** of an element $g \in G$ to be the set of all elements conjugate to g, that is,

$$C_g := \{h \in G : h = xgx^{-1},\ \text{for some } x \in G\}. \tag{47}$$

4.6: Prove that $h \in C_g \implies C_g = C_h$, and conclude that G is a disjoint union of conjugacy classes $C_1, \dots, C_k$.

4.7: Prove that $C_G(g)$ is a subgroup of G.

4.8: Prove that $C_g = \{g\} \iff C_G(g) = G \iff g \in Z(G)$.

4.9: Let G be a group with center $Z(G)$ such that $C_1, C_2, \dots C_k$ are the distinct conjugacy classes of *non-central* elements in G - that is, let C_i be distinct conjugacy classes in G such that

$$G - Z(G) = \bigcup_{i=1}^{k} C_i.$$

Derive the *class equation*:

$$|G| = |Z(G)| + |G| \sum_{i=1}^{k} \frac{1}{|C_G(g_i)|}, \tag{48}$$

where $g_i \in C_i$.

4.10: Let G be a finite group with size $|G| = p^n$, where p is a prime and $n \geq 1$. Prove that $|Z(G)| \geq p$.

5. Finitely generated Abelian groups

In this section, we prove a fairly explicit classification of all *finitely generated abelian groups*, that is, commutative groups which are generated by finitely many elements. While this classification can greatly simplify many problems involving abelian groups, it also carries the message that non-commutativity is somehow *essential* for making interesting groups, and for making group theory interesting.

What's the simplest finitely generated abelian group (FGAG) you can think of? The trivial group $\{e\}$, the integers $\mathbb{Z}$, and the integers modulo n, $\mathbb{Z}_n$, are all good answers. Using the direct product operation on groups (defined in exercise 3.9) finitely many times, we can build more FGAGs from these basic groups. That is, any group of the form

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \tag{49}$$

is certainly finitely generated and abelian. We can actually simplify such expressions a bit in the case that $(n_i, n_j) = 1$ for some i and j, using the following lemma.

Lemma 5.1 *If $(n, k) = 1$, then $\mathbb{Z}_n \times \mathbb{Z}_k \cong \mathbb{Z}_{nk}$.*

Proof: It suffices to find an element in $\mathbb{Z}_n \times \mathbb{Z}_k$ of order nk. I claim that $(1, 1)$ is such an element, and this follows from the fact that $\operatorname{lcm}(n, k) = nk$. □

Thus, by applying the above lemma inductively, any G as in (49) can be rewritten so that n_i divides n_{i+1}. It turns out that this actually gives a complete description of all FGAGs.

Theorem (Fundamental theorem of finitely generated abelian groups): *If G is a finitely generated abelian group, then G has the form in (49).*

Proof: We proceed by induction on the minimal number n of generators for G. The case $n = 1$ is trivial, so let $n > 1$ and $\{g_1, \dots, g_n\}$ be a set of generators of G of minimal size. Let $H = \langle g_1, \dots, g_{n-1}\rangle$, and let $K = \langle g_n \rangle$. If $H \cap K = \{1\}$ we are done, since then G splits as $H \times K$ which has the desired form by induction. If not, then there is some $h \in H$ and $i < o(g_n)$ such that $h = g_1^{e_1} \cdots g_{n-1}^{e_{n-1}} = g_n^i$.

6. Sylow's Theorems

7. Free groups and presentations