Group Theory 1
Examples to know, and the isomorphism theorems
by Ivan Aidun

These are notes interspersed with exercises. The purpose of these notes is to be more fleshed out than Evan Dummit's old notes, but shorter and more focused than a textbook treatment. Halfway between Dummit and Dummit and Foote, so to speak. I hope these are helpful to you!

Examples

Here are some groups that you should be familiar with. If you want more examples than you could ever know what to do with, check out this page.

1. Finite abelian groups.
2. The dihedral group D_n, which is the symmetries of a regular n-gon.
3. The symmetric group S_n, which is the group of permutations of a set with n elements.
4. The alternating group A_n, which is the group of even permutations.
5. The quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ subject to the usual laws of quaternion multiplication $i^2 = j^2 = k^2 = ijk = -1$ and $ab = -ba$.
6. The linear groups $\mathrm{GL}_n(R)$, invertible $n \times n$ matrices with entries in R, and $\mathrm{SL}_n(R)$, determinant 1 matrices.
7. The free group F_n on n generators or "letters", which is the group of all "words" (i.e. arbitrary strings) in the generators and their inverses, g_i, g_i^{-1}, subject only to the obvious relation $g_i g_i^{-1} = g_i^{-1} g_i = e$.
8. Given any group G, we can form another group consisting of all the isomorphisms $G \xrightarrow{\sim} G$. This is called the **automorphism group of** G, denoted $\mathrm{Aut}(G)$. For example, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times$, and for a free module R^n over a commutative ring R, $\mathrm{Aut}(R^n) = \mathrm{GL}_n(R)$.

Comment.

- It is common to write the group operation on an arbitrary abelian group as addition, but the group operation on any other arbitrary group as multiplication. There are two reasons why abelian groups get to be different. First, most abelian groups actually do come to us as additive groups of rings. Second, the automorphisms of a group like $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}^2$ are naturally written as multiplication, so if we wrote these groups as multiplication we would be left trying to write their automorphisms as exponentiation, which is somewhat awkward. However, there are times when an abelian group is genuinely better written multiplicatively, e.g. the group of nth roots of unity in $\mathbb{C}$ naturally has group operation multiplication.

For these reasons, I will sometimes distinguish between $\mathbb{Z}/n\mathbb{Z}$ and C_n, the latter being the cyclic group of order n but with group operation written multiplicatively. So, for example, I'd prefer to say "Q admits a surjective homomorphism to C_2" rather than "to $\mathbb{Z}/2\mathbb{Z}$".

- It is standard to denote the identity element of an arbitrary multiplicatively-written group as either e or 1, or e_G or 1_G if the group needs to be specified. In the context of writing exact sequences involving groups, I use 1 to mean the trivial group.
- It is standard to denote a subgroup of a group by using the $<$ symbol rather than $\subset$. For example, "let $H < G$ be a subgroup".
- Some people denote the dihedral groups as D_{2n}, so they write e.g. D_8 to mean what I will call D_4. In this stackexchange post Keith Conrad claims that this is the preferred convention among group theorists (and is the convention in Dummit and Foote).
- The linear groups GL and SL are usually defined over a field, on past quals usually $\mathbb{C}, \mathbb{R}$, or $\mathbb{F}_p$, but you can define these for any commutative ring R, and there has been a question about $\mathrm{SL}_n(\mathbb{Z})$ before (albeit not a very hard one). Note that if R is not a field, then $\mathrm{GL}_n(R)$ consists of invertible $n \times n$ matrices with coefficients in R whose inverse *also* has coefficients in R.
- Topologists and group theorists will sometimes write $\mathbb{F}_n$ for the free group on n letters.

Reminder about normal subgroups

For groups you have to be careful because you can't take a quotient by any subgroup, but rather only by **normal subgroups**. A subgroup $N < G$ is normal if for any $g \in G$, $gNg^{-1} = N$, or equivalently $gN = Ng$, or equivalently for all $n \in N$ there exists $n^g \in N$ so that $gng^{-1} = n^g$. (This condition is required so that coset multiplication works the way you want it to: $(g_1N)(g_2N) = g_1g_2N$.) Normal subgroups are denoted with a triangle: $N \triangleleft G$.

Exercise 1. Let $\phi\colon G \to H$ be a homomorphism. Prove that $\ker\phi$ is a normal subgroup of G.

Exercise 2. (January 2024 Problem 1 (c)) Give an example of a group G and a subgroup H, and a subgroup K of H, such that K is normal in H, and H is normal in G, but K is not normal in G.

The next problem is the first problem I could actually solve when I was studying for the qual.

Exercise 3. (August 2018 Problem 2) For a finite group G, denote by $s(G)$ the number of subgroups of G.

(a) Show that $s(G)$ is finite.

(b) Show that if H is a nontrivial normal subgroup of G, then $s(G/H) < s(G)$.

(c) Show that $s(G) = 2$ if and only if G is cyclic of prime order.

(d) Show that $s(G) = 3$ if and only if G is cyclic of order p^2 for a prime p.

Conjugation and the center

Given an element $h \in G$, an element of the form ghg^{-1} is said to be **conjugate** to h. The set of all elements conjugate to h is called the **conjugacy class** of h. In these notes, I am going to denote the conjugacy class of h by $[h]$. Both Dummit and Foote as well as the book I learned group theory from, *Groups and Symmetry* by Armstrong, avoid giving a notation for the conjugacy class of h. Wikipedia gives $\mathrm{Cl}(h)$, which is sensible, but I don't like it because it collides with the notation for the class group of a number field.

Exercise 4. Prove that a subgroup $H < G$ is normal iff it is a union of conjugacy classes.

The **center** of G, denoted $Z(G)$, is the set of elements $z \in G$ that commute with every other $g \in G$. Equivalently, the center consists of all $z \in G$ so that $[z] = \{z\}$.

Exercise 5. Prove that $Z(G)$ is a normal subgroup of G.

Exercise 6. (January 2018 Problem 4, modified) Let G be a finite group. Denote by $\mathrm{Aut}(G)$ the group of automorphisms of G, and by $Z(G) \subset G$ the center of G.

(a) Let $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$ be the subgroup consisting of automorphisms coming from conjugation, i.e. automorphisms of the form $x \mapsto gxg^{-1}$ for some $g \in G$. Prove that $\mathrm{Inn}(G)$ is isomorphic to $G/Z(G)$.

(b) Show that if $G/Z(G)$ is cyclic, then G is abelian.

(c) Show that if $\mathrm{Aut}(G)$ is cyclic, then G is abelian.

(d) Show that if G is abelian, then $x \mapsto x^{-1}$ is an automorphism of G. (**NB** in fact this is an if and only if.)

(e) Deduce that there is no group G such that $\mathrm{Aut}(G)$ is a nontrivial cyclic group of odd order.

Dihedral groups

Let us imagine a regular n-gon in the plane so that the vertices are on the unit circle at angles $2\pi k/n$, $0 \leq k \leq n-1$. One can show that the dihedral group D_n is generated by a rotation r, say counterclockwise by $2\pi/n$, and a reflection s, say about the horizontal axis. (I do not know why s is the letter chosen for the reflection other than that it is the letter after r. Some texts will instead call these ρ, σ because they're fancy.) The order of r is n, and the order of s is 2, and they have the relationship $srs = r^{-1}$.

We say that D_n has the **presentation** $\langle r, s : r^n, s^2, srsr \rangle$, where writing a string on the right of the presentation is the same as saying "$string = e$ in this group". The relationship $srs = r^{-1}$ means that s and r don't quite commute, but they come close enough that we know what changes we have to make when we try to commute them. So, even though this group is nonabelian, we can still write every element as $s^i r^k$ (or the other way around if you prefer) where $i \in \{0, 1\}$, $0 \leq k \leq n-1$. This idea of using group relations to write elements in a standardized way to make computations easier

is common in group theory, and one often says that the standardized way of writing them is the **normal form**. E.g. in topology, the fundamental group of the Klein bottle is the nonabelian group with presentation $\langle a, b : aba^{-1}b\rangle$, and you can do the same kind of thing to write every element in a normal form like $a^m b^n$.

Exercise 7. (Familiarize yourself with D_n)

(a) Draw or cut out your favorite n-gon ($n \geq 4$ bc triangles are a little misleading sometimes) and visually convince yourself that $srs = r^{-1}$.

(b) Write down the Cayley table (multiplication table) for D_4. Yes, I'm serious.

(c) Find all the subgroups of D_4 and draw its lattice of subgroups. Do the same for D_5.

(d) Find all the distinct conjugacy classes of D_4 and D_5.

(e) Find all the normal subgroups of D_4 and D_5.

Symmetric and alternating groups

The symmetric group S_n consists of all bijections $\pi\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$, with the group operation being function composition. (Using σ, π as the preferred letters for an arbitrary permutation is standard.) One can denote a permutation using "two-line" notation, by writing a two-row matrix with n in the top row and $\pi(n)$ in the bottom row, e.g.:

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

Since the top row is always the same, you can also just write the second line, so the above could just be written as $\pi = 3412$.

However, both of these notations are clunky if we need to compose two permutations, e.g. what is $3412 \circ 3124$? For this reason, nobody actually uses either of those notations. Instead, the good notation is **cycle notation**. A cycle in a permutation is what you get by applying π iteratively to a single element: $n, \pi(n), \pi(\pi(n)), \ldots$. Any given permutation splits up into a disjoint union of cycles, and so we can denote a permutation by its set of cycles. For example, the permutation I wrote as 3412 before has the cycle representation (13)(24), meaning that 1 has been swapped with 3 and 2 with 4. The permutation 3124 has cycle representation (123). (We omit any cycles of length one.)

Cycles are composed right-to-left, like functions, so the composition I asked about in the previous paragraph becomes (13)(24)(123). We can determine the cycle decomposition of the product by tracking each n:

(i) Starting with $n = 1$ and going right-to-left, we have $1 \mapsto 2 \mapsto 4$.

(ii) Since we ended on 4, now we start with 4 and have $4 \mapsto 2$.

(iii) We have $2 \mapsto 3 \mapsto 1$. This completes the cycle (142).

(iv) Only 3 is left, and must be mapped to itself. We can also see that going right-to-left we have $3 \mapsto 1 \mapsto 3$, as expected.

Thus, $(13)(24)(123) = (142)$.

Exercise 8. (Familiarize yourself with S_n)

(a) Compute $(1524)(14)(12)(34)$.

(b) Prove that S_n is generated by elements of the form (ij) (called **transpositions**). (Hint: prove that an arbitrary cycle can be written as a product of transpositions.)

(c) Prove that S_n is generated by elements of the form $(i, i+1)$ (adjacent transpositions).

(d) Prove that S_n is generated by elements of the form $(1i)$.

(e) Prove that S_n is generated by (12) and $(12\dots n)$.

(f) Prove that two elements $\pi_1, \pi_2 \in S_n$ are conjugate iff they have the same **cycle-type**. That is, iff the number and lengths of the cycles in the cycle decomposition of π_1 is the same as for π_2.

(g) Find all the subgroups of S_4 and draw its lattice of subgroups. Which subgroups are normal?

The symmetric group has an important subgroup, the alternating group A_n. By the previous exercise, every permutation can be written as a product of transpositions. The number of transpositions in a given representation is not an invariant of the permutation, but whether that number is even or odd actually is. The group A_n is the subgroup consisting of all even permutations, that is, all permutations whose representation as a product of transpositions has an even number of terms.

Equivalently, S_n can be embedded into $\mathrm{GL}_n(\mathbb{Z})$ as the permutation matrices, and then there is a homomorphism $\mathrm{GL}_n(\mathbb{Z}) \to \{\pm 1\}$ that takes a matrix to its determinant. (A matrix in $\mathrm{GL}_n(\mathbb{Z})$ always has determinant ± 1, because $1 = \det(AA^{-1}) = \det(A)\det(A^{-1})$, but $\det(A)$ and $\det(A^{-1})$ are both integers.) Composing these two maps gives a homomorphism $\epsilon\colon S_n \to \{\pm 1\}$ called the **sign homomorphism**, which is surjective because it takes any transposition to -1. The subgroup A_n is the kernel of this homomorphism, which moreover shows that it is a normal subgroup of S_n.

Exercise 9. (Familiarize yourself with A_n)

(a) Prove that a 3-cycle is even. More generally, any odd-length cycle is even.

(b) Prove that A_n is generated by 3-cycles, (ijk). (Hint: consider products of disjoint transpositions, and products of non-disjoint transpositions.)

(c) Find all the conjugacy classes in A_4.

(d) Give an example of two elements $\pi_1, \pi_2 \in A_4$ so that $[\pi_1] = [\pi_2]$ in S_4 but $[\pi_1] \neq [\pi_2]$ in A_4.

For $n \geq 5$, A_n is a simple group, i.e. it has no nontrivial normal subgroups. (I guess this is also true of A_3 but for a sorta silly reason.)

The quaternion group Q

Exercise 10. (Familiarize yourself with Q)

(a) Find all the conjugacy classes in Q.

(b) Find all the subgroups of Q, and draw its lattice of subgroups. Which subgroups are normal?

Free groups

The free group F_n has the following universal property: given any group G, and any function of sets $f\colon \{1, \ldots, n\} \to G$, there is a unique homomorphism $\widetilde{f}\colon F_n \to G$ such that $\widetilde{f}(g_i) = f(i)$. I don't have any really good questions to test your understanding of this one, if you come up with one let me know.

Isomorphism Theorems

Theorem (first isomorphism theorem)**.** Let $\phi\colon G \to H$ be a group homomorphism. Then $\ker \phi$ is a subgroup of G, $\operatorname{im} \phi$ is a subgroup of H, and the induced homomorphism $G/\ker \phi \to \operatorname{im} \phi$ is an isomorphism. In particular, if ϕ is surjective, then $H \cong G/\ker \phi$.

Theorem (second isomorphism theorem)**.** Let G be a group, $H < G$ a subgroup, and $N \triangleleft G$ a normal subgroup of G. Then $HN = \{hn : h \in H,\ n \in N\}$ is a subgroup of G, N is a subgroup of HN, $(HN)/N$ is a subgroup of G/N, $H \cap N$ is a normal subgroup of H, and the composition $H \hookrightarrow G \twoheadrightarrow G/N$ induces an isomorphism $H/(H \cap N) \xrightarrow{\sim} (HN)/N$.

Theorem (third isomorphism theorem)**.** Let G be a group, N a normal subgroup. Then if H is an subgroup of G such that $N < H < G$, then H/N is a subgroup of G/N. If, moreover, H is also normal, then H/N is normal in G/N, and the composition $G \twoheadrightarrow G/N \twoheadrightarrow (G/N)/(H/N)$ induces an isomorphism $G/H \xrightarrow{\sim} (G/N)/(H/N)$.

Theorem (lattice theorem)**.** The correspondence that takes a subgroup $H < G$ containing a normal subgroup N to the quotient H/N gives a bijection

$$\{\text{subgroups of } G \text{ containing } N\} \xrightarrow{\sim} \{\text{subgroups of } G/N.\}$$

Furthermore, this bijection preserves inclusions, products, and intersections.