Abstract Algebra Review

Ben Marlin

May 2025

1 Review

1.1 Main theorems

1. Lagrange's theorem
2. Cayley's theorem
3. Cauchy's theorem
4. Isomorphism theorems (which come from the universal property of the quotient) and the correspondence theorem
5. Orbit-stabilizer lemma
6. Sylow's theorems
7. Fundamental theorem of finitely generated abelian groups

We do not write out the details of these theorems here because they can be found easily in any textbook or online. You should know the statements of all these theorems and have basic facility with them. Most problems you encounter will use at least one of these theorems in some way.

1.2 Concrete examples

1. (In)finite cyclic groups $\mathbb{Z}/n\mathbb{Z}$ for each $n \geq 0$.
    - Subgroups of cyclic groups are cyclic. There is a unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d for each $d \mid n$. Subgroups of cyclic groups are characteristic.
    - Chinese remainder theorem: $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z}$ if and only if n and m are coprime.
2. Group of units $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.
3. Dihedral groups D_n for $n \geq 3$.

- D_n is a group of order $2n$ consisting of n rotations and n reflections. It is generated by r and s subject to the relations $s^2 = 1$ and $srs = r^{-1}$. The dihedral groups are a common source of examples and counterexamples.

4. Symmetric groups S_n for $n \geq 3$.

   - Every permutation can be written uniquely as the product of disjoint cycles. The order of a permutation is the least common multiple of its disjoint cycle lengths.
   - Elements of S_n are conjugate if and only if they have the same cyclic type. That is, they have the same multiset of disjoint cycle lengths. The conjugacy class of $\sigma \in S_n$ splits into multiple conjugacy classes in A_n if and only if the cycle decomposition of σ is a product of distinct cycles of odd length.
   - Any permutation can be written as the product of 2-cycles (transpositions). If a permutation is a product of an even number of transpositions we call it *even* and if it is the product of an odd number of transpositions we call it *odd*. The collection of all even permutations of S_n form a group called the alternating group A_n. There is a sign homomorphism $\operatorname{sgn} : S_n \to \{-1, 1\}$ sending a permutation to ± 1 depending on its parity. We can realize A_n as the kernel of this map.
   - The commutator subgroup of S_n is A_n.

5. Alternating groups A_n for $n \geq 3$.

   - A_n is generated by 3-cycles. This fact is used to show that the commutator subgroup of S_n is A_n.
   - A_n is simple for $n \geq 5$. In fact, A_5 is the smallest non-abelian simple group at size 60.

6. Group of quaternions Q_8.

   - Q_8 is a non-abelian group of order 8 not isomorphic to D_4. It is often a source of counterexamples. For example, Q_8 is an example of a non-abelian group where nonetheless every subgroup is normal.

7. Matrix groups such as $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{SL}_n(\mathbb{R})$, and $\mathrm{SO}_n(\mathbb{R})$ among others.

It may be a useful exercise to see if you can compute the conjugacy classes, center, commutator subgroup, and abelianization of these concrete examples. Understanding concrete examples and the main theorems of the course well will be very helpful for the final exam.

In the next few sections, we review some miscellaneous topics that could be useful.

1.3 Group actions

Definitions and remarks: Recall that a (left) action of a group G on a set X is a function $G \times X \to X$ such that $ex = x$ and $(gh)x = g(hx)$ for all $x \in X$ and $g, h \in G$. Equivalently, it is a homomorphism $G \to \mathrm{Sym}(X)$. If G acts on X, we define the orbit $Gx = \{gx \mid g \in G\}$ and the stabilizer $G_x = \{g \mid gx = x\}$ for all $x \in X$. As a consequence of the orbit stabilizer lemma and Lagrange's theorem, if G is a finite group, then the size of any orbit or stabilizer divides the order of G. In particular, the size of any conjugacy class of G divides the order of G.

We give some important examples:

- Any group G acts on itself by conjugation. The orbits of this action are precisely the conjugacy classes of G. The stabilizers are precisely the centralizers of elements of G.
- Any group G acts on itself by left multiplication. By considering the homomorphism induced by this action, we immediately get Cayley's theorem.
- If $H \leq G$, then G acts on the collection of left cosets of H by left multiplication. Equivalently, there is a homomorphism $\varphi : G \to \mathrm{Sym}(G/H)$. Very often, if you encounter a problem where you are given some information about the index of a subgroup, it is a good idea to consider this homomorphism. The kernel of φ is precisely $\mathrm{core}(H) = \bigcap_{g \in G} gHg^{-1}$.

1.4 Center and commutator subgroups

1. Recall that if G is a group then $Z(G)$ consists of all elements of G that commute with all other elements. In other words, it is the kernel of the homomorphism induced by the action of G on itself by conjugation.
   - An important fact about the center is that finite nontrivial p-groups have nontrivial center. This a consequence of the class equation (see if you can prove it!)
   - Another useful fact is that if $G/Z(G)$ is cyclic then G is abelian. This fact can be used to show that any group of order p^2 for a prime p is abelian (you should definitely know this latter fact).
2. Recall that if G is a group then its commutator subgroup $[G, G]$ is the subgroup generated by all commutators, i.e., generated by elements of the form $a^{-1}b^{-1}ab$. It is easy to verify that $[G, G]$ is characteristic, hence normal in G.
   - The commutator subgroup has a special property: $G/[G, G]$ is abelian and if H is any normal subgroup such that G/H is abelian then $[G, G] \subseteq H$. This tells us that $[G, G]$ is the smallest normal subgroup with an abelian quotient. We call $G/[G, G]$ the abelianization of G.

- This property is often useful for computing the commutator subgroup directly. For example, let us see how to prove $[S_n, S_n] = A_n$. First, note that A_n is generated by 3-cycles and any 3-cycle can be written as a commutator. Thus, $A_n \subseteq [S_n, S_n]$. How do we see the other inclusion? Well, $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$, which is abelian, so $[S_n, S_n] \subseteq A_n$.

1.5 Results on normal subgroups

1. Suppose $H \leq G$. If $[G : H] = 2$, then H is normal in G.

2. Suppose G is a finite group and p is the smallest prime dividing the order of G. Then, any subgroup H such that $[G : H] = p$ is normal in G.

3. Suppose $H \leq G$. Then, H is normal if in G if and only if H is a union of conjugacy classes. Note, however, that it is possible to have a union of conjugacy classes that is not a group at all, i.e., it is important we assume $H \leq G$ for this to work.

4. Suppose $H \leq G$ and consider the action of G by left multiplication on the set of cosets G/H. This induces a map $\varphi : G \to \mathrm{Sym}(G/H)$ with $\ker(\varphi) = \mathrm{core}(H) := \bigcap_{g \in G} gHg^{-1}$. In particular, if H is of finite index in G, then there exists a finite index normal subgroup of G contained in H.

5. Normality is not transitive in general. However, if H is normal in G and K is characteristic in H, then K is normal in G.

Product groups:

1. External direct product: If G and H are any groups, we can form their product group $G \times H$ with multiplication given coordinate-wise. Product groups play a prominent role in many classification problems such as the classification of finitely generated abelian groups.

2. Internal direct product: How can we identify when a group is isomorphic to an external direct product? We say that G is an internal direct product of subgroups H and K if $G = HK$, $H \cap K = 1$, and H and K are normal in G (this last condition is equivalent to $hk = kh$ for $h \in H$ and $k \in K$). If G is an internal direct product of H and K, then $G \cong H \times K$.

2 Practice Problems

1. Suppose that $G/H \cong K$ for some groups G, H, and K. Is it true that $G \cong K \times H$? Prove or give a counterexample.

2. Is the image of a group homomorphism always a normal subgroup? Prove or give a counterexample.

3. If G and H are groups, we can form their direct product $G \times H$. Are all subgroups of $G \times H$ of the form $G_0 \times H_0$ for some $G_0 \leq G$ and $H_0 \leq H$? Prove or give a counterexample.

4. Prove that $\mathbb{R}/\mathbb{Z} \cong S^1$, where S^1 is the circle group.

5. Prove that $(\mathbb{Q}, +)$ is not finitely generated.

6. Prove that there are no simple groups of order 81.

7. Prove that there are no simple groups of order 750.

8. Prove that there are no simple groups of order 20.

9. Classify all groups of order 77.

10. Compute the abelianization of D_n for $n \in \mathbb{N}$. Hint: consider the cases of n odd and n even separately.

11. Suppose that G is a group with normal subgroup N. Further, suppose N has a unique subgroup H of order k for some $k \in \mathbb{N}$. Prove that H is a normal subgroup of G.

12. Give an example of a group G such that $G = [G, G]$.

13. Prove that Q_8 is not isomorphic to D_4.

14. Prove that any non-abelian group G of order 6 is isomorphic to S_3. Hint: show that G has an element y of order 2 such that $\langle y \rangle$ is not normal. Then, consider the action of G on the cosets $G/\langle y \rangle$.

15. Suppose that G is an abelian group of order $2n$ where n is odd. Prove that there is a unique element $\iota \in G$ of order 2.

16. How many abelian groups of order 225 are there (up to isomorphism)?

17. Prove that any finite group is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbb{R})$. Studying group homomorphisms into general linear groups is the subject of (finite-dimensional) representation theory!

18. Consider the set $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ consisting of homomorphisms $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Describe a natural group structure on this set. To which familiar group is this group isomorphic? Can you describe $\mathrm{Hom}(\mathbb{Z}^k, \mathbb{Z}/n\mathbb{Z})$ up to isomorphism?