Summary of Introductory Group Theory

Daniel Gottesman

March 3, 2026

1 Basic Definitions

Definition 1. *A* group *G is a set with a multiplication rule satisfying the following axioms:*

- **Closure***: $g, h \in G \implies gh \in G$.*
- **Associativity***: $g, h, k \in G \implies (gh)k = g(hk)$.*
- **Identity***: $\exists e \in G$ such that $\forall g \in G$, $eg = ge = g$. e is called the* identity *element of the group.*
- **Inverse***: $\forall g \in G$, $\exists g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$. g^{-1} is the* inverse *of g.*

An Abelian *group satisfies the following additional axiom:*

- **Commutativity***: $\forall g, h \in G$, $gh = hg$.*

A group that is not Abelian is called a non-Abelian *group.*

For Abelian groups, multiplication is sometimes written as addition, i.e., we write $g + h$ instead of gh, the identity is written as 0, and the inverse of g is written as $-g$. For groups using multiplicative notation, the identity is sometimes written as 1.

Examples of infinite Abelian groups include the integers or the real numbers (using addition as the group "multiplication"), or the real numbers *without* 0 using multiplication as the group multiplication.

Exercise 1. *The integers (even without* 0*) are not a group using multiplication. Why not? Why do we need to exclude* 0 *for the real numbers to be a group under multiplication?*

Some useful finite Abelian groups are the integers $\mathbb{Z}_n$ modulo n under addition (that is, take the numbers $0, \ldots, n-1$ as the set, and group addition is defined by regular integer addition, taking only the remainder when the sum is divided by n). When $n = p$ is prime, the integers (without 0) modulo p also form a group under multiplication, written $\mathbb{Z}_n^*$.

Examples of finite non-Abelian groups are the permutation groups S_n consisting of permutations of n (distinguishable) objects.

Exercise 2. *Show that S_n is a group.*

We can also combine groups with a direct product structure by taking multiple copies of a group. The direct product $G \times H$ is the set consisting of pairs (g, h) with the multiplication rule $(g, h) \cdot (g', h') = (gg', hh')$.

Definition 2. *The* order *$|G|$ of a finite group G is the number of elements in the underlying set.*

The order of $\mathbb{Z}_n$ is n. The order of S_n is $n!$.

Definition 3. *A* field *$\mathbb{F}$ is a set with two operations, addition and multiplication, with the following properties:*

- *The field forms an Abelian group under addition.*
- *The field without the additive inverse* 0 *forms an Abelian group under multiplication.*
- **Distributivity***:* $x, y, z \in \mathbb{F} \implies x(y+z) = xy + xz$.

Examples of infinite fields are the real numbers, the rational numbers, and the complex numbers. Examples of finite fields are $\mathbb{Z}_p$, the integers modulo a prime p.

An abstract vector space is an abelian group (written additively) with a scalar multiplication by elements of a field. A 1-dimensional vector space over the field $\mathbb{F}$ is just equal to $\mathbb{F}$. The additive group for an n-dimensional vector space is the direct product of n copies of $\mathbb{F}$.

Definition 4. *The* direct product $G \times H$ *of two groups* G *and* H *is formed from the set* $G \times H$ *of ordered pairs* (g, h) *(*$g \in G$*,* $h \in H$*) with multiplication rule* $(g, h) \cdot (g', h') = (gg', hh')$.

Exercise 3. *Show that* $G \times H$ *is a group. What is the identity? What is the inverse of* (g, h)*?*

2 Subgroups

Definition 5. *A* subgroup H *of a group* G *is a subset of* G *which itself forms a group under the multiplication operation for* G*. That is,* H *is closed under multiplication and inverse, and contains the identity for* G*. The notation* $H \leq G$ *means that* H *is a subgroup of* G*.*

Any subgroup of the integers consists of multiples of some number. Thus, all even numbers form one subgroup of $\mathbb{Z}$, and all numbers divisible by 25 form another subgroup. An example of a subgroup of S_n is the set of cyclic permutations (starting from some particular ordering of the objects being permuted).

Theorem 1 (Lagrange's theorem)**.** *Suppose* $H \leq G$*, with* G *and* H *finite groups. The order of* G *is a multiple of the order of* H*.*

Definition 6. *The* left coset gH *of the subgroup* $H \leq G$ *(with* $g \in G$*) is the set* $\{gh | h \in H\}$*. The* right coset Hg *of* H *is the set* $\{hg | h \in H\}$*. In these cases* g *is called a* coset representative *for the left and right cosets* gH *and* Hg*.*

For groups written additively, we instead write $g + H$ for a coset. Note that the coset $eH = H$ and that $gH = g'H$ iff $g^{-1}g' \in H$. Thus, the cosets of a subgroup partition the group G. Also note that each coset has the same number of elements as H; this proves Lagrange's theorem.

Note that only the coset of the identity is a subgroup of G.

Definition 7. *Suppose* $H \leq G$*.* H *is a* normal *subgroup of* G *(written* $H \lhd G$*) iff left cosets of* H *are equal to the corresponding right cosets of* H*. That is,* $\forall g \in G$*,* $gH = Hg$*.*

For an Abelian group, all subgroups are normal. For a non-Abelian group, normal subgroups tell us a great deal about the structure of the group and play a critical role in group theory. Some groups have no nontrivial normal subgroups. (The identity element forms a subgroup, which is always normal; the full group is also always a normal subgroup of itself.)

Definition 8. *The* center $Z(G)$ *of the group* G *is the set of elements that commute with everything in the group:* $Z(G) = \{h | gh = hg \ \forall g \in G\}$*.*

Exercise 4. *Prove that* $Z(G) \lhd G$*.*

Definition 9. *Let* $S \subseteq G$ *be a set of group elements. Then the* subgroup generated by S*, sometimes denoted* $\langle S \rangle$*, is the smallest subgroup containing* S*. That is,* $\langle S \rangle$ *consists of all (finite) products (in any order, when* G *is non-Abelian) of elements of* S *and their inverses.* S *is called a* generating set *for the subgroup* $\langle S \rangle$*. A group is* cyclic *if it has a single-element generating set.*

Thus, in the integers, $\langle 2 \rangle$, the subgroup generated by just the element 2, consists of all even numbers, whereas 1 generates the full group of integers. The integers and all the groups $\mathbb{Z}_n$ are cyclic, since they each can be generated by the element 1.

Exercise 5. *Show that $\langle 6, 15 \rangle$, the subgroup of $\mathbb{Z}$ generated by 6 and 15, is equal to $\mathbb{Z}_3$, which consists of all numbers divisible by 3.*

Frequently we are interested in minimal generating sets for a group or subgroup — that is, sets for which removing even one element would mean generating a smaller group.

3 Homomorphisms

Definition 10. *Let G and H be groups. A function $f : G \to H$ is a* homomorphism *iff $\forall g, g' \in G, f(gg') = f(g)f(g')$.*

That is, a homomorphism is a function that preserves the group multiplication. Note that for a homomorphism f, $f(e) = e$ and $f(g^{-1}) = [f(g)]^{-1}$.

For example, the homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ are linear functions $k \mapsto ck$ (for integer c, k). We can also have homomorphisms $\mathbb{Z}$ to $\mathbb{Z}_n$. For instance, the map "take the remainder of k modulo n" is such a homomorphism.

Definition 11. *A homomorphism $f : G \to H$ which has an inverse homomorphism f^{-1} (that is, $f^{-1} : H \to G$ such that $f(f^{-1}(h)) = h \ \forall h \in H$ and $f^{-1}(f(g)) = g \ \forall g \in G$) is called an* isomorphism. *If there is an isomorphism from G to H, G and H are* isomorphic. *An isomorphism from G to itself is called an* automorphism.

Clearly isomorphic finite groups have the same order, so for instance, $\mathbb{Z}_n$ and $\mathbb{Z}_m$ are not isomorphic unless $m = n$, in which case there is an obvious isomorphism. However, there are also finite groups which have the same order but are not isomorphic. For instance, the direct product group $\mathbb{Z}_2 \times \mathbb{Z}_2$ (which has order 4) is not isomorphic to the cyclic group $\mathbb{Z}_4$ (which also has order 4).

Definition 12. *For any element $h \in G$, consider the map $f_h : G \to G$ defined by $f_h(g) = hgh^{-1}$. This is known as* conjugation by h. *The map f_h is called an* inner automorphism.

Thus, an equivalent definition of a normal subgroup is a subgroup H for which $f_g(H) = H$ for all $g \in G$. The inner automorphisms are good examples of nontrivial automorphisms of a group (at least, they are generally non-trivial for a non-Abelian group).

Exercise 6. *Prove that f_h is an automorphism from G to G. Show that the automorphism equals the identity iff $h \in Z(G)$.*

Definition 13. *Let $f : G \to H$ be a homomorphism. The kernel $K(f)$ of f is the set $\{g \in G \mid f(g) = e\}$.*

Theorem 2. *The kernel $K(f)$ of any homomorphism is a normal subgroup of G.*

Exercise 7. *Prove this.*

A more difficult and deep theorem is the converse:

Theorem 3. *Let $N \lhd G$. Then there exists group H and homomorphism $f : G \to H$ such that $N = K(f)$.*

To show this, we develop the notion of a quotient group:

Definition 14. *Let $N \lhd G$. Then the* quotient group *G/N is the set of cosets of N with multiplication defined by $(gN)(g'N) = (gg')N$.*

Theorem 4. *G/N is a group. If G is Abelian, then so is G/N.*

Proof. It's not even immediately obvious that this multiplication rule is well-defined, but it is, because N is a normal subgroup: suppose we pick different coset representatives $h \in gN$ and $h' \in g'N$ (so $gN = hN$ and $g'N = h'N$). Then we need to show that $(gg')N = (hh')N$; that is, that

$$(gg')^{-1}(hh') = g'^{-1}(g^{-1}h)h' \in N. \tag{1}$$

We know that $n = g^{-1}h \in N$. But since N is normal, $g'^{-1}N = Ng'^{-1}$. That means $\exists n' \in N$ such that $g'^{-1}n = n'g'^{-1}$. (Note that n' may not be equal to n, however.) Thus,

$$g'^{-1}(g^{-1}h)h' = (g'^{-1}n)h' = n'(g'^{-1}h'). \tag{2}$$

This is in N since $n' \in N$ and $g'^{-1}h' \in N$, and since N is a subgroup, and is therefore closed under multiplication.

From here it is easy to verify the group axioms. Closure and associativity are pretty much trivial. The identity element of G/N is the coset of the identity eN. The inverse of a coset gN is the coset $g^{-1}N$. If G is Abelian, then

$$(gN)(g'N) = (gg')N = (g'g)N = (g'N)(gN). \tag{3}$$

□

This enables us to prove theorem 3. When N is a normal subgroup, there is a fairly obvious homomorphism from G to $H = G/N$, namely, $g \mapsto gN$.

Exercise 8. *Show that $g \mapsto gN$ defines a homomorphism and show that N is the kernel of this map.*

Other interesting constructions are the normalizer and centralizer of a subgroup.

Definition 15. *The* normalizer $N_G(H)$ *of a subgroup $H \leq G$ is the largest subgroup of G for which H is a normal subgroup, $H \lhd N_G(H)$. The* centralizer $Z_G(H)$ *of H in G is the largest subgroup of G for which all elements of H commute with all elements of $Z_G(H)$.*

Thus, for instance, if G is Abelian, $N_G(H) = Z_G(H) = G$.

Exercise 9. *Show that $N_G(H) = \{g \,|\, g^{-1}hg \in H \,\forall h \in H\}$ and $Z_G(H) = \{g \,|\, g^{-1}hg = h \,\forall h \in H\}$. When is $H \leq N_G(H)$? When is $H \leq Z_G(H)$?*