# Handout 1: Group Theory Review

This course is all about the representation theory of finite groups. Thus some knowledge about group theory is a must. I assume you have taken Math 261 and Math 361, but perhaps you feel a bit rusty? Let's review.

## 1.1 · The Basics

**DEFINITION 1.1**

A **group** is a set $G$ with an operation $* : G \times G \to G$ such that the following axioms hold.

1. **(Associativity)** $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
2. **(Existence of Identity)** There is an element $1 \in G$ such that $1 * a = a * 1 = a$ for all $a \in G$.
3. **(Existence of Inverses)** For every $a \in G$, there is an element $b \in G$ such that $a * b = b * a = 1$.

When working with an abstract group we often simplify the notation by writing $ab$ instead of $a * b$. This is referred to as expressing the operation as *juxtaposition*, which is a fancy way of saying that we write the elements right next to each other. Inverses are unique and we write $a^{-1}$ to denote the inverse of $a$.

Groups typically contain many smaller groups living within them.

**DEFINITION 1.2**

Let $G$ be a group. A subset $H \subseteq G$ is called a **subgroup** if

1. $1 \in H$,
2. $h^{-1} \in H$ for all $h \in H$, and
3. $h_1 h_2 \in H$ for all $h_1, h_2 \in H$.

As the name suggests, every subgroup $H \subseteq G$ is itself a group.

The intersection of any collection of subgroups is again a subgroup. If $S \subseteq G$ is any arbitrary subset of $G$, we let $\langle S \rangle$ denote the smallest subgroup of $G$ containing $S$. That is,

$$\langle S \rangle := \bigcap_{\substack{S \subseteq H \subseteq G \\ H \text{ subgroup}}} H.$$

We call $\langle S \rangle$ the **subgroup generated by** $S$. If $S = \{g\}$ consists of a single element, then we simply write $\langle g \rangle$ instead of $\langle \{g\} \rangle$. Subgroups of the form $\langle g \rangle$ are called **cyclic subgroups** and they have a simple description:

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

**DEFINITION 1.3**
The **order** of a group $G$ is the cardinality of $G$, denoted $|G|$ or $\text{ord}(G)$. The order of an element $g \in G$ is denoted $\text{ord}(g)$ and is defined to be $\text{ord}(g) := |\langle g \rangle|$. A **finite group** is a group with finite cardinality.

## 1.2 · Cosets

If $G$ is a group and $S, T \subseteq G$ are subsets, then we write

$$ST := \{st : s \in S, t \in T\}$$

for the set of all products (in that particular order!) of elements of $S$ and $T$. If $S = \{s\}$ is a singleton, then we often write $sT$ in place of $\{s\}T$. Likewise, when $T$ is a singleton.

I like to refer to $sT$ as the *translation* of $T$ by $s$. For example, if $G = \mathbb{Z}$ is the group of integers, $T = \{0, 1, 2\}$ and $s = 5$, then

$$s + T = 5 + \{0, 1, 2\} = \{5, 6, 7\}.$$

Thus $s + T$ is literally $T$ translated 5 to the right. This example is a good intuition to keep in mind for thinking about sets of the form $sT$.

Now suppose that $H \subseteq G$ is a subgroup. Then sets of the form $gH$ with $g \in G$ are given the special name of **(left) cosets** of $H$. In this case we say $g$ **represents** the coset $gH$, although $g$ is just one of many such representatives. Let $G/H := \{gH : g \in G\}$ denote the set of all left cosets of $H$ and let $H\backslash G$ denote the set of all right cosets of $H$. The left and right cosets of $H$ are typically different from one another, both equally valid and useful, but we tend to use left cosets more since the notation looks nicer, among other conveniences.

Any given coset has multiple representatives. The following lemma is the key to showing two cosets are equal.

**LEMMA 1.4** (Coset Equality Criterion)
Let $H \subseteq G$ be a subgroup. Then $g_1H = g_2H$ if and only if $g_2^{-1}g_1 \in H$.

In words this says two elements $g_1, g_2 \in G$ represent the same coset of $H$ if and only if they differ by an element of $H$.

**EXAMPLE 1.5**
The key example to keep in mind is when $G = \mathbb{Z}$ and $H = \langle m \rangle$ is the cyclic subgroup generated by some $m \in \mathbb{Z}$. In this group our operation is additive, hence Lemma 1.4 reduces to saying $n_1 + \langle m \rangle = n_2 + \langle m \rangle$ if and only if $n_1 - n_2 \in \langle m \rangle$, which is to say that $m$ divides $n_1 - n_2$. Recall from number theory that this is precisely the definition of what it means to say that $n_1 \equiv n_2 \bmod m$. Hence in this case cosets of $\langle m \rangle$ correspond to congruence classes modulo $m$. The concept of cosets generalizes congruences modulo $m$ from the integers to congruence modulo a subgroup $H$ of an arbitrary group $G$. So keep this example close to your heart when thinking about more general cosets.

The **index** of $H$, denoted $[G : H]$, is the cardinality of $G/H$ (or $H\backslash G$, the cardinalities are the same). The following theorem is an essential result of group theory.

**THEOREM 1.6** (Lagrange's Theorem)
If $G$ is a finite group and $H \subseteq G$ is a subgroup, then

$$|G| = [G : H]|H|.$$

In particular, the order of every subgroup of $G$ divides the order of $G$.

Lagrange's theorem imposes rigid arithmetic constraints on the orders of subgroups and elements of a finite group. For example, Lagrange's theorem implies that every group of prime order must be cyclic.

## 1.3 · Homomorphisms

**DEFINITION 1.7**
Let $G_1, G_2$ be groups with operations $*_1$ and $*_2$, respectively. A function $\varphi : G_1 \to G_2$ is called a **homomorphism** if

$$\varphi(g *_1 h) = \varphi(g) *_2 \varphi(h)$$

for all $g, h \in G_1$. An invertible homomorphism is called an **isomorphism**. If there exists an isomorphism between $G_1$ and $G_2$, then we say $G_1$ and $G_2$ are **isomorphic** and write $G_1 \cong G_2$.

Homomorphisms are the *right kind of function* between groups; they are the maps which respect the group structure. From the definition you may deduce that homomorphisms map the identity of one group to the identity of the other and map inverses to inverses. Compositions of homomorphisms are homomorphisms.

To every homomorphism there are two important associated subgroups, one in the domain and the other in the codomain.

**DEFINITION 1.8**
If $\varphi : G \to H$ is a homomorphism, then the **kernel** of $\varphi$ is the subgroup $\ker(\varphi) \subseteq G$ defined by

$$\ker(\varphi) := \{g \in G : \varphi(g) = 1\}.$$

The **image** of $\varphi$ is the subgroup $\mathrm{im}(\varphi) \subseteq H$ defined by

$$\mathrm{im}(\varphi) := \{h \in H : h = \varphi(g) \text{ for some } g \in G\}.$$

These subgroups determine the injectivity and surjectivity of $\varphi$.

**PROPOSITION 1.9**
If $\varphi : G \to H$ is a homomorphism, then

1. $\varphi$ is injective if and only if $\ker(\varphi) = \{1\}$,
2. $\varphi$ is surjective if and only if $\mathrm{im}(\varphi) = H$.

The main content of Proposition 1.9 is part one: whenever you need to show a homomorphism is injective, this is the first tool you should reach for. The second part of this proposition is a tautology, but we include it to highlight the duality of the kernel and the image.

## 1.4 · Normal Subgroups and Quotients

**DEFINITION 1.10**
If $g, h \in G$, then we call $ghg^{-1}$ the **conjugate** of $h$ by $g$. Similarly if $H \subseteq G$ is a subgroup, then we call $gHg^{-1}$ the **conjugate subgroup** of $H$ by $g$. A **normal subgroup** $N \subseteq G$ is a subgroup such that $gNg^{-1} = N$ for all $g \in G$. We write $N \trianglelefteq G$ to denote that $N$ is a normal subgroup of $G$.

Despite their name, normal subgroups are quite special. Normal subgroups of $G$ are precisely those subgroups which are the kernels of some homomorphism.

**THEOREM 1.11**
A subgroup $N \subseteq G$ is normal if and only if there is a group $H$ and a homomorphism $\varphi : G \to H$ such that $N = \ker(\varphi)$.

Like many if and only if statements, this theorem has an easy direction and a hard direction. It is straightforward to show that kernels are always normal. For the other direction, we start with a normal subgroup $N \trianglelefteq G$ and need to produce from it a homomorphism which has $N$ as its kernel. This is done via the *quotient group* construction.

**THEOREM 1.12**
Let $N \trianglelefteq G$ be a normal subgroup. The operation $g_1N *_{G/N} g_2N := (g_1 *_G g_2)N$ on cosets $G/N$ is well-defined and makes $G/N$ into a group with identity $1N = N$. The map $\rho_N : G \to G/N$ defined by $\rho_N(g) := gN$ is a surjective homomorphism and $\ker(\rho_N) = N$.

We call $G/N$ the **quotient** of $G$ by $N$, or $G$ **modulo** $N$, and we call the homomorphism $\rho_N$ the **reduction modulo** $N$ map, or simply **mod** $N$. There is a convenient alternative notation for quotient groups which the aspiring number theorists among us may find especially enticing: We write $g \bmod N$ in place of the coset $gN$, and we write $g_1 \equiv g_2 \bmod N$ to mean $g_1N = g_2N$. The coset equality criterion implies this is also equivalent to $g_2^{-1}g_1 \in N$. Instead of thinking of the elements of $G/N$ as cosets, we can think of the elements as the same as elements of $G$ with the same operation, but with *equality* replaced by *congruence modulo* $N$. When $N$ is a normal subgroup, Theorem 1.12 implies that we may do algebra with congruences modulo $N$, freely replacing elements with anything they may be

congruent to.

Quotient groups naturally arise as the images of homomorphisms.

**THEOREM 1.13** (First Isomorphism Theorem)
If $\varphi : G \to H$ is a surjective homomorphism, then there is a well-defined isomorphism $\overline{\varphi} : G/\ker(\varphi) \to H$ given by

$$\overline{\varphi}(g\ker(\varphi)) := \varphi(g).$$

With this theorem in mind, I will often refer to any surjective homomorphism $\varphi : G \to H$ as a **quotient** of $G$. Indeed, Theorem 1.13 implies that every such $\varphi$ is a reduction modulo $N$ map composed with an isomorphism.

## 1.5 · Abelian Groups

Generally speaking, group operations do not satisfy the commutative property. We give a special name to those groups which do satisfy this property.

**DEFINITION 1.14**
We say a group $G$ is **abelian** if $gh = hg$ for all $g, h \in G$.

Cyclic groups are always abelian. If $G$ and $H$ are abelian, then so is their **direct product**

$$G \times H := \{(g, h) : g \in G, h \in H\},$$

where the operation is defined componentwise. Every subgroup of an abelian group is normal. This allows us to state a more satisfying version of Proposition 1.9 for abelian groups.

**DEFINITION 1.15**
If $\varphi : G \to H$ is a homomorphism between abelian groups, then the **cokernel** of $\varphi$ is defined by

$$\operatorname{coker}(\varphi) := H/\operatorname{im}(\varphi).$$

Thus in this case we have that $\varphi$ is surjective if and only if $\operatorname{coker}(\varphi) \cong \{1\}$. You can think of a finite abelian group $G$ as a generalization of an integer. Integers factor uniquely into a product of primes, and finite abelian groups factor uniquely as a direct product of $p$-groups. Recall that if $p$ is a prime, then a $p$-**group** is any finite group $H$ such that $|H|$ is a power of $p$.

**PROPOSITION 1.16**
Let $G$ be a finite abelian group and let $p$ be prime. Then there are $p$-subgroups $G_{(p)} \subseteq G$ such that

$$G \cong \prod_{p \mid \operatorname{ord}(G)} G_{(p)}.$$

Proposition 1.16 tells us that finite abelian groups may be diffracted into a direct product of

$p$-power pieces where $p$ varies through all the primes dividing $|G|$. Life is not so simple for non-abelian groups.

## 1.6 · Important Families of Groups

Here we review several families of groups which you should keep in mind.

### 1.6.1 Dihedral Groups

Let $n \geq 2$ be an integer. We define the **$n$th dihedral group** $D_n$ via the following presentation,

$$D_n := \langle r, s : r^n = s^2 = (sr)^2 = 1 \rangle.$$

This means $D_n$ is generated by two elements $r$ and $s$ and the only algebraic relations in $D_n$ are those which may be derived from the identities listed here. From these relations we can show that $\text{ord}(r) = n$ and $\text{ord}(s) = 2$. The last relation is often expressed as $sr = r^{-1}s$ or equivalently $srs = r^{-1}$. The natural interpretation of $D_n$ is that it is the group of linear symmetries of a regular $n$-gon: $r$ corresponds to a $2\pi/n$ counterclockwise rotation and $s$ corresponds to reflection across the $x$-axis. The group $D_n$ has order $|D_n| = 2n$ (note: some texts write $D_{2n}$ for what we call $D_n$. The $n$ corresponds to the size of the polygon whose symmetry group is $D_n$.) The subgroup $\langle r \rangle$ of rotations is a normal subgroup of $D_n$.

### 1.6.2 Affine Groups

Let $R$ be a commutative ring and let $R^\times$ be the multiplicative group of units in $R$. The **affine group** of $R$ is defined by

$$\text{Aff}(R) := \{ax + b : a \in R^\times, b \in R\},$$

where the operation is composition of functions: If $\ell_i(x) = a_i x + b_i$ for $i = 1, 2$, then

$$\ell_1 \ell_2 := \ell_1(\ell_2(x)) = a_1(a_2 x + b_2) + b_1 = (a_1 a_2)x + (a_1 b_2 + b_1).$$

If $R$ is a finite ring, then $|\text{Aff}(R)| = |R^\times||R|$. For example, if $R = \mathbb{Z}/n\mathbb{Z}$, then

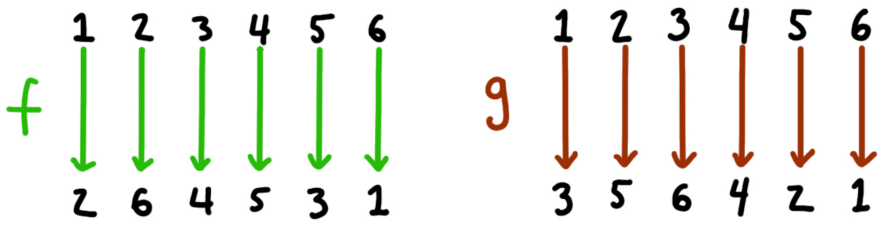
$$|\text{Aff}(\mathbb{Z}/n\mathbb{Z})| = \phi(n)n.$$

The subgroup $\{x + b : b \in R\} \cong R$ of translations is a normal subgroup of $\text{Aff}(R)$ and the quotient $\text{Aff}(R)/R$ is isomorphic to $R^\times$.

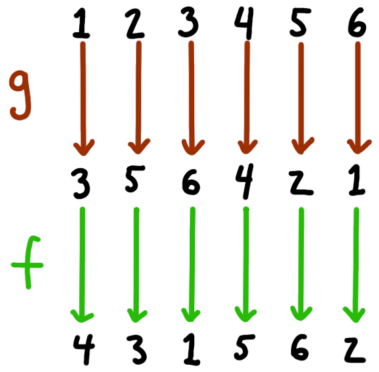
### 1.6.3 Symmetric Groups

Let $X$ be a set. A **permutation** of $X$ is a bijection $f : X \to X$. The **symmetric group** of $X$, denoted $S_X$, is the group of all permutations $f$ of $X$ where the operation is composition of functions. If $X$ is finite, then $|S_X| = |X|!$. Up to isomorphism, the group $S_X$ only depends on the cardinality of $X$. Hence it is convenient to pick some concrete models. For $n \geq 1$, let $S_n$ denote the symmetric group of the set $\{1, 2, \ldots, n\}$.

We can visualize a permutation $f$ by drawing a graph with an arrow $i \to j$ when $f(i) = j$. Since $f$ is a permutation, there will be exactly one arrow emanating from and arriving at each element in $\{1, 2, \ldots, n\}$. For example, if $f, g \in S_6$ are the permutations defined by

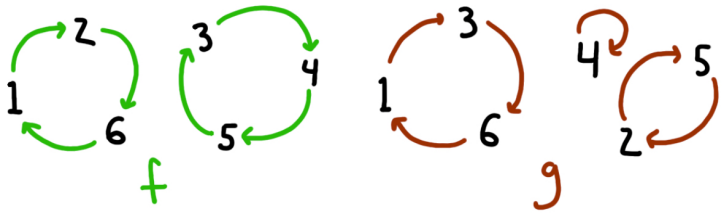



This visualization is convenient for composing permutations: we just link the arrows head to tail.




Note that composition of permutations is generally not commutative, so it's important to pay attention to which order you combine them.

This sort of picture is useful for composing permutations, but there is another picture we can draw that better illuminates the structure of the permutation. The idea is to write each element of $X$ one time, and then connect two points in $X$ with an arrow to show how the function maps each element.




This is called the **cycle decomposition** of a permutation. We can extract a convenient notation for permutations from the cycle decomposition. For each cycle, we pick a point $x_0$ in that cycle and write the elements of the cycle in order starting from $x_0$. We put each cycle in parentheses, and write these cycles next to each other,

$$f = (126)(345), \qquad g = (136)(4)(25).$$

We say that two cycles are **disjoint** if they do not have any elements in common. Thus every permutation may be expressed as a product of disjoint cycles. The order in which we write disjoint cycles does not matter.

When a point is fixed by a permutation, it belongs to a cycle of length 1. The common convention is to not bother writing the fixed points at all:

$$g = (136)(25).$$

The identity permutation fixes everything, so by this logic it would seem that we shouldn't bother writing this permutation. Most of the time that is true, but sometimes we will want to talk about the identity permutation, and in that case we denote it by $\varepsilon$.

In cycle notation, we write the group operation by juxtaposition, so

$$fg = (126)(345)(136)(25).$$

Notice that these cycles are not all disjoint, so in order to get them back into a product of disjoint cycles, we need to work out the composition.

So how does composition work? Let's work out the composition $(145)(48)(5968)$ step-by-step.

1. Pick an arbitrary element of $X$ to get started. When working with numbers, I usually just pick the smallest number 1, and write down a cycle beginning with 1.

   $$(1$$

2. Plug 1 into the rightmost cycle. Since $(5968)$ does not have a 1 in it, this cycle does nothing to 1, so it outputs 1 again.

3. Next take that outputted 1 and plug it into the next cycle, which is $(48)$. Again, nothing happens since there is no 1 here.

4. Finally we reach the last cycle $(145)$, which does have a 1 in it. This tells us that 1 maps to 4. Hence we write 4 as the next entry in our composition:

   $$(14$$

5. Now we repeat this process starting back at the right again, but plugging in 4. The first cycle $(5968)$ does not contain a 4, so nothing happens and we move on to the second cycle.

6. The second cycle $(48)$ has a 4 in it. This tells us that the second cycle maps 4 to 8, hence the output of the second cycle is 8.

7. We then take that 8 and plug it into the last cycle $(145)$, which does not contain an 8, so nothing happens. We record

   $$(148$$

8. We keep working on this cycle until we come back to the starting point. So let's begin again with 8 as an input. The first cycle $(5968)$ maps 8 back around to 5.

9. The second cycle $(48)$ does nothing to 5, so we then pass 5 to the last cycle $(145)$, which maps 5 to 1.

10. Therefore this composition of permutations maps 8 back to 1, completing our first cycle,

    $$(148).$$

11. Next we pick a number that shows up in one of our original cycles but is not in (148) and we start this whole process again. I usually pick the next smallest number that has not already appeared, which in this case would be 5.

$$(148)(5$$

12. This process repeats until this cycle closes, like this

$$(148)(596),$$

and now we have seen all 6 of the distinct numbers appearing in our original composition.

13. We conclude that

$$(145)(48)(5968) = (148)(596).$$

Cycle notation gives us a simple way to check if two permutations are conjugate. The **cycle type** of a permutation $f \in S_n$ is the number of cycles $f$ has of each length (including fixed points). If $f$ has $m_j$ cycles of length $j$, then we write

$$\lambda_f := (1^{m_1} 2^{m_2} \cdots n^{m_n})$$

to record the cycle type of $f$. For example, if $f = (34)(567)(89) \in S_9$, then $f$ has two fixed points (1 and 2), two 2-cycles, and one 3-cycle. Hence

$$\lambda_f = (1^2 2^2 3^1).$$

Note this is not a product, just a compact notation.

**PROPOSITION 1.17**
Two permutations $f, g \in S_n$ are conjugate if and only if they have the same cycle type.

For any $n \geq 2$ there is a surjective homomorphism $\operatorname{sgn}_n : S_n \to \mu_2$, where $\mu_2$ is the multiplicative group with elements $\{\pm 1\}$ called the **sign homomorphism**. There are several ways to construct the sign homomorphism, but it may be characterized as the unique homomorphism $\operatorname{sgn}_n : S_n \to \mu_2$ such that $\operatorname{sgn}_n(ij) = -1$ for each 2-cycle $(ij)$. The kernel of $\operatorname{sgn}_n$ is called the $n$**th alternating group** $A_n$.

### 1.6.4 General Linear Groups

Let $R$ be a commutative ring and let $n \geq 1$. The $n$**th general linear group** $\mathrm{GL}_n(R)$ is the group of $n \times n$ invertible matrices with entries in $R$. The operation is matrix multiplication. We will discuss these groups in more detail when we review linear algebra.