Math 211 - Group Theory

New concepts will be written in **bold**, and new formulas will be $\boxed{\text{boxed}}$.

Material which you have already encountered in Math 113 will be marked as such.

Details in the proofs that we purposely leave out of the notes, so that you may work out for yourselves, will be colored in blue. Ask your instructors (in person / on the forum) for help.

Table of contents:

Lecture 1

1.1

Change is one of the most interesting and important things in mathematics. Formally, the way we set this up is to consider a set X, and interpret a function

$$f : X \to X$$

as a "transformation" of X. In plain English, if x is an element of the set X before the transformation, then $f(x) \in X$ denotes how this element changes after the transformation. For example:

- Let $X = \{0, 1, \ldots, n-1\}$ denote the set of vertices of a regular n-gon, and let $f : X \to X$ denote some rotation or reflection that preserves the entire n-gon. However, f might change the individual vertices, for example it might send the vertex $x \in X$ to the vertex $f(x) \in X$.

- Imagine you have n locations indexed by the set $X = \{1, \ldots, n\}$, and that you label each location with a post-it note. A **permutation** is a function $f : X \to X$ which controls how the post-it notes are moved from one location to another, but with no more or less than one post-it note per location. Mathematically, the function f encodes the fact that we move the post-it from location $f(x)$ to location x, for every $x \in X$.

1.2

So what happens when we have two transformations

$$f : X \to X \quad \text{and} \quad g : X \to X$$

and we want to perform (or as mathematicians say, "apply") them in succession? This is very easy: applying the transformation g first and then f later is the same thing as directly applying the

$$\textbf{composition} \quad \boxed{f \circ g : X \to X} \quad \text{given by } (f \circ g)(x) = f(g(x)),\ \forall x \in X \tag{1}$$

In the first example on the previous page, this setup would mean that we apply

- two rotations, or
- two reflections, or
- a rotation and a reflection, or
- a reflection and a rotation

one after the other. If you draw a picture of this, then you will observe that the resulting transformation in the four cases above will be a rotation, rotation, reflection, reflection, respectively.

1.3

What about the question of when a transformation can be "undone", i.e. instead of going from x to $f(x)$ we go from $f(x)$ to x, for all $x \in X$? Mathematically, this is modeled by the notion of invertible transformation, namely a function $f : X \to X$ which has an **inverse**

$$\boxed{f^{-1} : X \to X} \tag{2}$$

whose defining property is that

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}_X \tag{3}$$

Above and henceforth, we write

$$\boxed{\mathrm{Id}_X : X \to X} \tag{4}$$

for the **identity** function which sends every $x \in X$ to itself. Intuitively, the identity does not really change anything, but we still consider it to be a "transformation". It has the property that

$$f \circ \mathrm{Id}_X = \mathrm{Id}_X \circ f = f \tag{5}$$

for any function $f : X \to X$.

Lemma 1. *If a function $f : X \to X$ has an inverse, then such an inverse is unique.*

Proof. Let's assume that the function f has two inverses $g_1 : X \to X$ and $g_2 : X \to X$. Formula (2) implies that

$$f(g_1(x)) = g_1(f(x)) = x \tag{6}$$

$$f(g_2(x)) = g_2(f(x)) = x \tag{7}$$

for all $x \in X$. If we apply formula (6) with x replaced by $g_2(x)$, then we infer that

$$g_1(f(g_2(x)) = g_2(x)$$

for all $x \in X$. However, if we apply the function g_1 to both sides of (7), we infer that

$$g_1(f(g_2(x)) = g_1(x)$$

for all $x \in X$. Comparing the two equalities above implies $g_1(x) = g_2(x)$ for all $x \in X$, i.e. the "two" inverses g_1 and g_2 are actually one and the same function.

□

1.4

It might seem like the proof above relies on a bunch of mathematical tricks, but this is not actually the case. In fact, Lemma 1 stems from the fact that a function $f : X \to X$ is invertible if and only if it is **bijective**, which means that it is both

- **injective:** whenever $x \neq x'$ are elements of X, we have $f(x) \neq f(x')$, and
- **surjective:** for any $y \in X$, there exists some $x \in X$ such that $f(x) = y$.

If a function is bijective, then for every y there exists a single x such that $f(x) = y$. Formulas (2) then force us to set $f^{-1}(y) = x$, which implies that the inverse is uniquely determined. This gives an intuitive argument for the validity of Lemma 1.

1.5

One of the great things about using mathematics to formalize transformations is that it makes it easy to do computations with them. For instance, recall the example in the first bullet in Subsection 1.1: a rotation preserves a regular n-gon P if and only if we rotate counterclockwise by an angle of $\frac{2\pi k}{n}$ radians around the center of P for some integer k. In formulas then, the corresponding function on the set of vertices $\{0, 1, \ldots, n-1\}$ takes the form

$$f_k : X \to X, \qquad f_k(x) = x + k \bmod n \tag{8}$$

(recall that $z \bmod n$ denotes the remainder of the integer z upon division by the natural number n, and that this remainder is an element of the set $\{0, 1, \ldots, n-1\}$). While the integer k can be arbitrary, only its residue class modulo n matters in formula (8), since $f_k = f_{k+n}$ for all $k \in \mathbb{Z}$. Geometrically, this says that

$$\frac{2\pi k}{n} \text{ radians is the same angle as } \frac{2\pi(k+n)}{n} = \frac{2\pi k}{n} + 2\pi \text{ radians}$$

Meanwhile, the reflections which preserve the regular n-gon P correspond to the functions

$$g_k : X \to X, \qquad g_k(x) = -x + k \bmod n \tag{9}$$

for some integer k. As before, only the residue class of k modulo n matters, because $g_k = g_{k+n}$ for all $k \in \mathbb{Z}$. Thus, we have exactly n rotations and n reflections which preserve the regular n-gon, and formulas (8) and (9) give us all the tools that we need to work with them. For instance, we may explicitly calculate the composition of two reflections g_k and g_ℓ by

$$g_k \circ g_\ell(x) = g_k(g_\ell(x)) = g_k(-x + \ell \bmod n) = x + k - \ell \bmod n$$

and the result is clearly a rotation (by $\frac{2\pi(k-\ell)}{n}$ radians).

1.6

Let's now use formulas to describe the example of permutations, i.e. the second bullet in Subsection 1.1. Permutations (for $n = 6$ in the examples below) will be represented as

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 6 & 5 & 3 \end{pmatrix} \tag{10}$$

which means that we move the put the post-it note 4 on location 1, the post-it note 2 on location 2, the post-it note 1 on location 3 etc. The composition of permutations is calculated by stacking permutations on top of each other. For instance, if we're trying to calculate $f \circ g$ where f is given by the formula (10) and g is given by formula

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 2 & 4 \end{pmatrix}$$

then we calculate $f \circ g$ by putting g above (because it is applied first) and f below (because it is applied second; note that we rearrange the columns of f so that its top row is compatible with the bottom row of g)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 2 & 4 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix} \qquad \Rightarrow \qquad f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix}$$

As for the inverse permutation f^{-1}, it is calculated by switching the two rows of (10) and then reordering the columns so as to have the numbers on the top row in increasing order:

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 1 & 5 & 4 \end{pmatrix}$$

The identity permutation is simply $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$.

1.7

The composition of transformations enjoys three important properties: the existence of the identity function (4) satisfying property (5), the existence of inverses (2) satisfying property (3), as well as

$$\boxed{f \circ (g \circ h) = (f \circ g) \circ h} \tag{11}$$

for all functions $f, g, h : X \to X$. Indeed, both sides of formula (11) represent the function $x \mapsto f(g(h(x)))$, which implies that they are equal to each other. Property (11) is called **associativity**. The features of compositions of functions listed above can be abstracted in the following notion.

Definition 1. *A **group** (as you learned in Math 113) is a set G endowed with*

- *an element $e \in G$ called the **identity***
- *for any element $g \in G$, an element $g^{-1} \in G$ called the **inverse***
- *for any two elements $g, h \in G$, an element $gh \in G$ called the **product** of g and h.*

which are required to satisfy the following properties

$$ge = eg = g, \qquad \forall g \in G \tag{12}$$

$$gg^{-1} = g^{-1}g = e, \qquad \forall g \in G \tag{13}$$

$$g(g'g'') = (gg')g'', \quad \forall g, g', g'' \in G \tag{14}$$

Two important examples of groups (which correspond to the two bullets in Subsection 1.1, and that you learned in Math 113) are the **dihedral group**

$$\boxed{D_{2n}} = \Big\{\text{rotations and reflections that preserve a regular } n\text{-gon}\Big\} \tag{15}$$

and the **symmetric group**

$$\boxed{S_n} = \Big\{\text{permutations, i.e. bijections } \{1, \dots, n\} \to \{1, \dots, n\}\Big\} \tag{16}$$

In both cases, the identity is the identity function, the inverse is given by inverse functions, and the product of elements is given by composition of functions. Recall that $|D_{2n}| = 2n$ (there are exactly n rotations and n reflections that preserve a regular n-gon) while $|S_n| = n!$. Both D_n and S_n are **finite** groups, in that they have finitely many elements.

1.8

Formulas (12), (13), (14) are not just coincidentally similar to (4), (2), (11), but the former are modeled after the latter. In other words, groups are simply the abstract mathematical structures which describe transformations of various sets X. This connection is made even more concrete by the following notion, which is central to many fields of mathematics (such as representation theory).

Definition 2. *An action of a group G on a set X is an assignment*

$$\forall g \in G \quad \rightsquigarrow \quad \text{a bijection } \Phi_g : X \to X \tag{17}$$

which respects

- *the identity, in the sense that*
$$\Phi_e = \mathrm{Id}_X \tag{18}$$

- *the inverse, in the sense that*
$$\Phi_{g^{-1}} = (\Phi_g)^{-1}, \qquad \forall g \in G \tag{19}$$

- *the product, in the sense that*
$$\Phi_{gg'} = \Phi_g \circ \Phi_{g'}, \quad \forall g, g' \in G \tag{20}$$

We will indicate an action, i.e. the assignment (17), by the symbol

$$\boxed{G \curvearrowright X} \tag{21}$$

Although rather imprecise, we will henceforth abbreviate the bijections Φ_g by the symbol

$$\boxed{\Phi_g(x) = g \cdot x}$$

for all $g \in G, x \in X$. With this in mind, formula (18) takes the form $e \cdot x = x$, while (20) reads

$$(gg') \cdot x = g \cdot (g' \cdot x) \tag{22}$$

for all $g, g' \in G$ and all $x \in X$.

Remark. *Note that properties* (18) *and* (19) *are actually superfluous, i.e. they follow from* (20) *and the fact that all the Φ_g are bijections. Indeed, just apply* (20) *for $g' = e$ and you will obtain*

$$\Phi_g = \Phi_{ge} = \Phi_g \circ \Phi_e$$

Composing with $(\Phi_g)^{-1}$ implies precisely (18)*. Then if we invoke* (22) *for $g' = g^{-1}$ we obtain*

$$\mathrm{Id}_X = \Phi_e = \Phi_{gg^{-1}} = \Phi_g \circ \Phi_{g^{-1}}$$

which implies (19)*.*

1.9

By their very construction (but you are encouraged to check this rigorously) the examples in the two bullets in Subsection 1.1 are equivalent to actions

$$D_{2n} \curvearrowright \left\{\text{vertices of a regular } n\text{-gon}\right\} \tag{23}$$

and

$$S_n \curvearrowright \{1, \ldots, n\} \tag{24}$$

respectively. In fact, the latter example can be generalized as follows.

Definition 3. *For any set X, we let*

$$S_X = \left\{\textit{bijections } X \to X\right\}$$

made into a group using the composition of functions. Then there is an action

$$S_X \curvearrowright X$$

simply by having every bijection $\sigma \in S_X$ act on X by σ itself.

Besides the examples of actions above, there are two special actions of a group on itself, as follows.

Definition 4. *For every group G, its **left action** $G \curvearrowright G$ is the assignment*

$$h \cdot g = hg, \quad \forall g, h \in G \tag{25}$$

Definition 5. *For every group G, its **adjoint action** $G \curvearrowright G$ is the assignment*

$$h \cdot g = hgh^{-1}, \quad \forall g, h \in G \tag{26}$$

Proposition 1. *The assignments* (25) *and* (26) *are well-defined actions.*

Proof. As we showed at the end of Subsection 1.8, it suffices to check that each Φ_g is a bijection, and that formula (22) holds. We will do so for the adjoint action, and leave the analogous case of the left action as an exercise to you. To check that $g \mapsto hgh^{-1}$ is a bijective function of g for every fixed $h \in G$, note that

$$hgh^{-1} = hg'h^{-1} \quad \Rightarrow \quad hg = hg' \quad \Rightarrow \quad g = g'$$

thus proving injectivity, while

$$h(h^{-1}gh)h^{-1} = (hh^{-1})g(hh^{-1}) = ege = g, \quad \forall g \in G$$

thus proving surjectivity. Finally, to show (22), we note that

$$(hh') \cdot g = hh'gh'^{-1}h^{-1} = h(h'gh'^{-1})h^{-1} = h \cdot (h' \cdot g)$$

for all $g, h, h' \in G$, as required. Note that all these checks made heavy use of associativity.

□

1.10

Let us now explore how the notion of action interacts with the notion of group homomorphism, which you learned in Math 113.

Definition 6. *Let G and G' be two groups, each with their own notions of identity element, inverse and product. A function*

$$f : G \to G'$$

is called a ***homomorphism*** *if it preserves*

- *the identity elements, in the sense that*
$$f(e) = e' \tag{27}$$
where e is the unit in G and e' is the unit in G'

- *the inverses, in the sense that*
$$f(g^{-1}) = (f(g))^{-1} \tag{28}$$
with the LHS involving the inverse in G and the RHS involving the inverse in G'.

- *the products, in the sense that*
$$f(gh) = f(g)f(h) \tag{29}$$
with the LHS involving the product in G and the RHS involving the product in G'.

As before, some of properties (27), (28) and (29) are superfluous: either the first or the second of them follow from the other two. Try proving this for practice.

1.11

A homomorphism which is also bijective function is called an **isomorphism**. If there exists an isomorphism between two groups G and G', we will denote this as

$$\boxed{G \cong G'} \tag{30}$$

and say that G and G' are isomorphic.

Lemma 2. *If $f : G \to G'$ is an isomorphism between two groups G and G', then its inverse*

$$f^{-1} : G' \to G$$

is also an isomorphism.

Proof. The inverse of a bijection is a bijection, so it remains to show that the inverse is also a homomorphism. As we explained at the end of Subsection 1.10, it suffices to check (27) (which is obvious, since the fact that $f(e) = e'$ implies $f^{-1}(e') = e$) and (29). Indeed, (29) follows from

$$gh = (f^{-1} \circ f)(gh) = f^{-1}(f(gh)) = f^{-1}(f(g)f(h))$$

for all $g, h \in G$. If we replace g and h by $f^{-1}(g)$ and $f^{-1}(h)$ in the relation above, we obtain

$$f^{-1}(g)f^{-1}(h) = f^{-1}(f(f^{-1}(g))f(f^{-1}(h))) = f^{-1}(gh)$$

which is exactly what we needed to prove.

□

1.12

The formalism of groups, actions and homomorphisms comes together within the following result.

Proposition 2. *To give an action of a group G on a set X is the same as to give a homomorphism*

$$G \to S_X \tag{31}$$

(recall the group S_X in Definition 3).

Proof. It is clear that the assignment $g \rightsquigarrow \Phi_g$ corresponds to a function (31). To show that the former assignment being an action is equivalent to the latter function being a homomorphism boils down to showing that properties (18), (19), (22) correspond to (27), (28), (29). This is a tautology, i.e. a mathematical statement which is obvious once you unpack it (though unpacking it is a useful exercise; please try your hand at it and ask one of your instructors if you're stuck).

□

Lecture 2

2.1

Let G be a group. Recall from Math 113 that a subset $H \subseteq G$ is called a **subgroup**, denoted by

$$\boxed{H \leq G} \tag{32}$$

if H is closed under

- the identity, in the sense that $e \in H$
- the inverse, in the sense that $g \in H$ implies $g^{-1} \in H$
- the product, in the sense that $g, g' \in H$ implies $gg' \in H$

If the conditions above hold, then H is a group in its own right, and the inclusion function

$$\iota : H \hookrightarrow G$$

is a homomorphism. In general, for any homomorphism

$$f : G \to G'$$

the image of f is a subgroup of G'. If moreover f is injective, then $\boxed{\text{Im } f \cong G}$.

2.2

We will now see how the language of actions allows us to describe general features of groups. The following theorem is due to Cayley.

Theorem 1. *Any group G is a **permutation group**, i.e. a subgroup of S_X for some set X.*

Thus, any group can be realized as "living" inside some group of permutations (if G is finite, then we will see that the set X can be chosen to be finite, and so every finite group is a subgroup of the symmetric group S_n for some $n \in \mathbb{N}$). To this end, let us consider any action $G \curvearrowright X$ and recall the homomorphism (31). The following is an easy result, which you proved in Math 113.

Lemma 3. *A homomorphism $f : G \to G'$ is injective if and only if its kernel*

$$\boxed{\text{Ker } f} = \left\{ g \in G \text{ s.t. } f(g) = e' \right\}$$

*is the **trivial** subgroup $\{e\} \leq G$.*

With the Lemma above in mind, we see that (31) is injective if and only if its kernel is trivial. However, in the context of a group action, this kernel can be explicitly described as

$$\left\{ g \in G \middle| g \cdot x = x, \forall x \in X \right\}$$

and it is called the **kernel of the action**. In other words, the kernel of the action consists of all those elements of G which act on X by the identity transformation. Thus, to prove Theorem 1, it suffices to find an action of G whose kernel is just the trivial subgroup, i.e. only the identity element of G acts on X by the identity transformation (such an action is called **faithful**). To this end, we simply choose the left action of G on $X = G$ from Definition 4: any element $g \neq e$ of G acts on G by sending e to g, and thus cannot act by the identity transformation.

2.3

Any action $G \curvearrowright X$ induces an equivalence relation on X via

$$x \sim y \quad \Leftrightarrow \quad \exists g \in G \text{ s.t. } g \cdot x = y \tag{33}$$

Properties (18), (19) and (20) precisely ensure that the above equivalence relation is reflexive, symmetric and transitive, respectively (try and prove this yourself, it's a great exercise).

Definition 7. *An equivalence class with respect to the relation* (33) *is called an* ***orbit*** *of the action* $G \curvearrowright X$*. It can be written as*

$$\boxed{G \cdot x} = \Big\{ g \cdot x \Big| g \in G \Big\} \tag{34}$$

and it will be called the "orbit of x*" (although any other* $y \sim x$ *has the same orbit as* x*).*

An action is called **transitive** if all elements of X are in one and the same orbit.

Definition 8. *Given an action* $G \curvearrowright X$ *and any element* $x \in X$*, its* ***stabilizer*** *is defined as*

$$\boxed{\mathrm{Stab}_G(x)} = \Big\{ g \in G \text{ s.t. } g \cdot x = x \Big\} \tag{35}$$

Prove for yourself that the stabilizer is always a subgroup of G*.*

The kernel of a group action, which we have already encountered, is by definition the intersection of the stabilizers of all elements $x \in X$. An action is called **free** if all stabilizers are equal to $\{e\}$. For instance, the action (23) is transitive, but it is not free (as there exist vertices which are preserved by reflections). However, the action of the subgroup of rotations in D_{2n} on the vertices is free.

2.4

As with any equivalence relation, X can be partitioned into the disjoint union of the orbits of a group action $G \curvearrowright X$. However, we can say more when G is finite.

Proposition 3. *If* $G \curvearrowright X$ *is an action of a finite group* G *on a set* X*, then we have*

$$|G \cdot x| = \frac{|G|}{|\mathrm{Stab}_G(x)|} \tag{36}$$

for every $x \in X$*.*

The result above is called the **orbit-stabilizer theorem**. When both G and X are finite, the fact that X is the disjoint union of its orbits means that (36) implies the following equation

$$|X| = \sum_{\text{orbits } G \cdot x} |G \cdot x| = \sum_{\text{orbits } G \cdot x} \frac{|G|}{|\mathrm{Stab}_G(x)|} \tag{37}$$

(while the set $\mathrm{Stab}_G(x)$ might change when modifying x within a given orbit, its cardinality does not change; try to prove the previous claim, although it implicitly follows from the proof below).

Proof. of Proposition 3: recall the description of orbits from (34). For fixed $x \in X$, the function

$$G \to G \cdot x, \qquad g \mapsto g \cdot x \tag{38}$$

is surjective. Let us compute how many elements are in the preimage of any element $g \cdot x$ of the function (38). In other words, we seek to count how many $g' \in G$ have the property that

$$g' \cdot x = g \cdot x \quad \Leftrightarrow \quad g^{-1}g' \cdot x = x \quad \Leftrightarrow \quad g^{-1}g' \in \text{Stab}_G(x) \quad \Leftrightarrow \quad g' \in \left\{ gh \middle| h \in \text{Stab}_G(x) \right\}$$

Since the elements gh (as h varies) are all distinct (prove this), there are $|\text{Stab}_G(x)|$ elements in the preimage of every element with respect to the function (38). This immediately proves (36). □

2.5

Let us continue working in the context of an action of a group G on a set X. While the stabilizer (35) describes the set of elements of G that fix a certain element $x \in X$, there exists the "mirror" notion of the set of elements of X that are fixed by any given $g \in G$

$$\boxed{X^g} = \left\{ x \in X \middle| g \cdot x = x \right\} \tag{39}$$

In general, all we can say is that X^g is a subset of X. But when X is finite, we have the following formula that is often called "Burnside's Lemma", although it goes back to Cauchy and Frobenius. It is a very useful count of the number of orbits in a group action

Lemma 4. *If G is a finite group acting on a finite set X, then*

$$\left| \text{orbits of } G \curvearrowright X \right| = \sum_{g \in G} \frac{|X^g|}{|G|} \tag{40}$$

Proof. The Lemma is a simple combinatorial exercise. Specifically, let us rewrite (40) as

$$|G| \cdot |\text{orbits of } G \curvearrowright X| = \sum_{g \in G} |X^g| \tag{41}$$

The right-hand side counts the number of pairs

$$(g, x) \in G \times X \text{ s.t. } g \cdot x = x$$

If we interpret this number as a sum over $x \in X$, we conclude that the right-hand side of (41) is

$$\sum_{x \in X} |\text{Stab}_G(x)|$$

Using Proposition 3, we see that the number above is

$$\sum_{x \in X} \frac{|G|}{|G \cdot x|}$$

We may replace the sum over $x \in X$ as a sum over the orbits; however, every orbit $G \cdot x$ appears a number of $|G \cdot x|$ times in the above sum, so we conclude that the number above is

$$\sum_{\text{orbits } G\cdot x} |G|$$

which is precisely the left-hand side of (41).

□

2.6

When H is a subgroup of a group G, the orbits of the left action

$$H \curvearrowright G, \qquad h \cdot g = hg$$

are called **right cosets**. The slightly unusual terminology is due to the fact that the orbits in question are explicitly given by the formula

$$\boxed{Hg} = \Big\{ hg \Big| h \in H \Big\} \tag{42}$$

in which g is on the right. The mirror image of this notion stems from the so-called **right action**

$$H \curvearrowright G, \qquad h \cdot g = gh^{-1}$$

(please check that the formula above satisfies all the properties of an action, much as we did for the left action of Definition 4) whose orbits are called **left cosets**

$$\boxed{gH} = \Big\{ gh \Big| h \in H \Big\} \tag{43}$$

Indeed, as h runs over H, the set of elements of the form gh^{-1} matches the set of elements of the form gh, due to the subgroup $H \leq G$ being closed under taking inverses. Both the left and right actions are free, in the sense that

$$\text{Stab}_H(g) = \{e\}, \quad \text{because } hg = g \text{ or } gh^{-1} = g \text{ if and only if } h = e \tag{44}$$

for all $g \in G$.

Definition 9. *Let* $\boxed{G/H}$ *(respectively* $\boxed{H\backslash G}$*) denote the set of left (respectively right) cosets of* G *with respect to a subgroup* H*.*

Let us now assume that G is finite, and $H \leq G$ is an arbitrary subgroup. Because of (44), Proposition 3 implies that every left or right coset has exactly $|H|$ elements. Since G is partitioned into either left or right cosets, we conclude that the number of such cosets is exactly

$$|G/H| = |H\backslash G| = \frac{|G|}{|H|} \tag{45}$$

One often denotes the number above by $\boxed{[G:H]}$ and calls it the **index** of the subgroup H of G.

2.7

Recall from Math 113 that the **order** of a finite group is its cardinality, i.e. its number of elements. With this in mind, (45) implies a foundational result in the theory of finite groups due to Lagrange

$$\textbf{the order of a group } G \textbf{ is a multiple of the orders of any of its subgroups} \tag{46}$$

In particular, we can take any $g \in G$ and consider the subgroup of G generated by g, i.e.

$$H := \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\} \subseteq G$$

If we assume that G is finite, then the subgroup H above must also be finite. In particular, this implies that there exists some integers $a < b$ such $g^a = g^b$, so $g^{b-a} = e$. This implies that the **order** of g, namely

$$\boxed{|g|} = \min\Big\{d > 0 \text{ s.t. } g^d = e\Big\} \tag{47}$$

is well-defined. If g has order d, then we have an isomorphism

$$\mathbb{Z}/d\mathbb{Z} \cong H, \qquad (k \bmod d) \mapsto g^k$$

where we recall that $\mathbb{Z}/d\mathbb{Z}$ is a group with respect to addition. In the particular case at hand, Lagrange's theorem (46) implies that the order of any element of a group divides the order of the whole group. This imposes significant restrictions on finite groups and their elements.

2.8

Now that we have studied the orbits of the left and right actions (of a subgroup on a group), let's consider the adjoint action of a group G on itself

$$G \curvearrowright G, \qquad h \cdot g = hgh^{-1}, \ \forall g, h \in G$$

Elements in the same orbit are called **conjugate**, and the orbits themselves are called **conjugacy classes** (you learned about them in Math 113). Specifically, the conjugacy class of $g \in G$ is the set

$$\Big\{hgh^{-1}\Big|h \in G\Big\} \tag{48}$$

Meanwhile, the stabilizer of g with respect to the adjoint action is called its **centralizer**

$$\boxed{C_G(g)} = \Big\{h \in G \text{ s.t. } hg = gh\Big\} \tag{49}$$

Proposition 4. *If g and g' are conjugate in a group G, then their centralizers are isomorphic.*

Proof. If $g' = hgh^{-1}$, then the assignment $x \mapsto h^{-1}xh$ gives an isomorphism $C_G(g') \to C_G(g)$. □

Thus, we will often refer to the centralizer of a conjugacy class $\widetilde{g} \subseteq G$, denoted by $C_G(\widetilde{g})$, as the isomorphism class of the centralizer of any element $g \in \widetilde{g}$.

2.9

When the group G is finite, formula (37) for the adjoint action implies the formula

$$|G| = \sum_{\text{conjugacy classes } \widetilde{g}} |\widetilde{g}| \tag{50}$$

called the **class equation** of G. However, Proposition 3 for the adjoint action implies that

$$|\widetilde{g}| = \frac{|G|}{|\mathrm{Stab}_G(\widetilde{g})|} \tag{51}$$

Keeping in mind the fact that the stabilizers are none other than the centralizers, we have

$$|\widetilde{g}| = \frac{|G|}{|C_G(\widetilde{g})|} \tag{52}$$

Note that in the formulas above, we are referring to "the stabilizer/centralizer of a conjugacy class". This is because any two elements in a conjugacy class $\widetilde{g}$ have isomorphic centralizers (according to Proposition 4), and so we may unambiguously define $\mathrm{Stab}_G(\widetilde{g}) = C_G(\widetilde{g})$ up to isomorphism. In particular, the order of this stabilizer/centralizer is well-defined, no matter what element $g \in \widetilde{g}$ we choose to define it. Putting the formulas above together, we have the following equivalent version of (50), which we will also refer to as the class equation of G

$$1 = \sum_{\text{conjugacy classes } \widetilde{g}} \frac{1}{|C_G(\widetilde{g})|} \tag{53}$$

2.10

Let us now apply all the notions above for the two main examples of groups we have studied in Subsection 1.1. Recall the dihedral group D_{2n} consisting of rotations and reflections that preserve a regular n-gon. The subset of n rotations is actually a subgroup of D_{2n} (try to argue why: you need to convince yourself that the identity is a rotation, that the inverse of a rotation is a rotation, and that the composition of rotations is a rotation), and in fact it is not hard to convince yourself that this subgroup is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Thus, we have an injective homomorphism

$$\mathbb{Z}/n\mathbb{Z} \hookrightarrow D_{2n}, \qquad (k \bmod n) \mapsto \Big(\text{rotation by } \frac{2\pi k}{n} \text{ radians}\Big)$$

Let us work out the conjugacy classes of the dihedral group in a small example, let's say

$$D_6 = \Big\{ \underbrace{e, \sigma, \sigma^2}_{\text{rotations}}, \underbrace{\tau, \tau\sigma, \tau\sigma^2}_{\text{reflections}} \Big\}$$

(recall from Math 113 that we have the formulas $\tau^2 = \sigma^3 = e$ and $\sigma\tau = \tau\sigma^{-1}$). The identity element is always alone in its conjugacy class

$$\{e\}$$

and its centralizer is always the whole group, which in this case has order 6. Meanwhile, the two non-trivial rotations

$$\{\sigma, \sigma^2\}$$

form their own conjugacy class, because $\sigma^2 = \sigma^{-1} = \tau^{-1}\sigma\tau$. The centralizer of one of these rotations is the subgroup of rotations, which has order 3 (check this using the symbols σ and τ). Finally, the reflections

$$\{\tau, \tau\sigma, \tau\sigma^2\}$$

are all conjugate to each other, because $\tau\sigma = \sigma\tau\sigma^{-1}$ and $\tau\sigma^2 = \sigma^{-1}\tau\sigma$. The centralizer of each reflection is simply the order 2 subgroup consisting of the identity and the reflection itself (check this using the symbols σ and τ). With this in mind, the class equation (53) reads

$$1 = \frac{1}{6} + \frac{1}{3} + \frac{1}{2} \tag{54}$$

which is definitely a true statement.

2.11

Let us now consider the symmetric group S_n. As you learned in Math 113, every permutation $\sigma \in S_n$ can be written as a disjoint product of cycles, for instance

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 8 & 6 & 5 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 6)(2\ 7)(3\ 8)(5)$$

Thus, to the permutation σ we may associate its **cycle type**, which is the set of lengths of its cycles in non-decreasing order. In the example above, the cycle type is $3 \geq 2 \geq 2 \geq 1$, because there is a single cycle of length 3, two cycles of length 2, and one cycle of length 1. In general, the cycle type of a permutation $\sigma \in S_n$ will be a **partition** of n, i.e. a collection of positive integers

$$\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k)$$

with total sum $|\lambda| = \lambda_1 + \lambda_2 + \cdots + \lambda_k$ equal to n.

Proposition 5. *Two elements of S_n are conjugate if and only if they have the same cycle type.*

Proof. This exercise is easier than it looks, and it is built on the fact that if we regard $\sigma, \tau \in S_n$ as bijections $\{1, \ldots, n\} \to \{1, \ldots, n\}$, then

$$\sigma = \begin{pmatrix} 1 & \ldots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix} \qquad \Longrightarrow \qquad \tau\sigma\tau^{-1} = \begin{pmatrix} \ldots & \tau(i) & \ldots \\ \ldots & \tau(\sigma(i)) & \ldots \end{pmatrix}$$

Thus, there is a one-to-one correspondence between cycles $i_1 \to i_2 \to \cdots \to i_k \to i_1$ of the permutation σ and cycles $\tau(i_1) \to \tau(i_2) \to \cdots \to \tau(i_k) \to \tau(i_1)$ of the permutation $\tau\sigma\tau^{-1}$. This immediately shows that any two conjugate permutations have the same cycle type, but it also shows the converse: any permutation σ with cycle type λ can be written as $\tau\sigma_\lambda\tau^{-1}$, where

$$\sigma_\lambda = (1\ 2\ \ldots\ \lambda_1)(\lambda_1 + 1\ \lambda_1 + 2\ \ldots\ \lambda_1 + \lambda_2)(\lambda_1 + \lambda_2 + 1\ \lambda_1 + \lambda_2 + 2\ \ldots\ \lambda_1 + \lambda_2 + \lambda_3)\ldots \tag{55}$$

and $\tau : \{1, \ldots, n\} \to \{1, \ldots, n\}$ is the function which sends the sequence $(\lambda_1 + \cdots + \lambda_{i-1} + 1, \ldots, \lambda_1 + \cdots + \lambda_i)$ to one of the cycles of σ of length λ_i, for all i.

□

Let us now work out the class equation for symmetric groups. To this end, we need to figure out the order of the centralizer of a given element in each conjugacy class. It suffices to do so for the representative (55). We have $\tau \in C_{S_n}(\sigma_\lambda)$ if and only if

$$\tau \sigma_\lambda \tau^{-1} = \sigma_\lambda$$

As we have seen in the proof of Proposition 5, this means that τ has to permute the cycles of σ_λ of length i among themselves. If we let $\#_\lambda^i$ denote the number of such cycles, this amounts to $\#_\lambda^i!$ choices. However, once we have fixed the fact that τ takes one cycle γ of length i to another cycle γ' of length i, we have the added freedom of choosing which particular entry of γ' will be the image of the first entry of the cycle γ. This amounts to i choices for every cycle of length i. Thus, we conclude that

$$|C_{S_n}(\sigma_\lambda)| = \prod_{i \geq 1} i^{\#_\lambda^i} \#_\lambda^i!$$

Do not worry about the fact that the product seems to be infinite. For i large enough, we have $\#_\lambda^i = 0$, and $i^0 0! = 1$. With this in mind, the class equation (53) reads

$$1 = \sum_{\lambda \text{ a partition of } n} \frac{1}{\prod_{i \geq 1} i^{\#_\lambda^i} \#_\lambda^i!} \tag{56}$$

For example, when $n = 4$, the formula above reads $1 = \frac{1}{24} + \frac{1}{4} + \frac{1}{8} + \frac{1}{3} + \frac{1}{4}$.

Lecture 3

3.1

Let us consider a group and a subgroup $H \leq G$. In general, the left and right cosets of G with respect to H are different. But in the event that they are equal, i.e.

$$\boxed{gH = Hg}, \qquad \forall g \in G \tag{57}$$

then you learned in Math 113 that we call H a **normal** subgroup of G, and denote this as $\boxed{H \trianglelefteq G}$.

Lemma 5. *If $f : G \to G'$ is any homomorphism, the kernel of f is a normal subgroup.*

Proof. Property (57) can be rewritten as

$$gHg^{-1} = H$$

for all $g \in G$. When $H = \text{Ker } f$, then any element $h \in H$ is characterized by the property that $f(h) = e'$. However, for any element $g \in G$, this is equivalent to

$$f(ghg^{-1}) = f(g)e'f(g^{-1}) = f(g)f(g)^{-1} = e'$$

which is equivalent to $ghg^{-1} \in \text{Ker } f = H$.

□

Important properties of normal subgroups (which you should check) are the facts that

- if H_1 and H_2 are normal in G, then $H_1 \cap H_2$ is normal in G
- if H is normal in G, then H is normal in any subgroup of G which contains H

3.2

You may recall from Math 113 that if $H \trianglelefteq G$ is a normal subgroup, then the set of (either left or right, since they are equal by virtue of normality) cosets

$$G/H$$

inherits a group structure from G. This group structure ensures that the so-called projection

$$\pi : G \to G/H, \quad g \mapsto [g]$$

is a homomorphism. The kernel of the homomorphism above is clearly H. This leads to an important result known as the **first isomorphism theorem**, which you learned in Math 113.

Theorem 2. *For any homomorphism $f : G \to G'$, we have an isomorphism*

$$G/\text{Ker } f \cong \text{Im } f \tag{58}$$

induced by $[g] \mapsto f(g)$, for all $g \in G$.

Example 1. *Take $G = \mathbb{Z}$ (made into a group with respect to addition, often called the infinite **cyclic** group) and $H = n\mathbb{Z}$ for some natural number n. The latter is a normal subgroup because $\mathbb{Z}$ is abelian (more on that later) and all subgroups of an abelian group are normal. Then we have*

$$G/H = \mathbb{Z}/n\mathbb{Z}$$

*to be the group of residues modulo n (often called the **cyclic** group of order n). More generally, you can choose two natural numbers m and n and consider the homomorphism*

$$f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \qquad f(k) = (mk \ mod \ n), \ \forall k \in \mathbb{Z}$$

In this case, Ker $f = \frac{n}{d}\mathbb{Z}$ *where $d = \gcd(m, n)$, so the first isomorphism theorem* (58) *implies that the subgroup of $\mathbb{Z}/n\mathbb{Z}$ consisting of elements which are multiples of m is isomorphic to $\mathbb{Z}/\frac{n}{d}\mathbb{Z}$. In particular, if $d = 1$, any element of $\mathbb{Z}/n\mathbb{Z}$ is a multiple of m, which implies that there exists $a \in \mathbb{Z}$ such that $am \equiv 1$ modulo n. In turn, this implies that there exists $b \in \mathbb{Z}$ such that*

$$am + bn = 1 \tag{59}$$

as integers, a well-known property of coprime numbers m and n.

3.3

Quotients have an important property with respect to group actions. Assume we have an action

$$G \curvearrowright X \tag{60}$$

and that a certain normal subgroup $H \trianglelefteq G$ acts on X trivially, i.e.

$$h \cdot x = x, \qquad \forall h \in H, x \in X \tag{61}$$

(in other words, h is contained in the kernel of the action). Then the action (60) induces an action

$$\boxed{G/H \curvearrowright X} \tag{62}$$

given by the formula

$$[g] \cdot x = g \cdot x, \qquad \forall g \in G, x \in X \tag{63}$$

Indeed, to ensure that this action is well-defined, all that one needs to show is that formula (63) is unchanged if we replace g by gh for arbitrary $h \in H$. However, this is an immediate consequence of the fact that $(gh) \cdot x = g \cdot (h \cdot x)$ and the assumption (61).

Remark. *If we let H be the kernel of the action* (60) *(which is normal, because it can be construed as the kernel of the homomorphism* (31)*), then the induced action* (62) *is faithful. Prove this.*

3.4

With the definitions above in mind, we now generalize the notion of centralizer from the previous lecture. The following notions have already been encountered in Math 113.

Definition 10. *For any subset X of a group G, define its **centralizer** as*

$$\boxed{C_G(X)} = \Big\{ g \in G \Big| gx = xg, \ \forall x \in X \Big\} \tag{64}$$

The centralizer of $X = G$ is called the **center** of the group G, and is denoted by

$$Z(G) = \Big\{ g \in G \Big| gh = hg, \forall h \in G \Big\} \tag{65}$$

Definition 11. *For any subset X of a group G, define its **normalizer** as*

$$\boxed{N_G(X)} = \Big\{ g \in G \Big| gX = Xg \Big\} \tag{66}$$

It is obvious that $C_G(X) \leq N_G(X)$ for any set $X \subseteq G$, because the property $gx = xg, \forall x \in X$ is stronger than $gX = Xg$. Moreover, the following stronger result is true.

Proposition 6. *For any subset $X \subset G$, its centralizer is a normal subgroup of its normalizer*

$$C_G(X) \trianglelefteq N_G(X) \tag{67}$$

Instead of proving Proposition 6 directly, we will argue for it using the language of group actions. For any subset X of a group G, we have an action

$$N_G(X) \curvearrowright X, \qquad g \cdot x = gxg^{-1}$$

The kernel of this action is, by definition, the centralizer subgroup $C_G(X)$. Since the kernel of any group action is normal, this implies Proposition 6. Moreover, according to the general principle in Subsection 3.3, we obtain a faithful action

$$N_G(X)/C_G(X) \curvearrowright X \tag{68}$$

3.5

We henceforth specialize to the case when X is a subgroup of G.

Definition 12. *An **automorphism** of a group K is an isomorphism $K \to K$, and we write*

$$\boxed{\mathrm{Aut}(K)} \tag{69}$$

for the group of automorphisms of K, with respect to composition.

Definition 13. *We say that a group L acts on a group K by automorphisms, still denoted by*

$$L \curvearrowright K$$

if the bijections $\Phi_\ell(k) = \ell \cdot k$ are homomorphisms for all $\ell \in L$.

Lemma 6. *If H is a subgroup of G, then the action*

$$N_G(H)/C_G(H) \curvearrowright H \tag{70}$$

of (68) is by automorphisms.

Proof. This is an immediate consequence of the formula

$$ghh'g^{-1} = (ghg^{-1})(gh'g^{-1})$$

for all $h, h' \in H$, $g \in G$.

□

With this in mind, formula (70) gives us an inclusion

$$\boxed{N_G(H)/C_G(H) \hookrightarrow \mathrm{Aut}(H)} \tag{71}$$

for any subgroup $H \leq G$. The fact (71) is often called the **normalizer/centralizer theorem**.

3.6

Let us now consider two subgroups H and K of a group G. We may form the subsets

$$HK = \left\{ hk \middle| h \in H, k \in K \right\}$$

and

$$KH = \left\{ kh \middle| h \in H, k \in K \right\}$$

of G, which in general will be different. The following is a rather easy result, which we leave as an exercise to you. You may also remember it from Math 113.

Proposition 7. *Let H and K be subgroups of a group G.*

- *We have $HK = KH$ if and only if HK is a subgroup of G.*
- *If H and K are normal subgroups of G, then HK is a normal subgroup of G.*

For instance, the condition $HK = KH$ in Proposition 7 holds if

$$K \leq N_G(H) \tag{72}$$

because then we have $Hk = kH$ for all $k \in K$. In turn, a significant source of examples for (72) is when $H \trianglelefteq G$, because in the latter case $N_G(H) = G$. Formula (72) is also the setting of the so-called **second isomorphism theorem**, which you also learned in Math 113.

Theorem 3. *If K and H are subgroups of G such that $K \leq N_G(H)$, then*

$$K/K \cap H \cong HK/H \tag{73}$$

(the facts that $K \cap H$ is normal in K and H is normal in HK is part of the Theorem).

3.7

The following result is often called the **correspondence theorem**. Some people call it the **lattice theorem**, while for others it's an amalgamation of the **third** and **fourth isomorphism theorems**.

Theorem 4. *For any group and normal subgroup $H \trianglelefteq G$, there is a one-to-one correspondence*

$$\Big\{\text{subgroups } H \leq K \leq G\Big\} \leftrightarrow \Big\{\text{subgroups } \bar{K} \leq \bar{G}\Big\} \tag{74}$$

where $\bar{G} = G/H$ with standard projection $\pi : G \to \bar{G}$. The correspondence (74) is given by

$$\bar{K} = \pi(K) \quad \text{and} \quad K = \pi^{-1}(\bar{K}) \tag{75}$$

and it enjoys the following properties:

1. *we have $K \leq K'$ if and only if $\bar{K} \leq \bar{K}'$, and in this case we have a bijection*

$$K'/K \leftrightarrow \bar{K}'/\bar{K}$$

2. *we have $K \trianglelefteq K'$ if and only if $\bar{K} \trianglelefteq \bar{K}'$, and in this case we have an isomorphism*

$$\boxed{K'/K \cong \bar{K}'/\bar{K}} \tag{76}$$

   In particular, K is normal if and only if $\bar{K}$ is normal.

Proof. We leave it to you to show that the assignments (75) are mutually inverse. The fact that K being a subgroup is equivalent to $\bar{K}$ being a subgroup is a consequence of the following.

Claim 1. *If $f : G \to G'$ is a homomorphism, then for any subgroups $H \leq G$ and $H' \leq G'$, we have*

$$f(H) \leq G' \qquad \text{and} \qquad f^{-1}(H') \leq G$$

We leave Claim 1 as an exercise. Property 1 is a trivial statement, with the bijection given by

$$[g \bmod K] \mapsto \Big[[g \bmod H] \bmod K/H\Big], \quad \forall g \in K' \tag{77}$$

Property 2 follows from

$$K \trianglelefteq K' \quad \Leftrightarrow \quad Kg = gK,\ \forall g \in K' \quad \Leftrightarrow \quad \bar{K}\bar{g} = \bar{g}\bar{K},\ \forall \bar{g} \in \bar{K}' \quad \Leftrightarrow \quad \bar{K} \trianglelefteq \bar{K}'$$

where the middle equivalence is none other than the correspondence (74). If K is normal in K', then the bijection (77) is easily seen to be a homomorphism, thus yielding the isomorphism (76). □

Lecture 4

4.1

We will now take the notion of subgroups and quotient groups one step further.

Definition 14. *A **short exact sequence** (of groups)*

$$1 \to K \xrightarrow{f} G \xrightarrow{g} L \to 1 \tag{78}$$

is the datum of two homomorphisms f and g as above, where f is injective, g is surjective, and

$$\text{Im } f = \text{Ker } g \tag{79}$$

The "1" on the left and on the right of the sequence (78) represent the trivial group.

An immediate consequence of the definition is that f induces an isomorphism between K and a normal subgroup $H \trianglelefteq G$, while the first isomorphism theorem implies that g induces an isomorphism between L and the quotient group G/H. Because of this, if there exists a short exact sequence (78), we will call G an **extension** of L by K.

Example 2. *The quintessential short exact sequence is*

$$1 \to \mathbb{Z}/m\mathbb{Z} \xrightarrow{f} \mathbb{Z}/mn\mathbb{Z} \xrightarrow{g} \mathbb{Z}/n\mathbb{Z} \to 1 \tag{80}$$

for any $m, n \in \mathbb{N}$, where f is multiplication by n and g is reduction mod n.

4.2

For any groups K and L, recall from Math 113 their **direct product**

$$K \times L$$

which is made into a group via the operation $(k, \ell)(k', \ell') = (kk', \ell\ell')$ (try for yourself to guess the identity and inverse, and to check all the group axioms). Then we have a short exact sequence

$$1 \to K \xrightarrow{f} K \times L \xrightarrow{g} L \to 1 \tag{81}$$

where $f(k) = (k, e)$ and $g(k, \ell) = \ell$, for all $k \in K$ and $\ell \in L$. You can check that the maps f and g are homomorphisms, and that (79) is satisfied. However, short exact sequences also account for the semidirect products of groups that you learned about in Math 113.

Definition 15. *If a group L acts on a group K by automorphisms (with notation as in Definition 13), then the corresponding **semidirect product***

$$K \rtimes L = \left\{ (k, \ell) \middle| k \in K, \ell \in L \right\} \tag{82}$$

is made into a group with identity element (e, e) via

$$(k, \ell)(k', \ell') = (k\Phi_\ell(k'), \ell\ell')$$

Direct products are the particular case of semidirect products for $\Phi_\ell = \text{Id}_K$, for all $\ell \in L$.

Proposition 8. *Given a semidirect product* (82)*, we have a short exact sequence*

$$1 \to K \xrightarrow{f} K \rtimes L \xrightarrow{g} L \to 1 \tag{83}$$

where $f(k) = (k, e)$ *and* $g(k, \ell) = \ell$*, for all* $k \in K$ *and* $\ell \in L$*.*

Proof. It is immediate to see that f is injective, g is surjective, and that Im f = Ker g (in fact, the proof of these statements is equivalent to the case of the direct product, which we have already treated). The only thing one needs to show is that f and g are homomorphisms. Let us show that they respect the product. For f, this is a consequence of the fact that

$$(k, e)(k', e) = (k\Phi_e(k'), ee) = (kk', e), \qquad \forall k, k' \in K$$

while for g, this is a consequence of the fact that

$$(k, \ell)(k', \ell') = (\text{some element of } K, \ell\ell'), \quad \forall k, k' \in K, \ell, \ell' \in L$$

□

4.3

We will now show that quite a lot of short exact sequences are of the form (82), although to do so, we must first formulate what it means for two short exact sequences to be "the same".

Definition 16. *Two short exact sequences*

$$1 \to K \xrightarrow{f} G \xrightarrow{g} L \to 1$$

and

$$1 \to K \xrightarrow{f'} G' \xrightarrow{g'} L \to 1$$

are called ***equivalent*** *if there exists a homomorphism* $s : G \to G'$ *which makes the squares in the following diagram commute*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{f} & G & \xrightarrow{g} & L & \longrightarrow & 1 \\ & & \mathrm{Id}_K \downarrow & & s \downarrow & & \mathrm{Id}_L \downarrow & & \\ 1 & \longrightarrow & K & \xrightarrow{f'} & G' & \xrightarrow{g'} & L & \longrightarrow & 1 \end{array} \tag{84}$$

Note that equivalence of short exact sequences is an equivalence relation, i.e. it is reflexive, symmetric and transitive (check these facts, please).

Lemma 7. *If two short exact sequences are equivalent, then the homomorphism* s *in Definition 16 must be an isomorphism.*

Proof. We will use the notation in Definition 16 and the commutativity of diagram (84). Assume that $s(x) = e$ for some $x \in G$. Then $g'(s(x)) = e$, so by the commutativity of the right-most square we must have $g(x) = e$. However, this implies that there exists $y \in K$ such that $x = f(y)$. Then we have $e = s(x) = s(f(y))$, which by commutativity of the left-most square implies that $f'(y) = e$. Since f' is injective, this implies $y = e$, therefore $x = e$. This establishes the injectivity of s.

Consider any $x' \in G'$. Because g is surjective, we can choose $x \in G$ such that $g(x) = g'(x')$. However, by the commutativity of the right-most square in (84), we have $g = g' \circ s$. Thus, we have

$$g'(s(x)) = g'(x') \quad \Rightarrow \quad g'(s(x)^{-1}x') = e$$

so there exists $y' \in K$ such that $f'(y') = s(x)^{-1}x'$. However, the commutativity of the left-most square in (84) reads $f' = s \circ f$, and so we have

$$x' = s(x)f'(y') = s(x)s(f(y')) = s(xf(y'))$$

This establishes the surjectivity of s.

□

4.4

We will now give criteria for when a short exact sequence is equivalent to either (81) or (83).

Proposition 9. *A short exact sequence* $1 \to K \xrightarrow{f} G \xrightarrow{g} L \to 1$ *is equivalent to* (81) *if and only if there exists a homomorphism*

$$\phi : G \to K \tag{85}$$

such that $\phi \circ f = \mathrm{Id}_K$.

Proof. We leave it to you to deduce the "only if" statement from the fact that the sequence (81) does indeed possess a homomorphism (85) (if $G = K \times L$, then you simply define ϕ to be the projection onto the first factor). As for the "if" statement, assume that we have a homomorphism (85). Then the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{f} & G & \xrightarrow{g} & L & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{Id}_K} & & \downarrow{\scriptstyle \phi \times g} & & \downarrow{\scriptstyle \mathrm{Id}_L} & & \\ 1 & \longrightarrow & K & \longrightarrow & K \times L & \longrightarrow & L & \longrightarrow & 1 \end{array}$$

(with the morphisms on the bottom row being $k \mapsto (k, e)$ and $(k, \ell) \mapsto \ell$) gives the required equivalence of short exact sequences.

□

Proposition 10. *An extension* $1 \to K \xrightarrow{f} G \xrightarrow{g} L \to 1$ *is equivalent to* (83) *if and only if there exists a homomorphism*

$$\psi : L \to G \tag{86}$$

such that $g \circ \psi = \mathrm{Id}_L$.

Proof. We leave it to you to deduce the "only if" statement from the fact that the sequence (83) does indeed possess a homomorphism (86) (if $G = K \rtimes L$, then you define $\psi(\ell) = (e, \ell), \forall \ell \in L$). As for the "if" statement, assume that we have a homomorphism (86). It allows us to define an action

$$L \curvearrowright K$$

as follows: for every $k \in K$ and $\ell \in L$, the fact that Im $f =$ Ker g and $g \circ \psi = \mathrm{Id}_L$ implies that

$$\psi(\ell) f(k) \psi(\ell)^{-1} \in G$$

lies in Ker $g =$ Im f, and thus may be written uniquely as $f(x)$ for some $x \in K$. Define the function

$$\Phi_\ell : K \to K, \qquad k \mapsto \text{the aforementioned } x$$

There are several things to check, all of which are easy, but we recommend you go through the steps yourselves:

- $\Phi_e = \mathrm{Id}_K$,
- Φ_ℓ is a bijection for all $\ell \in L$,
- Φ_ℓ is a homomorphism for all $\ell \in L$,
- $\Phi_\ell \circ \Phi_{\ell'} = \Phi_{\ell\ell'}$ for all $\ell, \ell' \in L$.

Thus, the Φ_ℓ defined above give rise to a semidirect product $K \rtimes L$. We claim that the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{f} & G & \xrightarrow{g} & L & \longrightarrow & 1 \\ & & {\scriptstyle \mathrm{Id}_K}\uparrow & & {\scriptstyle f\times\psi}\uparrow & & {\scriptstyle \mathrm{Id}_L}\uparrow & & \\ 1 & \longrightarrow & K & \longrightarrow & K \rtimes L & \longrightarrow & L & \longrightarrow & 1 \end{array}$$

(with the morphisms on the bottom row being $k \mapsto (k, e)$ and $(k, \ell) \mapsto \ell$, and the middle vertical map being $(k, \ell) \mapsto f(k)\psi(\ell)$) gives the required equivalence. Indeed, to show this we need to check two facts: the first is that the diagram commutes, which is obvious. The second fact is that the middle vertical map is a homomorphism, which follows from the equality

$$\begin{aligned} (f \times \psi)((k, \ell)(k', \ell')) = (f \times \psi)(k\Phi_\ell(k'), \ell\ell') = f(k\Phi_\ell(k'))\psi(\ell\ell') = \\ = f(k)f(\Phi_\ell(k'))\psi(\ell)\psi(\ell') = f(k)\psi(\ell)f(k')\psi(\ell') = (f \times \psi)(k, \ell)(f \times \psi)(k', \ell') \end{aligned}$$

□

4.5

Recall the following important definition from Math 113.

Definition 17. *A group is called* ***abelian*** *if all of its elements pairwise commute, i.e.*

$$gh = hg, \quad \forall g, h \in G \tag{87}$$

For an abelian group, it is customary to denote the product in "additive" notation, i.e.

$$g + h \quad \textit{instead of} \quad gh \tag{88}$$

and the identity by 0 *instead of* e*.*

The center $Z(G)$ of any group G is abelian. Other examples of abelian groups are the cyclic groups $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$. Let us now consider short exact sequences (78) with K, G, L abelian.

Lemma 8. *Let* K, L *be abelian groups, and consider an action* $L \curvearrowright K$ *by homomorphisms. Then*

$$K \rtimes L$$

is abelian if and only if the action is trivial, i.e. $\Phi_\ell(k) = k$ *for all* $k \in K$*,* $\ell \in L$*.*

Proof. The "if" statement is obvious. For the "only if" statement, note that $K \rtimes L$ being abelian implies that

$$k + \Phi_\ell(k') = k' + \Phi_{\ell'}(k)$$

for all $k, k' \in K$ and $\ell, \ell' \in L$. Letting k and ℓ' be the identity elements in the formula above implies that $\Phi_\ell(k') = k'$ for all $k' \in K$ and $\ell \in L$.

□

Lemma 8 implies that for short exact sequences of abelian groups (note that when working with abelian groups, it is customary to denote the trivial group as 0 instead of 1; this should make it clear whenever one of our short exact sequences is one of abelian vs general groups)

$$0 \to K \xrightarrow{f} G \xrightarrow{g} L \to 0 \tag{89}$$

the settings of Propositions 9 and 10 are actually one and the same. Thus, when all the groups involved are abelian, we conclude that the existence of a homomorphism

$$\phi : G \to K \qquad \text{s.t.} \qquad \phi \circ f = \mathrm{Id}_K$$

is equivalent to the existence of a homomorphism

$$\psi : L \to G \qquad \text{s.t.} \qquad g \circ \psi = \mathrm{Id}_L$$

In these two equivalent cases, we call the short exact sequence (89) **split**, and either of the maps ϕ or ψ will be called a splitting.

Example 3. *When* $\gcd(m, n) = 1$*, we claim that the short exact sequence* (80) *is split. Indeed, explicit splittings are given by* $\phi =$ *"multiplication by* b *and reduction modulo* m*" and* $\psi =$ *"multiplication by* am*", where the integers* a *and* b *are chosen as in* (59)*. In particular, we have*

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \tag{90}$$

whenever $\gcd(m, n) = 1$*.*

Lecture 5

5.1

We would like to classify abelian groups. However, we cannot hope to do so for all abelian groups, there are just too many of them. Instead, we will classify the finitely generated ones, as per the following definition.

Definition 18. *We say that elements $g_1, \dots, g_k$ **generate** an abelian group G if any element of G can be written (not necessarily uniquely) as a linear combination*

$$a_1 g_1 + \cdots + a_k g_k$$

for various $a_1, \dots, a_k \in \mathbb{Z}$. Here, we recall that we use additive notation, so ag means the same thing as g^a previously meant (i.e. the a-fold group operation of g with itself).

If an abelian group admits a finite set of generators, then we will call it **finitely generated**. Our main result in Lectures 5 and 6 will be the classification of such groups, namely the proof of the following result. We write $\mathbb{Z}^r = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ times}}$ for any number $r \geq 0$, and set $\mathbb{Z}^0 = 0$ the trivial group.

Theorem 5. *Any finitely generated abelian group G is isomorphic to a direct product*

$$\boxed{\mathbb{Z}^r \times \mathbb{Z}/p_1^{d_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{d_k}\mathbb{Z}} \tag{91}$$

*for some $r \geq 0$ (called the **rank** of G) and various prime powers $p_1^{d_1}, \dots, p_k^{d_k}$ (called the **elementary divisors** of G). The decomposition (91) is unique up to permuting the factors.*

Not all (and in fact, rather few) abelian groups are finitely generated, as the following result shows.

Proposition 11. *The group of rational numbers $\mathbb{Q}$ with respect to addition is not finitely generated.*

Proof. Assume for the purpose of contradiction that $\mathbb{Q}$ were finitely generated. Then there exist rational numbers

$$\frac{b_1}{c_1}, \dots, \frac{b_k}{c_k}$$

(for various $b_1, \dots, b_k \in \mathbb{Z}$ and $c_1, \dots, c_k \in \mathbb{N}$) such that any element of $\mathbb{Q}$ can be written as

$$a_1 \frac{b_1}{c_1} + \cdots + a_k \frac{b_k}{c_k} \tag{92}$$

for various $a_1, \dots, a_k \in \mathbb{Z}$. But the denominator of (92) must divide the fixed natural number $c_1 \dots c_k$, so it is impossible for all rational numbers to be of the form (92).

□

5.2

For any abelian group G and any $n \in \mathbb{Z}$, the function

$$G \to G, \qquad g \mapsto ng, \ \forall g \in G \tag{93}$$

is a homomorphism (I recommend you check this). The kernel of this homomorphism, namely

$$\boxed{\mathrm{Tors}_n(G)} = \Big\{ g \in G \Big| ng = 0 \Big\} \tag{94}$$

is called the n-**th torsion subgroup** of G. It is easy to see that the n-th torsion subgroup is the same as the $(-n)$-th torsion subgroup. Meanwhile, the 0-th torsion subgroup of G is the entire G, so it is not an interesting concept. Thus, we will only work with the n-th torsion for natural numbers n.

Lemma 9. *For any abelian group G, the set*

$$\boxed{\mathrm{Tors}(G)} = \bigcup_{n=1}^{\infty} \mathrm{Tors}_n(G) \tag{95}$$

is a subgroup. It will be called the ***torsion subgroup*** *of G.*

Proof. Since each $\mathrm{Tors}_n(G)$ is a subgroup of G, this implies that $\mathrm{Tors}(G)$ contains the identity element and that it is closed under taking inverses. It remains to show that the product of any two elements in $\mathrm{Tors}(G)$ lies in $\mathrm{Tors}(G)$. To this end, note the obvious fact that

$$\mathrm{Tors}_n(G) \subseteq \mathrm{Tors}_{mn}(G)$$

for all $m, n \in \mathbb{N}$. Thus, if we take an element $g \in \mathrm{Tors}_m(G) \subset \mathrm{Tors}(G)$ and an element $h \in \mathrm{Tors}_n(G) \subset \mathrm{Tors}(G)$, then both g and h lie in $\mathrm{Tors}_{mn}(G)$. Since the latter is a subgroup of G, this implies that $g + h \in \mathrm{Tors}_{mn}(G) \subset \mathrm{Tors}(G)$, as we were required to show.

□

An important aspect of torsion is that no element (except the identity element) can be simultaneously in the m-th torsion and the n-th torsion if $\gcd(m, n) = 1$. In other words

$$\{0\} = \mathrm{Tors}_m(G) \cap \mathrm{Tors}_n(G) \tag{96}$$

for any abelian group G, whenever $\gcd(m, n) = 1$. To see this, we invoke the existence of the integers a, b from (59). If an element $g \in G$ lied in both the m-th and n-th torsion subgroups, then

$$mg = ng = 0 \quad \Rightarrow \quad (am + bn)g = 0 \quad \Rightarrow \quad g = 0$$

5.3

An abelian group where the only torsion element is 0 (i.e. such that $ng = 0$ for some $n \in \mathbb{N}$ implies $g = 0$) is called **torsion-free**. It is clear that $\mathbb{Z}^r$ is torsion-free, as are all its subgroups. Meanwhile, no finite group (other than the trivial group) can be torsion-free, since all its elements have finite order.

Lemma 10. *For any abelian group G, the quotient group*

$$G/\mathrm{Tors}(G)$$

is torsion-free.

Proof. Suppose $g \in G$ has the property that $n[g] = 0$ in $G/\mathrm{Tors}(G)$ for some $n \in \mathbb{N}$. Then

$$ng \in \mathrm{Tors}(G)$$

which implies that there exists some $m \in \mathbb{N}$ such that $mng = 0$. This implies that $g \in \mathrm{Tors}(G)$, so $[g] = 0$ in $G/\mathrm{Tors}(G)$.

□

If G is a group of the form in (91), then please show by yourself that

$$\mathrm{Tors}(G) \cong \mathbb{Z}/p_1^{d_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{d_k}\mathbb{Z}$$

and $G/\mathrm{Tors}(G) \cong \mathbb{Z}^r$. Thus, as a stepping stone to proving Theorem 5, we will prove the following.

Proposition 12. *Any torsion-free finitely generated abelian group G is **free abelian**, i.e.*

$$\boxed{G \cong \mathbb{Z}^r}$$

for some $r \geq 0$.

5.4

Proposition 12 is an immediate consequence of Propositions 13 and 14.

Proposition 13. *Any torsion-free finitely generated abelian group G is isomorphic to a subgroup of $\mathbb{Z}^k$, for some $k \geq 0$.*

Proof. Let us adapt the notion of linear independence from linear algebra to the setting of abelian groups. We say that $g_1, \ldots, g_k \in G$ are **linearly independent** if for all $a_1, \ldots, a_k \in \mathbb{Z}$,

$$a_1 g_1 + \cdots + a_k g_k = 0 \quad \Rightarrow \quad a_1 = \cdots = a_k = 0$$

Let us now assume that G is a torsion-free finitely generated abelian group. Consider a set of generators $g_1, \ldots, g_{k+\ell}$ of G, and assume that $g_1, \ldots, g_k$ are a maximal subset of linearly independent

elements among the aforementioned generators (this is always possible up to relabeling the g's). Therefore, the following homomorphism is injective

$$\mathbb{Z}^k \xrightarrow{\gamma} G, \qquad (a_1, \ldots, a_k) \mapsto a_1 g_1 + \cdots + a_k g_k$$

However, the fact that the set $g_1, \ldots, g_k$ is maximal with respect to linear independence means that the elements $g_1, \ldots, g_k, g_i$ are linearly dependent, for all $i \in \{k+1, \ldots, \ell\}$. Therefore, there exist integers $a_i^1, \ldots, a_i^k, b_i$ (with $b_i \neq 0$ due to the linear independence of $g_1, \ldots, g_k$) such that

$$b_i g_i = a_i^1 g_1 + \cdots + a_i^k g_k$$

for all $i \in \{k+1, \ldots, \ell\}$. Let m be the least common multiple of $b_{k+1}, \ldots, b_\ell$. Thus, $mg_{k+1}, \ldots, mg_{k+\ell}$ can be written as linear combinations of $g_1, \ldots, g_k$; since $g_1, \ldots, g_{k+l}$ generate G, we therefore conclude that mg can be written as a linear combination of $g_1, \ldots, g_k$, for any $g \in G$. Therefore, the image of the homomorphism

$$G \xrightarrow{\delta} G, \qquad g \mapsto mg$$

is contained in the image of the injective homomorphism γ. This implies that δ factors as

$$\delta : G \to \mathbb{Z}^k \xrightarrow{\gamma} G$$

However, δ is injective because G is torsion-free, which implies that the homomorphism $G \to \mathbb{Z}^k$ we just constructed is also injective. Thus, G is isomorphic to the image of this homomorphism.

□

Proposition 14. *Any subgroup of $\mathbb{Z}^k$ is isomorphic to $\mathbb{Z}^r$ for some $r \geq 0$.*

Proof. We will prove the required statement by induction on k. When $k = 1$, consider any subgroup $G \subseteq \mathbb{Z}$. Either $G = 0$ or G contains some non-zero element n. Choose the smallest positive integer $n \in G$. Then $n\mathbb{Z} \subseteq G$. If this inclusion were not an equality of sets, then there would exist $m \in \mathbb{Z}$ with $n \nmid m$. But then the remainder of m mod n would also be in G, this contradicting the minimality of n. We conclude that $G = n\mathbb{Z} \cong \mathbb{Z}$.

Now we prove the induction step: suppose that any subgroup of $\mathbb{Z}^{k-1}$ is free, and let us show that the same is true of any given subgroup $G \subseteq \mathbb{Z}^k$. Consider the short exact sequence

$$0 \to \mathbb{Z}^{k-1} \xrightarrow{\iota} \mathbb{Z}^k \xrightarrow{\pi} \mathbb{Z} \to 0 \tag{97}$$

where the homomorphism π is projection onto the last coordinate. Then we define $K = G \cap \mathbb{Z}^{k-1}$ and $L = \pi(G)$, and leave it to you to check that (97) induces a short exact sequence

$$0 \to K \xrightarrow{\iota'} G \xrightarrow{\pi'} L \to 0 \tag{98}$$

However, we already classified the subgroups of $\mathbb{Z}$: if $L = 0$, then $G \cong K$ is a subgroup of $\mathbb{Z}^{k-1}$, which the induction hypothesis shows is free. Otherwise, $L \cong \mathbb{Z}$ and we may choose a splitting of the map π': simply send $1 \in L$ to an arbitrary element in $\pi'^{-1}(1)$. As we have seen at the end of Lecture 4, a split short exact sequence of abelian groups has the property $G \cong K \times L$. Since K is free by the induction hypothesis and $L \cong \mathbb{Z}$, we are done.

□

5.5

In the course of the proof of Proposition 14, we (essentially) proved the following interesting property of the abelian group $\mathbb{Z}^\ell$, for any $\ell \in \mathbb{N}$.

Lemma 11. *Any short exact sequence of abelian groups*

$$0 \to K \to G \xrightarrow{\pi} \mathbb{Z}^\ell \to 0 \tag{99}$$

is split, and in particular, $G \cong K \times \mathbb{Z}^\ell$.

Proof. For every $i \in \{1, \dots, \ell\}$, let e_i be the standard generator of $\mathbb{Z}^\ell$, namely the vector $(0, \dots, 1, \dots, 0)$ with a single 1 on the i-th position and 0 everywhere else. Since the homomorphism $\pi : G \to \mathbb{Z}^\ell$ in the given short exact sequence is surjective, we may choose $g_i \in \pi^{-1}(e_i)$ for all i. Then the function

$$\psi : \mathbb{Z}^\ell \to G, \qquad (n_1, \dots, n_\ell) \mapsto n_1 g_1 + \cdots + n_\ell g_\ell$$

is easily seen to be a homomorphism (please check this). Moreover, by construction, it is a splitting in the sense that $\pi \circ \psi = \mathrm{Id}_{\mathbb{Z}^\ell}$. Therefore, the short exact sequence (99) is split.

□

As a corollary of Lemma 10, Lemma 11 and Proposition 12, we have

$$G \cong \mathbb{Z}^r \times \mathrm{Tors}(G) \tag{100}$$

for any finitely generated abelian group G, for some $r \geq 0$. To see this, recall that Lemma 10 yields a short exact sequence

$$0 \to \mathrm{Tors}(G) \to G \xrightarrow{\pi} L \to 0$$

where L is a torsion-free abelian group. However, the fact that G is finitely generated means that the same is true for L (specifically, a finite set of generators for L is given by the images under π of some finite set of generators of G). Proposition 12 then implies that L is isomorphic to $\mathbb{Z}^r$ for some $r \geq 0$, and then Lemma 11 implies (100).

Lecture 6

6.1

Formula (100) reduces the classification problem of finitely generated abelian groups G (our sought-for Theorem 5) to understanding $\mathrm{Tors}(G)$. The first step is the following.

Proposition 15. *If G is a finitely generated abelian group, then any subgroup $H \leq G$ is also finitely generated.*

Note that Proposition 15 does not hold for non-abelian groups (for which there exists an analogous notion of finite generation).

Proof. The proof has much in common with that of Proposition 14. We will prove Proposition 15 by induction on the number of generators of G. When G has a single generator (i.e. is cyclic), then $G \cong \mathbb{Z}$ or $G \cong \mathbb{Z}/n\mathbb{Z}$. We have already showed that all subgroups of $\mathbb{Z}$ are either 0 or $m\mathbb{Z}$, and we leave it as an exercise to you to show that all subgroups of $\mathbb{Z}/n\mathbb{Z}$ are of the form $m\mathbb{Z}/n\mathbb{Z}$ for some divisor $m|n$.

Let us now assume that Proposition 15 holds for all abelian groups with fewer than n generators, and let us prove it for a group G with generators $g_1, \ldots, g_n$. Pick an arbitrary subgroup H, which we will prove to be finitely generated. Let $G' \subset G$ be the subgroup generated by $g_1, \ldots, g_{n-1}$, and consider the short exact sequence

$$0 \to G' \xrightarrow{\iota} G \xrightarrow{\pi} G/G' \to 0$$

If we let $K = H \cap G'$ and $L = \pi(H)$, then we have a short exact sequence

$$0 \to K \xrightarrow{\iota} H \xrightarrow{\pi} L \to 0$$

Since K and L are subgroups of G' and G/G' (which have $n-1$ and 1 generators, respectively), the induction hypothesis implies that K and L are both finitely generated. Let $x_1, \ldots, x_k$ be generators of K and $y_1, \ldots, y_\ell$ be generators of ℓ. Then we claim that

$$\iota(x_1), \ldots, \iota(x_k), g_1, \ldots, g_\ell \tag{101}$$

are generators of H, for any choice of $\{g_i \in \pi^{-1}(y_i)\}_{i \in \{1,\ldots,\ell\}}$. Indeed, for any $h \in H$, we may write

$$\pi(h) = b_1 y_1 + \cdots + b_\ell y_\ell$$

for various $b_1, \ldots, b_\ell \in \mathbb{Z}$. This implies that

$$h - b_1 g_1 - \cdots - b_\ell g_\ell \in \mathrm{Ker}\ \pi = \mathrm{Im}\ \iota$$

Because ι is injective, its image is isomorphic to K, so there must exist $a_1, \ldots, a_k \in \mathbb{Z}$ such that

$$h - b_1 g_1 - \cdots - b_\ell g_\ell = a_1 \iota(x_1) + \cdots + a_k \iota(x_k)$$

This establishes the claim that H is generated by the elements (101).

□

6.2

As a consequence of Proposition 15, the torsion subgroup of a finitely generated abelian group G is finitely generated. If we let $g_1, \ldots, g_k$ to be a collection of such generators of $\mathrm{Tors}(G)$ (which must have finite orders $a_1, \ldots, a_k \in \mathbb{N}$, respectively), then any element of $\mathrm{Tors}(G)$ is of the form

$$b_1 g_1 + \cdots + b_k g_k$$

where $b_i \in \{0, \ldots, a_i - 1\}$ for all $i \in \{1, \ldots, k\}$. Thus, we conclude that

any finitely-generated torsion abelian group is finite (102)

(when we say "torsion abelian group", we mean an abelian group in which every element has finite order). Therefore, it remains to classify finite abelian groups. To this end, we will need to study the structure of torsion subgroups in finer detail. A natural generalization of the direct product of two groups is the direct product of countably many abelian groups $G_1, G_2, \ldots$

$$\prod_{i=1}^{\infty} G_i = \Big\{ (g_1, g_2, \ldots) \Big| g_i \in G_i, \ \forall i \in \mathbb{N} \Big\}$$

(with all operations defined component-wise) which is also an abelian group. Moreover, the **direct sum** of countably many abelian groups $G_1, G_2, \ldots$

$$\bigoplus_{i=1}^{\infty} G_i = \Big\{ (g_1, g_2, \ldots) \Big| g_i \in G_i, \ \forall i \in \mathbb{N}, \text{ all but finitely many of the } g_i\text{'s are } 0 \Big\} \tag{103}$$

(with all operations still defined component-wise) is also an abelian group. If only finitely many of the groups $G_1, G_2, \ldots$ are non-trivial, then the direct product and direct sum are the same, but in general the former is bigger than the latter.

6.3

Let us now consider any abelian group G and any prime number p. The p-torsion subgroup (note the terminological distinction between this and the "p-th torsion subgroup" defined in Subsection 5.2) is

$$\boxed{A_p(G))} = \bigcup_{n=0}^{\infty} \mathrm{Tors}_{p^n}(G) \tag{104}$$

Just as in the proof of Lemma 9, one shows (and I advise you to redo the proof) that

$$\mathrm{Tors}_{p^0}(G) \subseteq \mathrm{Tors}_{p^1}(G) \subseteq \mathrm{Tors}_{p^2}(G) \subseteq \ldots$$

and that (104) is indeed a subgroup. Moreover, these torsion subgroups provide a direct sum decomposition of the entire torsion subgroup (95), as per the following result.

Lemma 12. *For any abelian group G, we have*

$$\mathrm{Tors}(G) \cong \bigoplus_{\text{prime } p} A_p(G) \tag{105}$$

with the direct sum of abelian groups defined as in (103).

Proof. There is a natural homomorphism from the right-hand side to the left-hand side of (105)

$$\sum_{\text{prime } p} g_p \leftarrow \Big(g_p \in A_p(G)\Big)_{\text{prime } p} \tag{106}$$

The fact that all but finitely many of the g_p's are equal to 0 (the defining feature of the direct sum) means that their sum is well-defined. It remains to show that (106) is

- *injective*: suppose we have a collection of elements $g_1, \dots, g_k \in G$ such that $p_1^{d_1} g_1 = \dots = p_k^{d_k} g_k = 0$, where $p_1, \dots, p_k$ are distinct primes and $d_1, \dots, d_k$ are natural numbers. If the collection of these g_i's lies in the kernel of (106), i.e. if

  $$g_1 + g_2 + \dots + g_k = 0$$

  then we may multiply the formula above by $p_2^{d_2} \dots p_k^{d_k}$. If we do so, we have

  $$p_2^{d_2} \dots p_k^{d_k} g_1 + \underbrace{p_2^{d_2} \dots p_k^{d_k} g_2}_{=0} + \dots + \underbrace{p_2^{d_2} \dots p_k^{d_k} g_k}_{=0} = 0 \quad \Rightarrow \quad p_2^{d_2} \dots p_k^{d_k} g_1 = 0$$

  However, we also have $p_1^{d_1} g_1 = 0$. Since $p_1^{d_1}$ and $p_2^{d_2} \dots p_k^{d_k}$ are coprime, then (96) implies that $g_1 = 0$. The analogous argument shows that $g_2 = \dots = g_k = 0$, which implies that the kernel of (106) is trivial.

- *surjective*: let's assume that we have an element $g \in \text{Tors}_n(G) \subset \text{Tors}(G)$ and let us consider the prime decomposition

  $$n = p_1^{d_1} p_2^{d_2} \dots p_k^{d_k}$$

  where $p_1, \dots, p_k$ are distinct primes, and $d_1, \dots, d_k \in \mathbb{N}$. Then the element

  $$g_i = p_1^{d_1} \dots p_{i-1}^{d_{i-1}} p_{i+1}^{d_{i+1}} \dots p_k^{d_k} g$$

  has order dividing $p_i^{d_i}$, and thus lies in $A_{p_i}(G)$. However, the natural numbers

  $$\left\{ p_1^{d_1} \dots p_{i-1}^{d_{i-1}} p_{i+1}^{d_{i+1}} \dots p_k^{d_k} \right\}_{i \in \{1,\dots,k\}}$$

  have greatest common divisor 1. By the same token as the existence of the integers a, b such that (59) holds, there exist integers $a_1, \dots, a_k$ such that

  $$\sum_{i=1}^{k} a_i p_1^{d_1} \dots p_{i-1}^{d_{i-1}} p_{i+1}^{d_{i+1}} \dots p_k^{d_k} = 1$$

  Therefore, we have

  $$a_1 g_1 + \dots + a_k g_k = \left(\sum_{i=1}^{k} a_i p_1^{d_1} \dots p_{i-1}^{d_{i-1}} p_{i+1}^{d_{i+1}} \dots p_k^{d_k} \right) g = g$$

  which implies that g lies in the image of the homomorphism (106).

□

6.4

The following is a key notion. Fix a prime number p.

Definition 19. *We call a group G a p-**group** if the order of every element of G is a power of p.*

Although the notion above makes sense for all groups (and we will see it applied as such in a few lectures), for the time being we will consider it in the context of abelian groups. By definition, $A_p(G)$ defined in (104) is a p-group for any abelian group G.

Proposition 16. *A finite abelian group G is a p-group if and only if $|G|$ is a power of p.*

The "if" statement is an immediate consequence of Lagrange's theorem, since the order of any element divides the order of the group. The "only if" statement is an immediate Corollary of the following fact.

Proposition 17. *If a prime p divides the order of a finite abelian group G, then G has an element of order p.*

Proof. We will prove the statement by induction on the order of G. If G is cyclic, then the result is easy to prove, so please do it yourselves. Otherwise, we may consider an element $h \in G$ which does not generate the whole of G, and assume for the purpose of contradiction that $a = \mathrm{ord}_G(h)$ is coprime with p (indeed, if $p|a$, then we can easily find a power of h whose order is exactly p). Then we let H be the subgroup genereated by h and consider the quotient subgroup

$$G/H$$

Because the order of H is coprime with p, then p divides the order of G/H. By the induction hypothesis, there exists an element $g \in G$ such that $[g]$ has order p in G/H. This implies that

$$pg \in H \quad \Rightarrow \quad apg = 0$$

in G. This implies that ag either has order p (in which case we are done) or that $ag = 0$. However, since $\gcd(a, p) = 1$, then $pg \in H$ and $ag = 0 \in H$ would imply that $g \in H$, which contradicts the fact that $[g]$ has order p in G/H.

□

6.5

If G is a finite abelian group, then it is equal to its torsion subgroup. In this case, only finitely many of $A_p(G)$ can be non-trivial, or else the right-hand side of (105) would be an infinite set. Therefore, any finite abelian group G has the property that

$$G \cong A_{p_1}(G) \times \cdots \times A_{p_k}(G) \tag{107}$$

for distinct primes $p_1, \ldots, p_k$, where each $A_{p_i}(G)$ is a finite abelian p_i-group.

Proposition 18. *Any finite abelian p-group is isomorphic to*

$$\mathbb{Z}/p^{d_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{d_k}\mathbb{Z} \tag{108}$$

for various positive integers $d_1, \ldots, d_k$.

Proof. We will prove the Proposition by induction on $|G|$, with the induction base corresponding to the trivial group. Consider an element of G of largest possible order: let us call it h and assume that its order is p^{d_1}. Let $H \cong \mathbb{Z}/p^{d_1}\mathbb{Z}$ be the subgroup of G generated by h. The quotient group

$$G/H$$

is a p-group, because of Proposition 16 (if a group has order equal to a power of p, then so do all of its subgroups, and therefore so do all of its quotients). By the induction hypothesis, there exist positive integers $d_2, \ldots, d_k$ such that $G/H \cong \mathbb{Z}/p^{d_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{d_k}\mathbb{Z}$. Any element of G/H has order less than (any preimage of the same element) in G, so the fact that p^{d_1} is the maximal order implies that $d_1 \geq d_2, \ldots, d_k$. We conclude that there exists a short exact sequence

$$0 \to \mathbb{Z}/p^{d_1}\mathbb{Z} \to G \xrightarrow{\pi} \mathbb{Z}/p^{d_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{d_k}\mathbb{Z} \to 0$$

To conclude the proof of Proposition 18, it suffices to construct a splitting of the homomorphism π above. To this end, for each $i \in \{2, \ldots, k\}$ we define g_i to be an arbitrary element of G whose image under π is $(0, \ldots, 1, \ldots, 0) \in \mathbb{Z}/p^{d_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{d_i}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{d_k}\mathbb{Z}$. We have

$$p^{d_i}[g_i] = 0 \in G/H \quad \Rightarrow p^{d_i} g_i = a_i h, \quad \forall i \in \{2, \ldots, k\}$$

for some $a_i \in \mathbb{Z}$. Let us write $a_i = p^{s_i} t_i$ where t_i is coprime with p. Then the formula above reads

$$p^{d_i} g_i = p^{s_i} t_i h \tag{109}$$

Since all elements of G have order a power of p that is by assumption $\leq p^{d_1}$, we have

$$0 = p^{d_1} g_i = p^{d_1 - d_i + s_i} t_i h$$

Since t_i is coprime with p, the order of h is the same as the order of th (find an argument for this, using the fact that G is a p-group) and so the formula above implies that $d_1 - d_i + s_i \geq d_1 \Rightarrow s_i \geq d_i$ for all $i \in \{2, \ldots, k\}$. But then we can rewrite (109) as

$$p^{d_i}(\underbrace{g_i - p^{s_i - d_i} t_i h}_{\text{call this } g_i'}) = 0$$

The formula above ensures that the assignment

$$\mathbb{Z}/p^{d_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{d_k}\mathbb{Z} \xrightarrow{\psi} G, \qquad (x_2, \ldots, x_k) \mapsto x_2 g_2' + \cdots + x_k g_k'$$

is a well-defined homomorphism. It is also clear that $\pi \circ \psi = \mathrm{Id}$ by construction, and we are done. □

Proof. of Theorem 5 (without the statement that the decomposition (91) *is unique up to permuting the factors, which we choose not to do):* By (100), any finitely generated abelian group is $\mathbb{Z}^r$ times its torsion subgroup. By Proposition 15 and equation (102), the latter is finite. This implies that the torsion subgroup in question is a product of factors as in (107), and Proposition 18 ensures that all these factors are products of the form $\mathbb{Z}/p^d\mathbb{Z}$ for various primes p and various $d \in \mathbb{N}$.

□

Lecture 7

7.1

One usually thinks of abelian groups as being simple, but this terminology actually belongs to a different family of groups.

Definition 20. *A group G is called* ***simple*** *if it has exactly two normal subgroups:* 1 *and* G *(thus the trivial group is not considered to be simple, much like the number 1 isn't considered to be prime).*

Alternatively, a group is simple if and only if its only quotients are itself and the trivial group. In particular, any action of a simple group must either be trivial (i.e. every group element acts by the identity) or faithful. Because any subgroup of an abelian group is normal, the only simple abelian groups are $\mathbb{Z}/p\mathbb{Z}$ for a prime number p. But among the non-abelian groups we have a lot more examples; the following is a particularly important one.

Theorem 6. *Although the symmetric group S_n is not simple, its index two normal subgroup*

$$A_n = \operatorname{Ker}\left(S_n \xrightarrow{\text{sgn}} \mathbb{Z}/2\mathbb{Z}\right)$$

is simple, for any $n \geq 5$ (recall that sgn *sends any length $k+1$ cycle to k mod 2).*

Proof. Let $H \trianglelefteq A_n$ be any non-trivial normal subgroup of A_n, and let $h \in H$ be any non-identity element. As we know from Math 113, the permutation h can be written as a product of disjoint cycles. Moreover, since H is normal, we may conjugate h by any permutation and get an element of H. As we have seen in the proof of Proposition 5, conjugating a permutation has the effect of changing the entries of its constituent cycles. So if

$$h = \ldots (i_1\ i_2\ \ldots\ i_k) \ldots \tag{110}$$

then

$$h' = \ldots (j_1\ j_2\ \ldots\ j_k) \ldots \tag{111}$$

also lies in H, where $\{j_1, \ldots, j_k\}$ is any permutation of $\{i_1, \ldots, i_k\}$. In particular, we may choose $j_1 = i_k$, $j_2 = i_{k-1}$, $\ldots$, $j_k = i_1$, and then the cycle in (111) will be the inverse of the cycle in (110). Or if we choose $j_1 = i_k$, $j_2 = i_{k-1}$, $\ldots$, $j_{k-3} = i_4$, $j_{k-2} = i_2$, $j_{k-1} = i_3$, $j_k = i_1$, and then the product of the cycle in (111) with the cycle in (110) will be the length 3 cycle $(i_1\ i_3\ i_2)$. Thus, by appropriately choosing (111) in relation to (110) we may ensure that H contains a length 3 cycle. By suitably conjugating the aforementioned length 3 cycle, we conclude that H contains all the length 3 cycles. However, any product of two transpositions (i.e. length 2 cycles) can be written as a product of length 3 cycles, due to the following identities for all distinct numbers a, b, c, d

$$\begin{aligned}
(a\ b)(a\ b) &= e \\
(a\ b)(a\ c) &= (c\ b\ a) \\
(a\ b)(c\ d) &= (c\ a\ d)(b\ c\ a)
\end{aligned}$$

Since any permutation is a product of transpositions, it follows that any element of A_n is a product of an even number of transpositions, from which it follows that every element of A_n is a product of length 3 cycles. Thus, $A_n = H$, which implies that A_n is simple.

□

7.2

One may use simple groups as the building blocks for more general groups, as follows.

Definition 21. *A **subnormal series** of **length** k of a group G is a collection of subgroups*

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G \tag{112}$$

such that G_{i-1} is a normal subgroup of G_i, for all $i \in \{1, \ldots, k\}$. If moreover all the quotients $G_1/G_0, \ldots, G_k/G_{k-1}$ are simple groups, then we call (112) *a **composition series** of G.*

By the correspondence theorem 4, it is easy to show that (112) is a composition series if and only if it is maximal, i.e. we cannot enlarge it further by inserting more normal subgroups in between G_{i-1} and G_i. Not every group has a composition series, for example $\mathbb{Z}$ does not. Indeed, any of its non-trivial subgroups is isomorphic to $\mathbb{Z}$ itself, so any series such as (112) is doomed to go on forever. However, finite groups all have composition series, as per the following result.

Proposition 19. *Any finite group has a composition series.*

Proof. By induction on the order of G. Take a maximal normal subgroup $H \triangleleft G$, which exists because G is a finite set. Then consider the homomorphism

$$\pi : G \to G/H$$

If the group G/H failed to be simple, then by Theorem 4

$$\pi^{-1}(\text{a proper normal subgroup of } G/H)$$

would be a normal subgroup of G strictly contained between H and G. This is not allowed, because of the assumption that H is maximal, so we conclude that G/H is simple. By the induction hypothesis, H has a composition series; adding G to its right gives the required composition series of G.

□

For a finite abelian group, composition series can be written down very explicitly. For instance

$$0 < \mathbb{Z}/p\mathbb{Z} < \mathbb{Z}/p^2\mathbb{Z} < \cdots < \mathbb{Z}/p^k\mathbb{Z}$$

is a composition series, where $\mathbb{Z}/p^{i-1}\mathbb{Z} = p\mathbb{Z}/p^i\mathbb{Z}$ is interpreted as a subgroup of $\mathbb{Z}/p^i\mathbb{Z}$.

7.3

Normal subgroups and quotient groups inherit composition series from their parent group, as we will show in the Propositions below.

Proposition 20. *If a group G has a composition series* (112)*, then for any normal subgroup $H \trianglelefteq G$ we may form*

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{k-1} \trianglelefteq H_k = H \tag{113}$$

where $H_i = H \cap G_i$. Upon removing redundancies from the series above (i.e. if $H_{i-1} = H_i$ for some i, then we remove H_i from the series), then (113) *yields a composition series for H.*

Proof. Let us show that for all i, the subgroup H_{i-1} is normal in H_i. To this end, take any $g \in H_i$ and $h \in H_{i-1}$. The element ghg^{-1} is

- in G_{i-1}, because G_{i-1} is normal in G_i, and
- in H, because H is a subgroup.

Thus $ghg^{-1} \in H_{i-1}$, which implies that H_{i-1} is normal in H_i. Having said this, we note that the inclusions $G_{i-1} \hookrightarrow G_i$ induce an injective homomorphism

$$H_i/H_{i-1} \overset{\varphi}{\hookrightarrow} G_i/G_{i-1} \tag{114}$$

Let us now show that Im φ is normal in G_i/G_{i-1}. Take any $[g], [h] \in G_i/G_{i-1}$ represented by some $g \in G_i$ and $h \in H_i$. Then the element ghg^{-1} is

- in G_i, because G_i is a subgroup, and
- in H, because H is normal in G

Thus $ghg^{-1} \in H_i$, so $[g][h][g]^{-1} \in$ Im φ. Since G_i/G_{i-1} is simple, then Im φ is either the trivial subgroup or the entire G_i/G_{i-1}. In the former case we have $H_i = H_{i-1}$ and in the latter case we have $H_i/H_{i-1} \cong G_i/G_{i-1}$. This implies the required conclusion.

□

Remark. *Non-normal subgroups do not necessarily inherit composition series. For instance, many simple groups G contain elements of infinite order (so they contain $\mathbb{Z}$ as a subgroup) but we have already seen that $\mathbb{Z}$ does not have a composition series.*

7.4

Just like normal subgroups inherit composition series (as we showed in the previous Subsection), we will now show that quotient groups also do.

Proposition 21. *If a group G has a composition series* (112)*, then for any normal subgroup $H \trianglelefteq G$ with corresponding quotient group $\bar{G} = G/H$, we may form*

$$1 = \bar{G}_0 \trianglelefteq \bar{G}_1 \trianglelefteq \cdots \trianglelefteq \bar{G}_{k-1} \trianglelefteq \bar{G}_k = \bar{G} \tag{115}$$

where $\bar{G}_i = HG_i/H$. Upon removing redundancies from the series above (i.e. if $\bar{G}_{i-1} = \bar{G}_i$ for some i, then we remove $\bar{G}_i$ from the series), then (115) *yields a composition series for $\bar{G}$.*

Proof. We first show that G_{i-1} being normal in G_i implies that HG_{i-1} is normal in HG_i. To see this, take any $hg \in HG_i$ and any $h'g' \in HG_{i-1}$ (with $h, h' \in H$, $g \in G_i$ and $g' \in G_{i-1}$). Then

$$(hg)(h'g')(hg)^{-1} = hgh'g'g^{-1}h^{-1} \in hgHg'g^{-1}h^{-1} = hH \underbrace{gg'g^{-1}}_{\text{some } g'' \in G_{i-1}} h^{-1} \subseteq Hg''H = Hg''$$

(the fact that H is normal implies that $gH = Hg$ for any $g \in G$). Now that we showed that HG_{i-1} is a normal subgroup of HG_i, Theorem 4 implies that $\bar{G}_{i-1}$ is a normal subgroup of $\bar{G}_i$.

By the second isomorphism theorem, we have $\bar{G}_i \cong G_i/H \cap G_i$ for all i. The inclusion $G_{i-1} \hookrightarrow G_i$ induces an injective homomorphism

$$\bar{G}_{i-1} \cong G_{i-1}/H \cap G_{i-1} \hookrightarrow G_i/H \cap G_i \cong \bar{G}_i$$

The quotient $\bar{G}_i/\bar{G}_{i-1}$ is isomorphic to G_i/K, where K is the subgroup of G_i generated by G_{i-1} and $H \cap G_i$. Since both G_{i-1} and $H \cap G_i$ are normal subgroups of G_i, then the second bullet of Proposition 7 implies that K is also normal in G_i. However, by the correspondence theorem, the simplicity of G_i/G_{i-1} implies that there are no normal subgroups strictly contained between G_{i-1} and G_i. Therefore, G_i/K is either the trivial group or a simple group, so (115) is (after removing redundancies) a composition series.

□

7.5

We will now study how composition series of smaller groups lift to bigger groups.

Proposition 22. *Suppose we have a short exact sequence of groups*

$$1 \to K \to G \xrightarrow{\pi} L \to 1$$

and that both K and L have composition series

$$1 = K_0 \lhd K_1 \lhd \cdots \lhd K_{m-1} \lhd K_m = K$$

$$1 = L_0 \lhd L_1 \lhd \cdots \lhd L_{n-1} \lhd L_n = L$$

Then there exists a composition series

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_{m+n-1} \lhd G_{m+n} = G \tag{116}$$

with $G_i \cong K_i$ for $i \leq m$ and $G_i \cong \pi^{-1}(L_{i-m})$ for $i > m$.

Proof. First of all, it is clear that the first m inclusions in (116) are normal subgroups, with quotients isomorphic to those in the composition series of K (thus the quotients are simple). As for the next m inclusions, the correspondence Theorem 4 states that there is a one-to-one correspondence

$$\Big\{\text{subgroups } K \leq H \leq G\Big\} \leftrightarrow \Big\{\text{subgroups } \bar{H} \leq L\Big\}$$

explicitly given by $H = \pi^{-1}(\bar{H})$. Property 2 of said theorem states that subgroups $\bar{H} \trianglelefteq \bar{H}'$ in the right-hand side correspond to subgroups $H \trianglelefteq H'$ in the left-hand side, such that

$$H'/H \cong \bar{H}'/\bar{H}$$

This shows that the last n inclusions in (116) are also normal subgroups, with quotients isomorphic to those in the composition series of L (thus the quotients are simple).

□

7.6

If a group has a composition series, then it is likely that it has a lot of them. However, any two composition series are related by the following result, called the Jordan-Hölder theorem.

Theorem 7. *For any group G, any two composition series*

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G = G'_\ell \triangleright G'_{\ell-1} \triangleright \cdots \triangleright G'_1 \triangleright G'_0 = 1 \tag{117}$$

are ***equivalent****, i.e. the sequences of quotients*

$$\left\{G_1/G_0, \ldots, G_k/G_{k-1}\right\} \quad \textit{and} \quad \left\{G'_1/G'_0, \ldots, G'_\ell/G'_{\ell-1}\right\} \tag{118}$$

are the same up to permutation and isomorphism. In particular, $k = \ell$. The (isomorphism classes of the) groups (118) *are called the* ***composition factors*** *of G.*

Note that equivalence of composition series is an equivalence relation. Before we jump into the proof of the Theorem, let us provide an illustrative example. There are two length 2 composition series of $\mathbb{Z}/6\mathbb{Z}$, one involving the subgroup $\{0, 3\} \cong \mathbb{Z}/2\mathbb{Z}$ and one involving the subgroup $\{0, 2, 4\} \cong \mathbb{Z}/3\mathbb{Z}$. The composition factors for these two composition series are $(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z})$ and $(\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$.

Proof. We will do induction on the number $\min(k, \ell)$ (and then by $k + \ell$ to break ties). The case when this number is 1 is trivial, because a simple group cannot have a composition series of length ≥ 2, on account of not having any non-trivial normal subgroups. Let us now assume $\min(k, \ell) \geq 2$, and prove the induction step. We may assume that $G_{k-1} \neq G'_{\ell-1}$ (otherwise we simply apply the induction hypothesis to $G_{k-1} = G'_{\ell-1}$ instead of G). Since G_{k-1} and $G'_{\ell-1}$ are both normal in G, both their product

$$P = G_{k-1}G'_{\ell-1}$$

and their intersection

$$H = G_{k-1} \cap G'_{\ell-1}$$

are normal in G (see Proposition 7). Then the second isomorphism Theorem 3 implies that

$$G_{k-1}/H \cong P/G'_{\ell-1} \quad \text{and} \quad G'_{\ell-1}/H \cong P/G_{k-1}$$

However, by the correspondence theorem, $P/G'_{\ell-1}$ is a normal subgroup of $G/G'_{\ell-1}$. Since the latter group is simple, we must have $P = G$ and so we have the following isomorphisms of simple groups

$$G_{k-1}/H \cong G/G'_{\ell-1} \quad \text{and} \quad G'_{\ell-1}/H \cong G/G_{k-1} \tag{119}$$

Proposition 20 ensures that H has a composition series (whose length m must be less than or equal to the lengths of composition series of either G_{k-1} or $G'_{\ell-1}$, which are $\leq k-1$ and $\leq \ell - 1$, respectively), which we may extend to composition series

$$1 \triangleleft H_1 \triangleleft \cdots \triangleleft H_{m-1} \triangleleft H \triangleleft G_{k-1} \triangleleft G \tag{120}$$

and

$$1 \triangleleft H_1 \triangleleft \cdots \triangleleft H_{m-1} \triangleleft H \triangleleft G'_{\ell-1} \triangleleft G \tag{121}$$

By the induction hypothesis, (120) and (121) are equivalent to the composition series on the left and on the right of (117), respectively. Since (120) and (121) are equivalent by (119), we are done. □

Lecture 8

8.1

We have already encountered groups that have composition series (112). The following is then a related notion.

Definition 22. *A group G is called **solvable** if it has a subnormal series*

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G \tag{122}$$

such that G_{i-1} is a proper normal subgroup of G_i such that G_i/G_{i-1} is abelian, for all $i \in \{1, \ldots, k\}$.

The terminology stems from Galois theory, specifically the theory of polynomial equations which admit solutions by radicals, in which solvable groups play a key role. Specifically, if you take a class in Galois theory you will definitely encounter the following result.

Proposition 23. *The symmetric group S_n is not solvable for $n \geq 5$.*

Proof. Suppose $G = S_n$ admitted a subnormal series (122) with abelian quotients, and we will consider such a series of maximal length k. Since S_n is finite, this implies that the abelian quotient groups G_i/G_{i-1} are finite for all $i \in \{1, \ldots, k\}$. If one of these abelian quotient groups G_i/G_{i-1} were not isomorphic to $\mathbb{Z}/p\mathbb{Z}$, then we may find a proper subgroup $1 \subsetneq \bar{H} \subsetneq G_i/G_{i-1}$ (prove this, it's quite easy). By the correspondence Theorem 4, this would mean the existence of a subgroup

$$G_{i-1} \triangleleft H \triangleleft G_i$$

which violates the maximality of the number k. However, $\mathbb{Z}/p\mathbb{Z}$ is also a simple group, so we conclude that S_n admits a composition series all of whose factors are $\mathbb{Z}/p\mathbb{Z}$. However, this contradicts the Jordan-Holder theorem 7 and the fact that S_n admits the composition series

$$1 \triangleleft A_n \triangleleft S_n$$

(recall from Theorem 6 that A_n is simple for $n \geq 5$).

□

8.2

Solvable groups enjoy much the same properties as groups with composition series, specifically the following analogues of Propositions 20, 21 and 22.

Proposition 24. *Any subgroup of a solvable group is solvable.*

Proof. The proof follows that of Proposition 20 closely, except that it applies to arbitrary subgroups and not just normal subgroups. Thus, take a solvable group G with a subnormal series

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G$$

with each G_i/G_{i-1} abelian. Then for any subgroup $H \leq G$, consider the series

$$1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_{k-1} \triangleleft H_k = H \tag{123}$$

with $H_i = H \cap G_i$. One shows that H_{i-1} is a subgroup of H_i just like in the proof of Proposition 20, and moreover we have an analogue of the injective homomorphism

$$H_i/H_{i-1} \overset{\varphi}{\hookrightarrow} G_i/G_{i-1}$$

of (114). Since any subgroup of an abelian group is abelian, the fact that G_i/G_{i-1} is abelian implies that H_i/H_{i-1} is abelian. Therefore, the existence of the series (123) implies that H is solvable. □

The following results are proved just like Propositions 21 and 22, so we will not repeat the proofs.

Proposition 25. *Any quotient of a solvable group is solvable.*

Proposition 26. *Suppose we have a short exact sequence of groups*

$$1 \to K \to G \overset{\pi}{\to} L \to 1$$

with K and L solvable. Then G is solvable.

Proposition 26 provides a rich class of examples of solvable groups: any group which can be obtained by finitely many steps of taking extensions (such as semi-direct products) from abelian groups. All dihedral groups are solvable, as is the alternating group A_4.

8.3

We will now provide an alternative description of solvable groups. Recall the following from Math 113.

Definition 23. *Given a subset X of a group G, the smallest subgroup $H \leq G$ which contains X is called the subgroup **generated** by X. Explicitly, H consists of arbitrary products of elements of X and their inverses.*

Definition 24. *Given subsets $X, Y \subseteq G$, let $[X, Y] \leq G$ denote the subgroup of G generated by*

$$\left\{ xyx^{-1}y^{-1} \middle| x \in X, y \in Y \right\}$$

*The **derived subgroup** (or **commutator subgroup**) of G is defined to be*

$$\boxed{[G, G]} \tag{124}$$

Proposition 27. *For any group G, the derived subgroup $[G, G]$ is a normal subgroup of G and*

$$G/[G, G]$$

is abelian. Moreover, if any $H \trianglelefteq G$ has the property that G/H is abelian, then $[G, G] \subseteq H$.

Proof. To show that a subgroup is normal, one must show that it is preserved under conjugation with an arbitrary $h \in G$. However, the conjugation by g of any commutator is another commutator, as

$$gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}$$

Therefore, the conjugation by g of an arbitrary product of commutators is a product of commutators, so $[G, G]$ is a normal subgroup of G. The quotient $G/[G, G]$ is clearly abelian since

$$[a][b][a^{-1}][b^{-1}] = [aba^{-1}b^{-1}] = e \in G/[G, G] \quad \Rightarrow \quad [a][b] = [b][a]$$

More generally, for any normal subgroup $H \trianglelefteq G$ such that the quotient G/H is abelian, we have

$$[a][b][a^{-1}][b^{-1}] = [aba^{-1}b^{-1}] = e \text{ in } G/H \quad \Rightarrow \quad aba^{-1}b^{-1} \in H$$

for all $a, b \in G$. Therefore, $[G, G] \subseteq H$.

□

8.4

The derived subgroup of a group is trivial if and only if the group is abelian. But the derived subgroup need not be abelian itself, so we can take the derived subgroup of the derived subgroup, and so on. This leads to the notion of **derived series** of a group G, which is defined as

$$\cdots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G \tag{125}$$

where $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$ is the derived subgroup of $G^{(i-1)}$ for all i.

Proposition 28. *A group G is solvable if and only if its derived series eventually becomes trivial, i.e. if there exists some $k \in \mathbb{N}$ such that $G^{(k)} = 1$.*

Proof. The "if" statement is trivial, because if the derived series is finite, then Proposition 27 ensures that it provides precisely the kind of subnormal series with abelian quotients, that characterizes solvable groups. To prove the "only if" statement, let us consider a solvable group G with series (122). The last sentence in Proposition 27 ensures the fact that

$$G^{(1)} \subseteq G_{k-1}$$

Taking the derived subgroups with respect of the inclusion above implies

$$G^{(2)} \subseteq [G_{k-1}, G_{k-1}] \subseteq G_{k-2}$$

where the second inclusion again stems from the fact that the quotient G_{k-1}/G_{k-2} is abelian (invoking the last sentence of Proposition 27). Repeating this argument $k-2$ more times ultimately implies $G^{(k)} \subseteq G_0 = 1$, which implies that the derived series eventually becomes trivial.

□

8.5

In Proposition 28, we considered the series of commutator subgroups starting from G, and showed that it terminates if and only if G is solvable. A stronger notion is the following.

Definition 25. *A group G is called **nilpotent** if the sequence of subgroups defined by $G^{\{0\}} = G$ and*

$$G^{\{i\}} = [G^{\{i-1\}}, G]$$

becomes the trivial group 1 after finitely many steps.

For an abelian group, we have $G^{\{1\}} = 1$, so nilpotent groups can be interpreted as generalizations of abelian groups. For a nilpotent group G, the sequence of subgroups

$$\cdots \trianglelefteq G^{\{2\}} \trianglelefteq G^{\{1\}} \trianglelefteq G^{\{0\}} = G \tag{126}$$

is actually a normal series, in the sense that every $G^{\{i\}}$ is a normal subgroup of G. One can prove this by induction on i: if one assumes that $G^{\{i-1\}}$ is normal in G, then any commutator

$$a \underbrace{ba^{-1}b^{-1}}_{\in G^{\{i-1\}}}, \quad \forall a \in G^{\{i-1\}}, b \in G \tag{127}$$

lies in $G^{\{i-1\}}$, and so $G^{\{i\}}$ is a subgroup of $G^{\{i-1\}}$. The fact that $G^{\{i\}}$ is normal in G comes from the fact that conjugating an element of the form (127) by an arbitrary element of G still produces an element of the form (127), which we leave to you as an exercise. The series (126) is called the **lower central series** of G.

Proposition 29. *Any nilpotent group is solvable.*

Proof. Let G be a nilpotent group. One can prove by induction on i that $G^{(i)} \subseteq G^{\{i\}}$ for all i, which is immediate, but important, so we leave it to you. Therefore, the fact that the sequence (126) terminates implies that (125) terminates, so G is also solvable.

□

Lecture 9

9.1

In Lecture 6, we studied finite abelian p-groups for some prime number p, see Definition 19. We will now drop the abelian hypothesis and study finite p-groups, i.e. those groups where the order of every element is a power of p (we will write this as "has order in $p^{\mathbb{N}}$ from now on).

Lemma 13. *A finite group is a p-group if and only if it has order p^n for some $n \in \mathbb{N}$.*

The "if" implication is an immediate consequence of Lagrange's theorem, because the order of any element divides the order of the group. The "only if" implication is an immediate consequence of the following result, often called **Sylow's first theorem**.

Theorem 8. *Let G be a finite group of order*

$$|G| = p^n r$$

for some prime p, some $n \geq 0$ and some r coprime with p. Then G has a subgroup of order p^n.

Indeed, once we have Theorem 8, the "only if" statement of Lemma 13 is quite imediate. If $|G|$ were not a power of p, then take some other prime number $q \neq p$ which divides $|G|$. Theorem 8 guarantees that $|G|$ has a subgroup of order in $q^{\mathbb{N}}$, and any element in that subgroup will have order in $q^{\mathbb{N}}$. This contradicts the fact that G is a p-group, i.e. every element has order in $p^{\mathbb{N}}$.

9.2

Clearly, the $n = 0$ case of Theorem 8 is trivial, so people typically assume $n > 0$.

Proof. of Theorem 8: We will do induction by $|G|$ (the base case is $|G| = p$, which is trivial, because the only group of prime order p is $\mathbb{Z}/p\mathbb{Z}$). If there exists a proper subgroup $H < G$ such that

$$[G : H] \text{ divides } r \tag{128}$$

then $|H| = p^n r'$ for some $r' < r$ that is coprime with p. The induction hypothesis then implies that there exists a subgroup of H of order p^n, which will also be the sought-for subgroup of G of order p^n. So we are left with the logical opposite of (128): for all proper subgroups $H < G$, we have

$$p \text{ divides } [G : H] \tag{129}$$

(indeed, since $[G : H] > 1$ is a divisor of $|G| = p^n r$, then (128) and (129) are logically opposite statements). Then let us apply the class equation (50)–(52)

$$|G| = \sum_{\text{conjugacy classes } \widetilde{g}} [G : C_G(\widetilde{g})]$$

The left-hand side is a multiple of p. By (129), so is any summand in the right-hand side for which $C_G(\widetilde{g}) \neq G$. Therefore, we conclude that

$$\text{the number of conjugacy classes for which } \Big(C_G(\widetilde{g}) = G\Big) \text{ is a multiple of } p$$

However, an element $g \in G$ has the property that $C_G(g) = G$ if and only if $g \in Z(G)$, the center of G. Since every element $g \in Z(G)$ lies in its own conjugacy class, the formula above reads

$$p \text{ divides } |Z(G)|$$

Since $Z(G)$ is abelian, Proposition 17 implies that exists $g \in Z(G)$ of order p. Therefore, the subgroup H generated by g has order p, and is normal because $g \in Z(G)$. The quotient group

$$\bar{G} = G/H$$

has order $p^{n-1}r$. By the induction hypothesis, $\bar{G}$ has a subgroup $\bar{K}$ of order p^{n-1}. By the correspondence Theorem 4, this subgroup corresponds to a subgroup $K \leq G$ of order p^n, as required.

□

9.3

A subgroup of order p^n as in Theorem 8 is called a **Sylow p-subgroup** of G. It is customary to denote such a subgroup by P. The next results give additional information on these subgroups. We start with **Sylow's second theorem**.

Theorem 9. *All Sylow p-subgroups of a group G are conjugate to each other.*

In other words, if we have one Sylow p-subgroup $P \leq G$, then all other Sylow p-subgroups of G are of the form gPg^{-1} for various $g \in G$.

Proof. Consider two Sylow p-subgroups P and P', and consider the left action of P on the set of left cosets of P'

$$P \curvearrowright G/P'$$

Applying formula (37) to this action reads

$$r = |G/P'| = \sum_{\text{orbits } P\cdot x} \frac{|P|}{|\text{Stab}_P(x)|}$$

Because the order of P is a power of p, all orbits in the right-hand side for which $\text{Stab}_P(x) \neq P$ will contribute a multiple of p. However, r is coprime with p, so this means that there must be at least one orbit whose stabilizer is the whole of P. This orbit precisely corresponds to a left coset gP' which is fixed by P, which means that

$$hgP' = gP', \quad \forall h \in P \quad \Leftrightarrow \quad g^{-1}hg \in P', \quad \forall h \in P \quad \Leftrightarrow \quad P \subseteq gP'g^{-1} \tag{130}$$

However, the fact that $|P| = |P'|$ implies that we must have $P = gP'g^{-1}$, as required.

□

9.4

The converse of Theorem 9 is an obvious statement: any conjugate of a Sylow p-subgroup is a Sylow p-subgroup. Thus, if for some reason there exists a single Sylow p-subgroup, it must be preserved by conjugation, and thus would be normal. With this in mind, it becomes very important to calculate the number of Sylow p-subgroups, which is the subject of **Sylow's third theorem**.

Theorem 10. *The number n_p of Sylow p-subgroups of a group G has the properties that*

- $n_p = [G : N_G(P)]$*, where P is any fixed Sylow p-subgroup, and n_p divides r*
- $n_p \equiv 1$ *modulo p*

Proof. By Sylow's second theorem, conjugation induces a transitive action

$$G \curvearrowright \Big\{\text{Sylow } p\text{-subgroups of } G\Big\} \tag{131}$$

and so n_p is the cardinality of the unique orbit. The stabilizer of any given Sylow p-subgroup P is none other than the normalizer $N_G(P)$. Therefore, the orbit-stabilizer theorem (36) implies that cardinality of the unique orbit is

$$\frac{|G|}{|N_G(P)|} = [G : N_G(P)]$$

Since $P \leq N_G(P)$, we have that $n_p = [G : N_G(P)]$ divides $[G : P] = r$. Let us now fix a Sylow p-subgroup P and consider the restriction of the conjugation action (131) to

$$P \curvearrowright \Big\{\text{Sylow } p\text{-subgroups of } G\Big\}$$

Applying (37) this action implies that

$$n_p = \sum_{\text{orbits } P\cdot P'} \frac{|P|}{|\text{Stab}_P(P')|}$$

Since $|P| = p^n$, every summand in the right-hand side is a multiple of p, except for those Sylow p-subgroups P' which are fixed by conjugation by any element of P. If we show that the only such Sylow p-subgroup P' is equal to P itself, then we conclude $n_p \equiv 1$ modulo p and we are done. However, P' being fixed by conjugation with any element of P implies that

$$P \leq N_G(P')$$

Because $|N_G(P')|$ divides $|G| = p^n r$, then P is a Sylow p-subgroup of $N_G(P')$. On the other hand, P' is a normal subgroup of $N_G(P')$ (by the very definition of the normalizer), so Sylow's second theorem (with G replaced by $N_G(P')$) implies that $P = P'$, as desired.

□

9.5

Let us now exemplify the Sylow theorems for the dihedral group D_{2n}. The following Lemma will be useful.

Lemma 14. *Consider a normal subgroup $H \trianglelefteq G$ of a finite group G. Then for any prime p, the intersection of a Sylow p-subgroup of G with H will be a Sylow p-subgroup of H.*

Proof. Let P be a p-Sylow subgroup of G. As the group $H \cap P$ has order in $p^{\mathbb{N}}$, we need to show that $[H : H \cap P]$ is coprime with p in order to ensure that the order of $H \cap P$ is the maximal power of p which divides $|H|$. The second isomorphism Theorem 3 implies that HP is a group of order

$$|HP| = \frac{|H||P|}{|H \cap P|}$$

Therefore,

$$[HP : P] = [H : H \cap P]$$

Since HP is a subgroup of G, the number on the left of the display above divides $[G : P]$, which is coprime with p by the definition of a Sylow p-subgroup. Therefore, the number on the right of the display above will also be coprime with p, thus implying that $H \cap P$ is a Sylow p-subgroup of H. □

Let us apply the Lemma above for $G = D_{2n}$ and $H \cong \mathbb{Z}/n\mathbb{Z}$ being the normal subgroup of rotations, where $n = 2^k r$ for some odd r. Since $\mathbb{Z}/n\mathbb{Z}$ is abelian, it has a single Sylow 2-subgroup, namely

$$P = \{0, r, 2r, \ldots, (2^k - 1)r\} \subseteq \{0, 1, 2, \ldots, 2^k r - 1\} = \mathbb{Z}/n\mathbb{Z}$$

Any Sylow 2-subgroup of $G = D_{2n}$ has order 2^{k+1}, and contains the order 2^k subgroup P by Lemma 14. Therefore, if we take any reflection $\tau \in G - H$, then any Sylow 2-subgroup must be of the form

$$P_\tau = P \sqcup P\tau \tag{132}$$

However, any set P_τ is a subgroup of G (try to prove it), so there are as many Sylow 2-subgroups as reflections τ modulo left multiplication by P. As there are n reflections in total and $|P| = 2^k$, then there are r distinct Sylow 2-subgroups P_τ, which supports Sylow's third Theorem 10. By the same theorem, the fact that $n_2 = r$ implies that $N_G(P_\tau) = P_\tau$, which you can also try to prove by hand.

Lecture 10

10.1

We will now use the Sylow theorems to draw conclusions about finite groups whose orders have few prime factors. First of all, we recall the basic fact that any group G of order p is isomorphic to

$$\mathbb{Z}/p\mathbb{Z}$$

To see this, take any non-identity element $g \in G$. Because the order of g divides $|G| = p$, then the order of g must be equal to p, and so G equals the cyclic group generated by g.

Proposition 30. *If p and q are distinct primes such that $p \nmid q-1$ and $q \nmid p-1$, any group of order pq is isomorphic to*

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \tag{133}$$

Note that such a group is also cyclic, due to (90)*.*

Proof. Assume $|G| = pq$. By Sylow's third theorem, the number n_p of Sylow p-subgroups divides q and is congruent with 1 mod p, so the only option is that $n_p = 1$. Similarly, we must have $n_q = 1$. Thus, we have a single Sylow p-subgroup P and a single q-subgroup Q, and they must be normal subgroups of G. Note that $P \cap Q = \{e\}$, because any element in the intersection of P and Q would have order dividing both the distinct primes p and q. But then we have an isomorphism

$$PQ \cong P \times Q \tag{134}$$

(you proved this in Math 113, and let us recall the argument: the function $P \times Q \to PQ, (x, y) \mapsto xy$ is injective because $P \cap Q = \{e\}$. It is surjective by definition, and the fact that it is a homomorphism follows from $xy = yx$ for all $x \in P, y \in Q$, which in turn is due to the commutator $xyx^{-1}y^{-1}$ lying in $P \cap Q = \{e\}$. The last statement uses the fact that P and Q are both normal). Since $|P| = p$ and $|Q| = q$, then $P \cong \mathbb{Z}/p\mathbb{Z}$ and $Q \cong \mathbb{Z}/q\mathbb{Z}$, while $|PQ| = pq \Rightarrow PQ = G$. Thus (134) $\Rightarrow$ (133). □

Note that Proposition 30 fails if $p|q-1$. For instance, $D_6 \cong S_3$ is a nonabelian group of order 6.

10.2

While it doesn't use the Sylow theorems, the following classification result is also very important.

Proposition 31. *If p is prime, then any group of order p^2 is isomorphic to either*

$$\mathbb{Z}/p^2\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \tag{135}$$

One of the key elements in the proof of Proposition 31 is the following.

Lemma 15. *If G is a non-trivial finite p-group for some prime p, then $Z(G)$ is non-trivial.*

Proof. The class equation (50) reads

$$|G| = |Z(G)| + \sum_{\text{conjugacy classes } \widetilde{g} \text{ of cardinality } >1} |\widetilde{g}|$$

However, since $|G| = p^n$ with $n > 0$ and the cardinality of any conjugacy class divides $|G|$ (due to formula (52)), we conclude that $|Z(G)|$ is a multiple of p. Therefore, $Z(G)$ must be non-trivial.

□

Proof. of Proposition 31: Let G be a group of order p^2. Because its center $Z(G)$ is non-trivial by Lemma 15, the center must have order either p^2 or p. In the former case, G must be abelian, so Proposition 18 implies that G must be isomorphic to one of the two options in (135). In the latter case, consider some element $g \in G - Z(G)$ and let $H = C_G(g)$. We claim that

$$Z(G) \subsetneq H \subsetneq G$$

which is a contradiction because the number $|H|$ would have to be simultaneously a proper multiple of $p = |Z(G)|$ and a proper divisor of $p^2 = |G|$. The first $\subsetneq$ above is due to the fact that $g \in H - Z(G)$, while the second $\subsetneq$ is due to the fact that $H = G$ would imply $g \in Z(G)$.

□

10.3

Combining the ideas of Propositions 30 and 31 gives us the following.

Proposition 32. *If p and q are distinct primes such that $p \nmid q - 1$ and $q \nmid p^2 - 1$, any group of order p^2q is isomorphic to either*

$$\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

Proof. As in the proof of Proposition 30, there exists a unique Sylow p-subgroup P and a unique Sylow q-subgroup Q. These subgroups must be normal by Sylow's third theorem and the assumptions $p \nmid q - 1$ and $q \nmid p^2 - 1$, and their intersection is trivial. Therefore, (134) holds for the same reason as in the proof of Proposition 30, and the proof is completed by the classification of groups of order p^2 in Proposition 31.

□

However, even when the non-divisibility assumptions in Propositions 30 and 32 fail, we can still use the Sylow theorems to deduce important information about groups. For example, you proved the following result by elementary means in Math 113, but using the Sylow theorems is much faster.

Proposition 33. *Any group of order 12 is isomorphic to either*

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \quad \text{or} \quad A_4 \quad \text{or} \quad D_{12} \tag{136}$$

*or the **dicylic group** that we will define in the course of the proof.*

Proof. Assume $|G| = 12$ and let us consider the number n_3 of Sylow 3-subgroups. By Sylow's third Theorem 10, we have $n_3|4$ and $n_3 \equiv 1 \bmod 3$. Thus, we can have either $n_3 = 1$ or $n_3 = 4$. In the case $n_3 = 4$, we have four Sylow 3-groups, which we will denote by P_1, P_2, P_3, P_4. Since they have order 3, these subgroups can only pairwise intersect in the identity element, so this means that our group contains at least $2 \times 4 = 8$ elements of order 3. Consider the action

$$G \curvearrowright \Big\{P_1, P_2, P_3, P_4\Big\}, \qquad g \cdot P_i = gP_ig^{-1}$$

which induces a homomorphism $f : G \to S_4$. Sylow's third Theorem 10 implies that $4 = n_3 = [G : N_G(P_i)]$, hence $N_G(P_i) = P_i$ for all i. Thus, the kernel of f must be contained in P_i for all i. As we explained in the preceding paragraph, we have $P_i \cap P_j = \{e\}$ for all $i \neq j$, so the kernel of f is trivial. Therefore, G is isomorphic to a subgroup of S_4. However, recall that G contains at least 8 elements of order 3. Inside the symmetric group S_4, the only elements of order 3 are the cycles of length 3, which are all contained in the alternating group A_4. Therefore, the subgroup $|\text{Im } f \cap A_4|$ of A_4 has order at least 8. However, since the order of this subgroup would have to divide $12 = |A_4|$, the only option is $\text{Im } f = A_4$, which implies that $G \cong A_4$.

Let us now consider the case $n_3 = 1$, i.e. there exists a single Sylow 3-subgroup of G, hence this subgroup must be normal by Sylow's second Theorem 9. We therefore obtain a short exact sequence

$$0 \to \mathbb{Z}/3\mathbb{Z} \to G \xrightarrow{\pi} L \to 0$$

where L is a group of order 4. However, let P be a Sylow 2-subgroup of G. Since its intersection with $\mathbb{Z}/3\mathbb{Z}$ consists of just the identity (otherwise P would contain a subgroup of order 3, which is implossible for a group of order 4), then π induces an isomorphism $\pi' : P \cong L$ of groups of order 4. The inverse of π' precisely provides a splitting to π, and so Proposition 10 implies that

$$G \cong \mathbb{Z}/3\mathbb{Z} \rtimes L$$

for some action $L \curvearrowright \mathbb{Z}/3\mathbb{Z}$ by automorphisms. If this action is trivial, then the two possibilities $L \cong \mathbb{Z}/4\mathbb{Z}$ and $L \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ give us the first two options in (136). On the other hand, we need to classify the non-trivial actions of L by automorphisms on $\mathbb{Z}/3\mathbb{Z}$. Since the only non-trivial automorphism of $\mathbb{Z}/3\mathbb{Z}$ is $\Phi(k) = (2k \bmod 3)$, then up to isomorphism we have two options

$$\begin{array}{lll} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \curvearrowright \mathbb{Z}/3\mathbb{Z}, & (a,b) \bmod 2 \text{ acts by } \Phi^a & \Rightarrow \quad G \cong D_{12} \\ \mathbb{Z}/4\mathbb{Z} \curvearrowright \mathbb{Z}/3\mathbb{Z}, & a \bmod 4 \text{ acts by } \Phi^a & \Rightarrow \quad G = \text{Dic}_{12} \end{array}$$

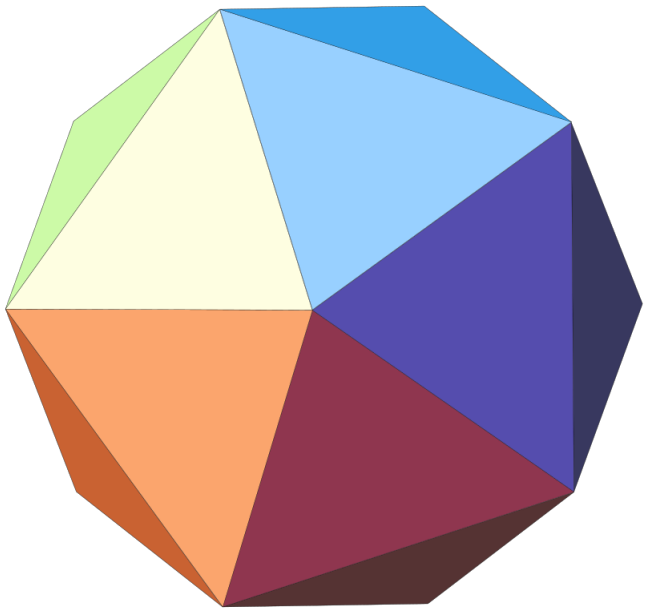
The latter equality is the definition of the dicylic group Dic_{12}. In the first equation above, I'm claiming that the dihedral group $\mathbb{Z}/6\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ is also isomorphic to $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ because the action of the last factor of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}/3\mathbb{Z}$ is trivial. This is a general fact about actions by automorphisms, which we leave for you to check: for any action $L \curvearrowright K$ by automorphisms and any group H, there is an isomorphism of semi-direct products $(K \times H) \rtimes L \cong K \rtimes (L \times H)$, where in the left-hand side the action on H is trivial and in the right-hand side the action of H is trivial. □

10.4

As shown in Theorem 6, the alternating group A_5 is a simple group of order $\frac{5!}{2} = 60$. In the next result, we will use the Sylow theorems to show that it is the only group of this kind.

Proposition 34. *If G is a simple group of order 60, then $G \cong A_5$.*

One interesting consequence of Proposition 34 is that A_5 is isomorphic to the icosahedral group I, i.e. the group of rotations of three dimensional space which preserve a regular icosahedron [1].



Indeed, geometrically describing the rotations in question (which we will not do) allows us to classify the conjugacy classes of I. The answer reveals that the class equation (50) for I is

$$60 = 1 + 12 + 12 + 15 + 20$$

If I had a proper normal subgroup H, then by normality H would need to be a disjoint union of conjugacy classes (so $|H| = 1+$ a proper subset of the numbers 12, 12, 15, 20), while by being a subgroup $|H|$ would have to divide 60. It is easy to see that this is numerically impossible, so I is a simple group. But then Proposition 34 implies that $I \cong A_5$.

Proof. of Proposition 34: Assume that G has a subgroup H of index $n \in \{2, 3, 4, 5\}$. The left action

$$G \curvearrowright \Big\{\text{left } H\text{-cosets}\Big\}$$

is transitive, so it induces a non-trivial homomorphism $f : G \to S_n$. Since G is simple, it has no proper normal subgroups, and therefore f must be injective. This is clearly impossible for $n \in \{2, 3, 4\}$ for cardinality reasons, while for $n = 5$ it implies that G is isomorphic to a subgroup of index 2 in S_n. However any subgroup of index 2 is normal, and the only normal subgroup of S_5 is A_5 (otherwise we would extend the normal subgroup in question to a composition series of S_5 which is non-equivalent to $1 \triangleleft A_5 \triangleleft S_5$, which would contradict the Jordan-Hölder Theorem 7).

We may therefore assume that all subgroups of G have index ≥ 6, i.e. have order ≤ 10. However, consider the number n_2 of Sylow 2-subgroups. By Sylow's third Theorem 10, this number divides

[1] Source of figure https://commons.wikimedia.org/w/index.php?curid=18278544

15 and is equal to the index of a subgroup of G, so the only option is $n_2 = 15$. We therefore have distinct Sylow 2-subgroups $P_1, \ldots, P_{15}$ of order 4 (hence abelian) so let us study their intersections.

- If $P_i \cap P_j \supsetneq \{e\}$ for some $i \neq j$, then choose an element $e \neq g \in P_i \cap P_j$. Since P_i and P_j are abelian, we have $P_i, P_j \leq C_G(g)$. However, the order of the subgroup $C_G(g)$ would have to be ≥ 6 (because it contains $P_i \cup P_j$ as a subset), a multiple of 4 (because it contains P_i as a subgroup), a divisor of 60 (because it is a subgroup of G) and ≤ 10 (by the assumption at the beginning of the paragraph above). This is clearly impossible for numerical reasons.

- If $P_i \cap P_j = \{e\}$ for all $i \neq j$, then $P_1 \cup \cdots \cup P_{15}$ contains $1 + 3 \times 15 = 46$ elements, all having order 1,2 and 4. However, by Sylow's third Theorem 10, the number n_5 is the index of a subgroup of G, and therefore $n_5 \geq 6$ by the assumption at the beginning of the paragraph above. We therefore have at least 6 Sylow 5-subgroups, all of which must be isomorphic to $\mathbb{Z}/5\mathbb{Z}$ and which cannot pairwise intersect except in the identity (indeed, show that in any group, different subgroups isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p'\mathbb{Z}$ for any prime numbers p, p' intersect only in the identity element). Therefore, G contains at least $4 \times 6 = 24$ elements of order 5, and since $46 + 24 > 60$, we counted more elements than the group G can admit.

□

Lecture 11

11.1

Formula (107) shows that any finite abelian group is a direct product of abelian p-groups. To make such a result hold in the non-abelian setting, we need to recall the nilpotent groups of Definition 25. With this in mind, the main result of this lecture is the following.

Theorem 11. *A finite group G is nilpotent if and only if it can be written as*

$$G \cong P_1 \times \cdots \times P_k \tag{137}$$

for distinct primes $p_1, \ldots, p_k$, where each P_i is a finite p_i-group.

Note that because each P_i is normal in the right-hand side of (137), we conclude that P_i would correspond to the unique Sylow p_i-subgroup of G. In fact, the proof of Theorem 11 shows that a finite group is nilpotent if and only if all of its Sylow subgroups are normal. Before we set up the proof of Theorem 11, we need to give an alternative characterization of nilpotent groups.

Proposition 35. *A group G is nilpotent if and only if it has a **central series***

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G \tag{138}$$

i.e. one in which every G_{i-1} is a normal subgroup of G (so not just of G_i), and every G_i/G_{i-1} is contained in the center of G/G_{i-1}.

Proof. The condition that $G_i/G_{i-1} \leq Z(G/G_{i-1})$ is equivalent to requiring

$$[G_i, G] \leq G_{i-1}$$

for all $i \in \{1, \ldots, k\}$. If G is nilpotent, once we remove all duplicates from the series (126), we will obtain the required series (138). Conversely, if we have a central series (138), it is straightforward, and left as an exercise to you to prove by induction on i that

$$G^{\{i\}} \leq G_{k-i}$$

Therefore we will have $G^{\{k\}} = 1$, which means that G is nilpotent.

□

11.2

The characterization of nilpotent groups in Proposition 35 is more robust that the original definition. In particular, it makes it quite straightforward to prove the following analogues of Propositions 24, 25 and 26.

Proposition 36. *Any subgroup of a nilpotent group is nilpotent.*

Proposition 37. *Any quotient of a nilpotent group is nilpotent.*

Proposition 38. *Suppose we have a short exact sequence of groups*

$$1 \to K \to G \xrightarrow{\pi} L \to 1$$

with $K \leq Z(G)$ and L nilpotent. Then G is nilpotent.

The proofs of Propositions 36 and 37 are very similar to the analogous results for solvable groups, so we will leave the details as an exercise to you. We will present the details behind the proof of Proposition 38 because of the extra assumption that $K \leq Z(G)$, which was not present in the case of solvable groups.

Proof. of Proposition 38: Consider a central series

$$1 = L_0 \lhd L_1 \lhd \cdots \lhd L_{k-1} \lhd L_k = L$$

in which every L_i/L_{i-1} is contained in the center of L/L_{i-1}. Then let us consider

$$G_{i+1} = \pi^{-1}(L_i)$$

for all $i \geq 0$. Note that $G_1 = K$. We claim that

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_k \lhd G_{k+1} = G$$

is the required central series of G. The fact that each G_{i+1} is normal in G follows by the correspondence theorem from the fact that each L_i is normal in L. Meanwhile, the property

$$[G_{i+1}, G] \leq G_i$$

follows immediately from $[L_i, L] \leq L_{i-1}$, for all $i \geq 1$ (please check this). Finally, the fact that

$$[G_1, G] = 1$$

follows from the fact that $G_1 = K$ is contained in the center of G.

□

11.3

Let us show that the direct product of nilpotent groups is nilpotent by using the original Definition 25. Indeed, we leave it to you to show by induction on i that

$$(G \times G')^{\{i\}} \cong G^{\{i\}} \times G'^{\{i\}}$$

The isomorphism above for large enough i shows that

$$\textbf{if } G \textbf{ and } G' \textbf{ are nilpotent, then } G \times G' \textbf{ is nilpotent} \tag{139}$$

Proposition 39. *For any prime number p, any finite p-group is nilpotent.*

Proof. We will argue by induction on the order of G. As shown in Lemma 15, $|Z(G)| > 1$. Therefore, Proposition 37 implies that $G/Z(G)$ is a p-group of strictly smaller order than G. By the induction hypothesis, $G/Z(G)$ is therefore nilpotent. However, G is (tautologically) an extension of this nilpotent subgroup by the center $Z(G)$, so Proposition 38 implies that G is nilpotent.

□

Since we already showed that the direct product of nilpotent groups is nilpotent, Proposition 39 establishes the fact that any group as in the right-hand side of (137) is nilpotent. Therefore, to complete the proof of Theorem 11, we must show that any finite nilpotent group breaks up as the direct product of its Sylow p-subgroups. This will be the subject of the subsequent subsections.

11.4

The last technical property of nilpotent groups concerns the behavior of normalizers of subgroups.

Proposition 40. *Any nilpotent group G has the **normalizer property**, i.e. for all proper subgroups $H < G$ we have*

$$H \subsetneq N_G(H) \tag{140}$$

In other words, "normalizers of subgroups strictly grow".

Proof. Let G be a nilpotent group, and consider any subgroup $H < G$. Consider the normal series (126), and any natural number i such that

$$G^{\{i\}} \subseteq H$$

(such an i exists because $G^{\{k\}} = 1$ for large enough k). However, we claim that

$$G^{\{i-1\}} \subseteq N_G(H)$$

because for any $g \in G^{\{i-1\}}$ and any $h \in H$ we have

$$ghg^{-1}h^{-1} \in G^{\{i\}} \subseteq H \quad \Rightarrow \quad ghg^{-1} \in H$$

So if H failed the normalizer property, i.e. if $H = N_G(H)$, then the argument above would recursively imply that $G = G^{\{0\}} \subseteq H$, which contradicts the fact that H is a proper subgroup.

□

11.5

For finite groups, the converse of Proposition 40 also holds. Indeed, all that we will use in the subsequent proof of Theorem 11 is that if a finite group G satisfies the normalizer property (140) for all proper subgroups $H < G$, then G is the direct product of its Sylow subgroups (and hence nilpotent by (139) and Proposition 39).

Proof. of Theorem 11: The "if" implication follows from (139) and Proposition 39. To prove the "only if" implication, take a finite nilpotent group G and let $p_1, \ldots, p_k$ be the distinct prime divisors of $|G|$. Let

$$P_1, \ldots, P_k$$

denote Sylow subgroups of G corresponding to the primes $p_1, \ldots, p_k$. For each $i \in \{1, \ldots, k\}$, let

$$H_i = N_G(P_i) \tag{141}$$

If $H_i = G$ for all i, then each P_i is normal, and thus the unique Sylow p_i-subgroup by Theorem 9. If this holds, then we claim that the function

$$P_1 \times \cdots \times P_k \xrightarrow{\tau} G, \qquad (g_1, \ldots, g_k) \mapsto g_1 \ldots g_k$$

is an isomorphism. This follows from the points below

- *τ is a homomorphism:* for all $i \neq j$, any $g_i \in P_i$ commutes with any $g_j \in P_j$. To this end, note that the normality of P_i and P_j implies that the commutator $g_i g_j g_i^{-1} g_j^{-1}$ lies in both P_i and P_j. However, any element in the intersection $P_i \cap P_j$ would need to have order dividing both a power of p_i and a power of p_j, so the order would have to be 1.

- *τ is injective:* if $g_1 \ldots g_k = g_1' \ldots g_k'$ for various $g_i, g_i' \in P_i$, then the previous bullet implies that

$$(g_1' g_1^{-1}) \ldots (g_k' g_k^{-1}) = e \quad \Rightarrow \quad \underbrace{(g_1' g_1^{-1}) \ldots (g_{k-1}' g_{k-1}^{-1})}_{x} = \underbrace{(g_k' g_k^{-1})^{-1}}_{y}$$

  The order of the element denoted by x above divides a power of $p_1 \ldots p_{k-1}$, while the order of the element denoted by y divides a power of p_k. Since $x = y$, the only possibility is that these elements are the identity, so $g_k' = g_k$. Analogously, one proves that $g_{k-1}' = g_{k-1}, \ldots, g_1' = g_1$.

- *The domain and target of τ have the same order:* this is because the order of a Sylow p-subgroup is, by definition, the maximal power of p which divides the order of the group.

Having proved the Theorem under the hypothesis that the subgroups H_i of (141) are all equal to G, let us now assume for the purpose of contradiction that one of these H_i's is a proper subgroup of G. If indeed $H_i < G$ for some $i \in \{1, \ldots, k\}$, then the normalizer property (140) implies that there exists $g \in N_G(H_i) - H_i$. Then we have

$$g P_i g^{-1} \subseteq g H_i g^{-1} = H_i$$

so we conclude that both P_i and $g P_i g^{-1}$ are Sylow p_i-subgroup of H_i. By Sylow's second Theorem 9, there must exist some $h \in H_i$ such that

$$g P_i g^{-1} = h P_i h^{-1} \quad \Rightarrow \quad (h^{-1} g) P_i = P_i (h^{-1} g)$$

which implies that $h^{-1} g \in H_i$. This contradicts the fact that $g \in N_G(H_i) - H_i$.

□

Lecture 12

12.1

We will now develop what is in a sense one of the most general (and fundamental) class of groups out there. Fix a set S, and define a **word** in S to be any sequence

$$s_1^{\pm 1} s_2^{\pm 1} \dots s_k^{\pm 1} \tag{142}$$

for various $s_1, \dots, s_k \in S$, where we write $s^{+1} = s$ and think of s^{-1} as a formal symbol, for any $s \in S$. A word is called **reduced** if it does not contain the length 2 sequences ss^{-1} or $s^{-1}s$, $\forall s \in S$.

Definition 26. *The **free group** F_S on S is the set of reduced words, made into a group with*

- *identity given by the empty word*
- *the inverse of (142) given by $s_k^{\mp 1} \dots s_2^{\mp 1} s_1^{\mp 1}$.*
- *the product of two words given by concatenation, followed by removing all sequences ss^{-1} and $s^{-1}s$ (for various $s \in S$) in order to make the result into a reduced word.*

We leave it to you to show that the group axioms in F_S are satisfied. Any function $f : S \to S'$ induces a homomorphism (which we will abusively also call) $f : F_S \to F_{S'}$, defined by the formula

$$s_1^{\pm 1} \dots s_k^{\pm 1} \rightsquigarrow f(s_1)^{\pm 1} \dots f(s_k)^{\pm 1}$$

for all words (142).

Lemma 16. *For any set S and any group G, there exists a one-to-one correspondence*

$$\Psi_{S,G} : \Big\{ \textit{functions } S \to G \Big\} \leftrightarrow \Big\{ \textit{homomorphisms } F_S \to G \Big\} \tag{143}$$

*which is **functorial** in the sense that the square*

$$\begin{array}{ccc} \Big\{ \textit{functions } S \to G \Big\} & \xrightarrow{\Psi_{S,G}} & \Big\{ \textit{homomorphisms } F_S \to G \Big\} \\ \downarrow & & \downarrow \\ \Big\{ \textit{functions } S' \to G' \Big\} & \xrightarrow{\Psi_{S',G'}} & \Big\{ \textit{homomorphisms } F_{S'} \to G' \Big\} \end{array} \tag{144}$$

commutes for all functions $f : S' \to S$ and all homomorphisms $g : G \to G'$ (the vertical maps are given by composition with f and g, as appropriate).

Proof. The content of (143) is simply that any function $\alpha : S \to G$ can be uniquely extended to a homomorphism $\beta : F_S \to G$. However, this is simply a consequence of the fact that the axioms of a homomorphism force us to set

$$\beta\left(s_1^{\pm 1} \dots s_k^{\pm 1}\right) = \alpha(s_1)^{\pm 1} \dots \alpha(s_k)^{\pm 1}$$

for all words (142). Functoriality is really easy to see, so please think about it.

□

12.2

We have $F_\emptyset = 1$ and $F_{\{x\}} = \{x^n | n \in \mathbb{Z}\} \cong \mathbb{Z}$. However, as soon as the set S has at least two elements, the free group F_S is a quite big and complicated group. Moreover, the following result shows that different sets S yield non-isomorphic free groups F_S, so this construction is quite rich.

Theorem 12. *There exists an isomorphism $F_S \overset{\cong}{\leftrightarrow} F_T$ if and only if there exists a bijection $S \leftrightarrow T$.*

Before we prove the Theorem above, let us introduce a closely related notion to that of free groups. Recall the derived subgroup (124). For any set S, the group

$$\boxed{F_S^{\mathrm{ab}} = F_S \Big/ [F_S, F_S]}$$

is called the **free abelian group** on S.

Proposition 41. *For any set S, we have an isomorphism*

$$F_S^{\mathrm{ab}} \cong \mathbb{Z}^S = \bigoplus_{s \in S} \mathbb{Z} \cdot s$$

In particular, if $|S| = r$, then $F_S^{\mathrm{ab}} \cong \mathbb{Z}^r$.

Proof. Consider the functions

$$\mathbb{Z}^S \to F_S^{\mathrm{ab}}, \qquad \sum_{s \in S} n_s \cdot s \mapsto \prod_{s \in S} s^{n_s} \tag{145}$$

for all collections $\{n_s \in \mathbb{Z}\}_{s \in S}$, such that all but finitely many of the n_s are zero (the fact that F_S^{ab} is abelian means that it does not matter in which order we take the product in the right-hand side of (145)) and

$$F_S^{\mathrm{ab}} \to \mathbb{Z}^S, \qquad \text{word (142)} \mapsto \sum_{i=1}^{k} \pm s_i \tag{146}$$

It is easy to see that these functions are mutually inverse. The fact that they are homomorphisms is a straightforward consequence (which we leave as an exercise to you) of the fact that in F_S^{ab} the word (142) is equal to any of its permutations. Thus, the freedom to arbitrarily move symbols around implies the formula

$$\ldots s^m \ldots s^n \cdots = \ldots s^{m+n} \ldots$$

in F_S^{ab}, no mater what words one places instead of the "...". □

12.3

We are now ready to prove Theorem 12. The proof that we are about to give below will also establish the following closely related claim

there exists an isomorphism $F_S^{\mathrm{ab}} \overset{\cong}{\leftrightarrow} F_T^{\mathrm{ab}}$ if and only if there exists a bijection $S \leftrightarrow T$

Proof. of Theorem 12: The "if" statement is obvious, so let us prove the "only if" statement. Assume that we have an isomorphism $F_S \cong F_T$. Then it naturally descends to an isomorphism of the corresponding quotients

$$\mathbb{Z}^S \cong F_S/[F_S, F_S] \cong F_T/[F_T, F_T] \cong \mathbb{Z}^T$$

However, the isomorphism above sends multiples of 2 (i.e. formal sums $\sum_{s\in S} n_s \cdot s$ with all the n_s being even) to multiples of 2. Since the subsets of multiples of 2 in either $\mathbb{Z}^S$ and $\mathbb{Z}^T$ are subgroups, which you can easily prove, we can quotient by them and obtain an isomorphism

$$(\mathbb{Z}/2\mathbb{Z})^S \cong (\mathbb{Z}/2\mathbb{Z})^T \tag{147}$$

The group $(\mathbb{Z}/2\mathbb{Z})^S$ consists of formal sums $\sum_{s\in S} n_s \cdot s$ where finitely many of the n_s can be equal to 1 mod 2, but all the others are equal to 0 mod 2. Such formal sums are in one-to-one correspondence with finite subsets of S (explicitly, to a formal sum $\sum_{s\in S} n_s \cdot s$ we associate the subset of those $s \in S$ for which $n_s = 1 \bmod 2$). Therefore, the isomorphism (147) gives a bijection

$$\Big\{\text{finite subsets of } S\Big\} \leftrightarrow \Big\{\text{finite subsets of } T\Big\} \tag{148}$$

- If S and T have finite cardinality m and n (respectively) then the set of finite subsets of S and T has cardinality 2^m and 2^n (respectively). The equality $2^m = 2^n$ implies $m = n$, hence there exists a bijection between S and T.

- If one of S and T is finite and the other is infinite, then (148) cannot hold.

- If both S and T are infinite, then we invoke the fact that any infinite set is in bijection to its set of finite subsets (proving this is not too hard, but it goes beyond the scope of our course). Therefore, the bijection (148) implies that there exists a bijection between S and T.

□

12.4

If G is a group and $X \subseteq G$ is a subset, then you learned in Math 113 that

$$K = \Big\{\text{products of } x^{\pm 1} \Big| x \in X\Big\} \tag{149}$$

is a subgroup of G, and that

$$H = \Big\{\text{products of } gx^{\pm 1}g^{-1} \Big| g \in G, x \in X\Big\} \tag{150}$$

is a normal subgroup of G. We will write G/X instead of G/H.

Definition 27. *Consider now a set R of words* (142)*. The quotient group (defined as above)*

$$\boxed{\langle S|R\rangle := F_S \Big/ R} \tag{151}$$

is called the group with ***generators*** *S and* ***relations*** *R.*

For a group G, to find a generators-and-relations presentation of G means to find an isomorphism

$$G \cong \langle S|R\rangle$$

for some sets S and R. If the set S is finite, then G is called **finitely generated**. If both S and R are finite, then G is called **finitely presented**.

Example 4. *For any set S, we have*

$$F_S^{\text{ab}} \cong \langle S|aba^{-1}b^{-1}, \forall a, b \in S\rangle$$

12.5

Finite cyclic groups admit the presentation

$$\mathbb{Z}/n\mathbb{Z} \cong \langle x|x^n\rangle$$

Dihedral groups admit the presentation

$$D_{2n} \cong \langle \sigma, \tau|\sigma^n, \tau^2, (\sigma\tau)^2\rangle$$

where σ is a rotation and τ is a reflection. Finally, symmetric groups admit the presentation

$$S_n \cong \langle \sigma_1, \ldots, \sigma_{n-1}|\sigma_i^2, (\sigma_i\sigma_j)^2, (\sigma_i\sigma_{i+1})^3\rangle$$

where i goes over all indices, and j goes over all indices other than $i-1, i, i+1$. The fact that these three groups admit generators-and-relations presentations is no coincidence, as the following result shows.

Proposition 42. *Any group G admits a generators-and-relations presentation.*

Proof. Taking $S = G$ and the identity in the left-hand side of (143) gives us a homomorphism

$$\pi : F_G \to G$$

Because any element of G is the image of the same-named generator, the homomorphism above is surjective. Then we let H be the kernel of π, and the first isomorphism theorem implies that $G \cong F_G/H$. It therefore remains to pick $X = H$ in (149) and (150), and with these choices we have

$$\langle G|H\rangle \cong G$$

□

The proof of Proposition 42 is very non-economical: we took every element of G to be a generator! More useful generators-and-relations presentations of a group have relatively few generators, and a "nice" set of a relations. Moreover, the same group often admits many different generators-and-relations presentations, and it is in general difficult to decide if $\langle S|R\rangle$ is isomorphic to $\langle S'|R'\rangle$.

12.6

For those of you who like more abstract mathematics, there exists an abstract definition of the group $\langle S|R\rangle$. The following is a generalization of Lemma 16.

Lemma 17. *For any set S, any set R of words* (142) *and any group G, there exists a one-to-one correspondence*

$$\Psi_{S|R,G} : \Big\{\textit{functions } S \xrightarrow{\alpha} G \textit{ s.t. } \alpha(r) = e, \forall r \in R\Big\} \leftrightarrow \Big\{\textit{homomorphisms } \langle S|R\rangle \to G\Big\} \tag{152}$$

(we write $\alpha(s_1^{\pm 1} \dots s_k^{\pm 1}) = \alpha(s_1)^{\pm 1} \dots \alpha(s_k)^{\pm 1}$) which is ***functorial*** *in the sense that the square*

$$\begin{array}{ccc} \Big\{\textit{functions } S \xrightarrow{\alpha} G \textit{ s.t. } \alpha(r) = e, \forall r \in R\Big\} & \xrightarrow{\Psi_{S,R|G}} & \Big\{\textit{homomorphisms } \langle S|R\rangle \to G\Big\} \\ \downarrow & & \downarrow \\ \Big\{\textit{functions } S' \xrightarrow{\alpha} G' \textit{ s.t. } \alpha(r) = e, \forall r \in R'\Big\} & \xrightarrow{\Psi_{S',R'|G'}} & \Big\{\textit{homomorphisms } \langle S'|R'\rangle \to G'\Big\} \end{array} \tag{153}$$

commutes for all functions $f : S' \to S$ which take any word in R' to a concatenation of words in R, and all homomorphisms $g : G \to G'$ (the vertical maps are given by composition with f and g).

Lemma 17 is proved just like Lemma 16, so we leave the details as an exercise to you. However, we will explain the sense in which it provides an abstract definition of the group $\langle S|R\rangle$, which in mathematics is called a **universal property**. For fixed S and R, assume that there exists a group $\langle S|R\rangle$ such that we have a functorial one-to-one correspondence (152), even though we do not need to know the fact that it is constructed as in (151). Then this correspondence uniquely determines $\langle S|R\rangle$ up to isomorphism. To see this, assume that there existed two groups $\langle S|R\rangle$ and $\langle S|R\rangle'$ such that we have functorial one-to-one correspondences

$$\Big\{\text{functions } S \xrightarrow{\alpha} G \text{ s.t. } \alpha(r) = e, \forall r \in R\Big\} \leftrightarrow \Big\{\text{homomorphisms } \langle S|R\rangle \to G\Big\}$$
$$\Big\{\text{functions } S \xrightarrow{\alpha} G \text{ s.t. } \alpha(r) = e, \forall r \in R\Big\} \leftrightarrow \Big\{\text{homomorphisms } \langle S|R\rangle' \to G\Big\}$$

By composing the bijections above, we obtain a one-to-one correspondence

$$\Upsilon_G : \Big\{\text{homomorphisms } \langle S|R\rangle \to G\Big\} \leftrightarrow \Big\{\text{homomorphisms } \langle S|R\rangle' \to G\Big\} \tag{154}$$

for any group G, which is functorial in the sense that the following diagram commutes

$$\begin{array}{ccc} \Big\{\text{homomorphisms } \langle S|R\rangle \to G\Big\} & \xrightarrow{\Upsilon_G} & \Big\{\text{homomorphisms } \langle S|R\rangle' \to G\Big\} \\ \downarrow & & \downarrow \\ \Big\{\text{homomorphisms } \langle S|R\rangle \to G'\Big\} & \xrightarrow{\Upsilon_{G'}} & \Big\{\text{homomorphisms } \langle S|R\rangle' \to G'\Big\} \end{array} \tag{155}$$

for all homomorphisms $g : G \to G'$ (the vertical arrows are given by composition with g). If we take $G = \langle S|R\rangle$ in (154), then the identity in the left-hand side yields a homomorphism

$$\langle S|R\rangle' \xrightarrow{\beta'} \langle S|R\rangle$$

in the right-hand side, while if we take $G = \langle S|R\rangle'$ in (154), then the identity in the right-hand side yields a homomorphism

$$\langle S|R\rangle \xrightarrow{\beta} \langle S|R\rangle'$$

in the left-hand side. If we consider the vertical maps in (155) to be composition with $G = \langle S|R\rangle \xrightarrow{\beta} \langle S|R\rangle' = G'$, the commutativity of the square applied to the identity function $\langle S|R\rangle \to \langle S|R\rangle$ in the top left corner implies the formula $\beta \circ \beta' = \mathrm{Id}$ in the bottom right corner.

Similarly, if we consider the vertical maps in (155) to be composition with $G = \langle S|R\rangle' \xrightarrow{\beta'} \langle S|R\rangle = G'$, the commutativity of the square applied to the identity function $\langle S|R\rangle' \to \langle S|R\rangle'$ in the top right corner implies the formula $\beta' \circ \beta = \mathrm{Id}$ in the bottom left corner. We have thus shown that β and β' provide mutually inverse functions $\langle S|R\rangle \leftrightarrow \langle S|R\rangle'$, hence $\langle S|R\rangle \cong \langle S|R\rangle'$.

Lecture 13

13.1

When we say that a group G acts on a set X, we mean that to every $g \in G$ we associate a function $\Phi_g : X \to X$ with various properties. When X has additional structure, we typically require the functions Φ_g to respect this additional structure: for example, in Definition 13, we saw that if X is a group, then we typically require the functions Φ_g to be themselves homomorphisms. The starting point of **representation theory** is to deal with the case when X is a vector space and the functions Φ_g are linear transformations over some henceforth fixed field $\mathbb{F}$.

Definition 28. *Let V be a $\mathbb{F}$-vector space. A* ***representation***

$$\boxed{G \curvearrowright V}$$

is an assignment

$$\forall g \in G \quad \rightsquigarrow \quad \textit{a linear transformation } \Phi_g : V \to V \tag{156}$$

which satisfies properties (18), (19) *and* (20).

Recall from your previous linear algebra courses that linear transformations are those functions $\Phi : V \to V$ which respect the addition and scalar multiplication in V:

$$\Phi(v + v') = \Phi(v) + \Phi(v') \quad \text{and} \quad \Phi(cv) = c\Phi(v)$$

for any $v, v' \in V$ and $c \in \mathbb{F}$. An example of a representation is

$$D_{2n} \curvearrowright \mathbb{R}^2$$

by the usual rotations and reflections, which are indeed linear transformations of $\mathbb{R}^2$.

13.2

You probably recall from your previous linear algebra courses that by choosing a basis, any finite-dimensional vector space can be made isomorphic to

$$\mathbb{F}^n = \left\{ \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \text{ for various } v_1, \ldots, v_n \in \mathbb{F} \right\} \tag{157}$$

Any linear transformation $\Phi : \mathbb{F}^n \to \mathbb{F}^n$ can be written uniquely as

$$\Phi(v) = Av$$

for some $n \times n$ matrix $A = (a_{ij})_{1 \leq i,j \leq n}$, where v represents a $n \times 1$ column vector as in (157). In this case, a representation

$$G \curvearrowright \mathbb{F}^n$$

boils down to an assignment

$$\forall g \in G \quad \rightsquigarrow \quad \text{a } n \times n \text{ matrix } A_g$$

such that:

- A_e is the $n \times n$ identity matrix
- $A_{g^{-1}} = A_g^{-1}$, for all $g \in G$
- $A_{gg'} = A_g A_{g'}$, for all $g, g' \in G$

With this in mind, it becomes clear that representation theory is the study of $n \times n$ matrices, and how their products replicate various group structures. In the abstract language of group theory, a representation $G \curvearrowright \mathbb{F}^n$ is the same as a homomorphism

$$G \to GL(n, \mathbb{F})$$

where in the right-hand side we have the **general linear group** consisting of invertible $n \times n$ matrices with coefficients in $\mathbb{F}$, with the product given by matrix multiplication.

13.3

The following notions should by now seem natural and predictable.

Definition 29. *Given representations $G \curvearrowright V$ and $G \curvearrowright W$ (determined by collections $\{\Phi_g : V \to V\}_{g \in G}$ and $\{\Psi_g : W \to W\}_{g \in G}$, respectively) a G-**intertwiner** is a linear transformation*

$$f : V \longrightarrow W$$

such that the following diagram commutes

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle \Phi_g}\downarrow & & \downarrow{\scriptstyle \Psi_g} \\ V & \xrightarrow{f} & W \end{array}$$

for all $g \in G$. If we write $\Phi_g(v) = g \cdot v$ and $\Psi_g(w) = g \cdot w$ for all $v \in V$ and $w \in W$, then the property of being a G-intertwiner is equivalent to

$$f(g \cdot v) = g \cdot f(v)$$

*for all $v \in V$ and all $g \in G$. If a G-intertwiner is moreover bijective, then we call it an **isomorphism** (of representations of G) and indicate this as*

$$\boxed{V \cong W}$$

Recall that a subset of a vector space is called a subspace if and only if it is preserved under addition of vectors and scalar multiplication. If we have a representation $G \curvearrowright V$, then a subspace $W \subseteq V$ is called a **subrepresentation** if

$$\Phi_g(W) \subseteq W$$

for all $g \in G$. Moreover, in this case there is an induced **quotient representation**

$$\boxed{G \curvearrowright V/W}$$

13.4

One of the most fundamental notions in representation theory is the following.

Definition 30. *A representation $G \curvearrowright V$ is called **irreducible** if it doesn't have any proper subrepresentations (i.e. no subrepresentations other than 0 or V).*

One of the main tools in representation theory is the following result, known as **Schur's lemma**.

Lemma 18. *Suppose we have a G-intertwiner $f : V \to W$ between two representations of G, which is not identically 0. If V is irreducible, then f is injective. If W is irreducible, then f is surjective.*

Proof. The Lemma is a quick consequence of the straightforward fact (whose proof we leave to you) that for any G-intertwiner $f : V \to W$, the kernel $f^{-1}(0)$ is a subrepresentation of V and the image of f is a subrepresentation of W. But if V is irreducible, this means that the kernel is either 0 (which implies that f is injective) or the kernel is the whole of V (which implies that f is identically 0). Similarly, if W is irreducible, then the image is either 0 (which implies that f is identically 0) or that the image is the whole of W (which implies that f is surjective).

□

As an immediate corollary of Lemma 18, any non-zero intertwiner between two irreducible representations must be an isomorphism.

13.5

We will henceforth specialize to $\mathbb{F} = \mathbb{C}$, i.e. consider representations which are vector spaces over the field of complex numbers. In this case, we can upgrade Lemma 18 to the following result.

Proposition 43. *For any irreducible representation $G \curvearrowright \mathbb{C}^n$, the only intertwiners*

$$f : \mathbb{C}^n \to \mathbb{C}^n$$

(the G actions in the domain and codomain of f are the same) are scalar multiples of the identity.

Proof. Since we are working over the complex numbers, any linear transformation $f : \mathbb{C}^n \to \mathbb{C}^n$ has an eigenvector, i.e. there exists some $0 \neq v \in \mathbb{C}^n$ and some $c \in \mathbb{C}$ such that

$$f(v) = cv$$

Then the function $f - c \cdot \mathrm{Id}$ is still an intertwiner (check this) but it cannot be injective anymore since it has v in its kernel. Then Schur's Lemma 18 implies that $f - c \cdot \mathrm{Id}$ is identically 0.

□

Since any n-dimensional representation V over the field of complex numbers is isomorphic to $\mathbb{C}^n$ (simply by choosing a basis of V) then Proposition 43 also applies to intertwiners $f : V \to V$. In particular, this shows that if two finite-dimensional representations of G over the complex numbers are isomorphic, then the isomorphism between them is unique up to scalar multiple. Indeed, if we have any two isomorphisms

$$f_1 : V \to W \quad \text{and} \quad f_2 : V \to W$$

then $f_1^{-1} \circ f_2$ is an isomorphism $V \to V$. Therefore, Proposition 43 implies that there exists $c \in \mathbb{C}$ such that $f_1^{-1} \circ f_2 = c \cdot \mathrm{Id}$, which in turn implies $f_2 = c \cdot f_1$.

13.6

If we have two representations $G \curvearrowright V$ and $G \curvearrowright W$, we can form the direct sum

$$V \oplus W = \Big\{ (v, w) \Big| v \in V, w \in W \Big\}$$

and make it into a representation of G via $g \cdot (v, w) = (g \cdot v, g \cdot w)$. In the language of Subsection 13.2, the matrices A_g that describe the representation $V \oplus W$ are block diagonal, with diagonal blocks given by the matrices that describe the representations V and W, respectively. If you will take Math 314, then you will learn the following very important result, known as **Maschke's theorem**.

Theorem 13. *Any finite dimensional representation of a finite group G over the field of complex numbers is isomorphic to a direct sum of irreducible representations.*

Let us illustrate Theorem 13 with the permutation representation $\mathbb{Z}/2\mathbb{Z} \curvearrowright \mathbb{C}^2$, which is given in matrix form by

$$0 \bmod 2 \mapsto A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad 1 \bmod 2 \mapsto A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The two coordinate subspaces of $\mathbb{C}^2$ are not subrepresentations, because they are not preserved by the matrix A_1. However, the two one-dimensional subspaces

$$V_1 = \Big\{ (c, c) \Big| c \in \mathbb{C} \Big\} \quad \text{and} \quad V_2 = \Big\{ (c, -c) \Big| c \in \mathbb{C} \Big\}$$

are subrepresentations. Because they are one-dimensional, they do not have any proper subspaces, so they are automatically irreducible. Therefore, Maschke's theorem in this case states that

$$\mathbb{C}^2 \cong V_1 \oplus V_2$$

is the decomposition of the representation $\mathbb{Z}/2\mathbb{Z} \curvearrowright \mathbb{C}^2$ into irreducible representations.

13.7

As a consequence of Theorem 13, any finite dimensional representation $G \curvearrowright V$ over the field of complex numbers can be written as

$$V \cong V_1^{\oplus n_1} \oplus \cdots \oplus V_k^{\oplus n_k} \tag{158}$$

where $V_1, \ldots, V_k$ are non-isomorphic irreducible representations of G, and $n_1, \ldots, n_k$ are some non-negative integers known as **multiplicities**. We claim that the multiplicities are actually completely determined by the representation V. To see this, consider any G-intertwiner

$$f : V_1^{\oplus n_1} \oplus \cdots \oplus V_k^{\oplus n_k} \longrightarrow V_1^{\oplus n_1'} \oplus \cdots \oplus V_k^{\oplus n_k'}$$

for various $n_1, \ldots, n_k, n_1', \ldots, n_k' \geq 0$, and let us ask when such an f can be an isomorphism. Lemma 18 and Proposition 43 imply that the G-intertwiner acts block diagonally, i.e.

$$f(\ldots, v_{i1}, \ldots, v_{in_i}, \ldots) = (\ldots, v_{i1}', \ldots, v_{in_i'}', \ldots)$$

(above, v_{ia} and v'_{ia} denote general vectors in the a-th direct summand of V_i and V'_i, respectively) where for all $i \in \{1, \ldots, k\}$ and $b \in \{1, \ldots, n'_i\}$, we have

$$v'_{ib} = \sum_{a=1}^{n_i} \gamma_{ab}^{(i)} v_{ia}$$

for some complex numbers $\gamma_{ab}^{(i)}$. It is then not hard to believe that such a G-intertwiner f can be an isomorphism only if $n_i = n'_i$ for all $i \in \{1, \ldots, k\}$ (this is a slightly fancier version of the statement that a $n' \times n$ matrix can be invertible only if $n = n'$), which implies that the numbers $n_1, \ldots, n_k$ in (158) are completely determined by V. In Math 314, you will learn how to use character theory in order to effectively compute these multiplicities for all finite dimensional representation of a finite group.

Lecture 14

14.1

Category theory provides a unifying language for many of the objects we discussed this semester. We will now give a brief introduction to the basics of this language.

Definition 31. *A (small)* ***category*** $\mathcal{C}$ *consists of the following data*

- *a set* $\mathrm{Ob}(\mathcal{C})$ *called the* ***objects****, and*
- *for any* $X, Y \in \mathrm{Ob}(\mathcal{C})$ *a set* $\mathrm{Mor}_{\mathcal{C}}(X, Y)$ *called the* ***morphisms****, together with*
- *an operation called* ***composition***

$$\mathrm{Mor}_{\mathcal{C}}(Y, Z) \times \mathrm{Mor}_{\mathcal{C}}(X, Y) \to \mathrm{Mor}_{\mathcal{C}}(X, Z), \qquad (f, g) \mapsto f \circ g$$

for all $X, Y, Z \in \mathrm{Ob}(\mathcal{C})$.

One typically writes $f : X \to Y$ *instead of* $f \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$. *The composition of morphisms is required to satisfy two axioms: firstly, there should exist an* ***identity*** *morphism*

$$\boxed{\mathrm{Id}_X : X \to X}$$

for all $X \in \mathrm{Ob}(\mathcal{C})$*, such that*

$$\mathrm{Id}_Y \circ f = f \circ \mathrm{Id}_X = f, \quad \forall f : X \to Y$$

Secondly, composition of morphisms should be associative, in the sense that

$$f \circ (g \circ h) = (f \circ g) \circ h$$

for any $h : X \to Y$, $g : Y \to Z$, $f : Z \to T$.

14.2

One typically draws a category $\mathcal{C}$ as a directed graph: the vertices are the elements of $\mathrm{Ob}(\mathcal{C})$ and the arrows from vertex X to vertex Y are in one-to-one correspondence with the elements of the set $\mathrm{Mor}_{\mathcal{C}}(X, Y)$. Note that there may be infinitely many vertices and arrows! Examples of categories include:

- Set: objects are sets and morphisms are functions (note that this is not a small category, so one has to slightly change the words "set" in the bullets of Definition 31)
- Gr: objects are groups and morphisms are homomorphisms (same comment about "set" as above)
- Rep_G: objects are representations of a fixed group G and morphisms are G-intertwiners

There is a notion of inverse morphisms in a category $\mathcal{C}$: we call $f : X \to Y$ and $g : Y \to X$ inverses of each other (and write this as $g = f^{-1}$) if

$$g \circ f = \mathrm{Id}_X \qquad \text{and} \qquad f \circ g = \mathrm{Id}_Y$$

The invertible morphisms in the examples of categories in the three bullets above are the bijections, the isomorphisms (of groups) and the isomorphisms of G-representations, respectively.

Proposition 44. *There is a one-to-one correspondence between groups on one hand, and categories with a single object where every morphism is invertible on the other hand.*

Proof. The Proposition is almost obvious: if $\bullet$ is the single object of the category in question, then $G = \mathrm{Mor}(\bullet, \bullet)$ has an identity element and an associative operation, and the assumption that every element of G has an inverse precisely completes the group axioms.

□

14.3

The following notion is key to category theory.

Definition 32. *A functor $F : \mathcal{C} \to \mathcal{D}$ between categories consists of*

- *a function $F : \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$*
- *an assignment*

$$f : X \to Y \qquad \rightsquigarrow \qquad F(f) : F(X) \to F(Y)$$

for all $X, Y \in \mathrm{Ob}(\mathcal{C})$, which sends identity to identity and respects composition of morphisms.

If we let $\bullet_G$ denote the category that corresponds to a group G in Proposition 44, then to give a functor $\bullet_G \to \bullet_{G'}$ is the same thing as to give a group homomorphism $G \to G'$.

Another example of a functor between categories is

$$\mathrm{Gr} \xrightarrow{\text{for}} \mathrm{Set}$$

which takes a group to the underlying set, and a homomorphism ϕ between groups to ϕ interpreted as a function between the underlying sets. It is called the **forgetful functor**.

Example 5. *The free group construction in Subsection 12.1 gives a functor*

$$\mathrm{Set} \xrightarrow{\text{free}} \mathrm{Gr}$$

It sends a set S to the group F_S, and a function $s : S \to T$ to the group homomorphism $F_S \to F_T$ induced by sending the generators $s^{\pm 1}$ of the group F_S to the generators $f(s)^{\pm 1}$ of the group F_T.

Definition 33. *Functors $F : \mathcal{D} \to \mathcal{C}$ and $G : \mathcal{C} \to \mathcal{D}$ are called **adjoint**, if there exist bijections*

$$\Psi_{X,Y} : \mathrm{Mor}_{\mathcal{C}}(F(X), Y) \leftrightarrow \mathrm{Mor}_{\mathcal{D}}(X, G(Y))$$

for any $X \in \mathrm{Ob}(\mathcal{D})$ and $Y \in \mathrm{Ob}(\mathcal{C})$. These bijections are required to be natural, in the sense that

$$\begin{array}{ccc} \mathrm{Mor}_{\mathcal{C}}(F(X), Y) & \xrightarrow{\Psi_{X,Y}} & \mathrm{Mor}_{\mathcal{D}}(X, G(Y)) \\ {\scriptstyle g\circ - \circ F(f)}\downarrow & & \downarrow{\scriptstyle G(g)\circ - \circ f} \\ \mathrm{Mor}_{\mathcal{C}}(F(X'), Y') & \xrightarrow{\Psi_{X',Y'}} & \mathrm{Mor}_{\mathcal{D}}(X', G(Y')) \end{array}$$

must commute for all morphisms $f : X' \to X$ in $\mathcal{D}$ and $g : Y \to Y'$ in $\mathcal{C}$.

Lemma 16 is precisely the statement that ($F =$ free) and ($G =$ for) yield a pair of adjoint functors.

14.4

Definition 34. *If $f : X \to Y$ and $f' : X \to Y'$ are morphisms in a category $\mathcal{C}$, then we say that their **pushout** is an object Z equipped with morphisms*

$$g : Y \to Z \quad \textit{and} \quad g' : Y' \to Z$$

*such that $g \circ f = g' \circ f'$, with the following **universal property**. For any object A and morphisms*

$$h : Y \to A \quad \textit{and} \quad h' : Y' \to A$$

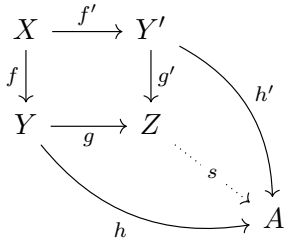
such that $h \circ f = h' \circ f'$, there exists a unique morphism

$$s : Z \to A$$

such that

$$h = s \circ g \qquad \textit{and} \qquad h' = s \circ g'$$

More visually, the condition above states that there exists a unique dotted arrow such that all squares and triangles in the diagram below commute



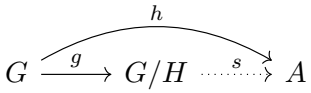
(159)

When a pushout exists, it is unique up to isomorphism (please prove this). We will now provide two examples that we have already encountered in our course.

Example 6. *In the category* Gr*, let $f : H \hookrightarrow G$ be the inclusion of a normal subgroup $H \trianglelefteq G$ and $f' : H \to 1$ to be the trivial homomorphism. In this case, pushout is none other than the quotient group $g : G \to G/H$. The universal property in this case can be summarized in words as*

$$\begin{aligned} &\textit{whenever we have a group homomorphism } h : G \to A \textit{ such that } h(H) = 1, \\ &\qquad\qquad \textit{there exists a unique homomorphism } s : G/H \to A \textit{ such that } h = s \circ g \end{aligned} \tag{160}$$

or more visually, that there exists a unique dotted arrow which makes the diagram below commute



If H is not normal in G, then the pushout is G/N, where N is the smallest normal subgroup of G that contains H (also known as the ***normal closure*** *of H). So the pushout construction does not distinguish between all subgroups (and in more general categories, pushouts might not even exist).*

Example 7. *In the category* Set*, any equivalence relation can be presented as a pushout. Specifically, if we let $R \subseteq X \times X$ denote the set of pairs (x, x') such that $x \sim x'$, then we claim that the pushout of the functions $f : R \to X,\ f(x, x') = x$ and $f' : R \to X,\ f'(x, x') = x'$ is the set of equivalence classes $Z = X/\sim$. Indeed, for any set A as in diagram* (159) *together with functions*

$$g : X \to A \quad \textit{and} \quad g' : X \to A$$

such that $g(x) = g'(x')$ whenever $x \sim x'$, then first of all we need to have $g = g'$ by reflexivity, and second of all we can define

$$s : X/\sim \to A$$

by setting $s([x]) = g(x)$. Since $g(x) = g(x')$ whenever $x \sim x'$, this definition is unambiguous.