Notes on
MATH 493
(Honors Algebra)

January 7, 2022

Faye Jackson

Contents

I. Introduction

Here is the basic information about the course.

Book) Artin's Algebra, 2nd Edition

Office Hours/Homework Dates

II. Group Theory

II.1. Basic Definitions

What are we studying in this course? Well, we study **groups**.

Definition II.1.1

A **group** is a set S equipped with a "binary operation":

$$\begin{aligned} \cdot : S \times S &\to S \\ (s, t) &\mapsto s \cdot t \end{aligned}$$

which satisfies the following axioms:

Associativity) $s(tu) = (st)u$

Identity) There is some element e such that $s \cdot e = e \cdot s$ for all $s \in S$.

Inverses) For every $s \in S$ there is some $t \in S$ such that $st = e = ts$.

We sometimes denote such a group by the triple $(S, \cdot, e)$. One should not think about it like this.

Groups arise as *symmetries* of objects in nearly all areas of mathematics. This allows them to be broadly applied and to solve a variety of problems. Furthermore, we understand groups very very very well, and this allows us to transform problems that are challenging in other areas into problems in group theory which are perhaps less challenging.

Example II.1.1

A classic example of a symmetry group is the symmetries of a *set*, aka for a set S we can consider the set $\mathrm{Aut}(S)$ of invertible functions $S \to S$ with the operation of function composition.

This is a great example to remember for thinking of groups as symmetries.

Remark II.1.1

Some results and ideas in this course are generalized in a subject called category theory. This starts exactly... now! Do not worry if you do not know category theory. However, some remarks will be left for those that do, as well as an appendix on the subject Appendix A.

Category Theory formalizes the idea of symmetries of an object being a group. Namely, for an object X lying in a category $\mathscr{C}$, there is a group $\mathrm{Aut}_{\mathscr{C}}(X)$ of invertible morphisms $X \to X$ in $\mathscr{C}$.

We now move on to some basic examples and results to guide our thinking about the subject.

Example II.1.2

Lets quickly give some examples of groups to see how amazing they really are.

Symbol	Set	Operation
$\mathbb{Z}$	$\mathbb{Z}$	$+$
$\mathbb{Q}^\times$	$\mathbb{Q} \setminus \{0\}$	$\times$
$\mathrm{SL}_3(\mathbb{Z})$	3×3 matrices with det one	Matrix Mult.
$\mathrm{SL}_3(\mathbb{Z}/10\mathbb{Z})$	3×3 matrices with det one and entries in $\mathbb{Z}/10\mathbb{Z}$	Matrix Mult.
$\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$	2×2 matrices with nonzero det and entries in $\mathbb{Z}/1\mathbb{Z}$	Matrix Mult.
S_n	Permutations of $\{1, \ldots, n\}$	Composition
$C_n = \mathbb{Z}/n\mathbb{Z}$	$\{1, \ldots, n\}$ Addition modulo n.	

The group $\mathbb{Z}/n\mathbb{Z}$ is called the cyclic group of order n and is extremely important.

Interesting Note: $\mathbb{Z}/n\mathbb{Z}$ is "generated" by 1. This means that any element of $\mathbb{Z}/n\mathbb{Z}$ may be obtained by repeatedly multiplying 1 by itself.

Proposition II.1.1

Here is a list of fundamental and basic results about about groups:

- The identity element is unique. If e, e' are both identities, $e' = ee' = e$.
- The inverse of a given element $s \in S$ is unique. We call this inverse s^{-1}. Suppose $s^{-1}s = e = st$ then:

  $$s^{-1} = s^{-1}e = s^{-1}(st) = (s^{-1}s)t = et = t$$

  Great!
- When multiplying many elements, there is no need to write parentheses. I.e. $s_1 s_2 \cdots s_n$ (for $s_i \in S$) always evaluates to the same element of S regardless of how it is grouped.

One might think that they should understand groups by going through all of the possible sizes one by one and classifying those groups. This is awful and a terrible idea. We do it anyway to show you that it works for very small groups:

Size 1) C_1.

Size 2) C_2.

Size 3) C_3.

Size 4) C_4 and $C_2 \times C_2$ (see Definition II.1.2).

Size 5) C_5.

Size 6) S_3, C_6.

Size 7) C_7.

Size 8) Ugly.

Definition II.1.2

Given two groups G, H with respective operations $\cdot, \star$ we have that $G \times H$ is a group with the operation

$$\begin{aligned}(\cdot, \star) : (G \times H) \times (G \times H) &\to G \times H \\ ((g_1, h_1), (g_2, h_2)) &\mapsto (g_1 \cdot g_2, h_1 \star h_2).\end{aligned}$$

To study groups well we should define extra structure to think about them.

Definition II.1.3

A subgroup of a group $(G, \cdot, e)$ is a subset H of G which contains e such that $(H, \cdot, e)$ is also a group.

An equivalent definition is that H is a subet of G containing e such that:

- If $s, t \in H$ then $st \in H$.
- If $s \in H$ then $s^{-1} \in H$.

Example II.1.3

Subgroups of $\mathbb{Z}$ under addition are all $n\mathbb{Z}$ with n some arbitrary non-negative integer.

Proof. Let H be a subgroup of $\mathbb{Z}$. By definition, any subgroup contains zero. $\{0\} = 0\mathbb{Z}$ is a subgroup.

Now $H \neq \{0\}$, so it contains some nonzero element, and so it must contain some positive element because inverses correspond to negation. We then may take the smallest positive element $n \in H$.

By repeated addition, $n\mathbb{Z} \subseteq H$, so we must show that $H \subseteq n\mathbb{Z}$. To show this, let $x \in H$. By the division algorithm, $x = nq + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < n$. But then $r = x - nq \in H$, so by minimality of n, we have that $r = 0$ and $x = nq$. ♥

Now we prove one of the most crucial results about finite groups right off the definition. To do we introduce a new concept, a "coset" and these cosets will partition our set.

Definition II.1.4

Given a group G, a subgroup H of G, and an element $g \in G$, the set $gH = \{gh \mid h \in H\}$ is called a coset of H or of g.

Theorem II.1.2 (Lagrange's Theorem)

If G is a finite group and H is a subgroup of G, then $|H|$ (the size of H) divides $|G|$. Notably the converse is not always true.

Spoecifically we have that $|G| = |H| \cdot [G : H]$, where $[G : H]$ is the number of different cosets of H in G

Proof. We do this by showing that the cosets partition G into equal pieces. Equivalently, this defines an equivalece relation on G ($g \sim g'$ if $gH = g'H$, or equivalently they belong to the same coset, equivalently $g'g^{-1} \in H$).

For $g \in G$, consider the coset gH. Clearly $|gH| = |H|$ since $gx = gy$ implies that $x = y$. Also $\bigcup_{g \in G} gH = G$ since $e \in H$, so $g = ge \in gH$.

We simply must show that $gH \cap g'H \neq \emptyset$ then $gH = g'H$. Let $x \in gH \cap g'H$, so $x = gh = g'h'$ for some $h, h' \in H$. Without loss of generality, it suffices to prove that $gH \subseteq g'H$, as the same method will show that $g'H \subseteq gH$.

Fix some $y \in gH$, then $y = gh_y$ for some $h_y \in H$. Then $y = gh_y = g'h'h^{-1}h_y \in g'H$.

Put another way, we can write this symbolically at the level of sets:

$$gH = ghh^{-1}H = g'h'h^{-1}H = gh'H = gH$$

Using the fact that $hH = H$ for any $h \in H$, which can be proven quickly using the fact that H is closed under the group operation and under inverses.

Therefore G is the union of disjoint subsets, each of size $|H|$, so $|H|$ divides $|G|$. Using the fact that $hH = H$ for any $h \in H$, which can be proven quickly using the fact that H is closed under the group operation and under inverses.

Therefore G is the union of disjoint subsets, each of size $|H|$, so $|H|$ divides $|G|$. ♥

Corollary II.1.3

Every $g \in G$ satisfies $g^{|G|} = 1_G$ (that is the identity in G)

Proof. Let H be the group generated by g, that is all "powers" of g. Then $|H|$ is the smallest nonnegative integer so that $g^{|H|} = 1_G$ Because $|H|$ divides G, we may then write $g^{|G|} = g^{s|H|} = 1_G^s = 1_G$ for some integer s. ♥

Announcements and Ideas

- Office Hours (via Zoom): MW, 8pm-9:30pm
- Don't read math line by line. Try not to spend time understanding the technical details and instead extract the key idea.

We now talk about different ways of describing groups, and a few common groups. To think about this, consider how awful it would be to describe a group with 100 elements via a 100 × 100 table to describe the operation $\cdot : S \times S \to S$.

Definition II.1.5

The **order of a group** G is its size as a set.

Definition II.1.6

The **cyclic group generated by an element** g (in a group S) is the smallest (ordered by inclusion) subgroup of S which contains g. We often denote this group by $\langle g \rangle$.

Equivalently, this is $\{g^n \mid n \in \mathbb{Z}\}$, where $g^n = \underbrace{ggg\cdots g}_{n \text{ copies}}$ (taking inverses for negative n). Note that all powers of g commute, that is $g^n g^m = g^m g^n$.

Proposition II.1.4

If this group is finite, then it's $\{g, g^2, \ldots, g^k\}$ where k is the smallest positive integer such that $g^k = e$.

Proof. Finiteness gives $g^i = g^j$ for some $0 < i < j$, so $(g^{-1})^i g^i = (g^{-1})^i g^j = g^{j-i}$. There is then a positive integer with $g^k = e$. Pick the smallest such k.

Then if $0 < a < b \leq n$ and $g^a = g^b$ then we would have $e = g^{b-a}$, which is impossible. Now just note that $\{g, g^2, \ldots, g^n\}$ is closed under multiplication, contains the identity, and contains inverses. Namely for $0 < i < n$ we have $g^i g^{n-i} = g^n = e$, and $g^n g^n = e$. ♥

Definition II.1.7

We define the **order of an element** g (in a group S) to be the size of $\langle g \rangle$. That is:

$$|g| = \begin{cases} n & \text{if } \langle g \rangle \text{ has } n \in \mathbb{N} \text{ elements} \\ \infty & \text{if } \langle g \rangle \text{ is infinite} \end{cases}$$

Definition II.1.8

We say a group G is **abelian** provided that any two elements of G commute. That is for all $g, h \in G$, $gh = hg$.

There is also a cancellation law for groups. If G is a group and $gh = gr$ for $g, h, r \in G$ then $h = r$ by mulitplying on the left by g^{-1}. Likewise if $hg = rg$ then $h = r$.

Recall that last time we proved the subgroups of $\mathbb{Z}$ are cyclic groups $n\mathbb{Z}$, with n being a non-negative integer. The key to the proof was that if a subgroup contains two positive integers a, b, then it also contains $a - bz$ for all $z \in \mathbb{Z}$. We then combine this iwth the division algorithm, which says that there is some $z, r \in \mathbb{Z}$ such that $a = bz + r$ and $0 \leq r < |b|$. We then can run through this multiple times to find that the subgroup is $n\mathbb{Z}$ for the smallest positive n in the group.

We can actually get more out of this!!!

Proposition II.1.5

Consider the subgroup $G = \langle a, b \rangle$ generated by two nonzero integers a, b. Then $G = \gcd(a, b)\mathbb{Z}$. Furthermore this does some number theory for us!

- There is a greatest common divisor of two nonzero integers.
- Every common divisor of a, b divides the greatest common divisor.
- The greatest common divisor is expressible as $\gcd(a, b) = ax + by$ for $x, y \in \mathbb{Z}$. This is called Bezout's Lemma.

Proof. Note that $G = a\mathbb{Z} + b\mathbb{Z}$, that is integer multiples of a plus integer multiples of b. G must clearly contain this set, and this set contains G by using commutativity of addition.

We know $G = n\mathbb{Z}$ for some $n > 0$. Note then that $a, b \in n\mathbb{Z}$, so n divides both a, b. But also $n \in a\mathbb{Z} + b\mathbb{Z}$, so $n = ax + by$ for some $x, y \in \mathbb{Z}$. Now if $d \in \mathbb{Z}$ divides both a and b then $d \mid n$. Why? Well, $dA = a$, $dB = b$ so $n = ax + by = d(Ax + By)$. Therefore n is the greatest common divisor of a, b. ∎

Corollary II.1.6

If a prime $p \in \mathbb{Z}$ divides $p \mid ab$ with $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.

Proof. If $p \mid a$ then $\gcd(p, a) = 1$ since p is prime. Therefore $1 = ax + py$ for $x, y \in \mathbb{Z}$. Then $b = abx + pby$. Since $p \mid ab$, we know then that $p \mid b$. ∎

Theorem II.1.7

Every positive integer can be written as a product of positive primes in exactly one way, up to permuting the prime factors. Where the empty product is one by convention.

Proof. Induct on n to show existence of a prime factorization (clear if $n = 1$ or n is prime, otherwise $n = ab$ for $a, b < n$, apply induction).

Now we must show uniqueness by induction as well. If $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$ with p_i, q_j prime. Then we use that $p_1 \mid q_1 q_2 \cdots q_\ell$, so $p_1 \mid q_i$ for some i. Because they are primes, $p_1 = q_i$, and by rearrangement we may assume $i = 1$.

By cancellation, $p_2 \cdots p_k = q_2 \cdots q_\ell < n$ because $p_1 = q_1 > 1$. By induction we're done. ∎

We now list some order-theoretic properties of these subgroups, noting that the intersection of two subgroups of a group G is always a subgroup of G. Let $a, b \in \mathbb{Z} \setminus \{0\}$.

- $a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z}$ with $n = \operatorname{lcm}(a, b)$. The proof is easy and is left as an exercise.
- $\langle a, b\rangle = a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ where $d = \gcd(a, b)$.

There is also an alternative proof of unique factorizations. Lets sketch it! Suppose n is the least positive integer with at least two prime factorizations $n = p_1 \cdots p_k = q_1 \cdots q_\ell$, and we might as well assume $p_1 \leq \cdots \leq p_k$ and $q_1 \leq \cdots \leq q_\ell$. Then one may consider $n - p_1 q_1$, and go from there, noting that if $p_1 = q_1$ then we're already done by the above ide ideaa.

Last time $a, b \in \mathbb{Z}$ not both zero, then $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ where $d = \gcd(a, b)$. So $d = am + bn$ with $m, n \in \mathbb{Z}$. A consequence is then that if $c \mid a$ and $c \mid b$ then $c \mid d$ (since $c \mid am + bn$).

If p is prime and $p \nmid a$ then $\gcd(a, p) = 1$. Thus $1 = am + pn$, where $m, n \in \mathbb{Z}$. Also, $1 = am \mod p$ ($\boxed{-am + 1 \in p\mathbb{Z}}$). This implies that $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ is a group under multiplication (this in fact makes $\mathbb{Z}/p\mathbb{Z}$ a field).

This type of multiplicative group is often denoted by $(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$ is a group under multiplication.

Definition II.1.9

For any group G and any subgroup H define an equivalence relation on G by

$$g_1 \sim g_2 \iff \boxed{g_1^{-1} g_2 \in H} \iff g_1 H = g_2 H$$

It's a standard check that this is an equivalence relation. Furthermore the conditions above are equivalent as:

$$g_1^{-1} g_2 \in H \iff g_1^{-1} g_2 H = H \iff g_2 H = g_1 H$$

Note how the condition $g_1^{-1} g_2 \in H$ matches the condition from modular arithmetic that $a = b \mod n$ provided that $\boxed{-a + b \in n\mathbb{Z}}$ (which we saw above).

Also note that $H \to gH$ given by $h \mapsto gh$ is a bijection. Further $g_1 H$ and $g_2 H$ are either equal or disjoint.

We now recall Theorem II.1.2

Theorem II.1.2 (Lagrange's Theorem)

If G is a finite group and H is a subgroup of G, then $|H|$ (the size of H) divides $|G|$. Notably the converse is not always true.

Spoecifically we have that $|G| = |H| \cdot [G : H]$, where $[G : H]$ is the number of different cosets of H in G

Extremely Useful Idea: Think of G as inducing permutations on G/H, the set of cosets of H, where $g \in G$ maps $g_1 H \mapsto g g_1 H$.

Corollary II.1.8

If a group G has prime order then it is cyclic.

Proof. If $g \in G$ isn't 1_G then g generates a subgroup $\langle g\rangle$ of G. $|\langle g\rangle|$ divides the prime $|G|$, but $|\langle g\rangle|$ isn't one. Thus $|\langle g\rangle| = |G|$, so $\langle g\rangle = G$. ♥

We now begin to relate groups to each other via particular nice types of functions.

Definition II.1.10

A **homomorphism** $f : G_1 \to G_2$ between groups G_1, G_2 is a function such that

$$f(xy) = f(x)f(y)$$

for all $x, y \in G_1$.

Lemma II.1.9

If $f : G_1 \to G_2$ is a homomorphism then $f(1_{G_1}) = 1_{G_2}$ and $f(g^{-1}) = f(g)^{-1}$.

Furthermore $f(G_1)$ is a subgroup of G_2.

Proof. We prove these by simple algebraic manipulation:

$$\begin{aligned} f(1_{G_1}) &= f(1_{G_1} \cdot 1_{G_1}) = f(1_{G_1}) \cdot f(1_{G_1}) \\ f(1_{G_1}) &= 1_{G_2} \end{aligned}$$

We also may write:

$$\begin{aligned} f(g)f(g^{-1}) = f(gg^{-1}) = f(1) = 1 \\ f(g^{-1}) = f(g)^{-1} \end{aligned}$$

The fact that $f(G_1)$ is a subgroup immediately follows, as it contains the identity, inverses, and is closed under multiplication

Example II.1.4

$\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$, where $\mathrm{GL}_n(\mathbb{R})$ are the invertible matrices under multiplication and $\mathbb{R}^\times$ is the nonzero reals under multiplication.

$\exp : \mathbb{R}^+ \to \mathbb{R}^\times$, where $\mathbb{R}^+$ is the group of reals under addition. We also have $|\cdot| : \mathbb{C}^\times \to \mathbb{R}^\times$.

The trivial homomorphism $G_1 \to G_2$ which takes everything to 1, as $g \mapsto 1$.

We now generalize a definition from linear algebra that turns out to be extremely extremely useful.

Definition II.1.11

Let $f : G_1 \to G_2$ be some homomorphism. Then define the **kernel** of f to be

$$\ker f := \{g \in G_1 \mid f(g) = 1\}.$$

This will be a subgroup of G_1 (exercise!), and it will satisfy some very nice properties. Namely if $b \in \ker f$ and $a \in G_1$ then $aba^{-1} \in \ker f$.

$$f(aba^{-1}) = f(a)f(b)f(a)^{-1} = f(a)f(a)^{-1} = 1$$

Definition II.1.12

Define a **normal subgroup** N of G to be a subgroup such that $gng^{-1} \in N$ for all $n \in N$ and $g \in G$. We notation this as $N \trianglelefteq G$.

> So, if $f : G_1 \to G_2$ is a homomorphism then $\ker(f)$ is a normal subgroup of G_1. Later we will show the converse, if N is a normal subgroup of G then N is the kernel of some homomorphism $G \to \widetilde{G}$ (in fact, as a set $\widetilde{G} = G/N$).

If $f : G_1 \to G_2$ is a homomorphism, then

$$f(x) = f(y) \iff f(x)^{-1} f(y) = 1 \iff f(x^{-1}) f(y) = f(x^{-1}y) = 1$$
$$\iff x^{-1}y \in \ker f \iff x\ker(f) = y\ker(f)$$

This implies that for any $g \in f(G_1)$, $\left|f^{-1}(g)\right| = |\ker(f)|$.

> **Corollary II.1.10**
>
> For a group homomorphism f, f is injective if and only if $\ker(f) = \{1\}$.

Note first that if G is an abelian group, then every subgroup of G is normal.

> **Definition II.1.13**
>
> A **simple group** G is a nontrivial group whose only normal subgroups are G and 1.

> **Example II.1.5**
>
> The only abelian simple groups are $\mathbb{Z}/p\mathbb{Z}$ for p a prime (isomorphic to cyclic of prime order).

> **Theorem II.1.11** (Feit-Thompson)
>
> If G is a simple group of odd order, then it is cyclic of prime order.

Proof. A 200 page book for a world-class expert in the subject.

> **Theorem II.1.12**
>
> The finite simple groups are known, and understood very very well.

Proof. The experts in group theory classified all the simple groups around the 1960s resulting in an approximately 15,000 page book.

<u>Fact</u>: There is a surjective homomorphism $S_m \to S_n$ if and only if $m = n$ or $n = 1$ or $n = 2$ or ($m = 4$ and $n = 3$).

> **Definition II.1.14**
>
> A map $f : G \to \widetilde{G}$ is an **isomorphism** provided that f is a bijective homomorphism.
>
> In this case we say that $G \cong \widetilde{G}$, and that G and $\widetilde{G}$ are **isomorphic**

> **Lemma II.1.13**
>
> Let $f : G \to \widetilde{G}$ is an isomorphism, then the inverse function $f^{-1} : \widetilde{G} \to G$ is an isomorphism.

Proof. Let $x = f(a)$ and $y = f(b)$. Then $f(ab) = f(a)f(b) = xy$. Thus

$$f^{-1}(xy) = ab = f^{-1}(x)f^{-1}(y)$$

Perfect!

Example II.1.6

The Klein 4-group $V_4 = C_2 \times C_2 = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\}$.

In S_4, there is a normal subgroup $\{1, (12)(34), (13)(24), (14)(23)\}$. This is not cyclic since everything has order two, and so it is isomorphic to V_4.

There is another copy of V_4 in S_4, namely $\{1, (12), (34), (12)(34)\}$, and this is **not** normal.

This means we need to be careful about talking about isomorphisms between subgroups of a given group.

Definition II.1.15

An **automorphism** of a group G is an isomorphism from G to itself.

The set of automorphisms form a group under composition, called $\mathrm{Aut}(G)$.

Definition II.1.16

For $g \in G$, define a function

$$\begin{aligned} \varphi_g : G &\to G \\ h &\mapsto ghg^{-1} \end{aligned}$$

called **conjugation by** g. This is an automorphism, and these are called the **inner automorphisms**

Proof. Well we see that

$$(gh_1g^{-1})(gh_2g^{-1}) = gh_1g^{-1}gh_2g^{-1} = g(h_1h_2)g^{-1}$$

So this is a group homomorphism. Furthermore it has inverse $h \mapsto g^{-1}hg$, as

$$\begin{aligned} h &\mapsto ghg^{-1} \mapsto g^{-1}ghg^{-1}g = h \\ h &\mapsto g^{-1}hg \mapsto gg^{-1}hgg^{-1} = h \end{aligned}$$

Perfect! ♥

We can also note that

$$\varphi_{g_1} \circ \varphi_{g_2} = \varphi_{g_1 g_2}$$

Which we can simply compute

$$h \mapsto g_2hg_2^{-1} \mapsto g_1g_2hg_2^{-1}g_1^{-1} = (g_1g_2)h(g_1g_2)^{-1}$$

Thus $g \mapsto \varphi_g$ is a homomorphism $G \to \mathrm{Aut}(G)$. We can ask what is the kernel of this homomorphism? Well

$$\ker = \{g \in G \mid \varphi_g = \mathrm{Id}_G\} = \{g \in G \mid \varphi_g(h) = h \ \ \forall h \in G\} = \{g \in G \mid gh = hg \ \ \forall h \in G\}$$

And this is a normal subgroup.

Definition II.1.17

This kernel of the conjugation homomorphism $G \to \mathrm{Aut}(G)$ is called the **center** of the group G and is denoted $Z(G)$.

$$Z(G) \coloneqq \{g \in G \mid gh = hg \ \ \forall h \in G\}.$$

> This is of course a normal subgroup.

Lets think about conjugation in S_n. For example consider

$$(123)(12)(132) = (23)$$

More concretely we can write this compositon as

$$\begin{tikzcd}
1 & 3 \arrow[l] & 3 \arrow[l] & 1 \arrow[l] \\
3 & 2 \arrow[l] & 2 \arrow[dl] & 3 \arrow[l] \\
2 & 1 \arrow[l] & 1 \arrow[ul] & 2 \arrow[l]
\end{tikzcd}$$

In general

$$\sigma \circ \theta \circ \sigma^{-1}$$

is gotten from θ by applying σ to all elements in all cycles of θ, when written in cycle notation.

$$\sigma(i) \xmapsto{\sigma^{-1}} i \overset{\theta}{\mapsto} \theta(i) \overset{\sigma}{\mapsto} \sigma(\theta(i))$$

> **Proposition II.1.14**
>
> Let G be a group and H be a subgroup, with G/H the set of all (left-)cosets gH for $g \in G$. Then let $\eta_g : xH \mapsto gxH$ be a map, then
>
> $$\begin{aligned} \eta : G &\to \mathrm{Sym}(G/H) = \{\text{permiutations of } G/H\} \\ g &\mapsto \eta_g \end{aligned}$$
>
> is a homomorphism.

Proof. η_g is in $\mathrm{Sym}(G/H)$ because $\eta_{g^{-1}}$ is an inverse by an easy computation.

η is a homomorphism because

$$\eta_{g_1} \circ \eta_{g_2} : xH \xmapsto{\eta_{g_2}} g_2 xH \xmapsto{\eta_{g_1}} (g_1 g_2)xH = \eta_{g_1 g_2}(xH)$$

Perfect!

In case $H = 1$, this homomorphism has trivial kernel, and so its an injective homomorphism $G \hookrightarrow \mathrm{Sym}(G)$. It then induces an isomorphism $G \xrightarrow{\cong} \eta(G) \subseteq \mathrm{Sym}(G)$. This says that every group is isomorphic to a subgroup of permutations.

II.2. **The Basic Tools**

Going from the well-behaved case of the cyclic groups C_n to the non-abelian case is really hard, and sometimes requires extra hypotheses. We should think of normal subgroups as analogous to divisors of an integer, and simple groups as prime numbers.

Definition II.2.1

For any $n > 1$, there is a surjective homomoprhism $\operatorname{sgn} : S_n \twoheadrightarrow S_2$.

First, there is an injective homomorphism:

$$\begin{aligned} \rho : S_n &\hookrightarrow \{n \times n \text{ integer matrices with } \det \text{ equal to } \pm 1\} \\ \sigma &\mapsto \left(A_{ij} = \delta_{i\sigma(j)}\right) \end{aligned}$$

where $\delta_{k\ell}$ is the Kroenecker Delta (which is 1 when $k = \ell$ and zero otherwise). Then $\det \circ \rho$ is a surjective homomorphism $S_n \twoheadrightarrow \{\pm 1\}$, where $\{\pm 1\}$ is a group under multiplication. We call this homomorphism $\operatorname{sgn} : S_n \twoheadrightarrow S_2$.

We define $A_n \coloneqq \ker \operatorname{sgn}$, and we say $\sigma \in S_n$ is **even** if $\operatorname{sgn} \sigma = 1$ and otherwise we say σ is **odd**.

Great fact: If $n \geq 5$ then A_n is simple.

Note: Any 2-cycle is odd.

Easy: Every element of S_n is a product of disjoint cycles (Hint: take a starting point, run it through σ over and over again until you get back to the starting point).

Consequence: Every element of S_n is a product of 2-cycles, since every cycle is a product of 2-cycles. Why? Well

$$(14)(13)(12) = (1234)$$

and likewise for any other cycle.

Restated: S_n is generated by the two-cycles.

This gives an immediate proof of the following:

Proposition II.2.1

An element σ of S_n is even if and only if it can be written as a product of an even # of 2-cycles if and only if it cannot be written as the product of an odd # of 2-cycles.

Proposition II.2.2

A_n is generated by 3-cycles.

Proof. From the above, we know A_n is all products of an even # of 2-cycles. Thus it suffices to show that 3-cycles are exactly products of two 2-cycles:

$$\begin{aligned} (ij)(ij) &= \mathrm{Id} \\ (ij)(ik) &= (ikj) && (i, j \neq k) \\ (ij)(k\ell) &= (ki\ell)(ijk) && (i, j \neq k,\ i, j \neq \ell) \end{aligned}$$

Thus every product of two 2-cycles is a product of some # of 3-cycles and every 3-cycle is in A_n. Great! ♥

Proposition II.2.3

Let H be a subgroup of G, recall that:

$$H \text{ is normal} \iff gHg^{-1} \subseteq H \quad \forall\, g \in G$$

$$\begin{aligned}
&\iff gHg^{-1} = H \quad \forall\, g \in G \\
&\iff gH = Hg \quad \forall\, g \in G \\
&\iff H \text{ is the kernel of some homomorphism } \varphi : K \to G
\end{aligned}$$

And in fact we have:

$$aHbH = a(Hb)H = a(bH)H = abHH = abH$$

This is suggesting we define a group. Namely G/H (the set of left cosets of H) is a group with operation $(aH)(bH) = (ab)H$.

Proof. If H is normal in G, then $gHg^{-1} \subseteq H$, and then $g^{-1}Hg \subseteq H$, so $H \subseteq gHg^{-1}$.

The backwards direction of this is clear, and the second holds if and only if the third holds by multiplication by g (resp. g^{-1}) on the right.

Now for the last bit, we know all kernels of homomorphisms are normal from last time. If $H \trianglelefteq G$ then we can write:

$$\begin{aligned}
G &\to G/H \\
g &\mapsto gH
\end{aligned}$$

is a surjective homomorphism with kernel H.

Definition II.2.2

If $H \trianglelefteq G$, then G/H is a group, called the quotient group. The operation is

$$(aH)(bH) = (ab)H.$$

And it is well defined because by the above proposition if H is normal that as sets

$$(aH)(bH) = a(Hb)H = a(bH)H = (ab)H.$$

Details to be checked that this is a group.

So if $H \trianglelefteq G$ then G/H is a group, called the quotient group.

Lemma II.2.4

If $[G : H] = 2$ (the **index** of H in G, that is $|G/H|$), then $H \trianglelefteq G$.

Proof. If $g \in H$ then $gH = H = Hg$. Then if $g \notin H$ then $gH = G \setminus H = Hg$.

Note: There is a bijection between G/H and the set of right cosets Hg for $g \in G$ given by inversion:

$$gH \mapsto Hg^{-1}$$

Note: Automorphisms of G preserve "reasonable" properties. E.g. if $\sigma \in \operatorname{Aut} G$ and $H \leq G$ then $H \trianglelefteq G$ if and only if $\sigma(H) \trianglelefteq H$. Also $[G : H] = [G : \sigma(H)]$. Also H is abelian if and only if $\sigma(H)$ is abelian.

So for instance, if H is the unique subgroup of G with a given index $[G : H]$, then $H \trianglelefteq G$ (since H must be preserved by conjugation by any $g \in G$).

Announcements: Midterms

- Friday October 22nd, 6pm-8:30pm
- Thursday: December 9th, 6pm-8:30pm
- NO FINAL EXAM

Given a group G and a subgroup H we defined G/H to be the set of all (left)-cosets of H in G. Recall that:

- $[G : H] \coloneqq |G/H|$.
- If $H \trianglelefteq G$ then G/H is a group under the operation induced by G. That is $(aH)(bH) = (ab)H$. As a set this is exactly:

  $$\{ah_1bh_2 \mid h_1, h_2 \in H\}$$

  And so either way of interpreting $(aH)(bH)$ is correct!
- There is a quotient map $G \to G/H$ given by $g \mapsto gH$, which is clearly a surjective homomorphism. And in fact the kernel of this map is H.

Theorem II.2.5 (Artin calls this the Correspondence Theorem)

Let $f : G \twoheadrightarrow G'$ be a surjective homomorphism with kernel K. There is then a natural bijection between subgroups of G containing K, and subgroups of G'. This is given by taking image/preimage under f.

$$H \mapsto f(H)$$
$$f^{-1}(J) \mapsfrom J$$

Proof. The images and preimages will in fact be subgroups (easy check). Furthermore if $J \leq G'$, then $f^{-1}(J)$ contains K because $1 \in J$, and every $k \in K$ maps to 1.

It's immediate that $f(f^{-1}(J)) = J$ because f is surjective. We then need to show for $K \leq H \leq G$ that $H = f^{-1}(f(H))$. From set theory we know that $H \subseteq f^{-1}(f(H))$. So we just need to show the other direction.

Let $x \in f^{-1}(f(H))$, so then $f(x) = f(h)$ for some $h \in H$. But then $f\left(xh^{-1}\right) = 1$, so $xh^{-1} \in K \subseteq H$. Thus $xh^{-1} \in H$ and we then know that $x = xh^{-1}h \in H$, and we are done!

Another proof looks like this. Preimages of points are exactly cosets of the kernel, so we have:

$$f^{-1}(f(H)) = \bigcup_{h \in H} f^{-1}(f(h)) = \bigcup_{h \in H} hK = H$$

Using the fact that $K \leq H$, so any element of hK lies in H. ♥

Note if $K \leq H \leq G$ then $[G : H] = [G' : f(H)]$. Send the coset gH to $f(g)f(H)$, and this will be a bijection. The argument is standard from similar ideas to the above.

If G is a group and N is a normal subgroup, then the homomorphism $G \twoheadrightarrow G/H$ is called the quotient homomorphism/quotient map/canonical homomorphism. The correspondence theorem then tells us that subgroups of G/H are in bijection with the subgroups of G containing N.

Theorem II.2.6 (The First Isomorphism Theorem)

Let $f : G \to \overline{G}$ be some surjective homomorphism with kernel K. Then $G/K \cong \overline{G}$. Precisely, let $\pi : G \twoheadrightarrow G/K$ be the quotient map. Then there is a unique isomorphism $\overline{f} : G/K \to \overline{G}$ which makes the following diagram commute:

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[dr, "\pi"'] & \overline{G} \\
 & G/K \arrow[u, dashed, "\overline{f}"']
\end{tikzcd}$$

Proof. A function $\overline{f} : G/K \to \overline{G}$ such that $\overline{f} \circ \pi = f$ is completely determined by f because π is surjective. Namely for $gK \in G/K$, we know:

$$\overline{f}(gK) = \overline{f}(\pi(g)) = f(g)$$

We now just need to show that's a well-defined isomorphism.

Say that $gK = \widetilde{g}K$, then:

$$f(gK) = f(g)f(K) = f(g) = f(\widetilde{g}) = f(\widetilde{g})f(K) = f(\widetilde{g}K)$$

Great! Thus this function $\overline{f} : G/K \to \overline{G}$ is well-defined.

$\overline{f}$ is a homomorphism clearly because:

$$\overline{f}((g_1K)(g_2K)) = \overline{f}(g_1g_2K) = f(g_1g_2) = f(g_1)f(g_2) = \overline{f}(g_1K)\overline{f}(g_2K).$$

Furthermore $\overline{f}$ is surjective. Take $\overline{g} \in \overline{G}$, then $\overline{g} = f(g)$ for some $g \in G$, so:

$$\overline{f}(\pi(g)) = f(g) = \overline{g}$$

Finally, $\overline{f}$ is injective. To show this we show $\ker \overline{f} = 1$. Let $gK \in \ker \overline{f}$, then $f(g) = 1$, so $g \in \ker f = K$, and $gK = K$ and we're done! ♥

Lets look at symmetries of a triangle:

- Rotation by 120 degrees around the center (order 3)
- Reflect through an angle bisector (order 2)

These generate S_3.

In general, a regular n-gon has $2n$ symmetries by rotations/reflections. These are generated by the reflections, as two reflections makes a rotation.

Definition II.2.3

The dihedral group of order $2n$ is the largest group generated by x, y satisfying the relations

$$x^2 = y^2 = (xy)^n = 1$$

One can show that the elements are $z^i x^j$ for $0 \leq i < n$ and $0 \leq j \leq 1$.

This is a non-abelian group!

Definition II.2.4

An isometry $f : M \to N$ between two metric spaces M, N is a function such that

$$d(x, y) = d(f(x), f(y)).$$

Lemma II.2.7

Every isometry $\mathbb{R}^2 \to \mathbb{R}^2$ is invertible, and the inverse is an isometry.

Lemma II.2.7 is a consequence of

Lemma II.2.8

The isometries of the plane are precisely translations composed with rotations about the origin through some angle composed with either the identity or a reflection about the x-axis.

Proof. It's clear that these are isometries (and are invertible).

Conversely, given any isometry f, we peel off each piece in layers. Write $f_1(x) = f(x) - f(0)$. Then:

$$d(f_1(x), f_1(y)) = d(f(x) - f(0), f(y) - f(0)) = d(f(x), f(y)) = d(x, y)$$

This is then an isometry so that $f_1(0) = 0$. We prove these isometries which fix 0 are rotations about the origin composed with either the identity or a reflection about the x-axis

Now consider $\|f_1(1, 0)\| = \|(1, 0)\| = 1$ must lie on the unit circle. Thus $f_1(1, 0) = (\cos\theta, \sin\theta)$ for some $\theta \in [0, 2\pi)$. Simply set f_2 to be f_1 composed on the left with a rotation by $-\theta$ about the origin, to undo this. Then $f_2(1, 0) = f_2(1, 0)$ and $f_2(0) = 0$. Furthermore this is an isometry, we prove isometries fixing the origin and $(1, 0)$ are either the identity or reflection through the x-axis.

The proof then goes by saying that $(0, 1)$ is distance 1 from $(0, 0)$ and distance $\sqrt{2}$ from $(1, 0)$. Thus $f_2(0, 1)$ lies on circles of distance 1 from $(0, 0)$ and distance $\sqrt{2}$ from $(1, 0)$. Circles only ever intersect at at most two points, and so $f_2(0, 1) = (0, 1)$ or $f_2(0, 1) = (0, -1)$.

Thus write $f_3 = f_2$ or $f_3 = \text{reflect} \circ f_2$. Thus f_3 is an isometry fixing $(0, 0)$, $(1, 0)$, $(0, 1)$. We show f_3 is the identity.

First we show the x-axis and y-axis are fixed. $(x, 0)$ is the only point in $\mathbb{R}^2$ with distance $|x|$ from $(0, 0)$ and distance $(|x - 1|$ from $(1, 0)$. Similarly, the y-axis is fixed. Then (x, y) is the unique point with distance $|y|$ from $(x, 0)$, distance $|x|$ from $(y, 0)$ and distance $\sqrt{x^2 + y^2}$ from $(0, 0)$.

Theorem II.2.9

The isometries are precisely

(1) Translations

(1) Rotation about some point through some angle

(1) Reflection through some line

(1) "Glide reflection," reflect through a line ℓ and then translate by a nonzero vector along ℓ.

Translations and rotations are orientation-preserving, and the reflections and glide reflections are orientation-reversing. If we envision these as symmetries of a plane lying in $\mathbb{R}^3$ this is exactly talking about preserving the "top" of the plane.

Proof. Suppose $f = \tau_Q \circ \rho_\theta$, a translation by a point Q and rotation counterclockwise about $(0, 0)$ by $0 \le \theta < 2\pi$. If $\rho_\theta = \text{Id}$ we 're done, so assume $\rho_\theta \ne \text{Id}$.

We must show that f is a rotation about some point. Our first goal is to show f has one and only one fixed point R (the point which it rotates about), and then to translate that point back to the origin via a conjugation (by a translation). We then show that $\tau_R^{-1} f \tau_R = \rho_\psi$ is rotation about the origin, proving the claim that $f = \tau_R \rho_\psi \tau_R^{-1}$ is rotation about R (as the translation τ_R just changes coordinates).

We want $f(R) = R$, so that means we want $(\rho_\theta - \text{Id})R = -Q$ for one and only one R. Thus we show $\rho_\theta - \text{Id}$ is an invertible linear transformation. Well:

$$\det(\rho_\theta - I) = \begin{vmatrix} \cos\theta - 1 & -\sin\theta \\ \sin\theta & \cos\theta - 1 \end{vmatrix} = 2 - 2\cos\theta \ne 0$$

Because $\rho_\theta \ne \text{Id}$, so $\cos\theta \ne 1$.

The rest of the proof is similar in flavor, and will be completed Thursday.

Continued proof of Theorem II.2.9. We now know there is a unique fixed point R of our isometry given by $\tau_Q \circ \rho_\theta$.

We then have that $\tau_{-R} \circ \tau_Q \circ \rho_\theta \circ \tau_R$ is a rotation about the origin. Why? It's an orientation-preserving isometry that fixes the origin, so the composition $\tau_{Q'} \circ \rho_{\theta'} \circ (\text{Id or } r)$ cannot have $Q' \ne 0$ or r.

Thus $\tau_Q \circ \rho_\theta$ is a rotation about R.

Now suppose the isometry reverses orientation, that is it equals $\tau_Q \circ \rho_\theta \circ r$.

Then all we need to understand is $\rho_\theta \circ r$, and show that this is a reflection through some line. Namely it's reflection through the line which passes through $(0, 0)$ and is $\rho_{\theta/2}(x - \text{axis})$.

Change coordinates to make this line be the x-axis, then we have $\tau_{Q'} \circ r$, which is a reflection through a horizontal line if Q' is on the y-axis and a glide reflection otherwise.

Theorem II.2.10

Every finite group of isometries of $\mathbb{R}^2$ is cyclic or dihedral.

Proof. We do this in a few simple steps

Step a) There are no nonidentity translations and there are no nonidentity glide reflections, because these have infinite order.

Step b) All rotations in this group G have the same center. To show this, pick any point R_0. We may then form a new point R_1 via:

$$R_1 = \frac{1}{|G|} \sum_{g \in G} g(R)$$

We claim that R_1 is fixed by each $g' \in G$. If g' is a linear transformation $\mathbb{R}^2 \to \mathbb{R}^2$, then $g'(R_1) = R_1$ Why? Well:

$$g'(R_1) = \frac{1}{|G|} \sum_{g \in G} g'(g(R)) = \frac{1}{|G|} \sum_{g \in G} (g'g)(R) = \frac{1}{|G|} \sum_{h \in G} h(R) = R_1$$

The second to last equality is fundamental, and follows because $g \mapsto h = g'g$ is a bijection $G \to G$.

Also we have that τ_Q maps R_1 to $R_1 + Q$, why? Well:

$$\tau_Q(R_1) = Q + \frac{1}{|G|}\sum_{g\in G} g(R) = \frac{1}{|G|}\sum_{g\in G}[g(R) + Q] = \frac{1}{|G|}\sum_{g\in G}\tau_Q(g(R_1))$$

In fact, this means that every isometry maps the center of mass of a set of points to the center of mass of the images of these points.

Because the set $\{g(R) \mid g \in G\}$ and the image set $\{g'(g(R)) \mid g \in G\}$ are the same, this means that each $g' \in G$ fixes R_1. Rotations have a unique fixed point which is their center, and so we're done.

Step c) Suppose G consists solely of rotations. They all have a common fixed point, we may as well assume it is $(0, 0)$ without loss of generality. Say the rotations are by angles $0 = \theta_1 < \theta_2 < \ldots < \theta_k < 2\pi$.

We claim rotation by θ_2 generates the group. Well we know each $\theta_i = n_i\theta_2 + \delta_i$ for $n_i \in \mathbb{Z}$ and $0 \leq \delta < \theta_2$. But then this would imply that rotation by δ_i is in the group, showing that we must have $\delta_i = 0$ by minimality of θ_2.

This finishes this piece!

Step d) If we have a reflection, we can choose coordinates so it is through the x-axis, giving us the dihedral group. Why? Well, we generate the dihedral group, and any two r_1, r_2 composed give a rotation ρ_θ, so $r_1 = \rho_\theta \circ r_2^{-1}$, showing that r_1 must be in the dihedral group as well.

♥

III. Group Actions

Groups most often arise in other fields of mathematics via the automorphisms of certain objects. As such, it makes sense to study groups by looking in the opposite direction. Namely, for a group G, we can study homomorphisms $G \to \mathrm{Aut}(W)$ for some automorphism group of some structure W. We call these maps *representations* of a group, and we say that G *acts* on W.

The two most most common objects to consider for a group to act on are sets and vector spaces. These give *permutation representations* and *linear representations* respectively, and these are given as homomorphisms $G \to \mathrm{Sym}(S)$ and $G \to \mathrm{GL}(V)$ respectively.

For notational reasons, we take the name *group action* to mean a permutation representation, and *representation* by itself to mean a linear representation.

III.1. Permutation Representations

Definition III.1.1

Suppose G is a group and S is a set. We say that a group action of G on S is a homomorphism $\rho : G \to \mathrm{Sym}(S)$

Carrying around this homomorphism can clutter notation, so we often use the following equivalent definition

Definition III.1.2

Suppose G is a group and S is a set. We say that a group action is a map $G \times S \to S$, written by

$g \cdot s$, such that for all $g_1, g_2 \in G$ and $s \in S$

$$g_1 \cdot (g_2 \cdot s) = (g_1 g_2) \cdot s$$
$$1 \cdot s = s$$

We leave the fact that these are equivalent definitions as a simple exercise.

Definition III.1.3

Suppose G is group acting on a set S. We say that the kernel K of the action is the kernel of the associated group homomorphism ρ, equivalently

$$K \coloneqq \{g \in G \mid \forall s \in S, g \cdot s = s\}$$

The kernel is then a normal subgroup of G

Definition III.1.4

Suppose G is a group acting on a set S, and that $s \in S$. We say that the stabilizer of s is the set

$$\mathrm{Stab}_G(s) = \{g \in G \mid g \cdot s = s\}$$

We sometimes also denote the stabilizer of s by G_s

Note that for G acting on S throug the homomorphism ρ, if H is the subgroup of $\mathrm{Sym}(S)$ which fixes s, then $G_s = \rho^{-1}(H)$. In this way, we immediately see that G_s is a subgroup of G.

Definition III.1.5

Suppose G is a group acting on a set S, and let $s \in S$. We say that the orbit of s is the set

$$\mathrm{Orb}_G(s) = \{g \cdot s \mid g \in G\} = \{t \in S \mid \exists g \in G \text{ s.t. } g \cdot t = s\}$$

We sometimes also denote the orbit of s by $\mathcal{O}_s$.

Lemma III.1.1 (Orbits partition)

Suppose G is a group acting on a set S. Then the set $\{\mathcal{O}_s\}_{s \in S}$ is a partition of S.

Proof. We see that the orbits cover S as for any $s \in S$ we know $s \in \mathcal{O}_s$. Thus we just need to show these are disjoint.

Fix $r \in \mathcal{O}_s \cap \mathcal{O}_t$. Now pick an arbitrary $x \in \mathcal{O}_s$. Then we know that there is some $a, g, h \in G$ such that $r = g \cdot s = h \cdot t$ and $x = a \cdot s$. Then

$$a \cdot s = ag^{-1} \cdot r = ag^{-1}h \cdot t$$

Thus $x \in \mathcal{O}_t$, and $\mathcal{O}_s \subseteq \mathcal{O}_t$. By symmetry, $\mathcal{O}_t \subseteq \mathcal{O}_s$. We then see that these are equal sets, and we're done. ♥

Sometimes we will pick a specific representative of an orbit to work with. However, this is really arbitrary in nature, and we should understand what effect this choice has on us.

Lemma III.1.2

Suppose G is a group acting on a set S. Then for $s \in S$ and $g \in G$ we have

$$G_{g\cdot s} = gG_sg^{-1}$$

Proof. This is simple logic

$$\begin{aligned} h \in G_{g\cdot s} &\iff hg \cdot s = g \cdot s \\ &\iff g^{-1}hg \cdot s = g^{-1}g \cdot s \\ &\iff g^{-1}hg \cdot s = s \\ &\iff g^{-1}hg \in G_s \\ \iff h \in gG_sg^{-1} \end{aligned}$$

♥

The intuition is that if h fixes s, and if we relabel $g \cdot s$ to s, h will then fix $g \cdot s$, and we do this relabeling via conjugation.

Definition III.1.6

Suppose G is a group acting on a set S, we say that the action is transitive provided that there is only one orbit $\mathcal{O}_s = S$ for some $s \in S$.

Theorem III.1.3 (Orbit Stabilizer)

Supppose G is a group acting on the set S. Then, for arbitrary $s \in S$

$$[G : G_s] = |\mathcal{O}_s|$$

Proof. Fix arbitrary $s \in S$. Consider the map $f : G \to \mathcal{O}_s$ given by $f : g \mapsto g \cdot s$. We see that f is surjective by the definition of an orbit.

The structure of the theorem is the following

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[dr, "\pi"'] & \mathcal{O}_s \\ & G/G_s \arrow[u, dashed, "\overline{f}"'] \end{tikzcd}$$

In this case, as G_s need not be a normal subgroup of G, π is not a homomorphism, and G/G_s is only a set.

The function $\overline{f}$ which makes the diagram commute is essentially already defined for us. Why? Well $\overline{f} \circ \pi = f$ if and only if for all $gG_s \in G/G_s$ we have

$$\overline{f}(gG_s) = \overline{f}(\pi(g)) = f(g) = g \cdot s$$

This is well defined because if $gG_s = hG_s$ then $g^{-1}h \in G_s$ and

$$\overline{f}(gG_s) = g \cdot s = g(g^{-1}h) \cdot s = h \cdot s = \overline{f}(hG_s)$$

We see that $\overline{f}$ is injective as if $\overline{f}(gG_s) = \overline{f}(hG_s)$ we conclude that $g \cdot s = h \cdot s$, so $g^{-1}h \in G_s$, and then $gG_s = hG_s$.

Finally, we see that $\overline{f}$ is surjective by surjectivity of f, $f = \overline{f} \circ \pi$. ♥

Example III.1.1

If H is a subgroup of G, then G acts on G/H via $g(g'H) = (gg')H$.

This gives a homomorphism $G \to \mathrm{Sym}(G/H)$.

$$\begin{aligned} G_H &= \{g \in G \mid gH = H\} = H \\ G_{gH} &= gHg^{-1} \end{aligned}$$

This action is transitive (i.e., there's only one orbit). As $G/H = \mathcal{O}_H$.

Remark III.1.1

The orbits $\{\mathcal{O}_s\}_{s \in S}$ form a partition of S.

Remark III.1.2

Every transitive action of G on S is isomorphic to the left-multiplication action of G on G/G_s (for any $s \in S$).

Actions of G on sets S and T are isomorphic if there is a bijection $f : S \to T$ such that $gf(s) = f(gs)$.

G acts on G by conjugation:

$$g \cdot h = ghg^{-1}$$

This gives a homomorphism $G \to \mathrm{Aut}(G) \leq \mathrm{Sym}(G)$ as we've discussed before.

The kernel is exactly the center of G. We know that

$$G_h = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\} := C_G(h)$$

where $C_G(h)$ denotes the "centralizer of h in G." Then the center of G is $Z(G) = \bigcap_{h \in H} C_G(h)$, which is the same as the kernel $\bigcap_{h \in H} G_h$.

Applying orbit stabilizer gets us that

$$|\text{conjugacy class of } h \in G| = [G : C_G(h)]$$

A corollary, the size of the conjugacy class divides the size of the group. Since G is the (disjoint) union of its conjugacy classes, it follows that if we have representatives $h_1, \ldots, h_k$ of all the distinct conjugacy classes then

$$\sum_{i=1}^{k} [G : C_G(h_i)]$$

This is called the class equation of G.

Example III.1.2

If $G = S_5$ then the representatives of conjugacy classes are

h_i	$C_G(h_i)$	size	$[S_5 : C_G(h_i)]$
(1)	S_5	120	1
(12)	$C_2 \times S_3$	12	10
(123)	$C_3 \times S_2$	6	20
(1234)	C_4	4	30
(12345)	C_5	5	24
$(12)(34)$	D_4	8	15
$(12)(345)$	$C_2 \times C_3$	6	20
			120

IV. Sylow's Theorems and p-groups

Definition IV.0.1

A p-group (if p is prime) is a group of order p^n for some $n > 0$.

Theorem IV.0.1

Every p-group has nontrivial center.

Proof. The class equation tells us that

$$p^n = \sum_{i=1}^{k} [G : C_G(h_i)]$$

Where h_i are representatives of the distinct conjugacy classes in G. $h \in Z(G)$ if and only if $C_G(h) = G$ if and only if $[G : C_G(h)] = 1$ if and only if the conjugacy class of h is $\{h\}$.

Since $|G| = p^n$, $[G : C_G(h_i)]$ are all powers of p (since they divide $|G|$). This is then either one of a multiple of p. Modding out by p on both sides of the class equation gives:

$$0 \equiv |Z(G)| \mod p$$

Because $1 \in Z(G)$, we know the right hand side has at least one element. Therefore it has at leas tP elements because it is divisible by p. Thus there is more than one element in the center and we're done!

Proposition IV.0.2

All groups of order p^2 (for p a prime) are abelian.

Proof. Note that $Z(G)$ is nontrival, so $|Z(G)| = p$ or $|Z(G)| = p^2$ by Lagrange's theorem. If $|Z(G)| = p^2$ then $Z(G) = G$ and we're done. Thus we just need to see that something goes wrong if $|Z(G)| = p$.

Take some element $g \in G \setminus Z(G)$, we know that g commutes with itself and commutes with $Z(G)$. Thus $C_G(g) \supseteq \langle Z(G), g\rangle \supsetneq Z(G)$. Because $|C_G(g)| \mid |G| = p^2$ and $|C_G(g)| > p$, we then know that $|C_G(g)| = p^2$. Thus $g \in Z(G)$. Contradiction!

Definition IV.0.2

A Sylow p-subgroup is a subgroup of G of order p^n where $|G| = p^n m$ with $p \nmid m$.

Theorem IV.0.3

If G is a finite group, and $p^k \mid |G|$ where p is prime and $k > 0$ then G has a subgroup of order p^k. Furthermore

- Any two Sylow p-subgroups of G are conjugate.
- Any p-subgroup of G is contained in a Sylow p-subgroup of G.
- The # of Sylow p-subgroups divides $|G|$ and is $\equiv 1 \mod p$.

Proof. Say $p^k \mid |G|$ and write $|G| = p^n m$ for $p \nmid m$. The proof proceeds via acting on a clever set.

Let S be the set of subsets of G of size p^k. G acts on S by left multiplication.

$$g \cdot T = \{gt \mid t \in T\}.$$

Goal: Show there exists a $T \in T$ such that G_T has order p^k.

The first thing to notice is that this is the largest possible order of any stabilizer. Why? Well for any $t \in T \in S$, we know $G_T \cdot t \subseteq T$. Thus because $|G_T \cdot t| = |G_T|$ we have $|G_T| \leq |T| = p^k$.

Therefore by orbit-stabilizer we know

$$|\mathcal{O}_T| = \frac{|G|}{|G_T|}$$

this is divisible by p^{n-k}, and this is the smallest power of p dividing $|\mathcal{O}_T|$ (prime factorization). We want to show there exists T such that $|\mathcal{O}_T|$ is not divisible by p^{n-k+1}.

Consider the orbits $\mathcal{O}_T$ for varying T's. These form a partition of S. So we'll show $|S|$ is not divisible by p^{n-k+1}, and so we have to have some T so that $|\mathcal{O}_T|$ is not divisible by p^{n-k+1}. Thus $p^k \mid |G|_T$ and $|G_T| = p^k$.

Claim

The largest power of p dividing $|S|$ is p^{n-k}.

Well, we see that

$$\begin{aligned} |S| = \binom{|G|}{p^k} = \binom{p^n m}{p^k} &= \frac{(p^n m)(p^n m - 1) \cdots (p^n m - p^k + 1)}{p^k(p^k - 1) \cdots (p^k - p^k + 1)} \\ &= (p^{n-k} m) \prod_{i=1}^{p^k - 1} \frac{p^n m - i}{p^k - i} \end{aligned}$$

If $i = p^\ell j$ for $p \nmid j$ then

$$\begin{aligned} p^k - i = p^k - p^\ell j = p^\ell (p^{k-\ell} - j) \\ p^n m - i = p^n m - p^\ell j = p^\ell (p^{n-\ell} m - j) \end{aligned}$$

Both $p^{k-\ell} - j$ and $p^{n-\ell} m - j$ are coprime to p, so $p^k - i$ and $p^n m - i$ are divisible by exactly rhe same powers of p. Thus $|S| = p^{n-k} \cdot$ (some # coprime to p).

This is an awful way to prove this fact. Lets do it in a better way. A better proof is that $\binom{pa}{pb}$ is the coefficient of x^{pb} in $(x+1)^{pa}$. Thus in $\mathbb{Z}/p\mathbb{Z}$ we have

$$\begin{aligned}(x+y)^p &= x^p + y^p \\ (x+1)^{pa} &= (x^p+1)^a.\end{aligned}$$

Thus the coefficient of x^{pb} is $\binom{a}{b}$. Therefore

$$\binom{pa}{pb} \equiv \binom{a}{b} \mod p$$

This proves the existence of p-subgroups.

Now we prove that any two Sylow p-subgroups are conjugate and any p-subgroup of G is contained in a Sylow p-subgroup of G. We first need a lemma.

Lemma IV.0.4

If H is a p-group acting on a set X then $|X| = (\#\text{ of fixed points of } H) \mod p$.

X is a union of disjoint H-orbits, each H-orbit has size dividing $|H|$, so this size is a power of p. The number of length-1 orbits is then equivalent to $|X| \mod p$, and we're done.

We now show that for any p-subgroup H of G and any Sylow p-subgroup J of G that there exists $g \in G$ such that $g^{-1}Hg \leq J$.

H acts on G/J by multiplication $h \cdot (gJ) = hgJ$. Since J is a Sylow p-subgroup, $|G/J|$ is coprime to p. Thus the # of fixed points of H on G/J is nonzero (because it is coprime to p).

This says there exists a $g \in G$ such that $HgJ = gJ$. Thus $g^{-1}HgJ = J$. Therefore $g^{-1}Hg \subseteq J$.

Finally we need to show that the number of Sylow p-subgroups divides $|G|$ and is $\equiv 1 \mod p$. Let A be the set of all Sylow p-subgroups. G acts on A by conjugation. This action is transitive (i.e., has one orbit). Pick a Sylow p-subgroup J. Then by orbit-stabilizer

$$|A| = |\mathcal{O}_J| = [G : G_J] = \frac{|G|}{|G_J|}$$

Thus $|A| \mid |G|$. Furthermore, note that $J \subseteq G_J$, so $p^n \mid |G|_J$. Therefore $|A|$ is coprime to p. Now we need to see that it is $\equiv 1 \mod p$.

Well, restrict the action so that J is acting on A. It then suffices to determine the fixed points, which we claim is just $J \in A$. Well

$$\begin{aligned} J \text{ fixes some } H \in S &\iff jHj^{-1} = H \quad \forall\, j \in J \\ &\iff J \subseteq N_G(H) && \text{(i.e., normalizer of } H \text{ in } G) \end{aligned}$$

H and J are now Sylow p-subgroups of $N_G(H)$. Thus they are conjugate in$N_G(H)$. But wait! Then $J = xHx^{-1} = H$ for some $x \in N_G(H)$. Perfect!

Thus there is one fixed point, and by the lemma $|A| \equiv 1 \mod p$. ♥

IV.1. Applications of Sylow's Theorems

> **Proposition IV.1.1**
>
> We have the following applications of Sylow's theorems
>
> (1) If p, q are distinct primes with $p > q$, then no group of order $p^a q$ can be simple ($a > 0$).
>
> (2) There are no simple groups of order 12
>
> (3) If $|G| = 28$ and G has a normal Sylow 2-subgroup then G is abelian.
>
> (4) There are no simple groups G of order 120.

Proof of (1). Let H be a Sylow p-subgroup, so $|H| = p^a$. The number of Sylow p-subgroups is $\equiv 1 \mod p$ and divides q. Because $p > q$ this implies that the number of Sylow p-subgroups is one.

Thus H is normal in this group, and it is not simple. ♥

Proof of (2). Consider the # of Sylow 3-subgroups divides 4 and is $1 \mod 3$. Thus it's 1 or 4. If there is 1 then the Sylow 3-subgroup is normal and G is not simple.

If there are 4 Sylow 3-subgroups, then since these groups have prime order and have trivial intersection, G has $4 \cdot 2 = 8$ order three elemenets. This leaves three elements of G having order not 1 or 3. But any Sylow 2-subgroup of G contains 3 elements having order not 1 or 3. Thus there is exactly on Sylow 2-subgroup, and it is normal. ♥

Proof of (3). The # of Sylow 7-subgroups divides 4 and is $1 \mod 7$, so there is only one Sylow 7-subgroup. Thus we have a normal Sylow 2-subgroup N and a normal Sylow 7-subgroup H. Their orders are coprime so $N \cap H = 1$. Thus from homework

$$G = \langle N, H \rangle = NH \cong N \times H.$$

All groups of order 4 and order 7 are abelian, and direct products of abelian groups are abelian. Thus G is abelian. ♥

Proof of (4). The # of Sylow 5-subgroups divides 24 and is $1 \mod 5$, so it's 1 or 6. If it's one then G is not simple.

So assume the # of Sylow 5-subgroups is 6. G acts transitively by conjugation on these 6 Sylow 5-subgroups. This yields a homomorphism $\varphi G \to S_6$. Under the assumption that G is simple, the kernel must be trivial (as G doesn't fix the Sylow 5-subgroups).

Thus $G \cong \operatorname{im} \varphi$. Since $A_6 \trianglelefteq S_6$ we know that $\varphi(G) \cap A_6 \trianglelefteq \varphi(G)$. But then we have

$$[\varphi(G) : \varphi(G) \cap A_6] \leq 2.$$

Thus $\varphi(G) \subseteq A_6$, or else we would have that $\varphi(G) \cap A_6$ is a nontrivial normal subgroup.

But then by comparing sizes $[A_6 : \varphi(G)] = 3$. Then A_6 acts by left multiplication on $A_6/\varphi(G)$, which gives a homomorphism $A_6 \to S_3$. Because A_6 is bigger than S_3, this has a nontrivial kernel. Thus the kernel must be A_6 beause A_6 is simple. But the left-multiplicaiton action is transitive, so it can't be trivial. ♥

> **Definition IV.1.1**
>
> Say a subgroup G of S_n is k-transitive (for $k \leq n$) if G acts transitively on the set of k-tuples of pairwise distinct elements of $\{1, \ldots, n\}$.

> For example, if G is 2-transitive, this means G is transitive on the set of pairs $\{(i, j) \in \{1, \ldots, n\}^2 \mid i \neq j\}$. I.e. for all $i, j, k, \ell \in \{1, \ldots, n\}$ with $i \neq j$ and $k \neq \ell$ there exists a $g \in G$ with $g \cdot i = k$ and $g \cdot j = \ell$.

Here are some theorems about k-transitivity, all of which rely on the classification of finite simple groups.

> **Theorem IV.1.2**
>
> If $G \leq S_n$ is 6-transitive (or k-transitive for any $k \geq 6$), then $G = A_n$ $(n \geq 8)$ or S_n $(n \geq 6)$.
>
> Note that A_n is $(n-2)$-transitive and S_n is n-transitive.
>
> If $G \leq S_n$ is 5-transitive then $G = A_n$ $(n \geq 7)$, or S_n $(n \geq 5)$, or M_{23} $(n = 23)$, or M_{11} $(n = 11)$.
>
> These $M_{\_}$ are some sporadic simple groups discovered by Matthew.
>
> If $G \leq S_n$ is 4-transitive then $G = A_n$ $(n \geq 6)$, S_n $(n \geq 4)$, and four small groups in low degree.
>
> For 3-transitive and 2-transitive groups there are infinite families but the list is small enough to be tractable. Namely for 2-transitive groups we have if $G \leq S_n$ is 2-transitive
>
> - $G = A_n$ $(n \geq 4)$
> - $G = S_n$ $(n \geq 2)$
> - $\mathrm{PSL}_d(q) \leq G \leq \mathrm{Aut}(\mathrm{PSL}_d(q))$ acting on $\mathbb{P}^d(\mathbb{F}_q)$ for $n = \frac{q^d-1}{q-1}$
> - Similar description with $\mathrm{PSU}_3(q0$ for $n = q^3 + 1$.
> - Similar description with $\mathrm{PSp}_{2k}(2)$ for $n = 2^{2k-1} \pm 2^{k-1}$
> - Two other small families.
> - Seven sporadic small simple groups.
> - A few others
>
> If G is a transitive subgroup of S_p (for p prime) then $G = S_p$ or A_p or
>
> $$G \leq \mathrm{AGL}_1(\mathrm{p}) = \{x \mapsto ax + b \mid a, b \in \mathbb{Z}/p\mathbb{Z}, a \neq 0\}$$
>
> unless $p = 11, 23, \frac{q^d-1}{q-1}$ for $d \geq 2$ or q a prime power.
>
> Then also the doubly transitive ones.

> **Claim**
>
> $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has a cyclic subgroup of order $p^2 - 1$.

Proof. Idea: construct a field $\mathbb{F}_{p^2}$ of order p^2 and identify $\mathbb{F}_{p^2}$ with $(\mathbb{Z}/p\mathbb{Z})^2$. Then $\mathrm{GL}_1(\mathbb{F}_{p^2}) \leq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and $\mathrm{GL}_1(\mathbb{F}_{p^2}) \cong C_{p^2-1}$ so we're done.

For $p = 3$ we set $F_9 = (\mathbb{Z}/3\mathbb{Z}) + (\mathbb{Z}/3\mathbb{Z})i$ where $i^2 = -1$. Also, lets denote $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$. Another way to see this is

$$\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 1)\mathbb{F}_3[x]$$

We will prove in 494 that if k is a field and $p(x)$ is an irreducible polynomial then $k[x]/p(x)k[x]$ is a field. The key ideas are the same as the ideas used to prove $\mathbb{Z}/p\mathbb{Z}$ is a field–the division algorithm!!!

In general, if p is odd then the squaring map $\mathbb{F}_p \to \mathbb{F}_p$ is not injective because $(-1)^2 \equiv_p 1^2$, and so it cannot be surjective. Pick some $d \in \mathbb{F}_p$ without a square root. Then of course $x^2 - d$ is an irreducible polynomial (as it has no roots). We then take

$$\mathbb{F}_{p^2} := \mathbb{F}_p[x]/(x^2 - c)\mathbb{F}_p[x]$$

Every $f \in \mathbb{F}_p[x]$ can be written in exactly one way as

$$f(x) = q(x) \cdot (x^2 - d) + r(x)$$

where $q, r \in \mathbb{F}_p[x]$ and $\deg r \leq 1$. Then each coset contains exactly one polynomial of degree ≤ 1. There are then p^2 ways to pick the coefficients and $\left|\mathbb{F}_{p^2}\right| = p^2$. (Note: $\mathbb{F}_{p^2} \cong C_p \times C_p$ as a group under addition).

Now we need the multiplication, both that it's well-defined and it is invertible. Start with

$$f_1(x) \equiv f_2(x) \mod x^2 - d g_1(x) \equiv g_2(x) \mod x^2 - d$$

where $f_1, f_2, g_1, g_2 \in \mathbb{F}_p[x]$. Then we should show that $f_1(x)g_1(x) \equiv f_2(x)g_2(x) \mod x^2 - d$. To do this we see that for some $A, B \in \mathbb{F}_p[x]$ we have

$$\begin{aligned} f_1(x) &= f_2(x) + (x^2 - d)A(x) \\ g_1(x) &= g_2(x) + (x^2 - d)B(x) \\ f_1(x)g_1(x) &= f_2(x)g_2(x) + (x^2 - d)(f_2(x)B(x) + A(x)g_2(x)) + (x^2 - d)^2 A(x)B(x) \end{aligned}$$

And thus the multiplication is well-defined, commutative, associative, distributes with respect to addition, and has an identity element 1 because these hold in $\mathbb{F}_p[x]$.

Now we show it has multiplicative inverses. This is clear for nonzero elements of $\mathbb{F}_p$. Now we want to find the inverse of $c + \overline{x}$, where $\overline{x}$ is the image of x in $\mathbb{F}_{p^2}$. Well

$$(c + \overline{x})(c - \overline{x}) = c^2 - \overline{x}^2 = c^2 - d \in \mathbb{F}_p$$

and this is nonzero as d is not a square in $\mathbb{F}_p$. We then have that

$$(c + \overline{x}) \cdot \frac{c - \overline{x}}{c^2 - d} = 1$$

Similarly, $a + b\overline{x}$ has an inverse in $\mathbb{F}_{p^2}$ for $b \neq 0$, as we can multiply by b^{-1} and then multiply by the inverse of $\frac{a}{b} + \overline{x}$.

♥

> **Proposition IV.1.3**
>
> If k is a finite field with n elements then $k^\times$ is a cyclic group of order $n - 1$.

Proof. Fact: In $k[x]$ for any field k a degree-n polynomial has at most n roots. The reason being that for c a root

$$f(x) = (x - c)g(x) + r$$

where $r \in \mathbb{F}_p$, this implies since $f(c) = 0$ that $r = 0$. Then if $c \neq c'$ and $f(c) = f(c')$ then

$$f(c') = (c' - c)g(c')$$

And so $g(c') = 0$, and we can factor it as well. Because degrees add when multiplying this implies the fact.

In C_{n-1} all elements have order dividing $n - 1$, and the # of elements of order dividing d (for any d dividing $n - 1$) is d.

In $k^\times$, all elements have order dividing $n-1$, and if $d \mid n-1$ then every $c \in k^\times$ of order dividing d is a root of $x^d - 1$. But this means there are at most d elements of order dividing d in $k^\times$.

Now we just compare.

C_{n-1}	Both	$k^\times$
	size $= n-1$	
	all elements have order dividing $n-1$	
exactly d elements of order dividing d		at most d elements of order dividing d

It follows that C_{n-1} and $k^\times$ have the same number of elements of each order. Thus $k^\times$ has an element of order $n-1$ and hence is cyclic.

V. Midterm Review

There is a good list of review problems located at

http://www.math.kent.edu/ white/qual/list/group.pdf

For these review problems you should know the following definitions.

Definition V.0.1

For two elements $g, h \in G$, their commutator $[g,h] = ghg^{-1}h^{-1}$. If $[g,h] = 1$ then g, h commute. The commutator subgroup $[G,G] = G'$ of G is generated by the commutators. This is the smallest normal subgroup of G so that G/G' is abelian.

Theorem V.0.1 (Jordan-Hölder)

If G is a group and $N_0 = G \trianglerighteq N_1 \trianglerighteq N_2 \cdots \trianglerighteq N_k = 1$ is a chain so that N_{i+1} is a maximal normal subgroup in N_i, then the successive quotients N_i/N_{i+1} are simple. Furthermore, the sequence $N_0/N_1, N_1/N_2, \ldots, N_{k-1}/N_k = N_{k-1}$ depends only on the group G (up to reordering).

This should be thought of as an analogue of

Definition V.0.2

A group G is called solvable if the simple groups coming from the Jordan-Hölder Theorem are all cyclic groups of prime order.

V.1. Some Cool Stuff

Theorem V.1.1 (From Homework)

Let G be a finite group, then every minimal (nontrivial) normal subgroup of G is isomorphic to $L \times \cdots \times L$ for some simple group L.

A consequence: every minimal normal subgroup of a minimal normal subgroup of G is simple.

Fact: if a subgroup G of S_n is doubly transitive (i.e., G acts transitively on $\{(i,j) \mid i \neq j \; 1 \leq i,j \leq n\}$), then G has exactly one minimal normal subgroup N, which is either $(C_p)^k$ or a nonabelian simple group.

We have $\rho : G \to \mathrm{Aut}(N)$ by conjugation whose kernel K is a normal subgroup of G. If $K = 1$, then ρ is injective and it induces an isomorphism $G \to \rho(G) \le \mathrm{Aut}(N)$, so we can understand G by understanding subgroups of $\mathrm{Aut}(N)$.

If N is nonabelian, then $K = 1$. Why? If $K \neq 1$, then K is a nontrivial normal subgroup of G, so it contains the minimal normal subgroup N. But then this would show N is abelian.

If G is doubly transitive then either $L \le G \le \operatorname{Aut} L$ for some nonabelian simple L, or $N \cong C_p^k$. In this case, $\mathbb{F}_p^k \le G \le \mathrm{AGL}_k(\mathbb{F}_p)$. Where

$$\mathrm{AGL}_k(\mathbb{F}_p) = \{\vec{x} \mapsto A\vec{x} + \vec{b} \mid \vec{A} \in \mathrm{GL}_k(\mathbb{F}_p), \vec{b} \in \mathbb{F}_p^k\}$$

V.2. **Main Takeaways**

Here are some of the main takeaways from the class.

- Subgroups of $\mathbb{Z}$ and cyclic groups Definition II.1.6.
- Subgroups and Cosets. See Definition II.1.3 and Definition II.1.4.
- Lagrange's Theorem: $H \le G \implies |H|\,|G/H| = |G|$ (cosets). See Theorem II.1.2
- Normal subgroups + kernels are the same. Normal subgroups $\sim$ factors. See Definition II.1.12, Definition II.1.11
- Simple groups. See Definition II.1.13.
- Quotient Groups, Correspondence Theorem, first isomorphism theorem. See Theorem II.2.5 and Theorem II.2.6
- Actions and Orbit-Stabilizer (action by conjugation, action on the cosets, etc.). See Definition III.1.1, Definition III.1.5, Definition III.1.4, and Theorem III.1.3
- Sylow's Theorems, including Cauchy's theorem (order p elements). See Theorem IV.0.3
- Direct and semidirect products (see homework).
- Second and Third Isomorphism Theorem. See Piazza Post.

The idea of semi-direct products

- Internal: G is the internal semi-direct product of $N \trianglelefteq G$ by $H \le G$ (written $G = N \rtimes H$) if N is normal in G, H is a subgroup of G, $N \cap H = 1$, and $G = \langle N, H\rangle$.

  In this case $G = NH$, and the action $\varphi : H \to \mathrm{Aut}(N)$ by conjugation provides all the information about how to multiply elements of N and H together.
- External: If H, N are groups and $\varphi : H \to \mathrm{Aut}(N)$ is homomorphism, then there is a group G (unique up to isomorphism) with subgroups $\overline{N} \cong N$, $\overline{H} \cong H$, such that $G = \overline{N} \rtimes \overline{H} = N \rtimes_\varphi H$ where $\overline{H} \to \mathrm{Aut}(\overline{N})$ by conjugation is identified with φ via $N \cong \overline{N}$, $H \cong \overline{H}$.
- Morally/How to Use: If $N \trianglelefteq G, H \le G, N \cap H = 1, G = \langle N, H\rangle$, then we can understand G entirely by understanding the action $H \to \mathrm{Aut}(N)$ by conjugation. We may also understand it by understanding all homomorphisms $\varphi : H \to \mathrm{Aut}(N)$, since $G \cong N \rtimes_\varphi H$ (external) for some φ. This is often used to classify things.

Note: $N \rtimes_\varphi H \cong N \rtimes_\psi H$ (external) if $\operatorname{im}\varphi$ and $\operatorname{im}\psi$ are conjugates. Many people proved this on Homework #5 and Homework #6. This is fully citeable.

Idea of semi-direct products: If $N \trianglelefteq G$, $H \leq G$, $N \cap H = 1$, $G = \langle N, H \rangle$ then (internal semidirect product) $G = N \rtimes H = NH$. This tells us we can understand G by understanding the actions $H \to \operatorname{Aut}(N)$ (internally by conjugation, externally more generally, say when classifying).

VI. **Applications of Group Theory**

VI.1. **Polynomials**

If $f(x) \in \mathbb{C}[x]$ has degree n, then the function $f : \mathbb{C} \to \mathbb{C}$ is n-to-1 over all but finitely many values (since $f(x) - c$ has n distinct roots unless c is a critical value of $f(x)$).

For each critical value c, let $E_f(c)$ be the collection (multiset) of multiplicities of the roots of $f(x) - c$. I.e.,

$$f(x) - c = \alpha \cdot \prod_{i=1}^{k} (x - \gamma_i)^{e_i}$$

with $\gamma_i \neq \gamma_j$, $e_i > 0$, then $E_f(c) = [e_1, e_2, \ldots, e_k]$. Note that $\sum_i e_i = n$.

Thus $E_f(c)$ is a partition of n, and $E_f(c) \neq [1, 1, \ldots, 1]$ if and only if c is a critical value of f.

Questions:

(1) For a degree n $f(x) \in \mathbb{C}[x]$, what are the possibilities for the collection of pairs

$$(c_1, E_f(c_1)), \ldots, (c_\ell, E_f(c_\ell))$$

where $c_1, \ldots, c_\ell$ are the critical values of f.

There is no known algebraic proof of this.

(2) For a given choice of this data (the collection of pairs), how many corresponding f's are there.

(3) The analogous questions for rational functions are open.

Definition VI.1.1

For $f(x) \in \mathbb{C}[x] \setminus \mathbb{C}$, and $a \in \mathbb{C}$. Define $m_a(f)$ (the "multiplicity of a as a root of $f(x)$") to be the largest integer $k \geq 0$ such that $(x - a)^k$ divides $f(x)$.

Equivalently this says that $m_a(f)$ is the largest k such that $f(a), f'(a), \ldots, f^{(k-1)}(x) = 0$, or equivalently that this is the smallest $k \geq 0$ such that $f^{(k)}(a) \neq 0$.

Theorem VI.1.1 (Riemann-Hurwitz)

If $f(x) \in \mathbb{C}[x]$ has degree n, then $n - 1 = \sum_{c \in \mathbb{C}} (n - |E_f(c)|) = \sum_{c \in \mathbb{C}} (n - \left|f^{-1}(c)\right|)$.

Proof. We count in two ways

$$\begin{aligned} n - 1 = \deg(f'(x)) &= \sum_{a \in \mathbb{C}} m_a(f'(x)) \\ &= \sum_{a \in \mathbb{C}} (m_a(f(x) - f(c)) - 1) \\ &= \sum_{c \in \mathbb{C}} \sum_{a \in f^{-1}(c)} (m_a(f(x) - c) - 1) \\ &= \sum_{c \in \mathbb{C}} (\deg(f(x) - c) - \left|f^{-1}(c)\right|) = \sum_{c \in \mathbb{C}} (n - \left|f^{-1}(c)\right|). \end{aligned}$$

Great!

Answers to questions **??**.

(1) Answered by Thom. Exactly the collections $(c_1, P_1), \dots, (c_\ell, P_\ell)$ where $c_1, \dots, c_\ell \in \mathbb{C}$ are distinct, $P_1, \dots, P_\ell$ are partitions of n, $P_1 \neq [1, 1, \dots, 1]$ for all i such that

$$n - 1 = \sum_{i=1}^{\ell} (n - |P_i|).$$

(2) Given distinct $c_1, \dots, c_\ell \in \mathbb{C}$ and partitions $P_1, \dots, P_\ell$ of n satisfying $P_i \neq [1, 1, \dots, 1]$ and $n - 1 = \sum_{i=1}^{\ell} (n - |P_i|)$, then the # of degree n $f(x) \in \mathbb{C}[x]$ with $E_f(c_i) = P_i$, up to $f(x) \sim f(ax + b)$ ($a \in \mathbb{C}^\times, b \in \mathbb{C}$), that is up to linear changes of variable, is

the # of equivalence claseses of tuples $(g_1, \dots, g_\ell)$ of elements o S_n such that P_i is the collection of cycle lengths of g_i and $g_1 g_2 \cdots g_\ell$ is an n-cycle, where $(g_1, \dots, g_\ell) \sim (\sigma g_1 \sigma^{-1}, \dots, \sigma g_\ell \sigma^{-1})$ for $\sigma \in S_n$.

For rational functions if $f(x) \in \mathbb{C}(x)$ has degree n then

$$2n - 2 = \sum_{c \in \mathbb{C}_\infty} (n - |E_f(c)|) = \sum_{c \in \mathbb{C}_\infty} \left(n - \left|f^{-1}(c)\right|\right)$$

People believe that this is the main constraint, but it is not true that it is the <u>only</u> contraint.

But it's not true that $P_1, \dots, P_\ell$ are partitions of n such that $\sum_{i=1}^{\ell} (n - |P_i|) = 2n - 2$ then $\exists$ $f(x)$ such that $E_f(c_i) = P_i$.

e.g. $[2, 2], [2, 2], [1, 3]$ doesn't occur.

<u>Fact</u>: Given distinct $c_1, \dots, c_\ell \in \mathbb{C}_\infty$ and partitions $P_1, \dots, P_\ell$ of n such that

$$2n - 2 = \sum_{i=1}^{\ell} (n - |P_i|),$$

Then the # of $f(x) \in \mathbb{C}(x)$ such that $E_f(c_i) = P_i$ for all i modulo the equivalence relation $f \sim f \circ \mu$, $\deg \mu = 1$ is exactly the # of $(g_1, \dots, g_\ell)$ elements of S_n such that

- P_i is the collection of cycle lengths of g_i.
- $g_1 \cdots g_\ell = 1$.
- The group generated by the g_i is transitive.

VII. Representation Theory

We will study groups via their actions on vector spaces over $\mathbb{C}$. Namely via group homomorphisms $G \to \mathrm{GL}(V)$, where V is some vector space over $\mathbb{C}$.

VII.1. Review of Linear Algebra (over $\mathbb{C}$)

Definition VII.1.1

A <u>vector space</u> V is an abelian group (under $+$) with an operation $(c, v) \mapsto cv$ for $c \in \mathbb{C}$ and $v \in V$ such that

$$c(dv) = (cd)v$$

$$c(v+w) = cv + cw$$
$$(c+d)v = cv + dv$$
$$1v = v$$

Example VII.1.1

$V = \mathbb{C}^n$ under the standard rules of the game.

Definition VII.1.2

A subspace of V is a subset of V which is a vector space under the induced $+, \cdot$. That is a subgroup of $(V, +)$ which is preserved by multiplication by $\mathbb{C}$.

Definition VII.1.3

A sequence $v_1, \dots, v_n$ of vectors in a vector space V is linearly independent if

$$c_1 v_1 + \cdots + c_n v_n = 0 \iff c_1, \dots, c_n = 0$$

Definition VII.1.4

A sequence $v_1, \dots, v_n$ of vectors in V spans V provided that

$$V = \{c_1 v_1 + \cdots + c_n v_n \mid c_1, \dots, c_n \in \mathbb{C}\}.$$

Definition VII.1.5

$v_1, \dots, v_n$ is a basis of V if $v_1, \dots, v_n$ is linearly independent and spans V (i.e., every $v \in V$ can be written as a linearly combination of $v_1, \dots, v_n$ in exactly one way).

Proposition VII.1.1

Any two bases of V have the same size which we call the "dimension of V" and write $\dim V$. Moreover any linearly independent sequence in V can be extended to yield a basis of V. Likewise any spanning sequence then some subsequence is a basis.

Definition VII.1.6

A linear transformation $T : V \to W$ between two vector spaces V, W is a homomorphism of additive groups which respects scalar multiplication. That is for $v, w \in V$ and $c \in \mathbb{C}$ we have

$$T(cv) = cT(v)$$
$$T(v+w) = T(v) + T(w).$$

Naturally we have notions of kernel and image, these turn out to be vector subspaces (as they should be).

Definition VII.1.7

$\operatorname{nullity} T := \dim \ker(T)$ (i.e., the nullity of T) and $\operatorname{rank}(T) := \dim \operatorname{im}(T)$ (i.e., the rank of T)

Theorem VII.1.2 (Rank-Nullity)

We have for any linear transformation $T : V \to W$ that

$$\operatorname{rank}(T) + \operatorname{nullity}(T) = \dim V.$$

A linear transformation $T : \mathbb{C}^n \to \mathbb{C}^m$ has the form $v \mapsto Av$ for some $m \times n$ matrix A in $\mathbb{C}$. This holds because a linear transformation is exactly determined by the values it takes on a basis, and $\mathbb{C}^n$ has a standard basis

$$(e_i)_j = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

That is e_i has a 1 in the i-th position and zeroes elsewhere

$$e_2 = (0, 1, 0, \dots, 0).$$

In fact we can do a similar thing for any linear transformation $T : V \to W$ given finite bases $\mathbb{v}$, $\mathbb{w}$ of the domain and codomain.

If $v_1, \dots, v_n$ is a basis of $\mathbb{C}^n$, and $T : v \mapsto Av$ is a linear transformation $\mathbb{C}^n \to \mathbb{C}^n$ then the matrix for T with respect to the basis $v_1, \dots, v_n$ is $C^{-1}AC$ where $C = \begin{bmatrix} v_1 & v_2 & \cdots & v_n \end{bmatrix}$.

$$\text{usual coords} \qquad Cv \xrightarrow{A} ACv \mathbb{v} \text{ coords} \qquad v \xrightarrow[C^{-1}Ac]{} Tv$$

This is referred to as "change-of-basis."

Definition VII.1.8

If A is an $m \times n$ matrix then the tranpose A^T of A is a $n \times m$ matrix defined by

$$(A^T)_{ij} = A_{ji}.$$

Definition VII.1.9

There is a unique function $\det : \{n \times n \text{ matrices}\} \to \mathbb{C}$ such that

- $\det(\mathrm{Id}) = 1$
- det is linear in each individual row of the matrix. (aka multilinear in the rows).
- $\det(A) = 0$ if two adjacent rows of A are equal.

This is called the determinant.

This has the following key properties

$$\det(AB) = (\det A)(\det B)$$

if A, B are $n \times n$ matrices. It follows that

$$\det(C^{-1}AC) = \det A$$

if C is invertible. Therefore $\det T$ for $T : V \to W$ is well-defined for a linear transformation $T : V \to W$. A useful property is that

$$\det \begin{bmatrix} a_{11} & * & * & * \\ 0 & a_{22} & * & * \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix} = a_{11}a_{22}\cdots a_{nn}$$

We also have the cofactor expansion formula, which says that if

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}.$$

then

$$AC^T = (\det A) \cdot \mathrm{Id}_n .$$

where C is the cofactor matrix and C^T is its transpose. C's ij-th entry is $(-1)^{i+j} \cdot \det M_{ij}$ with M_{ij} a matrix gotten from A by removing the i-th row and j-th column.

This shows us that A is invertible if and only if $\det A \neq 0$.

Definition VII.1.10

If $T : V \to V$ is a linear transformation then an eigenvector for T is some nonzero $v \in V$ such that

$$Tv = \lambda v$$

for some $\lambda \in \mathbb{C}$. Then λ is called an eigenvalue.

Eigenvectors with distinct eigenvalues are automatically linearly independent.

If $\mathbb{v} = (v_1, \ldots, v_n)$ is a basis of V then the matrix of $T : V \to V$ with respect to this basis $\mathbb{v}$ is

$$\begin{bmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{bmatrix}$$

if and only if $T(v_i) = \lambda_i v_i$ (i.e., each v_i is an eigenvector with eigenvalue λ_i). This is called an eigenbasis of V for T.

Definition VII.1.11

The characteristic polynomial of a linear transformation $T : V \to V$ is $\det(T - \lambda \, \mathrm{Id}_V)$ for $\lambda \in \mathbb{C}$.

The eigenvalues are precisely the roots of this polynomial. There are n roots counting with multiplicity by the Fundamental Theorem of Algebra, as this will be a degree n polynomial.

Theorem VII.1.3 (Cayley-Hamilton)

A linear transformation $T : V \to V$ (likewise an $n \times n$ matrix A) satsifies its own characteristic polynomial (aka yields zero as a linear transformation [or $n \times n$ matrix]).

If the characteristic polynomial of A (an $n \times n$ matrix) has n distinct roots, then there is an eigenbasis for A.

Thus there exists an invertible $n \times n$ matrix C such that $C^{-1}AC$ is a diagonal matrix.

note also that if $Av = \lambda v$ then $A^k v = \lambda^k v$.

.

VII.2. The Basics

Definition VII.2.1

A linear representation of a group G on a vector space V is a homomorphism $\rho : G \to \mathrm{GL}(V)$ (where $\mathrm{GL}(V)$ is the group of invertible linear transformations $V \to V$).

This is also sometimes called a G-representation.

Definition VII.2.2

If $\rho : G \to \mathrm{GL}(V)$ is a linear representation then $\deg \rho := \dim \rho := \dim V$.

Example VII.2.1

Here are a few simple examples

- The trivial representation $g \overset{\rho}{\mapsto} \mathrm{Id}_V$.
- Representation of C_3 on $V = \mathbb{C}^3$ mapping

$$(123) \mapsto \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

- For any action of G on a finite set S, let V be a vector space with basis in bijection with S. Say the basis is e_s ($s \in S$). Where $\rho(g)$ maps $e_s \mapsto e_{g \cdot s}$. For example $S_3 \to \mathrm{GL}_3(\mathbb{C})$ via the action of S_3 on $\{1, 2, 3\}$. As another example, $D_4 \to \mathrm{GL}_4(\mathbb{C})$ via the action of D_4 on the vertices of a square.
- $D_4 \to \mathrm{GL}_2(\mathbb{R})$ via the action of D_4 on a square geometrically (center the square at $(0, 0)$), as reflections about a line through the origin and rotations about the origin are linear transformations.
- The sign representation of S_n is $\rho : S_n \to \mathrm{GL}_1(\mathbb{C})$ given by $\sigma \mapsto \mathrm{sgn}(\sigma)$.

Definition VII.2.3

The regular representation is the representation associated to the action of G on itself by left multiplication (dimension is $|G|$).

Definition VII.2.4

If V is a G-representation then a sub-representation of V is a subspace W of V which is G-invariant, that is $g \cdot W \subseteq W$.

A subspace W of V is a subrepresentation if and only if $\rho : G \to \mathrm{GL}(V)$ factors as

$$\begin{tikzcd}
G \arrow[rr, "\rho"] \arrow[dr, dashed] & & \mathrm{GL}(V) \\
& \{\psi \in \mathrm{GL}(V) \mid \psi(W) \subseteq W\} \arrow[ur, hook] &
\end{tikzcd}$$

Example VII.2.2

The following

- The trivial representation of G on V acts as the trivial representation of G on V acts as the trivial representation on every subspace of V
- The action of D_4 on $\mathbb{R}^2$ via rotations, but there is no 1-dimensional subspace of $\mathbb{R}^2$ which is D_4-invariant because of rotations.
- If G acts on a set S, then the linear representation of G on some V with basis S has a 1-dimensional invariant subspace

  $$V_1 := \mathbb{C}\left(\sum_s e_s\right).$$

  It induces the trivial representation on this subspace. There is also a $(|S|-1)$-dimensional invariant subspace given by

  $$V_{|S|-1} := V_1^{\perp} = \left\{\vec{v} \in V \mid \sum_s v_s e_s = 0\right\}.$$

  Note that the direct sum of these is all of V. All of the interesting behavior happens in $V_1^{\perp}$.
- If $G = D_4$, $S = \{1, 2, 3, 4\}$, and $V = \mathbb{C}^4$. Then V_3 has a G-invariant subspace $W = \mathrm{span}(e_1 - e_2 + e_3 - e_4)$. We can take the orthogonal complement of W in V_3 which is

  $$W^{\perp} := \left\{c_1 e_1 + \cdots + c_4 e_4 \mid \sum c_i = 0,\ c_1 - c_2 + c_3 - c_4 = 0\right\}$$

  This $W^{\perp}$ has no 1-dimensional G-invariant subspace (check!).

Definition VII.2.5

If V, W are G-representations then so is $V \oplus W$ via $g \cdot (v, w) = (g \cdot v, g \cdot w)$. In terms of matrices, for $\rho_V : G \to \mathrm{GL}(V)$ and $\rho_W : G \to \mathrm{GL}(W)$ then

$$g \mapsto \begin{bmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{bmatrix}$$

.

Example VII.2.3

We have

$$\begin{aligned} \rho_1 : C_2 &\to \mathbb{C}^{\times} \\ g &\mapsto 1 \\ \rho_{-1} : C_2 &\to \mathbb{C}^{\times} \\ g &\mapsto \mathrm{sgn}(g). \end{aligned}$$

Then $\rho_1 \oplus \rho_2$ is also a linear representation

$$\rho_1 \oplus \rho_{-1} : g \mapsto \begin{bmatrix} 1 & 0 \\ 0 & \operatorname{sgn}(g) \end{bmatrix}$$

Example VII.2.4

For any n-th root of unity $\zeta \in \mathbb{C}$ (that is $\zeta^n = 1$), we have a representation $\rho_\zeta : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^\times$ given by $i \mapsto \zeta^i$.

Definition VII.2.6

A representation is irreducible if it has no proper positive dimensional subrepresentations.

Definition VII.2.7

Two representations $\rho_V : G \to \mathrm{GL}(V), \rho_W : G \to \mathrm{GL}(W)$ are called isomorphic provided that there is an isomorphism $T : V \to W$ of vector spaces making the following diagram commute

$$\begin{tikzcd}
& G \arrow[ld, "\rho_V"'] \arrow[rd, "\rho_W"] & \\
\mathrm{GL}(V) \arrow[rr, "T \circ - \circ T^{-1}"'] & & \mathrm{GL}(W)
\end{tikzcd}$$

Put another way for every $g \in G$ we have

$$g \cdot T(v) = T(g \cdot v).$$

Or in other words a commutative diagram

$$\begin{tikzcd}
V \arrow[r, "\rho_V(g)"] \arrow[d, "T"'] & V \arrow[d, "T"] \\
W \arrow[r, "\rho_W(g)"'] & W
\end{tikzcd}$$

Recall: A linear representation of a group G is a homomorphism $\rho : G \to \mathrm{GL}(V)$ for some vector space V. We say ρ is irreducible if V has no subrepresentations except $\{0\}$ and V, where a subrepresentation is a subspace V of V such that $g \cdot W \subseteq W$ for all $g \in G$ (so that ρ induces a homomorphism $G \to \mathrm{GL}(W)$).

1-dimensional representations have the form $\rho : G \to \mathrm{GL}(\mathbb{C}) \cong \mathbb{C}^\times$. But if G is finite then $\rho(G)$ is a finite subgroup of $\mathbb{C}^\times$, hence is cyclic ($|G|$-th roots of unity). So ρ is a homomorphism from G to a cyclic group.

Theorem VII.2.1 (Maschke's Theorem)

Every finite-dimensional complex representation of a finite group G can be written as a direct sum of irreducible subrepresentations.

That is: given $\rho : G \to \mathrm{GL}(V)$ we can write $V = W_1 \oplus \cdots \oplus W_k$ with W_i subspaces of V such that each (ρ, W_i) is an irreducible subrepresentation of (ρ, V).

This follows from the following by induction

Theorem VII.2.2

If $\rho : G \to \mathrm{GL}(V)$ is a finite-dimensional complex representation of a finite group G and W is a subrepresentation, then there is some subrepresentation W' of V such that $V = W \oplus W'$.

> **Remark VII.2.1**
>
> Same proof works over any field K such that $|G|$ is invertible in K.

Proof. Pick any "projection map" $\pi : V \to W$, meaning a linear transformation $V \to W$ which restricts to the identity map on W. This can be done by extending a basis of W to a basis on V, defining π to be the identity on the basis of W and anything in W on the other basis elements for V.

We want to be able to take the kernel of π, but this won't work because π is not a G-invariant map. We have to somehow "fix" π.

Define

$$\begin{aligned} \phi : V &\to W \\ v &\mapsto \frac{1}{|G|} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot v). \end{aligned}$$

This should fix our problem

> **Claim**
>
> ϕ is a G-invariant projection map $V \to W$

Fix $w \in W$. Then $g^{-1} \cdot w \in W$ and we have:

$$\phi(w) = \frac{1}{|G|} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot w) = \frac{1}{|G|} \sum_{g \in G} g \cdot g^{-1} \cdot w = \frac{1}{|G|} \sum_{g \in G} w = w$$

It clearly maps into W. It is also linear since it is a linear combination of the linear transformations $v \mapsto g \cdot \pi(g^{-1} \cdot v)$.

We now check that ϕ is G-invariant. Let $h \in G$ and $v \in V$, then

$$\begin{aligned} h \cdot \phi(v) &= \frac{1}{|G|} \sum_{g \in G} h \cdot (g \cdot \pi(g^{-1} \cdot v)) \\ &= \frac{1}{|G|} \sum_{g' \in G} g' \cdot \pi((g')^{-1} h \cdot v) \\ &= \phi(h \cdot v) \end{aligned}$$

where we've made the subsitution $g' = hg$ (since $g \mapsto hg$ is a bijection $G \to G$).

This proves the claim. Now we need to show that $W' := \ker \phi$ satisfies the desired properties.

W' will clearly be a subrepresentation of V because ϕ is G-invariant. Then because ϕ is a projection map, $V = W \oplus W'$. Why? Well $v \in V$ has the form $\phi(v) + (v - \phi(v))$, $\phi(v) \in W$, and $v - \phi(v) \in W'$. This is a unique decomposition, as the intersection of W and W' is zero.

Great! This finishes the proof! ♥

> **Theorem VII.2.3**
>
> If V is a finite-dimensional complex representation of a finite group G, then V can be written in

exactly one way as an (internal) direct sum

$$V = V_1 \oplus \cdots \oplus V_k$$

where each V_i is itself a direct sum of (one or more) copies of an irreducible subrepresentation W_i and $W_i \ncong W_J$ for $i \neq j$.

This is a sort of generalization of eigenspaces. Said another way (more explicitly) if we write $V = U_1 \oplus \cdots \oplus U_\ell$ and $V = R_1 \oplus \cdots \oplus R_m$ with U_i, R_j irreducible subrepresentations, then they have the same length, for each i the number of U_j's isomorphic to U_i equals the number of R_j's isomorphic to U_i, and the direct sum of these U_j equals (not just isomorphic) the direct sum of these R_j.

Lemma VII.2.4

A homomorphism $\phi : V \to W$ between irreducible G-representations ie either zero or an isomorphism.

Proof. $\ker \phi$ is a subrepresentation of V. Thus $\ker \phi = 0$ or $\ker \phi = V$. If $\ker \phi = V$ then we're done.

$\operatorname{im} \phi$ is a subrepresentation of W. Thus $\operatorname{im} \phi = 0$ or $\operatorname{im} \phi = W$. If $\operatorname{im} \phi = 0$ we're done.

But if $\ker \phi = 0$ and $\operatorname{im} \phi = W$ then the function is bijective, and we're done.

Proof of Theorem VII.2.3. Now say $V = U_1 \oplus \cdots \oplus U_\ell = R_1 \oplus \cdots \oplus R_m$ with U_i, R_j irreducible subrepresentations of V.

Consider $U_i \hookrightarrow V \twoheadrightarrow R_j$ as inclusion then projection. This is a homomorphism of irreducible G-representations, and so it is either zero or an isomorphism by the lemma. However it can't be zero for all j, because $U_i \neq 0$ and $V = \bigoplus R_j$.

Thus there is some j such that $U_i \hookrightarrow V \twoheadrightarrow R_j$ is an isomorphism of G-representations. We get that the set of U_i's, up to $\cong$, equals the set of R_j's, up to $\cong$ (go the other way as well $R_j \to U_i$).

We may then write $V = U_1^{a_1} \oplus \cdots U_k^{a_k}$ and $V = R_1^{b_1} \oplus \cdots \oplus R_k^{b_k}$ where $a_i, b_i > 0$, $U_i \cong R_i$ irreducible, $U_i \ncong U_j$ for $i \neq j$.

Then consider that $U_1^{a_1} \hookrightarrow V \twoheadrightarrow R_2^{b_2} \oplus \cdots \oplus R_k^{b_k}$ is zero by the lemma. This shows $U_1^{a_1} \subseteq R_1^{b_1}$. Similarly $R_1^{b_1} \subseteq U_1^{a_1}$. Comparing dimensions gives $a_1 = b_1$. Can do similarly for the rest.

VII.3. Characters: The Power of the Trace

First a **warning**

For the remainder of representation theory we will work almost always with finite-dimensional complex representations over a finite group G

unless otherwise specified, this is assumed.

Definition VII.3.1

If $A = n \times n$ matrix then the trace of A (denoted $\operatorname{tr}(A)$) is the sum of the diagonal entries of A.

Key properties

- $\operatorname{tr}(AB) = \operatorname{tr}(BA)$
- $\operatorname{tr}(C^{-1}AC) = \operatorname{tr}(ACC^{-1}) = \operatorname{tr}(A)$.
- $\operatorname{tr}(A + B) = \operatorname{tr}(A) + \operatorname{tr}(B)$.

Thus the trace of a linear map $V \to V$ is defined.

Definition VII.3.2

Given a representation $\rho : G \to \mathrm{GL}(V)$, its character $\chi = \operatorname{tr} \circ \rho$, that is

$$\begin{aligned} \chi : G &\to \mathbb{C} \\ g &\mapsto \operatorname{tr}(\rho(g)). \end{aligned}$$

An irreducible character is a character of an irreducible representation

Fact: $\chi(hgh^{-1}) = \chi(g)$ because

$$\chi(hgh^{-1}) = \operatorname{tr}(\rho(h)\rho(G)\rho(h)^{-1}) = \operatorname{tr}(\rho(g)) = \chi(g).$$

. Thus χ is a "class function," meaning a function $G \to \mathbb{C}$ which is constant on each conjugacy class of G.

Further, $\rho_i : G \to \mathrm{GL}(V_i)$ $(i = 1, 2)$ then the character of $\rho_1 \oplus \rho_2$ is exactly $\chi_1 + \chi_2$. Thus the character of any finite-dimensional representation is the sum of the characters of finitely many irreducable characters.

Amazing Fact: We lose no information by replacing a finite-dimensional complex representation $\rho : G \to \mathrm{GL}(V)$ of a finite group G with its character $\chi : G \to \mathbb{C}$. Formally

Proposition VII.3.1

Two representations ρ_1, ρ_2 are isomorphic if and only if their characters are equal (as functions $G \to \mathbb{C}$).

Great Fact: The irreducable characters of a finite group G form a basis for the space of class functions on G. This implies that the number of irreducible representations of G (up to $\cong$) equals the # of conjugacy classes on G.

Definition VII.3.3

We can define an inner product on functions $\varphi, \psi : G \to \mathbb{C}$ via

$$\langle \varphi, \psi \rangle := \frac{1}{|G|} \cdot \sum_{g \in G} \varphi(g)\overline{\psi(g)}$$

where $\overline{z}$ is the complex conjugate of $z \in \mathbb{C}$. This is linear in the first component and antilinear in the second component as desired.

Furthermore $\langle \varphi, \varphi \rangle \in \mathbb{R}_{\geq 0}$ and $\langle \varphi, \varphi \rangle = 0 \iff \varphi = 0$.

Greater Fact: This basis of irreduciable characters for the space of class functions is orthonormal with respect to the above inner product.

Before we prove these facts we'll do some applications and examples

VII.3.1. Applications + Examples of Characters

If G acts on a finite set S, then the corresponding linear representation $\rho : G \to \mathrm{GL}(\mathbb{C}^{|S|})$ has character χ where

$$\chi(g) = \text{The \# of fixed points of } g \text{ on } S.$$

The character of the regular representation (that is G acting on G by left multiplication) is exactly

$$\chi(g) = \begin{cases} 0 & \text{if } g \neq 1 \\ |G| & \text{if } g = 1 \end{cases}$$

We will prove that every irreducible character occurs in the decomposition of the regular representation, and that the multiplicity says something about the dimension.

Example VII.3.1

The irreducible representations/characters of S_3 are

- The trivial representation $G \to \mathbb{C}^\times$ mapping $g \mapsto 1$ has $\chi_0 = 1$.
- The sign representation $G \to \mathbb{C}^\times$ given by $g \mapsto \operatorname{sgn}(g)$. Then

$$\begin{aligned} \chi_s : (123) &\mapsto 1 \\ (12) &\mapsto -1 \\ (1) &\mapsto 1. \end{aligned}$$

- A two-dimensional representation $G \to \mathrm{GL}(V)$ for $V = \{(a,b,c) \in \mathbb{C}^3 \mid a+b+c=0\}$, where G permutes the coordinates in V.

  This character χ satisfies $\chi + 1 = \chi_\sigma$, where χ_σ is the permutation representation of S_3 via the action on $\{1,2,3\}$. Thus

$$\begin{aligned} \chi : (123) &\mapsto -1 \\ (12) &\mapsto 0 \\ (1) &\mapsto 5 = |S_3| - 1 \end{aligned}$$

We may then check that

$$\begin{aligned} \langle \chi_0, \chi_0 \rangle &= \frac{1}{|G|} \sum_{g \in G} 1 = 1 \\ \langle \chi, \chi \rangle &= \frac{1}{6}(2(-1 \cdot \overline{-1}) + 3(0) + 1(4)) = 1 \\ \langle \chi_0, \chi \rangle &= \frac{1}{|6|}(2(-1) + 3(0) + 1(2)) = 0 \\ \langle \chi_s, \chi_s \rangle &= \frac{1}{6}(2(1) + 3(-1 \cdot \overline{-1}) + 1(1)) = 1 \\ \langle \chi_s, \chi \rangle &= \frac{1}{6}(2(-1) + 3(0) + 1(2)) = 0 \end{aligned}$$

There was a file system error erasing my notes for this day. Before I retype them, I do still have the pdf. Here it is!

Lemma .0.1

If $\rho : G \to \mathrm{GL}(V)$ is a finite-dimensional $\mathbb{C}$-representation of a finite group G and χ is the character of ρ, then the multiplicity of the trivial representation in any decomposition of ρ as the sum of irreducible representations is $(\chi_{\text{triv}}, \chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g)$

Using this, if ρ, χ is nontrivial/irreducible then $\sum_{g \in G} \chi(g) = 0$.

Proof. Let $V^G = \{v \in V \mid g \cdot v = v \ \forall g \in G\}$. This is the subspace of V on which ρ acts as the trivial representation.

Consider the G-equivariant projection $\pi : V \to V^G$ given by

$$v \mapsto \frac{1}{|G|} \sum_{g \in G} g \cdot v.$$

This is a G-equivariant linear projection $V \to V^G$, by the reindexing trick.

Thus $V = (\ker \pi) \oplus V^G$. We see that $\mathrm{tr}(\pi) = \dim V^G$ by block matrices. We can also compute the trace in terms of characters

$$\mathrm{tr}(\pi) = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

Theorem .0.2

If $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(W)$ are irreducible representations of G with characters χ and χ', then

$$(\chi, \chi') = \begin{cases} 1 & \text{if } \rho \cong \rho' \\ 0 & \text{otherwise} \end{cases}$$

Proof. This says that

$$\frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi'(g)} = \begin{cases} 1 & \text{if } \rho \cong \rho' \\ 0 & \text{otherwise} \end{cases}$$

Note from homework that $\chi\overline{\chi'}$ is the character of the induced representation on $\mathrm{Hom}(V, W)$. Thus we are looking for the number of copies of the trivial representation present in the induced representation on $\mathrm{Hom}(V, W)$. Namely

$$v \xmapsto{g \cdot \varphi} g \cdot \varphi(g^{-1} \cdot v)$$

φ is fixed by G when for all $g \in G$ we have $g \cdot \varphi(g^{-1} \cdot v) = \varphi(v)$. That is $\varphi(g^{-1} \cdot v) = g^{-1} \cdot \varphi(v)$. That is φ is fixed by G exactly when φ is a homomorphism of G-representations.

From homework, we know that because V, W are irreducible φ is either zero or an isomorphism (in which case it is a scalar times the identity). If $\rho \not\cong \rho'$ then $\varphi = 0$ so $(\chi, \chi') = 0$ as desired. If $\rho \cong \rho'$, then $\dim(\text{space of } \varphi) = 1$ because we are only varying the scalar.

This proves the claim!

Lemma .0.3

Let $f : G \to \mathbb{C}$ be a class function (i.e. a function which is constant on each conjugacy class of G. Let $\rho : G \to \mathrm{GL}(V)$ be a representation. Let $\varphi : V \to V$ be $\varphi = \sum_{g \in G} f(g)\rho(g)$.

If ρ is irreducible of $\deg n$ with character χ then φ is always scaling by $\frac{1}{n}\sum_{g\in G} f(g)\chi(g) = \frac{|G|}{n}(f, \overline{\chi})$.

Proof. φ is $\mathscr{C} - linear$ and G-invariant. Clearly φ is linear. To show invariance Consider that

$$\rho(g_\star) \circ \varphi = \sum_{g \in G} f(g)\rho(g_\star g) = \sum_{h \in G} f(g_\star^{-1} h)\rho(h)$$

$$\varphi \circ \rho(g_\star) = \sum_{g \in G} f(g)\rho(g g_\star) = \sum_{h \in G} f(h g_\star^{-1})\rho(h)$$

Because $f(g_\star^{-1}h) = f(hg_\star^{-1})$ we have G-equivariance.

Thus φ is a homomorphism of G-representations from $V \to V$ so it must be scaling by some constant α. We then see that

$$\mathrm{tr}(\varphi) = \alpha \dim V$$

$$\mathrm{tr}(\varphi) = \sum_{g\in G} f(g)\,\mathrm{tr}(\rho(g)) = \sum_{g \in G} f(g)\chi(g) = |G|\,(\chi, f).$$

Thus $\alpha = \frac{|G|}{n}(\chi, f)$ as desired.

Theorem .0.4

The characters $\chi_1, \ldots, \chi_n$ of the non-isomorphic irreducible representations of G form an orthonormal basis of the space of class functions on G.

Proof. Just need to show that χ_i's span the space of class functions by previous work. Pick any class function f.

We can replace f by $f - \sum_{i=1}^{n}(f, \chi_i)\chi_i$ to asume f is orthogonal to every χ_i. Then we wish to show $f = 0$.

By the lemma, for all i the φ_i corresponding to χ_i is zero. By Maschke's theorem, for every representation ρ the φ coming from ρ is zero.

We now apply this to the regular representation. Let $\{v_g\}_{g\in G}$ be a basis for the regular representation. Then we have that

$$\varphi(v_1) = \sum_{g \in G} f(g) v_{g \cdot 1} = 0.$$

Therefore $f(g) = 0$ for all g. This finishes the problem!

Proposition .0.5

For $g \in G$, let $C(G)$ be the size of the conjugacy class of G. Then if $\chi_1, \ldots, \chi_n$ are the irreducible characters of G then

$$\sum_{i=1}^{n} \overline{\chi_i(g)}\chi_i(g) = \frac{|G|}{C(g)} = |Z_G(g)|\,.$$

where $Z_G(g)$ is the centralizer of $g \in G$. Furthermore if $g' \in G$ is not conjugate to g

$$\sum_{i=1}^{n} \overline{\chi_i(g)} \chi_i(g') = 0$$

Proof. Let $f : G \to \mathbb{C}$ be the indicator function for the conjugacy class $C(g)$ (that is 1 on this conjugacy class, and 0 elsewhere).

Then we have that

$$\begin{aligned}
f &= \sum_{i=1}^{n} (f, \chi_i) \chi_i \\
(\chi_i, f) &= \frac{1}{|G|} \sum_{g' \in G} \overline{\chi_i(g') f(g')} = \frac{1}{|G|} \sum_{g' \in C(g)} \overline{\chi_i(g')} = \frac{|C(g)|}{|G|} G \overline{\chi_i(g)} \\
f &= \sum_{i=1}^{n} \frac{|C(g)|}{|G|} \sum_{i=1}^{n} \overline{\chi_i}(g) \chi_i \\
f(g') = 1 &= \frac{|C(g)|}{|G|} \sum_{i=1}^{n} \overline{\chi_i}(g) \chi_i(g') && (g' \in C(g)) \\
f(g') = 0 &= \frac{|C(g)|}{|G|} \sum_{i=1}^{n} \overline{\chi_i}(g) \chi_i(g') && (g' \notin C(g))
\end{aligned}$$

This proves the result. ♥

Example .0.1

Consider the following "character table" of S_3, considering representatives $(1), (12), (123)$ of each conjugacy class with size 1,3,2 respectively

	1	3	2
	(1)	(12)	(123)
χ_1	1	1	1
χ_{sgn}	1	-1	1
χ	2	0	-1

The character table of G determines

- Recover the position of 1 because $\sum_\chi \chi(1)^2$ is maximal among $\sum_\chi |\chi(g)|^2$, and $\{\chi(1)\}_\chi$ contains only integers.
- Size of the group, $|G| = \sum_\chi \chi(1)^2$
- Sizes of conjugacy classes of G $|G|/C(g) = \sum_\chi |\chi(g)|^2$.
- Sizes of the normal subgroups of G (and their intersections).

If $\rho : G \to \mathrm{GL}(V)$ is a representation, then

$$\ker(\rho) = \{g \in G \mid \rho(g) = \mathrm{Id}_V\} = \{g \in G \mid \chi(g) = \dim V\} = \{g \in G \mid \chi(g) = \chi(1)\}$$

where χ is a character of ρ by diagonalization. The $\supseteq$ inclusion follows from the fact that a sum of n roots of unity which is literally n implies that each root of unity is 1.

Further $\ker(\rho_1 \oplus \rho_2) = \ker \rho_1 \cap \ker \rho_2$. Thus the kernels of all representations come from intersecting kernels of irreducible characters (which we can read off the character tables).

For any normal subgroup $N \trianglelefteq G$, N is the kernel of the homomorphism $G \twoheadrightarrow G/N$. Let $\rho : G \to \mathrm{GL}(\mathbb{C}^{|G/N|})$ be the associated linear representation (by left multiplication). The kernel of this representation is N. Well

$$\begin{aligned}\ker \rho &= \{g \in G e_{ghN} = e_{hN} \ \forall h \in G\} \\ &= \{g \in G \mid ghN = hN \ \forall h \in G\} = N.\end{aligned}$$

By setting $h = 1$ for $\subseteq$, and by simple algebra for $\supseteq$.

For an example of a fabulous representation theory result

Theorem VII.3.2 (Gowers, Nikolav-Pyber)

Let G be a nontrivial finite group. Let r be the smallest dimension of a nontrivial irreducible representation of G.

For any subsets A, B, C of G such that $\frac{|A||B||C|}{|G|^3} > \frac{1}{r}$, then we have $G = ABC$ (as sets).

Corollary VII.3.3

For $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ for an odd prime p we have that $r = (p-1)/2$.

Thus for A a subset of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ with

$$\frac{|A|}{|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})|} > \left(\frac{2}{p-1}\right)^{1/3}$$

Then for all $g \in \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ we have $a, b, c \in A$ with $g = abc$.

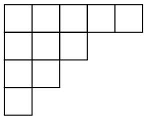
VII.4. Representations of S_n

Conjugacy classes of S_n are in bijection with partitions of n (i.e., expresions $n = \lambda_1 + \cdots + \lambda_k$, $\lambda_i \in \mathbb{Z}$, $\lambda_1 \leq \cdots \leq \lambda_k$) via a correspondence consisting of all $g \in S_n$ whose cycle lengths are $\lambda_1, \ldots, \lambda_n$.

Call the number of such partitons $p(n)$. A result of Ramanujan tells us that

$$p(n) \sim \frac{1}{4\sqrt{3}n} e^{\frac{2\pi}{\sqrt{6}}\sqrt{n}} \text{ as } n \to \infty$$

Now: produce an irreducible representation of S_n from a partition $\lambda = (\lambda_1, \ldots, \lambda_n)$ of n. Given λ, first maake the "Young diagram," which looks like this for $\lambda = (1, 2, 3, 5)$.



Next make a λ-tableau by filling in each box with a # in $\{1, \ldots, n\}$ with no repetitions. So for all λ there are $n!$ such λ-tableaux.

Say two λ-tableaux are equivalent if, $\forall i$, the i-th row of one tableau is a permutation of the i-th row of the other tableau.

A λ-tabloid is an equivalence class of a λ-tableaux.

The # of λ-tabloids is

$$\binom{n}{\lambda_1, \ldots, \lambda_k} = \frac{n!}{\lambda_1! \cdots \lambda_k!}.$$

S_n acts on the λ-tableaux in the natural way, and this descends to an action on the set of λ-tabloids. This yields a linear representation of the above dimension. Consider the subrepresentation on the subspace generated by the following, where t is a λ-tableaux

$$e_t = \sum_{\substack{\sigma \in S_n \\ \sigma \text{ permutes the columns of } t}} = \operatorname{sgn}(\sigma)(\sigma \cdot t).$$

Theorem VII.4.1

This is an irreducible representation, and these are all of the irreducible representaitons of S_n.

Goal: Show that every rational # in the character table is an integer.

Definition VII.4.1

An algebraic integer is a complex number α which is a root of a monic polynomial in $\mathbb{Z}[x]$.

Lemma VII.4.2

The algebraic integers in $\mathbb{Q}$ are precisely $\mathbb{Z}$.

Proof. Suppose $\alpha \in \mathbb{Q}$ is a root of $x^n + c_1 x^{n-1} + \cdots + c_n$ with $c_i \in \mathbb{Z}$.

Write $\alpha = a/b$ for a, b coprime integers. Then we see that

$$\begin{aligned} 0 &= \frac{a^n}{b^n} + c_1 \frac{a^{n-1}}{b^{n-1}} + \cdots + c_n. && = \frac{a^n + b\,(\text{some integer})}{b^n} \\ &= \frac{(\text{integer coprime to b})}{b^n}. \end{aligned}$$

But 0 is coprime to b if and only if $b = \pm 1$. Thus $\alpha \in \mathbb{Z}$

The other direction is trivial, if $z \in \mathbb{Z}$ consider the polynomial $x - z$.

Proposition VII.4.3

If α_1, α_2 are algebraic integers then $\alpha_1 + \alpha_2$ and $\alpha_1\alpha_2$ are algebraic integers.

Lemma VII.4.4

For $\alpha \in \mathbb{C}$, α is an algebraic integer if and only if α is an eigenvalue of a square integer matrix.

Proof. If α is an eigenvalue of $A \in M_{n\times n}(\mathbb{Z})$ then α is a root of the characteristic polynomial of A, i.e., of $\det(x \operatorname{Id}_n - A)$, which is a monic polynomial in $\mathbb{Z}[x]$ with integer coefficients (since the determinant is a polynomial in the entries).

Conversely, let α be an algebraic integer, say α isa root of $x^n + c_1x^{n-1} + \cdots + c_n$ with $c_i \in \mathbb{Z}$.

This polynomial is the characteristic polynomial of

$$\begin{bmatrix} 0 & & & \cdots & 0 & -c_n \\ 1 & 0 & & \cdots & 0 & -c_{n-1} \\ & 1 & 0 & \cdots & 0 & -c_{n-2} \\ & & \ddots & \ddots & \vdots & \vdots \\ & & & \ddots & 0 & -c_{n-1} \\ & & & & 1 & -c_n \end{bmatrix}$$

so α is an eigenvalue of this matrix. ♥

Proof of Proposition VII.4.3. Let α_1, α_2 be eigenvalues of $A_1 \in M_{m\times m}(\mathbb{Z})$ and $A_2 \in M_{n\times n}(\mathbb{Z})$ respectively.

We can then consider $A_1 \otimes A_2$, defined by the following block form

$$A_1 \otimes A_2 = \begin{bmatrix} a_{11}A_2 & a_{12}A_2 & \cdots & a_{1m}A_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}A_2 & a_{m2}A_2 & \cdots & a_{mm}A_2 \end{bmatrix}$$

where $A_1 = (a_{ij})$. If $A_i\vec{v}_i = \alpha_i\vec{v}_i$ then write $\vec{v}_1 = (d_1, \ldots, d_m)^T$ then write $\vec{w} = (d_1\vec{v}_2, \ldots, d_m\vec{v}_m)^T$.

Then of course $(A_1 \otimes A_2)\vec{w} = \alpha_1\alpha_2\vec{w}$ by explicit computation.

$\alpha_1 + \alpha_2$ is an eigenvalue of

$$(A_1 \otimes \operatorname{Id}_n) + (\operatorname{Id}_m \otimes A_2).$$

This can be computed explicitly, or via the tensor properties

$$\begin{aligned} ((A_1 \otimes \operatorname{Id}_n) + (\operatorname{Id}_m \otimes A_2))(v_1 \otimes v_2) &= A_1v_1 \otimes v_2 + v_1 \otimes A_2v_2 \\ &= \alpha_1(v_1 \otimes v_2) + \alpha_2(v_1 \otimes v_2) \\ &= (\alpha_1 + \alpha_2)(v_1 \otimes v_2). \end{aligned}$$

♥

Fact: If χ is the character of an n-dimensional representation of C_k, then

$$\sum_{g=\text{generator of } C_k} |\chi(g)|^2 \geq \#\text{ of generatos of } C_k = \varphi(k).$$

where $\varphi(k)$ is the number of integers less than k which are coprime to k. UNLESS $\chi(g) = 0$ for all generators g of C_k.

Note: Everything from last time works over any ring.

Definition VII.4.2

A ring R is an abelian group under $+$ equipped with a multiplication $\cdot$ which is associative, has an identity, and distributes over addition.

Example VII.4.1

Given any abelian group G, then the set of endomorphisms $\operatorname{End}(G) \coloneqq \operatorname{Hom}(G, G)$ is naturally a group under addition and becomes a ring when equipped with composition.

Rings will be the first thing we study next semester.

Definition VII.4.3

An algebra over a field K is a vector space A over K with the structure of a ring such that for vectors $a, b \in A$ and scalars $c, d \in K$ we have

$$(ca) \cdot (db) = (cd)(a \cdot b).$$

This product is bilinear.

Definition VII.4.4

Let G be a finite group. Then $\mathbb{C}[G]$ is the group algebra.

As a vector space this is $\mathbb{C}$-linear combinations of a basis $\{e_g\}_{g \in G}$. For convenience we identify $c \in \mathbb{C}$ with ce_1. Another way to see this as as $\{\text{functions } G \to \mathbb{C}, g \mapsto c_g\}$.

Recall that G acts on $\mathbb{C}[G]$ by the regular representation

$$h \cdot \left(\sum_{g \in G} c_g e_g \right) = \sum_{g \in G} c_g e_{hg}.$$

Define then a ring structure on $\mathbb{C}[G]$ by the following for all $g, h \in G$ and $c \in \mathbb{C}$

$$e_h e_g = e_{hg} \qquad\qquad ce_g = e_g c.$$

Secretly the above formula is

$$ce_g = e_g(ce_1).$$

What is the center of $\mathbb{C}[G]$ (under multiplication)? This is the set of all $\theta \in \mathbb{C}[G]$ with $\theta x = x\theta$ for all $x \in \mathbb{C}[G]$. Equivalently $\theta e_g = e_g \theta$ for all $g \in G$.

Write $\theta = \sum_{h \in G} c_h e_h$. Then what this means is

$$\theta e_g = \sum_{hinG} c_h e_{hg} = \sum_{h \in G} c_h e_{gh} = e_g \theta.$$

Reindexing then gives

$$\sum_{h \in G} c_h e_{hg} = \sum_{h \in G} c_h e_{(ghg^{-1})g} = \sum_{h' \in G} c_{g^{-1}h'g} e_{h'g}$$

Therefore $c_h = c_{g^{-1}hg}$ for every $h \in G$. This means that

$$\begin{aligned} \text{center of } \mathbb{C}[G] &= \left\{ \sum_{h\in G} c_h e_h \mid c_h = c_{g^{-1}hg} \ \ \forall\, g \in G \right\} \\ &= \left\{ \sum_{h\in G} c_h e_h \mid c_- : G \to \mathbb{C} \text{ is a class function} \right\} \\ &= \text{the class functions on } G \\ &= \left\{ \mathbb{C}\text{-linear combinations of } \sum_{h\in C} e_h \ \ \forall \text{ conjugacy classes } C \subseteq G \right\} \end{aligned}$$

Definition VII.4.5

If $\rho : G \to \mathrm{GL}(V)$ is a representaiton and π is an irreducible representation, then we can decompose V by Maschke's Theorem into a direct sum of subspaces on which ρ acts isomorphically to irreducibles.

Collecting all the subspaces on which ρ acts as π into a direct sum gives the π-isotypic part of V. This is well-defined by Machke's Theorem.

Recall VII.4.2

If $\rho : G \to \mathrm{GL}(V)$ is a representation, and π is an irreducible representation of G, then the projection of V onto its π-isotypic part (aka a direct sum of things isomorphic to π) is

$$v \mapsto \frac{\dim \pi}{|G|} \sum_{g\in G} \chi_\pi(g^{-1})(g \cdot v).$$

In group algebra language (when ρ is the regular representation), this projection is multiplication of each element in $\mathbb{C}[G]$ by

$$e_\pi := \frac{\dim \pi}{|G|} \sum_{g\in G} \chi_\pi(g^{-1}) e_g.$$

Lemma VII.4.5

Let π be an irreducible representation of G. Let $s = \sum_g c_g e_g$ lie in the center of $\mathbb{C}[G]$. Define

$$\omega_\pi(s) := \frac{1}{\dim \pi} \sum_{g\in G} c_g \chi_\pi(g).$$

Then $s \mapsto \omega_\pi(s)$ is a homomorphism (linearly, and multiplicatively) from $\mathrm{Center}(\mathbb{C}[G]) \to \mathbb{C}$.

Theorem VII.4.6 (Burnside)

Let $\rho : G \to \mathrm{GL}(V)$ be an irreducible representation of a finite group G. If $g \in G$ and the size of the conjugacy class of g is coprime to $\dim V$ then either $\chi(g) = 0$ or g is in the kernel of $G \xrightarrow{\rho} \mathrm{GL}(V) \twoheadrightarrow \mathrm{PGL}(V)$, where $\mathrm{PGL}(V) = \mathrm{GL}(V)/\{c \cdot \mathrm{Id}_V \mid c \neq 0\}$.

That is either $\chi(g) = 0$ or $\rho(g) = c\,\mathrm{Id}_V$ for some $c \neq 0$.

Theorem VII.4.7 (Burnside)

Let $s = \sum_{h\in G} c_h e_h \in \mathbb{C}[G]$ where each c_h is an algebraic integer. If s is in the center of $\mathbb{C}[G]$ then

> s acts on any irreducible representation $\rho : G \to \mathrm{GL}(V)$ as multiplication by a scalar $\omega_\rho(s)$, and even better, this scalar is also an algebraic integer.
>
> In particular, for any $g \in G$,
>
> $$\frac{\chi_\rho(g) \cdot (\text{size of conjugacy class of } g)}{\dim \rho}$$
>
> is an algebraic integer.

Proof of very last part. Apply the first part to $s = \sum_{h \in C} e_h$, where C is the conjugacy class of g. Then

$$\omega_\rho(s) = \frac{1}{\dim \rho} \sum_{h \in C} \chi_\rho(h) = \frac{\chi_\rho(g) \cdot |C|}{\dim \rho}.$$

This is then an algebraic integer. ♥

Next time: Proofs!!!

> **Theorem VII.4.8**
>
> Let $\rho : G \to \mathrm{GL}(V)$ be an irreducible representation. If $g \in G$ has conjugacy class C, where $|C|$ is coprime to $\dim \rho$, then either $\chi_\rho(g) = 0$ or $\rho(g)$ acts on V as $\lambda \cdot \mathrm{Id}_V$ for some $\lambda \in \mathbb{C}^\times$
>
> Note: $\rho(g) = \lambda \cdot \mathrm{Id}_V$ if and only if $\overline{\rho}(g) = 1$, with
>
> $$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[rr, dashed, bend right, "\overline{\rho}"'] & \mathrm{GL}(V) \arrow[r, two heads] & PGL(V). \end{tikzcd}$$
>
> Where $PGL(V) = \mathrm{GL}(V)/\{\lambda \mathrm{Id}_V \mid \lambda \in \mathbb{C}^\times\}$.

We will use Theorem VII.4.8 to prove

> **Theorem VII.4.9**
>
> If $|G| = p^a q^b$ with p, q distinct primes and $a, b > 0$ then G is not simple.

> **Claim**
>
> If G is any nontrivial finite group, and $p \neq q$ are primes dividing $|G|$, then there exists $g \in G \setminus \{1\}$ and an irreducible nontirvial representation $\rho : G \to \mathrm{GL}(V)$ such that $\chi_\rho(g) \neq 0$ and p does not divide the conjugacy class of G and $q \nmid \dim \rho$.

Proof of Theorem VII.4.9. First find $g \neq 1$ such that p does not divide the conjugacy class of G.

If center of G is nontrivial, let $g \in Z(G) \setminus \{1\}$. If $Z(G) = 1$ then

$$|G| = \sum_C |C|$$

$$|G| - 1 = \sum_{C \neq 1} |C| \cong -1 \mod p$$

Thus there is some $C \neq 1$ so that $p \nmid |C|$. Fix $g \in C$.

Then the orthogonality of columns for 1 and g gives that

$$\begin{aligned} 0 &= \sum_{\chi \text{irr.}} \chi(g)\overline{\chi(1)} = \sum_{\chi} \chi(g) \dim \chi \\ -1 &= \sum_{\chi \neq 1} \chi(g) \cdot \dim \chi \\ -\frac{1}{q} &= \sum_{\chi \neq 1} \chi(g) \cdot \frac{\dim \chi}{q} \end{aligned}$$

Thus there exists a $\chi \neq 1$ such that $\chi(g) \neq 0$ and $(\dim \chi)/q$ is not an algebraic integer. Why? Well $-1/q$ is not an algebraic integer, and $\chi(g)$ is always an algebraic integer, so we must have some non-algebraic integer part of the sum.

Since $(\dim \chi)/q \in \mathbb{Q}$, this means that $q \nmid \dim \chi$.

When $|G| = p^a q^b$ this implies that the size of the conjugacy class is coprime to $\dim \rho$. Then Theorem VII.4.8 implies that $g \in \ker \overline{\rho}$ (where $\overline{\rho} = \rho/\lambda$ for some $\lambda \in \mathbb{C}^\times$). Then $\ker \overline{\rho}$ is a nontrivial normal subgroup of G, and G is not simple unless $\ker \overline{\rho} = G$.

But then $\rho(h)$ acts as $\lambda \operatorname{Id}_V$ for fixed $\lambda \in \mathbb{C}^\times$, implying that $\dim V = 1$ because ρ is irreducible.

Thus ρ is a homomorphism $G \to \mathbb{C}^\times$. We then have that

$$G/\ker \rho \cong \operatorname{im} \rho = \text{cyclic}$$

But then ρ is nontrivial, so $\ker \rho \neq G$. Thus if G is simple, $\ker \rho = 1$, so G is cyclic, and clearly then G is not simple. ♥

It remains to prove Theorem VII.4.8. Use

Theorem VII.4.10

Let $c = \sum_{g \in G} c_g e_g$ in the group algebra $\mathbb{C}[G]$. Assume that c lies in the cneter of $\mathbb{C}[G]$, i.e. $c_g = c_h$ when g, h are conjugate.

Assume further that each c_g is an algebraic integer. Then c acts on any irreducible representation as scalar multiplication by an algebraic integer

The action is for $\rho : G \to \mathrm{GL}(V)$. c maps $V \to V$ via

$$v \mapsto \sum_{g} c_g (g \cdot v)$$

Since $ce_g = e_g c$ for all g, c is a homomorphism of representations from ρ to ρ, so c is a scalar multiple by Schur's Lemma (see homework).

In particular, for $g \in G$ and any irreducible representation $\rho : G \to \mathrm{GL}(V)$,

$$\frac{\chi_\rho(g) \cdot |C(g)|}{\dim \rho}$$

is an algebraic integer. This is given by setting $c = \sum_{h \in C(g)} e_h$.

Proof. The value of the scalar is

$$\omega_\rho(c) = \frac{1}{\dim \rho} \sum_g c_g \chi_\rho(g).$$

We see that

$$\sum_g c_g \chi(g) = \operatorname{tr}\left(\sum_g c_g \rho(g)\right).$$

We then compute this trace which must be $(\dim \rho)\omega_\rho(c)$ because c acts as a scalar.

Since this expresion in c respects addition and scalar multiplication, it suffices to prove $\omega_\rho(c)$ is an algebraic integer when $c = \sum_{g \in C} e_g$ for some conjugacy class C in G. That is we can assume each c_g is zero or one.

Let $e_\rho \in \mathbb{C}[G]$ induce projection of any representation $\theta : G \to \mathrm{GL}(V)$ onto its ρ-isotypic part. Then we see that

$$c \cdot e_\rho = \omega_\rho(c) \cdot e_\rho$$

so e_ρ is an eigenvector of the action on $\mathbb{C}[G]$, with eigenvalue $\omega_\rho(c)$. To see this explicitly

Consider the regular representation on $\mathbb{C}[G]$ given by θ, with $e_\rho = \sum_g e_{\rho,g} e_g$. Then necessarily

$$c \cdot e_\rho = \sum_g \sum_h c_g e_{\rho,h}(e_{gh}) = \sum_g \sum_h c_g e_{\rho,h}(\theta(g) e_h) = \sum_g c_g(\theta(g) \cdot e_\rho).$$

Writing $e_1 = \sum_i \vec{v}_i + \vec{w}$ where each $\vec{v}_i$ lies in a copy of $\mathbb{C}[G]$ isomorphic to ρ, and $\vec{w}$ lies in the complement of the ρ-isotypic part of $\mathbb{C}[G]$. Then

$$\begin{aligned} c \cdot e_\rho &= \sum_g c_g(\theta(g) \cdot e_\rho \cdot e_1) = \sum_g \sum_i c_g(\rho(g) \cdot e_\rho \cdot \vec{v}_i) \\ &= \sum_i (\omega_\rho(g) \vec{v}_i) = \omega_\rho(g) \cdot e_\rho \end{aligned}$$

because $\sum_i \vec{v}_i = e_\rho$ by definition. Perfect!

But $\mathbb{C}[G] \to \mathbb{C}[G]$ given by $x \mapsto cx$ can be represented as an <u>integer</u> matrix in terms of the basis e_g, because

$$\begin{aligned} ce_g &= \left(\sum_{h \in G} c_h e_h\right) e_g \\ &= \sum_{h \in G} c_h e_{hg} = \sum_{h' \in G} c_{h' g^{-1}} e_{h'} \end{aligned}$$

and each $c_{h'g^{-1}}$ is zero or one by assumption. The eigenvalues are the roots of the characteristic polynomial, and this then proves that $\omega_\rho(c)$ is an algebraic integer.

Proof of Theorem VII.4.8. Suppose $|C(g)|$ is coprime to $\dim \rho$ for an irreducible representation $\rho : G \to \mathrm{GL}(V)$.

Then let $c = \sum_{h \in C(g)} e_h$. We then know that

$$\omega_\rho(c) = \frac{\chi_\rho(g) \cdot |C(g)|}{\dim \rho}$$

is an algebraic integer. If $\chi_\rho(g) \neq 0$, then because $|C(g)|$ and $\dim \rho$ are coprime this implies that $\chi_\rho(g) = (\dim \rho) \cdot \lambda$ for some algebraic integer $\lambda \in \mathbb{C}$, as otherwise we will not be able to cancel the denominator of $\dim \rho$, and it will show up in any monic polynomial with integer coefficients (similar to the proof that if $\alpha \in \mathbb{Q}$ is an algebraic integer then $\alpha \in \mathbb{Z}$).

By using the relevant inequalities by which we showed that $\chi_\rho(g) = \dim \rho$ if and only if $\rho(g)$ is trivial, we can then derive that all the eigenvalues of $\rho(g)$ are equal, showing that $\rho(g)$ acts by scalar multiplication just as desired.

> **Theorem VII.4.11** ($\dim \rho \mid |G|$)
>
> If $\rho : G \to \mathrm{GL}(V)$ is an irreducible representation then $\dim \rho \mid |G|$.

Proof. We know by orthonormality that

$$\begin{aligned}
|G| &= \sum_{g \in G} \chi_\rho(g) \overline{\chi_\rho(g)} \\
\frac{|G|}{\dim \rho} &= \sum_{g \in G} \frac{\chi_\rho(g)}{\dim \rho} \overline{\chi_\rho(g)} \\
\frac{|G|}{\dim \rho} &= \sum_{C(g)} \frac{\chi_\rho(g)\,|C|}{\dim \rho} \overline{\chi_\rho(g)}
\end{aligned}$$

where $\sum_{C(g)}$ is a sum over distinct conjugacy classes.

By **??** we know that the right hand side is an algebraic integer, and so because the left hand side is in $\mathbb{Q}$ we know that the left hand side lies in $\mathbb{Z}$ as desired.

VII.5. **Representations of Infinite Groups**

We now look at finite-dimensional representations of infinite groups. Unfortunately, there are too many to be useful, as an example

> **Example VII.5.1**
>
> Consider the group $\mathbb{R}$ with addition, and we're going to look at its 1-dimensional representations. These are just the homomorphisms $\mathbb{R} \to \mathbb{C}^\times$. How many of these are there? We see that $\mathbb{R}$ contains a direct sum of uncountably many copies of $\mathbb{Z}$. One can map the generators of each copy of $\mathbb{Z}$ to an arbitrary element of $\mathbb{C}^\times$. This is larger than even the number of real numbers!
>
> The moral of the story is that $\mathbb{R}$ has more structure than just being a group, and we should instead analyze representations that respect some other structure (for example the analytic structure).
>
> Say we require that the maps $\mathbb{R} \to \mathbb{C}^\times$ are continuous.

> **Lemma VII.5.1**
>
> Every continuous group homomorphism $\chi : \mathbb{R} \to \mathbb{C}^\times$ is $\chi_s(t) = e^{st}$ for some fixed $s \in \mathbb{C}$.

Proof. If χ is differentiable then

$$\begin{aligned}\chi'(t) &= \lim_{\Delta t \to 0} \frac{\chi(t+\Delta t) - \chi(t)}{\Delta t} \\ &= \lim_{\Delta t \to 0} \frac{\chi(t)\chi(\Delta t) - \chi(t)}{\Delta t} \\ &= \chi(t) \cdot \lim_{\Delta t \to 0} \frac{\chi(\Delta t) - 1}{\Delta t} \\ &= \chi(t) \cdot \chi'(0)\end{aligned}$$

Writing $s := \chi'(0)$, this satisfies $\chi'(t) = s\chi(t)$, which implies that $\chi(t) = C \cdot e^{sx}$ for some constant C, but $\chi(0) = 1$, so $C = 1$.

> We can justify this with the following manipulations. Letting $\psi(t) :- \chi(t)/e^{st}$, then ψ satisfies
>
> $$\psi'(t) = \frac{\chi'(t) - s\chi(t)}{e^{st}} = 0$$
>
> Thus ψ is a constant C.

It remains to show that every continous homomorphism $\chi : \mathbb{R} \to \mathbb{C}^\times$ is differentiable. Define $\psi(t) := \int_0^t \chi(x)\,\mathrm{d}x$. Then $\psi'(t) = \chi(t)$. Then

$$\psi(t+r) = \int_0^{t+r} \chi(x)\,\mathrm{d}x = \int_0^{x} \chi(x)\,\mathrm{d}x + \int_t^{t+r} \chi(x)\,\mathrm{d}x$$

$$l = \psi(t) + \int_0^{r} \chi(t+u)\,\mathrm{d}u = \psi(t) + \chi(t)\psi(r)$$

We know $\psi'(0) = \chi(0) = 1$ is nonzero, so ψ is not identically zero. Thus there is some r so that $\psi(r) \neq 0$. Fix one, then

$$\chi(t) = \frac{\psi(t+r) - \psi(t)}{\psi(r)}.$$

But then χ is a combination of differentiable functions, and so χ is differentiable. ♥

Definition VII.5.1

A topological group is a group G which is also a topological space where the relevant maps are continuous

$$\begin{aligned} G \times G &\longrightarrow G & \qquad G &\longrightarrow G \\ (g,h) &\longmapsto gh & g &\longmapsto g^{-1}\end{aligned}$$

A great example is $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{C})$.

Definition VII.5.2

Direct sums and tensor pro A continuous represention of a topological group G is a continuous homomorphism $\rho : G \to \mathrm{GL}_n(\mathbb{C})$.

Note: $\mathbb{C}^n$ has an inner product, so lets restrict to representations $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ where each $\rho(g)$ (with $g \in G$) preserves this inner product. That is

$$\langle v, u\rangle = \langle \rho(g)v, \rho(g)u\rangle$$

Definition VII.5.3

Say $\theta \in \mathrm{GL}_n(\mathbb{C})$ is unitary if θ preserves the inner product on $\mathbb{C}^n$.

Say a representation $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ is unitary if $\rho(g)$ is unitary for each $g \in G$.

Lemma VII.5.2

If G is a topological group, and $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ is a continuous unitary representation, then

- Any subrepresentation of ρ and any restriction of ρ to $H \leq G$ is continuous and unitary.
- Direct sums and tensor products of (continuous) unitary representations are (continuous) unitary.

Npote that if $\theta \in \mathrm{GL}_n(\mathbb{C})$ is unitary, then all eigenvalues of θ have absolute value 1. Why? Well if $\theta(v) = \lambda v$, then

$$|\lambda|^2 \|v\|^2 = \langle \theta v, \theta v \rangle = \langle v, v \rangle = \|v\|^2.$$

Great!

Proposition VII.5.3

Let $\rho : G \to \mathrm{GL}(V)$ be a unitary (continuous) representation of a topological group G.

Then any subrepresentation W has a complementary subrepresentation $W^\perp$ with $V = W \oplus W^\perp$.

Proof. Let $W^\perp$ be the orthogonal complement of W. Then we see that if $w^\perp \in W^\perp$ then

$$\langle g \cdot w^\perp, w \rangle = \langle w^\perp, g^{-1} \cdot w \rangle = 0.$$

For every $g \in G$ and $w \in W$ (because $g^{-1} \cdot w \in W$). Thus $g \cdot w^\perp \in W^\perp$, making $W^\perp$ a subrepresentation. ♥

Last time we showed that the 1-dimensional continuous representations of $\mathbb{R}$ are

$$\begin{aligned} \rho_s : \mathbb{R} &\to \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times \\ x &\mapsto e^{sx} \end{aligned}$$

for all $s \in \mathbb{C}$.

A 2-dimensional continuous representation of $\mathbb{R}$

$$\begin{aligned} \mathbb{R} &\to \mathrm{GL}_2(\mathbb{R}) \subseteq \mathrm{GL}_2(\mathbb{C}) \\ x &\mapsto \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

The vector $(1,0)^T$ is fixed by these matrices, so its span $W := \mathrm{span}((1,0)^T)$ is an isomorphic copy of the trivial representation.

But $\mathbb{R}^2$ (or $\mathbb{C}^2$) is not $W \oplus W'$ for any subrepresentation W' of $\mathbb{R}$. This means that Maschke's Theorem fails for this representation. The problem is that the matrices in the image are not unitary.

Last time: if $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ is a continuous representation of a topological space whose image $\rho(G)$ is contained in the set of unitary matrices in $\mathrm{GL}_n(\mathbb{C})$, then Maschke's Theorem holds.

Observation: From any 1-dimensional representation of

$$\theta : S^1 \cong \mathbb{R}/\mathbb{Z} \to \mathbb{C}^\times$$

we get a representation of $\mathbb{R}$

$$\mathbb{R} \twoheadrightarrow \mathbb{R}/\mathbb{Z} \xrightarrow{\theta} \mathbb{C}^\times$$

Which representations $\rho_s : \mathbb{R} \to \mathbb{C}^\times$ arise in this way? But we see that

$$\begin{tikzcd}
\mathbb{R} \arrow[r] & \mathbb{R}/\mathbb{Z} \arrow[r] & \mathbb{C}^\times \\
1 \arrow[r, mapsto] & 0 \arrow[r, mapsto] & 1
\end{tikzcd}$$

and thus $e^s = 1$. Therefore $s = (2\pi i)n$ for some $n \in \mathbb{Z}$.

Schur's Lemma didn't require G to be finite (and most of it works over any field). Namely if $L : V \to W$ is a homomorphism of representations between two irreducible representations, then L is either zero or invertible.

Lemma VII.5.4 (Schur's Lemma)

Suppose $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(W)$ are two irreducible representations (even infinite-dimensional), and let $L : V \to W$ be a homomorphism of G-representations.

That is the following commutes for all $g \in G$

$$\begin{tikzcd}
V \arrow[r, "\rho(g)"] \arrow[d, "L"'] & V \arrow[d, "L"] \\
W \arrow[r, "\rho'(g)"'] & W
\end{tikzcd}.$$

Then either L is an isomorphism or zero.

Proof. $\ker L$ is a subrepresentation of ρ, so $\ker L = 0$ or $\ker L = V$ by irreducibility. Thus L is injective or $L = 0$.

$\operatorname{im} L$ is a subrepresentation of ρ'. Thus ρ' is irreducible, and either $\operatorname{im} L = 0$ or $\operatorname{im} L = W$. Thus $L = 0$ or L is surjective.

Therefore if $L \neq 0$ then L is bijective. We may then check that its inverse on the level of sets is an isomorphism ♥

If we work over a finite-dimensional vector space over $\mathbb{C}$ (or any algebraically closed field), it is easy to then derive that if $L : V \to V$ then $L = \lambda \operatorname{Id}_V$ for some $\lambda \in \mathbb{C}$ (by finding an eigenvalue).

Proof. Let $\vec{v}$ be an eigenvector for L with $L\vec{v} = \lambda\vec{v}$ for some λ.

Then $\vec{v} \in \ker(L - \lambda \operatorname{Id}_V)$ is also a subrepresentation of V.

Since V is irreducible, $\ker(L - \lambda \operatorname{Id}_V) = V$, and so $L = \lambda \operatorname{Id}_V$. ♥

Corollary VII.5.5

If G is abelian any (finite-dimensional) irreducible representation of G (over $\mathbb{C}$) is 1-dimensional.

Proof. For all $g \in G$, $\rho(g)$ is an invertible linear map $V \to V$. We claim that it is a homomorphism of G-representations. This is precisely the statement that for any $g' \in G$ and $v \in V$

$$g \cdot (g' \cdot v) = g' \cdot (g \cdot v).$$

Clearly this holds when G is abelian. By Schur's Lemma (Lemma VII.5.4), we know for all $g \in G$ there is a λ such that $\rho(g) = \lambda \operatorname{Id}_V$.

We then know that $\rho(g)$ maps every 1-dimensional subspace of V to itself. So each such subspace is a subrepresentation. Because ρ is irreducible, this implies any such subspace must be all of V.

VII.6. **Compact Groups (namely $S^1 \cong \mathbb{R}/\mathbb{Z}$)**

Let $G = \{x \in \mathbb{C}^\times \mid |x| = 1\} = S^1$. Then G is a compact topological group. Furthermore

$$\begin{aligned} \mathbb{R}/\mathbb{Z} &\xrightarrow{\cong} G \\ x &\mapsto e^{2\pi i x} \end{aligned}$$

is an isomorphism of topological groups. G is abelian, so the irreducible representations of G are 1-dimensional. Earlier, we showed that the 1-dimensional representations are

$$\begin{aligned} \rho : \mathbb{R}/\mathbb{Z} &\to \mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times \\ x &\mapsto e^{2\pi i n x} \end{aligned}$$

for some $n \in \mathbb{Z}$, and these are of course unitary.

Thus the finite-dimensional unitary representations of these are the direct sums of copies of the above representations.

Decomposing a representation into irreducibles turns into the problem of writing a function as a combination of these ρ's.

For any integrable function φ, the fourier series of φ is

$$\sum_{n\in\mathbb{Z}} c_n e^{2\pi i n x} = \sum_{n\in\mathbb{Z}} c_n \rho_n(x)$$

such that $c_n \in \mathbb{R}$. Furthermore the c_n is given in terms of an integral.

$$c_n = \int_{\mathbb{R}/\mathbb{Z}} \varphi(x) e^{2\pi i n x} \, \mathrm{d}x$$

VIII. **Review for Midterm II**

If you have a finite group G and any inner product $\langle -, - \rangle_{\mathrm{bad}}$ you can upgrade it to a G-invariant inner product via

$$\langle v, w \rangle := \frac{1}{|G|} \sum_{g\in G} \langle g \cdot v, g \cdot w \rangle_{\mathrm{bad}}$$

The big theorems for finite-dimensional representations of finite groups over $\mathbb{C}$

(1) Every (finite-dimensional complex) representation of a finite group is the direct sum of irreducible subrepresentations [**thm:maschke-exist**].

(2) If $V = V_1 \oplus \cdots \oplus V_k = W_1 \oplus \cdots \oplus W_\ell$ (internal direct sums) where V is a G-representation, and V_i's, W_j's are irreducible then $k = \ell$ and after relabeling the W_i's we can make $V_i \cong W_i$ for all i. Furthermore, for any irreducible representation ψ of G,

$$\bigoplus_{V_i \cong \psi} V_i = \bigoplus_{W_j \cong \psi} W_j$$

See [**thm:maschke-unique**]. This is called the ψ-isotypic part of V.

(3) Given a representation $\rho : G \to \mathrm{GL}(V), \rho' : G \to \mathrm{GL}(W)$, get representations of G acting on $V^*, \mathrm{Hom}(V, W), V \oplus W, V \otimes W$. This also has a nice action on characters

- $\chi_{V^*} = \overline{\chi_V}$
- $\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V}\chi_W$
- $\chi_{V\otimes W} = \chi_V \chi_W$
- $\chi_{V\oplus W} = \chi_V + \chi_W$.

(4) Given a finite-dimensional representation $\rho : G \to \mathrm{GL}(V)$, the character is

$$\begin{aligned} \chi : G &\to \mathbb{C} \\ g &\mapsto \mathrm{tr}(\rho(g)). \end{aligned}$$

Properties of characters

- Two represenions have the same character $\iff$ they're $\cong$.
- Characters are class functions, that is $\chi(ghg^{-1}) = \chi(h)$ for all $g, h \in G$. If C is a conjugacy class then we can unambiguously write $\chi(C) \coloneqq \chi(g)$ for any $g \in C$.
- The irreducible characters form an orthonormal basis for the space of class functions under the usual inner product on $\mathbb{C}^G$

  $$(\alpha, \beta) = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)}$$

  This means that every class function $f : G \to \mathbb{C}$ satisfies

  $$f = \sum_{\substack{\text{irr char} \\ \chi}} (f, \chi)\chi$$

  It also tells you that the # of irreducible characters equals the # of conjugacy classes of G.
- If ρ is a representation and ρ_{irr} is an irreducible representation then

  $$\langle \chi_{\mathrm{irr}}, \chi_\rho \rangle$$

  is the number of copies of ρ_{irr} in the decomposition of ρ into irreducibles.
- We also have orthogonality of columns, that is given two distinct conjugacy classes C, C'

  $$\frac{1}{|G|} \sum_{\substack{\text{irr char} \\ \chi}} \chi(C)\overline{\chi(C')} = 0$$

  $$\frac{1}{|G|} \sum_{\substack{\text{irr char} \\ \chi}} \chi(C)\overline{\chi(C)} = \frac{1}{|C|}$$

  Here is a proof of this fact

  If C is a conjugacy class of h in G, then let

  $$f_C : G \to \mathbb{C}$$

$$g \mapsto \begin{cases} 1 & \text{if } g \in C \\ 0 & \text{otherwise} \end{cases}$$

thus $f_C = \sum_{\text{irr } \chi} (f_C, \chi)\chi$, but we know (f_C, χ). Namely

$$(f_C, \chi) = \frac{1}{|G|} \sum_{g \in C} \overline{\chi(g)} = \frac{|C|\,\overline{\chi(C)}}{|G|}.$$

Therefore

$$f_C = \sum_{\text{irr } \chi} \frac{|C|}{|G|} \cdot \overline{\chi(C)} \cdot \chi.$$

Evaluating at some g we see that if $g \in C$ then

$$1 = \frac{|C|}{|G|} \cdot \sum_{\text{irr } \chi} \overline{\chi(g)}\chi(g)$$

and if $g \notin C$ then

$$0 = \frac{|C|}{|G|} \cdot \sum_{\text{irr } \chi} \overline{\chi(C)}\chi(g)$$

- If $\rho : G \to \mathrm{GL}(V)$ is a representation, where $n := \dim V$, then $\chi_\rho(g)$ is a sum of n (order of g)-th roots of unity. This can be useful for finding the order of elements from a character table.
- If $\rho_1, \dots, \rho_n$ are the irreducible representations, with $\chi_1, \dots, \chi_n$ their characters, then

$$|G| = \sum_{i=1}^{n} (\dim \rho_i)^2 = \sum_{i=1}^{n} \chi_i(1).$$

- If ρ is an irreducible representation with character χ then

$$\ker \rho = \{g \in G \mid \chi(g) = \chi(1) = \dim \rho\}$$

  is a normal subgroup of G. Furthermore, every normal subgroup is an intersection of subgroups of this form.
- Fact: If ρ is an irreducible representation of G then $\dim \rho \mid |G|$.

  Note: if $|G|$ is odd, then $\dim \rho$ is odd, so because an odd number squared is $1 \mod 8$, we have

$$|G| \equiv (\#\text{ conjugacy classes of G}) \mod 8$$

- If $\rho = \sum_{i=1}^{k} e_i \rho_i$ with ρ_i non-isomorphic irreducibles and $e_i \in \mathbb{Z}_{>0}$ then

$$(\chi_\rho, \chi_\rho) = \sum_{i=1}^{k} e_i^2$$

Information we should be able to recover from a character table.

- Orders of elements from a conjugacy class
- Normal subgroups as unions of conjugacy classes based on kernels of the irreducible representations (and then their intersections)
- Be able to fill in a partial character table

Some representations you should know

- Representations of C_n, D_5, S_3.
- Representations of group actions

$$\text{character of regular representation} = \sum_{\text{irr. }\chi} (\dim \chi)\chi$$

IX. Wrap-Up

IX.1. Representations of C_n

Let $C_n = \langle g \rangle$. Then

$$\rho : C_n \to \mathrm{GL}_k(\mathbb{C})$$
$$g \mapsto \rho(g) = M$$

where $M^n = \mathrm{Id}_k$.

What are the subrepresentations? Well M is diagonalizable

Theorem IX.1.1

General Fact: A $k \times k$ matrix A (over F) is diagonalizable over a field F if and only if $h(A) = 0$ for some monic degree-d $h(x) \in F[x]$ which has d distinct roots in F.

Theorem IX.1.2 (Cayley-Hamilton)

A matrix A satisfies its characteristic polynomial.

Because M is diagonalizable, $\mathbb{C}^k = V_1 \oplus \cdots \oplus V_r$ where V_i are eigenspaces fro M with eigenvalue λ_i (where λ_i are pairwise distinct element of $\mathbb{C}^\times$). What are all subrepresentations? They're all $W_1 + \oplus + W_r$ with W_i a subspace of V_i.

Theorem IX.1.3 (Brouwer's Theorem)

Every (complex finite-dimensional) character of every finite group G is a $\mathbb{Z}$-linear combination of characters that are induced from degree-1 characters of "elementary" subgroups.

Elementary subgroups are direct products of cyclic groups with p-groups, $C_m \times P$, where P is a p-group for some prime p.

IX.2. Products of Conjugacy Classes

Suppose G is a finite group and $C_1, \ldots, C_k$ are conjugacy classes in G. What can you say about the multiset $C_1 C_2 \cdots C_k$? It's a $(\mathbb{Z}_{\geq 0})$-linear combination of conjugacy classes.

$$\sum_{\substack{\text{conj. class}\\ C}} n_C C$$

where $n_C \in \mathbb{Z}_{\geq 0}$ are called the "structure constants of G."

In terms of the group algebra, define $e_C := \sum_{g \in C} e_g$. Then we are examining

$$e_{C_1} e_{C_2} \cdots e_{c_K} = \sum_{\substack{\text{conj. class}\\ C}} n_C e_C$$

We define

$$\mathcal{N}(C_1, \ldots, C_k) \coloneqq \#\text{ of } (g_1, \ldots, g_k) \in C_1 \times \cdots \times C_k \text{ s.t. } g_1 \cdots g_k = 1$$

If $k = 1$, then

$$\mathcal{N}(C_1) = \begin{cases} 1 & \text{if } C_1 = \{1\} \\ 0 & \text{otherwise} \end{cases} .$$

For $k = 2$, we have

$$\mathcal{N}(C_1, C_2) = \begin{cases} |C_1| & \text{if } C_1 = C_2^{-1} \\ 0 & \text{otherwise} \end{cases}$$

secretly this is the column orthogonality relation for characters.

For $k = 3$, we have

$$\mathcal{N}(C_1, C_2, C_3) = \#\{(g_1, g_2) \in C_1 \times C_2 \mid g_1 g_2 \in C_3^{-1}\}$$

this doesn't tell us much...

The answer! Representation Theory!

Theorem IX.2.1 (Frobenius's Theorem)

We have that

$$\mathcal{N}(C_1, \ldots, C_k) = \frac{|C_1| \cdots |C_k|}{|G|} \sum_{\substack{\text{irr.} \\ \chi}} \frac{\chi(C_1) \cdots \chi(C_k)}{\chi(1)^{k-2}}$$

We should verify it for small k. If $k = 1$, this reads as

$$\begin{aligned} \mathcal{N}(C_1) &= \frac{|C_1|}{|G|} \sum_{\chi} \frac{\chi(C_1)}{\chi(1)^{-1}} \\ &= \frac{|C_1|}{|G|} \sum_{\chi} \chi(C) \overline{\chi(1)} \\ &= \begin{cases} 1 & \text{if } C = \{1\} \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

by the column orthogonality relation. For $k = 2$, this reads as

$$\begin{aligned} \mathcal{N}(C_1, C_2) &= \frac{|C_1|\,|C_2|}{|G|} \sum_{\chi} \frac{\chi(C_1)\chi(C_2)}{\chi(1)^0} \\ &= |C_1| \cdot \frac{|C_2^{-1}|}{|G|} \sum_{\chi} \chi(C_1) \overline{\chi(C_2^{-1})} \\ &= \begin{cases} |C_1| & \text{if } C_1 = C_2^{-1} \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

Proof of Theorem IX.2.1. If C is a conjugacy class of G, define

$$e_C \coloneqq \sum_{g \in C} e_g \in \mathbb{C}[G]$$

for all representations $\rho : G \to \mathrm{GL}(V)$, any element $f \in \mathbb{C}[G]$ of the group algebra acts on V. Formally if $f = \sum_g f_g e_g$ we have L_f given by

$$\begin{aligned} L_f : V &\to V \\ v &\mapsto \sum_{g \in G} f_g(\rho(g)v) \end{aligned}$$

which is a $\mathbb{C}$-linear map. We simplify notation by writing $L_C = L_{e_C}$. It turns out that L_C is a representation of homomorphisms

$$L_C \rho(h) v = \sum_{g \in C} \rho(gh) v = \sum_{g \in C} \rho(hgh^{-1}h) v = \sum_{g \in C} \rho(hg) v = \rho(h) L_C v$$

If ρ is irreducible, then Schur's Lemma implies that L_C is a scalar multiple by some constant $\omega_\rho(C)$. Taking traces, we see that

$$\omega_\rho(C) \cdot \dim \rho = \mathrm{tr}(L_C) = \mathrm{tr}\left(\sum_{g \in C} \rho(g)\right) = \sum_{g \in C} \chi(g) = |C|\, \chi(C) = |C|\, \omega_\rho(C).$$

Therefore

$$\omega_\rho(C) = \frac{|C|\, \chi(C)}{\chi(1)}$$

We now compute the action $e_{C_1} \cdots e_{C_k}$ on $\mathbb{C}[G] = \bigoplus_{\substack{\text{irr.}\\ V_i}} (\dim V_i) V_i$ by the regular representation. On one hand we have

$$\begin{aligned} e_{C_1} \cdots e_{C_k} &= \sum_{g_i \in C_i} e_{g_1 \cdots g_k} \\ \mathrm{tr}(e_{C_1} \cdots e_{C_k}) &= \sum_{g_i \in C_i} \begin{cases} |G| & \text{if } g_1 g_2 \cdots g_k = 1 \\ 0 & \text{otherwise} \end{cases} \\ &= |G|\, \mathcal{N}(C_1, \ldots, C_k) \end{aligned}$$

But also $e_{C_1} \cdots e_{C_k}$ acts on V_i as scalar multiplication by $\omega_{\rho_i}(C_1) \cdots \omega_{\rho_i}(C_k)$. Then

$$\mathrm{tr}(e_{C_1} \cdots e_{C_k}) = \sum_i n_i^2 \omega_{\rho_i}(C_1) \cdots \omega_\rho(C_k)$$

where $n_i = \dim V_i = \chi_i(1)$ where χ_i is the character of ρ_i. We may then just substitute

$$\begin{aligned} \mathrm{tr}(e_{C_1} \cdots e_{C_k}) &= \sum_i n_i^2 \prod_{j=1}^{k} \frac{|C_j|\, \chi_i(C_j)}{\chi_i(1)} \\ &= \sum_i \prod_{j=1}^{k} \frac{|C_j|\, \chi_j(C_j)}{\chi_i(1)^{k-2}} \end{aligned}$$

Appendix A. Introduction to Category Theory

A.1. The Motivation

Category Theory as a subject grows out of a need to study the relationships between different areas of mathematics. Often this comes in the form of associating to every object in a certain area some object in another area according to some rules. A classic example is the fundamental group, which associates a group to every topological space (for more about algebraic topology, see [Hat02]).

To be able to formalize these types of mappings and their properties, we need a general setting for objects and also for maps between them. These will be our categories.

In the process, we will be able to give nice descriptions of many familiar objects in more abstract settings. The technique for doing so uses what are called universal properties. The advantage of these is that we can prove many results about things like free groups, tensor products, cartesian products, direct sums, and many more in extremely general settings. Such settings occur all throughout modern mathematics wherever groups might not be enough structure.

Most importantly though, we will develop a new way of looking at mathematics and of looking at definitions. This method of looking at things is sometimes appropriate and sometimes not. But it's a crucial tool in my mathematical toolbox, and one of the most elegant.

For my standard reference on this material see [Rie16]. For a more algebraic perspective see [Alu09]

A.2. The Basic Definitions

Lets go ahead and jump right into things!!!

Definition A.2.1

A category $\mathscr{C}$ has the following data:

- A class of objects $\operatorname{Ob}(\mathscr{C})$
- For any two objects $X, Y \in \mathscr{C}$ a class of arrows (aka morphisms aka maps, lots of names) $\operatorname{Hom}_{\mathscr{C}}(X,Y)$. We often write $f : X \to Y$ when the ambient category is clear to mean that $f \in \operatorname{Hom}_{\mathscr{C}}(X,Y)$. Sometimes one writes $\operatorname{Mor}_{\mathscr{C}}(X,Y)$ in place of $\operatorname{Hom}_{\mathscr{C}}(X,Y)$.
- For any three objects X, Y, Z, a function $\circ : \operatorname{Hom}_{\mathscr{C}}(Y,Z) \times \operatorname{Hom}_{\mathscr{C}}(X,Y) \to \operatorname{Hom}_{\mathscr{C}}(X,Z)$.

and it has the following structure:

- For every object X in $\mathscr{C}$, there is an arrow $\operatorname{Id}_X : X \to X$ so that for all $f : X \to Y$ and $g : Z \to X$ we have

$$f \circ \operatorname{Id}_X = f \qquad\qquad \operatorname{Id}_X \circ g = g$$

- Composition is associative. That is for $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$ we have

$$h \circ (g \circ f) = (h \circ g) \circ f$$

We say a category is **small** if it only has a set's worth of arrows in total (note this implies it has a set's worth of objects as well)

A category is **locally small** if it only has a set's worth of arrows between any two objects. We will mostly work with locally small categories.

One might ask what we can do that's interesting with such a broad collection of objects. For those wondering, remember how abstract groups are and how much structure they contain. Categories are not quite so well-behaved, but they are an extremely good setting for defining many many many well-behaved and beautiful things.

Example A.2.1

With this in mind, lets see some examples of categories. Many of these will be familiar to you!

Category	Objects	Morphisms
Set	sets	functions
Grp	groups	homomorphisms
Ab	abelian groups	homomorphisms
Vect_F	vector spaces over F	F-linear maps
R-Mod	modules over R	R-linear maps
Top	spaces	continuous maps
Haus	Hausdorff spaces	continuous maps
SmoothMan	smooth manifolds	smooth maps
Nat	natural numbers	ordering (a unique arrow $a \to b$ if $a \leq b$)

Notice that the collection of objects can be huge. This is why I specified a class of objects in the definition.

Exercise A.2.2

Show that these are all categories.

We can also make some suggestive definitions which give us a whole class of examples.

Definition A.2.2

We say that an arrow $f : X \to Y$ in a category is **invertible** (or is an **isomorphism**) provided there are arrows $g, h : Y \to X$ so that

$$g \circ f = \text{Id}_X \qquad f \circ h = \text{Id}_Y$$

In this case we may in fact show $g = h$ and that g is unique (exercise...). When only g exists, g is called a left inverse, and when only h exists, h is called a right inverse. We also say that X and Y are **isomorphic** via the isomorphism f, which may be written as $X \cong Y$ or more specifically $X \overset{f}{\cong} Y$.

We call a category $\mathscr{C}$ a **groupoid** provided that all of its morphisms are invertible.

Example A.2.3

To give an idea of how useful the idea of an isomorphism is, we list here the different isomorphisms in the above categories:

Category	Isomorphisms
Set	bijections
Grp	isomorphisms
Ab	isomorphisms
F-Vect	F-linear isomorphisms
R-Mod	R-linear isomorphisms
Top	homeomorphisms
Haus	homeomorphisms
SmoothMan	diffeomorphisms
Nat	equality of naturals

As one should expect, groupoids get their name for a reason! Which we now verify.

Exercise A.2.4

Show that groups and groupoids with one object are exactly the same.

Definition A.2.3

There are a variety of nice names for particular types of morphisms. We list them here

- An **endomorphism** is an arrow $f : X \to X$
- An **automorphism** is an invertible endomorphism
- A **monomorphism** is a morphism $f : X \to Y$ such that for all morphisms $g, h : Z \to X$ we have
$$f \circ g = f \circ h \implies g = h$$
- An **epimorphism** is a morphism $f : X \to Y$ such that for all morphisms $g, h : Y \to Z$ we have
$$g \circ f = h \circ f \implies g = h$$

We can describe a morphism as being **endo** (**auto, mono, epi**) as shorthand.

Example A.2.5

Category	Monomorphisms	Epimorphisms
Set	injections	surjections
Haus	continuous injection	continuous maps with dense image
Nat	any arrow	any arrow

Note that in the category Haus there are arrows which are both mono and epi but which are not isomorphisms. Consider the inclusion $A \hookrightarrow X$ of a dense subspace A in a space X.

We also make some convenient notation for talking about categorical concepts. Namely, we specify what a commutative diagram is at an informal level. Later we will make this formal in order to talk about other categorical concepts.

Definition A.2.4

A **commutative diagram** consists of drawn arrows and objects, and we specify that any way to get between two objects by composing morphisms are the same. A **diagram** simply removes the condition that any composition of arrows is equivalent.

This is best explained via many examples. As the simplest example, saying the left diagram commutes says that $g \circ f = h$, and saying that the right diagram commutes specifies that $p_2 \circ q_1 = q_2 \circ p_1$:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "h"'] & Y \arrow[d, "g"] \\ & Z \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "p_1"] \arrow[d, "q_1"'] & B \arrow[d, "q_2"] \\ C \arrow[r, "p_2"'] & D \end{tikzcd}$$

An often useful concept in category theory is *dualization*. Formally, this consists of replacing a category $\mathscr{C}$ by its "opposite" category $\mathscr{C}^{\text{op}}$

Definition A.2.5

Let $\mathscr{C}$ be some category. We define $\mathscr{C}^{\text{op}}$ by $\text{Ob}\,\mathscr{C}^{\text{op}} := \text{Ob}\,\mathscr{C}^{\text{op}}$, and $\text{Hom}_{\mathscr{C}^{\text{op}}}(X, Y) = \text{Hom}_{\mathscr{C}}(Y, X)$. The composition is then defined for $f : X \xrightarrow{\text{op}} Y, g : Y \xrightarrow{\text{op}} Z$ by

$$g \circ_{\text{op}} f = f \circ_{\text{op}} g$$

Identities remain the same as they are in the original category.

A.3. Functors and Natural Transformations

The natural question to ask in algebraic or categorical subjects when given a collection of objects is whether they form a category, that is what is the appropriate notion of a "morphism" between such objects. This of course extends to categories themselves.

Definition A.3.1

Given two categories $\mathscr{C}, \mathscr{D}$, a **functor** $F : \mathscr{C} \to \mathscr{D}$ consists of the following data

- For every object $X \in \text{Ob}\,\mathscr{C}$ a unique object $F(X) \in \mathscr{D}$
- For every arrow $f : X \to Y$ in $\mathscr{C}$ a unique arrow $F(f) : F(X) \to F(Y)$ in $\mathscr{D}$

satisfying the functoriality laws

- $F(\text{Id}_X) = \text{Id}_{F(X)}$
- For $f : X \to Y$ and $g : Y \to Z$ in $\mathscr{C}$ we have

$$F(g \circ f) = F(g) \circ F(f).$$

A functor $F : \mathscr{C}^{\text{op}} \to \mathscr{D}$ might be called a **contravariant functor** from $\mathscr{C}$ to $\mathscr{D}$, whereas $F : \mathscr{C} \to \mathscr{D}$ is called **covariant**. A contravariant functor satisfies for $f : X \to Y$, $g : Y \to Z$ in $\mathscr{C}$ that

$$F(g \circ f) = F(f) \circ F(g).$$

Example A.3.1

Say $\mathscr{C} = \text{Grp}$ and $\mathscr{D} = \text{Set}$. Then there is a functor from $\mathscr{C}$ to $\mathscr{D}$ given by taking a group G and "forgetting" the group structure to obtain a mere set G. The action on group homomorphisms is to "forget" that they respect the group operation.

There is also a functor Set → Grp, which associates a set S to the "free group" on S. Formally, this consists of all words in the language $S \cup S^{-1}$ (where S^{-1} is a formal copy of S, where we take $s^{-1} \in S^{-1}$ if $s \in S$). Two words are considered equivalent via the reduction rule which deletes pairs $ss^{-1}, s^{-1}s$, and the operation on words is concatenation. (The empty word being the identity element)

These two functors are intimately related, and we will discover they are "adjoint" in **??**

Example A.3.2

There is a functor $\pi_0 : \mathrm{Top} \to \mathrm{Set}$ given on objects by taking a topological space X and mapping it to the set of path components of X (that is the largest subspaces of X which are path-connected).

Given a continuous map $f : X \to Y$, $\pi_0(f)$ is given by consdering some path component U of X, then $f(U)$ is path-connected and non-empty, so it belongs to a unique path component V of Y. We then set $[\pi_0(f)](U) = V$.

Generally, there are many techniques to associate sets, groups, rings, and other algebraic structures to spaces. This is the realm of algebraic topology, and almost always these associations are functorial. In fact the notation π_0 suggests the corresponding $\pi_1, \pi_2, \ldots$. In this case $\pi_1 : \mathrm{Top} \to \mathrm{Grp}$, and for $n > 1$ we have $\pi_n : \mathrm{Top} \to \mathrm{Ab}$.

For more on this subject, [Hat02] is the standard reference, and [May99] is a more concise and modern treatment.

Example A.3.3

Given two categories $\mathscr{C}, \mathscr{D}$ one can form the product category $\mathscr{C} \times \mathscr{D}$ in the natural way. Then for locally small categories there is a functor

$$\mathrm{Hom}_{\mathscr{C}} : \mathscr{C}^{\mathrm{op}} \times \mathscr{C} \to \mathrm{Set}\,.$$

On objects this agrees with the notation we have previously established, so that $\mathrm{Hom}(X, Y)$ is the set of arrows from X to Y in $\mathscr{C}$. On arrows, if we have $f : X' \to X$ and $g : Y \to Y'$ in $\mathscr{C}$ (seeing that $f^{\mathrm{op}} : X \to X'$ in $\mathscr{C}^{\mathrm{op}}$) we have the function

$$\begin{aligned} \mathrm{Hom}(f, g) : \mathrm{Hom}(X, Y) &\to \mathrm{Hom}(X', Y') \\ h &\mapsto g \circ h \circ f \end{aligned}$$

Functoriality may be easily verified. As we should expect, the Hom functor carries a lot of the information about $\mathscr{C}$, as it encodes composition in the category.

We also have for fixed $X \in \mathrm{Ob}\,\mathscr{C}$ that $\mathrm{Hom}(X, -), \mathrm{Hom}(-, X)$ are contravariant/covariant functors respectively from $\mathscr{C} \to \mathrm{Set}$, as one should expect.

Exercise A.3.4

Prove that Hom is functorial.

Exercise A.3.5

There is a functor $\mathrm{Vect}^{\mathrm{op}} \to \mathrm{Vect}$ given by taking a vector space V to its dual V^*.

Work out the details of how this functor acts on linear maps and why it is functorial.

Exercise A.3.6

Show that, informally (that is without regards to set-theoretic size issues), define the category of all categories Cat.

The next natural question to ask is what are the arrows between functors themselves?

Definition A.3.2

A **natural transformation** $\eta : F \Rightarrow G$ between two functors $F, G : \mathscr{C} \to \mathscr{D}$ is a collection of maps $\eta_X : F(X) \to G(X)$ for each $X \in \operatorname{Ob} C$ satisfying the following commutative diagram for each arrow $f : X \to Y$

$$\begin{tikzcd} F(X) \arrow[r, "F(f)"] \arrow[d, "\eta_X"'] & F(Y) \arrow[d, "\eta_Y"] \\ G(X) \arrow[r, "G(f)"'] & G(Y) \end{tikzcd}$$

This is called the **naturality condition** or **naturality square**.

Exercise A.3.7

For fixed categories $\mathscr{C}, \mathscr{D}$, define a category $[\mathscr{C}, \mathscr{D}]$ whose objects are functors $\mathscr{C} \to \mathscr{D}$ and whose arrows are natural transformations.

Exercise A.3.8

Show that the "double dual" functor taking V to $(V^*)^*$ from Vect → Vect is naturally isomorphic (that is isomorphic in $[\mathrm{Vect}, \mathrm{Vect}]$) to the identity functor $\mathrm{Id}_{\mathrm{Vect}}$.

Fortunately, this marks the "end of the line" for standard category theory. At higher levels of category theory, we can define higher morphisms, but for most mathematical purposes this level is sufficient.

Exercise A.3.9

Try to come up with a cohesive definition of arrows between two natural transformations $\eta, \mu : F \Rightarrow G$.

Exercise A.3.10

Given $\eta : F \Rightarrow G$, where $F, G : \mathscr{C} \to \mathscr{D}$ and $\mu : F' \Rightarrow G'$ where $F', G' : \mathscr{D} \to \mathscr{E}$ define

$$\eta \cdot \mu : F' \circ F \Rightarrow G' \circ G$$

this is called the "horizontal composition" of natural transformations, whereas the other composition is called the "vertical composition" and written $\eta \circ \eta'$. Show that where it makes sense we have

$$(\eta \circ \eta') \cdot (\mu \circ \mu') = (\eta \cdot \mu) \circ (\eta' \cdot \mu').$$

This is called the **interchange law**.

Functors / Natural Transformations

A.4. Presheaves and the Yoneda Lemma

A.5. Adjoint Functors

Write a Category Theory Appendix with Good References

References

[Alu09] Paolo Aluffi. *Algebra : Chapter 0*. American Mathematical Society, 2009. ISBN: 9780821847817.

[Hat02] Allen. Hatcher. *Algebraic Topology*. Algebraic Topology. Cambridge University Press, 2002. ISBN: 052179160X. URL: https://pi.math.cornell.edu/~hatcher/AT/ATpage.html.

[May99] J Peter May. *A concise course in algebraic topology*. University of Chicago press, 1999.

[Rie16] Emily Riehl. *Category Theory in Context*. Dover Publications Inc, 2016. URL: https://math.jhu.edu/~eriehl/context.

TODOS: