If the upper central series terminates at $G$, then $G$ is <u>nilpotent</u>. (ie, $Z_k(G) = G$ for some $k \in \mathbb{N}$).

<u>Prop</u>: Suppose $G$ is a finite $p$-gp. Then $G$ is nilp.

<u>Pf</u>: $1 \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots$

$Z_1(G) = Z(G)$ ↑ non trivial

$G/Z(G)$ is a $p$-gp (by Lagrange), so $Z(G/Z(G)) \neq 1$

so $|Z(G/Z(G))| \geq p \Rightarrow |Z_{i+1}(G)| \geq p \cdot |Z_i(G)|$

↑ if $Z_i(G) \neq G$ ↑ b/c inv. image of

so series doesn't stabilize,

$\therefore$ must terminate at $G$.

<u>Heisenberg Gp</u>: $H_3(R) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \; a,b,c \in R \right\}$ ← any commutative ring w/ unity

$|H_3(\mathbb{F}_p)| = p^3$, so finite $p$-gp & $\therefore$ nilpotent.

[u.c.s. is unique, so length is well-def, so can classify nilp gp by length of ucs]

$1 \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) = G$

↑ order $p$ or ~~$p^2$~~ b/c $\neq H_3$, not abel.

any gp of order $p^2$ is abel $\Leftarrow |G/Z(G)| = p^2$

~~$p^2$~~ b/c then cyclic & $H_3$ abel. $\Rightarrow$ order $p$

so $Z_1(G) = Z(G) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \; b \in \mathbb{F}_p \right\}$ so $Z(G/Z_1(G)) = G/Z_1(G)$

$\Rightarrow Z_2(G) = G$

Thm: $A_n$ is simple for $n \geq 5$.

Pf: $N \trianglelefteq A_n$. If $N$ has a 3-cycle, then $A_n = N$
(since $A_n$ acts transitively on 3-cycles).

- If $\exists \tau \in N$ whose disjoint cycle decomp contains a $n$-cycle. for $n \geq 4$, then $n$ contains a 3-cycle.
  $\tau = \sigma_1 \sigma_2 \cdots \sigma_k \pi$ , $\pi = (a_1 a_2 a_3 a_4 \cdots)$
  $\pi' = (a_1 a_2 a_3) \pi (a_3 a_2 a_1)$ (conjugate of $\pi$)
  $= (a_2 a_3 a_1 a_4 \cdots)$
  $\tau' = \sigma_1 \sigma_2 \cdots \sigma_k \pi' = (a_1 a_2 a_3) \tau (a_3 a_2 a_1) \in N$
  $\tau' \tau^{-1} = \pi \pi' = (a_1 a_2 a_4)$
- 2 cycles of length $\leq 3 \Rightarrow$ length 4 $\Rightarrow$ length 3

⋮

$N$ can only contain $\pi_e$.

10/18 Serre, Linear Representations of Finite Gps } 1st chapter
Fulton-Harris, Representation Theory
Maclane, Categories for the Working Mathematician

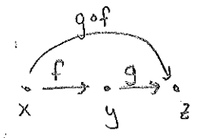
We have seen that the study of gp actions on sets is useful for the intrinsic study of gps.
We can get even more from studying group actions on other things (on gps, on top sp's, on vector sp's, etc.).
Warning: When we say "$G$ acts on a top. sp", eg $\mathbb{Z}/2\mathbb{Z}$ @ circle $S^1$, we mean a map $f: S_1 \to S_1$ s.t. $f \circ f = id$. (a continuous map b/c of the context, not just an arbitrary assignment) [$f: G \to H$ means gp homomorphism]
Similarly if $V, W$ are vector sp's over $\mathbb{R}$, then $f: V \to W$ must mean an $\mathbb{R}$-linear map ($f(v+w) = f(v) + f(w)$, $f(xv) = x f(v)$ $\forall x \in \mathbb{R}$)

Category Theory formalizes this notion of context & forms the language of modern alg

Def: A category $C$ consists of:
- a set of objects $Ob(C)$
- for each pair of objects, $x, y$ a set of morphisms $Mor_C(x,y)$

endowed with a composition law,

$Mor_C(x,y) \times Mor_C(y,z) \to Mor_C(x,z)$,




which is associative

$h \circ (g \circ f) = (h \circ g) \circ f \in Mor_C(x,w)$

and for each object $x \in Ob(C)$, $\exists$ a special morphism $id_x : x \to x$ (ie, $id_x \in Mor_C(x,x)$)

s.t. $\forall f: x \to y$, $f \circ id_x = f = id_y \circ f \in Mor_C(x,y)$

Ex: ① Set = C; Ob(C) = sets
Mor(x,y) = functions from x to y

② C = Top; Ob(C) = top. sp's
Mor(x,y) = continuous fcns from x to y

③ C = Grp; Ob(C) = groups
Mor(x,y) = homomorphisms from x to y.

④ C = Vect/$\mathbb{C}$; Ob(C) = $\mathbb{C}$-vector sp's
Mor(v,w) = $\mathbb{C}$-linear homomorphisms.

⑤ Let X be a fixed top. sp.

i) Ob(C) = pts of X
Mor(x,y) = paths from x to y


ii) Ob(C) = pts of X
Mor(x,y) = isotopy classes of paths from x to y.

Isotopic


Disc

not isotopic

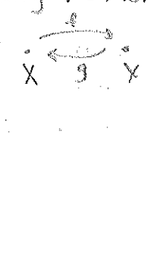

Annulus

↑ 2 paths are in same class if can continuously move from one path to the other

- When X = disc, $|Mor(x,y)| = 1$ b/c only one class
- When X = annulus, many diff classes

Interesting feature of Isotopx: For any $f \in Hom(x,y)$, there is an inverse:

a morphism $g: y \to x$ s.t. $g \circ f = id_x$ & $f \circ g = id_y$







A category in which every morphism has an inverse is a groupoid.

(almost a gp except can't compose any 2 morphisms)

Suppose C is a groupoid w/ only one object. Then the only morphisms in C are those from $x \to x$, & these form a group.

Def: A group is a groupoid with one object.

A monoid is a category w/ one object.

What are morphisms from one category to another?

ie, what is the category of categories?

Def: If C & D are categories, a functor from C to D, F, is the following data:

- A map of sets $F: Ob(C) \to Ob(D)$
- Maps of sets $F_{xy}: Mor_C(x,y) \to Mor_D(F(x), F(y))$

s.t. $F(f \circ g) = F(f) \circ F(g)$ & $F(id_x) = id_{F(x)}$.

Ex: ⑥ Ab = category of abelian gps

(a full subcategory of Grp ← contains all morphisms of Grp).

Abelianization is a functor from Grp to Ab.:

$F(G) = G^{ab} \in Ob(Ab)$ ✓

$\in Ob(G)$

NTS: given $f \in Mor_{Grp}(G,H)$ $\exists$ $F(f) \in Mor_{Ab}(F(G),F(H))$

$= Mor_{Ab}(G^{ab}, H^{ab})$

(done in HW)

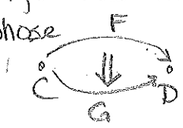
By contrast, "center" is not a functor: I could try to define a functor $Z: \underline{Grp} \to \underline{Ab}$ s.t. $Z(G) = Z_G$, the center of $G$.
But - what would you do on morphisms?
given $f: G \to H$, want $Z(f): Z_G \to Z_H$.
eg: $\mathbb{Z}/2\mathbb{Z} \to S_3$ but $S_3$ has trivial center, while
$1 \longmapsto (12)$ $\mathbb{Z}/2\mathbb{Z}$ is abelian.

For any category $C$ & any object $x$,

For a gp $G$, thought of as a 1-object category, $C_G$,
a set $X$ w/ a $G$-action is a functor, $F$, from $C_G$ to $\underline{set}$.
- $F$(the unique object) is $X$
- morphism from obj. to self go to morphisms of the set $X$.

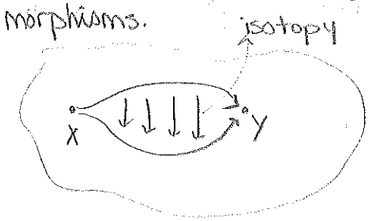
A top. sp. w/ $G$-action is a functor from $C_G$ to $\underline{top}$.
A vector sp. over $\mathbb{C}$ w/ $G$-action (is a $\underline{\text{representation of } G}$) is a functor from $C_G \to \underline{Vect}/\mathbb{C}$.

$\underline{Cat}$, $Ob(\underline{Cat})$ are categories, $Mor_{\underline{cat}}$ are functors.
But, $Mor_{cat}(x,y)$ has more structure. It is a category, whose obj's are functors, & morphisms btwn functors are natural transformations.




$C, D$ are cats, $F, G$ are functors

This is called a 2-category w/ a 3-level structure of morphisms.




w/ 2 isotopies, could be cont. transformed into e/o, so $\exists$ iso. btwn iso's.

10/23 Serre, Lin. Rep's of Finite Gps

**Def**: Let $K$ be a field (eg, $\mathbb{C}, \mathbb{R}, \mathbb{F}_q$) & $G$ a gp.
A *representation of $G$ over $K$* is a pair $(V, \rho)$, where $V$ is a vector sp over $K$ & $\rho$ is an action of $G$ on $V$ by $K$-linear homomorphisms.
ie, $\rho$ is a gp hom.

$$\rho : G \to GL(V) \quad \text{(General Linear Gp on } V\text{)}$$
$$\hookrightarrow \text{gp of } K\text{-linear autō's of } V.$$

* Note: when $V = K^n$, then a $K$-lin. auto of $V$ is given by an $n \times n$ matrix w/ coeff's in $K$ that's invert. (b/c auto) ie $GL(K^n) = GL_n(K)$.

(any 2 $n$-dim vector sp's are isomorphic)

**Ex**: ① $D_p$, the dihedral gp of order $2p$.

$= \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$
(generator $\sigma$, generator $\tau$)

There is a representation $\rho : D_p \to GL(\mathbb{R}^2)$ where
$\rho(\sigma) =$ counterclockwise rotation by $2\pi/p$

$$= \begin{pmatrix} \cos\frac{2\pi}{p} & -\sin\frac{2\pi}{p} \\ \sin\frac{2\pi}{p} & \cos\frac{2\pi}{p} \end{pmatrix}$$

& $\rho(\tau) =$ reflection through $x$-axis

$$= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Note :: $D_p = \langle \sigma, \tau \mid \tau\sigma\tau^{-1} = \sigma^{-1},\ \tau^2 = 1,\ \sigma^p = 1 \rangle$
(not same set of generators given in HW)
* to show $\rho$ a hom, need to check 3 relations hold: true.

Easy to check $\rho$ injective, so $\rho(D_p) \leq GL_2(\mathbb{R}) \simeq D_p$.
In fact, it is the stabilizer in $GL_2(\mathbb{R})$ of the regular $p$-gon

② 1-dim $\mathbb{C}$-reps of $\mathbb{Z}/n\mathbb{Z}$:

$V = \mathbb{C}$

we need to specify $\rho: \mathbb{Z}/n\mathbb{Z} \to GL_1(\mathbb{C}) = \mathbb{C}^*$, which amounts to specifying $\rho(1) = z \in \mathbb{C}^*$ s.t. $z^n = 1$.

$z = n^{th}$ root of unity; $n$ choices:

$\rho(1) = 1, e^{2\pi i/n}, e^{4\pi i/n}, \dots, e^{(n-1)2\pi i/n}$

③ The gp $S_3$ has a 3-dim rep $(\mathbb{C}^3, \rho)$ defined as follows:

[Note: dim of rep = dim(V)]

$\mathbb{C}^3$ has as a basis $e_1, e_2, e_3$ & can define for each $\pi \in S_3$: $\underbrace{\rho(\pi)}_{\text{auto of } \mathbb{C}^3}(e_i) = e_{\pi(i)}$

More generally, let $X$ be a finite set with an action of $G$. Then there is a <u>permutation representation</u> of $G$ assoc. to $X$ where $V$ is the vector sp w/ basis $\{e_x\}_{x \in X}$ ($\dim V = |X|$) (called $K\langle X \rangle$ (free vector sp on basis $X$)) ie,

$V = \{\sum_{x \in X} a_x e_x\}$. $a_x \in K$. & $\rho$ is defined by:

$\rho(g)(\sum_{x \in X} a_x e_x) = \sum_{x \in X} a_x e_{gx}$ (since $gx \in X$ b/c $G \curvearrowright X$)

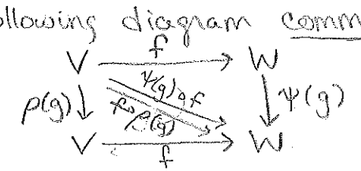
Return to 3-dim perm rep $\rho: S_3 \to GL_3(\mathbb{C})$.

Note: if $\alpha \in GL_3(\mathbb{C})$ then we can define another rep' of $S_3$, $\rho_\alpha$, by $\rho_\alpha(\pi) = \alpha^{-1}\rho(\pi)\alpha$. This is still a hom. b/c

$\rho_\alpha(\pi_1)\rho_\alpha(\pi_2) = \alpha^{-1}\rho(\pi_1)\alpha\alpha^{-1}\rho(\pi_2)\alpha = \alpha^{-1}\rho(\pi_1)\rho(\pi_2)\alpha$

$= \alpha^{-1}\rho(\pi_1\pi_2)\alpha = \rho_\alpha(\pi_1\pi_2)$.

We say 2 rep's of $G$ $(V, \rho)$ & $(W, \Psi)$ are <u>isomorphic</u> if $\exists$ an isomorphism $f: V \to W$ (ie, $\dim V = \dim W$) s.t. the following diagram <u>commutes</u> $\forall g \in G$: ↳ $\Psi(g) \circ f = f \circ \rho(g)$




$V \to W$ ↓ ↻ ↓ $V \to W$

f <u>intertwines</u> $\rho$ & $\Psi$.

Ex: $\rho$ & $\rho_\alpha$ are isomorphic: the map intertwining $\rho$ & $\rho_\alpha$ is $\alpha : \mathbb{C}^3 \to \mathbb{C}^3$ (or $\alpha^{-1}$)

In particular, if $(V,\rho)$ a rep of $G$ & $\dim V = n$, then $\exists\ f: V \xrightarrow{\sim} K^n$

$$\begin{array}{ccc} V & \xleftarrow{f} & K^n \\ {\scriptstyle \rho(g)}\downarrow & & \downarrow{\scriptstyle \Psi(g) := f\circ\rho(g)\circ f^{-1}} \\ V & \xleftarrow[f]{} & K^n \end{array}$$

Defining $\Psi = f\circ\rho(g)\circ f^{-1}$, we have $(V,\rho) \simeq (K^n, \Psi)$ where $\Psi: G \to GL_n(K)$

In other words, every f.d. rep of $G$ is $\simeq$ to one where the vector sp is $K^n$.

Fact: (proof will come later) If $G$ is finite, then there are only finitely many isomorphism classes of $n$-dim. reps of $G$.

Recall: (re: gp actions on sets) If $G \curvearrowright X$ & $Y \subseteq X$ which is stable under the action of $G$ (ie, $gy \in Y\ \forall g\in G\ \forall y \in Y$) then $X\setminus Y$ is also stable under $G$ & we can break up $X = Y \amalg X\setminus Y$, a disjoint union of 2 diff. sets w/ $G$-action.

[But note, it's not the case that a general fcn $f: X \to X$ has this property. eg. $X = \{1,\dots,n\}$, $f(x) = x+1$ if $x \le n-1$ & $f(n) = n$. $1 \to 2 \to 3 \to 4 \to 5 \to 6 \to \cdots \to n-1 \to n \circlearrowright$

so $\{n\}$ is stable for $f$. But $\{n\}^c$ is not stable.]

(but since $G$ a gp, its elts act invertibly on $X$)

Def: Let $(V,\rho)$ a rep of $G$. A subrep of $(V,\rho)$ is a subspace $W \subseteq V$ which is stable under $G$, (ie $gw \in W\ \forall g\in G\ \forall w \in W$)

↑ means $\rho(g)(w)$

Ex: Permutation rep of $S_3$ on $\mathbb{C}^3$. If $W = \mathbb{C}\cdot(e_1+e_2+e_3)$, $W$ is stable under $S_3$, so this is a 1-dim. subrep.

Def: If $(V,\rho)$ & $(W,\Psi)$ are reps of $G$, their direct sum is the rep $(V\oplus W, \rho\oplus\Psi)$
ie. $\rho\oplus\Psi(v,w) = (\rho(v),\Psi(w))$

Thm: If $K$ is a field of characteristic 0 (eg $\mathbb{C}$), & $G$ is finite & $V$ a f.d. rep of $G$ & $W$ a subrep., then $\exists$ another subrep $W'$ of $V$ s.t. $V = W\oplus W'$.

Ex (from above: $S_3$ on $\mathbb{C}^3$). By thm, there should be a complementary subrep $W'$ to $W$. Must be 2-dim, stable under $G$, & disj. from $W$.
- Is $e_1 \in W'$? Then so is $e_2$ & $e_3$ b/c $e_2 = ge_1$, etc., but then $W' = \mathbb{C}^3$. $e_1 \notin W'$.
- Is $e_1+e_2 \in W'$? Then also have $e_2+e_3$ & $e_1+e_3 \Rightarrow e_1+2e_2+e_3 \Rightarrow 2e_2 \Rightarrow e_2 \in W'$, so then $W' = \mathbb{C}$; $e_1+e_2 \notin W'$.
- Need another comb of $e_i$ invariant under $G$, but then just $a(e_1+e_2+e_3) \Rightarrow$ No others
- Is $e_1-e_2 \in W'$? Then $e_2-e_1$, $e_1-e_3$, $e_2-e_3$, & sums get other differences. These generate the desired 2-dim subrep $W'$.

So, $W' = \{a_1e_1+a_2e_2+a_3e_3 \mid a_1+a_2+a_3 = 0\}$ (stable under $G$).

10/25

Recall: If $V$ a rep. of $G$, a subrep of $V$ is a subsp $W \subseteq V$ which is stable under $G$-action (ie $gw = w \ \forall g \in G$).

Thm: Let $G$ a finite gp & $K$ a field of char 0, & $V$ a rep of $G$ over $K$ & $W$ a subrep of $V$. Then $\exists$ another subrep $W' \subset W$ s.t. $V = W \oplus W'$.

Pf: Let $W_0$ be a subsp. of $V$ complementary to $W$ (ie $W_0 \cap W = \{0\}$ & $W_0 + W = V$) so that every $v \in V$ has a unique expression $v = w + w_0$ $w \in W$, $w_0 \in W_0$ (ie, $V = W \oplus W_0$).

Thus we have a projection map $p: V \to W$ defined by $p(w + w_0) = w$.

$\ker p = W_0$. It would be nice if $W_0$ were stable under $G$-action. Make it so!

Define $\pi : V \to W$ as $\pi = \frac{1}{|G|} \sum_{g \in G} g \circ p \circ g^{-1}$.

More precisely,

$$\pi(v) = \frac{1}{|G|} \sum_{g \in G} \rho(g)\big(\underbrace{p(\rho^{-1}(g)(v))}_{\in W \text{ \& stable under } G\text{-action}}\big) \in W$$

$$\begin{array}{ccc} \rho(g^{-1}) \circlearrowleft & & \rho(g) \circlearrowright \\ V & \xrightarrow{p} & W \end{array}$$

Define $W'$ to be $\ker \pi$. Claim this $W'$ is the desired complementary subrep of $V$.

- Why is $W'$ stable under $G$?

  Let $w' \in W'$, NTS $hw' \in W' \ \forall h \in G$.

  ie, $\pi(hw') = 0$

$$\pi(hw') = \frac{1}{|G|} \sum_{g \in G} g \circ p \circ g^{-1} \circ h(w')$$

$$h^{-1}(\pi(hw')) = \frac{1}{|G|} \sum_{g \in G} h^{-1} \circ g \circ p \circ g^{-1} \circ h(w')$$

$$= \frac{1}{|G|} \sum_{g \in G} (h^{-1}g) \circ p \circ (h^{-1}g)^{-1}(w') \quad \leftarrow \text{will still sum over } \forall g \in G.$$

$$= \pi(w') = 0$$

$\Rightarrow \pi(hw') = h(h^{-1}(\pi(hw'))) = h(0) = 0$.

*P not invariant under conjugates by G, so take avg. of sums of conjugates of P by G, & that will fix the problem *

Recall: $p(\omega) = \omega \quad \forall \omega \in W$.

So $\pi(\omega) = \frac{1}{|G|} \sum_{g \in G} g \circ p \circ g^{-1}(\omega) = \frac{1}{|G|} \sum_{g \in G} g \circ g^{-1}(\omega) = \frac{1}{|G|} \sum_{g \in G} \omega$
$= |G| \cdot \frac{1}{|G|} = \omega$.

So if $\omega \in W \cap W'$, then $\pi(\omega) = \omega$ but $\pi(\omega) = 0$ (b/c $W' = \ker \pi$). $\Rightarrow \omega = 0$.

So $W \cap W' = 0$. And $\pi : V \to W$ is surjective
$\Rightarrow \dim W' = \dim V - \dim W$
$\Rightarrow V = W \oplus W'$!

- We used G finite to make $\sum_{g \in G}$. (more generally, works for G a cpt gp, instead of $\sum$, do $\int$)
- We used char $K = 0$ to make $\frac{1}{|G|}$ make sense. (if char $k = p$ & $|G| = np$, then would be $\div$ ing by 0)

In fact, assertion is false w/o hypotheses:

ex: ① $G = \mathbb{Z}/p\mathbb{Z} = \langle \gamma \rangle$, $k = \mathbb{F}_p$

$V$ = 2-dim. rep, basis $e_1, e_2$

A homomorphism

$\rho : G \to GL(V) = GL_2(\mathbb{F}_p)$

$\rho(\gamma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$\rho(\gamma^p) = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Note that $\rho(\gamma) e_1 = e_1$, so $ke_1$ is stable under action of G. But it is not the case that V has another 1-dim subrep (b/c that would be another eigenvector, but $\rho(\gamma)$ only has 1).

(diagonalizable = basis of eigenvector ie → eigenvalues distinct)

So V does not split as the sum of 2 1-dim subreps

② $G = \mathbb{Z} = \langle \gamma \rangle$ $\quad K = \mathbb{C}$

$\rho(\gamma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

won't decompose for same reason.

**Def:** We say a rep $V$ of $G$ is <u>irreducible</u> if it has no subreps other than $0$ & $V$.

**Cor:** If $G$ finite & $\mathrm{char}\, k = 0$, every f.d rep $V$ splits up as a direct sum $V = V_1 \oplus \cdots \oplus V_r$ with $V_i$ irred.

**Pf:** Induction on $\dim V$.

Let $V$ be smallest counterexample, so $V$ cannot be irred (b/c counter-ex) so $\exists\ W \subset V$, $\dim W < \dim V$, $\dim W > 0$, so $V = W \oplus W'$, & $W$ & $W'$ can be written as direct sum of irreds by ind. hyp.

**Ex:** Irred. reps of $S_3$. (over $\mathbb{C}$)

① Trivial rep: $V = \mathbb{C}$, $g$ acts trivially on $G$ $\forall g \in S_3$ ($\dim V = 1 \Rightarrow$ irred.)

② Permutation rep: $V =$ perm rep ($\dim V = 3$)

$V = \mathbb{C} \oplus V_0 \qquad \dim(V_0) = 2$

$\mathbb{C} = \langle e_1 + e_2 + e_3 \rangle$, $V_0 = \{a_1 e_1 + a_2 e_2 + a_3 e_3 \mid a_1 + a_2 + a_3 = 0\}$

<u>Claim</u>: $V_0$ is irred.

Suppose not. Then $V_0 = W \oplus W'$, both 1-dim.

Note that $(123)$ is a <u>commutator</u> in $S_3$

$[(12)(23)(12)^{-1}(23)^{-1}]$

[Derived subgp of $S_n$ is $A_n$]

$\rho_W : S_3 \to GL(W) \leftarrow$ abel. ($1 \times 1$ matrix is abelian gp)

$\rho_{W'} : S_3 \to GL(W')$

so $\rho_W(123) = \mathrm{id}$, $\rho_{W'}(123) = \mathrm{id}$ } b/c commutator vanishes in hom. to abel. gp.

So $(123)$ acts trivially on $W$ & $W'$, whence on $W \oplus W'$

but $(123)(e_1 - e_2) = e_2 - e_3$ ↯ so $V_0$ is irred.

③ Let $V$ be an irred. rep. of $S_3$.
$\sigma = (123)$
$\rho(\sigma) \in GL(V)$ is an elt of order 3.
[A finite order matrix is diagonalizable]
We can restrict $\rho$ to $\langle\sigma\rangle \cong \mathbb{Z}/3\mathbb{Z}$. In this case, $V$ breaks up as $\oplus V_i$, where $V_i$ are irred reps of $\mathbb{Z}/3\mathbb{Z}$. (could have subsp's that are stable under $\mathbb{Z}/3\mathbb{Z}$ but not under $S_3$).

Sidebar: Irreps of $\mathbb{Z}/n\mathbb{Z}$?
Lemma: An irrep of $\mathbb{Z}/n\mathbb{Z}$ is 1-dim.
Pf: Let $V$ an irrep of $\mathbb{Z}/n\mathbb{Z} = \langle\gamma\rangle$. Let $v$ be an eigenvector of $\gamma$, so $\gamma v = \lambda v$
$\gamma^2 v = \lambda^2 v$
$\gamma^n v = \lambda^n v = v$ (b/c $\gamma^n = 1$)
$\Rightarrow \lambda^n = 1$
So $\mathbb{C}v$ is stable under $G$-action. (b/c $G$-action on this is just mult. by scalar). So $V$ has a 1 dim subrep, so dim $V = 1$.
To define $V_i$, just need to give $\lambda$, & there are only $n$ of them. (b/c $\lambda^n = 1$)

③ (cont.) So $V = \oplus V_i$ where each $V_i$ is a 1-dim sp. on which $\rho(\sigma)$ acts as either $1$, $\omega = e^{2\pi i/3}$, $\omega^2$ } these are $\lambda$ (eigenvalues)

$V_1 = \langle$eigenvectors of $\sigma$ w/ e-val $1\rangle$
similarly, $V_\omega$, $V_{\omega^2}$.
$V = V_1 \oplus V_\omega \oplus V_{\omega^2}$ (this is w/ $\rho$ restricted to $\langle\sigma\rangle$)
Claim: $V_1$ is stable under $S_3$.
Suppose $v \in V_1$, $\sigma v = v$. Let $\tau = (12)$
($\sigma$ & $\tau$ gen. $S_3$, so enough to show $\tau v \in V_1$)
$\sigma(\tau v) = ?$
$\tau^{-1}\sigma\tau v = \sigma^{-1} v = \sigma^2 v = v \Rightarrow \sigma(\tau v) = \tau v$ (so $\tau v \in$ gp gen by $\sigma = V_1$)

Thm: More generally, if $H \trianglelefteq G$ & $V$ a rep of $G$, then $V^H = \{v \in V \mid hv = v \ \forall h \in H\}$ is a sub-$G$ rep. of $V$.

③ (cont) Either $V_1 = V$ or $V_1 = 0$.

Suppose $V_1 = V$. Let $v \in V_1$, & $V(v) = \text{span}(v, \sigma v, \sigma^2 v, \tau v, \tau\sigma v, \tau\sigma^2 v)$.

$V(v)$ is clearly stable under $S_3$ (b/c $S_3$ just moves these vectors around but doesn't leave span). $\Rightarrow \dim V(v) \leq 6$.

(∃ an upper bound for reps : $|G|$)

Since $v \in V_1$, $\sigma v = \sigma^2 v = v$ & $\tau v = \tau\sigma v = \tau\sigma^2 v$,

so $V(v) = \text{span}(v, \tau v)$, so $\dim V(v) \leq 2$.

In fact, consider

$\left.\begin{array}{l} \text{span}(v + \tau v) = V(v)^+ \\ \text{span}(v + \tau v) = V(v)^- \end{array}\right\}$ $\dim V(v)^{\pm} \leq 1$

These are stable under $S_3$-action:

eg: $\sigma(v + \tau v) = \sigma v + \sigma\tau v = v + \tau\sigma^2 v = v + \tau v$

(true for both elts & all elt in $S_3$)

$\Rightarrow V(v)^+$ is a subrep of $V$, so either

$V(v)^+ = V$ (so $\dim V = 1$) or $V(v)^+ = 0$

Similarly, either $V(v)^- = V$ ($\dim V = 1$) or $V(v)^- = 0$

But if $V(v)^+ = 0$ & $V(v)^- = 0 \Rightarrow$ $v + \tau v = 0$

$+ \ v - \tau v = 0$

$v = 0$

so $\dim V = 1$.

10/30 Tensor Products

$\langle , \rangle : V \times W \to X$ a bilinear pairing.

ie $\langle v_1 + v_2, w \rangle = \langle v_1, w \rangle + \langle v_2, w \rangle$

& $\langle v, w_1 + w_2 \rangle = \langle v, w_1 \rangle + \langle v, w_2 \rangle$

& $\langle cv, w \rangle = c\langle v, w \rangle = \langle v, cw \rangle \quad \forall c \in F$

(F-vector spaces $V$ & $W$)

$\langle a(v,w) \rangle = \langle av, aw \rangle = a^2 \langle v, w \rangle$, so $\langle , \rangle$ is not a homomorphism on $V \times W$.

*Bilinear maps come from linear maps on a tensor prod*.

Def: $V \otimes W$ is called $V$ tensor $W$, or the tensor product of $V$ & $W$, which are F-vector sp's over F

$V \otimes W$ is the free vector space generated by $\{v \otimes w \mid v \in V, w \in W\}$ mod the relations:

$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$

$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$

$(cv) \otimes w = v \otimes (cw) = c(v \otimes w) \quad \forall c \in F$

Ex: $\mathbb{R}^2 \otimes \mathbb{R}^2$

$\langle v_1, v_2 \rangle \quad \langle w_1, w_2 \rangle$

$(\alpha_1 v_1 + \alpha_2 v_2) \otimes (\beta_1 w_1 + \beta_2 w_2) = \alpha_1\beta_1 (v_1 \otimes w_1) + \alpha_1\beta_2 (v_1 \otimes w_2) + \alpha_2\beta_1 (v_2 \otimes w_1) + \alpha_2\beta_2 (v_2 \otimes w_2)$

so $\mathbb{R}^2 \otimes \mathbb{R}^2 = \langle v_i \otimes w_j \rangle$

*In general, if $V$ & $W$ are vector sp's w/ bases $\{v_1, \dots, v_n\}$ & $\{w_1, \dots, w_m\}$, resp, then the basis of $V \otimes W$ is $\{v_i \otimes w_j \mid 1 \le i \le n, 1 \le j \le m\}$, and $\dim(V \otimes W) = \dim(V) \cdot \dim(W)$.

Ex: $V \otimes 0 = V \otimes (0 \cdot 0) = 0(V \otimes 0) = 0$

So a vector sp tensor a trivial vector sp will be trivial.

* elements of $V \otimes W$ of the form $v \otimes w$ are called pure tensors (as opposed to sums)

Ex: $0 = V \otimes w$

$= 0 (V \otimes w)$

$= (0v) \otimes w$ or $= v \otimes (0w)$

Property (*) of $(T, \tau)$: ($\tau : W \times V \to T$ bilinear)

If $f : (W, V) \to X$ is bilinear, then $\exists! h : T \to X$ linear s.t. $h \circ \tau = f$.

$W \times V \xrightarrow{f} X$

$\tau \searrow \quad \nearrow \exists!$ linear map $h$

$T$

Thm: $g : W \times V \to W \otimes V$ bilinear

$(w, v) \mapsto w \otimes v$

If $f : W \times V \to X$ is bilinear, then there exists a unique linear map $h : W \otimes V \to X$ s.t. $f = h \circ g$.

(the bilinear map factors uniquely through $h$) (the tensor prod.)

Pf: $h(w \otimes v) = h(g(w, v)) = f(w, v)$ so $h$ unique.

NTS $h$ well-defined: $h(\text{relation}) = 0$ :

$h((w_1 + w_2) \otimes v - (w_1 \otimes v + w_2 \otimes v))$

$= h((w_1 + w_2) \otimes v) - h(w_1 \otimes v) - h(w_2 \otimes v)$ b/c $h$ linear

$= f(w_1 + w_2, v) - f(w_1, v) - f(w_2, v)$

$= f(w_1, v) + f(w_2, v) - f(w_1, v) - f(w_2, v) = 0$ b/c $f$ bilinear.

$h((cw) \otimes v - c(w \otimes v))$

$= h((cw) \otimes v) - h(c(w \otimes v))$

$= f(cw, v) - cf(w, v) = 0$ b/c $f$ bilinear

Suppose $(T_1,\tau_1)$ & $(T_2,\tau_2)$ satisfy (*). Then $T_1 \cong T_2$:
Let $f_1 : W\times V \to T_1$ $(f_1=\tau_1)$
$\Rightarrow \exists! h_1 : T_2 \to T_1$ (by applying (*) to $(T_2,\tau_2)$),
$\tau_1 = f_1 = h_1\circ\tau_2$
Do the same for $\tau_2=f_2 : W\times V \to T_2$
$\exists! h_2 : T_1 \to T_2$ s.t. $\tau_2 = f_2 = h_2\circ\tau_1$
So, $\tau_2 = h_2\circ(\underbrace{h_1\circ\tau_2}_{=\tau_1})$

$\tau_1 = h_1\circ(h_2\circ\tau_1)$
Take any pair $(T_i,\tau_i)$ & $f: W\times V \xrightarrow{\tau_i} T_i$
$\exists$ unique $h_i : T_i \to T_i$ s.t. $\tau_i = f = h\circ\tau_i \Rightarrow h = id$.
(b/c id works & h unique)
So above, $h_2\circ h_1 = id : T_2\to T_2$ & $h_1\circ h_2 = id : T_1 \to T_1$
$\therefore h_1, h_2$ are isomorphisms & $T_1 \cong T_2$.

Ex: (Extension of scalars) Let $V$ be a $k$-vector sp & let $L$ be an extension of the field $k$. ($k\subseteq L$) (can think of $L$ as a $k$-vector sp).
$V\otimes_k L$ is a $k$-vector sp (& only things in $k$ move across $\otimes$:
$L$ can act on $V\otimes L$ by: $\alpha\in L$, $\alpha(v\otimes x) = v\otimes(\alpha x)$
if $\alpha\in k\subseteq L$, then $\alpha(v\otimes x) = (\alpha v)\otimes x$, as well, & $\uparrow$ action is the $k$-action on $V\otimes L$, b/c doesn't matter which side.).
So $V\otimes_k L$ is an $L$-vector sp, as well (b/c explained how to multiply elts in sp w/ elts. of $L$) & coherently extends vect sp structure over $k$.
$V\otimes_k L$ has a $k$-dim (prod. of $V$ & $k$) & $L$-dim (the $k$-dim of $V$?).

Tensor product of abelian gps:

$\langle , \rangle : G_1 \times G_2 \to G'$ bilinear

$\langle g_1 g_1', g_2 \rangle = \langle g_1, g_2 \rangle \cdot \langle g_1', g_2 \rangle$

$\langle g_1, g_2 g_2' \rangle = \langle g_1, g_2 \rangle \cdot \langle g_1, g_2' \rangle$

$\langle g_1^a, g_2 \rangle = \langle g_1, g_2 \rangle^a = \langle g_1, g_2^a \rangle \quad \forall a \in \mathbb{Z}$

→ not a group homomorphism, but comes from gp hom. on tensor prod. of gps

$G_1 \otimes_{\mathbb{Z}} G_2$ is the free abelian gp generated by $g_1 \otimes g_2$ w/ $g_1 \in G_1, g_2 \in G_2$ mod the relations from bilinearity (written additively).

Prop(*) holds: $f: G_1 \times G_2 \to G'$ bilinear & $G_1 \otimes G_2$ w/ $g: G_1 \times G_2 \to G_1 \otimes G_2$

$\exists!\ h: G_1 \otimes G_2 \to G'$ s.t. $f = h \circ g$, as before

↑ a gp hom.

& same as before w/ isomorphisms.

Ex: $\mathbb{Z}/5 \otimes_{\mathbb{Z}} \mathbb{Z}/7$

$5(n \otimes m) = 5n \otimes m = 0n \otimes m = 0(n \otimes m) = 0$

$7(n \otimes m) = 0$

$5(m \otimes n) - 2(2m \otimes n) = m \otimes n$

$0 - 2(7m \otimes n) =$

$-2(m \otimes 7n) =$

$0 = m \otimes n \quad \forall$ pure tensors $m \otimes n$

⇒ all tensors $= 0$

Generally $\mathbb{Z}/m \otimes_{\mathbb{Z}} \mathbb{Z}/n = 0$ if $(m,n) = 1$

* If the orders of 2 gps are rel prime, their tensor prod. $= 0$. (2 gps? abel?)

$G \otimes \mathbb{Z}/q = \mathbb{Z}^r \oplus \left(\bigoplus_p G[p^\infty]\right) \otimes \mathbb{Z}/q = (\mathbb{Z} \otimes \mathbb{Z}/q)^r \oplus G[q^\infty] \otimes \mathbb{Z}/q$

($p^\infty$ torsion in $G$; $= 0$ $\forall p \neq q$; $\mathbb{Z} \otimes \mathbb{Z}/q \cong \mathbb{Z}/q$)

$= (\mathbb{Z}/q)^r \oplus G[q^\infty] \otimes \mathbb{Z}/q$

↑ a f.g. abel gp.

→ describe the "$q$-part" of $G$.

11/1 To finish classifying irreducible representations of $S_3$:

If $V$ is a rep of $S_3$ & $v \in V^{(v\neq 0)}$, we denote $V_v \subseteq V$ the space spanned by $\{gv\}_{g\in S_3}$. ($V_v$ is stable under $S_3$), which is a subrep of $V$. If $V$ is irred, then $V_v = V$. for all $\forall v \in V, v \neq 0$.

Let $V$ be an irred. rep of $S_3$, $\sigma = (123)$, & let $v \in V$ be an eigenvector of $\sigma$. eigenvalue is either $1, \omega, \text{or } \omega^2$ (b/c $\sigma^3 = 1$)

Let's analyze $V_v$ ($=V$). $\sigma(v) = \lambda v$, & $\lambda = 1, \omega, \omega^2$ $\quad (\tau = (12))$

$\in \text{span}(v)$ $\quad \in \text{span}(\tau v)$

We see that $V_v = \text{span}\{v, \sigma v, \sigma^2 v, \tau, \tau\sigma v, \tau\sigma^2 v\}$

$= \text{span}\{v, \tau v\} \Rightarrow$ dim of any irred rep is $\leq 2$.

- If $\lambda = \omega$, ($\sigma v = \omega v$) $\quad (\sigma\tau = \tau\sigma^{-1})$

$\sigma(\tau v) = \tau\sigma^{-1} v = \tau\omega^2 v = \omega^2 \tau v \Rightarrow \tau v$ is an eigenvector of $\sigma$ w/ eigenvalue $\omega^2$.

I have now told you what $V_v$ is! $\quad$ * $\tau v$ & $v$ are lin. ind. b/c they have diff. eigenval's *

$\rho(\sigma) = \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}$ w/ basis $v, \tau v$

$\rho(\tau) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

& since $\sigma$ & $\tau$ generate the group, this is all you need.

So we have constructed a 2-dim rep.

Check this is isomorphic to 2-dim rep. we studied before, namely, permutation action on $(z_1, z_2, z_3)$ subject to $z_1 + z_2 + z_3 = 0$. This is irred. b/c $\sigma$ acts nontrivially. (But $\sigma$ may act trivially if $\lambda = 1$ :)

- If $\lambda = 1$ ($\sigma v = v$), then $\sigma\tau v = \tau\sigma^2 v = \tau v$

Now $\tau v$ & $v$ have same eigenvalue, so may not be lin. ind. In fact, if $v$ & $\tau v$ were lin. ind, then dim $V_v = 2$ & $\rho(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ & $\rho(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ but this is not irreducible: $\langle v \rangle = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle$ (ie, $\mathbb{C}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ is a stable so a 1-dim subrep. so is $\mathbb{C}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

So $v$ & $\tau v$ are not lin. ind., since $V$ was irred.
So $\tau v = \mu v$ & $v$ is an eigenvector for $\tau$ &
$\mu = 1 \vee \mu = -1$ (b/c $\tau^2 = 1$).
Now $\dim V = \dim V_v = 1$, & there are 2 cases:.

- Trivial rep ($\mu = 1$); $\sigma$ acts as 1, $\tau$ acts as 1
  $gv = v \quad \forall g \in G$.
- Sign (alternating) rep ($\mu = -1$); $\sigma$ acts as 1, $\tau$ acts as $-1$.

$S_3 \xrightarrow{\varepsilon} GL_1(\mathbb{C}) = \mathbb{C}^*$

sign hom. $\searrow$ $\nearrow$ 2 choices (2 2nd roots of unity)

$\mathbb{Z}/2\mathbb{Z}$

$\varepsilon$ = non-trivial $\circ$ sign

We say the sign rep of $S_3$ is "pulled back" from the non-trivial 1-dim rep of $\mathbb{Z}/2\mathbb{Z}$

3 irred reps of $S_3$, 2 of dim 1, 1 of dim 2.

Pullback in general:
If $G \xrightarrow{f} H$ a hom. & $\rho : H \to GL_n(\mathbb{C})$ is a rep, then
$\rho \circ f : G \to GL_n(\mathbb{C})$ is a rep.
(Sometimes call $f^*\rho$)

Ex: Reps of $S_4$. $S_4 \twoheadrightarrow S_3$ which gives us corresp. reps of $S_4$ by pullback (dims 1,1,2)

* If a rep is irred, its pullback is irred, if the hom. is a surjection*. These are not the only ones, though. Need character theory.

# Character Theory

A square matrix of finite size has a trace.

$Tr(A) = \sum_i a_{ii}$.

- Basis-free: if $f: V \to V$ is an endomor, then $f$ has a characteristic polynomial:

$P_f(\lambda) = \det(-f + \lambda \cdot id)$ [det is prop. of a lin. transf.]

$= \lambda^n - Tr(f)\lambda^{n-1} + \cdots$

[Tr also = $\sum$ eigenvalues]

Note: $Tr(\gamma A \gamma^{-1}) = Tr(A) \quad \forall \gamma \in GL_n$.

Def: Let $(V, \rho)$ be a finite-dim. complex rep. of a gp $G$. The character $\chi_V$ is a function

$\chi_V : G \to \mathbb{C}$ defined by $\chi_V(g) = Tr(\rho(g))$.

Remarks & Ex's:

① $\chi_V$ is a class function, ie, $\chi_V(hgh^{-1}) = \chi(g)$

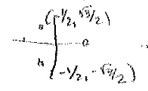
→ conjugacy invariant on gp.

② $\chi_V(1) = \dim V$

③ Ex: Character of irred. 2-dim rep of $S_3$.

$\chi_V$ where $V =$ ↗ ↙ roots of $x^3 - 1 = 0 \Rightarrow \sum$ roots $= 0$

$\chi_V(\rho) = tr\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} = \omega + \omega^2 = -1$ (these are 3 roots of $3^{rd} = 1$, so $\sum 2 = -1$)

$\chi_V(\tau) = tr\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 0$ or 


$\chi_V(id) = \dim V = 2$

All other elts are conjugate to these.

④ Ex: char of alternating 1-dim. rep of $S_3$

$\chi_V(\sigma) = 1 \qquad \chi_V(\tau) = -1 \qquad \chi_V(id) = 1$

⑤ Ex: Char of trivial rep of $S_3$

$\chi(\sigma) = 1 \quad \chi(\tau) = 1 \quad \chi(id) = 1$

⑥ Let $\rho_1, \rho_2$ be reps of $G$ on $V_1, V_2$. Then

$$\rho_1 \oplus \rho_2(g) = \left(\begin{array}{c|c} \rho_1(g) & \\ \hline & \rho_2(g) \end{array}\right)$$

$Tr(\rho_1 \oplus \rho_2) = Tr(\rho_1) + Tr(\rho_2)$

$\chi_{V_1 \oplus V_2} = \chi_{V_1} + \chi_{V_2}$.

Thm: Two f-d reps of $S_3$ are isomorphic iff they have the same character. [actually true $\forall$ finite gps]

Pf

| | id | $\tau$ | $\sigma$ |
|---|---|---|---|
| triv | 1 | 1 | 1 |
| alt | 1 | -1 | 1 |
| standard | 2 | 0 | -1 |

- these 3 class fcns on $S_3$ are linearly ind. But the space of class fcns on $S_3$ is 3-dim'l, so $\chi_{triv}, \chi_{alt}, \chi_{stan}$ are a basis for the sp. of class fcns on $S_3$.

Let $V, W$ be reps of $S_3$. We can write

$V = \bigoplus V_i = V_{triv}^{\oplus a_1} \oplus V_{alt}^{\oplus a_2} \oplus V_{stand}^{\oplus a_3}$

$W = \bigoplus W_i = V_{triv}^{\oplus b_1} \oplus V_{alt}^{\oplus b_2} \oplus V_{std}^{\oplus a_3}$

So $\chi_V = a_1 \chi_{triv} + a_2 \chi_{alt} + a_3 \chi_{std}$

$\chi_W = b_1 \chi_{triv} + b_2 \chi_{alt} + b_3 \chi_{std}$

b/c the 3 $\chi$'s are lin ind, then $a_i = b_i \ \forall i$

$\Rightarrow V \cong W$.

Schur's Lemma: Let $V_1, V_2$ be irred reps & let $f: V_1 \to V_2$ be a G-equivariant map.
(ie, $f \circ \rho_1(g) = \rho_2(g) \circ f$) (ie a hom. of rep's of V)
↑ compatible w/ action of G on both sides.
Then either $f=0$ or $f$ is an isomorphism.

* In particular, if $V_1 \not\cong V_2$, there is no non-zero G-equivariant map from $V_1$ to $V_2$ *

Pf: Consider $\ker f \subset V_1$. It is stable under G b/c
If $v \in \ker f$ ($f(v)=0$), then $f(\rho_1(g)(v)) = \rho_2(g)(f(v)) = 0$
so $\rho_1(g)(v) \in \ker f$. So $\ker f$ is a subrep of $V_1$
& $V_1$ irred, so $\ker f = V_1$ & $f=0$
or $\ker f = 0$ & $f$ is injective.
Same argument on $\operatorname{im}(f)$ shows that
$\operatorname{im}(f)$ is a subrep, so $\operatorname{im}(f)=0$ & $f=0$ or
$\operatorname{im}(f) = V_2$ & $f$ surjective.
⇒ $f$ an isomorphism.

11/6 $V_1, V_2$ be irreps of G: We showed:
(Schur 1) If $V_1 \not\cong V_2$, $\operatorname{Hom}_G(V_1, V_2) = 0$ (G-equivariant maps)
(Schur 2) If $V_1 = V_2$, then $\operatorname{Hom}_G(V_1, V_1) = \mathbb{C}$
(ie $= \mathbb{C} \cdot id \to$ scalar mult.)

Pf(2): Let $f: V_1 \to V_1$ be a G-equiv. hom. Then
$\ker f \subset V_1$ & $\operatorname{im} f \subset V_1$ are sub-G-reps, so they're
$=0$ or $= V_1$. (b/c $V_1$ irrep.). If $f=0$, done. $\lambda \in \operatorname{Hom}_G(V_1, V_1)$
Let $\lambda \in \mathbb{C}$ be an eigenvalue of $f$. Then $f - \lambda$ is
also a G-equi hom $V_1 \to V_1$ so $f - \lambda = 0$ or is iso.
But if $v$ an eigenvector for $\lambda$, $(f-\lambda)v = fv - \lambda v = 0$ ($fv \overset{b/c}{=} \lambda v$)
so $f - \lambda$ is not an iso (b/c has nontrivial kernel)
so $f - \lambda = 0 \Rightarrow f = \lambda$.

Let $h: V_1 \to V_2$ be a linear map, not necessarily, $(V_1,\rho_1), (V_2,\rho_2)$ commuting w/ action of $G$.

Let $h_0 = \frac{1}{|G|}\sum_{g\in G} \rho_2(g)^{-1} \circ h \circ \rho_1(g)$ $\quad \left(\begin{matrix}\rho_1(g): V_1 \to V_1 \\ \rho_2(g): V_2 \to V_2\end{matrix}\right)$

(If $h$ equiv, then $h_0 = h$). But either way, $h_0$ is $G$-equivariant, & thus (If $V_1$ & $V_2$ irred) is either $0$ or $\cong$.

If $V_1 = V_2$, then $h_0 =$ scalar $: V_1 \to V_1$. Which scalar? $(= \operatorname{tr} h_0 / n)$

$$\operatorname{tr} h_0 = \frac{1}{|G|}\sum_{g\in G} \operatorname{tr}(\rho_1(g)^{-1} \circ h \circ \rho_1(g)) = \operatorname{tr} h_0$$

$$= \frac{1}{|G|}\sum_g \operatorname{tr}(h) \qquad \text{(Note: tr is a prop of endomorphs)}$$

$$= \operatorname{tr} h$$

So $h_0 = \frac{1}{n}\cdot \operatorname{tr} h$ where $\dim V_1 = n$, $\dim V_2 = m$

Choose bases for $V_1, V_2$ so that $h$ an $m\times n$ matrix $= (h_{ij})$

$\rho_1(g)$ $n\times n$ $= (\rho^1_{ij})$

$\rho_2(g)$ $m\times m$ $= (\rho^2_{ij})$

(*) So $(h_0)_{ij} = \frac{1}{|G|}\sum_g \sum_{k,\ell} \rho^2(g^{-1})_{ik} \cdot h_{k\ell} \cdot \rho^1(g)_{\ell j}$ $\quad$ ($h_0$ is $m\times n$)

$\left[\text{to multiply for 2 } \sum_k a_{ik} b_{kj} = (\ )_{ij}\right]$

Suppose first that $V_1, V_2$ irreps & $V_1 \not\cong V_2$. So $(h_0)_{ij}$ is $0$ $\forall i,j$ and $\forall$ choices of $h$.

Choose $h$ s.t. $h_{k\ell} = 1$ & all other entries $= 0$. (elementary matrix)

Then (*) tells us

$$0 = \frac{1}{|G|}\sum_g \rho^2(g^{-1})_{ik}\, \rho^1(g)_{\ell j} \qquad (\text{true } \forall\, k,\ell)$$

Choose $k=i$ & $\ell = j$. Then

$$0 = \frac{1}{|G|}\sum_g \rho^2_{ii}(g^{-1}) \cdot \rho^1_{jj}(g), \text{ so sum over all } i,j$$

$$0 = \frac{1}{|G|}\sum_g \left(\sum_{i,j} \rho^2_{ii}(g^{-1})\rho^1_{jj}(g)\right)$$

$$0 = \frac{1}{|G|}\sum_g \left(\sum_i \underbrace{\rho^2_{ii}(g^{-1})}_{\chi_{V_2}(g^{-1})} \sum_j \underbrace{\rho^1_{jj}(g)}_{\chi_{V_1}(g)}\right) =$$

$$\overline{\chi_{V_2}(g)}$$

**Def:** $\langle \chi_{V_1}, \chi_{V_2} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{V_1}(g) \cdot \overline{\chi_{V_2}(g)}$ is an hermetian inner product

[$\because \langle \chi_{V_1}, \chi_{V_1} \rangle \geq 0$ ]

**Conclusion:** If $V_1, V_2$ irreducible & $V_1 \not\cong V_2$, then $\langle \chi_{V_1}, \chi_{V_2} \rangle = 0$ ie $\chi_{V_1} \& \chi_{V_2}$ are orthogonal.

**Ex:** $S_3$:

| | (1) id | (3) (12) | (2) (123) |
|---|---|---|---|
| $\chi_{triv}$ | 1 | 1 | 1 |
| $\chi_{alt}$ | 1 | −1 | 1 |
| $\chi_0$ | 2 | 0 | −1 |

$\frac{1}{6}(1\cdot 2 + 3(0\cdot 1) + 2(1\cdot 1)) = 0$ ✓

1st & 3rd $\to \frac{1}{6}(1\cdot 2 + 3(0\cdot 1) + 2(1\cdot -1)) = 0$ ✓

$\Rightarrow$ so all 3 $\chi$'s are orthogonal.

$\langle \chi_0, \chi_0 \rangle = \frac{1}{6}(4\cdot 1 + 0\cdot 3 + 1\cdot 2) = 1$

(true for all 3) $\Rightarrow$ actually orthonormal.

**Prop:** $\langle \chi, \chi \rangle = 1$ for any irred. char $\chi$. (actually iff) (Now, $V_1 = V_2$)

**Pf:** Take $h$ s.t. $h_{ij} = 1$, all other entries $= 0$:

$h_0 = \frac{1}{n} \operatorname{tr}(h) = \frac{1}{n} \delta_{ij} \cdot I$

$(h_0)_{ij} = \frac{1}{|G|} \sum_{g \in G} \rho^{V}_{ii}(g)^{-1} \cdot \rho^{V}_{jj}(g)$ sum over all $i,j$:

$\frac{1}{n}\delta_{ij}$

$\sum_{i,j} \frac{1}{n}\delta_{ij} = 1 = \frac{1}{|G|} \sum_{g} \overline{\chi_{V_1}} \cdot \chi_{V_1}$

($n$ non-zero entries $= 1$)

So $\langle \chi_{V_1}, \chi_{V_1} \rangle = 1$

Consequences of Orthogonality:

① Let $V$ be a fd rep of $G$, so $V \cong V_1^{\oplus a_1} \oplus V_2^{\oplus a_2} \oplus \cdots \oplus V_k^{\oplus a_k}$ for $V_i$ irred. Then $a_i = \langle \chi_V, \chi_{V_i} \rangle$.

Pf. $\chi_V = \sum a_j \chi_{V_j}$ so

$$\langle \chi_V, \chi_{V_i} \rangle = \sum_j a_j \underbrace{\langle \chi_{V_j}, \chi_{V_i} \rangle}_{= 1 \text{ if } i=j \text{ \& otherwise.}} = a_i \quad \checkmark$$

② If 2 reps $V, W$ of $G$ have the same character, then $V \cong W$.

Pf: $V \cong \oplus X_i^{\oplus a_i}$ $X_i$ = list of all f-d reps of $G$.
$W \cong \oplus X_i^{\oplus b_i}$

Then $\langle \chi_V, \chi_{X_i} \rangle = a_i \Rightarrow a_i = b_i \ \forall i$.
$\langle \chi_W, \chi_{X_i} \rangle = b_i$

Ex: $\mathbb{Z}/k\mathbb{Z} = G$. In this case a rep of $G$ of dim $n$ is a matrix $\gamma$ in $GL_n(\mathbb{C})$ w/ $\gamma^k = 1$. Two reps $\gamma_1, \gamma_2$ are $\cong$ if $\gamma_1$ & $\gamma_2$ are conjugate.

Claim: $\gamma_1$ is conjugate to $\gamma_2$ iff $tr(\gamma_1) = tr(\gamma_2)$

When $k=2$, e-vals of $\rho$ are 1's & -1's (& tr = sum e-vals)

Given a bunch of $n$ $\pm$1's, the sum determines how many of each (2 matrices are conjugate if they have same e-vals).

What if $k=5$, 


Suppose this didn't work, ie $\sum a_i \xi_5^i = \sum b_i \xi_5^i$ w/ $\sum a_i = \sum b_i = n$.

ie, $\sum (a_i - b_i) \xi_5^i = 0$ w/ not all $a_i, b_i = 0$. In other words, I need to use the fact that $\xi_5, \xi_5^2, \xi_5^3, \xi_5^4$ are lin. ind. over $\mathbb{Q}$. If there were a lin. relation $\sum c_i \xi_n^i = 0$, then you would have a relation among the vectors....

11/8 Last time, we were asking why can you recover the conjugacy class of a finite order matrix from its trace? ie, why are there no non-trivial relations of the form $\sum c_i \zeta_n^i = 0$ with $\sum c_i = 0$. ($\zeta_n$: $n^{th}$ roots of units)

Suppose there is such a relation, eg suppose $(n=3)$

$c_0 + c_1\zeta_3 + c_2\zeta_3^2 = 0$ But then also, since (complex conj) ↑ swaps roots of unity

$c_0 + c_1\zeta_3^2 + c_2\zeta_3 = 0$

(n-2 rabbits out of hat, ie, can get n-2 more relations)

A relation $\sum c_i \zeta_n^i = 0$ holds iff $\sum c_i \zeta_n^{ai} = 0$ for any $a \in (\mathbb{Z}/n\mathbb{Z})^*$

(can replace $\zeta_n$ w/ a diff $n^{th}$ root of unity & relation still holds)

So in fact, there is a relation between the vectors (n prime)

$1\ \zeta_n\ \zeta_n^2 \dots \zeta_n^{n-1}$

$1\ \zeta_n^2\ \zeta_n^4 \dots \zeta_n^{2(n-1)}$

$\vdots$

$1\ \zeta_n^{n-1}\ \zeta_n^{2(n-1)} \dots \zeta_n^{(n-1)(n-1)}$

if relation true for one column, true for all other columns

these are the irred. characters of $\mathbb{Z}/n\mathbb{Z}$

(how do we know this matrix has lin. ind. rows? Easiest to show they're orthogonal.)

dot prod. of row a w/ $\overline{\text{row } b} = \sum_{i=0}^{n-1} \zeta^{ai}\overline{\zeta^{bi}} = \sum_{i=0}^{n-1} \zeta^{ai-bi}$

$= \sum_{i=0}^{n-1} (\zeta^{a-b})^i = n\delta_{ab}$ (b/c sum of roots of unity = 0 unless root is 1, then sum = n)

$= 0$ if $a \neq b$

$\Rightarrow$ lin. ind.

Therefore, irr. chars. of a gp are orthogonal.

## Regular Representation

$G$ a finite gp, $G \curvearrowright G$ by left multiplication.

$\rho_{reg}$ the corresp. perm rep'n.

$V_{reg}$ has a basis $\{e_g\}_{g \in G}$ & action of $G$ permutes these by permutation.

$\therefore \dim V_{reg} = |G|$. $\quad V_{reg} = \{\sum_{g \in G} c_g e_g \mid c_g \in \mathbb{C}\}$

We know $V_{reg} \simeq \bigoplus V_i^{\oplus a_i}$ $\quad V_i$ irrep.

Which irreps of $G$ arise, & how many times?

Recall: $\chi_{reg}(g)$ = # of fixed pts of $g$ acting on $G$, ie,

# of $g' \in G$ s.t. $gg' = g'$

$= \begin{cases} 0 & \text{if } g \neq e \\ |G| & \text{if } g = e \end{cases}$

Let $V_i$ irrep of $G$. $\quad a_i = \langle \chi_{reg}, \chi_{V_i} \rangle$

$a_i = \langle \chi_{reg}, \chi_{V_i} \rangle = \frac{1}{|G|} \sum_g \chi_{V_i}(g) \overline{\chi_{reg}(g)} = \frac{1}{|G|}(|G| \cdot \chi_{V_i}(1)) = \chi_{V_i}(1)$

$= \dim V_i$

so all irreps appear, & it appears $\dim V_i$ times.

$(g \cdot f)(h) = f(gh)$

[Can also think of $V_{reg}$ as space of fcns $G \to \mathbb{C}$ ]

eg think of a space like $L^2(\mathbb{R})$ or Schwartz fcns on $\mathbb{R}$, or $C_c(\mathbb{R})$ or $C^\infty(\mathbb{R})$. $\mathbb{R}$ acts on all of these spaces. by translation $(t)$ $\quad f_t(x) = f(x+t)$.

Schwartz($\mathbb{R}$) $\quad$ interwined by Fourier transform $\quad$ Schwartz($\mathbb{R}$)

$\mathbb{R} \curvearrowright$ by trans. $\quad$ $\mathbb{R} \curvearrowright$ by ? ← something ... diff?

1 sends $f(x)$ to $f(x+1)$ $\quad$ 1 sends $f(x)$ to ? →

So $V_{reg} = \bigoplus_{\substack{\text{irreps} \\ V_i}} V_i^{\oplus d_i}$ ; $d_i = \dim V_i$

$$\dim V_{reg} = |G| = \sum_{\text{irreps}} d_i^2 = \sum_{\text{irreps.}} (\chi_{V_i}(1))^2$$

Ex: $S_3$ has irreps of $1, 1, 2$, & $6 = 1^2 + 1^2 + 2^2$.

Ex: Computing irreps of $S_4$.
Recall that if $S_4 \twoheadrightarrow Q$ (quotient gp) and irrep $Q$ pulls back into an irrep of $S_4$.

a) $S_4 \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$ by sign hom. which has 2 irreps, or trivial & one sending $1 \to -1$.

| | 1 | 6 | 8 | 3 | 6 | # elts |
|---|---|---|---|---|---|---|
| | id | (12) | (123) | (12)(34) | (1234) | conj. classes of $S_4$ |
| $\chi_{triv}$ | 1 | 1 | 1 | 1 | 1 | |
| from $\mathbb{Z}/2\mathbb{Z}$ $\chi_{alt}$ | 1 | -1 | 1 | 1 | -1 | (all elts of $A_4 \in$ ker of map to $A_4 \Rightarrow$ sign=1 |
| $\chi_2$ | 2 | 0 | -1 | 2 | 0 | |
| $\chi_3$ | 3 | 1 | 0 | -1 | -1 | (by subtracting 1) |
| $\chi_3 \cdot \chi_{alt}$ | 3 | -1 | 0 | -1 | 1 | |

b) $S_4 \twoheadrightarrow S_3$, which has 3 irreps. But 2 are pulled back from $S_3 \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$, so 1 new irrep: 2-dim $\chi_2$
elts in Ker of map to $S_3$, get $\chi_2(1)$ b/c those elts map to id

| id | (12) | (123) | |
|---|---|---|---|
| 2 | 0 | -1 | order 2 $\Rightarrow$ order 2 |
| | | | order 4, but square is double flip $\Rightarrow$ order 2 |

c) $S_4 \curvearrowright \{1,2,3,4\}$ yielding perm rep
(character assign to each class the # of fixed pts)

| | 1 | 6 | 8 | 3 | 6 | |
|---|---|---|---|---|---|---|
| $\chi_{perm}$ | 4 | 2 | 1 | 0 | 0 | by # of fixed pts |

not irred b/c if pair it w/ any other $\chi$ will be pos.
$\langle \chi_{perm}, \chi_{triv} \rangle = 1$, so has one copy of $\chi_{triv}$
So $V_{perm} = V_3 \oplus V_{triv}$
So $\chi_{V_3} = \chi_{perm} - \chi_{triv}$. this is irred, b/c a rep is irred iff $\langle \chi, \chi \rangle = 1$.

d) Need one more 3-dim rep.
Let $V, W$ be reps of $G$. recall, if $f$ is a map $V \to V$ $g: W \to W$, $\exists!$ lin. map $f \otimes g: V \otimes W \to V \otimes W$.

In particular, if $(V,\rho_1)$ & $(W,\rho_2)$ are reps of a gp $G$, then for each $g$, I have an endomorph $\rho_1(g)\otimes\rho_2(g): V\otimes W \to V\otimes W$

So $(V\otimes W, \rho_1\otimes\rho_2)$ is a new rep of $G$.

$\dim(V\otimes W) = \dim V \cdot \dim W$

fact: $\forall$ $\operatorname{tr}(f\otimes g) = \operatorname{tr}(f)\cdot\operatorname{tr}(g)$

So $\chi_{V\otimes W} = \operatorname{tr}(\rho_1\otimes\rho_2(g)) = \chi_V \cdot \chi_W$.

($\oplus$ & $\otimes$ of reps is like $\sqcup$ & $\times$ of sets)

To get another 3-dim rep, tensor a 3-dim rep w/ a 1-dim rep.

$V_3 \otimes V_{\text{triv}}$ is a rep.

11/13 Rings and Modules

Def: A ring $(R,+,\cdot)$ s.t. $(R,+)$ is an abel. gp &
- is assoc. & distributes over + in both directions
  $a(b+c) = ab+ac$, etc.
- add id. = 0.

If $R$ has mult. id, 1, then we say $R$ is unital.

If $\cdot$ is commutative, $R$ is commutative.

- If $R$ has 1, & $a\in R$ w/ $b\in R$ s.t. $ab=ba=1$, $a$ is a unit (ie, $a$ has a 2-sided inverse) If $a$ has a left & right inv, they are equal: $ab=bc=1 \Rightarrow c=abc=a$.
  Units in $R$: $R^\times$.
- If every nonzero elt is a unit, $R$ is a division ring
  - If $R$ is also commutative, $R$ is a field.
  (Thm: A finite div. ring is a field).
- If $a\in R$ has a $b\neq 0$ s.t. $ab=0$ or $ba=0$, $a$ is a zero divisor
- If $R$ is commutative & has no zero divisors, $R$ is an integral domain. (or just domain)
  - $ac=bc$ in a domain $\Rightarrow c=0 \vee a=b$
    $ca=cb \Rightarrow$ ——— ||
- A finite int. dom w/ 1 is a field; $a\neq 0$: $\{a,a^2,\dots,a^n,\dots\}$
  $\Rightarrow a^m = a^n \Rightarrow a^{m-n}=1 \Rightarrow a$ a unit $\Rightarrow$ all nonzero elts units & comm $\Rightarrow$ field

## Finishing Rep'n Theory

11/20 Last time, by decomposing the regular rep of $G$ into irreducibles, we saw $\chi_{reg} = \sum \chi_i(1)\chi_i$.

$\rho_{reg} \cong \bigoplus V_i^{\dim V_i}$

$|G| = \sum_i \chi(1)^2$

### The number of irreps of $G$:

Write $\mathbb{C}[G/G]$ for the space of class fcns on $G$, ie, all $f: G \to \mathbb{C}$ s.t. $f(hgh^{-1}) = f(g)$. (ie, const. on conj. classes)

$\dim \mathbb{C}[G/G]$ = # of conjugacy classes of $G$.

↑ ($\div |G|$ = probability that 2 elts commute)

**Prop:** Let $f$ a class fcn & $(V, \rho)$ an irrep. Then ($\dim V = n$)

$\mathrm{End}(V) \ni \rho_f := \sum_{g \in G} f(g) \cdot \rho(g)$ is equal to

($\mathbb{C}$; $\rho(g) \in \mathrm{End}(V)$ = a matrix)

$\frac{|G|}{n} \cdot \langle f, \chi_V^* \rangle \cdot id_V$ (ie, scalar mult of $id_V$)

↑ identity endomorphism of $V$

**Pf:** (By Schur's Lemma) It suffices to show $\rho_f : V \to V$ is $G$-equivariant; ie, $\rho(g)\rho_f = \rho_f \rho(g)$. Ie,

$\rho(g)\rho_f\rho(g)^{-1} = \rho_f$.

$\rho(g)\rho_f\rho(g)^{-1} = \rho(g)\left[\sum_{h \in G} \rho(h) f(h)\right]\rho(g)^{-1}$

$= \sum_{h \in G} f(h)\rho(ghg^{-1})$ write $k = ghg^{-1}$ & $h = g^{-1}kg$

$= \sum_{k \in G} f(g^{-1}kg)\rho(k) = \sum_{k \in G} f(k)\rho(k) = \rho_f$.

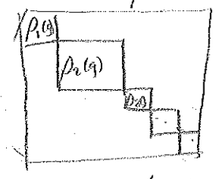
So $\rho_f$ is a scalar, but which? ↙ complex conj of $\chi_V$.

$\mathrm{Tr}(\rho_f) = \sum_g f(g)\chi_V(g) = |G| \cdot \langle f, \chi_V^* \rangle$

↑ $\mathrm{Tr}(\rho(g))$

& the scalar is $\mathrm{Tr}(\rho_f) \cdot \frac{1}{n}$. QED

Let $X \subset \mathbb{C}[G/G]$ be the space spanned by irred. chars. Let $f$ be a nonzero vector in $X^\perp$. Then $\rho_f = 0$ for all irreps $(V,\rho)$. But then, by decomposability, if $\rho = \bigoplus \rho_i$ then $\rho_f = \sum f(g)\rho(g) = \sum f(g) \bigoplus \rho_i(g) = 0 \oplus 0 \oplus \cdots \oplus 0 = 0$

$\rho(g) =$ 

can sum over each block separately.

So $\rho_f = 0$ $\forall$ reps $V$ (not just irreps)

Applying this to the regular rep, we find

$\sum_{g \in G} f(g)\rho_{reg}(g) = 0$ . Recall, $V_{reg} = \text{span}\{e_g\}_{g \in G}$ (on which $G$ acts by perm - left mults)

$\rho_{reg}(g)e_1 = e_g$.

So

$0 = (\rho_{reg})_f(e_1) = \sum_{g \in G} f(g)\rho_{reg}(g)e_1 = \sum_{g \in G} f(g)e_g \Rightarrow f(g) = 0 \ \forall g \in G$,

since $\{e_g\}$ are basis, they are lin. ind., ie $f = 0$.

So $X^\perp = \{0\} \Rightarrow X = \mathbb{C}[G/G]$.

Thus:

Prop: The irreducible characters of $G$ are an orthonormal basis for the space of class fcns on $G$.

Cor: The # of irred. chars. of $G$ = # of conjugacy classes of $G$.

[They're not, in general, related by bijection]

Cor: The number of 1-dim reps of $G$ is $|G^{ab}|$ ($G/[G,G]$; commutator subgp) (the abelianization of $G$) & all irreps are 1-dim iff $G$ is abelian.

Pf: If $\rho: G \to GL_1$ is a 1-dim rep, then $\rho$ factors through $G \to G^{ab} \to GL_1$ (abel. gp). So this is really a question about 1-dim reps of $G^{ab}$. # irreps of $G^{ab}$ = # of conjugacy classes of $G^{ab} = |G^{ab}|$. So $\sum_{\text{irreps } \chi_i} d_i^2 = |G^{ab}|$

$\Rightarrow d_i = 1 \ \forall i$, since summing over $|G^{ab}|$ elts. QED(a).

If $G$ abel, # of 1-dim reps $= |G|$ by argument above, & all reps are 1-dim. Conversely, if all reps are 1-dim, then $|G| = \sum_i d_i^2 = \sum_i 1 =$ # of conjugacy classes of $G$
$\Rightarrow G$ abel.

(Martin) Dan

Deeper questions:
- Which $G$ have irred. 2-dim reps & what are they?
- Groups whose lowest-dim. nontrivial character is "large" relative to $|G|$. Gromov,
  ("random groups" - Gowers, Breuillard-Green-Tao)
- Contrast: - $S_n$ has $(n-1)$-dim. irrep (reduced perm. rep)
  $n-1$ is really small relative to $n!$
  - $PSL_2(\mathbb{F}_p)$: smallest irrep. has dim. $\sim p$.
    $p$ big compared to $|PSL_2(\mathbb{F}_p)| \approx p^3$.

Examples of Rings:

① What are the Gaussian integers?
One pt. of view: they are the subring of $\mathbb{C}$ generated by $i$ (the pt $e^{\pi i/2}$ in the plane) → bad def b/c shouldn't have to define $\mathbb{C}$ first... ⇒ extrinsic b/c requires knowing $\mathbb{C}$.
More intrinsic: $\mathbb{Z}[x]$ has a principal ideal $(x^2+1)$ consisting of all multiples of $x^2+1$. $(x^2 = -1)$
$R := \mathbb{Z}[x]/(x^2+1) = \{a+b\bar{x}\}_{a,b\in\mathbb{Z}}$ $(x^3 = -x,\ x^4 = -x^2 = 1)$, $\bar{x}$ = image of $x$ in $\mathbb{Z}[x]/(x^2+1)$
(called $\bar{x}$ instead of $i$...)
XIs $R$ a subring of $\mathbb{C}$?
Better: Can $R$ be embedded as a subring of $\mathbb{C}$?
(ie, is there an injection?) Yes, in 2 distinct ways!
$\phi: R \to \mathbb{C}$ is determined by $\phi(\bar{x})$ (b/c $1 \to 1$)
which must satisfy $\phi(\bar{x})^2 = -1$. So
$\phi(\bar{x}) = i$ or $\phi(\bar{x}) = -i$

When we study a ring, we study its set of ideals.
& eventually its set of modules, & (lattice)
its category of modules. ↑ subring structure

ideal is a special case of a module.

## ② Ideals of $\mathbb{Z}$.

First of all, $\mathbb{Z}$ is Noetherian $\Rightarrow$, all ideals are f.g.
$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ an ascending chain of ideals

Let $n \in I_1$ & $I_0 = n\mathbb{Z}$.

$\mathbb{Z}/I_0 \twoheadrightarrow \mathbb{Z}/I_1 \twoheadrightarrow \mathbb{Z}/I_2 \twoheadrightarrow \cdots$

$\mathbb{Z}/n\mathbb{Z}$ a finite set

the sets in the sequence are getting smaller b/c modding out by larger ideals.

A descending sequence of finite sets must stabilize, so eventually $\mathbb{Z}/I_k = \mathbb{Z}/I_{k+1} \Rightarrow I_k = I_{k+1}$. so all ideals are finitely generated. Actually gen. by 1 elt → next time.

11/27

**Prop**: Every ideal of $\mathbb{Z}$ is principal, ie of the form $n\mathbb{Z}$ or $(n)$ for some $n \in \mathbb{Z}$.

**Pf**: Induction on # of generators, $k$.

Suppose $I = (a_1, \ldots, a_k)$ & $k$ minimal s.t. $\exists$ non-principal ideal gen by $k$ elts: $I = (a_1, \ldots, a_{k-1}) = (n)$ for some $n$, by induction, so $I = (n, a_k)$.

Thus it suffices to show that all ideals of form $(a,b)$ are principal:

Let $d = \gcd(a,b)$ so $a \in (d) : d\mathbb{Z}$

$b \in (d)$ so $(a,b) \subseteq (d)$ ← principal ideal

But (Euclidean Alg) $\exists\, m, n \in \mathbb{Z}$ s.t. $am + bn = d$

**Note**: $(a,b) = \{am + bn \mid m,n \in \mathbb{Z}\}$ ie, $(a,b)$ is precisely the set of $\mathbb{Z}$-linear combinations of $a$ & $b$.

So, $d \in (a,b) \Rightarrow (d) \subseteq (a,b)$

$\Rightarrow (a,b) = (d)$.