Last time (1) For any orbit $G\cdot x$ (for an action $G\times X\to X$)
there is a bijection $\psi: G/G_x \to G\cdot x$, $\psi(gG_x)=g\cdot x$
where $G_x \equiv \mathrm{Stab}(x) = \{a\in G \mid a\cdot x = x\}$
Hence, if G is finite, $|G\cdot x| \,\big|\, |G|$.

(2) A group G acts on itself by conjugation
$$G\times G\to G, \quad g\bullet x = gxg^{-1}.$$
The orbits of this action are called conjugacy classes
For example if $G=S_n$ and x = r-cycle
$$S_n\bullet x = \text{the set of all r-cycles.}$$

Remark An action of G on X $\longleftrightarrow$ a homomorphism $G\to \mathrm{Sym}(X)$.
If X is a group, $\mathrm{Sym}(X) = \{f: X\to X \mid f \text{ is a bijection}\}$
has a subgroup
$$\mathrm{Aut}(X) = \{f: X\to X \mid f \text{ is an isomorphism}\}$$
$\mathrm{Aut}(X)$ is a subgroup of $\mathrm{Sym}(X)$ since
1) id_X is an iso
2) if $f: X\to X$ is an iso so is $f^{-1}: X\to X$
3) if $f,g: X\to X$ are two iso's so is $f\circ g$.

Note well When a group G acts on itself by conjugation
the image of the corresp homomorphism
$$c: G\to \mathrm{Sym}(G), \quad g\mapsto c_g$$
$$c_g(a) = gag^{-1}, \quad \forall a\in G$$
lands in $\mathrm{Aut}(G)$ since $\forall g\in G$, $\forall a,b\in G$
$$c_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = c_g(a)\,c_g(b)$$
i.e. each c_g is an isomorphism.

"Ex"

If $\mu \in S_n$, μ is a product of disjoint cycles:

$$\mu = x_1 \cdot x_2 \cdots x_k.$$

$x_i = r_i$-cycle and $r_1 + r_2 + \cdots + r_k = n$.

For any $g \in S_n$

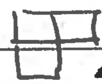
$$c_g(\mu) = c_g(x_1) \cdots c_g(x_k)$$

$\Rightarrow$ The conjugacy class of μ is the set of <u>all</u> partitions of $\{1, \ldots n\}$ into sets of sizes $r_1, r_2, \ldots r_k$.

SubEx $n = 3$. Possible partitions of $\{1,2,3\}$ are

single set of size 3 = 3-cycles

$\{(123), (132)\}$



← 2-cycles
← 1 cycle

$\{(12), (13), (23)\}$

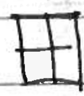
3 sets of size 1

$\{id\}$.

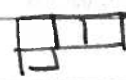
<u>$n=4$</u>

$\{id\}$

all 2-cycles



pairs of disjoint 2-cycles



all 3-cycles

all 4 cycles

<u>Ex</u> 5.1.19 (Goodman)

<u>Q.</u> How many subsets of $\{1, 2, \ldots n\}$ with exactly k $(1 \le k \le n)$ elements are there?

<u>A</u> Let $X = \{A \subseteq \{1, \ldots n\} \mid |A| = k\}$.

S_n acts on X: $\sigma \cdot A := \{\sigma(a) \mid a \in A\}$, which is a subset of X of size k.

The action of S_n on X is <u>transitive</u> ie $\forall A \in X$ $\exists \sigma \in S_n$ s.t. $A = \sigma \cdot \{1, \ldots k\}$.

<u>Reason</u> Since $|A| = k$, $A = \{a_1, \ldots a_k\}$ for some $a_1, \ldots a_k \in \{1, \ldots n\}$. Then $\{1, \ldots n\} \setminus A = \{\underbrace{a_{k+1}, \ldots a_n}_{n-k \text{ elements}}\}$

Define $\sigma \in S_n$ by $\sigma(i) = a_i$

Then $\sigma \cdot \{1, \ldots k\} = \{a_1, \ldots a_k\}$

$$|X| = |S_n \cdot \{1, \ldots k\}| = \frac{|S_n|}{\mathrm{Stab}(\{1, \ldots k\})} = \frac{|S_n|}{|S_k|\,|S_{n-k}|} = \frac{n!}{k!\,(n-k)!}$$

"The class equation" (p 255 of Goodman)

Let G be a group acting on itself by conjugation
$\forall\, x \in G$

$$G_x = \{g \in G \mid gxg^{-1} = x\} =: \mathrm{Cent}(x), \text{ the } \underline{\text{centralizer}} \text{ of } x.$$

<u>Recall</u> The <u>center</u> $Z(H)$ of a group H is

$$\begin{aligned} Z(H) &= \{z \in H \mid hzh^{-1} = z \ \forall\, h \in H\} \\ &= \{z \in H \mid \mathrm{Cent}(z) = H\} \\ &= \{z \in H \mid H \circ z = \{z\}\}. \end{aligned}$$

Now suppose G is finite. Then G has finitely many conjugacy classes. We then have

disjoint union

$$G = \underset{\substack{\uparrow \\ \text{union of all} \\ \text{1-element conj classes}}}{Z(G)} \sqcup G \cdot x_1 \sqcup \ldots \sqcup G \cdot x_k$$

for some $x_1, \ldots x_k \in G$.

<u>Ex</u> $G = S_4 = \{id\} \sqcup S_4 \circ (12) \sqcup S_4 \circ (123) \sqcup S_4 \cdot (1234) \sqcup$
$\sqcup\, S_4 \cdot (12)(34)$

The class equation is

$$|G| = |Z(G)| + \sum_{i=1}^{k} |G \cdot x_i|$$

$$= |Z(G)| + \sum \frac{|G|}{|\mathrm{Cent}(x_i)|}$$

"Application" of the class equation:

<u>Prop 5.4.2</u> Suppose G is a group with p^n elements (p prime). Then $p \mid |Z(G)|$. In particular $|Z(G)| > 1$.

<u>Proof</u>

$$p^n = |G| = |Z(G)| + \sum_{i=1}^{k} |G \cdot x_i| \quad \text{where } |G \cdot x_i| > 1.$$

Since $|G\cdot x_i| \mid |G| = p^n$ and since $|G \cdot x_i| > 1$, $p \mid |G \cdot x_i| \ \forall i$

$\Rightarrow \quad p \mid p^n - \Sigma |G \cdot x_i| = |Z(G)|$.

<u>Corollary 5.4.3</u> If $|G| = p^2$ (p prime) then either $G \simeq \mathbb{Z}_{p^2}$ or $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

<u>Proof</u> For any $g \in G$, $|\langle g \rangle| \mid p^2 \Rightarrow |\langle g \rangle| = 1, p$ or p^2.

If $|\langle g \rangle| = 1$, $g = e$. If $|\langle g \rangle| = p^2$, $\langle g \rangle = G$ and $f: \mathbb{Z}_{p^2} \to \langle g \rangle = G$, $f([k]) = g^k$ is an iso.

Now suppose $\nexists g \in G$ with $|\langle g \rangle| = p^2$. Then $\forall g \in G \setminus \{e\}$, $|\langle g \rangle| = p$. By 5.4.2 $|Z(G)| > 1$.

So $\exists\, a \in Z(G)$ with $a \neq e$. Then $|\langle a \rangle| = p$. In particular $\emptyset \neq G \setminus \langle a \rangle$ (since G has p^2 elements and $\langle a \rangle$ has p elements)

Choose $b \in G \setminus \langle a \rangle$. Since $a \in Z(G)$ $bab^{-1} = a$, ie a, b commute. $\Rightarrow$ $f: \langle a \rangle \times \langle b \rangle \longrightarrow G$

$f(a^k, b^l) = a^k b^l$ is a homomorphism

(<u>Check</u>: $f((a^k, b^l)\cdot(a^r, b^s)) = f(a^{k+r}, b^{l+s}) = a^{k+r} b^{l+s}$

$= a^k b^l a^r b^s = f(a^k, b^l) \cdot f(a^r, b^s)$.)

<u>Claim</u> f is 1-1. (hence since $|\langle a \rangle \times \langle b \rangle| = |\langle a \rangle| |\langle b \rangle| = p^2 = |G|$, f is an iso)

<u>Proof</u> $a^k b^l = a^r b^s \Rightarrow a^{-r} a^k = b^s \cdot b^{-l} \in \langle a \rangle \cap \langle b \rangle$.

$\langle a \rangle \cap \langle b \rangle$ is a subgroup of $\langle a \rangle$. Since $|\langle a \rangle| = p$, $|\langle a \rangle \cap \langle b \rangle| = p$ or 1.

If $|\langle a \rangle \cap \langle b \rangle| = p$, $\langle a \rangle \cap \langle b \rangle = \langle a \rangle$. $\Rightarrow b \in \langle a \rangle$. But $b \in G \setminus \langle a \rangle$. Contradicti

$\Rightarrow \langle a \rangle \cap \langle b \rangle = \{e\}$. $\Rightarrow a^{k-r} = e = b^{s-l} \Rightarrow a^k = a^r$ and $b^s = b^l$. D