Content:

Definition	orbit
Definition	stabilizer
Definition	Cycle structure
Proposition	$G_x \leq G$
Definition	conjugacy class
Definition	centralizer
Definition	normalizer
Proposition	$G \times X \to X$ is a function. Let $a, b \in X$. Define $a \sim b$ if $\exists\, g \in G$ such that $g \bullet a = b$. This is an equivalence relation.
Theorem	If G acts on a finite set X, then $\lvert X\rvert = \sum_i \lvert \mathcal{O}(x_i)\rvert$ where one x_i is taken from each orbit.
Theorem	If G acts on X and $x \in X$, then $\lvert \mathcal{O}(x)\rvert = [G{:}G_x]$.
Corollary	General Class Equation $\lvert X\rvert = \sum_i [G : G_{x_i}]$ where one x_i is taken from each orbit.
Theorem	The Class Equation $\lvert G\rvert = \lvert Z(G)\rvert + \sum_i [G : G_{x_i}]$
Corollary	$\lvert \mathcal{O}(x)\rvert \mid \lvert G\rvert$.
Corollary	$\lvert x^G\rvert \mid \lvert G\rvert$.
Corollary	If G is a finite group and $H \leq G$, then the number of conjugates of H is equal to $[G{:}N_G(H)]$. This is just a special case of $\lvert \mathcal{O}(x)\rvert = [G{:}G_x]$.
Theorem	Cauchy's Theorem, If G is a finite group such that $p \mid \lvert G\rvert$ and p is prime, then G contains an element of order p.

Exam 2 will be moved to possibly Wednesday, October 28 or Monday, November 9.

Group action was defined last week. This extra structure on groups will help us classify them.

Cayley's Theorem was a group acting on itself by left multipliction.
Representation on Cosets Theorem was a group acting on G/H by left multliplication.

A group action means we have a permutation on X.

Definition Let G act on X, $x \in X$. The *orbit* of X is $\mathcal{O}(x) = \{g \bullet x \mid g \in G\}$.

Definition Let G act on X, $x \in X$. The *stabilizer* of x is $G_x = \{g \in G \mid g \bullet x = x\}$.

Example Let G act on itself by left multiplication.

$\mathcal{O}(x) = \{gx \mid g \in G\} = G$ (like one row of the Cayley Table)

$G_x = \{g \in G \mid gx = x\} = \{e\}$

Example Let G act on G/H by left multiplication.

$\mathcal{O}(xH) = \{gxH \mid g \in G\} = G/H$ (convince yourself of this)

(Since $\{gx \mid g \in G\} = G$ in the example above, then $\{gxH \mid g \in G\}$ is like $\{aH \mid a \in G\}$.)

$G_x = \{g \in G \mid gxH = xH\} = ?$

(I claim $\{g \in G \mid gxH = xH\} = xHx^{-1}$.
Pf: $xHx^{-1}xH = xHeH = xHH = xH$.)

Proposition $G_x \le G$

Proof:

This is all things that fix x. So $e \in G_x$. So $G_x \ne \varnothing$.

Let $a, b \in G_x$. We want to show $ab^{-1} \in G_x$ or $ab^{-1} \bullet x = x$.

$a \bullet x = x$ and $b \bullet x = x$. Since $b^{-1} \in G$ and $b \bullet x \in X$, then

$x = e \bullet x = (b^{-1}b) \bullet x = b^{-1} \bullet (b \bullet x) = b^{-1} \bullet x$. So $b^{-1} \in G_x$.

$\therefore\ x = a \bullet x = a \bullet (b^{-1} \bullet x) = (ab^{-1}) \bullet x$.

Example Let G act on itself by conjugation. Let $x \in G$. Then $g \bullet x = gxg^{-1}$.

$\mathcal{O}(x) = x^G = \{gxg^{-1} \mid g \in G\}$. This is called the *conjugacy class* of x in G.

$G_x = C_G(x) = \{g \in G \mid gxg^{-1} = x\}$. Called the *centralizer* of x in G.

1) $C_G(x) \le G$.

Pf: $exe^{-1} = x$, so $C_G(x) \ne \varnothing$. Let $a, b \in C_G(x)$. Then $axa^{-1} = x$ and $bxb^{-1} = x$. This gives us $a^{-1}xa = x = b^{-1}xb$. Hence $x = ab^{-1}x(ab^{-1})^{-1}$. $\therefore\ C_G(x) \le G$.

2) $Z(G) \le C_G(x)$.

Pf: $Z(G)$ is a group. We only need to show it is a subset of $C_G(x)$.

Let $z \in Z(G)$. Then $\forall\ x \in G, xzx^{-1} = z$. Hence $x = zxz^{-1}$. $\therefore\ z \in C_G(x)$.

3) $C_G(e) = G$ (i.e. Everything commutes with e.)

Pf: $C_G(e) = \{g \in G \mid geg^{-1} = e\}$. Clearly, $\forall\ g \in$ G, $geg^{-1} = gg^{-1} = e$.

Example Let G be an Abelian group where the group action is conjugation.

Let $x \in G$.

$x^G = \{x\}$.

Pf: $x^G = \mathcal{O}(x) = \{gxg^{-1} \mid g \in G\}$.

Since G is Abelian, then $gxg^{-1} = gg^{-1}x = ex = x, \forall\ g \in G$. $\therefore\ x^G = \{x\}$.

$C_G(x) = G$.

Pf: $C_G(x) = \{g \in G \mid gxg^{-1} = x\}$. As noted above, $\forall\ g \in G, gxg^{-1} = x$.

$\therefore\ C_G(x) = G$.

Example Let S_3 act on itself by conjugation.

$(12)^{S_3} = \{(12), (13), (23)\}$.

$(123)^{S_3} = \{(123), (132)\}$.

$(1)^{S_3} = \{(1)\}$.

$C_{S_3}(12) = \{\sigma \in S_3 \mid \sigma(12)\sigma^{-1} = (12)\} = \{(1), (12)\}$.

$C_{S_3}(123) = \{\sigma \in S_3 \mid \sigma(123)\sigma^{-1} = (123)\} = \{(1), (123), (132)\}$.

$C_{S_3}(1) = \{\sigma \in S_3 \mid \sigma(12)\sigma^{-1} = (1)\} = S_3$.

Example Let G act on the set of its subgroups by conjugation. Let $H \le G$.

Then $g \bullet H = gHg^{-1}$.

$\mathcal{O}(H) = \{gHg^{-1} \mid g \in G\}$.

Notice $H \lhd G \Leftrightarrow \mathcal{O}(H) = \{H\}$.

$N_G(H) = C_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is called the *normalizer* of H in G.

(This measures how close or far away H is from being normal.)

Note: (1) $H \triangleleft N_G(H)$.

Pf: Clearly, $H \subseteq N_G(H)$ and H is a group, so $H \leq N_G(H)$. Let $x \in N_G(H)$. Then $xHx^{-1} = H$. $\therefore$ $H \triangleleft N_G(H)$.

(2) $N_G(H) = G \Leftrightarrow H \triangleleft G$.

Pf: Assume $N_G(H) = G$. Then $\forall\, g \in G, gHg^{-1} = H$, hence $H \triangleleft G$. Assume $H \triangleleft G$. Then $\forall\, g \in G, gHg^{-1} = H$, hence $G \subseteq N_G(H)$. We know $N_G(H) \subseteq G$. $\therefore$ $N_G(H) = G$.

(3) $N_G(H)$ is the largest subgroup of G in which H is normal.

Pf: Let $K \leq G$ such that $H \triangleleft K$. Let $k \in K$. Then $kHk^{-1} = H$. $\therefore$ $k \in N_G(H)$.

Back to S_3.

Example Let S_3 act on its subgroups by conjugation.

$X = \{\langle(1)\rangle, \langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle, \langle(123)\rangle, S_3\}$.

$N_{S_3}(\langle(123)\rangle) = S_3$. (Since $\langle(123)\rangle$ is normal, since $[S_3{:}\langle(123)\rangle] = 2$)

$N_{S_3}(\langle(12)\rangle) = \{(1), (12)\}$. (so it's far from normal)

Back to group actions in general:

Proposition $G \times X \to X$ is a function. Let $a, b \in X$. Define $a \sim b$ if $\exists\, g \in G$ such that $g \bullet a = b$. This is an equivalence relation.

Proof: Do on your own.

To show **reflexivity**, note that $e \in G$ and $e \bullet a = a$, hence $a \sim a$.

To show **symmetry**, let $a, b \in X$ such that $a \sim b$. So $\exists\, g \in G$ such that $g \bullet a = b$. Since G is a group, then $g^{-1} \in G$ and $g^{-1} \bullet g \bullet a = (g^{-1}g) \bullet a = e \bullet a = a = g^{-1} \bullet b$. $\therefore$ $b \sim a$.

To show **transitivity**, let $a, b, c \in X$ such that $a \sim b$ and $b \sim c$. Then $\exists\, g_1$ and g_2 such that $g_1 \bullet a = b$ and $g_2 \bullet b = c$.

$\therefore$ $g_2 \bullet g_1 \bullet a = (g_2 g_1) \bullet a = g_2 \bullet b = c$.

Since $g_2 g_1 \in G$ by closure, then $a \sim c$.

Proposition $\mathcal{O}(x)$ is the equivalence class of x.

Proof: Do on your own.

We need to show

$\mathcal{O}(x) = \{g \bullet x \mid g \in G\} = \{b \in X \mid \exists\, g \in G \text{ such that } g \bullet a = b\} = [x]$.

Let $a \in \mathcal{O}(x)$. Then $a = g \bullet x$ for some $g \in G$. $\therefore$ $x \sim a$. $\therefore$ $a \in [x]$.

Let $b \in [x]$. Then $\exists\, g \in G$ such that $g \bullet x = b$. $\therefore$ $b \in \mathcal{O}(x)$.

Hence $\mathcal{O}(x) = [x]$.

Theorem If G acts on a finite set X, then $|X| = \sum_i |\mathcal{O}(x_i)|$ where one x_i is taken from each orbit.

Proof: This follows from equivalence relation. The orbits partition X. Since the orbits are disjoint, no element in X is counted more than once.

Theorem If G acts on X and $x \in X$, then $|\mathcal{O}(x)| = [G:G_x]$.

Proof: Define $\phi: G/G_x \to \mathcal{O}(x)$ by $\phi(gG_x) = g \bullet x$.
We will show ϕ is a bijection, hence the orders of the sets are equal.
To show ϕ is a well-defined injection, we let gG_x, and $hG_x \in G/G_x$ such that $\phi(gG_x) = \phi(hG_x)$. Then we note that

$$\begin{aligned} \phi(gG_x) = \phi(hG_x) &\Leftrightarrow g \bullet x = h \bullet x \\ &\Leftrightarrow h^{-1} \bullet (g \bullet x) = h^{-1} \bullet (h \bullet x) \\ &\Leftrightarrow (h^{-1}g) \bullet x = (h^{-1}h) \bullet x \\ &\Leftrightarrow (h^{-1}g) \bullet x = x \\ &\Leftrightarrow h^{-1}g \in G_x \quad (\text{recall } G_x = \{g \in G \mid g \bullet x = x\}) \\ &\Leftrightarrow gG_x = hG_x. \end{aligned}$$

$\therefore$ ϕ is a well-defined injection.
To show ϕ is surjective, let $a \in \mathcal{O}(x)$.
Then $\exists\, g \in G$ such that $g \bullet x = a$. So $\phi(gG_x) = g \bullet x = a$.
$\therefore$ ϕ is surjective.
$\therefore$ ϕ is a bijection and $|\mathcal{O}(x)| = [G:G_x]$.

Corollary General Class Equation
$|X| = \sum_i [G : G_{x_i}]$ where one x_i is taken from each orbit.

What is this saying if G is acting on itself by conjugation?
$|G| = \sum_i [G : C_G(x_i)]$. (Recall $C_G(x)$ is special case of G_x)
If $x \in Z(G)$, then $C_G(x) = G$ and $[G:C_G(x_i)] = 1$. (Since x commutes with everything in G)

Theorem The Class Equation
$|G| = |Z(G)| + \sum_i [G : G_{x_i}]$
where one x_i is taken from each conjugacy class with more than 1 element.

More corollaries of the fact that $|\mathcal{O}(x)| = [G:G_x]$:

Corollary $|\mathcal{O}(x)| \mid |G|$.
Proof: $|\mathcal{O}(x)| = [G:G_x] \mid |G|$ by Lagrange's theorem.

Corollary $|x^G| \mid |G|$.
Note: This is just a special case of $|\mathcal{O}(x)| \mid |G|$.

Recall that the number of permutations of same cycle structure divides the order of the group.

Corollary If G is a finite group and $H \leq G$, then the number of conjugates of H is equal to $[G:N_G(H)]$. This is just a special case of $|\mathcal{O}(x)| = [G:G_x]$.

Theorem Cauchy's Theorem
If G is a finite group such that $p \mid |G|$ and p is prime, then G contains an element of order p.

Proof:
Note: We have proven this for G Abelian. So we will assume G is not Abelian. Outline: Suppose $|G| = pm$ where p is prime.
We'll induct on m.
The result is true for base case as $|G| = p \bullet 1 \Rightarrow |G|$ is cyclic $\Rightarrow G$ is Abelian and we've already proven the result for G Abelian.
Read the proof in the text.

I will collect #83, 89(ii) on Monday and #94 on Wednesday.
For #98, use the Index Factorial Theorem.