Group Actions

Def: An <u>action</u> of a group G on a set X is a function
$$*: G \times X \longrightarrow X$$
satisfying the following two conditions:

(1) $1_G * x = x$ for all $x \in X$

(2) For all $g, h \in G$ and $x \in X$
$$g * (h * x) = (gh) * x$$

One says that <u>G acts on X via $*$.</u>

<u>Examples</u> 1. Trivial action: For any gp G and set X have
$$*: G \times S \longrightarrow S$$
$$(g, s) \longmapsto s$$

2. G acts on itself via left multiplication
$$m: G \times G \longrightarrow G.$$
$$m(g,h) = gh$$

Axioms 1: $\forall g \in G$, $1_G\, g = g$

2: $\forall g, h, k \in G$
$$g(hk) = (gh)k$$
by associativity

3. $G = GL_2(\mathbb{R})$ and $X = \mathbb{R}^2$: G acts on X via matrix multiplication.
$$GL_2(\mathbb{R}) \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$
$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix}\right) \longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$$

Axioms: 1. $\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x\\y\end{pmatrix} \quad \forall \begin{pmatrix}x\\y\end{pmatrix}\in\mathbb{R}^2$

2. $\begin{pmatrix}a&b\\c&d\end{pmatrix}\left(\begin{pmatrix}e&f\\g&h\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}\right)=\left(\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}e&f\\g&h\end{pmatrix}\right)\begin{pmatrix}x\\y\end{pmatrix}$

4. There is the natural action of $Sym(X)$ on X:

$$Sym(X)\times X \longrightarrow X$$
$$(f,x)\longmapsto f(x)$$

This is where the definition comes from.

5. There is a natural action of G on itself by what is called conjugation:

$$G\times G \longrightarrow G$$
$$(g,h)\longmapsto \cancel{ghg^{-1}} \qquad g*h=ghg^{-1}$$

Axioms: 1. $\forall h\in G,\ 1_G h 1_G^{-1}=h.$

2. $\forall g,h,k\in G$ have

$$g*(h*k)=g*(hkh^{-1})=ghkh^{-1}g^{-1}=ghk(gh)^{-1}=(gh)*k$$

Prop: Let G act on a set X via $*$. For every $g\in G$, the function

$$\sigma_g: X\longrightarrow X$$
$$x\longmapsto g*x$$

is a bijection. The resulting function

$$\rho: G\longrightarrow Sym(X)$$
$$g\longmapsto \sigma_g$$

is a group homomorphism.

Proof: To show that σ_g is a bijection, we show that σ_g has an inverse. We claim that $\sigma_{g^{-1}}$ is the inverse of σ_g.

Indeed, let $x \in X$. Then

$$\begin{aligned}
\sigma_g \circ \sigma_{g^{-1}}(x) &= \sigma_g(g^{-1} * x) && \text{by def of } \sigma_{g^{-1}} \\
&= g * (g^{-1} * x) && \text{by def of } \sigma_g \\
&= (g * g^{-1}) * x && \text{by gp action axiom 2} \\
&= 1_G * x && \text{since } g * g^{-1} = 1_G \\
&= x && \text{by gp action axiom 1.}
\end{aligned}$$

Similarly, $\sigma_{g^{-1}} \circ \sigma_g(x) = x$.

Now we show that ρ is a gp homomorphism. Let $g, h \in G$. Then

$$\rho(gh) = \sigma_{gh} \quad \text{and} \quad \rho(g)\rho(h) = \sigma_g \circ \sigma_h$$

Therefore we need to show that the function σ_{gh} and $\sigma_g \circ \sigma_h$ are the same. Let $x \in X$. Then

$$\begin{aligned}
\sigma_{gh} &= (gh) * x && \text{by def of } \sigma_{gh}. \\
&= g * h * x && \text{by gp action axiom 2} \\
&= g * \sigma_h(x) && \text{by def of } \sigma_h. \\
&= \sigma_g(\sigma_h(x)) && \text{by def of } \sigma_g \\
&= \sigma_g \circ \sigma_h(x).
\end{aligned}$$

Hence ρ is a group homomorphism.

Prop: Let G be a gp and X a set. Let $\rho: G \to \mathrm{Sym}(X)$ be a gp homomorphism. Then the function

$$\begin{aligned} *: G \times X &\to X \\ (g, x) &\mapsto (\rho(g))(x) \end{aligned}$$

defines an action of G on X.

proof: Axiom 1: Let $x \in X$. Then

$$\begin{aligned} 1_G * x &= (\rho(1_G))(x) && \text{by def of } * \\ &= \mathrm{id}_X(x) && \text{since } \rho \text{ is a gp hom.} \\ &= x && \text{by def. of } \mathrm{id}_X \end{aligned}$$

Axiom 2: Let $g, h \in G$ and let $x \in X$. Then

$$\begin{aligned} g * h * x &= g * (\rho(h))(x) && \text{by def of } * \\ &= \rho(g)((\rho(h))(x)) && \text{by def of } * \\ &= (\rho(g) \circ \rho(h))(x) && \text{by def of composition of functions} \\ &= (\rho(gh))(x) && \text{since } \rho \text{ is a gp hom} \\ &= (gh) * x && \text{by def of } *. \quad \square \end{aligned}$$

Remark: The two constructions of the previous two propositions are inverse to each other. Therefore to give an action of G on X is equivalent to giving a gp hom. from G to $\mathrm{Sym}(X)$!

Cayley's Thm: Let G be a gp. Then G is isomorphic to a subgp of $Sym(G)$.
If $|G| = n$, then G is isomorphic to a subgp of $Sym(n)$.

proof: Let G act on itself via left multiplication. This induces a gp homomorphism

$$\rho: G \to Sym(G)$$
$$g \mapsto \sigma_g : G \to G,\quad h \mapsto gh$$

We claim that ρ is injective.

$$g \in \ker(\rho) \quad \text{iff} \quad \sigma_g = id_G$$
$$\text{iff} \quad \sigma_g(h) = h \quad \forall\, h \in G$$
$$\text{iff} \quad gh = h \ \forall h \in G \text{ by def of } \sigma_g$$

If $gh = h$ for all $h \in G$, then taking $h = 1_G$ implies $g = 1_G$.
Therefore we've shown that $\ker(\rho) = \{1_G\}$. Hence ρ is injective,
So by 1^{st} isom. thm, G is isomorphic to $im(\rho)$.
For the second part of the Thm, we just note that
If $|X| = n$, then $Sym(X) \cong Sym(n)$. $\square$.

proof that if $|X| = n$, then $\mathrm{Sym}(X) \cong \mathrm{Sym}(n)$.

$|X| = n$ means that there is a bijection

$$\Phi : X \longrightarrow \{1, 2, \dots, n\}$$

Let $\Psi : \{1, 2, \dots, n\} \longrightarrow X$ be the inverse of Φ.

We claim that

$$\begin{aligned} \varphi : \mathrm{Sym}(X) &\longrightarrow \mathrm{Sym}(n) \\ \sigma &\longmapsto \Phi \circ \sigma \circ \Psi \end{aligned}$$

is a gp isomorphism.

First we show φ is a gp hom. Let $\sigma, \tau \in \mathrm{Sym}(X)$. Then

$$\begin{aligned} \varphi(\sigma \circ \tau) &= \Phi \circ \sigma \circ \tau \circ \Psi \\ &= \Phi \circ \sigma \circ \Psi \circ \Phi \circ \tau \circ \Psi \quad \text{since } \Psi \circ \Phi = id_X \\ &= \varphi(\sigma) \circ \varphi(\tau) \end{aligned}$$

To show φ is an isomorphism, we write an inverse:

$$\begin{aligned} \rho : \mathrm{Sym}(n) &\longrightarrow \mathrm{Sym}(X) \\ \sigma &\longmapsto \Psi \circ \sigma \circ \Phi \end{aligned}$$

Then

$$\begin{aligned} \rho \circ \varphi(\sigma) &= \rho(\Phi \circ \sigma \circ \Psi) \quad \text{by def. of } \varphi \\ &= \Psi \circ \Phi \circ \sigma \circ \Psi \circ \Phi \quad \text{by def of } \rho \\ &= \sigma \quad \text{since } \Psi \circ \Phi = id_X \text{ and } \Phi \circ \Psi = id_{\{1,2,\dots,n\}}. \end{aligned}$$

Similarly $\varphi \circ \rho(\sigma) = \sigma$.

Group Actions Continued

Prop: Let the group G act on the set X via $*$. Then the relation defined by

$$x \sim y \quad \text{iff} \quad \exists g \in G \text{ such that } g * x = y$$

is an equivalence relation.

proof: 1. (reflexivity) $\forall x \in X$, by gp action axiom 1, $1_G * x = x$.

Hence $x \sim x$.

2. (symmetry) Let $x, y \in X$ be such that $x \sim y$. Then $\exists g \in G$ such that $g * x = y$. We the have that

$$\begin{aligned}
g^{-1} * y &= g^{-1} * (g * x) && \text{since } g * x = y \\
&= (g^{-1} g) * x && \text{by gp action axiom 2} \\
&= 1_G * x && \text{since } g^{-1} g = 1_G \\
&= x && \text{by gp action axiom 1.}
\end{aligned}$$

Hence $y \sim x$.

3. (transitivity) Let $x, y, z \in X$ be such that $x \sim y$, $y \sim z$. This means $\exists g, h \in G$ such that $g * x = y$, $h * y = z$.

We need to show that $\exists\, k \in G$ s.t. $k * x = z$. Letting $k = hg$, we have

$$
\begin{aligned}
k * x &= (hg) * x && \text{since } k = hg \\
&= h * (g * x) && \text{gp action axiom 2} \\
&= h * y && \text{since } g * x = y \\
&= z && \text{since } h * y = z
\end{aligned}
$$

Hence $x \sim z$. $\square$

~~Def: The equivalence classes of the above equivalence relation~~

Def: Given an action of a group G on a set X via $*$, the equivalence classes of the equivalence relation in the proposition are called the orbits of G in X. For $x \in X$, the equivalence class containing x is denoted $\mathrm{orb}_G(x)$ (or $\mathcal{O}_x$ in the notes).

Remark: We have the following ~~major~~ observation: Let G act on a set X via $*$ and let $x \in X$. Then

$$
\begin{aligned}
\mathrm{orb}_G(x) &= \{ y \in X : \exists\, g \in G \text{ such that } g * x = y \} \\
&= \{ g * x : g \in G \}
\end{aligned}
$$

By the proposition, the orbits of G in X partition X.

Def: Let G act on a set X via $*$. We say that the action is transitive if for all $x,y \in X$ there exists a $g \in G$ such that $g * x = y$.

Remark: Let G act on a set X via $*$. To say the action is transitive means that there is only one orbit of G in X, (that there is only one equivalence class in the equivalence relation). Therefore, to show an action of G on a set X is transitive it is enough to exhibit one $x \in X$ and show that $\forall y \in X$, $\exists g \in G$ such that $g * x = y$.

Def: Let G act on a set X via $*$. For $x \in X$, we define the stabilizer of x in G as the set

$$\mathrm{stab}_G(x) = \{ g \in G : g * x = x \}$$

Prop: Let G act on a set X via $*$, and let $x \in X$. Then

$$\mathrm{stab}_G(x) \subseteq G$$

is a subgroup of G.

proof: 1. By gp action axiom 1, $1_G * x = x$, so $1_G \in \mathrm{stab}_G(x)$.
2. Let $g, h \in \mathrm{stab}_G(x)$.

Then we have

$$(gh) * x = g*(h*x) \quad \text{by axiom 2,}$$
$$= g*x \quad \text{since } h \in stab_G(x),$$
$$= x \quad \text{since } g \in stab_G(x),$$

Therefore $gh \in stab_G(x)$.

3. Let $g \in stab_G(x)$. Then.

$$g^{-1} * x = g^{-1}*(g*x) \quad \text{since } g \in stab_G(x)$$
$$= (g^{-1}g)*x \quad \text{by axiom 2}$$
$$= 1_G * x \quad \text{since } g^{-1}g = 1_G$$
$$= x \quad \text{by axiom 1.}$$

Therefore $g^{-1} \in stab_G(x)$. $\square$

<u>Prop</u>: Let G act on a set X via $*$. Then $\forall x \in X, g \in G$,

$$stab_G(g*x) = g\, stab_G(x) g^{-1}$$

<u>proof</u>: Show inclusion both ways.

$\subseteq$ Let $h \in stab_G(g*x)$, so $h*(g*x) = g*x$. Then.

$$(g^{-1}hg) * x = g^{-1} * (hg*x) \quad \text{by axiom 2}$$
$$= g^{-1} * (h*(g*x)) \quad \text{by axiom 2}$$

$= g^{-1} * (g * x)$ since $h*(g*x) = g*x$

$= g^{-1}g * x$ by axiom 2

$= 1_G * x$ $g^{-1}g = 1_G$

$= x$ axiom 1

Therefore $g^{-1}hg \in \mathrm{stab}_G(x)$, so $h \in g\,\mathrm{stab}_G(x)g^{-1}$.

$\supseteq$ Let $h \in g\,\mathrm{stab}_G(x)g^{-1}$, so $h = gkg^{-1}$ for some $k \in \mathrm{stab}_G(x)$. Then

$h*(g*x) = gkg^{-1} * (g*x)$ since $h = gkg^{-1}$

$= (gkg^{-1}g) * x$ axiom 2

$= g*(k*x)$ $g^{-1}g = 1_G$, axiom 1, and axiom 2

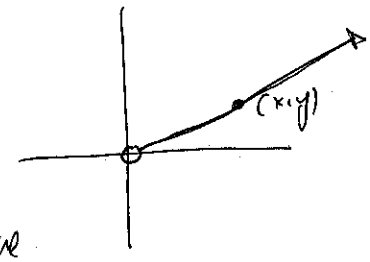
$= g*x$ since $k \in \mathrm{stab}_G(x)$

Therefore $h \in \mathrm{stab}_G(g*x)$. $\square$

<u>Examples:</u> 1. Let the group $\mathbb{R}_{>0}$ with multiplication act on the set $\mathbb{R}^2$ via scalar multiplication

$$* : \mathbb{R}_{>0} \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$
$$(c, (x,y)) \longmapsto (cx, cy)$$

Given $(x,y) \in \mathbb{R}^2$ if $(x,y) \neq (0,0)$, then



$\cancel{\text{orb}}$ orb$((x,y)) = \{(cx, cy) : c \in \mathbb{R}_{>0}\}$

ray with open endpoint at the origin passing through the point (x,y)

if $(x,y) = (0,0)$, then

$\text{orb}((0,0)) = \{(c\cdot 0, c\cdot 0) = (0,0) : c \in \mathbb{R}_{>0}\} = \{(0,0)\}$

so the orbit is the single point $(0,0)$.

if $(x,y) \neq (0,0)$, then

$\text{stab}((x,y)) = \{c \in \mathbb{R}_{>0} : (cx, cy) = (x,y)\} = \{1\} \subseteq \mathbb{R}_{>0}$

if $(x,y) = (0,0)$, then

$\text{stab}((0,0)) = \{c \in \mathbb{R}_{>0} : (c\cdot 0, c\cdot 0) = (0,0)\} = \mathbb{R}_{>0}$

2. Conjugation: Let G act on itself via conjugation

$$*: G \times G \to G$$
$$(g,h) \mapsto ghg^{-1}$$

and let $\rho: G \to \text{Sym}(G)$ be the corresponding gp hom.

$$g \mapsto \sigma_g : G \to G$$
$$h \mapsto ghg^{-1}$$

Observe that the kernel of ρ is the set of elements of G that commute with all of G:

$$\ker(\rho) = \{g \in G : \sigma_g = id_G\} \quad \text{by def. of kernel}$$

$$= \{g \in G : \forall h \in G, \ \sigma_g(h) = id_G(h)\} \quad \text{by def. of two functions being the same,}$$

$$= \{g \in G : \forall h \in G \ \ g h g^{-1} = h\} \quad \text{by def. of } \sigma_g \text{ and } id_G$$

$$= \{g \in G : \forall h \in G \ \ gh = hg\} \quad \text{since } ghg^{-1} = h \text{ iff } gh = hg$$

We call the kernel of ρ ~~and denote it~~ the center of G and denote it by $Z(G)$:

$$Z(G) = \{g \in G : \forall h \in G, \ gh = hg\}$$

Note that $Z(G)$ is a normal subgp of G since it is the kernel of a group hom. Exercise: Show this using the definition.

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

The orbits of the action of G on its self by conjugation are called the conjugacy classes of G.

Given $g \in G$, the stabiliser of g under the action of conjugation is called the centraliser of g in G and denoted

$$C_G(g) = Z(g) = \operatorname{stab}(g) = \{a \in G : a g a^{-1} = g\} = \{a \in G : ag = ga\}$$

Group Actions Continued

Recall: Conjugation action, center of a group, conjugacy classes

Def: Two elements $a, b \in G$ are called **conjugate** if $\exists c \in G$ such that $a = cbc^{-1}$.

Exercise: If $a, b \in G$ are conjugate, then a and b have the same order.

Proof: Say $a = cbc^{-1}$. The map

$$\varphi_c : G \longrightarrow G$$
$$\varphi_c(g) = cgc^{-1}$$

is a group ~~[illegible]~~ isomorphism, so the order of b is the same as the order of $\varphi_c(b) = cbc^{-1} = a$.

Conjugacy classes of the symmetric group

Def: Let $\sigma \in Sym(n)$. If a cycle decomposition of σ contains cycles of lengths $n_1, n_2, \ldots, n_r$, then we say that σ has **cycle type** $n_1, n_2, \ldots, n_r$.

Recall: If $\sigma \in Sym(n)$ has cycle type $n_1, n_2, \ldots, n_r$, then the order of σ is the least common multiple of $n_1, n_2, \ldots, n_r$.

Prop: $\sigma, \tau \in Sym(n)$ are conjugate iff σ and τ have the same cycle type.

proof: see written lecture notes.

Exercise on homework (the last homework): If $n > 2$, then $Z(Sym(n)) = \{id\}$.

Called Burnside's orbit equation in Boltje's notes

<u>Thm</u> (orbit-stabiliser thm): Let G be a finite group acting on a set X via $*$. Let $x \in X$. Then

$$|G| = |\operatorname{stab}(x)| \cdot |\operatorname{orb}(x)| \quad \text{or equiv.} \quad |G|/|\operatorname{stab}(x)| = |\operatorname{orb}(x)|$$

<u>proof</u>: We show that the function

$$f : G/\operatorname{stab}(x) \longrightarrow \operatorname{orb}(x)$$
$$g\operatorname{stab}(x) \longmapsto g * x$$

is a bijection. Then

$$|G|/|\operatorname{stab}(x)| = |G/\operatorname{stab}(x)| = |\operatorname{orb}(x)|$$

First we show f is well defined: If $g\operatorname{stab}(x) = h\operatorname{stab}(x)$, then $g^{-1}h \in \operatorname{stab}(x)$, so

$$g^{-1}h * x = x$$

Then $h * x = gg^{-1}h * x = g * (g^{-1}h * x) = g * x$ so

$$f(h\operatorname{stab}(x)) = f(g\operatorname{stab}(x))$$

Now we show f is injective: Say $f(a\operatorname{stab}(x)) = f(b\operatorname{stab}(x))$. This means $a * x = b * x$. Then $a^{-1}b * x = a^{-1}a * x = 1_G * x = x$ so $a^{-1}b \in \operatorname{stab}(x)$ implying $a\operatorname{stab}(x) = b\operatorname{stab}(x)$. Therefore f is injective.

Finally, f is surjective because

$$\operatorname{orb}(x) = \{g * x : g \in G\} = \operatorname{im}(f). \quad \square$$

Group Actions Cont.

Class equation: Let G be a finite group and let G act on itself via conjugation. Let $g_1, \ldots, g_k, g_{k+1}, \ldots, g_r$ be representatives of the conjugacy class of G and ~~assume that~~ order the g_i so that if $i > k$, then $g_i \in Z(G)$.

Since the conjugacy class partition G, we have

$$|G| = \sum_{i=1}^{r} |\mathrm{ord}_G(g_i)|$$

We can simplify the sum further in two ways

(1) $|\mathrm{ord}_G(g_i)| = 1$ iff $g_i \in Z(G)$!

(2) $|\mathrm{ord}_G(g_i)| = |G| / |\mathrm{stab}_G(g_i)| = [G : C_G(g_i)]$ by orbit-stabilizer thm

Therefore we have

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(g_i)]$$

The signifigance of this representation of $|G|$ is that all the terms in the sum on the RHS of the equation divide $|G|$. We will see a consequence of this in a moment.

Def: Let p be a prime. A p-group is a finite group G such that $|G| = p^a$ for some $a \in \mathbb{N}$. That is a p-group is a group with a power of p many elements. Note that every subgp and every factor gp of a p-group is also a p-group and every element of a p-group has order a power of p.

Thm Let G be a p-group. Then $|Z(G)| > 1$.

proof: We use the class equation, which gives

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(g_i)]$$

where $g_1, g_2, \dots, g_k$ are representatives for the conjugacy classes that have size larger than 1.

Observe that p divides $|G|$ and p divides $[G : C_G(g_i)]$ for all i since G is a p-group. Therefore p divides $|Z(G)|$ since

$$|Z(G)| = |G| - \sum_{i=1}^{k} [G : C_G(g_i)]$$

Hence $|Z(G)| > 1$. □

* NOT COVERED IN LECTURE *

Def: Let $\sigma \in \mathrm{Sym}(n)$. If a cycle decomposition of σ has cycles of length $r_1, r_2, \dots, r_m$, then we say that σ has cycle type $r_1, r_2, \dots, r_m$.

Thm: $\sigma, \tau \in \mathrm{Sym}(n)$ are in the same conjugacy class if and if σ and τ have the same ~~type~~ cycle type.

proof: First we show that conjugating and element $\sigma \in \mathrm{Sym}(n)$ by $\tau \in \mathrm{Sym}(n)$ does not change the cycle type. We will do this in three steps.

Step 1: We may assume σ is a k-cycle.

Write $\sigma = \gamma_1\gamma_2\cdots\gamma_m$ as a product of disjoint $\underbrace{\text{cycles}}^{\text{of lengths } r_1, r_2, \ldots, r_m}$. Then

$$\tau\sigma\tau^{-1} = \tau\gamma_1\gamma_2\cdots\gamma_m\tau^{-1}$$
$$= \tau\gamma_1\tau^{-1}\tau\gamma_2\tau^{-1}\cdots\tau\gamma_{m-1}\tau^{-1}\tau\gamma_m\tau^{-1}$$

Therefore if $\tau\gamma_i\tau^{-1}$ is an r_i-cycle for all i, then the cycle type of $\tau\sigma\tau^{-1}$ is the same as the cycle type of σ.

Step 2: We may assume τ is a transposition.

Write $\tau = \delta_1\delta_2\cdots\delta_k$ as a product of transpositions. Then

$$\tau\sigma\tau^{-1} = \delta_1\delta_2\cdots\delta_k\sigma(\delta_1\delta_2\cdots\delta_k)^{-1}$$
$$= \delta_1\delta_2\cdots\delta_k\sigma\delta_k^{-1}\delta_{k-1}^{-1}\cdots\delta_2^{-1}\delta_1^{-1}$$

Therefore $\underbrace{\cancel{\text{if}}}_{\text{we need to have that}}$ $\delta_k\sigma\delta_k^{-1}$ has same cycle type as σ

$\delta_{k-1}(\delta_k\sigma\delta_k^{-1})\delta_{k-1}^{-1}$ has same cycle type as $\delta_k\sigma\delta_k^{-1}$

$\vdots$

$\delta_1(\delta_2\cdots\delta_k\sigma\delta_k^{-1}\delta_{k-1}^{-1}\cdots\delta_2)\delta_1^{-1}$ has same cycle type as $\delta_2\delta_3\cdots\delta_k\sigma\delta_k^{-1}\delta_{k-1}^{-1}\cdots\delta_2$

which, since the δ_i are all transpositions, is true ~~iff~~ if $\delta\sigma\delta^{-1}$ has same same cycle type as σ for transpositions δ.

Step 3: Let $\sigma = (a_1 a_2 \cdots a_k)$ be a k-cycle and $\tau = (ij)$ be a transposition.

Then $\tau\sigma\tau^{-1}$ is a k-cycle.

Within step 3 there are 3 cases.

__Case 1__: $a_\ell \neq i$ or j $\forall \ell$. Then σ and τ are disjoint, so

$$\tau\sigma\tau^{-1} = (ij)(a_1 a_2 \cdots a_k)(ij) = (ij)(ij)(a_1 \cdots a_k) = (a_1 \cdots a_k) = \sigma$$

so $\tau\sigma\tau^{-1} = \sigma$ is a k-cycle.

__Case 2__: ~~$a_\ell \neq i$ and $a_\ell \neq j$ for some ℓ (we may assume~~
i and j both appear in $\{a_1, a_2, \ldots, a_k\}$. Then after reordering σ, we may assume $a_1 = i$ and $a_\ell = j$ for some $\ell > 1$.
Then

$$\tau\sigma\tau^{-1} = (ij)(i\, a_2 \cdots a_{\ell-1}\, j\, a_{\ell+1} \cdots a_k)(ij)$$

$$= \underbrace{(i\, a_{\ell+1}\, a_{\ell+2} \cdots a_k\, j\, a_2 a_3 \cdots a_{\ell-1})}_{k\text{-cycle}}$$

__Case 3__: i appears in $\{a_1, a_2, \ldots, a_k\}$ but j does not.
After reordering, we may assume $a_1 = i$. Then

$$\tau\sigma\tau^{-1} = (ij)(i\, a_2 \cdots a_k)(ij)$$

$$= \underbrace{(j\, a_2 \cdots a_{k-1}\, a_k)}_{k\text{-cycle}}$$

We've shown that conjugation does not change the cycle type. To finish we need to show that if $\sigma, \tau \in \mathrm{Sym}(n)$ have the same cycle type, then $\exists\, \delta \in \mathrm{Sym}(n)$ such that $\delta\sigma\delta^{-1} = \tau$.

Similarly to the previous step, we may reduce to the case of when σ and τ are k-cycles. Let $\sigma = (a_1 a_2 \cdots a_k)$, $\tau = (b_1 b_2 \cdots b_k)$.

Define δ in the following way:

On $\{a_1, a_2, \dots, a_k\}$ define $\delta(a_i) = b_i$.

Observe that both sets $S_1 = \{1, 2, \dots, n\} - \{a_1, a_2, \dots, a_k\}$ and $S_2 = \{1, 2, \dots, n\} - \{b_1, b_2, \dots, b_k\}$ have cardinality $n-k$. Let δ be any bijection from S_1 to S_2.

Then we have, for $i = 1, \dots, k$

$$\delta \sigma \delta^{-1}(b_i) = \delta \sigma (a_i) = \delta(a_{i+1}) = b_{i+1}$$

and if $\ell \in S_2$, then $\delta^{-1}(\ell) \in S_1$ so $\delta^{-1}(\ell) \notin \{a_1, a_2, \dots, a_k\}$, so ~~[illegible]~~ $\sigma(\delta^{-1}(\ell)) = \delta^{-1}(\ell)$. Hence

$$\delta \sigma \delta^{-1}(\ell) = \delta \sigma(\delta^{-1}(\ell)) = \delta(\delta^{-1}(\ell)) = \ell$$

Therefore $\delta \sigma \delta^{-1} = \tau$. $\square$

~~Cor: $Z(\mathrm{Sym}(n)) = \{id\}$ if $n > 2$.~~

~~proof: [illegible]~~

~~Let $\sigma \in \mathrm{Sym}(n)$ be such that $\sigma \neq id$. Then if σ is a transposition, since $n > 2$ there exists another transposition in $\mathrm{Sym}(n)$ so σ is conjugate to another element of $\mathrm{Sym}(n)$.~~

~~If σ~~

* BACK TO WHAT IS IN LECTURE *

<u>Lemma</u>: If G is a group such that $G/Z(G)$ is cyclic, then G is abelian.

<u>proof</u>: ~~G/Z(G) cyclic means that~~

Let $a, b \in G$. We need to show that $ab = ba$.

$G/Z(G)$ cyclic means $\exists\, x \in G$ such that $G/Z(G) = \langle xZ(G) \rangle$.

Then $a = x^k c_1$, $b = x^\ell c_2$ for $k, \ell \in \mathbb{Z}$, $c_1, c_2 \in Z(G)$.

Then ~~there~~ we have

$$
\begin{aligned}
ab &= x^k c_1 x^\ell c_2 \\
&= x^k x^\ell c_1 c_2 && \text{because } c_1 \in Z(G) \\
&= x^{k+\ell} c_2 c_1 && \text{because } c_2 \in Z(G) \\
&= x^{\ell} c_2 x^k c_1 && \text{because } x^k x^\ell = x^{k+\ell} = x^{\ell+k} = x^\ell x^k \text{ and } c_2 \in Z(G) \\
&= ba
\end{aligned}
$$

so G is abelian. $\square$

<u>Cor</u>: Assume that p is a prime and that G is a gp of order p^2. Then G is abelian.

<u>proof</u>: By previous theorem $Z(G) \neq \{1_G\}$, so $|Z(G)| = p$ or p^2 by Lagrange's Thm. Hence $|G/Z(G)| = |G|/|Z(G)| = p$ or 1, so $G/Z(G)$ is cyclic and therefore by the lemma abelian. $\square$

Def: Let G act on a set X via $*$. An element $x \in X$ is called a G-fixed point if $g * x = x$ for all $g \in G$. The set of G-fixed points in X is denoted X^G, so

$$X^G = \{x \in X : g * x = x \ \forall g \in G\}$$

Example: If we take $X = G$ and let G act on itself via conjugation, then

$$X^G = Z(G).$$

Prop: Let G be a p-group and let G act on the set X via $*$. Assume X is a finite set. Then

$$|X^G| \equiv |X| \mod p$$

proof: Let $\mathcal{R}$ be a set of representatives for the orbits of G in X. Then since the orbits partition X, we have:

$$|X| = \sum_{x \in \mathcal{R}} |\mathrm{orb}(x)|$$

By the orbit-stabilizer thm, we have

$$|X| = \sum_{x \in \mathcal{R}} |G/\mathrm{stab}(x)|$$

Now observe that $x \in X^G$ iff $|\mathrm{orb}(x)| = 1$ iff $\mathrm{stab}(x) = G$. Hence we have

$$|X| = \sum_{\substack{x \in R \\ x \in X^G}} 1 + \sum_{\substack{x \in R \\ stab(x) \neq G}} |G/stab(x)|$$

since G is a p-grp and $stab(x) \neq G$, p divides all the terms in the second sum

$= |X^G| +$ some number divisible by p

$\equiv |X^G| \mod p.$ $\square$

<u>Thm</u> (Cauchy's Thm): Let G be a finite group and let p be a prime which divides $|G|$. Then G has an element of order p and a subgroup of order p.

<u>proof</u>: Consider the set

$$X = \{(x_1, x_2, \dots, x_p) \in G \times G \times \cdots \times G : x_1 x_2 \cdots x_p = 1\}$$

We claim that $|X| = |G|^{p-1}$. Indeed, for an arbitrary element $x = (x_1, x_2, \dots, x_p) \in X$, there are $|G|$ choices for what $x_1, x_2, \dots, x_{p-1}$ could be, and then x_p must be equal to ~~[illegible]~~ $(x_1 x_2 \cdots x_{p-1})^{-1}$:

$$x_p = (x_1 x_2 \cdots x_{p-1})^{-1}$$

Hence there are a total of $|G|^{p-1}$ choices for x, so $|X| = |G|^{p-1}$.

Now observe that $\mathbb{Z}/p\mathbb{Z}$ acts on X by permuting the coordinates cyclically: Define

$$*: \mathbb{Z}/p\mathbb{Z} \times X \longrightarrow X$$

$$\bar{i} * (x_1, x_2, \dots, x_p) = (x_{i+1}, x_{i+2}, \dots, x_p, x_1, \dots, x_i)$$

where i is the standard representative of $\bar{i}$ mod p.

We show that $\bar{i} * (x_1, x_2, \dots, x_p) = (x_{i+1}, x_{i+2}, \dots, x_p, x_1, \dots, x_i)$ is indeed an element of X:

$$\begin{aligned} x_{i+1}x_{i+2}\cdots x_p x_1 \cdots x_i &= (x_1x_2\cdots x_i)^{-1}(x_1x_2\cdots x_i)x_{i+1}x_{i+2}\cdots x_p x_1\cdots x_i \\ &= (x_1x_2\cdots x_i)^{-1}(x_1x_2\cdots x_p)(x_1x_2\cdots x_i) \\ &= (x_1x_2\cdots x_i)^{-1}(x_1x_2\cdots x_i) \\ &= 1 \end{aligned}$$

Now observe ~~that~~ what the fixed points of the action are:

$$X^{\mathbb{Z}/p\mathbb{Z}} = \{(x, x, \dots, x) \in G \times G \times \cdots G : x^p = 1\}$$

since any element fixed by $\mathbb{Z}/p\mathbb{Z}$ must have the same ~~coordinate~~ element of G in every slot. We have that $X^{\mathbb{Z}/p\mathbb{Z}} \neq \emptyset$ since $1^p = 1$, so $(1, 1, \dots, 1) \in X^{\mathbb{Z}/p\mathbb{Z}}$. Therefore $|X^{\mathbb{Z}/p\mathbb{Z}}| \geq 1$. On the other hand, by the previous proposition,

$$|X| \equiv |X^{\mathbb{Z}/p\mathbb{Z}}| \mod p$$

and we know $|X| = |G|^{p-1} \equiv 0 \mod p$ since p divides $|G|$. Hence $|X^{\mathbb{Z}/p\mathbb{Z}}| \geq 1$ and p divides $|X^{\mathbb{Z}/p\mathbb{Z}}|$, so $|X^{\mathbb{Z}/p\mathbb{Z}}| > 1$. Let $(x, x, \dots, x) \in X^{\mathbb{Z}/p\mathbb{Z}}$ be such that $(x, x, \dots, x) \neq (1, 1, \dots, 1)$. Then $x \in G$, $x^p = 1$ and $x \neq 1$. Hence $o(x) \neq 1$ and $o(x) \mid p$. Therefore $o(x) = p$. $\square$