Group Actions

Def: An action of a group $G$ on a set $X$ is a function $*: G \times X \rightarrow X$ satisfying the following two conditions:

1. $I_x * x = x$ for all $x \in X$
2. For all $gh \in G$ and $x \in X$
   
   $g*(h*x) = (gh)*x$

One says that $G$ acts on $X$ via $*$.

Examples 1. Trivial action: For any group $G$ and set $X$ there is

   $*: G \times S \rightarrow S$

   $(g,s) \mapsto s$

2. $G$ acts on itself via left multiplication

   $m: G \times G \rightarrow G$

   $m(g,h) = gh$

   Axioms: $\forall g \in G, \exists e \in G$

   $1. \forall g \in G$

   $g*e = e * g = g$

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

   $g(hk) = (gh)k$

   by associativity

3. $G = \text{GL}_2(\mathbb{R})$ and $X = \mathbb{R}^2$: $G$ acts on $X$ via matrix multiplication.

   $\text{GL}_2(\mathbb{R}) \times \mathbb{R}^2 \rightarrow \mathbb{R}^2$

   $\left( \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix} \right) \mapsto \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$
Axioms:

1. \( \Phi(x, y) = \Phi(y, x) \quad \forall (x, y) \in \mathbb{R}^2 \)

2. \( \left( (a, b) \times (f, g) \right) = \left( (a f, b g) \right) \)

4. There is the natural action of \( \text{Sym}(X) \) on \( X \):

\[
\text{Sym}(X) \times X \longrightarrow X \quad (f, x) \longmapsto f(x)
\]

This is where the definition comes from.

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

\[
G \times G \longrightarrow G, \quad (g, h) \longmapsto g hg^{-1}
\]

Axioms:

1. \( \forall h \in G, \quad 1g h 1^g = h \),

2. \( \forall g, h, k \in G \) then,

\[
g \ast (h \ast k) = g \ast (h k^{-1}) = g h k h^{-1} g^{-1} = g h (g h)^{-1} = (g h) \ast k
\]

Prop: Let \( G \) act on a set \( X \) via \( \ast \). For every \( g \in G \), the function

\[
\Phi_g : X \longrightarrow X, \quad x \longmapsto g \ast x
\]

is a bijection. The resulting function

\[
\varphi : G \longrightarrow \text{Sym}(X)
\]

\( g \longmapsto \Phi_g \)

is a group homomorphism.

Proof: To show that \( \Phi_g \) is a bijection, we show that \( \Phi_g \) has an inverse. We claim that \( \Phi_{g^{-1}} \) is the inverse of \( \Phi_g \).
Indeed, let \( x \in X \). Then

\[
\delta g \circ \delta g' (x) = \delta g (g' \ast x) \quad \text{by def of } \delta g
\]
\[
= g \ast (g' \ast x) \quad \text{by def } \ast \text{ of } g
\]
\[
= (g \ast g') \ast x \quad \text{by gp action axiom 2}
\]
\[
= 1_g \ast x \quad \text{since } g \ast g' = 1_g
\]
\[
= x \quad \text{by gp action axiom 1,}
\]

Similarly, \( \delta g^{-1} \circ \delta g (x) = x \).

Now we show that \( \rho \) is a gp homomorphism. Let \( gh \in G \). Then

\[
\rho (gh) = \delta g h \quad \text{and } \quad \rho (g) \rho (h) = \delta g \circ \delta h.
\]

Therefore we need to show that the function \( \delta g h \) and \( \delta g \circ \delta h \) are the same. Let \( x \in X \). Then

\[
\delta g h = (gh) \ast x \quad \text{by def of } \delta g h
\]
\[
= g \ast h \ast x \quad \text{by gp action axiom 2}
\]
\[
= g \ast \delta h (x) \quad \text{by def } \ast \text{ of } g
\]
\[
= \delta g (\delta h (x)) \quad \text{by def } \ast \text{ of } g
\]
\[
= \delta g \circ \delta h (x).
\]

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

$$
*: G \times X \to X
$$

$$(g, x) \mapsto (p(g))(x)$$

defines an action of $G$ on $X$.

**Proof.** **Axiom 1:** Let $x \in X$. Then

$$1_g \ast x = (p(1_g))(x) \quad \text{by def of } *$$

$$= \text{id}_X(x) \quad \text{since } p \text{ is a gp hom.}$$

$$= x \quad \text{by def of } \text{id}_X$$

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

$$g \ast (h \ast x) = g \ast (p(h))(x) \quad \text{by def of } *$$

$$= p(g)(p(h))(x) \quad \text{by def of } *$$

$$= (p(g)p(h))(x) \quad \text{by def of composition of functions}$$

$$= (p(gh))(x) \quad \text{since } p \text{ is a gp hom.}$$

$$= (gh) \ast x \quad \text{by def of } * \quad \square$$

**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 $\text{Sym}(X)$.
Cayley's Theorem: Let $G$ be a group. Then $G$ is isomorphic to a subgraph of $\text{Sym}(G)$. If $|G| = n$, then $G$ is isomorphic to a subgraph of $\text{Sym}(n)$.

**Proof:** Let $G$ act on itself via left multiplication. This induces a group homomorphism

$$\phi: G \rightarrow \text{Sym}(G)$$

We claim that $\phi$ is injective.

$g \in \ker(\phi)$ if and only if $\phi(g) = \text{id}_G$

iff $\phi(g)(h) = h$ for all $h \in G$

iff $gh = h$ for all $h \in G$

If $gh = h$ for all $h \in G$, then taking $h = ba$ implies $g = ba$.

Therefore we've shown that $\ker(\phi) = \{e\}$ (Hence $\phi$ is injective, $\ker(\phi) = \{e\}$.

By 1st Isom. Thm., $G$ is isomorphic to $\text{im}(\phi)$.

For the second part of the Thm, we just note that $\text{Sym}(X) \cong \text{Sym}(n)$. Q.E.D.
proof that if $|X| = n$, then $\text{Sym}(X) \cong \text{Sym}(n)$.

$|X| = n$ means that there is a bijection $\varphi: X \to \{1, 2, \ldots, n\}$.

Let $\alpha: \{1, 2, \ldots, n\} \to X$ be the inverse of $\varphi$.

We claim that 

$$\phi: \text{Sym}(X) \to \text{Sym}(n)$$

is a group isomorphism.

First we show $\phi$ is a group homomorphism. Let $\sigma, \tau \in \text{Sym}(X)$. Then

$$\phi(\sigma \circ \tau) = \varphi \circ \phi(\tau) \circ \phi(\sigma) \quad \text{since } \varphi \circ \tau = \varphi \circ \sigma \circ \tau = \varphi \circ \sigma$$

To show $\phi$ is an isomorphism, we write an inverse:

$$\rho: \text{Sym}(n) \to \text{Sym}(X)$$

Then $\rho \circ \phi(\sigma) = \rho(\varphi \circ \sigma)$ by def. of $\rho$

$= \varphi \circ \rho(\sigma)$ by def. of $\rho$

$= \sigma$ since $\varphi \circ \sigma = \text{id}_X$ and $\text{id}_X = \text{id}_{\{1, 2, \ldots, n\}}$.

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

/
Group Actions Continued

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

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

is an equivalence relation.

Proof:

1. (Reflexivity) $\forall x \in X$, by $g = 1_G$ action axiom 1, $1_G \ast x = x$.
   Hence $x \sim x$.

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

   $$g \ast y = g \ast (g \ast x) \quad \text{since } g \ast x = y$$

   $$= (g \ast g) \ast x \quad \text{by } g \ast \text{ action axiom 2}$$

   $$= 1_G \ast x \quad \text{since } g \ast g = 1_G$$

   $$= x \quad \text{by } g \ast \text{ action axiom 1}.$$

   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 $g \ast x = y$, $h \ast y = z$. This...
We need to show that \[ \forall h \in G \text{ s.t. } k \cdot x = z. \] Letting \( k = hy \),
we have
\[
h \cdot x = (hy) \cdot x \quad \text{since } h = hy
\]
\[
= h \cdot (y \cdot x) \quad \text{gp action axiom 2}
\]
\[
= h \cdot y \quad \text{since } g \cdot x = y
\]
\[
= z \quad \text{since } h \cdot y = z
\]

Hence \( x \sim z \). \( \Box \)

**Def:** The **equivalence relation** \( \sim \) on the set \( X \) induced by the action of \( G \) on \( X \) is called the \textit{equivalence relation} relative to \( \text{Action of } G \text{ on } X \).

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

**Remark:** We have the following \textit{regular} observation: Let \( G \) act on a set \( X \) via \( \ast \) and let \( x \in X \). Then

\[
\text{orb}_G(x) = \{ y \in X : \exists g \in G \text{ such that } g \cdot x = y \}
\]
\[
= \{ g \cdot x : g \in G \}
\]

By the proposition, the orbits of \( G \text{ in } X \) partition \( X \).
Def: Let $G$ act on a set $X$ via $\ast$. We say that the action is **transitive** if for all $x, y \in X$ there exists a $g \in G$ such that $g \ast x = y$.

Remark: Let $G$ act on a set $X$ via $\ast$. 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 $g \ast x = y$.

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

$$\text{stab}_G(x) = \{ g \in G : g \ast x = x \}$$

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

$$\text{stab}_G(x) \leq G$$

is a subgroup of $G$.

Proof: 1. By gp action axiom 1, $1 \ast x = x$, so $1 \in \text{stab}_G(x)$.

2. Let $g, h \in \text{stab}_G(x)$. Then
Then we have

\[(gh) \ast x = g \ast (h \ast x) \] by axiom 2,

\[= g \ast x \]

\[= x \]

since \( h \in \text{staba}(x) \),

since \( g \in \text{staba}(x) \).

Therefore \( gh \in \text{staba}(x) \).

3. Let \( g \in \text{staba}(x) \). Then

\[g' \ast x = g' \ast (g \ast x) \]

\[= (g'g) \ast x \]

\[= L_{g'} \ast x \]

\[= x \]

since \( g \in \text{staba}(x) \),

by axiom 2

since \( g'g = L' \)

by axiom 1.

Therefore \( g' \in \text{staba}(x) \). \( \Box \)

**Prop.** Let \( G \) act on a set \( X \) via \( \ast \). Then \( \forall x \in X, g \in G, \)

\[\text{staba}(g \ast x) = g \ast \text{staba}(x) \ast g' \]

**Proof.** Show inclusion both ways.

\[\subseteq \] Let \( h \in \text{staba}(g \ast x) \), so \( h \ast (g \ast x) = g \ast x \). Then

\[(g' \ast h)g \ast x = g' \ast (hg \ast x) \]

\[= g' \ast (h \ast (g \ast x)) \]

by axiom 2

by axiom 2.
\[
\begin{align*}
\bar{g}^* (g^* x) &= g^* (g^* x) \\
&= g^* g^* x \\
&= 1_g^* x \\
&= x
\end{align*}
\]

since \( h^* (y^* x) = y^* x \)
by axiom 2
\( g^* y = 1_g \)
axiom 1

Therefore \( \bar{g}^* y \in \text{stabc}(x) \), so \( h \in g \text{stabc}(x) \).

\( \bar{g}^* (g^* x) = g^* (g^* x) \)
\( = (g^* g^* g)^* x \)
\( = g^* (x^* x) \)
\( = g^* x \)

Therefore \( h \in \text{stabc}(g^* x) \). \( \square \)

Examples: 1. Let the group \( \mathbb{R}^* \) with multiplication act on the set \( \mathbb{R}^2 \) via scalar multiplication

\[ \star : \mathbb{R}^* \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \]

\( (c, (x, y)) \mapsto (cx, cy) \)
Given \((x,y) \in \mathbb{R}^2\), if \((x,y) \neq (0,0)\), then

\[ \text{stab}(x,y) = \{ c \in \mathbb{R} : (cx, cy) = (x, y) \} = \{ 1 \} \subseteq \mathbb{R} \]

Ray with open endpoint at the origin passing through the point \((x, y)\).

If \((x, y) = (0, 0)\), then

\[ \text{stab}(0, 0) = \{ c \in \mathbb{R} : (0, c) = (0, 0) \} = \mathbb{R} \]

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

If \((x, y) \neq (0, 0)\), then

\[ \text{stab}(x, y) = \{ c \in \mathbb{R} : (cx, cy) = (x, y) \} = \{ 1 \} \subseteq \mathbb{R} \]

If \((x, y) = (0, 0)\), then

\[ \text{stab}(0, 0) = \{ c \in \mathbb{R} : (0, c) = (0, 0) \} = \mathbb{R} \]

2. Conjugation: Let \(G\) act on itself via conjugation

\[ \ast : G \times G \rightarrow G \]

\[ (g, h) \mapsto g h g^{-1} \]

and let \(p : G \rightarrow \text{Sym}(G)\) be the corresponding gp hom.
Observe that the kernel of \( \rho \) is the set of elements of \( G \) that commute with all of \( G \):

\[
\ker(\rho) = \{ g \in G : \rho(g) = \text{id}_G \} \quad \text{by def. of kernel}
\]

\[
= \{ g \in G : \forall h \in G, \rho(g)(h) = \text{id}_G(h) \} \quad \text{by def. of being the same}
\]

\[
= \{ g \in G : \forall h \in G, ghg^{-1} = h \} \quad \text{by def. of } \rho \text{ and } \text{id}_G
\]

\[
= \{ g \in G : \forall h \in G, gh = hg \} \quad \text{since } ghg^{-1} = h \Rightarrow gh = hg
\]

We call the kernel of \( \rho \) 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 subgroup 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 stabilizer of \( g \) under the action of conjugation is called the centralizer of \( g \) in \( G \), and denoted

\[
C_G(g) = Z(g) = \text{stab}(g) = \{ a \in G : aga^{-1} = g \} = \{ a \in G : ag = ga \}
\]
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

$$\phi_c : G \to G$$

$$\phi_c(g) = cgc^{-1}$$

is a group homomorphism, so the order of $b$ is the same as the order of $\phi_c(b) = cbc^{-1} = a$.

Conjugacy classes of the symmetric group

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

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

Prop. $\sigma, \tau \in \text{Sym}(n)$ are conjugate iff $\sigma$ and $\tau$ have the same cycle type.

Proof: see written lecture notes.

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

\[ /1 \]
*Called Burnside's orbit equation in Beltje's notes*

**Theorem (orbit-stabiliser theorem):** Let $G$ be a finite group acting on a set $X$ via $\ast$. Let $x \in X$. Then

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

**Proof:** We show that the function

$$f: G/\text{stab}(x) \to \text{orb}(x)$$

$$\text{gstab}(x) \mapsto g \ast x$$

is a bijection. Then

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

First we show $f$ is well defined: If $g\ast x = h\ast x$, so

$$g' = gh \in \text{stab}(x)$$

Then

$$h \ast x = g' \ast h \ast x = g' (g' \ast x) = g' x$$

Thus

$$f(h \ast x) = f(g \ast x)$$

Now we show $f$ is injective: Say $f(a\ast x) = f(b\ast x)$. Then $a^{-1} b \ast x = a' a \ast x = 1a' x = x$

So $a^{-1} b \in \text{stab}(x)$ implying $a\ast x = b\ast x$. Therefore $f$ is injective.

Finally, $f$ is surjective because

$$\text{orb}(x) = \{g \ast x : g \in G\} = \text{im}(f)$$
Group Actions Cont.

Class equations. Let $G$ be a finite group and let $G$ act on itself via conjugation. Let $g_1, g_2, \ldots, g_r$ be representatives of the conjugacy classes of $G$ and assume that we order the $g_i$ so that if $i > k$, then $g_i \in Z(G)$.

Since the conjugacy class partition $G$, we have

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

We can simplify the sum further in two ways:

1. $|\text{ord}_G(g_i)| = 1$ if $g_i \in Z(G)$
2. $|\text{ord}_G(g_i)| = |G|/|\text{stab}_G(g_i)| = [G : C_G(g_i)]$ by orbit-stabilizer theorem.

Therefore we have:

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

The significance 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 $a \geq 1$. This is a $p$-group if it has a power of $p$ many elements. Note that every subgroup 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 $g_1, g_2, \ldots, g_k$ 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 $1 = |Z(G)| = 1|G| - \sum_{i=1}^{k} [G : C_G(g_i)]$.

Hence $|Z(G)| > 1$. Q.E.D.

---

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

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

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

Step 1: We may assume $\sigma$ is a $k$-cycle.
Write $\sigma = y_1y_2 \cdots y_m$ as a product of disjoint cycles. Then

$\tau \sigma \tau^{-1} = \tau y_1y_2 \cdots y_m \tau^{-1}$

$= \tau y_1 \tau y_2 \tau^{-1} \cdots \tau y_{m-1} \tau \tau^{-1} \tau y_m \tau^{-1}$

Therefore if $\tau y_i \tau^{-1}$ 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 $\sigma$.

**Step 2**: We may assume $\tau$ is a transposition.

Write $\tau = s_1s_2 \cdots s_k$ as a product of transpositions. Then

$\tau \sigma \tau^{-1} = s_1s_2 \cdots s_k \sigma \sigma^{-1} s_k \cdots s_2 s_1$

Therefore $s_1s_2 \cdots s_k \sigma \sigma^{-1}$ has same cycle type as $\sigma$.

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

$s_1(s_2 \cdots s_k \sigma s_{k-1} \cdots s_2) \sigma^{-1}$ has same cycle type as $s_2 \sigma s_{k-1} \cdots s_2$

Which, since the $s_i$ are all transpositions, is true if $s_0 \sigma$ has same same cycle type as $\sigma$ for transpositions $s_i$.

**Step 3**: Let $\sigma = (a_1a_2 \cdots a_k)$ be a $k$-cycle and $\tau = (i\ i)$ be a transposition. Then $\tau \sigma \tau^{-1}$ is a $k$-cycle.
Within step 3 there are 3 cases.

Case 1: \( a_k \neq i \) or \( j \neq l \). Then \( a \) and \( i \) are disjoint, so

\[ \sigma \circ \sigma' = (ij) (a_1 a_2 \ldots a_k) C_{ij} = (ij) (C_i (a_1 \ldots a_k) = a_i - a_k = 0 \]

so \( \sigma \circ \sigma' = 1 \), a k-cycle.

Case 2: \( i \leq \ell \leq j \) for some \( \ell \). We may assume \( i \) and \( j \) both appear in \( \{a_1, a_2, \ldots, a_k\} \). Then after reordering, we may assume \( a_l = i \) and \( a_{l+1} = j \) for some \( l > 1 \).

Then

\[ \sigma \circ \sigma' = (ij) (i a_2 \ldots a_{l-1} a_{l+1} \ldots a_k (ij)) \]

\[ = (i a_2 \ldots a_{l+1} \ldots a_k a_{l+2} \ldots a_{k-1} a_l) \]

a k-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

\[ \sigma \circ \sigma' = (ij) (i a_2 \ldots a_k (ij)) \]

\[ = (j a_2 \ldots a_{k-1} a_k) \]

a k-cycle

We've shown that conjugation does not change the cycle type. To finish we need to show that if \( \sigma, \ell \in \text{Sym}(n) \) have the same cycle type, then \( \ell \in \text{Sym}(n) \) such that \( \sigma \circ \ell = \tau \).
Similarly to the previous step, we may reduce to the case when \( \sigma \) and \( \tau \) are k-cycles. Let \( \sigma = (a_1, a_2, \ldots, a_k) \), \( \tau = (b_1, b_2, \ldots, b_k) \).

Define \( \delta \) in the following way:

1. On \( a_1, a_2, \ldots, a_k \), define \( \delta(a_i) = b_i \).
2. Observe that both sets \( \{1, 2, \ldots, n\} \setminus \{a_1, a_2, \ldots, a_k\} \) and \( \{b_1, b_2, \ldots, b_k\} \) have cardinality \( n-k \). Let \( \delta \) be any bijection from \( S_i \) to \( S_k \).

Then we have, for \( i = 1, \ldots, k \),

\[
\delta \circ \delta'(b_i) = \delta \circ \delta(a_i) = \delta(a_{\sigma(i)}) = b_{\tau(i)}
\]

and if \( e \in S_j \), then \( \delta'(e) \in S_i \) so \( \delta'(e) \in S_j \) and \( \delta(\delta'(e)) = \delta'(e) \). Hence

\[
\delta \circ \delta'(e) = \delta \circ \delta'(\delta'(e)) = \delta(\delta'(e)) = e
\]

Therefore \( \delta \circ \delta' = \text{id} \). \( \Box \)

Con: \( \mathbb{Z}(\text{Sym}(n)) = \{ \text{id} \} \) if \( n > 2 \).

**Proof:**

Let \( \sigma \in \text{Sym}(n) \) be such that \( \sigma \neq \text{id} \). Then if \( \sigma \) is a transposition, since \( n > 2 \) there exists another transposition in \( \text{Sym}(n) \) so \( \sigma \) is conjugate to another element of \( \text{Sym}(n) \). If \( \sigma \) is not a transposition, then \( \sigma \) is a product of disjoint cycles, and since \( n > 2 \), there exists another cycle disjoint from \( \sigma \) in \( \text{Sym}(n) \) so \( \sigma \) is conjugate to another element of \( \text{Sym}(n) \).
* BACK TO WHAT IS IN LECTURE *

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

**Proof:** $G/Z(G)$ cyclic means $\exists x \in G$ such that $G/Z(G) = \langle x \rangle_{Z(G)}$.

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

Then we have

$$ab = x^k c_1 x^l c_2$$

$$= x^{k+l} c_1 c_2$$

because $c_1 \in Z(G)$

$$= x^{k+l} c_2 c_1$$

because $c_2 \in Z(G)$

$$= x^{k+l} x^{k+l}$$

because $x^{k+l} = x^{l+k} = x^{l+k}$ and $c_2 \in Z(G)$

$$= x^{2k+l}$$

so $G$ is abelian. \(\square\)

**Cor.** Assume that $p$ is a prime and that $G$ is a group of order $p^2$. Then $G$ is abelian.

**Proof:** By previous theorem $\mathbb{Z}/p^2 \mathbb{Z}$, so $|\mathbb{Z}/p^2 \mathbb{Z}| = p$ 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 $R$ be a set of representatives for the orbits of $G$ in $X$. Then since the orbits partition $X$, we have

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

By the orbit-stabilizer theorem, we have

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

Now observe that $x \in X^G$ iff $|\text{orb}(x)| = 1$ iff $\text{stab}(x) = G$. Hence we have
\[ |X| = \sum_{x \in R} 1 + \sum_{x \in R} |G/\text{stab}(x)| \]

Since \( G \) is a \( p \)-group and \( \text{stab}(x) \neq G \), \( p \) divides all two terms in the second sum.

\[ = |X^G| + \text{some number divisible by } p \]

\[ \equiv |X^G| \mod p. \]

Thus (Cauchy's Theorem): 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 \( p \).

**Proof:** Consider the set

\[ X = \left\{ (x_1, x_2, \ldots, x_p) \in G \times G \times \cdots \times G : x_1 x_2 \cdots x_p = 1 \right\} \]

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

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

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

\[ \ast : \mathbb{Z}/p \mathbb{Z} \times X \rightarrow X \]

\[ i \ast (x_1, x_2, \ldots, x_p) = (x_i x_1 x_2 \cdots x_p) (x_1, x_2, \ldots, x_i) \]

where \( i \) is the standard representative of \( i \mod p \).
We show that \( T \times (x_1 \cdots x_p) = (x_1, x_1 + 1, x_2, x_2 + 1, \ldots, x_i) \) is indeed an element of \( X \):

\[
X_{x_1} x_{x_2} \cdots x_{x_i} x_{x_i} = (x_1 x_2 \cdots x_i)^{-1} (x_1, x_2, \ldots, x_i) x_1 \cdots x_{x_i} x_{x_i} \cdots x_i
\]

\[
= (x_1, x_2, \ldots, x_i)^{-1} (x_1, x_2, \ldots, x_i) (x_1, x_2, \ldots, x_i)
\]

\[
= (x_1, x_2, \ldots, x_i)
\]

\[= 1\]

Now observe what the fixed points of the action are:

\[
X = \{ (x, y, z) \in \mathbb{Z}^3 : x^2 = 1 \}
\]

Since any element fixed by \( \mathbb{Z}/p\mathbb{Z} \) must have the same element of \( G \) in every slot, we know that \( X \neq \emptyset \) since \( 1^p = 1 \), so \((1,1,1) \in X\). 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 \( g \in G \) \((x_1, x_2, \ldots, x_i) \in X^{\mathbb{Z}/p\mathbb{Z}} \) be such that \((x_1, x_i-1) \neq (1,1,1)\). Then \( x_i = 0 \), \( x_i = 1 \) and \( x_i \neq 1 \). Hence \( o(1) = 1 \) and \( o(x_1) = p \).

Therefore \( o(x_1) = p\). \( \square \)