Group action

- G gp. X set. An action of G on X is a map
$$G\times X \to X, \quad (g,x) \mapsto gx$$
s.t. (1) $1x = x \quad \forall x \in X$

(2) $(g_1 g_2)x = g_1(g_2 x) \quad \forall x \in X$ and $g_1, g_2 \in G$.

We may informally denote it by $G \curvearrowright X$

Prop. An action of G on X is equivalent to a gp hom
$$\rho: G \to S_X, \text{ where } S_X \text{ is the gp of permutation on } X.$$

Pf. Given a gp action $m: G\times X \to X$,

we define $\rho(g): X \to X$ by $x \mapsto g\cdot x$

Check $\rho(g)$ is bijective (use the fact that g has inverse)

Then $\rho(g) \in S_X$

Now by (2) of def of G-action,
$$\rho(g_1 g_2)(x) = \rho(g_1)(\rho(g_2)(x)), \quad \forall x \in X$$

So $\rho(g_1 g_2) = \rho(g_1)\circ\rho(g_2)$. Thus ρ is a gp hom.

On the other hand, given $\rho: G \to S_X$, define
$$m: G\times X \to X \quad \text{by} \quad (g,x) \mapsto \rho(g)(x).$$

Then (1) $1\cdot x = \rho(1)\cdot x = id_X(x) = x. \quad \forall x \in X.$

(2) $(g_1 g_2)\cdot x = \rho(g_1 g_2)(x) = \rho(g_1)(\rho(g_2)x) = g_1(g_2 x).$ $\square$

Example. (1) The trivial action, $g \cdot x = x \quad \forall g \in G, x \in X$.

(2) $S_n \circlearrowright \{1, \cdots, n\}$ as permutations

(3) $D_n \circlearrowright$ regular n-gon as symmetries

(4) $GL_n(F) \circlearrowright F^n$.

(5) $G \circlearrowright G$ left action $\quad (g, x) \mapsto gx$

(6) $G \circlearrowright G$ right action $\quad (g, x) \mapsto xg^{-1}$ (check why g^{-1}).

(7) $G \circlearrowright G$ conjugation action $\quad (g, x) \mapsto gxg^{-1}$

Th (Cayley) Every group is isomorphic to a group of permutations.

In particular, every finite gp is isomorphic to a subgp of S_n for some n.

Rmk. Slogan: groups are symmetries.

Pf. Consider the left action $G \circlearrowright G$, $(g, x) \mapsto gx$.

This gives a gp hom $\rho: G \to S_G$

where $\rho(g) \in S_G$ is defined by $\rho(g)x = gx$.

Check that ρ is injective. (Hence G is a subgp of S_G)

If $\rho(g) = id_G$, then $\rho(g) \cdot 1 = 1$. But $\rho(g) \cdot 1 = g1 = g$.

So $g = 1$. $\square$

Def. A G-action on X is faithful if $\rho: G \to S_X$ is injective

transitive if $\forall x_1, x_2 \in X, \exists g$ s.t. $gx_1 = x_2$

Eg. $S_n \curvearrowright \{1, \cdots, n\}$ faithful and trans.

$Gl_n(F) \curvearrowright F^n$ is faithful but not transitive.

Left and right G action on G are faithful and trans.

Conj action is faithful iff $Z(G) = \{1\}$

transitive iff $G = \{1\}$

Def. let $g \in G$, define $X^g = \{x \in X \mid gx = x\}$

This is the subset of X fixed by g.

$X^G := \bigcap_{g \in G} X^g = \{x \in X \mid g \cdot x = x \ \forall g \in G\}$ is the set of fixed pt of the G-action.

Eg. $S_n \curvearrowright \{1, \cdots, n\}$. fixed pt set $= \emptyset$.

For $G \curvearrowright G$ conjugation, $G^G = Z(G)$.

Def. $G_x = \{g \in G \mid gx = x\} < G$ is called the stabilizer (or isotropy subgp) of $x \in X$.

Check. G_x is a subgp.

Eg. For conjugation action of G,

$G_x = Z_G(x)$ is the centralizer of $x \in G$.

Def. $G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X$ is the orbit of x

Rmk. G acts on X transitively iff # orbits $= 1$

Prop. $|G\cdot x| = [G : G_x]$

Pf. Define a map $f: G/G_x \to G\cdot x$

$$gG_x \mapsto g\cdot x.$$

Check
- well-defined
- surj
- inj

$\square$

Cor. If $|X|$ is finite and $G\cdot x_1, \cdots, G\cdot x_n$ are all the distinct orbits in X with $|G\cdot x_i| \geq 1$, then

$$|X| = |X^G| + \sum [G : G_{x_i}]. \qquad \text{(Class equation)}$$

Conjugation action: $G\times G \to G$, $(g, x) \mapsto gxg^{-1}$. $i: G \to \mathrm{Aut}(G)$

- The orbit of $x\in G$ is called a conjugacy class of x
- The stabilizer of x is called the centralizer of x.
- Each $i(g)$ is called an inner automorphism of G.

  $\mathrm{Im}(i) = \mathrm{Inn}(G)$.
- $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$
- $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ outer automorphism gp of G.

Eg. In S_n, two permutations are conj iff they have the same cycle type.

In S_4

Conj class	4-cycle	(3,1) cycle	(2,2)-cycle	(2,1,1)	(1,1,1,1)
size	6	8	3	6	1

Total $= 6+8+3+6+1 = 24 = 4!$

As an application of the class equation, we have

Cor. Let G be a finite gp. Then

$$|G| = |Z(G)| + \sum [G : Z_G(x_i)]$$

Prop. Let G be a finite p-gp (i.e. the order of G is a power of p), then $Z(G)$ is nontrivial.

Pf. $|G| = |Z(G)| + \sum [G : Z_G(x_i)]$.

Suppose that $|G| = p^r$. Then $Z_G(x_i)$ are proper subgp of G,

hence $|Z_G(x_i)| = p^{r_i}$ with $r_i < r$.

In particular, $p \mid [G : Z_G(x_i)]$ $\forall i$.

Thus $|Z(G)| = |G| - \sum [G : Z_G(x_i)]$ is divisible by p.

So $Z(G)$ is nontrivial $\square$

Cor. If $|G|=p^2$, then G is abelian

Pf. Since $Z(G)$ is nontrivial, $|Z(G)|=p$ or p^2.

If $|Z(G)|=p$, then $G/Z(G)\cong \mathbb{Z}_p$ is cyclic.

Then contradiction by Ex15, Q37. $\square$

Cor. If $|G|=p^3$, then G is abelian or

G is nonabelian with $Z(G)\cong\mathbb{Z}_p$, $G/Z(G)\cong\mathbb{Z}_p\times\mathbb{Z}_p$

Pf. ① $|Z(G)|=p^3$, then G is abelian

~~②~~ $|Z(G)|=p^2$, then G is cyclic, and G is abelian (contradiction)

③ $|Z(G)|=p$, then $|G/Z(G)|=p^2$. So $G/Z(G)$ is abelian

~~(i)~~ $G/Z(G)$ cyclic, then by Ex15, Q37, G abelian

(ii) $G/Z(G)\cong\mathbb{Z}_p\times\mathbb{Z}_p$ $\square$

Rmk. Nonabelian gps of order 8 are iso to D_4

or the quaternion gp $\{\pm1,\pm i,\pm j,\pm k\}$.

Def. A p-gp is a finite gp of order p^n for some n.

Prop. Let G be a p-gp and X be a finite G-set. Then

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

Pf. By class equation, $|X|=|X^G|+\Sigma[G:G_i]$, where G_i are proper subgp of G. So $[G : G_i] \equiv 0 \mod p$.

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

Cauchy's Thm. Let G be a finite gp with $p \mid |G|$. Then $\exists g \in G$ s.t. $|g| = p$.

Pf. Let $X = \{(g_1, \cdots, g_p) \mid g_i \in G,\ g_1 g_2 \cdots g_p = 1\}$.

Then $X \cong G^{p-1}$ (as g_p is determined by $g_1, \cdots, g_{p-1}$)

So $p \mid |X|$.

let $H = \langle \sigma \rangle \subseteq S_p$, where $\sigma = (1 2 \cdots p)$

H acts on X by $\sigma \cdot (g_1, \cdots, g_p) = (g_2, \cdots, g_p, g_1)$

Then by Prop. $0 \equiv |X| \equiv |X^H| \mod p$.

Note that $X^H = \{(g, \cdots, g) \mid g^p = 1\}$

Then $\exists g \neq 1$ s.t. $g^p = 1$ So $|g| = p$ $\square$

Def. Let $H < G$. Set $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ normalizer of H.

Rmk. • $N_G(H) = G$ iff $H \trianglelefteq G$.

• $N_G(H)$ is the largest subgp of G in which H is normal.

Lem. If H is a p-subgp of a finite gp G. Then
$$[N_G(H):H] \equiv [G:H] \mod p$$

Pf. Let $X = G/H$ and H acts on X on the left.

Check $X^H = N_G(H)/H$

So $[G:H] = |X| \equiv |X^H| = [N_G(H):H] \mod p.$

Cor. If H is a p-subgp of a finite gp G and $p \mid [G:H]$, then $N_G(H) \neq H$.

Pf. $[N_G(H):H] \equiv [G:H] \equiv 0 \mod p$. So $[N_G(H):H] \neq 1$ $\square$

1st Sylow Th. Let G be a gp of order $p^n m$ with $n \geq 1$ and $(p,m)=1$. Then G contains a subgp of order p^n

Moreover, (1) G contains a subgp H_i of order p^i for each $1 \leq i \leq n$

(2) Each H_i is normal in H_{i+1}.

Pf. By Cauchy Th, G contains a subgp H_1 of order p.

Suppose that H_i is defined. (for some $i<n$). Then by above Cor.

$p \mid [N_G(H_i):H_i]$. So by Cauchy Th, $N_G(H_i)/H_i$ contains a subgp of order p. Thus $N_G(H_i)$ contains a subgp H_{i+1} s.t. $H_i \subseteq H_{i+1}$ and $|H_{i+1}/H_i| = p$.

Since $H_{i+1} \subseteq N_G(H_i)$, H_i is normal in H_{i+1}. $\square$

Cor. Any p-gp is solvable

Pf. By 1^{st} Sylow Th, we have a subnormal series with quotient gps iso to $\mathbb{Z}_p$. So G is solvable $\square$

Def. Let G be a finite gp of order $p^n m$ with $(p,m)=1$. A subgp of G is called a Sylow p-subgp if it is of order p^n.

1^{st} Sylow Th $\Rightarrow$ Sylow p-subgp always exists.

2^{nd} Sylow Th. If H is a p-subgp of G, and P is a Sylow p-subgp. Then $\exists\, g \in G$ st. $H < gPg^{-1}$.

In particular, any two Sylow p-subgp of G are conjugate.

Pf. Let $X = G/P$ and H acts on X on the left.

Then $|X^H| \equiv |X| = [G:P] \not\equiv 0 \mod p$. So $X^H \neq \phi$.

Note that $aP \in G/P$ is fixed by H iff $H < aPa^{-1}$.

So $\exists\, a \in G$, st. $H < aPa^{-1}$. $\square$

3^{rd} Sylow Th. Let n_p be the number of Sylow p-subgp of G.

Then $n_p \mid |G|$ and $n_p \equiv 1 \mod p$.

Pf. By 2^{nd} Sylow Th, $n_p = [G:N_G(P)]$ So $n_p \mid |G|$.

Now let $X = \{\text{Sylow p-subgp of } G\}$ with P acts by conjugation

Then $X^p = \{p\}$. So $|X| \equiv |X^p| = 1 \mod p$ $\square$

Application in number theory.

Wilson's Th. $(p-1)! \equiv -1 \mod p$

Pf. Let $G = S_p$. Then the Sylow p-subgps are of order p, and hence are subgp gen by p-cycles.

$\#$ p-cycles $= (p-1)!$

$\{p\text{-cycles}\} \xrightarrow{(p-1):1} \{\text{subgp of order } p\}$

as each subgp contains $(p-1)$ of p-cycles.

So $n_p = (p-2)!$

By 3rd Sylow Th, $(p-2)! \equiv 1 \mod p$.

So $(p-1)! \equiv (p-1) \equiv -1 \mod p$ $\square$