L12: Lagrange's Theorem

Lagrange's thm

Thm $|G/H| = \frac{|G|}{|H|}$

Def Let $G \times X \to X$ be a group action. We define

- $Gx := \{gx \mid g \in G\}$ the orbit of x
- $G\backslash X := \{Gx \subseteq X \mid x \in X\}$ the set of orbits / quotient

We say that G acts transitively if there is only one orbit.

Convention We could also define right actions $X \times G \to X$ and denote the quotient by G/X. However, given a right action $S_r : X \times G \to X$ we can define a left-action by $S_\ell(g, x) = S_r(x, g^{-1})$. Moreover $\underset{S_r}{G\backslash X} = \underset{S_\ell}{X/G}$. Exercise!

Thus we might write X/G for $G\backslash X$ in either case.

Prop G/H is the set of orbits of the action $H \circlearrowright G$ given by $h.g = gh^{-1}$.

Thm Let $G \circlearrowright X$ be a group action. Then X is the disjoint union of its orbits, i.e. $X = \bigcup_{Gx \in G\backslash X} Gx$ and $Gx_1 \cap Gx_2 \neq \emptyset \Rightarrow Gx_1 = Gx_2$.

In part, $|X| = \sum_{Gx \in G\backslash X} |Gx|$

Pf Let $x_0 \in X$, then $x_0 = e \cdot x_0 \in G \cdot x_0 \subseteq \bigcup_{Gx \in G\backslash X} G \cdot x$.

For the second part, suppose that $Gx_1 \cap Gx_2 \neq \emptyset$ i.e. $\exists\, g_1, g_2 \in G$ s.t. $g_1 x_1 = g_2 x_2$. Let us show that $Gx_1 \subseteq Gx_2$ (the other direction works the same). Let $gx_1 \in G$, we write

$$g x_1 = g g_1^{-1} g_1 x_1 = g g_1^{-1} g_2 x_2 \in G x_2. \qquad \square$$

Thm Let $H \leq G$ be a finite subgroup, then $|G/H| = \frac{|G|}{|H|}$.
In part. $|H|$ divides $|G|$ if $|G|$ is finite.

Pf Recall that $H \curvearrowright G$ and the orbit through g is given by gH.
We obtain $|G| = \sum_{gH \in G/H} |gH|$. But $m_g : H \to gH$ defines a bijection.

$$|G| = \sum_{gH \in G/H} |gH| = \sum_{gH \in G/H} |H| = |G/H| \cdot |H|$$

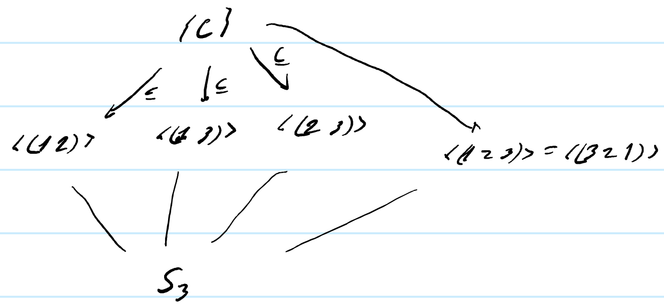
Def The number $|G/H|$ is called the __index__ of H in G.

Cor Let $x \in G$ be of order k, then $k \mid |G|$.
Pf Let $H = \langle x \rangle$ and recall that $|H| = |x|$.

Cor Let $x \in G$, then $x^{|G|} = e$

Cor If $|G| = p$ is prime, then G is cyclic, hence $G \cong \mathbb{Z}/p\mathbb{Z}$
Pf Let $e \neq x \in G$. Then $1 < |\langle x \rangle|$ divides $|G|$ hence $|\langle x \rangle| = |G|$
$\Rightarrow \langle x \rangle = G$.

Ex Subgroups of S_3
$|S_3| = 6$
$H \leq S_3 \Rightarrow |H| \in \{1, 2, 3, 6\}$



Claim There are no more subgroups.
Pf Let $H \leq G$. As $H \neq \{e\}$, $\exists\, e \neq h \in H$.
Hence $\langle h \rangle \subseteq H$. If $\langle h \rangle \neq H$
we get $|G| = |G/H| \cdot |H| = |G/H| \cdot \underbrace{|H/\langle h \rangle|}_{\neq 1} \cdot \underbrace{|\langle h \rangle|}_{\neq 1}$
$\Rightarrow |G/H| = 1$
$\Rightarrow G = H$.

Thm Let A be an abelian group and $p \mid |A|$ for a prime p. Then A has an element of order p.

Pf We proceed by induction on $|A|$.

Take any $e \neq a \in A$. If $p \mid |a|$ we take $x = a^{\frac{|a|}{p}}$, and obtain $|x| = p$ and are done. If $p \nmid |a|$, then

$$p \mid |A/\langle a \rangle| \qquad (\text{as } p \mid |A| = |\langle a \rangle| \; |A/\langle a \rangle| \,)$$

Since A is abelian, $\langle a \rangle \trianglelefteq A$ and hence $A/\langle a \rangle$ is an abelian group with $|A/\langle a \rangle| = |A|/|a| < |A|$. By the induction hypothesis we obtain $[y] \in A/\langle a \rangle$ s.t. $\cdot\ [y] \neq [e]$

$\cdot\ [y]^p = [e]$

From this we get $y \notin \langle y^p \rangle$ and hence $\langle y^p \rangle \neq \langle y \rangle$

But $|y^p| = \frac{|y|}{(p, |y|)}$ and thus $(p, |y|) \neq 1$ i.e. $p \mid |y|$ and we proceed as in the first step ($x = y^{\frac{|y|}{p}}$). $\square$