Lecture 23:

Last time: cosets $H \leq G$ subgroup

- we defined an equivalence relation on the group G:

$$a \sim_H b \iff \exists\, h \in H \text{ s.t. } ah = b.$$

- equivalence classes of this equivalence relation:

$$aH = \{ah \mid h \in H\}.$$

are called left-H-cosets.

- Similarly: $a \;{}_H\!\sim b \iff \exists\, h \in H$ st $ha = b$.

$Ha = \{ha \mid h \in H\}$ are (right H-cosets) the equivalence classes of ${}_H\!\sim$.

<u>Example:</u> In D_6, let $H = \langle r \rangle = \{1, r, r^2\}$.

left H-cosets are

$$1.H = \{1, r, r^2\}$$
$$\shortparallel \qquad\quad \shortparallel$$
$$rH = \{r, r^2, 1\}$$
$$\shortparallel \qquad\quad \shortparallel$$
$$r^2H = \{r^2, 1, r\}.$$

and

$$sH = \{s, sr, sr^2\}$$
$$\shortparallel$$
$$srH = \{sr, sr^2, s\}$$
$$\shortparallel$$
$$sr^2H = \{sr^2, s, sr\}.$$

So there are only two cosets!

$1.H = \{1, r, r^2\}$ and $sH = \{s, sr, sr^2\}$.

Remark: Since cosets are equivalence classes, they partition the group G into disjoint subsets.

Indeed, if $aH \cap bH \neq \emptyset$, then there is a $c \in aH \cap bH$, so $a \sim_H c$ and $c \sim_H b$

so $a \sim_H b$, so $aH = bH$.

they are equivalent, so they have the same equivalence class.

So the group is automatically a disjoint union

$$H \sqcup a_1H \sqcup a_2H \sqcup \cdots \sqcup a_kH.$$

"disjoint union".

Remark: Every coset has exactly the same number of elements, i.e. $|H|$.

proof: We want to show that there is a bijection of sets: $f: H \to aH$.

defined by $f(h) = ah$.

f is bijective since it has an inverse

$f^{-1}(h) = a^{-1}h$ so $f \circ f^{-1}(h) = aa^{-1}h = h$.

and $f^{-1} \circ f(h) = a^{-1}ah = h$.

Hence $\forall a$, $|H| = |aH|$ $\square$

Since $G = H \amalg a_1 H \amalg \ldots \amalg a_k H$.

Then: $|G| = |H| + |a_1 H| + \ldots + |a_k H|$

$= |H| + |H| + \ldots + |H|$

$= k|H|$. so $|H| \,\big|\, |G|$

We just proved:

<u>Theorem</u>: (Lagrange's Theorem) Let H be a subgroup of a finite group G.

Then $|H|$ divides $|G|$.

<u>Corollary</u>: Every group of prime order is cyclic (and therefore isomorphic to $\mathbb{Z}/p\mathbb{Z}$)

<u>proof</u>: If $|G| = p$, then G cannot have subgroups of order $\neq 1$ or $\neq p$. (by Lagrange's theorem)

trivial whole group.

So if $g \in G$ $g \neq e$, then $\langle g \rangle = G$.

$\square$

<u>Corollary</u>: The order of every $g \in G$ divides $|G|$.

<u>proof</u>: $\underset{|g|}{\overset{\shortparallel}{|\langle g \rangle|}} \,\big|\, |G|$ by Lagrange's Theorem

$\square$

Exercise: find an element a and subgroup H in a group G st $aH \neq Ha$.

first try: we know that abelian groups won't work since $ah = ha$ $\forall a, h$, so

$$aH = Ha.$$

Let's try D_6, $H = \{1, r, r^2\}$.

we know that sH and Hs will both be the remaining coset containing three elements.

So this doesn't work.

Try: $G = D_6$, $H = \{1, s\}$, $a = r$.