Last time • A homomorphism $f: G \to H$ is an isomorphism of groups $\Leftrightarrow \exists$ a homomorphism $k: H \to G$ so that $f \circ k = id_H$, $k \circ f = id_G$.

• The kernel of a homomorphism $f: G \to H$ is

$$\ker f = \{ g \in G \mid f(g) = e_H \}$$

Proved For a homomorphism $f: G \to H$

$f(a) = f(b) \Leftrightarrow ab^{-1} \in \ker f$

Hence f is 1-1 $\Leftrightarrow \ker f = \{e\}$.

Def A subgroup N of a group G is **normal** if $\forall g \in G \ \forall n \in N$ $gng^{-1} \in N$.

"Ex" If G is **abelian** (ie $ab = ba \ \forall a, b \in G$) then any subgroup of G is normal.

Proof: homework.

Non Ex $G = S_3$ $H = \langle (12) \rangle = \{e, (12)\}$ is **not** normal.

Reason $(13)(12)(13)^{-1} = (13)(12)(13) = (1)(23) \notin H$.

Ex $K = \langle (123) \rangle = \{e, (123), (132)\}$ **is** normal in S_3.

Check it! Hint: $\sigma (123) \sigma^{-1} = (\sigma(1) \ \sigma(2) \ \sigma(3))$

Lemma 12.5 Let $f: G \to H$ be a homomorphism. Then $\ker f$ is a normal subgroup of G.

Proof (i) $\forall a, b \in \ker f$

$f(ab^{-1}) = f(a)(f(b))^{-1} = e_H \cdot e_H^{-1} = e_H$

$\Rightarrow ab^{-1} \in \ker f$. $\Rightarrow \ker f$ is a subgroup.

(ii) $\forall g \in G \ \forall a \in \ker f$

$f(gag^{-1}) = f(g) f(a) (f(g))^{-1} = f(g) e_H (f(g))^{-1} = e_H$

$\Rightarrow gag^{-1} \in \ker f$.

Cosets

Proposition 13.1 Let H be a subgroup of a group G. The relation $\sim$ on G defined by

$$a \sim b \iff ab^{-1} = h \text{ for some } h \in H$$

(h depends on a, b)

is an equivalence relation.

Proof (i) $\forall a \in G \quad aa^{-1} = e_G \in H$ since H is a subgroup

(ii) If $a \sim b$, there is $h \in H$ s.t. $ab^{-1} = h$.

Since H is a subgroup $H \ni h^{-1} = (ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$

$\Rightarrow b \sim a$.

(iii) Suppose $a \sim b$ and $b \sim c$. Then $\exists h_1, h_2 \in H$ so that

$ab^{-1} = h_1$, $bc^{-1} = h_2$. $\Rightarrow cH \ni h_1 h_2 = ab^{-1}bc^{-1} = ac^{-1}$.

$\Rightarrow a \sim c$.

Def The right cosets of H are the equivalence classes of the relation $\sim$ defined above: for $a \in G$

$$[a] = \{b \mid b \sim a\} = \{b \mid b a^{-1} = h \text{ for some } h \in H\}$$
$$= \{b \mid b = ha \text{ for some } h \in H\}$$
$$= \{ha \mid h \in H\} \equiv Ha.$$

Note Equivalence classes form a partition of G: And indeed

$a \in Ha$ (since $a = e_G \cdot a$)

and $Ha \cap Hb \neq \emptyset \iff Ha = Hb \iff a = hb$ for some $h \in H$.

Ex $G = \mathbb{Z}$, $H = n\mathbb{Z}$

$[k] = n\mathbb{Z} + k$

Definition $H \backslash G = \{Hg \mid g \in G\}$ = the set of right cosets of H

Ex $n\mathbb{Z} \backslash \mathbb{Z} = \{n\mathbb{Z} + k \mid k \in \mathbb{Z}\} = \mathbb{Z}_n$

Similarly the relation $\sim$ on G defined by

$$a \sim b \iff a^{-1}b \in H \iff b = ah \text{ for some } h \in H$$

is an equivalence relation.

The corresponding equivalence classes are the <u>left</u> cosets of H

$$[a] = \{ah \mid h \in H\} = aH$$

$G/H := \{aH \mid a \in G\}$ the set of <u>left</u> cosets of G.

<u>Notation</u> For a finite set X, $|X| = \#$ of elements of X

<u>Lagrange's theorem</u> Let H be a subgroup of a <u>finite</u> group G

Then

$$|G/H| \cdot |H| = |G|.$$

<u>Ex</u> $G = S_3$ $\quad H = \langle (123) \rangle = \{e, (123), (132)\}$.

$H = eH$ is a coset of H

$(12)H = \{(12), (12)(123), (12)(132)\}$

$= \{(12), (32), (13)\}$

$G/H = \{H, (12)H\}$

And $|S_3| = 6 = 2 \cdot 3 = |G/H| \cdot |H|$

<u>Proof of Lagrange's theorem</u> For every $a \in G$ we have a map

$$L_a : H \to aH, \quad L_a(h) = ah.$$

L_a is invertible. The inverse is $L_a^{-1}(x) := a^{-1}x$.

(<u>Check</u> $L_a^{-1} L_a(h) = a^{-1}ah = h$, $L_a(L_a^{-1}(x)) = a(a^{-1}x) = x$)

$\Rightarrow |aH| = |H|$ for all $a \in G$.

Now the distinct cosets of H partition G:

$$G = eH \cup a_1 H \cup \dots \cup a_{k-1} H \qquad eH, a_1 H, \dots, a_{k-1} H = |G/H|$$

are all disjoint.

$$\Rightarrow |G| = |eH| + |a_1 H| + \dots + |a_{k-1} H| = |H| + \dots + |H|$$

$\Rightarrow |G| = |G/H|\,|H|$.

Corollary The order $|H|$ of a subgroup H of a group G divides the order $|G|$ of G:

$$|H| \mid |G|.$$

Proof $|G| = |G/H|\,|H|$. □

Def The order of an element $g \in G$ is the order $|\langle g\rangle|$ of the subgroup $\langle g\rangle$ generated by g.

Remark We'll prove that if $|\langle g\rangle|$ is finite then

$$|\langle g\rangle| = \min\{n \in \mathbb{N} \mid g^n = e_G\}.$$

Corollary 2.5.9. Let G be a finite group. Then

$$\forall g \in G \qquad |\langle g\rangle| \mid |G|.$$

Proof Since G is finite, $\langle g\rangle$ is finite. By cor to Lagrange's theorem, $|\langle g\rangle| \mid |G|$.

Corollary 2.5.8 Suppose G is a finite group and $p = |G|$ is prime. Then (i) the only subgroups of G are G and $\{e\}$.

(ii) For any $g \in G$, $g \neq e$, $\langle g\rangle = G$

(iii) For any homomorphism $f: G \to H$ out of G either f is 1-1 or $f(g) = e_H \ \forall g \in G$.

Proof (i) If H is a subgroup of G then $|H| \mid p = |G|$

$\Rightarrow |H| = p$ (and then $H = G$) or $|H| = 1$ (and then $H = \{e\}$)

(ii) Since $g \neq e$, $\langle g\rangle \neq \{e\}$. (i) $\Rightarrow \langle g\rangle = G$.

(iii) $\ker f$ is either G (and then $f(g) = e \ \forall g$) or $\{e_G\}$ (and then f is 1-1.)