Previously in Math 103a

A subgroup $H \subseteq G$ is <u>normal</u> if $xH = Hx \ \forall x \in G$.

<u>Thm:</u> H normal $\Longrightarrow$ $G/H = \{aH : a \in G\}$ is a group with multiplication given by

$$(aH)(bH) = (ab)H.$$

<u>Ex.</u> $G = D_4$, $\mathcal{H} = \{R_0, R_{180}\} = Z(D_4)$

We showed
$$R_0\mathcal{H} = R_{180}\mathcal{H} = \mathcal{H}$$
$$H\mathcal{H} = V\mathcal{H}$$
$$R_{90}\mathcal{H} = R_{270}\mathcal{H}$$
$$D\mathcal{H} = D'\mathcal{H}.$$

Cayley table for G/H can be constructed from the Cayley table for G by taking 4×4 blocks:

	R_0 R_{180}	R_{90} R_{270}	H V
R_0 R_{180}	R_0 R_{180} R_{180} R_0		
R_{90} R_{270}		R_{180} R_0 R_0 R_{180}	
H V		D D' D' D	R_0 R_{180} R_{180} R_0

This block represents product in G/H

Since every el't in $D_4/\mathcal{H}$ is of order 2,

$$D_4/\mathcal{H} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Ex. $G = U(32)$, $H = U_{16}(32) = \{1, 17\}$

$|G/H| = 8$ We know G/H is abelian.

Is $G/H \approx \mathbb{Z}_8$ or $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$?

$U(32) = \{1, 3, 5, 7, \ldots, 29, 31\}$

$|U(32)| = 2^5/2 = 16.$

Work by process of elimination to decide which one. Check orders of el'ts

$G/H = \{H, 3H, 5H, 7H, 9H, 11H, 15H\}$

$= \{\{1,17\}, \{3,19\}, \{5,21\}, \{7,23\}, \{9,25\}, \{11,27\}, \{13,29\}, \{15,31\}\}$

Pick 1, say $\{7, 23\}$ and check its order $\{7,23\}^2 = 49\{1,17\} = 17\{1,17\} = \{1,17\}$

so $7H$ is of order 2.

Try $5H$: $(5H)^2 = 25\{1,17\}$. Which of the cosets contains 25? $\boxed{9H}$ $\therefore (5H)^2 = 9H$

$\therefore$ $5H$ is <u>not</u> of order 2

$\therefore G/H \not\approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ (in which all nonidentity el'ts are of order 2)

$(9H)^2 = 81H = (81-64)H = 17H = H.$

$\therefore$ $9H$ is of order 2.

$\langle 9H \rangle$ & $\langle 7H \rangle$ are both subgroups of order 2. $\therefore$ G/H cannot be cyclic! (why?) By process of elimination, $\boxed{G/H \approx \mathbb{Z}_4 \oplus \mathbb{Z}_2.}$

$U(32)/U_{16}(32)$

Cauchy's Thm for finite abelian groups.

$|G| < \infty$, G abelian & $p \mid |G|$, p prime, Then $\exists$ $g \in G$ with $|g| = p$.

Lemma G any finite group, $|G| \geq 2$, not necessarily abelian. Then $\exists$ $a \in G$ with $|a|$ prime.

Pf. choose any $x \in G$, $x \neq e$. Then for any prime q for which $q \mid |x|$, there is an element $a \in \langle x \rangle \subset G$ of order q. (why?)

Pf of thm. By induction on $|G|$: OK for $|G| \leq 2$. Assume true for all G with

$|G| \le n-1$. Now suppose $|G| = n$ & $p|n$.
Need to find an element of order p.
By Lemma, $\exists$ $a \in G$, $|a|$ prime, say $|a| = q$.
If $q = p$ done. If not, consider the factor group $\boxed{\bar{G} = G/\langle a \rangle}$. $|\bar{G}| < n$.
also, $p \mid |\bar{G}|$, since $|\bar{G}| = n/q$ & $q \neq p$.

By inductive hypothesis, $\exists$ $x \in G$ s.t. $\boxed{|x\langle a \rangle| = p}$. This means $x^p \in \langle a \rangle$ or
$x^p = a^j$ some j $0 \le j < q$. If $x^p = e$, then done. If not, $(x^q)^p = a^{jq} = e$.
Since $x^q \neq e$, it follows that $|x^q| = p$. //

Note: we used 2 facts:

① G any group, $x \in G$, $x \neq e$, $x^p = e$, p prime.
then $|x| = p$.

② G any group, $x \in G$, $x \neq e$, p, q prime, $p \neq q$. If $x^p = e$, then $x^q \neq e$.

check these out!

Internal direct product.

Def. G is the (internal) direct product of normal subgroups H, K if

$$\boxed{G = HK \quad \text{with} \quad H \cap K = \{e\}}$$

Notation: $G = H \times K$.

Here $HK = \{hk : h \in H, k \in K\}$

Ex. $G = \mathbb{Z}_{10}$, $H = \{0, 5\}$, $K = \{0, 2, 4, 6, 8\}$

Check: $H \cap K = \{0\}$ ✓

Need to show if $n \in \mathbb{Z}_{10}$, then $n \in \{0,5\} + \{0,2,4,6,8\}$

n even ✓

n odd

$$\begin{cases} 5+0=5 \\ 5+2=7 \\ 5+4=9 \\ (5+6) \bmod 10 = 1 \\ (5+8) \bmod 10 = 3 \end{cases}$$

This proves $\mathbb{Z}_{10} = H \times K$.

Thm. $\boxed{H \times K \approx H \oplus K.}$

Ex: If $G = G_1 \oplus G_2$, then $\exists$ subgroups $\bar{G}_1, \bar{G}_2 \subset G$ with $G = \bar{G}_1 \times \bar{G}_2$. Just take

$$\boxed{\begin{aligned} \bar{G}_1 &= G_1 \oplus \{e_2\} \\ \bar{G}_2 &= \{e_1\} \oplus G_2 \end{aligned}}$$

$e_2 = \text{id in } G_2$

$e_1 = \text{id in } G_1$

VS

Pf of Thm: Lots of stuff to check.

Define an isomorphism

$H \oplus K \longrightarrow HK$ by

$\boxed{(h, k) \longmapsto h \cdot k}$ $\quad h \in H, k \in K.$

1-1? $\quad h'k' = hk \Longleftrightarrow \underset{H}{\underset{\uparrow}{h^{-1}h'}} = \underset{K}{\underset{\uparrow}{kk'^{-1}}}$

since $H \cap K = e$, $h^{-1}h' = e \Longrightarrow h = h'$

$kk'^{-1} = e \Longrightarrow k = k'$ ✓

Onto ✓

Preserves products.

$(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$

$(h_1, k_1) \longmapsto h_1k_1$

$(h_2, k_2) \longmapsto h_2k_2$

$\therefore \left.\begin{array}{l} (h_1, k_1)(h_2, k_2) \longmapsto (h_1k_1)(h_2k_2) \\ (h_1h_2, k_1k_2) \longrightarrow (h_1h_2)(k_1k_2) \end{array}\right\}$ same?

$h_1h_2k_1k_2 = h_1k_1h_2'k_2$ normality of K

$= h_1k_1'h_2k_2$ normality of H.

$\therefore h_1k_1h_2'k_2 = h_1k_1'h_2k_2$

$\Longrightarrow k_1h_2' = k_1'h_2$

$\Longrightarrow k_1 = k_1', \; h_2' = h_2$ why?