## Previously in Math 103a

**Def** Internal direct product:

$H, K$ $\boxed{\text{normal}}$ subgroups of $G$

$G = H \times K$ if $G = HK$ & $H \cap K = \{e\}$

We proved:

**Thm** $H \times K \approx H \oplus K$

More generally, $H_1 \times H_2 \times \cdots \times H_n \approx H_1 \oplus \cdots \oplus H_n$

**Ex:** $G_1 \oplus G_2 \approx \bar{G}_1 \times \bar{G}_2$

with $\bar{G}_1 = G_1 \oplus \langle e_2 \rangle$ $\quad \bar{G}_2 = \langle e_1 \rangle \oplus G_2$

$\bar{G}_1 \subset G_1 \oplus G_2$ $\quad \bar{G}_2 \subset G_1 \oplus G_2$

Caution: $G_1$ is not a subgroup of $G_1 \oplus G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$

these are ordered pairs

**Application**

**Thm** If $|G| = p^2$, $p$ prime, then either $\boxed{G \approx \mathbb{Z}_{p^2} \text{ or } G \approx \mathbb{Z}_p \oplus \mathbb{Z}_p}$. In particular $G$ is abelian.

**Pf** If $\exists\, x \in G$ with $|x| = p^2$, then $|\langle x \rangle| = p^2$

so $G$ is cyclic & $G \approx \mathbb{Z}_{p^2}$. Done!

so assume $|x| = p$ $\forall x \in G$, $x \neq e$.

Step 1. Claim that for any $a \in G$, the subgroup $\langle a \rangle$ is normal. Suppose not. Use criterion $bHb^{-1} \subset H$ $\forall b \in G$.

$\langle a \rangle$ not normal $\Rightarrow$ $\exists\, b \in G$ and $j$, $0 < j < p$

s.t. $ba^jb^{-1} \notin \langle a \rangle = \langle a^j \rangle$

a and $a^j$ generate same group

Replacing $a^j$ by $a$, have $\underbrace{\langle bab^{-1} \rangle \cap \langle a \rangle}$ $= \{e\}$

this is a subgroup of order dividing $p$

Note that $(bab^{-1})^k = ba^kb^{-1}$

As sets, $G = \langle bab^{-1} \rangle \langle a \rangle$

(This does not use normality)

Then $\exists\, j, k$ so that

$\boxed{b = ba^jb^{-1}a^k}$ which $\Rightarrow$ $e = a^jb^{-1}a^k$

solve for $b$ to find $b \in \langle a \rangle$

contradiction!

$\therefore$ all subgroups are normal.

Step 2. Take $x \in G$, $x \neq e$ and choose $y \in G$ with $y \notin \langle x \rangle$. Then

$\langle x \rangle$, $\langle y \rangle$ normal (step 1), $\langle x \rangle \cap \langle y \rangle = \{e\}$

$G = \langle x \rangle \langle y \rangle$ (by checking orders)

& by Thm, $G \approx \langle x \rangle \oplus \langle y \rangle \approx \mathbb{Z}_p \oplus \mathbb{Z}_p$.

**Ex** Any group of order 25 is abelian (since $25 = 5^2$).

---

Back to internal direct products

**Ex** Write $U(55)$ as an internal direct product of 2 subgroups.

**Ans.** $55 = 11 \times 5$, so $U(55) \approx U(11) \oplus U(5)$

by isom. $\underset{U(55)}{\overset{x}{\wedge}} \longmapsto (x \bmod 11,\ x \bmod 5)$

Recall subgroups $U_5(55) = \{x \in U(55) : x \bmod 5 = 1\}$

$U_{11}(55) = \{x \in U(55) : x \bmod 11 = 1\}$

$\boxed{U_5(55) \approx U(11) \oplus \{1\}}$

by $x \longmapsto (x \bmod 11, 1)$

& $\boxed{U_{11}(55) \approx U(5) \oplus \{1\}}$

by $x \longmapsto (1, x \bmod 5)$

$(x \bmod 11, 1)(1, x \bmod 5) = (x \bmod 11, x \bmod 5)$

$U(55) = U_5(55) \times U_{11}(55)$

# Homomorphisms: $\boxed{\text{Really important!}}$

Ex. 1. $\phi: \mathbb{Z} \to \mathbb{Z}_2$ given by $\boxed{\varphi(x) = x \bmod 2}$

preserves operations:

$$\varphi(n+m) = (n+m) \bmod 2$$
$$= (n \bmod 2 + m \bmod 2) \bmod 2$$
$$= \varphi(n) + \varphi(m) \text{ in } \mathbb{Z}_2.$$

This works with $\mathbb{Z}_2$ replaced by $\mathbb{Z}_n$, any $n$. $\phi(x) = x \bmod n$ preserves operations.

Def. Let $G$, $\bar{G}$ groups. A homomorphism from $G$ to $\bar{G}$ is a map $\varphi: G \to \bar{G}$ preserving operations

i.e. $\varphi(g_1 \underset{\text{mult in } G}{\cdot} g_2) = \varphi(g_1) \underset{\text{mult in } \bar{G}}{\cdot} \varphi(g_2)$

No assumption that $\varphi$ is 1-1 or onto.

An isomorphism is a homomorphism that is 1-1 & onto.

**Def** The kernel of a homomorphism $\varphi$ is $\boxed{\operatorname{Ker}\varphi = \{x \in G : \varphi(x) = e\}}$

In Ex 1, $\operatorname{Ker}\varphi = 2\mathbb{Z} = \langle 2 \rangle \subset \mathbb{Z}$

**Ex 2.** $\mathbb{R}^* =$ nonzero reals, $\mathbb{R}^*_+ =$ positive reals

operation = mult$^n$ in both

$\varphi : \mathbb{R}^* \longrightarrow \mathbb{R}^*_+$ is homormorphism

$\varphi(x) = |x|$ onto

$\operatorname{Ker}\varphi = \{\pm 1\}$

**Ex 3.** $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $G = \bar{G} = \mathbb{R}^2$ addition

$$\boxed{\varphi\begin{pmatrix} x \\ y \end{pmatrix} = A\begin{bmatrix} x \\ y \end{bmatrix}}$$

$$A\left(\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} x' \\ y' \end{bmatrix}\right) = A\begin{bmatrix} x \\ y \end{bmatrix} + A\begin{bmatrix} x' \\ y' \end{bmatrix}$$

$\varphi$ is a homomorphism $\mathbb{R}^2 \longrightarrow \mathbb{R}^2$

isomorphism $\Longleftrightarrow$ $\det A \neq 0$

Could replace $A$ by any $m \times n$ matrix $A$

$A : \mathbb{R}^n \longrightarrow \mathbb{R}^m$

WS

Observations about homomorphisms:

$$\varphi : G \longrightarrow \bar{G}$$

(a) $\boxed{\varphi(e) = \bar{e}}$ = identity in $\bar{G}$

(b) $|g|$ finite $\Longrightarrow$ $|\varphi(g)|$ divides $|g|$

Reason: If $g^n = e$, then $(\varphi(g))^n = \varphi(g^n)$
$= e$

(and then what?)

(c) $\ker \varphi$ is a subgroup of $G$.

(d) $\varphi(G)$ is a subgroup of $\bar{G}$.

(e) $\varphi(a) = \varphi(b) \Longleftrightarrow a^{-1}b \in \ker \varphi \Longleftrightarrow$
$a \operatorname{Ker} \varphi = b \operatorname{Ker} \varphi$