External Direct Products

If G, H groups, can form new group

$$G \oplus H = \{(g,h),\ g \in G,\ h \in H\}$$

group operation coordinate wise

Question: what is $\text{ord}(g,h)$?

Theorem: $\text{ord}(g,h) = \text{lcm}(\text{ord}(g), \text{ord}(h)) = L$

proof $(g,h)^L = (g^L, h^L) = (e,e)$

↑ identity elem. of G ↖ identity elem. of H

because $\text{ord}(g) \mid L$

and $\text{ord}(h) \mid L$

$\Rightarrow \text{ord}(g,h) \mid L$

assume $m < L = \operatorname{lcm}(\operatorname{ord}(g), \operatorname{ord}(h))$

$\Rightarrow$ $\operatorname{ord}(g) \nmid m$ or $\operatorname{ord}(h) \nmid m$

$\Rightarrow$ $g^m \neq e (= e_G)$ or $h^m \neq e (= e_H)$

$\Rightarrow$ $(g,h)^m = (g^m, h^m) \neq (e,e)$

$\Rightarrow$ $\operatorname{ord}(g,h) > m$.

$\Rightarrow$ claim.

Remark: Can be generalized to $G_1 \oplus G_2 \oplus \cdots \oplus G_n$

$$\operatorname{ord}(g_1, g_2 \cdots, g_n) = \operatorname{lcm}(\operatorname{ord}(g_1), \operatorname{ord}(g_2), \cdots, \operatorname{ord}(g_n))$$

(can be proved by induction on n)

Ex: what is $\operatorname{ord}(1,9,2)$, where $(1,9,2) \in \mathbb{Z}_6 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_5$

$\operatorname{ord}(1) = 6$ in $\mathbb{Z}_6$, $\operatorname{ord}(9) = \frac{12}{\gcd(9,12)} = \frac{12}{3} = 4$, $\operatorname{ord}(2) = 5$ in $\mathbb{Z}_5$.

$\operatorname{ord}(1,9,2) = \operatorname{lcm}(6,4,5) = 60$

Question: How many elements of order 7 in $\mathbb{Z}_{49} \oplus \mathbb{Z}_7$?

Sol. $\text{ord}(a,b) = 7 \Rightarrow \text{lcm}(\text{ord}(a), \text{ord}(b)) = 7$

3 cases:

- $\text{ord}(a) = 7$, $\text{ord}(b) = 1 \Rightarrow$ 6 elem: $b = 0$

  $\text{ord}(a) = 7 \Rightarrow \frac{49}{\gcd(a, 49)} = 7$

  $\Rightarrow a = 7, 14, 21, 28, 35, 42$

- $\text{ord}(a) = 1$ $\text{ord}(b) = 7 \Rightarrow$ 6 elem.

  $b = 1, 2, 3, 4, 5, 6$ $a = 0$

- $\text{ord}(a) = 7$, $\text{ord}(b) = 7 \Rightarrow$ 36 elem.

$6 + 6 + 36$

48

Question: when is $G \oplus H$ cyclic?

Theorem Assume G, H are finite cyclic groups

$G \oplus H$ cyclic $\iff$ $|G|$ and $|H|$ are relatively prime.

Proof. Let $|G| = n$, $|H| = m$ and $d = \gcd(n, m)$

"$\Rightarrow$" $G \oplus H = \langle (g, h) \rangle$ in particular:

$$\operatorname{ord}(g,h) = |G \oplus H| = mn$$

$$(g,h)^{mn/d} = \left((g^n)^{m/d}, (h^m)^{n/d} \right)$$

$$= (e^{m/d}, e^{n/d}) = (e, e) = \text{identity of } G \oplus H$$

$$\Rightarrow mn = \operatorname{ord}(g,h) \mid \frac{mn}{d}$$

↖ previous calculation.

$$\Rightarrow d = 1 \quad \checkmark$$

"$\Leftarrow$" $G = \langle g \rangle$, $H = \langle h \rangle$

$$\text{ord}(g,h) = \text{l.c.m.}(\text{ord}(g), \text{ord}(h))$$

$$= \frac{nm}{\gcd(n,m)} = nm \quad \text{by assumption.}$$

$\Rightarrow$ $\langle (g,h) \rangle$ has nm elements

$\cap$

$G \oplus H$ $\Rightarrow$ $\langle (g,h) \rangle = G \oplus H$ cyclic.

<u>Corollary:</u> $G_1, G_2 .. G_n$ cyclic groups

$\Rightarrow$ $G_1 \oplus G_2 \oplus .. \oplus G_n$ cyclic

$\Leftrightarrow$ $\gcd(|G_i|, |G_j|) = 1$

$\forall i \neq j$

e.g. $\mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$ is a cyclic group

$\Rightarrow \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_{3\cdot 5\cdot 7} = \mathbb{Z}_{105}$

Remark: If $\gcd(n,m) \neq 1$

$\mathbb{Z}_n \oplus \mathbb{Z}_m \not\cong \mathbb{Z}_{nm}$

new group.

Can show: $\mathbb{Z}_{27}$, $\mathbb{Z}_9 \oplus \mathbb{Z}_3$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$

are non isomorphic abelian groups of order 27.

Remark: If G, H abelian $\Rightarrow G \oplus H$ abelian

To prove groups are nonisomorphic observe.

$\mathbb{Z}_9 \oplus \mathbb{Z}_3$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ have no element of order 27

(follows from theorem about order of elem.) $\Rightarrow$ they are not isom. to $\mathbb{Z}_{27}$.

check: $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ has no elem. of order 9

$\Rightarrow \not\cong \mathbb{Z}_9 \oplus \mathbb{Z}_3$

Question: Given a group, is it a direct product of simpler groups?

Theorem $U(st) \cong U(s) \oplus U(t)$ **IF** $\gcd(s,t)=1$

(e.g. $U(15) \cong U(3) \oplus U(5)$
but $U(8) \not\cong U(2) \oplus U(4)$)

Proof need to find an isom.!

$\Phi: x \in U(st) \longmapsto (x \bmod s,\ x \bmod t)$

(e.g. $s=3, t=5$. $7 \in U(15) \mapsto (7 \bmod 3,\ 7 \bmod 5)$
$= (1,2)$

Operation preserving

$$\Phi(xy) = (xy \bmod s,\ xy \bmod t)$$

$$= (x \bmod s,\ x \bmod t) \cdot (y \bmod s,\ y \bmod t)$$

$$= \phi(x) \cdot \phi(y)$$ ✓

1-1:

assume $x \bmod s = 1$

$x \bmod t = 1$

(details later).

$\Rightarrow |\Phi(u(st))| = |u(st)| =$ $\phi(st) = \phi(s)\phi(t)$ (Euler function)

$\uparrow$ $\gcd(s,t) = 1$

$= |u(s) \oplus u(t)|$

$\uparrow$ $\phi(s)$ elem. $\uparrow$ $\phi(t)$ elem.

$\Rightarrow$ As $\Phi(u(st)) \subset u(s) \oplus u(t)$

it must be surjective.

Consequence: If $n = pq$ p, q prime

$$\Rightarrow \quad \mathcal{U}(n) \cong \mathcal{U}(p) \oplus \mathcal{U}(q)$$

$$\cong \mathbb{Z}(p-1) \oplus \mathbb{Z}(q-1)$$

↑ number theory

key idea for RSA encryption more later.