

Product gps

$$G_1, G_2 \text{ gps} \quad \underline{G_1 \times G_2} = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$$

can put a gp structure on this set

Multiplication is component-wise meaning

$$(g_1, g_2) \cdot (g'_1, g'_2) = (g_1 g'_1, g_2 g'_2).$$

This forms a gp.

Propⁿ Suppose $N = rs$ with $N \in \mathbb{Z}_{>0}$, $r, s \in \mathbb{Z}_{>0}$ with $\gcd(r, s) = 1$. Then

$$\underbrace{C_N}_{\text{cyclic gp of order } N} \cong C_r \times C_s.$$

Pf: Let x be a generator of C_N

y	$\xrightarrow{\quad}$	C_r
z	$\xrightarrow{\quad}$	C_s

Consider $\varphi: C_N \rightarrow C_r \times C_s$

$$\underbrace{x^k} \mapsto (y^k, z^k) \quad \text{for integers } k.$$

Q: Is this a well-defined gp homom?

Yes: We're taking $x \mapsto (y, z)$ and $(y, z)^N = 1$.

Yes: We're taking $x \mapsto (y, z)$ and $(y, z)^N = 1$.

$$(y, z)^N = (y^N, z^N) = (y^{rs}, z^{rs}) = (\underbrace{1}_b, \underbrace{1}_b) \text{ b/c } y^r = 1, z^s = 1.$$

Claim: φ is a bijection.

Pf: Both C_N and $C_r \times C_s$ have size $N = rs$.

$\Rightarrow$ Suffices to check that φ is an injection.

Suppose $x^k \in \ker(\varphi)$, so that $(y^k, z^k) = 1$ in $C_r \times C_s$.

Well, $y^k = 1$ in $C_r \Rightarrow r$ divides k

$z^k = 1$ in $C_s \Rightarrow s$ divides k .

$\Rightarrow r \cdot s$ divides k
b/c $\gcd(r, s) = 1$.

$$N | k \Rightarrow x^k = 1 \text{ in } C_N$$

$\Rightarrow \varphi$ is injective.

Rmk: What does $\varphi: \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ look like?

Select $x=1, y=1, z=1$

then $\boxed{\varphi(k) = (k, k)}$

More precisely: $k + N\mathbb{Z} \mapsto (k + r\mathbb{Z}, k + s\mathbb{Z})$.

φ is an isom. of abl^{ie} grps

Rmk: How to see directly that φ is a surjection?

Rmk: How to see directly that φ is a surjective?

In other words, given integers a, b want to find an integer k so that

$$k \equiv a \pmod{r}$$

$$k \equiv b \pmod{s}$$

} Frequently called
"Chinese Remainder
Theorem".

$$\text{I.e. } \varphi(k) = (a, b)$$

$$r, s \text{ rel prime} \Rightarrow \exists \text{ int. } u, v \text{ with } ur + vs = 1$$

$$vs = 1 - ur \equiv \begin{cases} 1 & \pmod{r} \\ 0 & \pmod{s} \end{cases}$$

$$ur = 1 - vs \equiv \begin{cases} 0 & \pmod{r} \\ 1 & \pmod{s} \end{cases}$$

$$\Rightarrow \underbrace{avs + bur}_{\equiv k} \equiv \begin{cases} a & \pmod{r} \\ b & \pmod{s} \end{cases} \quad \checkmark$$

Propⁿ . H, K subgrp of a gp G

• $f: H \times K \rightarrow G$ the map of sets

$$f(h, k) = h \cdot k$$

w/ image $HK = \{hk : h \in H, k \in K\}$.

a) f is injective $\Leftrightarrow H \cap K = \{1\}$

b) f is homom from $H \times K$ to G $\Leftrightarrow hk = kh \quad \forall h \in H, k \in K$.

b) f is homom from $H \times K$ to G $\Leftrightarrow h_k = k_h \quad \forall h \in H, k \in K$.

c) If H is normal in G then HK is a subgroup of G .

d) f is an isom from $(H \times K) \rightarrow G$ $\Leftrightarrow H \cap K = \{1\}$,
 $HK = G$, and H & K are normal subgroups of G .

Prf: a) $f(\underset{\substack{\parallel \\ h_1 k_1}}{h_1, k_1}) \stackrel{?}{=} f(\underset{\substack{\parallel \\ h_2 k_2}}{h_2, k_2})$

If $H \cap K \neq \{1\}$, then it contains $x \in H \cap K$.

$$f(1, 1) = f(x, x^{-1}) = 1.$$

Conversely, suppose $H \cap K = \{1\}$ and $h_1 k_1 = h_2 k_2$.

$$\Rightarrow \underset{\substack{\cap \\ H}}{h_2^{-1} h_1} = \underset{\substack{\cap \\ K}}{k_2 k_1^{-1}} \in H \cap K = \{1\}$$

$$h_2^{-1} h_1 = 1 \Rightarrow h_2 = h_1, \text{ similarly } k_1 = k_2$$

$$b) f(h_1, k_1) f(h_2, k_2) = f(h_1 h_2, k_1 k_2) \quad \forall h_1, h_2, k_1, k_2$$

$$\Leftrightarrow h_1 k_1 h_2 k_2 = h_1 h_2 k_1 k_2$$

$$\Leftrightarrow k_1 h_2 = h_2 k_1 \quad \forall h_2 \in H, k_1 \in K.$$

c) H normal.

$$\bullet (h_1 k_1) (h_2 k_2) = \underbrace{h_1}_{\in H} \underbrace{(k_1 h_2 k_1^{-1})}_{\in H} \underbrace{k_1 k_2}_{\in K}$$

$$\bullet (h_1 k_1)(h_2 k_2) = \underbrace{h_1}_{\in H} \underbrace{(k_1 h_2 k_1^{-1})}_{\in H} \underbrace{k_2}_{\in K}$$

$$\in H$$

$\Rightarrow HK$ is closed under product

$$\bullet (hk)^{-1} = k^{-1} h^{-1} = \underbrace{k^{-1} h^{-1} k}_{\in H} \cdot \underbrace{k^{-1}}_{\in K} \quad \checkmark$$

d) Suppose first $f: H \times K \rightarrow G$ is a gp isom.

Then w/ $H \cap K = \{1\}$, w/ $HK = G$, H, K normal subgps of $H \times K \Rightarrow H, K$ normal subgps of G .

Conversely, suppose $H \cap K = \{1\} \Rightarrow f$ inj
 $HK = G \Rightarrow f$ surj.

To see that $hk = kh \quad \forall k \in K, h \in H$ consider

OTone H: $\underbrace{h k h^{-1} k^{-1}}_{\in K} \in K \quad \text{b/c } K \text{ normal}$

OT other H: $\underbrace{h k h^{-1} k^{-1}}_{\in H} \in H \quad \text{b/c } H \text{ is normal}$

$$\Rightarrow h k h^{-1} k^{-1} \in H \cap K = \{1\}$$

$$\Rightarrow hk = kh \quad \forall h \in H, k \in K.$$

Consequence

Consequences

C_4 : cyclic gp of order 4

K_4 : Klein four gp $= \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\}$

Claim: C_4 & K_4 are the only gps of order 4, up to isom.

Pf: Suppose G gp of order 4.

• Lagrange $\Rightarrow$ order of any elt divides 4

• Case 1 $\exists x \in G$ of order 4. $\Rightarrow \langle x \rangle \cong C_4 \subseteq G$ & $C_4 = G$

• Case 2 All $g \in G$ satisfy $g^2 = 1$.

Suppose $x, y \in G$. $xyx^{-1}y^{-1} = xyxy = (xy)^2 = 1$
 $\text{b/c } x^2 = 1$
 $y^2 = 1$

$\Rightarrow xy = yx \Rightarrow G$ is abelian.

$\Rightarrow$ every subgroup is normal.

Consider $x \neq 1$ in G & $y \notin \{1, x\}$.

Then $H = \langle x \rangle = \{1, x\}$

$K = \langle y \rangle = \{1, y\}$

H, K normal, $H \cap K = \{1\}$

$\Rightarrow H \times K \rightarrow G$ injective b/c $H \cap K = \{1\}$
surjective b/c $|H \times K| = |G| = 4$

$\Rightarrow HK = G$.

So: Propⁿ above $\Rightarrow G \cong H \times K$. $\square$

$$\Rightarrow H \cap K = \{e\}.$$

So: Propⁿ above $\Rightarrow G \cong \underbrace{H \times K}_{\text{Klein 4-grp}}.$ $\square$