Internal products

Reminder: CAPE!

Way of breaking a group down into smaller pieces.
Can't always do this, but when you can, it's very useful.

Defn. G a group. If H & K are normal subgroups, $G = HK$, and $H \cap K = \{e\}$, then G is the internal direct product of H & K, written $G = H \times K$.

Thm. Suppose $G = H \times K$. Then the function $\varphi: H \oplus K \longrightarrow G$ given by $\varphi(h,k) = hk$ is an isomorphism.

Pf Sketch.

- φ is surjective $\rightsquigarrow G = HK$.
- Any element of H commutes with any element of K in G.

  If $h \in H$ & $k \in K$, we want to show $hk = kh$. That's equivalent to $hk(kh)^{-1} = e$, ie, $hkh^{-1}k^{-1} = e$.

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in KK^{-1} = K$$

(K is normal.)

$$hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in hH = H$$

(H is normal)

  So $hkh^{-1}k^{-1} \in H \cap K = \{e\}$.
- φ is injective homomorphism $\rightsquigarrow$ lemma we just proved. □

Thm. Suppose $\gcd(m,n) = 1$. Then:

- $U(mn) = U_m(mn) \times U_n(mn)$
- $U_m(mn) \approx U(n)$.

Recall: $U_k(n) = \{x \in U(n) \mid x \bmod k = 1\}$

Ex. $U(35) = U(5 \cdot 7)$.

$$U(35) = \{1, 2, 3, 4, 6, 8, \dots\}$$
$$U_5(35) = \{1, 6, 11, 16, \cancel{21}, 26, 31\}$$
$$U_7(35) = \{1, 8, \cancel{15}, 22, 29\}$$

We see that $U_5(35) \cap U_7(35) = \{1\}$.
$U(35)$ abelian, so any subgroup is normal.

$\{\ h \bmod 5 = 1,\ k \bmod 7 = 1,\ hk \bmod 35 = \ \hookrightarrow\ \}$

Pick anything in $U(35)$. Say 18. It should be true that $18 = hk$ for some $h \in U_5(35)$ and $k \in U_7(35)$. can take $h = 11$ & $k = 8$, since then

$$hk = 11 \cdot 8 \bmod 35 = 88 \bmod 35 = 18.$$

Nothing special about 18, will be able to do this for any elt of $U(35)$.

inspect proof of thm from chapter 8 to see why this true in general. Can also do a counting argument.

$U(35)$ isn't literally an external product

$$U_5(35) \oplus U_7(35) = \{(1,1), (6,8), (11,29), (11,8), \ldots\}$$

Not literally the same as $U(35)$, not the same elements, but it is isomorphic.

1. $\mathbb{Z}$ $H=\langle 5\rangle$ $K=\langle 7\rangle$. Is $\mathbb{Z} = H \times K$?

No, $H \cap K = \langle 5\rangle \cap \langle 7\rangle = \langle 35\rangle$. In particular, 35 is a nonzero element of $H \cap K$.

These subgroups are normal, because $\mathbb{Z}$ is abelian.

It is true that $\mathbb{Z} = H + K$

$\mathbb{Z}$ in an additive group!

because of Bezout's thm! since $\gcd(5,7)=1$, I can write 1 as a linear combination of 5 & 7.

$$1 = \underbrace{3\cdot 5}_{\in H} - \underbrace{2\cdot 7}_{\in K}$$

so far any other k, have

$$k = \underbrace{3k\cdot 5}_{\in H} + \underbrace{(-2k)\cdot 7}_{\in K}$$

so every integer is in $H+K$!

2. $G = \mathbb{Z}_4 \oplus \mathbb{Z}_{12}$

$H = \langle (2,2)\rangle = \{(0,0), (2,2), (0,4), (2,6), (0,8), (2,10)\}$

G/H $\quad |G| = 48$ $\quad |H| = 6$ $\quad |G/H| = 8$

By Lagrange, any elt of G/H has order 1, 2, 4, 8.

$2((1,1)+H) = (2,2)+H = H$ $\quad (1,1)+H$ has order 2.

$4((a,b)+H) = (4a,4b)+H = (0,4b)+H = H$

so any element has order ≤ 4. ruled out (A).

$2((3,4)+H) = (6,8)+H = (2,8)+H$

$4((3,4)+H) = (0,4)+H = H.$

so $(3,4)+H$ has order 4. so answer must be (B).