Quiz 2

$\mathbb{Z}_4 \oplus \mathbb{Z}_{10}$ have (possible orders in $\mathbb{Z}_4$ are $1,2,4$)
(possible orders in $\mathbb{Z}_{10}$ are $1,2,5,10$)

So possible orders in $\mathbb{Z}_4 \oplus \mathbb{Z}_{10}$ are $\text{lcm}(m,n)$ where $m \in \{1,2,4\}$
$n \in \{1,2,5,10\}$

8 will never be possible.

3. Of order 1: trivial group
2: cyc
3: cyc
4: $\mathbb{Z}_4$
5: Cyclic
6: S_3 is non-abelian D_3 - non abelian $S_3 \approx D_3$

4. $\mathbb{Z}_{13} \oplus \mathbb{Z}_{12}$ is cyclic b/c $\gcd(13,12)=1$

Group Homomorphism

Def'n: A homomorphism $\phi: G \to \overline{G}$ (where $G, \overline{G}$ are groups) is a map that preserves the group operation i.e. $\forall a,b \in G$, $\phi(ab) = \phi(a)\phi(b)$

Remark: This is exactly the same as the def of isomorphism except we don't require ϕ to be a bijection.

Def'n: The kernel of a homomorphism $\phi: G \to \overline{G}$ is denoted $\text{Ker}(\phi) = \{g \in G \mid \phi(g) = e\}$

Remark: if ϕ is an isomorphism, $\text{Ker}(\phi) = \{e\}$

Example: ① $\det: GL_n(\mathbb{R}) \to \mathbb{R}^*$
$\det(A) =$ determinant of A.

Since $\det(AB) = \det(A)\det(B)$
det is a homomorphism
$\text{Ker}(\det) = SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\}$

② $\phi: \mathbb{R}^* \to \mathbb{R}^*$
$\phi(x) = |x|$
$\text{Ker}(\phi) = \{\pm 1\}$

③ $\phi: \mathbb{Z} \to \mathbb{Z}_n$
$\phi(m) = m \pmod n$
$\text{Ker}(\phi) = n\mathbb{Z}$

Properties of homomorphisms

Let $\phi: G \to \overline{G}$ be a homomorphism.

(1) $\phi(e) = e$

(2). $\phi(g^n) = \phi(g)^n \quad \forall n \in \mathbb{Z}, g \in G$

(3). If $g \in G$, and $|g|$ is finite, then $|\phi(g)|$ is also finite and $|\phi(g)|$ divides $|g|$.
(4). $Ker(\phi) \leq G$
(5). $\phi(a) = \phi(b) \iff aKer(\phi) = bKer(\phi)$
(6). If $\phi(g) = g' \in \bar{G}$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = gKer(\phi)$
an inverse image

Proof of 5:
$\phi(a)=\phi(b) \iff \phi(a)\phi(b)^{-1} = e \iff \phi(a)\phi(b^{-1}) = e$
$\iff \phi(ab^{-1}) = e$
$\iff ab^{-1} \in Ker(\phi)$
$\iff aKer(\phi) = bKer(\phi)$

Behavior of subgroups under homomorphisms
Let $\phi: G \to \bar{G}$ be a homomorphism. and let $H \leq G$.
(1). $\phi(H) = \{\phi(h) \mid h \in H\} \leq \bar{G}$
(2). H is cyclic implies $\phi(H)$ is cyclic
(3). H is abelian, implies $\phi(H)$ is abelian
(4). $H \lhd G$, then $\phi(H) \lhd \phi(G)$
(5) Ignore
(6). If $|H|$ is finite, then $|\phi(H)|$ divides $|H|$
(7). If $\bar{K} < \bar{G}$, $\phi^{-1}(\bar{K}) = \{g \in G \mid \phi(g) \in \bar{K}\} \leq G$
(8). If $\bar{K} \lhd \bar{G}$, then $\phi^{-1}(\bar{K}) \lhd G$
(9). If ϕ is onto and $Ker(\phi) = \{e\}$, then ϕ is an isomorphism.

Proof of 9).
Proposition: If $\phi: G \to \bar{G}$ is a homomorphism, ϕ is one-to-one iff $Ker(\phi) = \{e\}$
Pf:
$\Rightarrow$ If ϕ is 1-1, $\phi(g) = e \Rightarrow g = e$ since $\phi(e) = e$
So $Ker(\phi) = \{e\}$

$\Leftarrow$ Suppose $Ker(\phi) = \{e\}$, and sps $\phi(a) = \phi(b)$ for some $a, b \in G$
By what we computed before, this is equivalent to $ab^{-1} \in Ker(\phi) = \{e\}$. So
$ab^{-1} = e$, i.e. $a = b$

$\blacksquare$

(8).
det: $GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$
Consider: $\bar{K} = \{\pm 1\} \leq \mathbb{R}^*$ ($\{\pm 1\} \lhd \mathbb{R}^*$)
Let $H = det^{-1}(\bar{K}) = \{A \in GL_n(\mathbb{R}) \mid det\, A = \pm 1\}$
So we know $H \leq GL_n(\mathbb{R})$. in fact, $H \lhd GL_n(\mathbb{R})$
example: Let $\bar{S} = \{2^n \mid n \in \mathbb{Z}\} \lhd \mathbb{R}^+$ Then $det^{-1}(\bar{S}) \lhd GL_n(\mathbb{R})$
$\qquad = \{A \in GL_n(\mathbb{R}) \mid det(A) = 2^n$ for some $n \in \mathbb{Z}\}$

Consider $\bar{K} = \{e\} \lhd \bar{G}$, then $\phi^{-1}(\{e\}) = Ker(\phi)$
So $Ker(\phi) \lhd G$.
Proposition: If $\phi: G \to \bar{G}$ is a homomorphism, then $Ker(\phi) \lhd G$
Proof: Let $x \in G$. We want to show $xKer(\phi)x^{-1} \subset Ker(\phi)$. So let $k \in Ker(\phi)$
So $xkx^{-1} \in xKer(\phi)x^{-1}$

Then $\phi(xkx^{-1}) = \phi(x)\underbrace{\phi(k)}_{e}\phi(x^{-1}) = \phi(xx^{-1}) = \phi(e) = e$

So $xkx^{-1} \in Ker(\phi)$

example:

(1). $\phi: S_n \to \{\pm 1\}$

$$\phi(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is even} \\ -1 & \sigma \text{ is odd} \end{cases}$$

ϕ is a homomorphism

$Ker(\phi) = A_n$

Therefore, we can conclude $A_n \lhd S_n$

(2). $\phi: D_n \to \{\pm 1\}$

$$\phi(x) = \begin{cases} +1 & \text{if } x \text{ is a rotation} \\ -1 & x \text{ is a reflection} \end{cases}$$

ϕ is a homomorphism

$Ker(\phi) = \{\text{all rotations in } D_n\}$

$\{\text{rotations}\} \lhd D_n$

(3). $\det: GL_n(\mathbb{R}) \to \mathbb{R}^*$

$Ker(\det) = SL_n(\mathbb{R})$

$SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$

Recall: From practice problems

"rotation rotation = rotation

rotation reflection = reflection

reflection reflection = rotation"

↓ Recall: $\phi(G) = \{\phi(g) \mid g \in G\}$ = "image of ϕ"

First Isomorphism Theorem

Let $\phi: G \to \overline{G}$ be a homomorphism, then define $\tilde{\phi}: G/Ker(\phi) \to \phi(G)$ by $\tilde{\phi}(g\,Ker(\phi)) = \phi(g)$

Then $\tilde{\phi}$ is an isomorphism.

Pf: First let's show that $\tilde{\phi}$ is well-defined. If $g_1 Ker(\phi) = g_2 Ker(\phi)$, then we need to show $\phi(g_1) = \phi(g_2)$.

Aside: To construct an ismorphism/homomorphism, ① write down a formula for a map. ② Check that the formula in ① is well-defined. ③ check it preserves the operation ④ Only for isomorphism $\to$ check the map is one-to-one and onto.

Let n be even.

Define: $\phi: \mathbb{Z}_n \to \{\pm\}$

by $$\phi(k) = \begin{cases} +1 & \text{if } k \text{ is even} \\ -1 & \text{odd} \end{cases}$$

We need to check that ϕ is well-defined.

So if $k = k'$ mod n, then k is even iff k' is even (because n is even)

So ϕ is well-defined.

Let n be odd $(n=3)$

Define $\phi(k) = \begin{cases} +1 & \text{if } k \text{ is even} \\ -1 & \text{odd} \end{cases}$

is ϕ well-defined?

No. because $1 \equiv 4 \bmod 3$

odd   even

So ϕ does not define a function.

Let n be even

Define $\phi : \mathbb{Z}_n \to \{\pm 1\}$ by $\phi(k) = \begin{cases} +1 & \text{if } k \text{ is even} \\ -1 & k \text{ is odd} \end{cases}$

we need to check that ϕ is well-defined

So if $k \equiv k' \bmod n$, then k is even iff k' is even (because n is even)

So ϕ is well-defined. ϕ defines a function.

Let n be odd

Define: $\phi : \mathbb{Z}_n \to \{\pm 1\}$

by $\phi(x) = \begin{cases} +1 & \text{if } r \text{ is even where } r \equiv k,\ 0 \le r < n \\ -1 & \text{odd where } r \equiv k,\ 0 \le r < n \end{cases}$

ϕ is well-defined, ϕ is not a homomorphism.

continue the proof:

But $g_1 \mathrm{Ker}(\phi) = g_2 \mathrm{Ker}(\phi) \iff g_1 g_2^{-1} \in \mathrm{Ker}(\phi)$

$\iff \phi(g_1 g_2^{-1}) = e$

$\iff \phi(g_1) = \phi(g_2)$

And $\bar{\phi}(g\mathrm{Ker}(\phi) h\mathrm{Ker}(\phi)) = \bar{\phi}(gh\mathrm{Ker}(\phi)) = \phi(gh) = \phi(g)\phi(h)$

$= \bar{\phi}(g\mathrm{Ker}(\phi))\bar{\phi}(h\mathrm{Ker}(\phi))$

So $\bar{\phi}$ is a homomorphism

For all $x \in \phi(G), \exists\ g \in G$ s.t. $x = \phi(g)$.

Moreover, $x = \bar{\phi}(g\mathrm{Ker}(\phi))$ So $\bar{\phi}$ is onto

Finally, we need to show $\bar{\phi}$ is 1-1.

Equivalently, that $\mathrm{Ker}(\bar{\phi}) = \{e\} = \{\mathrm{Ker}(\phi)\}$

Sps $\bar{\phi}(g\mathrm{Ker}(\phi)) = e$ i.e. $\phi(g) = e$

Then $g \in \mathrm{Ker}(\phi)$, so $g\mathrm{Ker}(\phi) = \mathrm{Ker}(\phi)$ $\blacksquare$

Cor: If $\phi : G \to \bar{G}$ is a homomorphism and $|G|$ is finite then $|\phi(G)|$ divides $|G|$.

Pf: By the First isomorphism, $G/\mathrm{ker}(\phi) \approx \phi(G)$, so $|\phi(G)| = |G| / |\mathrm{Ker}(\phi)|$ $\blacksquare$

Example :

① Let $\phi: \mathbb{Z} \to \mathbb{Z}_n$ be the homomorphism given by $\phi(k) = k \pmod n$

Then $\phi(\mathbb{Z}) = \mathbb{Z}_n$

But $Ker(\phi) = n\mathbb{Z}$ So $\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}_n$

② $det: GL_n(\mathbb{R}) \to \mathbb{R}^*$

So $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \approx \mathbb{R}^*$

③ $\phi: S_n \to \{\pm 1\}$

Then $S_n/A_n \approx \{\pm 1\}$

④ $\phi: \mathbb{R} \to S'$ $\quad (S' = \{z \in \mathbb{C}^* \mid |z| = 1\})$

$\phi(r) = \exp(2\pi i r)$

$\phi(\mathbb{R}) = S'$ But $Ker(\phi) = \mathbb{Z}$, So $\mathbb{R}/\mathbb{Z} \approx S'$.

Every normal subgroup is the kernel of some homomorphism.

Thm: Let G be a group, $N \lhd G$, define $\phi: G \to G/N$ by $\phi(g) = gN$. Then ϕ is a homomorphism

Then $Ker(\phi) = N$

Pf: If $g_1, g_2 \in G$, then $\phi(g_1 g_2) = g_1 g_2 N = g_1 N g_2 N = \phi(g_1)\phi(g_2)$

So ϕ is a homomorphism.

If $\phi(g) = e = N$, then $g \in N$. So $ker(\phi) = N$ (b/c $gN = N$ iff $g \in N$)

∎

THE FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS

Not Required

G : abelian finite gp. Then $G \approx \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \mathbb{Z}_{p_k^{n_k}}$

where p_i are primes, $n_i \geq 1$

And this representation is unique up to reordering the factors.

Sketch: Let G be finite abelian. Let $p \mid |G|$. By Cauchy's thm, $\exists x \in G$ s.t. $|x| = p$.

Ask: $\exists y \in G$ s.t. $y^p = x$.

If yes, $|y| = p^2$

Ask: $\exists z \in G$ s.t. $\dots z^p = y$

Then $|z| = p^3$

Sps $w \in G$, $|w| = p^n$ but $\nexists u$ s.t. $u^p = w$. Then $N = \langle w \rangle$. $N \lhd G$.