# Exam II Review

Shaoyun Yi

MATH 546/701I

University of South Carolina

Spring 2022

# Review

- A group isomorphism $\phi : (G_1, *) \to (G_2, \cdot)$
  - **Find**/**Verify** $\phi$: well-defined; 1-to-1 & onto; respects two operations
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1, n \in \mathbf{Z}$. e.g., $n = 0$ & $n = -1$
  - $o(a) = n \rightsquigarrow o(\phi(a)) = n$ & abelian (cyclic) $\rightsquigarrow$ abelian (cyclic)
- **Lagrange's Theorem** If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \,\big|\, n$.
  - The converse is false: e.g., No subgroup of order 6 in $A_4$
  - $|\langle a \rangle| = o(a) \,\big|\, n$ for any $a \in G$.
  - Any group of prime order is cyclic ($\rightsquigarrow$ abelian).
- Cayley's Theorem Every group is isomorphic to a permutation group.
  - **Cyclic group:** Infinite: $\cong \mathbf{Z}$ & Finite: $\cong \mathbf{Z}_n$ $\rightsquigarrow$ multiplicative $G$

    subgroups of $\mathbf{Z}$ & subgroups of $\mathbf{Z}_n$ $\dashrightarrow$ **subgroup diagram**

    $G$ finite abelian with exponent $N = \max\{o(a)\}$ $\rightsquigarrow$ $G$ cyclic $\Leftrightarrow N = |G|$

    $\mathbf{Z}_n^\times$ is not always cyclic.
  - **Dihedral group** $D_n, |D_n| = 2n$
  - **Alternating group** $A_n, |A_n| = n!/2$
- Product of two subgroups is not always a subgroup.

  If $h^{-1}kh \in K$ for all $h \in H, k \in K$, then $HK$ is a subgroup. $\rightsquigarrow$ $G$ abelian 🙂
- Direct product of (two $\rightsquigarrow$ $n$) groups: e.g., $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \cdots \mathbf{Z}_{p_m^{\alpha_m}} \rightsquigarrow \varphi(n)$

  The order of an element is the **lcm** of the orders of each component.

# Example 1

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group $G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} : m \neq 0 \right\}$ under matrix multiplication.

Define $\phi : G_1 \to G_2$ by $\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$. To show $\phi$ is an isomorphism:

well-defined: For $f_{m,b} \in G_1$, we have $\phi(f_{m,b}) \in G_2$ since $m \neq 0$.

For any $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$, to show $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$:

For any $x \in \mathbf{R}$, we have $f_{m_1,b_1} \circ f_{m_2,b_2}(x) = \cdots = m_1 m_2 x + (m_1 b_2 + b_1)$.

$\rightsquigarrow \phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1 m_2, m_1 b_2 + b_1}) = \begin{bmatrix} m_1 m_2 & m_1 b_2 + b_1 \\ 0 & 1 \end{bmatrix}$;

Also $\phi(f_{m_1,b_1})\phi(f_{m_2,b_2}) = \begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m_2 & b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_1 m_2 & m_1 b_2 + b_1 \\ 0 & 1 \end{bmatrix}$.

one-to-one: $\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = e_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \rightsquigarrow m = 1, b = 0$. To show $f_{1,0} = e_1$

$$f_{1,0} \circ f_{m,b}(x) = f_{1,0}(mx + b) = mx + b \overset{\checkmark}{=} f_{m,b}(x); \quad f_{m,b} \circ f_{1,0}(x) \overset{\checkmark}{=} f_{m,b}(x)$$

onto: It is obvious by definition of $\phi$. □

# Example 2

Let $G$ be an abelian group with subgroups $H$ and $K$.

$$\text{If } HK = G \text{ and } H \cap K = \{e\}, \text{ then } G \cong H \times K.$$

**Proof:** Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$ for all $(h,k) \in H \times K$.

i) well-defined: It is true since $HK = G$.

ii) $\phi$ preserves the products: For all $(h_1, k_1), (h_2, k_2) \in H \times K$ we have

$$\begin{aligned}\phi((h_1,k_1)(h_2,k_2)) &= \phi((h_1h_2, k_1k_2)) \\ &= h_1h_2k_1k_2 \\ &\overset{!}{=} h_1k_1h_2k_2 \\ &= \phi((h_1,k_1))\phi((h_2,k_2))\end{aligned}$$

iii) one-to-one: If $\phi((h,k)) = e$ for $(h,k) \in H \times K$, then we have $hk = e$.

$$hk = e \quad \rightsquigarrow h = k^{-1} \in H \cap K \quad \rightsquigarrow h = k = e.$$

Thus $\phi$ is one-to-one.

iv) onto: It is true since $HK = G$. □

# Example 3

Let $G$ be a finite abelian group, and let $n \in \mathbf{Z}^+$. Define a function

$$\phi : G \to G \text{ by } \phi(g) = g^n, \quad \text{for all } g \in G.$$

Then $\phi$ is an isomorphism if and only if $G$ has no non-identity element whose order is a divisor of $n$.

**Proof:** The well-definedness of $\phi$ is clear. [Why?]

i) $\phi$ preserves the products: For any $g, h \in G$, we have

$$\phi(gh) = (gh)^n \stackrel{!}{=} g^n h^n = \phi(g)\phi(h).$$

ii) one-to-one and onto: If $\phi$ is one-to-one, then $\phi$ is also onto. [Why?]

To show that $\phi$ is one-to-one. $\rightsquigarrow$ To show $\phi(g) = e \rightsquigarrow g = e$.

$$\phi(g) = g^n = e \rightsquigarrow g = e \qquad \Leftrightarrow \qquad o(g) \nmid n \text{ for all } g \neq e.$$

Thus $G$ has no non-identity element whose order is a divisor of $n$. □

# Example 4

Any cyclic group of even order $2n$ has exactly one element of order 2. $(\star)$

**Proof 1:** $\rightsquigarrow$ To show that $\mathbf{Z}_{2n}$ has exactly one element of order 2. [Why?]

If $o([x]_{2n}) = 2$ then $2[x]_{2n} = [0]_{2n}$, i.e., $2x \equiv 0 \pmod{2n}$. Thus

$x \equiv 0 \pmod{n}$ $\rightsquigarrow$ $x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$.

However, $x \neq [0]_{2n}$. [Why?] Thus $x = [n]_{2n}$. □

**Proof 2:** In $\mathbf{Z}_{2n}$, there is exactly one subgroup $H$ of order 2.

In particular, $H \cong \mathbf{Z}_2$ and $\mathbf{Z}_2$ has exactly one generator. □

**By $(\star)$, showing that $\mathbf{Z}_n^\times$ is not cyclic for some $n$ is much easier.**

Observe that $[-1]_n$ always has order 2 in $\mathbf{Z}_n^\times$ ($|\mathbf{Z}_n^\times|$ is even) for all $n \geq 3$.

$\mathbf{Z}_8^\times$ is not cyclic since $[3]_8$ is another element of order 2.

$\mathbf{Z}_{15}^\times$ is not cyclic since $[4]_{15}$ is another element of order 2.

$\mathbf{Z}_{21}^\times$ is not cyclic since $[8]_{21}$ is another element of order 2.

# Example 5

Let $H := \left\{ \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix} \middle| c \in \mathbf{Z}_p, d = \pm 1 \right\} \subseteq \mathrm{GL}_2(\mathbf{Z}_p)$. Then $H \cong D_p, p > 2$.

**Proof:** First, $H$ is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$. [Why?] And $|H| = 2p = |D_p|$.

Recall that $D_p = \{a^k, a^k b \mid 0 \le k < p\}$, where $a^p = e, b^2 = e, ba = a^{-1}b$.

Let

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in H \qquad \text{and} \qquad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in H.$$

Then $A^p = I_2, B^2 = I_2$ and $A^i \neq A^j B$ for $0 \le i, j < p$. Moreover,

$$BA = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = A^{-1}B.$$

Thus we can define $\phi : H \to D_p$ by $\phi(A) = a$ and $\phi(B) = b$.

From the above calculations, it is clear that $\phi$ is a group isomorphism. □

# Example 6

Recall that $D_n = \{a^k, a^k b \mid 0 \le k < n\}$, where $a^n = e, b^2 = e, ba = a^{-1}b$.

$$D_{12} \not\cong D_4 \times \mathbf{Z}_3$$

**Proof:** In $D_{12}$, we have $o(a^k) = 12/\gcd(k, 12)$. [Why?] Thus,

| $a^k$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^7$ | $a^8$ | $a^9$ | $a^{10}$ | $a^{11}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $o(a^k)$ | 1 | 12 | 6 | 4 | 3 | 12 | 2 | 12 | 3 | 4 | 6 | 12 |

**Q:** What about $a^k b$ for $0 \le k < n$? **A:** They all have the order 2. [Why?]

| $a^k b$ | $b$ | $ab$ | $a^2 b$ | $a^3 b$ | $a^4 b$ | $a^5 b$ | $a^6 b$ | $a^7 b$ | $a^8 b$ | $a^9 b$ | $a^{10} b$ | $a^{11} b$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| order | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |

$\rightsquigarrow$ There are only two elements of order 6 in $D_{12}$. ("6" is NOT the only choice. e.g., 2)

However, there are ten elements of order 6 in $D_4 \times \mathbf{Z}_3$:

- In $D_4$, the possible orders of elements are $1, 2, 4$. (with #'s $1, 5, 2$)
- In $\mathbf{Z}_3$, the possible orders of elements are $1, 3$. (with #'s $1, 2$)

$6 = \operatorname{lcm}[2, 3]$: Choose $(x, y)$ such that $o(x) = 2$ in $D_4$ and $o(y) = 3$ in $\mathbf{Z}_3$.

$$x \in \{a^2,\ b,\ ab,\ a^2 b,\ a^3 b\} \qquad \& \qquad y \in \{[1]_3,\ [2]_3\}$$

□