Final Review

Shaoyun Yi

MATH 546/701I

University of South Carolina

Summer 2021

Brief review from § 1.3, 1.4, 2.3 & § 3.1-3.8 (next slide)

Division Algorithm: $a = bq + r$, with $0 \leq r < b$. $\rightsquigarrow$ Euclidean Algorithm

A useful skill: To show $b|a$, write $a = bq + r$ first and then to show $r = 0$.

$d = \gcd(a, b)$ is the smallest positive linear combination of a and b.
An integer x is a linear combination of a and b if and only if $\gcd(a, b)|x$.

$(a, b) = 1$ if and only if there exist integers m, n such that $ma + nb = 1$.

i) If $b|ac$ and $(a, b) = 1$, then $b|c$.
ii) If $b|a, c|a$ and $(b, c) = 1$, then $bc|a$.
iii) $(a, b) \cdot [a, b] = ab$.

- Two groups: $(\mathbf{Z}_n, +_{[\,]})$ with $|\mathbf{Z}_n| = n$ & $(\mathbf{Z}_n^\times, \cdot_{[\,]})$ with $|\mathbf{Z}_n^\times| = \varphi(n)$
- The symmetric group $(S_n, \circ)$ of degree n with $|S_n| = n!$.
  - Disjoint cycles are commutative.
  - $\sigma \in S_n$ can be written as a *unique* product of disjoint cycles.
  - The order of σ is the **lcm** of the orders of its disjoint cycles.

- Group G: closure, associativity, identity, inverses; (non)abelian, (in)finite
- Subgroup $H \subseteq G$: closure, identity, inverses
  - Alternative way: H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.
  - $|H| < \infty$: To show H is nonempty and $ab \in H$ for all $a, b \in H$.
  - Cyclic subgroup $\langle a \rangle$ generated by $a \in G$ & $|\langle a \rangle| = o(a)$ if $\langle a \rangle$ is finite.
  - Product of two subgroups v.s. Direct product of (two $\rightsquigarrow n$) groups
  - N is a normal subgroup of G if $gng^{-1} \in N$ for all $n \in N, g \in G$.
    - N is normal if and only if its left and right cosets coincide.
    - G/N: Factor group under the coset multiplication $aNbN = abN$.
    - Any normal subgp N is the kernel of natural projection $\pi: G \to G/N$.
    - $G \neq \emptyset$ is called *simple* if it has no proper nontrivial normal subgroups.
- **Lagrange's Thm** If $|G| = n < \infty$ and $H \subseteq G$, then $|H| | n$. $\rightsquigarrow o(a)|n$
- (well-defined) Group homomorphism $\phi : G_1 \to G_2$ if $\phi(ab) = \phi(a)\phi(b)$.
  - $\phi(a^m) = (\phi(a))^m$ for all $a \in G_1, m \in \mathbf{Z}$.
  - If $o(a) = n$, then $o\big(\phi(a)\big)|n$. ($\rightsquigarrow o\big(\phi(a)\big) = n$ if ϕ is an isomorphism)
  - ϕ is onto: if G_1 is abelian (cyclic), then G_2 is also abelian (cyclic).
  - If $G_1 = \langle a \rangle$, then ϕ is completely determined by $\phi(a)$ and so $\mathrm{im}(\phi) = \langle \phi(a) \rangle$.
- **Fundamental Homomorphism Theorem** $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$
- Cayley's Theorem Every group is isomorphic to a permutation group.

  Cyclic group: ($\cong \mathbf{Z}$ or $\cong \mathbf{Z}_n$), Dihedral group D_n, Alternating group A_n

Example 1: Which of the groups below are isomorphic to each other?

Groups of order 8: $\mathbf{Z}_8, \quad \mathbf{Z}_4 \times \mathbf{Z}_2, \quad \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2, \quad \mathbf{Z}_{24}^\times, \quad \mathbf{Z}_{30}^\times, \quad D_4.$

In the proof of Euler's totient function $\varphi(n)$ (see § 3.5, slide #13)

$$\mathbf{Z}_n^\times \cong \mathbf{Z}_{p_1^{\alpha_1}}^\times \times \mathbf{Z}_{p_2^{\alpha_2}}^\times \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}}^\times$$

	Structure Property
$\mathbf{Z}_8$	cyclic
$\mathbf{Z}_4 \times \mathbf{Z}_2$	abelian, not cyclic; possible orders of an element: 1, 2, 4
$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$	abelian, not cyclic; each non-identity element has order 2
$\mathbf{Z}_{24}^\times$	abelian, not cyclic; $\mathbf{Z}_{24}^\times \cong \mathbf{Z}_3^\times \times \mathbf{Z}_8^\times \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$
$\mathbf{Z}_{30}^\times$	abelian, not cyclic; $\mathbf{Z}_{30}^\times \cong \mathbf{Z}_5^\times \times \mathbf{Z}_3^\times \times \mathbf{Z}_2^\times \cong \mathbf{Z}_4 \times \mathbf{Z}_2$
D_4	not abelian

Example 2: HW 6 #(9) (bonus question)

Let G be any group with no proper, nontrivial subgroups, and assume that G has more than one element. Prove that $G \cong \mathbf{Z}_p$ for some prime p.

Proof: There exists a non-identity element $a \in G$. Then

$$G = \langle a \rangle \text{ [Why?]} \quad \rightsquigarrow G \text{ is cyclic.}$$

Moreover, G must be a finite cyclic group. If not, then $\langle a^k \rangle$ is a proper, nontrivial subgroup of $G = \langle a \rangle$ for any positive integer k, a contradiction.

Let $|G| = n > 1$. Thus $G \cong \mathbf{Z}_n$. [Why?] Then $\mathbf{Z}_d \subset \mathbf{Z}_n$ for $d|n$. [Why?]

By assumption, $d = 1$ or $d = n$. $\rightsquigarrow$ n has to be a prime number p. □

Let G be a group with $|G| = pq$, where $p \neq q$ are prime numbers. Then every proper nontrivial subgroup of G is cyclic.

Proof: Let H be a proper nontrivial subgroup of G. By Lagrange's Thm, $|H|$ has to be p or q. Hence H is cyclic. [Why?] □

Example 3

Let G be an abelian group. Let $H := \{a \in G \mid o(a) < \infty\}$. Show that

i) H is a subgroup of G.

ii) $K = \{a \in G \mid o(a)|k\}$ is a subgroup of H for a fixed positive integer k.

iii) Is $\widetilde{K} = \{a \in G \mid o(a) \leq k\}$ also a subgroup of H for a fixed $k \in \mathbf{Z}_{>0}$?

Proof: i) Nonempty: $e \in H$. For any $a, b \in H$, we have $o(a), o(b) < \infty$.

$$(ab^{-1})^{o(a)\cdot o(b)} \overset{!}{=} (a)^{o(a)\cdot o(b)}(b^{-1})^{o(a)\cdot o(b)} = \cdots = e. \quad \rightsquigarrow ab^{-1} \in H$$

ii) Nonempty: $e \in K$. For any $a, b \in K$, we have $o(a)|k, o(b)|k$.

$$(ab^{-1})^{[o(a),o(b)]} \overset{!}{=} (a)^{[o(a),o(b)]}(b^{-1})^{[o(a),o(b)]} = ee = e. \quad \rightsquigarrow ab^{-1} \in K$$

iii) Might not be. Counterexample: Let $H = G = \mathbf{Z}_6$.

	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
order	1	6	3	2	3	6

However, the set $\{[0]_6, [2]_6, [3]_6, [4]_6\}$ is not a subgroup of H, which is the collection of all the elements whose order is less than 4. □

Example 4

Let $p > 2$ be a prime. Any group G of order $2p$ has an element of order 2 and an element of order p.

Proof: By Lagrange's theorem, an element can have order $1, 2, p$ or $2p$.

i) If G has an element of order $2p$, then $G \cong \mathbf{Z}_{2p} \cong \mathbf{Z}_2 \times \mathbf{Z}_p$. ✓

ii) If G is not cyclic, then the only possible orders of elements are $1, 2, p$.

Since $|G|$ is even, it must contain one element of order 2. (see § 3.6, #13)

Proof: If not, $\{a, a^{-1}\} \in G$ with $a \neq a^{-1}$ for any $a \neq e$ & $\{e, e^{-1}\} = \{e\}$.
$\rightsquigarrow$ G has an odd number of elements, which is impossible. □

G must contain an element of order p. (similarly as in § 3.6, #13)

Proof: If not, assume that every non-identity element of G has order 2.
Then we can always find a subgroup of order 4 as in § 3.6, #13, which is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$, a contradiction. [Why?] □ □

Example 5: The second isomorphism theorem

Let H and N be subgroups of a group G, and assume that N is normal.

i) N is a normal subgroup of HN.

ii) $\phi : H \to HN/N$ defined by $\phi(h) = hN$ is an onto homomorphism.

iii) $HN/N \cong H/K$, where $K = H \cap N$.

Proof: i) HN is a subgroup: Nonempty since $e \in HN$. For any $h_1 n_1, h_2 n_2 \in HN$, $h_1 n_1 (h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = h_1 h_2^{-1}(h_2 n_1 n_2^{-1} h_2^{-1}) \in HN$. [Why?]
N is normal in HN: For any $a \in N, hn \in HN$, we have $hna(hn)^{-1} \in N$. [Why?]
ii) well-defined: $hN = hnN \in HN/N$ for any $n \in N$. ϕ is a homomorphism:

For any $h_1, h_2 \in H$, we have $\phi(h_1 h_2) = h_1 h_2 N \overset{!}{=} h_1 N h_2 N = \phi(h_1)\phi(h_2)$.

ϕ is onto by the definition of ϕ.

iii) $\ker(\phi) = \{h \in H \mid \phi(h) = hN = N\} = \{h \in H \mid h \in N\} = H \cap N$.
By the fundamental homomorphism thm (The first isomorphism theorem),

$$HN/N \cong H/H \cap N.$$

□

Example 6: The third isomorphism theorem

Let H and N be normal subgroups of a group G with $N \subseteq H$. Define

$$\phi : G/N \to G/H \text{ by } \phi(xN) = xH, \quad \text{for all cosets } xN \in G/N.$$

i) ϕ is a well-defined onto homomorphism.

ii) $(G/N)/(H/N) \cong G/H$.

Proof: i) well-defined: If $xN = yN$, then $y^{-1}x \in N$, and so $y^{-1}x \in H$. This implies that $xH = yH$, i,e., $\phi(xN) = \phi(yN)$.

ϕ is a homomorphism: For any $xN, yN \in G/N$, we have

$$\phi(xNyN) \stackrel{!}{=} \phi(xyN) = xyH \stackrel{!}{=} xHyH = \phi(xN)\phi(yN).$$

ϕ is onto since any coset xH occurs as the image of xN under ϕ.

ii) $\ker(\phi) = \{xN \in G/N \mid \phi(xN) = xH = H\} = \{xN \in G/N \mid x \in H\}$.

This implies that $\ker(\phi)$ is the left cosets of N in H, i.e., $\ker(\phi) = H/N$.

In fact, N is normal in H. [Why?] By the fundamental homomorphism thm,

$$(G/N)/(H/N) \cong G/H. \qquad \square$$