Final Review

Shaoyun Yi

MATH 546/701I

University of South Carolina

June 18, 2020

Review from Chapter 1, I

Theorem (Theorem 2: Division Algorithm)

For any integers a and b, with $b > 0$, there exist unique integers q and r such that $a = bq + r$, with $0 \leq r < b$.

Example (A useful skill)

Theorem (Theorem 2: Division Algorithm)

For any integers a and b, with $b > 0$, there exist unique integers q and r such that $a = bq + r$, with $0 \leq r < b$.

Example (A useful skill)

To show $b|a$: We write $a = bq + r$ first and then to show $r = 0$.

Theorem (Theorem 5)

Review from Chapter 1, I

Theorem (Theorem 2: Division Algorithm)

For any integers a and b, with $b > 0$, there exist unique integers q and r such that $a = bq + r$, with $0 \leq r < b$.

Example (A useful skill)

To show $b|a$: We write $a = bq + r$ first and then to show $r = 0$.

Theorem (Theorem 5)

$d = \gcd(a, b)$ is the smallest positive linear combination of a and b. Moreover, an integer x is a linear combination of a and b $\Leftrightarrow$ $\gcd(a, b)|x$.

Remark (Use Group Theory:)

Review from Chapter 1, I

Theorem (Theorem 2: Division Algorithm)

For any integers a and b, with $b > 0$, there exist unique integers q and r such that $a = bq + r$, with $0 \leq r < b$.

Example (A useful skill)

To show $b|a$: We write $a = bq + r$ first and then to show $r = 0$.

Theorem (Theorem 5)

$d = \gcd(a, b)$ is the smallest positive linear combination of a and b. Moreover, an integer x is a linear combination of a and b $\Leftrightarrow \gcd(a, b)|x$.

Remark (Use Group Theory:)

$a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$, *where* $d = \gcd(a, b)$. $a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z}$, *where* $m = \mathrm{lcm}[a, b]$.

Review from Chapter 1, II

Question 1

How to find $d = \gcd(a, b)$ *and the linear combination* $as + bt = d$*?*

Answer 1

Review from Chapter 1, II

Question 1

How to find $d = \gcd(a, b)$ *and the linear combination* $as + bt = d$*?*

Answer 1

(*Matrix form of the*) **Euclidean algorithm !**

Proposition (Proposition. 1)

Review from Chapter 1, II

Question 1

How to find $d = \gcd(a, b)$ *and the linear combination* $as + bt = d$*?*

Answer 1

(*Matrix form of the*) **Euclidean algorithm !**

Proposition (Proposition. 1)

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

Proposition (Proposition. 2)

Review from Chapter 1, II

Question 1

How to find $d = \gcd(a, b)$ *and the linear combination* $as + bt = d$*?*

Answer 1

(*Matrix form of the*) **Euclidean algorithm !**

Proposition (Proposition. 1)

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

Proposition (Proposition. 2)

(a) *If* $b|ac$*, then* $b|(a, b) \cdot c$.

(b) *If* $b|ac$ *and* $(a, b) = 1$*, then* $b|c$.

(c) *If* $b|a, c|a$ *and* $(b, c) = 1$*, then* $bc|a$.

(d) $(a, bc) = 1$ *if and only if* $(a, b) = 1$ *and* $(a, c) = 1$.

Review from Chapter 1, III

Proposition (Proposition. 3)

Let $a, b, n \in \mathbf{Z}$ *and* $n > 0$. *Then* $a \equiv b \pmod{n}$ *if and only if* $n|(a-b)$.

Theorem (Theorem 10)

Proposition (Proposition. 3)

Let $a, b, n \in \mathbf{Z}$ and $n > 0$. Then $a \equiv b \pmod{n}$ if and only if $n|(a-b)$.

Theorem (Theorem 10)

(1) *$ax \equiv b \pmod{n}$ has a solution $\Leftrightarrow d|b$, where $d = \gcd(a, n)$.*
(2) *If $d|b$, then there are d distinct solutions modulo n, and these solutions are congruent modulo n/d.*

Question 2

Review from Chapter 1, III

Proposition (Proposition. 3)

Let $a, b, n \in \mathbf{Z}$ *and* $n > 0$. *Then* $a \equiv b \pmod{n}$ *if and only if* $n|(a-b)$.

Theorem (Theorem 10)

(1) $ax \equiv b \pmod{n}$ *has a solution* $\Leftrightarrow d|b$, *where* $d = \gcd(a, n)$.
(2) *If* $d|b$, *then there are* d *distinct solutions modulo* n, *and these solutions are congruent modulo* n/d.

Question 2

How to solve linear congruences $ax \equiv b \pmod{n}$*?*

Answer 2

Review from Chapter 1, III

Proposition (Proposition. 3)

Let $a, b, n \in \mathbf{Z}$ *and* $n > 0$. *Then* $a \equiv b \pmod{n}$ *if and only if* $n | (a - b)$.

Theorem (Theorem 10)

(1) $ax \equiv b \pmod{n}$ *has a solution* $\Leftrightarrow d | b$, *where* $d = \gcd(a, n)$.
(2) *If* $d | b$, *then there are* d *distinct solutions modulo* n, *and these solutions are congruent modulo* n/d.

Question 2

How to solve linear congruences $ax \equiv b \pmod{n}$*?*

Answer 2

See the slide (16 of 31): "An algorithm for solving linear congruences".

Theorem (Theorem 11)

Review from Chapter 1, III

Proposition (Proposition. 3)

Let $a, b, n \in \mathbf{Z}$ *and* $n > 0$. *Then* $a \equiv b \pmod{n}$ *if and only if* $n|(a-b)$.

Theorem (Theorem 10)

(1) $ax \equiv b \pmod{n}$ *has a solution* $\Leftrightarrow d|b$, *where* $d = \gcd(a, n)$.
(2) *If* $d|b$, *then there are* d *distinct solutions modulo* n, *and these solutions are congruent modulo* n/d.

Question 2

How to solve linear congruences $ax \equiv b \pmod{n}$*?*

Answer 2

See the slide (16 of 31): "An algorithm for solving linear congruences".

Theorem (Theorem 11)

Chinese Remainder Theorem: *Solve the system of congruences.*

Review from Chapter 1, IV

Definition (Definition 12 & Definition 17)

$\mathbf{Z}_n = \{[a]_n\}$ **vs.** $\mathbf{Z}_n^\times = \{[a]_n \mid \gcd(a, n) = 1\}$

Remark (Use Group Theory:)

Review from Chapter 1, IV

Definition (Definition 12 & Definition 17)

$\mathbf{Z}_n = \{[a]_n\}$ **vs.** $\mathbf{Z}_n^\times = \{[a]_n \mid \gcd(a, n) = 1\}$

Remark (Use Group Theory:)

Two Groups: $(\mathbf{Z}_n, +_{[\,]})$ **vs.** $(\mathbf{Z}_n^\times, \cdot_{[\,]})$

Example

Review from Chapter 1, IV

Definition (Definition 12 & Definition 17)

$\mathbf{Z}_n = \{[a]_n\}$ **vs.** $\mathbf{Z}_n^\times = \{[a]_n \mid \gcd(a, n) = 1\}$

Remark (Use Group Theory:)

Two Groups: $(\mathbf{Z}_n, +_{[\,]})$ **vs.** $(\mathbf{Z}_n^\times, \cdot_{[\,]})$

Example

$|\mathbf{Z}_n| = n$ **vs.** $|\mathbf{Z}_n^\times| = \varphi(n) =$ *the number of generators of* $\mathbf{Z}_n$.

Definition (Definition 16 & Proposition. 8)

Review from Chapter 1, IV

Definition (Definition 12 & Definition 17)

$\mathbf{Z}_n = \{[a]_n\}$ **vs.** $\mathbf{Z}_n^\times = \{[a]_n \mid \gcd(a,n) = 1\}$

Remark (Use Group Theory:)

Two Groups: $(\mathbf{Z}_n, +_{[\,]})$ **vs.** $(\mathbf{Z}_n^\times, \cdot_{[\,]})$

Example

$|\mathbf{Z}_n| = n$ **vs.** $|\mathbf{Z}_n^\times| = \varphi(n) =$ *the number of generators of* $\mathbf{Z}_n$.

Definition (Definition 16 & Proposition. 8)

$\varphi(n)$: **Euler's φ-function**, *or the* **totient function**.

Note (Theorem 18 & Corollary 19: Euler's Thm $\Rightarrow$ Fermat's Thm)

Review from Chapter 1, IV

Definition (Definition 12 & Definition 17)

$\mathbf{Z}_n = \{[a]_n\}$ **vs.** $\mathbf{Z}_n^\times = \{[a]_n \mid \gcd(a, n) = 1\}$

Remark (Use Group Theory:)

Two Groups: $(\mathbf{Z}_n, +_{[\,]})$ **vs.** $(\mathbf{Z}_n^\times, \cdot_{[\,]})$

Example

$|\mathbf{Z}_n| = n$ **vs.** $|\mathbf{Z}_n^\times| = \varphi(n) =$ *the number of generators of* $\mathbf{Z}_n$.

Definition (Definition 16 & Proposition. 8)

$\varphi(n)$: **Euler's φ-function**, *or the* **totient function**.

Note (Theorem 18 & Corollary 19: Euler's Thm $\Rightarrow$ Fermat's Thm)

If $(a, n) = 1$, *then* $a^{\varphi(n)} \equiv 1 \pmod{n}$. $\Rightarrow$ $a^p \equiv a \pmod{p}$ *if* p *is a prime.*

Review from §2.3, I

Definition (Definition 1)

A function $\sigma : S \to S$ is a **permutation** *of S if σ is one-to-one and onto.*

Remark (Use Group Theory: Proposition. 1)

Review from §2.3, I

Definition (Definition 1)

A function $\sigma : S \to S$ *is a* **permutation** *of* S *if* σ *is one-to-one and onto.*

Remark (Use Group Theory: Proposition. 1)

$(\mathrm{Sym}(S), \circ)$ *is a group.*

Proposition (Proposition. 2)

Review from §2.3, I

Definition (Definition 1)

A function $\sigma : S \to S$ *is a* **permutation** *of* S *if* σ *is one-to-one and onto.*

Remark (Use Group Theory: Proposition. 1)

$(\mathrm{Sym}(S), \circ)$ *is a group.*

Proposition (Proposition. 2)

$|S_n| = n!$.

Definition (Definition 2)

Review from §2.3, I

Definition (Definition 1)

A function $\sigma : S \to S$ is a **permutation** *of S if σ is one-to-one and onto.*

Remark (Use Group Theory: Proposition. 1)

$(\mathrm{Sym}(S), \circ)$ *is a group.*

Proposition (Proposition. 2)

$|S_n| = n!$.

Definition (Definition 2)

$\sigma = (a_1 a_2 \cdots a_k)$*: a cycle of length k. And the order $o(\sigma) = k$.*

Example

Review from §2.3, I

Definition (Definition 1)

A function $\sigma : S \to S$ is a **permutation** *of S if σ is one-to-one and onto.*

Remark (Use Group Theory: Proposition. 1)

$(\mathrm{Sym}(S), \circ)$ *is a group.*

Proposition (Proposition. 2)

$|S_n| = n!$.

Definition (Definition 2)

$\sigma = (a_1 a_2 \cdots a_k)$*: a cycle of length k. And the order $o(\sigma) = k$.*

Example

Know how to compute $\sigma\tau = \sigma \circ \tau$ and σ^{-1}.

Review from §2.3, II

Proposition (Definition 3 & Proposition. 3)

If σ and τ are disjoint cycles in $\mathrm{Sym}(S)$, then $\sigma\tau = \tau\sigma$.

Theorem (Theorem 4)

Review from §2.3, II

Proposition (Definition 3 & Proposition. 3)

If σ and τ are disjoint cycles in $\mathrm{Sym}(S)$, then $\sigma\tau = \tau\sigma$.

Theorem (Theorem 4)

Every $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.

Proposition (Proposition. 5)

Review from §2.3, II

Proposition (Definition 3 & Proposition. 3)

If σ and τ are disjoint cycles in $\mathrm{Sym}(S)$, then $\sigma\tau = \tau\sigma$.

Theorem (Theorem 4)

Every $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.

Proposition (Proposition. 5)

The order of σ is the **lcm** *of the lengths (orders) of its disjoint cycles.*

Proposition (Definition 6 & Proposition. 6)

Proposition (Definition 3 & Proposition. 3)

If σ and τ are disjoint cycles in $\mathrm{Sym}(S)$, then $\sigma\tau = \tau\sigma$.

Theorem (Theorem 4)

Every $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.

Proposition (Proposition. 5)

The order of σ is the **lcm** *of the lengths (orders) of its disjoint cycles.*

Proposition (Definition 6 & Proposition. 6)

Every $\sigma \in S_n$ can be written as a (NOT unique) product of transpositions.

Definition (Theorem 7 & Definition 8)

Review from §2.3, II

Proposition (Definition 3 & Proposition. 3)

If σ and τ are disjoint cycles in $\mathrm{Sym}(S)$, then $\sigma\tau = \tau\sigma$.

Theorem (Theorem 4)

Every $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.

Proposition (Proposition. 5)

The order of σ is the **lcm** *of the lengths (orders) of its disjoint cycles.*

Proposition (Definition 6 & Proposition. 6)

Every $\sigma \in S_n$ can be written as a (NOT unique) product of transpositions.

Definition (Theorem 7 & Definition 8)

Product of transpositions: Even permutation **vs.** *Odd permutation*

Review from §3.1, I

Definition (Definition 5)

$(G, *)$ is a group if $*$ is a binary operation, and the following are satisfied:

(i) **Closure**: *For all $a, b \in G$, $a * b$ is a well-defined element of G.*

(ii) **Associativity**: *For all $a, b, c \in G$, we have*

$$a * (b * c) = (a * b) * c.$$

(iii) **Identity**: *There exists an* **identity** *element $e \in G$, i.e.,*

$$a * e = a \quad \text{and} \quad e * a = a \qquad \text{for all } a \in G.$$

(iv) **Inverses**: *For each $a \in G$ there exists an inverse element $a^{-1} \in G$:*

$$a * a^{-1} = e \quad \text{and} \quad a^{-1} * a = e.$$

Definition (Definition 6)

Review from §3.1, I

Definition (Definition 5)

$(G, *)$ is a group if $*$ is a binary operation, and the following are satisfied:

(i) **Closure**: *For all $a, b \in G$, $a * b$ is a well-defined element of G.*

(ii) **Associativity**: *For all $a, b, c \in G$, we have*

$$a * (b * c) = (a * b) * c.$$

(iii) **Identity**: *There exists an* **identity** *element $e \in G$, i.e.,*

$$a * e = a \quad \text{and} \quad e * a = a \qquad \text{for all } a \in G.$$

(iv) **Inverses**: *For each $a \in G$ there exists an inverse element $a^{-1} \in G$:*

$$a * a^{-1} = e \quad \text{and} \quad a^{-1} * a = e.$$

Definition (Definition 6)

A group is a nonempty set G with an **associative** *binary operation, such that G contains an* **identity** *element for the operation, and each element of G has an* **inverse** *in G.*

Review from §3.1, II

Proposition (Proposition 4)

(i) *If* $ab = ac$*, then* $b = c$*.* (ii) *If* $ac = bc$*, then* $a = b$*.*

Definition (Definition 9)

Review from §3.1, II

Proposition (Proposition 4)

(i) *If* $ab = ac$, *then* $b = c$. (ii) *If* $ac = bc$, *then* $a = b$.

Definition (Definition 9)

A group G *is said to be* **abelian** *if* $ab = ba$ *for all* $a, b \in G$.

Example (Propositions 6-7)

Review from §3.1, II

Proposition (Proposition 4)

(i) *If* $ab = ac$, *then* $b = c$. (ii) *If* $ac = bc$, *then* $a = b$.

Definition (Definition 9)

A group G *is said to be* **abelian** *if* $ab = ba$ *for all* $a, b \in G$.

Example (Propositions 6-7)

$(\mathbf{Z}_n, +_{[\,]})$ *is abelian with* $|\mathbf{Z}_n| = n$. $(\mathbf{Z}_n^\times, \cdot_{[\,]})$ *is abelian with* $|\mathbf{Z}_n^\times| = \varphi(n)$.

Definition (Definition 14)

Review from §3.1, II

Proposition (Proposition 4)

(i) *If* $ab = ac$, *then* $b = c$. (ii) *If* $ac = bc$, *then* $a = b$.

Definition (Definition 9)

A group G *is said to be* **abelian** *if* $ab = ba$ *for all* $a, b \in G$.

Example (Propositions 6-7)

$(\mathbf{Z}_n, +_{[\,]})$ *is abelian with* $|\mathbf{Z}_n| = n$. $(\mathbf{Z}_n^\times, \cdot_{[\,]})$ *is abelian with* $|\mathbf{Z}_n^\times| = \varphi(n)$.

Definition (Definition 14)

$\sim$ *is an* **equivalence relation** *if and only if for all* $a, b, c \in S$ *we have*

(1) *Reflexive:* $a \sim a$;

(2) *Symmetric: if* $a \sim b$, *then* $b \sim a$;

(3) *Transitive: if* $a \sim b$ *and* $b \sim c$, *then* $a \sim c$.

Review from §3.2, I

Proposition (Proposition 1)

H is a subgroup of G if and only if the following conditions hold:

(i) **Closure:** $ab \in H$ *for all* $a, b \in H$;

(ii) **Identity:** $e \in H$;

(iii) **Inverses:** $a^{-1} \in H$ *for all* $a \in H$.

Corollary (Corollary 7)

Review from §3.2, I

Proposition (Proposition 1)

H is a subgroup of G if and only if the following conditions hold:

(i) **Closure:** $ab \in H$ *for all* $a, b \in H$;

(ii) **Identity:** $e \in H$;

(iii) **Inverses:** $a^{-1} \in H$ *for all* $a \in H$.

Corollary (Corollary 7)

H is a subgroup of G $\Leftrightarrow$ H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

Corollary (Corollary 8: Let H be a finite subset of G.)

Proposition (Proposition 1)

H is a subgroup of G if and only if the following conditions hold:

(i) **Closure:** $ab \in H$ *for all* $a, b \in H$;

(ii) **Identity:** $e \in H$;

(iii) **Inverses:** $a^{-1} \in H$ *for all* $a \in H$.

Corollary (Corollary 7)

H is a subgroup of G $\Leftrightarrow$ H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

Corollary (Corollary 8: Let H be a finite subset of G.)

H is a subgroup of G $\Leftrightarrow$ H is nonempty and $ab \in H$ for all $a, b \in H$.

Example (Note 1)

Review from §3.2, I

Proposition (Proposition 1)

H is a subgroup of G if and only if the following conditions hold:

(i) **Closure:** *$ab \in H$ for all $a, b \in H$;*

(ii) **Identity:** *$e \in H$;*

(iii) **Inverses:** *$a^{-1} \in H$ for all $a \in H$.*

Corollary (Corollary 7)

H is a subgroup of G $\Leftrightarrow$ H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

Corollary (Corollary 8: Let H be a finite subset of G.)

H is a subgroup of G $\Leftrightarrow$ H is nonempty and $ab \in H$ for all $a, b \in H$.

Example (Note 1)

H is nonempty: Easy to show that H **contains the identity element** *e.*

Review from §3.2, II

Definition (Definition 11)

Cyclic subgroup generated by a**:** $\langle a \rangle = \{x \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$.
G is called a **cyclic group** *if $G = \langle a \rangle$ for some (***generator***) $a \in G$.*

Proposition (Proposition 2)

Review from §3.2, II

Definition (Definition 11)

Cyclic subgroup generated by a**:** $\langle a \rangle = \{x \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$.
G is called a **cyclic group** *if $G = \langle a \rangle$ for some (***generator***) $a \in G$.*

Proposition (Proposition 2)

The cyclic subgroup $\langle a \rangle$ is the **smallest** *subgroup of G containing $a \in G$.*

Example (Examples 14-16)

Review from §3.2, II

Definition (Definition 11)

Cyclic subgroup generated by a**:** $\langle a \rangle = \{x \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$.
G is called a **cyclic group** *if $G = \langle a \rangle$ for some (***generator***) $a \in G$.*

Proposition (Proposition 2)

The cyclic subgroup $\langle a \rangle$ is the **smallest** *subgroup of G containing $a \in G$.*

Example (Examples 14-16)

$(\mathbf{Z}, +)$ *and* $(\mathbf{Z}_n, +_{[\ ]})$ *are cyclic.* $(\mathbf{Z}_n^{\times}, \cdot_{[\ ]})$ *is not always cyclic.*

Note (Homework 3 (6) & Homework 4 (4))

Review from §3.2, II

Definition (Definition 11)

Cyclic subgroup generated by a**:** $\langle a \rangle = \{x \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$.
G is called a **cyclic group** *if $G = \langle a \rangle$ for some (***generator***) $a \in G$.*

Proposition (Proposition 2)

The cyclic subgroup $\langle a \rangle$ is the **smallest** *subgroup of G containing $a \in G$.*

Example (Examples 14-16)

$(\mathbf{Z}, +)$ *and* $(\mathbf{Z}_n, +_{[\ ]})$ *are cyclic.* $(\mathbf{Z}_n^\times, \cdot_{[\ ]})$ *is not always cyclic.*

Note (Homework 3 (6) & Homework 4 (4))

Any cyclic group is abelian, but conversely not true.

Definition (Definition 17)

Review from §3.2, II

Definition (Definition 11)

Cyclic subgroup generated by a**:** $\langle a \rangle = \{x \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$.
G is called a **cyclic group** *if $G = \langle a \rangle$ for some (***generator***) $a \in G$.*

Proposition (Proposition 2)

The cyclic subgroup $\langle a \rangle$ is the **smallest** *subgroup of G containing $a \in G$.*

Example (Examples 14-16)

$(\mathbf{Z}, +)$ *and* $(\mathbf{Z}_n, +_{[\ ]})$ *are cyclic.* $(\mathbf{Z}_n^{\times}, \cdot_{[\ ]})$ *is not always cyclic.*

Note (Homework 3 (6) & Homework 4 (4))

Any cyclic group is abelian, but conversely not true.

Definition (Definition 17)

The order of a**:** $o(a) = \min\{n \in \mathbf{Z}^+ \mid a^n = e\}$. *Note: $o(a)$ might be ∞.*

Review from §3.2, III

Proposition (Proposition 3)

(a) *If* $o(a) = \infty$*, then* $a^k \neq a^m$ *for all integers* $k \neq m$*.*

(b) *If* $o(a) = n < \infty$ *and* $k \in \mathbf{Z}$*, then* $a^k = e$ *if and only if* $n | k$*.*

(c) *If* $o(a) = n < \infty$*, then* $a^k = a^m$ *if and only if* $k \equiv m \pmod{n}$ *for all integers* k, m*. Furthermore,* $|\langle a \rangle| = o(a)$*.*

Theorem (Theorem 18: Lagrange's Theorem)

Review from §3.2, III

Proposition (Proposition 3)

(a) *If* $o(a) = \infty$, *then* $a^k \neq a^m$ *for all integers* $k \neq m$.

(b) *If* $o(a) = n < \infty$ *and* $k \in \mathbf{Z}$, *then* $a^k = e$ *if and only if* $n|k$.

(c) *If* $o(a) = n < \infty$, *then* $a^k = a^m$ *if and only if* $k \equiv m \pmod{n}$ *for all integers* k, m. *Furthermore,* $|\langle a \rangle| = o(a)$.

Theorem (Theorem 18: Lagrange's Theorem)

If H *is a subgroup of the finite group* G, *then* $|H|$ *is a divisor of* $|G|$.

Corollary (Corollary 20: Let G be a finite group of order n.)

Review from §3.2, III

Proposition (Proposition 3)

(a) *If $o(a) = \infty$, then $a^k \neq a^m$ for all integers $k \neq m$.*

(b) *If $o(a) = n < \infty$ and $k \in \mathbf{Z}$, then $a^k = e$ if and only if $n|k$.*

(c) *If $o(a) = n < \infty$, then $a^k = a^m$ if and only if $k \equiv m \pmod{n}$ for all integers k, m. Furthermore, $|\langle a \rangle| = o(a)$.*

Theorem (Theorem 18: Lagrange's Theorem)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

Corollary (Corollary 20: Let G be a finite group of order n.)

(a) *For any $a \in G$, $o(a)$ is a divisor of n.*

(b) *For any $a \in G, a^n = e$.*

Corollary (Corollary 21)

Review from §3.2, III

Proposition (Proposition 3)

(a) *If $o(a) = \infty$, then $a^k \neq a^m$ for all integers $k \neq m$.*

(b) *If $o(a) = n < \infty$ and $k \in \mathbf{Z}$, then $a^k = e$ if and only if $n|k$.*

(c) *If $o(a) = n < \infty$, then $a^k = a^m$ if and only if $k \equiv m \pmod{n}$ for all integers k, m. Furthermore, $|\langle a \rangle| = o(a)$.*

Theorem (Theorem 18: Lagrange's Theorem)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

Corollary (Corollary 20: Let G be a finite group of order n.)

(a) *For any $a \in G$, $o(a)$ is a divisor of n.*

(b) *For any $a \in G, a^n = e$.*

Corollary (Corollary 21)

Any group of prime order is cyclic.

Review from §3.3, I

Example (Groups of small orders)

(i) *Groups of order 2, 3, 5 are cyclic.*

(ii) *Groups of order 4 are abelian: cyclic* [$\mathbf{Z}_4$] **vs.** *non-cyclic* [$\mathbf{Z}_8^\times$]

(iii) *Groups of order 6: abelian (cyclic)* [$\mathbf{Z}_6$] **vs.** *nonabelian* [S_3]

Proposition (Defintion 2 & Question 3 & Proposition 1)

Example (Groups of small orders)

(i) *Groups of order 2, 3, 5 are cyclic.*

(ii) *Groups of order 4 are abelian: cyclic* [$\mathbf{Z}_4$] **vs.** *non-cyclic* [$\mathbf{Z}_8^\times$]

(iii) *Groups of order 6: abelian (cyclic)* [$\mathbf{Z}_6$] **vs.** *nonabelian* [S_3]

Proposition (Defintion 2 & Question 3 & Proposition 1)

Product of two subgroups: *HK is not always a subgroup of G.*
If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G.

Note

Example (Groups of small orders)

(i) *Groups of order 2, 3, 5 are cyclic.*

(ii) *Groups of order* 4 *are abelian: cyclic* [$\mathbf{Z}_4$] **vs.** *non-cyclic* [$\mathbf{Z}_8^{\times}$]

(iii) *Groups of order* 6*: abelian (cyclic)* [$\mathbf{Z}_6$] **vs.** *nonabelian* [S_3]

Proposition (Defintion 2 & Question 3 & Proposition 1)

Product of two subgroups: *HK is not always a subgroup of G.*
If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G.

Note

If G is abelian, then the product of any two subgroups is again a subgroup.
If G is a finite group, then $|HK| = |H||K|/|H \cap K|$.

Review from §3.3, II

Proposition (Definition 5 & Proposition 2 & Remark 1)

(a) *The* **direct product** $G_1 \times G_2$ *is a group under the operation defined for all* $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$ *by* $(a_1, a_2)(b_1, b_2) = (a_1 * b_1, a_2 \cdot b_2)$*.*

(b) *If* $o(a_1) = n$ *and* $o(a_2) = m$*, then* $o((a_1, a_2)) = \mathrm{lcm}[n, m]$ *in* $G_1 \times G_2$*.*

(c) *If* G_1, G_2 *are finite groups, then* $|G_1 \times G_2| = |G_1| \cdot |G_2|$*.*

Example (Example 6 & Proposition 3)

Proposition (Definition 5 & Proposition 2 & Remark 1)

(a) *The* **direct product** $G_1 \times G_2$ *is a group under the operation defined for all* $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$ *by* $(a_1, a_2)(b_1, b_2) = (a_1 * b_1, a_2 \cdot b_2)$.

(b) *If* $o(a_1) = n$ *and* $o(a_2) = m$, *then* $o((a_1, a_2)) = \mathrm{lcm}[n, m]$ *in* $G_1 \times G_2$.

(c) *If* G_1, G_2 *are finite groups, then* $|G_1 \times G_2| = |G_1| \cdot |G_2|$.

Example (Example 6 & Proposition 3)

$\mathbf{Z} \times \mathbf{Z}$ *is not cyclic.* $\mathbf{Z}_n \times \mathbf{Z}_m$ *is cyclic if and only if* $\gcd(n, m) = 1$.

Proposition (Definition 10 & Proposition 7)

Review from §3.3, II

Proposition (Definition 5 & Proposition 2 & Remark 1)

(a) *The* **direct product** $G_1 \times G_2$ *is a group under the operation defined for all* $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$ *by* $(a_1, a_2)(b_1, b_2) = (a_1 * b_1, a_2 \cdot b_2)$.

(b) *If* $o(a_1) = n$ *and* $o(a_2) = m$, *then* $o((a_1, a_2)) = \mathrm{lcm}[n, m]$ *in* $G_1 \times G_2$.

(c) *If* G_1, G_2 *are finite groups, then* $|G_1 \times G_2| = |G_1| \cdot |G_2|$.

Example (Example 6 & Proposition 3)

$\mathbf{Z} \times \mathbf{Z}$ *is not cyclic.* $\mathbf{Z}_n \times \mathbf{Z}_m$ *is cyclic if and only if* $\gcd(n, m) = 1$.

Proposition (Definition 10 & Proposition 7)

Subgroup generated by S**:** $\langle S \rangle$ *is the smallest subgroup that contains* S.

Review from §3.4, I

Definition (Definition 1)

$(G_1, *) \cong (G_2, \cdot)$: *A group isomorphism* $\phi : G_1 \to G_2$ *satisfies*

- ϕ *is well-defined*
- ϕ *is a group homomorphism:* $\phi(a * b) = \phi(a) \cdot \phi(b)$
- ϕ *is one-to-one and onto*

Proposition (Proposition 1)

Definition (Definition 1)

$(G_1, *) \cong (G_2, \cdot)$: *A group isomorphism* $\phi : G_1 \to G_2$ *satisfies*

- ϕ *is well-defined*
- ϕ *is a group homomorphism:* $\phi(a * b) = \phi(a) \cdot \phi(b)$
- ϕ *is one-to-one and onto*

Proposition (Proposition 1)

Let $\phi : G_1 \to G_2$ *be an isomorphism. Let* $e_1 = e_{G_1}$ *and* $e_2 = e_{G_2}$. *Then*

(a) $\phi(e_1) = e_2$.

(b) $\phi(a^{-1}) = (\phi(a))^{-1}$ *for all* $a \in G_1$.

(c) $\phi(a^n) = (\phi(a))^n$ *for all* $a \in G_1$ *and all* $n \in \mathbf{Z}$.

Proposition (Proposition 2)

Review from §3.4, I

Definition (Definition 1)

$(G_1, *) \cong (G_2, \cdot)$: *A group isomorphism* $\phi : G_1 \to G_2$ *satisfies*

- ϕ *is well-defined*
- ϕ *is a group homomorphism:* $\phi(a * b) = \phi(a) \cdot \phi(b)$
- ϕ *is one-to-one and onto*

Proposition (Proposition 1)

Let $\phi : G_1 \to G_2$ *be an isomorphism. Let* $e_1 = e_{G_1}$ *and* $e_2 = e_{G_2}$. *Then*

(a) $\phi(e_1) = e_2$.

(b) $\phi(a^{-1}) = (\phi(a))^{-1}$ *for all* $a \in G_1$.

(c) $\phi(a^n) = (\phi(a))^n$ *for all* $a \in G_1$ *and all* $n \in \mathbf{Z}$.

Proposition (Proposition 2)

The isomorphism $\cong$ *is an equivalence relation.*

Note (Examples 4-5 & Propositions 5-6: Show one-to-one and onto:)

- *Direct proof; Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$*
- *If ϕ is a homomorphism, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$. That is, $\ker(\phi) = \{e_1\}$.*
- *If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.*

Example (Note 3 & Proposition 6)

Note (Examples 4-5 & Propositions 5-6: Show one-to-one and onto:)

- *Direct proof; Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$*
- *If ϕ is a homomorphism, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$. That is, $\ker(\phi) = \{e_1\}$.*
- *If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.*

Example (Note 3 & Proposition 6)

$\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn}$ *if and only if* $\gcd(m, n) = 1$.

Proposition (Proposition 3: Let $\phi : G_1 \to G_2$ be an isomorphism.)

Review from §3.4, II

Note (Examples 4-5 & Propositions 5-6: Show one-to-one and onto:)

- *Direct proof; Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$*
- *If ϕ is a homomorphism, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$. That is, $\ker(\phi) = \{e_1\}$.*
- *If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.*

Example (Note 3 & Proposition 6)

$\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn}$ *if and only if* $\gcd(m, n) = 1$.

Proposition (Proposition 3: Let $\phi : G_1 \to G_2$ be an isomorphism.)

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian (cyclic), then so is G_2.*

Note (Note 2 & Examples 6-9)

Review from §3.4, II

Note (Examples 4-5 & Propositions 5-6: Show one-to-one and onto:)

- *Direct proof; Find its inverse function ϕ^{-1}: $\phi^{-1}\phi = 1_{G_1}, \phi\phi^{-1} = 1_{G_2}$*
- *If ϕ is a homomorphism, then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$, for all $x \in G_1$. That is, $\ker(\phi) = \{e_1\}$.*
- *If $|G_1| = |G_2| < \infty$, then any one-to-one mapping must be onto.*

Example (Note 3 & Proposition 6)

$\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn}$ *if and only if* $\gcd(m, n) = 1$.

Proposition (Proposition 3: Let $\phi : G_1 \to G_2$ be an isomorphism.)

(a) *If a has order n in G_1, then $\phi(a)$ has order n in G_2.*

(b) *If G_1 is abelian (cyclic), then so is G_2.*

Note (Note 2 & Examples 6-9)

This gives us a technique for proving that two groups are not isomorphic.

Review from §3.5, I

Theorem (Theorems 1-2)

- *Every subgroup of a cyclic group G is cyclic.*
- *Let G be a cyclic group.* $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$

Corollary (Corollary 3)

Theorem (Theorems 1-2)

- *Every subgroup of a cyclic group G is cyclic.*
- *Let G be a cyclic group.* $\begin{cases} \textit{If } G \textit{ is infinite, then } G \cong \mathbf{Z}. \\ \textit{If } |G| = n, \textit{ then } G \cong \mathbf{Z}_n. \end{cases}$

Corollary (Corollary 3)

(a) *Any two infinite cyclic groups are isomorphic to each other.*

(b) *Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.*

Note (Note 1 & Corollary 4 & Remark 1: Subgroups of $\mathbf{Z}$)

Theorem (Theorems 1-2)

- *Every subgroup of a cyclic group G is cyclic.*
- *Let G be a cyclic group.* $\begin{cases} \text{If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{If } |G| = n, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$

Corollary (Corollary 3)

(a) *Any two infinite cyclic groups are isomorphic to each other.*

(b) *Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.*

Note (Note 1 & Corollary 4 & Remark 1: Subgroups of $\mathbf{Z}$)

For any $m \in \mathbf{Z}$, $m\mathbf{Z} = \langle m \rangle \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

• $m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m$. • $m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n$.

Review from §3.5, II

Proposition (Proposition 1 & Corollary 5 & Note 3: Subgroups of $\mathbf{Z}_n$)

Let $d = \gcd(m, n)$. *Then* $\langle [m]_n \rangle = \langle [d]_n \rangle$. *And* $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

(a) *The element* $[k]_n$ *generates* $\mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, *i.e.*, $[k]_n \in \mathbf{Z}_n\times$.

(b) *If* H *is any subgroup of* $\mathbf{Z}_n$, *then* $H = \langle [d]_n \rangle$ *for some divisor* d *of* n.

(c) *If* $d_1|n$ *and* $d_2|n$, *then* $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ *if and only if* $d_2|d_1$.

(c)' *If* $d_1|n$ *and* $d_2|n$ *and* $d_1 \neq d_2$, *then* $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.

Remark (Below Proposition 1 & Corollary 5: $G = \langle a \rangle$ with $o(a) = n$.)

Proposition (Proposition 1 & Corollary 5 & Note 3: Subgroups of $\mathbf{Z}_n$)

Let $d = \gcd(m, n)$. Then $\langle [m]_n \rangle = \langle [d]_n \rangle$. And $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

(a) *The element $[k]_n$ generates $\mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, i.e., $[k]_n \in \mathbf{Z}_n\times$.*

(b) *If H is any subgroup of $\mathbf{Z}_n$, then $H = \langle [d]_n \rangle$ for some divisor d of n.*

(c) *If $d_1|n$ and $d_2|n$, then $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ if and only if $d_2|d_1$.*

(c)' *If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*

Remark (Below Proposition 1 & Corollary 5: $G = \langle a \rangle$ with $o(a) = n$.)

Know how to translate above proposition to the multiplicative version.

Example (Definition 8 & Example 9)

Review from §3.5, II

Proposition (Proposition 1 & Corollary 5 & Note 3: Subgroups of $\mathbf{Z}_n$)

Let $d = \gcd(m, n)$. *Then* $\langle [m]_n \rangle = \langle [d]_n \rangle$. *And* $|\langle [m]_n \rangle| = |\langle [d]_n \rangle| = n/d$.

(a) *The element* $[k]_n$ *generates* $\mathbf{Z}_n \Leftrightarrow \gcd(k, n) = 1$, *i.e.,* $[k]_n \in \mathbf{Z}_n \times$.

(b) *If* H *is any subgroup of* $\mathbf{Z}_n$, *then* $H = \langle [d]_n \rangle$ *for some divisor* d *of* n.

(c) *If* $d_1 | n$ *and* $d_2 | n$, *then* $\langle [d_1]_n \rangle \subseteq \langle [d_2]_n \rangle$ *if and only if* $d_2 | d_1$.

(c)' *If* $d_1 | n$ *and* $d_2 | n$ *and* $d_1 \neq d_2$, *then* $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.

Remark (Below Proposition 1 & Corollary 5: $G = \langle a \rangle$ with $o(a) = n$.)

Know how to translate above proposition to the multiplicative version.

Example (Definition 8 & Example 9)

Subgroup diagram *shows all subgroups of* $\mathbf{Z}_n$ *and the inclusion relations.*

Review from §3.5, III

Definition (Definition 10)

Direct product $G_1 \times \cdots \times G_n$ *of n groups* $G_1, \ldots, G_n$ *is defined as follows*

- *The elements are n-tuples* $(g_1, \ldots, g_n)$, *where* $g_i \in G_i$ *for each* i.
- *The operation is componentwise multiplication:*

$$(g_1, \ldots, g_n)(g'_1, \ldots, g'_n) = (g_1 g'_1, \ldots, g_n g'_n).$$

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

Example (Theorem 11 & Examples 14-15)

Review from §3.5, III

Definition (Definition 10)

Direct product $G_1 \times \cdots \times G_n$ *of* n *groups* $G_1, \ldots, G_n$ *is defined as follows*

- *The elements are* n*-tuples* $(g_1, \ldots, g_n)$, *where* $g_i \in G_i$ *for each* i.
- *The operation is componentwise multiplication:*

$$(g_1, \ldots, g_n)(g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n').$$

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

Example (Theorem 11 & Examples 14-15)

Let $n \in \mathbf{Z}^+$ *which has the prime decomposition* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. *Then*

$$\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}}, \text{ where } p_1 < p_2 < \ldots < p_m.$$

Corollary (Corollary 12 (Proposition. 8 in Chapter 1))

Review from §3.5, III

Definition (Definition 10)

Direct product $G_1 \times \cdots \times G_n$ *of n groups* $G_1, \ldots, G_n$ *is defined as follows*

- *The elements are n-tuples* $(g_1, \ldots, g_n)$, *where* $g_i \in G_i$ *for each i.*
- *The operation is componentwise multiplication:*

$$(g_1, \ldots, g_n)(g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n').$$

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

Example (Theorem 11 & Examples 14-15)

Let $n \in \mathbf{Z}^+$ *which has the prime decomposition* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. *Then*

$$\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}}, \text{ where } p_1 < p_2 < \ldots < p_m.$$

Corollary (Corollary 12 (Proposition. 8 in Chapter 1))

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

Definition (Definition 16)

Exponent *of group* $G = \min\{N \in \mathbf{Z}^+ \mid a^N = e \text{ for all } a \in G\}$.

Proposition (Proposition 2: Let G be a finite abelian group.)

Review from §3.5, IV

Definition (Definition 16)

Exponent *of group* $G = \min\{N \in \mathbf{Z}^+ \mid a^N = e \text{ for all } a \in G\}$.

Proposition (Proposition 2: Let G be a finite abelian group.)

(a) *The exponent of G is equal to* $\max\{o(a) \mid a \in G\}$..

(b) *The group G is cyclic if and only if its exponent is equal to its order.*

Note

Definition (Definition 16)

Exponent *of group* $G = \min\{N \in \mathbf{Z}^+ \mid a^N = e \text{ for all } a \in G\}$.

Proposition (Proposition 2: Let G be a finite abelian group.)

(a) *The exponent of G is equal to* $\max\{o(a) \mid a \in G\}$..

(b) *The group G is cyclic if and only if its exponent is equal to its order.*

Note

This characterizes cyclic groups among all finite abelian groups.

Example (Two Examples: $\mathbf{Z}_{15}^\times$ is not cyclic & $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$)

Review from §3.5, IV

Definition (Definition 16)

Exponent *of group* $G = \min\{N \in \mathbf{Z}^+ \mid a^N = e \text{ for all } a \in G\}$.

Proposition (Proposition 2: Let G be a finite abelian group.)

(a) *The exponent of G is equal to* $\max\{o(a) \mid a \in G\}$..

(b) *The group G is cyclic if and only if its exponent is equal to its order.*

Note

This characterizes cyclic groups among all finite abelian groups.

Example (Two Examples: $\mathbf{Z}_{15}^\times$ is not cyclic & $\mathbf{Z}_7^\times \cong \mathbf{Z}_{14}^\times$)

For small n, check $\mathbf{Z}_n^\times$ cyclic or not without using primitive root theorem.

Review from §3.6, I

Definition (Definition 1)

Permutation group: *Any subgroup of the symmetric group* $\mathrm{Sym}(S)$.

Theorem (Theorem 2: Cayley's Theorem)

Review from §3.6, I

Definition (Definition 1)

Permutation group: *Any subgroup of the symmetric group* $\mathrm{Sym}(S)$.

Theorem (Theorem 2: Cayley's Theorem)

Every group is isomorphic to a permutation group.

Definition (Definition 4 & Example: Rigid motions of a regular *n*-gon)

Review from §3.6, I

Definition (Definition 1)

Permutation group: *Any subgroup of the symmetric group* $\mathrm{Sym}(S)$.

Theorem (Theorem 2: Cayley's Theorem)

Every group is isomorphic to a permutation group.

Definition (Definition 4 & Example: Rigid motions of a regular ***n*****-gon)**

The nth dihedral group D_n *is the group of rigid motions of a regular n-gon.*

Proposition (Propositions 2-3 & Note 5)

Definition (Definition 1)

Permutation group: *Any subgroup of the symmetric group* $\mathrm{Sym}(S)$.

Theorem (Theorem 2: Cayley's Theorem)

Every group is isomorphic to a permutation group.

Definition (Definition 4 & Example: Rigid motions of a regular *n*-gon)

The nth dihedral group D_n is the group of rigid motions of a regular n-gon.

Proposition (Propositions 2-3 & Note 5)

$D_n = \{a^k, a^k b \mid 0 \leq k < n\}$, *where* $a^n = e, b^2 = e, ba = a^{-1}b$ *and* $n \geq 3$.
a : *A counterclockwise rotation about the center through* $360/n$ *degrees.*
b : *A a flip about the line of symmetry through position number* 1.

Review from §3.6, II

Example (Slides 14-16 of 23)

Subgroups of D_3 and D_4: Subgroup diagrams of D_3 and D_4

Note (Homework 7 (3)-(4))

Review from §3.6, II

Example (Slides 14-16 of 23)

Subgroups of D_3 and D_4: Subgroup diagrams of D_3 and D_4

Note (Homework 7 (3)-(4))

In D_n, $o(a^k) = \dfrac{n}{\gcd(k, n)}$ and $o(a^k b) = 2$ for all $0 \leq k < n$.

Definition (Proposition 5 & Definition 5)

Example (Slides 14-16 of 23)

Subgroups of D_3 and D_4: Subgroup diagrams of D_3 and D_4

Note (Homework 7 (3)-(4))

In D_n, $o(a^k) = \dfrac{n}{\gcd(k, n)}$ and $o(a^k b) = 2$ for all $0 \leq k < n$.

Definition (Proposition 5 & Definition 5)

*The **alternating group** A_n is the set of all even permutations of S_n.*

Theorem (Theorem 6)

Example (Slides 14-16 of 23)

Subgroups of D_3 and D_4: Subgroup diagrams of D_3 and D_4

Note (Homework 7 (3)-(4))

In D_n, $o(a^k) = \dfrac{n}{\gcd(k,n)}$ and $o(a^k b) = 2$ for all $0 \leq k < n$.

Definition (Proposition 5 & Definition 5)

*The **alternating group** A_n is the set of all even permutations of S_n.*

Theorem (Theorem 6)

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$

Definition (Definition 7)

The **decomposition type** *of a permutation σ in S_n is the list of all the cycle lengths involved in a decomposition of σ into disjoint cycles.*

Example (Slides 19-20 of 23)

Definition (Definition 7)

The **decomposition type** *of a permutation σ in S_n is the list of all the cycle lengths involved in a decomposition of σ into disjoint cycles.*

Example (Slides 19-20 of 23)

List all the elements of A_3 and A_4.

Example (Proposition 6: The converse of Lagrange's theorem is false)

Definition (Definition 7)

The **decomposition type** *of a permutation σ in S_n is the list of all the cycle lengths involved in a decomposition of σ into disjoint cycles.*

Example (Slides 19-20 of 23)

List all the elements of A_3 and A_4.

Example (Proposition 6: The converse of Lagrange's theorem is false)

A_4 has no subgroup of order 6.

Theorem (Definition 8 & Theorem 10)

Review from §3.6, III

Definition (Definition 7)

The **decomposition type** *of a permutation σ in S_n is the list of all the cycle lengths involved in a decomposition of σ into disjoint cycles.*

Example (Slides 19-20 of 23)

List all the elements of A_3 and A_4.

Example (Proposition 6: The converse of Lagrange's theorem is false)

A_4 has no subgroup of order 6.

Theorem (Definition 8 & Theorem 10)

Let $\Delta_n = \prod_{1 \le i < j \le n} (x_i - x_j)$ *and* $\sigma(\Delta_n) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)})$.

Then $\sigma \in A_n \Leftrightarrow \sigma(\Delta_n) = \Delta_n$.

Review from §3.7, I

Definition (Definition 1)

$\phi : G_1 \to G_2$ is a **homomorphism** *if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.*

Note (Note 1)

Review from §3.7, I

Definition (Definition 1)

$\phi : G_1 \to G_2$ is a **homomorphism** *if $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.*

Note (Note 1)

Every isomorphism is a homomorphism, but conversely not true.

Proposition (Propositions 1-2: Let $\phi : G_1 \to G_2$ be a homomorphism.)

Review from §3.7, I

Definition (Definition 1)

$\phi : G_1 \to G_2$ *is a* **homomorphism** *if* $\phi(a * b) = \phi(a) \cdot \phi(b)$ *for all* $a, b \in G_1$.

Note (Note 1)

Every isomorphism is a homomorphism, but conversely not true.

Proposition (Propositions 1-2: Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) $\phi(e_1) = e_2$;

(b) $\phi(a^{-1}) = (\phi(a))^{-1}$ *for all* $a \in G_1$;

(c) $\phi(a^n) = (\phi(a))^n$ *for all* $a \in G_1$ *and all* $n \in \mathbf{Z}$;

(d) *if* $o(a) = n$ *in* G_1, *then* $o(\phi(a))$ *in* G_2 *is a divisor of* n.

(e) ϕ *is onto: If* G_1 *is abelian (cyclic), then* G_2 *is also abelian (cyclic).*

Example (Examples 7-8)

Review from §3.7, I

Definition (Definition 1)

$\phi : G_1 \to G_2$ *is a* **homomorphism** *if* $\phi(a * b) = \phi(a) \cdot \phi(b)$ *for all* $a, b \in G_1$.

Note (Note 1)

Every isomorphism is a homomorphism, but conversely not true.

Proposition (Propositions 1-2: Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) $\phi(e_1) = e_2$;

(b) $\phi(a^{-1}) = (\phi(a))^{-1}$ *for all* $a \in G_1$;

(c) $\phi(a^n) = (\phi(a))^n$ *for all* $a \in G_1$ *and all* $n \in \mathbf{Z}$;

(d) *if* $o(a) = n$ *in* G_1, *then* $o(\phi(a))$ *in* G_2 *is a divisor of* n.

(e) ϕ *is onto: If* G_1 *is abelian (cyclic), then* G_2 *is also abelian (cyclic).*

Example (Examples 7-8)

If $G_1 = \langle a \rangle$ *is cyclic, then* $\phi : G_1 \to G_2$ *is completely determined by* $\phi(a)$.

Review from §3.7, II

Definition (Definition 9 & Note 2 & Theorem 10)

$\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} \subseteq G_1$ & $\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\} \subseteq G_2$

Theorem (Theorem 11)

Definition (Definition 9 & Note 2 & Theorem 10)

$\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} \subseteq G_1$ & $\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\} \subseteq G_2$

Theorem (Theorem 11)

ϕ *is one-to-one* $\Leftrightarrow \ker(\phi) = \{e_1\}$ & ϕ *is onto* $\Leftrightarrow \mathrm{im}(\phi) = G_2$

Example (ϕ's between cyclic groups: Example 8 & Propositions 3-5)

Review from §3.7, II

Definition (Definition 9 & Note 2 & Theorem 10)

$\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} \subseteq G_1$ & $\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\} \subseteq G_2$

Theorem (Theorem 11)

ϕ is one-to-one $\Leftrightarrow \ker(\phi) = \{e_1\}$ & *ϕ is onto* $\Leftrightarrow \mathrm{im}(\phi) = G_2$

Example (ϕ's between cyclic groups: Example 8 & Propositions 3-5)

(1) *Define $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(x) = mx$.*

(2) *Define $\phi : \mathbf{Z} \to \mathbf{Z}_n$ by $\phi(x) = [mx]_n$.*

(3) *Define $\phi : \mathbf{Z}_n \to \mathbf{Z}$ by $\phi([x]_n) = 0$.* *This ϕ is the only one.*

(4) *Define $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ by $\phi([x]_n) = [mx]_k$.* *ϕ is well-defined $\Leftrightarrow k|mn$.*

Review from §3.7, III

Definition (Definition 12)

Normal subgroup *H of G: If $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.*

Example (Proposition 6 & Example 13)

Review from §3.7, III

Definition (Definition 12)

Normal subgroup *H of G: If $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.*

Example (Proposition 6 & Example 13)

(1) $\ker(\phi)$ *is a normal subgroup of G_1.*

(2) *If $H = G$ or $H = \{e\}$, then H is normal.*

(3) *Any subgroup of an abelian group is normal.*

Proposition (Proposition 7: Let $\phi : G_1 \to G_2$ be a homomorphism.)

Review from §3.7, III

Definition (Definition 12)

Normal subgroup *H of G: If $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.*

Example (Proposition 6 & Example 13)

(1) $\ker(\phi)$ *is a normal subgroup of G_1.*

(2) *If $H = G$ or $H = \{e\}$, then H is normal.*

(3) *Any subgroup of an abelian group is normal.*

Proposition (Proposition 7: Let $\phi : G_1 \to G_2$ be a homomorphism.)

(a) *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.*
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.*
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

Review from §3.7, IV

Theorem (Definition 14 & Proposition 8 & Theorem 15)

Let $\phi : G_1 \to G_2$ *be a homomorphism. Define* $\overline{\phi} : G_1/\phi \to \phi(G_1)$ *by* $\overline{\phi}([a]_\phi) = \phi(a)$, *for all* $[a]_\phi \in G_1/\phi$. *Then* $\overline{\phi}$ *is a group isomorphism.*

Example (Slides 20-21 of 23)

Theorem (Definition 14 & Proposition 8 & Theorem 15)

Let $\phi : G_1 \to G_2$ be a homomorphism. Define $\overline{\phi} : G_1/\phi \to \phi(G_1)$ by $\overline{\phi}([a]_\phi) = \phi(a)$, for all $[a]_\phi \in G_1/\phi$. Then $\overline{\phi}$ is a group isomorphism.

Example (Slides 20-21 of 23)

(1) *Reprove "Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$".*

(2) *Reprove "Cayley's Theorem: Every group $G \cong$ a permutation group".*

Proposition (Proposition 9: Let ϕ be a homomorphism. TFAE:)

Review from §3.7, IV

Theorem (Definition 14 & Proposition 8 & Theorem 15)

Let $\phi : G_1 \to G_2$ be a homomorphism. Define $\overline{\phi} : G_1/\phi \to \phi(G_1)$ by $\overline{\phi}([a]_\phi) = \phi(a)$, for all $[a]_\phi \in G_1/\phi$. Then $\overline{\phi}$ is a group isomorphism.

Example (Slides 20-21 of 23)

(1) *Reprove "Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$".*

(2) *Reprove "Cayley's Theorem: Every group $G \cong$ a permutation group".*

Proposition (Proposition 9: Let ϕ be a homomorphism. TFAE:)

(1) $\phi(a) = \phi(b)$; (2) $ab^{-1} \in \ker(\phi)$; (3) $a = kb$ for some $k \in \ker(\phi)$;
(2)′ $b^{-1}a \in \ker(\phi)$; (3)′ $a = bk$ for some $k \in \ker(\phi)$.

Theorem (Remark 1: Fundamental Homomorphism Theorem)

Theorem (Definition 14 & Proposition 8 & Theorem 15)

Let $\phi : G_1 \to G_2$ be a homomorphism. Define $\overline{\phi} : G_1/\phi \to \phi(G_1)$ by $\overline{\phi}([a]_\phi) = \phi(a)$, for all $[a]_\phi \in G_1/\phi$. Then $\overline{\phi}$ is a group isomorphism.

Example (Slides 20-21 of 23)

(1) *Reprove "Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$".*

(2) *Reprove "Cayley's Theorem: Every group $G \cong$ a permutation group".*

Proposition (Proposition 9: Let ϕ be a homomorphism. TFAE:)

(1) $\phi(a) = \phi(b)$; (2) $ab^{-1} \in \ker(\phi)$; (3) $a = kb$ *for some* $k \in \ker(\phi)$;
(2)′ $b^{-1}a \in \ker(\phi)$; (3)′ $a = bk$ *for some* $k \in \ker(\phi)$.

Theorem (Remark 1: Fundamental Homomorphism Theorem)

Let $\phi : G_1 \to G_2$ be a homomorphism. Then $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$.

Review from §3.8, I

Definition (Definition 5 & Corollary 4 & Note 3)

Left coset of H in G: $\{aH \mid a \in G\}$. Right coset of H in G: $\{Ha \mid a \in G\}$.
Index $[G : H]$ *of H in G: The number of left (right) cosets of H in G.*

Note (Note 3)

Review from §3.8, I

Definition (Definition 5 & Corollary 4 & Note 3)

Left coset of H in G: $\{aH \mid a \in G\}$. Right coset of H in G: $\{Ha \mid a \in G\}$.
Index $[G : H]$ *of H in G: The number of left (right) cosets of H in G.*

Note (Note 3)

There is a one-to-one correspondence between left cosets and right cosets.

Proposition (Proposition 1 & Note 2: TFAE:)

Review from §3.8, I

Definition (Definition 5 & Corollary 4 & Note 3)

Left coset of H in G: $\{aH \mid a \in G\}$. Right coset of H in G: $\{Ha \mid a \in G\}$.
Index $[G : H]$ *of H in G: The number of left (right) cosets of H in G.*

Note (Note 3)

There is a one-to-one correspondence between left cosets and right cosets.

Proposition (Proposition 1 & Note 2: TFAE:)

(1) $aH = bH$; (2) $aH \subseteq bH$; (3) $a \in bH$; (4) $b^{-1}a \in H$;

(2)′ $bH \subseteq aH$; (3)′ $b \in aH$; (4)′ $a^{-1}b \in H$.

Proposition (Proposition 2: TFAE:)

Review from §3.8, I

Definition (Definition 5 & Corollary 4 & Note 3)

Left coset of H in G: $\{aH \mid a \in G\}$. Right coset of H in G: $\{Ha \mid a \in G\}$.
Index $[G : H]$ *of H in G: The number of left (right) cosets of H in G.*

Note (Note 3)

There is a one-to-one correspondence between left cosets and right cosets.

Proposition (Proposition 1 & Note 2: TFAE:)

(1) $aH = bH$; (2) $aH \subseteq bH$; (3) $a \in bH$; (4) $b^{-1}a \in H$;

(2)′ $bH \subseteq aH$; (3)′ $b \in aH$; (4)′ $a^{-1}b \in H$.

Proposition (Proposition 2: TFAE:)

(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;

(2)′ $Hb \subseteq Ha$; (3)′ $b \in Ha$; (4)′ $ba^{-1} \in H$.

Example (Proposition 3)

The left coset aH has the same number of elements as H.

Example (Examples 6-9 & Question 1)

Review from §3.8, II

Example (Proposition 3)

The left coset aH has the same number of elements as H.

Example (Examples 6-9 & Question 1)

Algorithm for listing the left cosets of a given subgroup H of a finite group:

(1) *The first coset we can identify is H itself.*

(2) *If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.*

(3) *For the next coset we choose any element not in H or aH (if possible).*

(4) *Continuing in this way provides a method for listing all cosets.*

Remark

Review from §3.8, II

Example (Proposition 3)

The left coset aH has the same number of elements as H.

Example (Examples 6-9 & Question 1)

Algorithm for listing the left cosets of a given subgroup H of a finite group:

(1) *The first coset we can identify is H itself.*

(2) *If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.*

(3) *For the next coset we choose any element not in H or aH (if possible).*

(4) *Continuing in this way provides a method for listing all cosets.*

Remark

The above two Examples also hold for the right cosets of H.

Note (Slide 12 of 35)

Review from §3.8, II

Example (Proposition 3)

The left coset aH has the same number of elements as H.

Example (Examples 6-9 & Question 1)

Algorithm for listing the left cosets of a given subgroup H of a finite group:

(1) *The first coset we can identify is H itself.*

(2) *If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.*

(3) *For the next coset we choose any element not in H or aH (if possible).*

(4) *Continuing in this way provides a method for listing all cosets.*

Remark

The above two Examples also hold for the right cosets of H.

Note (Slide 12 of 35)

For abelian groups, left cosets and right cosets are always the same.

Theorem (Theorem 11)

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

Definition (Definition 12)

Review from §3.8, III

Theorem (Theorem 11)

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

Definition (Definition 12)

If N is a normal subgroup of G, then the group of left cosets of N in G is called the **factor group** *of G determined by N. It will be denoted by G/N.*

Example (Example 13: Order of an element in the factor group G/N)

Review from §3.8, III

Theorem (Theorem 11)

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

Definition (Definition 12)

If N is a normal subgroup of G, then the group of left cosets of N in G is called the **factor group** *of G determined by N. It will be denoted by G/N.*

Example (Example 13: Order of an element in the factor group G/N)

The order of aN is the smallest positive integer n such that $a^n \in N$.

Review from §3.8, IV

Proposition (Proposition 4: Let N be a normal subgroup of G.)

(a) *The natural projection* $\pi : G \to G/N$ *defined by* $\pi(x) = xN$, *for all* $x \in G$, *is a group homomorphism, and* $\ker(\pi) = N$.

(b) *There is a one-to-one correspondence between*

$$\{\text{subgroups } K \text{ of } G/N\} \longleftrightarrow \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Under this correspondence, normal subgroups $\longleftrightarrow$ *normal subgroups.*

Proposition (Proposition 5)

Review from §3.8, IV

Proposition (Proposition 4: Let N be a normal subgroup of G.)

(a) *The natural projection* $\pi : G \to G/N$ *defined by* $\pi(x) = xN$, *for all* $x \in G$, *is a group homomorphism, and* $\ker(\pi) = N$.

(b) *There is a one-to-one correspondence between*

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Under this correspondence, normal subgroups $\longleftrightarrow$ *normal subgroups.*

Proposition (Proposition 5)

H is normal if and only if its left and right cosets coincide.

Example (Slides 22-24 of 35)

Review from §3.8, IV

Proposition (Proposition 4: Let N be a normal subgroup of G.)

(a) *The natural projection* $\pi : G \to G/N$ *defined by* $\pi(x) = xN$, *for all* $x \in G$, *is a group homomorphism, and* $\ker(\pi) = N$.

(b) *There is a one-to-one correspondence between*

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Under this correspondence, normal subgroups $\longleftrightarrow$ *normal subgroups.*

Proposition (Proposition 5)

H is normal if and only if its left and right cosets coincide.

Example (Slides 22-24 of 35)

This gives us a technique for determining that a subgroup is normal or not.

Fact (Slides 23 of 35: A useful fact)

Review from §3.8, IV

Proposition (Proposition 4: Let N be a normal subgroup of G.)

(a) *The natural projection* $\pi : G \to G/N$ *defined by* $\pi(x) = xN$*, for all* $x \in G$*, is a group homomorphism, and* $\ker(\pi) = N$*.*

(b) *There is a one-to-one correspondence between*

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Under this correspondence, normal subgroups $\longleftrightarrow$ *normal subgroups.*

Proposition (Proposition 5)

H is normal if and only if its left and right cosets coincide.

Example (Slides 22-24 of 35)

This gives us a technique for determining that a subgroup is normal or not.

Fact (Slides 23 of 35: A useful fact)

Subgroups of index 2 are normal.

Review from §3.8, V

Theorem (Theorem 15: Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

Remark (How to use Fundamental Homomorphism Theorem)

Review from §3.8, V

Theorem (Theorem 15: Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

Remark (How to use Fundamental Homomorphism Theorem)

To show $G_1/\ker(\phi) \cong \phi(G_1)$:

(i) *Show that ϕ is well-defined.*

(ii) *Show that ϕ is a homomorphism.*

(iii) *Find $\phi(G_1)$. In particular, $\phi(G_1) = G_2$ if ϕ is onto.*

(iv) *Find $\ker(\phi)$. In particular, $\ker(\phi) = \{e_1\}$ if ϕ is one-to-one.*

Definition (Remark 2 & Definition 16 & Example 17)

Review from §3.8, V

Theorem (Theorem 15: Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

Remark (How to use Fundamental Homomorphism Theorem)

To show $G_1/\ker(\phi) \cong \phi(G_1)$:

(i) *Show that ϕ is well-defined.*

(ii) *Show that ϕ is a homomorphism.*

(iii) *Find $\phi(G_1)$. In particular, $\phi(G_1) = G_2$ if ϕ is onto.*

(iv) *Find $\ker(\phi)$. In particular, $\ker(\phi) = \{e_1\}$ if ϕ is one-to-one.*

Definition (Remark 2 & Definition 16 & Example 17)

The nontrivial group G is called a **simple** *group if it has no proper nontrivial normal subgroups. For example, $\mathbf{Z}_p$ is simple for any prime p.*

Example (Proposition 6: Factor groups of direct products)

Let N_i be a normal subgroup of G_i with $i \in \{1, 2\}$. Then $N_1 \times N_2$ is a normal subgroup of the direct product $G_1 \times G_2$ and

$$(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2).$$

Example (Proposition 7: Internal direct product)

Review from §3.8, VI

Example (Proposition 6: Factor groups of direct products)

Let N_i be a normal subgroup of G_i with $i \in \{1, 2\}$. Then $N_1 \times N_2$ is a normal subgroup of the direct product $G_1 \times G_2$ and

$$(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2).$$

Example (Proposition 7: Internal direct product)

A group G with subgroups H and K is called the **internal direct product of H and K** *if*

(i) *H and K are normal in G,*

(ii) *$H \cap K = \{e\}$, and*

(iii) *$HK = G$.*

Then in this case $G \cong H \times K$.