MATH 3175 Notes

Xin Guan

1. 01.22

   (a) Definition: 7.1
   Function $f : X \to Y$ is bijection if f is both surjection(on to) and injection (one to one)

   (b) Theorem: 7.2
   $f : X \to Y$ is bijection $\Leftrightarrow$
   $\exists g : Y \to X$ s.t. $g \circ f = id_x, f \circ g = id_y$ (id_x means identity)
   Such g is called the inverse of f. Denoted by f^{-1}

   (c) Recall:
   ◦ Composition of two injective functions is injective.
   ◦ Composition of two surjective functions is surjective.
   ◦ Composition of two bijective functions is bijective.

   (d) Definition: 7.4 Permutation:
   Permutation on set X is a bijection $f : X \to X$

   (e) prop 7.5
      i. if $f : X \to X$ is a permutation then $\exists f^{-1} : X \to X$ which is also permutation.
      ii. composition of two permutation is again a permutation.

   (f) Definition: 7.6
   if $X = \{1, 2, \ldots, n\}$ then, $S_n := \{\text{all permutation on } X\}$

   (g) EX 7.7
   $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$
   $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}$
   Find $\alpha\beta$ (composition of α and β), α^{-1}
   Solution:
   $(\alpha\beta)(1) = \alpha(\beta(1)) = \alpha(5) = 5$
   $(\alpha\beta)(2) = \alpha(\beta(2)) = \alpha(1) = 3$
   $(\alpha\beta)(3) = \alpha(\beta(3)) = \alpha(4) = 2$
   $(\alpha\beta)(4) = \alpha(\beta(4)) = \alpha(5) = 1$
   $(\alpha\beta)(5) = \alpha(\beta(5)) = \alpha(2) = 4$
   Then, $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$

$\alpha^{-1} = \begin{pmatrix} 3 & 4 & 1 & 2 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$
rearrange:
$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$

(h) Homework: 2.1 9(b)
$g : \mathbf{Z}_8 \Rightarrow \mathbf{Z}_12, g([x]_8) = [6x]_12$ show that g is well defined.
Solution:

Proof. Suppose $[x]_8 = [x']_8$, WTS $g([x]_8) = g([x']_8)$
Let $[x]_8 = [x']_8$
$\Rightarrow x \equiv x'(mod\ 8)$
$\Rightarrow 8|(x - x')$
$\Rightarrow x - x' = 8 * q$ for some $q \in \mathbf{Z}$
$x = 8 \cdot q + x'$
By definition of g, $g([x]_8) = [6x]_{12}$
Then, $g([x]_8) = [6(8q + x')]_{12} = [48q + 6x']_{12}, g([x']_8) = [6x']_{12}$
WTS $[48q + 6x']_{12} = [6x']_{12}$
Enough to show: $12|(48q + 6x' - 6x')$
Since $48q + 6x' - 6x' = 48q = 12 \cdot 4 \cdot q$
$\Rightarrow 12|12 \cdot 4 \cdot q$
$\Rightarrow 12|(48q + 6x' - 6x')$
$\Rightarrow g([x]_8) = g([x']_8)$ □

2. 01.23

(a) Recall:
DEF: Permutation on set X is a bijection $f : X \to X$
NOTE: S_x = {permutation on X}, S_n = {permutation on {1,2,3, ... n}}
PROPERTIES:
composition of permutation is again a permutation.
identity map: $id : X \to X(id(x) = x)$ is a permutation.
each permutation f there is an inverse f^{-1} such that $f \circ f^{-1} = id, f^{-1} \circ f = id$.

(b) Definition: 8.1 Disjoint cycle decomposition
Suppose $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 8 & 1 & 2 & 6 & 7 & 5 \end{pmatrix}$
= (1 3 8 5 2 4)(6)(7) or (1 3 8 5 2 4) (in cycle notation)

(c) Definition: 8.2
2-cycle $\to$ (i j) $i \neq j$
3-cycle $\to$ (i j k) i,j,k distinct
r-cycle $\to$ $(i_1, i_2, \ldots, i_r)$, $i_1, i_2, \ldots, i_r$ distinct

(d) Example: 8.3
$\alpha = (142), \beta = (13)$ $\alpha \to$ 3-cycle, $\beta \to$ 2-cycle.

(e) identity permutation in S_n

i. (1)(2)...(n)

ii. fixes $\forall i$

iii. 1-cycle (i) fixes i

iv. often we do not note 1-cycle: $\alpha = (142) = (142)(3)$

v. id = (1) = (1)(2)...(n)

(f) Example: 8.5 multiplication of permutation

$\alpha = (142), \beta = (13), \in S_4$

compute - write as a product of disjoint cycles (same as Example: 7.7 with new notation)

$\alpha\beta = (142)(13) = (1342)$

HOWTO: $\beta : 1 \longrightarrow 3$, then $\alpha : 3 \longrightarrow 3$, then (13) now.

$\beta : 3 \longrightarrow 1$, then $\alpha : 1 \longrightarrow 4$, then (134) now.

$\beta : 4 \longrightarrow 4$, then $\alpha : 4 \longrightarrow 2$, then (1342).

Similarly: $\beta\alpha = (13)(142) = (1423)$

(g) Remark: 8.6 In general $\alpha\beta \neq \beta\alpha$

if α, β are disjoint then $\alpha\beta = \beta\alpha$

(h) Definition: 8.7

Order of permutation α is the smallest positive integer n such that $\alpha^n = (1)$ where $\alpha^n = \alpha\alpha\ldots\alpha$ (there are n α's)

(i) Example: 8.8

$\alpha = (142)$

$\alpha^2 = \alpha\alpha = (142)(142) = (124)$

$\alpha^3 = \alpha\alpha\alpha = (142)(142)(142) = (142)(124) = (1)(2)(4) = (1)$

Then $|\alpha| = 3$. Order of α is 3.

$\beta = (13)$

$\beta^2 = (13)(13) = (1)$

Then $|\beta| = 2$

(j) Prop: 8.10 Order of an r-cycle is r

(k) Example: 8.11 $\alpha = (143)(25)$

$|\alpha| = LCM(|(143)|, |(25)|) = LCM(3, 2) = 6$

(l) Prop: 8.12 Let α, β be two disgoint permutation. Then $|\alpha\beta| = LCM(|\alpha|, |\beta|)$

(m) Possible Disjoint Cycles

Partition of 6	Disjoint cycles	Example	Order	# different permutations
6	6 cycle	(132654)	6	$\frac{6!}{6} = 5!$
5 + 1	5 cycle, 1 cycle	(13465)(2)	5	$\binom{6}{5}\frac{5!}{5}\frac{1!}{1} = \binom{6}{5} \cdot 4!$
4 + 2	4 cycle, 2 cycle	(1354)(26)	4	$\binom{6}{4}\binom{2}{2}\frac{4!}{4}\frac{2!}{2}$
4 + 1 + 1	(4,1,1)	(1354)(2)(6)	4	$\binom{6}{4}\frac{4!}{4}\binom{2}{1}\frac{2!}{2}\binom{1}{1}\frac{1!}{1}\frac{1}{2!}$

NOTE: We need to divide by the order since (123) = (231) = (312). We need to eliminate repeative terms.

Also, we need to eliminate possible arrangement of cycles of the same length. In (4,1,1) the 1 cycles can appear in different orders but representing the same disjoint cycles.

Notation: (6), (5,1), (4,2), (4,1,1), (3,3), (3,2,1), (3,1,1,1), (2,2,2), (2,2,1,1), (2,1,1,1,1), (1,1,1,1,1,1)

3. 01.27 GROUPS!

(a) Definition: 9.11 G set

i. $G \times G \to *G$ binary operation: $(x,y) \to x * y$

ii. associative law:
$(x*y)*z = x*(y*z), \forall x,y,z \in G$

iii. $\exists e \in G$ is identity s.t. $e*x = x, x*e = x, \forall x \in G$

iv. $\forall x \in G, \exists y \in G s.t. x*y = e, y*x = e$
and y is called inverse of x. (it is not necessarily unique)

v. $x*y = y*x \forall x,y \in G$

If only the **first 2** properties hold, it is called **semigroups**.

If only the **first 3** properties hold, it is called **monoid**.

If only the **first 4** properties hold, it is called **group**.

If only the **all** properties hold, it is called **Commutative group (Abelian group)**.

(b) **Examples:**

i. $(\mathbb{Z},+)$

A. $x,y \in \mathbb{Z}, x+y \in \mathbb{Z}$

B. $(x+y)+z = x+(y+z)$

C. $x+0 = x, 0+x = x, \forall x \in \mathbb{Z}$ therefore $e = 0$

D. $x+y = 0, y+x = 0 \to y = -x$

E. $x+y = y+x$
Then, $(\mathbb{Z},+)$ is **Abelian group**

ii. $(\mathbb{Z},\cdot)$

A. $x,y \in \mathbb{Z}, x\cdot y \in \mathbb{Z}$

B. $(x\cdot y)\cdot z = x\cdot(y\cdot z)$

C. $x\cdot 1 = x, 1\cdot x = x, \forall x \in \mathbb{Z}$ therefore $e = 1$

D. $x\cdot y = 1, y\cdot x = 1 \to$ NO inverse in general. {1,-1} have inverse

E. $x\cdot y = y\cdot x$
Then, $(\mathbb{Z},+)$ is a **commutative monoid** but not a **group**

iii. $(\mathbb{Z},-)$

A. $x,y \in \mathbb{Z}, x-y \in \mathbb{Z}$

B. $(x-y)-z \neq x-(y-z)$ example: $2-(1-5) \neq (2-1)-5$
Then, $(\mathbb{Z},+)$ is not even a **semigroup**.
We don't need to check following properties since it does not have an operation. All the following properties are target at the operation.

iv. $(\mathbb{Z}_6,+_6)$

A. $[x]_6,[y]_6 \in \mathbb{Z}_6, [x]_6+[y]_6 = [x+y]_6 \in \mathbb{Z}_6$

B. $(x+y)+z = x+(y+z)$

C. $e = [0]_6$

D. inverse: $[-x]_6 + [x_6] = e$

E. $[x]_6+[y]_6 = [y]_6+[x]_6$
$(\mathbb{Z}_6,+_6)$ is **Abelian group**

v. $(\mathbb{Z}_6, \cdot_6)$

A. $[x]_6, [y]_6 \in \mathbb{Z}_6, [x]_6 \cdot [y]_6 = [x \cdot y]_6 \in \mathbb{Z}_6$

B. works

C. $e = [1]_6$

D. y does not always exists. only when $gcd(x, 6) = 1$ inverse exists.

E. $[x]_6 \cdot [y]_6 = [y]_6 \cdot [x]_6$

$(\mathbb{Z}_6, +_6)$ is **commutative monoid** but not a **group**

vi. $(\mathbb{Z}_6^{\times}, \cdot_6)$

$\mathbb{Z}_6^{\times} = \{[x]_6 \in \mathbf{Z}_6 | gcd(x, 6) = 1\}$

$\mathbb{Z}_6^{\times} = \{[1]_6, [5]_6\}$

A. $[x]_6, [y]_6 \in \mathbb{Z}_6, [x]_6 \cdot [y]_6 = [x \cdot y]_6 \in \mathbb{Z}_6$

B. works

C. $e = [1]_6$

D. holds!

E. $[x]_6 \cdot [y]_6 = [y]_6 \cdot [x]_6$

$(\mathbb{Z}_6^{\times}, +_6)$ is **Abelian group**

vii. $(M_2(\mathbb{R}), +)$, $M_2(\mathbb{R}) = M \in \mathbb{R}^{2\times 2}$

A. Yes, there is a closed binary operation.

B. associate law is inherted from +

C. $e = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

D. inverses exist.

E. commutative property holds.

$(M_2(\mathbb{R}), +)$ is **Abelian group**

viii. $(M_2(\mathbb{R}), \cdot)$

A. Yes, there is a closed binary operation.

B. (AB)C = A(BC)

C. $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

D. inverses not necessaily exist. only $det(x) \neq 0$

E. commutative property dose not hold.

$(M_2(\mathbb{R}), +)$ is **monoid**

ix. $(GL_2(\mathbb{R}), \cdot)$ GL: general linear group – determinants is $\neq 0$

A. $det(AB) = det(A)det(B) \neq 0$

B. (AB)C = A(BC)

C. $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

D. inverse exists

E. $AB \neq BA$ in general

$(GL_2(\mathbb{R}), \cdot)$ is **Abelian group**

x. $(S_3, \cdot)$

$S_3 = \{(123), (132), (12), (13), (23), (1)\}$

A. $\alpha \cdot \beta = \alpha\beta$

B. associative law good
C. $e = (1)$
D. inverse exists $(123)^{-1} = (321)\dots$

4. 01.29

(a) Recall: 10.2
monoids(prop 1,2,3) $\subseteq$ semigroups (prop 1,2)
groups(prop 1,2,3,4) $\subseteq$ monoids(prop 1,2,3)
Abelian groups(prop 1,2,3,4,5) $\subseteq$ groups(prop 1,2,3,4)

(b) 10.3 Let G be a monoid, then G has a unique identity element e

Proof. By definition of monoid, $\exists e \in G$ s.t $ex = x, xe = x, \forall x \in G$
Suppose that e and e' are identity of G. i.e $ex = x, xe = x, e'x = x, xe' = x$
WTS $e = e'$
$e = ee'(e'$ is identity$) = e'(e$ is identity$)$
NOTE: we are using symmetric and transitive property of = $\square$

(c) Prop: 10.4
Leg G be a group. Let $x \in G$ then $\exists! y \in G$ s.t. $xy = e$ and $yx = e$

Proof. let $x \in G$ by definition, $\exists y \in G$ s.t. $xy = e, yx = e$
Suppose y and $y' \in G$ s.t. $xy = e, yx = e; xy' = e, y'x = e$
WTS $y = y'$
by assumption:

$$xy = e$$

operate y' on the left:

$$y'(xy) = y'e$$

associate law:

$$(y'x)y = y'e$$

by assumption:

$$y = y'e$$

property of e:

$$y = y'$$

Therefore, $\exists! y \in G$ s.t. $xy = e$ and $yx = e$ $\square$

(d) Prop: 10.5
Let G be a group then cancellation laws hold. i.e.

$$ax = ay \Rightarrow x = y$$

$$xa = ya \Rightarrow x = y$$

Proof.

$$ax = ay$$

Let a^{-1} be the inverse of a, then operate a^{-1} on both sides.

$$a^{-1}(ax) = a^{-1}(ay)$$

associative law:

$$(a^{-1}a)x = (a^{-1}a)y$$

property of inverse:

$$ex = ey$$

property of identity:

$$x = y$$

Therefore $ax = ay \Rightarrow x = y$
similarly, $xa = ya \Rightarrow x = y$ □

(e) Definition: 10.6 Subgroup
Let G be a group. A subgroup of G is H if:
- $H \subset G$ is a subset of G
- H is a group under the same operation. i.e. $(H, *)$ is a group

(f) Example: 10.7
G = $(\mathbf{Z}, +)$, H = $(3\mathbf{Z}, +)$

(g) Example: 10.8
G = $(\mathbf{Z}_6, +_6)$, H = $(3\mathbf{Z}, +)$
H = $(\{[2],[4],[0]\}, +_6)$
Need to show: 1. H is a subset 2. (H,$+_6$) is a group
Just write a cayley table.

5. 01.30

(a) Definition: 11.1
Let $(G, *)$ be a group, then H is a subgroup of G if
- $H \subseteq G$, H is a subset of G
- $(H, *)$ is a group.

(b) Example: 11.2
$G = S_3 = \{(1),(123),(132),(12),(13),(23)\}$
Operation - multiplication of permutation.
$H = \{(1),(123),(132)\}$ is a subgroup of G
H is a proper subgroup of $G \Leftrightarrow H \neq G$
- S_0 $H \subset G$
- S_{00} H is nonempty (i.e $H \neq \emptyset$) Usually, we check for identity.
- S_1 H is closed under operation
- S_2 H has inverse

How To Check:

- H is a subset of G: by def of elements of H
- H is a group under operation: 1. closed 2. associative 3. identity 4. inverse

When checking small sets, just use Cayley Table:

	(1)	(123)	(132)
(1)	(1)	(123)	(132)
(123)	(123)	(132)	(1)
(132)	(132)	(1)	(123)

It is closed. Identity: e = (1). Inverse exists.

(c) Remark: 11.3
Let $(G,*)$ be a group then $(G,*)$ is a subgroup of itself.

(d) Definition: 11.4
Proper subgroup of G is a subgroup H s.t. $H \neq G$

6. 02.03

(a) Remark: 12.2 We proved that if G is a group, $x \in G$, then $\exists!$ inverse $y \in G$

(b) Prop: 12.3
Leg G be a group, let $x \in G$. If $xy = e$, then $y = x^{-1}$.
i.e. If $xy = e$, then $yx = e$

- since G is a group $\exists! x^{-1} \in G$, multiply by x^{-1} on the left.

$$x^{-1}(xy) = x^{-1}e$$

$x^{-1}(xy) = (x^{-1}x)y = ey = y = x^{-1}$

(c) 12.4 Restating 12.3:
Let G be a group, $x \in G$, it is enough to check $xy = e$ to claim that $y = x^{-1}$

(d) 12.5 Let G be a group. Suppose $x^n = e$ for some n postive integer. Then $x^{-1} = x^{n-1}$.

(e) Definition: 12.6 Let G be a group. Let $x \in G$ then order of x, denoted by $|x|$ is the **smallest positive integer** n s.t. $x^n = e$. If such n does not exist then $|x| = \infty$

(f) Definition: 12.7
G is a Group, $x \in G$.

i. $x^n := xxx \dots x$ (n-times) if n is positive integer.
ii. $x^0 := e$
iii. x^{-1} :=the inverse
iv. $x^{-n} := (x^{-1})^n = (x^n)^{-1}$

Then x^n is defined on $\mathbb{Z}$

(g) Prop: 12.8 G a group, $x \in G$ then
$x^n x^m = x^{n+m}, \forall n, m \in \mathbb{Z}$

Proof.
- n, m positive integer
$x^n x^m = x \dots x$ (n-times) $x \dots x$ (m-times) $= x \dots x$(n+m times)
Or use induction.

- ...

Just use definition 12.7 to check all. □

(h) H is asubgroup of G if
- H is a subset of G
- $e \in H$ (check for not empty)
- $a, b \in H$ then $ab \in H$
- $a \in H$ then $a^{-1} \in H$

(i) Remark: 12.10 If H is finite, then it is enough to check:
- H is subset of G
- H closed under operation

Proof. $x \in H$ then we have to take $x, x^1, x^2 \ldots, x^n \ldots$ since we are closed under operation.
H is finite $\Rightarrow \exists m, n$ s.t. $x^n = x^m$
Suppose $n \geq m, x^n = x^m$,

$$x^n = x^m x^{n-m} = x^m$$
$$\Rightarrow x^m x^{n-m} = x^m e$$
$$\Rightarrow x^{n-m} = e$$

Then it guarantees that there is identity in H □

(j) Definition: 12.12 G a group, $x \in G$
$< x >:= \{x^n | n \in \mathbb{Z}\}$

(k) Prop: 12.13 $< x >$ is a subgroup of G

Proof. 1. WTS $< x > \subset G$
- Positive power: G is closed, then $x^2 = xx$ then x^2 is in G By induction, x^n is in G for all positive n.
- 0 power: $x^0 = e$, e is in G since G is a group.
- negative power: x^{-1} is in G, then x^{-n} is in G (the same reason as the positive powers)

Then $< x > \subset G$

2. WTS $a, b \in < x >$, then $ab \in < x >$
$a \in < x > \Rightarrow a = x^n, n \in \mathbb{Z}$
$b \in < x > \Rightarrow b = x^m, m \in \mathbb{Z} \Rightarrow ab = x^n x^m = x^{n+m} \in < x >$

3.a^{-1} in $< x >$ □

7. 02.06

(a) Definition: 14.1 Let G be a group, let $x \in G$, then conjugate of x by $g \in G$ is gxg^-1

(b) Remark: 14.2

- $(13254)^{-1} = (45231)$
- $(13)^{-1} = (31) = (13)$
- $(ij)^{-1} = (ji)$
- $a^n = e \to a^{-1} = a^{n-1}$

(c) Example: 14.3 $G = S_4$. Find a conjugate of $x = (143)$
$g = (23)\ gxg^{-1} = (23)(143)(23)^{-1} = (23)(143)(32) = (142)(3) = (142)$

(d) Example: Let $G = S_3$ Find all conjugate of $x = (13)$
Since $S_3 = \{(1), (12), \dots\}$
$(1)(13)(1)^{-1} = (13)$
$(12)(13)(12)^{-1} = (23)$
$(13)(13)(13)^{-1} = (13)$
$(23)(13)(23)^{-1} = (12)$
$(123)(13)(123)^{-1} = (12)$
$(132)(13)(132)^{-1} = (23)$

(e) Prop: 14.5 Let $\alpha \in S_n$, all conjugate of α = all permutations which have the none disjoint cycle decomposition as α

(f) Example: 14.7 $G = S_5$ $\alpha = (142)(35)$ How many conjugates of α are there in S_5?
i.e. How many permutations in S_5 has the form of (3-cycle)(2-cycle)? $\binom{5}{3}\frac{3!}{3}\binom{2}{2}\frac{2!}{2}$

(g) Prop: Let G be a group, Let $x \sim y$ if x is conjugate to y. Conjugate is an equivalece relation.

(h) Definition: 14.9 Let G be a group, $x \in G$, then conjugate(x):= $\{gxg^{-1} \mid g \in G\}$

(i) Remark: 14.10 Conj. class of x = equivelence class of x under $y \sim z$ if y is conj to z

(j) Example: 14.11 Let $\alpha = (147)(235) \in S_8$. Find the size of conj class (α).

(k) $|\text{conj. class}(\alpha)| = \binom{8}{3}\frac{3!}{3}\binom{5}{3}\frac{2!}{2}\frac{1}{2!}$

(l) Example: 14.12 $G = (\mathbb{Z}_4, +_4)$ Find all conj of $[2]_4$
$[0] + [2] + [-0] = [2]$
$[1] + [2] + [-1] = [1] + [2] + [3] = [2]$
$[2] + [2] + [-2] = [2]$
$[3] + [2] + [-3] = [2]$

(m) Prop: 14.13 Let G be an ebelian group.
Conj. class(x) = {x} |Conj. class(x)| = 1 (property of commutative show that $gxg^{-1} = gg^{-1}x = ex = x$)

(n) Conj. Class(x) = {x} $\Rightarrow$ then x commutes with all $g \in G$
G is disjoint union of its conj classes.

(o) Definition: 14.15 Let G be a group be H be a subgroup of G. Let $g \in G$. Define $gHg^{-1} : \{ghg^{-1} \mid h \in H\}$ This is called conjugate of H by g.

(p) Example: 14.16 Let $G = S_3$ let $H = \{(13), (1)\}$. Find conjugate of H by $g = (123)$
$(123)(13)(123)^{-1} = (123)(13)(321) = (1)(23)(321) = (12)$
$(123)(1)(123)^{-1} = (1)$
$gHg^{-1} = \{(12), (1)\}$

(q) Prop: 14.17 Let G be a goup, Let H be a subgroup of G. Let $g \in G$ then gHg^{-1} is a subgroup of G.

Proof. WTS: gHg^{-1} is a subgroup of G
0. gHg^{-1} is a subset of G.
00. $e \in gHg^{-1}$
1. If $a,b \in gHg^{-1}$, then $ab \in gHg^{-1}$
2. If $a \in gHg^{-1}$, then $a^{-1} \in gHg^{-1}$

- Show gHg^{-1} is a subset of G.
  $\forall h \in H, g \in G, g, h, g^{-1} \in G$, G is closed under operation.
  $\Rightarrow ghg^{-1} \in G$. Then gHg is a subset of G.
- Show $e \in gHg^{-1}$
  Since H is a group, $\Rightarrow e \in H$.
  $geg^{-1} = e \Rightarrow e \in gHg^{-1}$.
- Show If $a,b \in gHg^{-1}$, then $ab \in gHg^{-1}$
  $\exists a', b' \in H$ such that $ga'g^{-1} = a, gb'g^{-1} = b$.
  $ab = ga'g^{-1}gb'g^{-1} = ga'(g^{-1}g)b'g^{-1} = g(a'b')g^{-1}$
  Therefore, $ab \in gHg^{-1}$
- Show If $a \in gHg^{-1}$, then $a^{-1} \in gHg^{-1}$
  $\exists a' \in H$ such that $ga'g^{-1} = a$
  Since H is a group, $a'^{-1} \in H$
  Then, $ga'^{-1}g^{-1} \in gHg^{-1}$.
  $a \cdot ga'^{-1}g^{-1}$
  $= ga'g^{-1}ga'^{-1}g^{-1}$
  $= ga'(g^{-1}g)a'^{-1}g^{-1}$
  $= ga'ea'^{-1}g^{-1}$
  $= ga'a'^{-1}g^{-1}$
  $= g(a'a'^{-1})g^{-1}$
  $= geg^{-1}$
  $= gg^{-1}$
  $= e$
  Therefore, $a^{-1} = ga'^{-1}g^{-1} \in gHg^{-1}$

□

8. 02.10 **ISOMORPHISMS of GROUPS**

   (a) Definition: 15.1 Let G, G' be groups. A function $f : G \to G'$ is called isomorphisms of groups if:
   - $f(x * y) = f(x) * f(y)$
   - f is one to one (injective)
   - f is onto (surjective)

   (b) Remark: 15.2
   First multiply and then apply f is the same as first apply f and then multiply

   (c) Example: 15.3
   $G = (S_2, \cdot) = \{(1), (12)\}, G' = (Z_2, +_2) = \{[0]_2, [1]_2\}$
   Then $f : (1) \to [0]_2, (12) \to [1]_2$
   We need to check:
   $f((1) \cdot (1)) =? f(1) +_2 f(1)$
   Check: $f((1) \cdot (1)) = f((1)) = [0]_2$

$f(1) +_2 f(1) = [0]_2 + [0]_2 = [0]_2$
$f((1)\cdot(12)) =? f(1) +_2 f(12)$
Check: $f((1)\cdot(12)) = f((12)) = [1]_2$
$f(1) +_2 f(12) = [0]_2 + [1]_2 = [1]_2$
$f((12)\cdot(12)) =? f(12) +_2 f(12)$
Check: $f((12)\cdot(12)) = f((1)) = [0]_2$
$f(12) +_2 f(12) = [1]_2 + [1]_2 = [0]_2$
$f((12)\cdot(1)) =? f(12) +_2 f(1)$
Check: $f((12)\cdot(1)) = f((12)) = [1]_2$
$f(12) +_2 f(1) = [1]_2 + [0]_2 = [1]_2$
For small groups, just use cayley tables

S_2	(1)	(2)
(1)	(1)	(12)
(12)	(12)	(1)

,

Z_2	0	1
0	0	1
1	1	0

If the cayley tables are the same under the mapping f, then it is isomorphism.

(d) Example: 15.4 $G = (S_2, \cdot)$, $G' = (Z_2, +_2)$ consider the mapping: $(1) \to [1]_2, (12) \to [0]_2$
Property 2, 3 is trivial, Check the property one.
$f((1)(12)) = f((12)) = [0]_2$. while $f(1) + f(12) = [1]_2 + [0]_2 = [1]_2$
Therefore, this mapping is not a isomorphism.

(e) Example: 15.5 $G = (Z_4, +_4)$, $G' = (Z_1^{\times}0, *_10)$
$G = \{[0],[1],[2],[3]\}$, $G' = \{1,3,7,9\}$
NOTE: $G =< [1]_1 >$, $G' =< 3 >$.
Therefore, a possible way to define a map is $[1]_4^i \to 3^i$.
i.e. $[1] \to 3$
$[1]^2 = [2] \to 3^2 = 9$
$[1]^3 = [3] \to 3^3 = 7$
$[1]^4 = [0] \to 3^4 = 1$

(f) Definition: 15.6 Let G be a group, If G is finite then order of $G = |G|$ is defined to be the number of elements in G. If G is not finite, then $|G| = \infty$

(g) Prop: 15.7 Suppose $G \cong G'$ i.e. $\exists f : G \to G'$ that is isomorphic. Then $|G| = |G'|$.

(h) Prop: 15.8 Suppose $G \cong G'$ Then G is abelian $\Leftrightarrow$ G' is abelian. (which implies that abelian group and non abelian group is not isomorphic)

(i) Definition: 15.10 A group G is cyclic if $G =< a >$ for some $a \in G$

(j) Remark: 15.11 $(Z_4, +_4)$ is cyclic, $(Z_{10}^{\times}, \cdot_{10})$ is cyclic

(k) Prop: 15.12 if G and G' are cyclic and $|G| = |G'|$ then $G \cong G'$

Proof. idea of proof:
G cyclic, $G =< a >$, G' cyclic, $G' =< a' >$
Then $f : G \to G'$: $a^i \to (a')^i$
Then check f is bijection. □

(l) Prop: 15.13 Let $G = (Z_n, +_n) = \{[0],[1]\cdots,[n-1]\}$, $G' = (Z_n, +_n) = (\{0,1,2,\cdots,n-1\}, +_n)$
Then $G \cong G'$ and the isomorphisim can be take $[x]_n \to x$

9. 02.12

(a) Definition: 16.1 Order of a group: # of elements in that group.

(b) Definition: 16.2 Order of an element: smallest positive integer n such that $g^n = e$

(c) Prop: 16.3 Let $g \in G$, $| < g > | = |g|$

Proof. $< g >= \{\dots, g^{-1}, g^0, g^1, g^2, \dots\}$
$|g| = n \Rightarrow g^n = e$ n is the smallest positive integer.
Then $< g >= \{e, g, g^2 \dots, g^{n-1}\}$
CLAIM: they are all distinct elements
proof: suppose $g^i = g^j$ for some $0 \leq i, j \leq n-1$
Suppose $i \leq j$
$g^{-i}g^i = g^{-i}g^j$
$e = g^{j-i}$
Since $i \leq j$, then $j - i \geq 0$
Therefore, $j - i = 0$
Therefore, $j = i$
Therefore, $g^i = g^j$
Therefore, for all $0, 1, 2, \dots, n-1$, g^i are all distinct.
Therefore, g^i are all distinct.
Therefore, $| < g > | = n \Rightarrow | < g > | = |g|$ □

(d) Remark: 16.4 Let $g \in G$ then $< g >$ is a subgroup of G.

(e) Remark: 16.5 $< g >$ is cyclic group (is a cyclic subgroup of G)

(f) Theorem: 16.6 Let H be a subgroup of group G then $|H|$ divides $|G|$

(g) Example: 16.7 Let G be a group with $G = 7$, Then the only subgroups of G are $H = G$ or $H = \{e\}$
If $H < G$ is a subgroup of G then $|H|$ divides $|G|$
Therefore, $|H| = 1$ or 7.
Therefore, $H = G$ or $H = \{e\}$

(h) Corollary: 16.8 $g \in G$, then $|g|$ divides $|G|$

Proof. $|g| = | < g > |$, $< g >$ is a subgroup of $|G|$.
Then $| < g > |$ divides $|G|$.
Then $|g|$ divides $|G|$. □

(i) Let $G = S_3$ let $x \in G$ what are the possible orders of x?
$|G| = |S_3| = 6$
$\Rightarrow |x| = 1, 2, 3, 6$ We know that orders are only 1,2,3. Not all divisors appear as order of elements.

(j) Prop: 16.10 Let G be a group, $|G| = n < \infty$ then G is cyclic $\Leftrightarrow \exists x \in G, |x| = n$

Proof. **Exercise** □

(k) 16.11 $G = S_3$ G is not cyclic since there is no element of order $|G|$.

(l) Remark: 16.12 $< g >= \{g^i\}$
Under addition: $(G, +)$ then $< g >= \{0, g, 2g, 3g, \dots, ng\}$

(m) Recall: 16.14
$G = (Z_1 2, +_1 2)$ then $G = \{4, 8, 12 = 0\}$

(n) Example: 16.14 $G = (Z_1 2, +_1 2)$, show, G is cyclic

Proof. To show G is cyclic, we need to find an element of order 12.
1 has order 12 since $< 1 >= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 = 0 = e\}$
Then we can say: **1 is a generator of G**
Any number that is relatively prime to 12 is a generator of G
1,5,7,11 are generators of G □

(o) Definition: 16.15 Let G be a group. Let H be a subgroup. Let $a \in G$. a **left coset** of H in G

$$aH := \{ah \mid h \in H\}$$

NOTE: Not simply mean multiplication. It is the binary operation in the group

(p) Example: 16.16 Let $G = S_3$ Let $H =< (13) >= \{(13), (1)\}$. Find all left cosets of H

	(13)	(1)
(1)	(13)	(1)
(12)	(132)	(12)
(13)	(1)	(13)
(23)	(123)	(23)
(123)	(23)	(123)
(132)	(12)	(132)

- Disjoint (or the same) cosets
- aH = H $\Leftrightarrow a \in H$
- $a \in aH$
- $a \in bH \Leftrightarrow aH = bH \Leftrightarrow b \in aH$
- $|H| = |aH|$
- # of disjoint cosets = 3 = $\frac{|G|}{|H|}$
- $G = \cup$ all cosets.

10. 02.13

(a) Remark: 17.1 If H is a subgroup of G, then $|H| \mid |G|$ ($|H|$ divides $|G|$)

(b) Prop: 17.3
- All subgroup of Z are cyclic
- All subgroup of Z_n are cyclic

(c) Prop: 17.4 Let $G = Z_n$, k—n then $| < k > | = |k| = \frac{n}{k}$

(d) Prop: 17.5 Let $G = Z_n$, k—n then $| < k > | = |k| = |gcd(n, k)| = \frac{n}{gcd(n,k)}$

(e) Prop: 17.6 Let $G = Z_n$, $d|n$ then $\exists!$ subgroup of order d. It is given as $k = \frac{n}{d}$, $| < k > | = d$

+1 (01.27)