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)
$g : \mathbf{Z}_8 \Rightarrow \mathbf{Z}_1 2, g([x]_8) = [6x]_1 2$ 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 → (i j) $i \neq j$
3-cycle → (i j k) i,j,k distinct
r-cycle → $(i_1, i_2, \ldots, i_r)$, $i_1, i_2, \ldots, i_r$ 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. $\forall x \in G, \exists y \in Gs.t. x*y = e, y*x = e$
          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 = □

(c) 10.4 Prop:
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 $yx = e$ □

(d) 10.5 Prop:
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) 10.6 Definition: 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) 10.7 Example:
G = $(\mathbf{Z}, +)$, H = $(3\mathbf{Z}, +)$

(g) 10.8 Example:
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.

+1 (01.27)