Discrete Mathematics Recitation Class

Tianyu Qiu

University of Michigan - Shanghai Jiaotong University

Joint Institute

Summer Term 2019

Contents

Groups

Definitions

1. *group* $(G, \cdot)$ (P150)
   - set G
   - group Operation $\cdot$
   - associativity
   - unique identity element $(e_1 = e_1 \cdot e_2 = e_2)$
   - unique inverse element $(y_2 = y_2 \cdot e = y_2 \cdot x \cdot y_1 = e \cdot y_1 = y_1)$
2. *abelian*: $\forall x, y \in G, x \cdot y = y \cdot x$ (P151)
3. *trivial group*: Any group that consists only of an identity element. (P160)

e.g.

- If $(G, \circ)$ is a group, then $G \neq \emptyset$ (existence of identity) (P160).
- $X = \{f : \mathbb{R} \longrightarrow \mathbb{R} | f \text{ is linear with non-zero slope}\}$. Then $(X, \circ)$ is a group that is not abelian. (P152)
- $X' = \{f \in X | f(0) = 0\}$. Then $(X', \circ)$ is an abelian group. (P152)

Algebra in Groups

Lemma

Let $(G, \cdot)$ be a group. If $a, b, c \in G$ and $a \cdot b = a \cdot c$, then $b = c$. (P153)

Proof.

P153 $\square$

Corollary

Let $(G, \ )$ be a group and $a \in G$. If $a \cdot a = a$, then $a = e$. (P154)

Proof.

P154 $\square$

Symmetric Group

Definitions (P155)

1. *symmetric group $(X, \circ)$*:
   - X is a set of bijections $f : [n] \to [n]$.
   - group operation is composition of functions.
2. *cycle notation*: bijection $f : [n] \to [n]$:

$$(k_1 k_2 \cdots k_m) \equiv f(x) = \begin{cases} f(k_i) = k_{i+1} & \text{if } i < m \\ f(k_m) = k_1 & \\ f(x) = x & \text{if } x \text{ is not any of the } k_i\text{s} \end{cases}$$

with $m \leqslant n, k_i < n, k_i \in [n], m, n \in \mathbb{N}$

Reading order for cycles: (P157)

- different cycles: right to left
- inside one cycle: left to right (then back to the left)

Examples for Cycles

e.g.

- In S_n the identity bijection $id_{[n]} : [n] \to [n]$ can be written as (k) for any $k \in [n]$ or as empty cycle $()$ (more generally, as e_{S_n} or just e).
- $(k_1 k_2 \cdots k_m) \equiv (k_2 k_3 \cdots k_m k_1)$
- The inverse of $(k_1 k_2 \cdots k_m)$ is $(k_m k_{m-1} \cdots k_1)$

The Symmetric Group (P160)

Theorem

Let $n \in \mathbb{N} \setminus \{0\}$. The group S_n is not abelian if and only if $n \geqslant 3$.

Proof.

- Suppose $n \geq 3$. In S_n the product of (01) and (012) is $(01)(012) = (12)$, and the product of (012) and (01) is $(012)(01) = (02)$. Therefore $(01)(012) \neq (012)(01)$, and so S_n is not abelian.
- We prove the the contrapositive: "if $0 < n < 3$, then S_n is abelian". $S_1 = \{e\}$, $S_2 = \{e, (01)\}$ are abelian.

$\square$

Cycles (P161)

Definitions

1. *length m*: a cycle with m distinct natural numbers.
2. *disjoint*: two cycles have no natural numbers in common.

Lemma

If α and β are disjoint cycles in S_n then $\alpha\beta = \beta\alpha$ in S_n.

Proof.

$\forall x \in [n]$, there are three possibilities:

1. $x \in \alpha$, then $x \notin \beta, \alpha(x) \notin \beta$, $\alpha\beta(x) = \alpha(x) = \beta\alpha(x)$.
2. $x \in \beta$, then $x \notin \alpha, \beta(x) \notin \alpha$, $\alpha\beta(x) = \beta(x) = \beta\alpha(x)$.
3. $x \notin \alpha \cup \beta$, then $\alpha\beta(x) = x = \beta\alpha(x)$

$\square$

Cycles (P162)

Theorem

Every element of S_n can be written as a product of disjoint cycles.

Proof.

P162-P163 $\square$

e.g.

- $(124)(352) = (12354)$
- $(05)(132)(21)(143)(560) = (1423)(56) = (56)(1423)$
- $(45)(12)(31)(54)(02)(32)(45) = (013)(45) = (45)(013)$

Cycles (P164)

Theorem

Let $n \geqslant 2$. Every element of S_n can be written as the product of 2 -cycles.

Proof.

P164 $\square$

e.g. $(2143) = (23)(214) = (23)(24)(21)$

Cycles (P165)

Definition

Let $\sigma \in S_n$. If σ can be written as a product of an odd number of 2-cycles, then we say that σ is odd. If σ can be written as a product of an even number of 2-cycles, then we say that σ is even.

Theorem

Every element of S_n is either even or odd, but not both. (uniqueness of odevity of natural numbers)

e.g.

- $(1032) = (12)(13)(10)$, so (1032) is odd.
- Identity is even. $(e = (10)(01))$

Orders

Definition(P166)

- x^n: recursively defined by $x^0 = e, x^{n+1} = x \cdot x^n$.
- *finite order*: $\exists n \geqslant 1$ such that $x^n = e$
- *order of* x: the least n satisfying $x^n = e$.
- *infinite order*: no finite order

e.g.(P167)

- In $S_4, (012)^3 = (012)(012)(012) = e$
- In the group $(\mathbb{Z}, +)$, the element 6 has infinite order because for all $n \in \mathbb{N}\backslash\{0\}, 6^n = \underbrace{6 + \cdots + 6}_{\text{n times}} \neq 0$

Orders (P168)

Theorem

If $(G, \cdot)$ is a finite group, then every element of G has finite order.

Proof.

Prrof by Contradiction (P168) $\square$

Example for Group Order (P169)

e.g.
Let $A = \{T, F\}$ and let $X = \{f | f : \mathbb{N} \longrightarrow A\}$. Define $\cdot$: $X \times X \longrightarrow X$ by: for all $f, g, h \in X$,

$$f \cdot g = h \text{ iff } \forall n \in \mathbb{N}, f(n) \oplus g(n) = h(n)$$

- $(X, \cdot)$ is an abelian group
- The identity of $(X, \cdot)$ is the function $f : \mathbb{N} \longrightarrow A$ defined by: for all $n \in \mathbb{N}, f(n) = F$
- $(X, \cdot)$ is infinite. In fact, X is uncountable.
- For $g \in X, g \cdot g = e$. So, every element of $(X, \cdot)$ that is not the identity has order 2.

Subgroups (P170)

Definition

subgroup: Let $(G,\cdot)$ be a group. We say that $H \subseteq G$ is a subgroup of $(G,\cdot)$, and write $H \leq G$ or $(H,\cdot) \leq (G,\cdot)$, if $e \in H$ and for all $x, y \in H, x \cdot y^{-1} \in H$.

Lemma

Let $(G,\cdot)$ be a group and let $H \subseteq G$. Then $H \leq G$ if and only if $(H,\cdot)$ is a group.

Proof.

P170 □

Examples for Subgroups (P171)

e.g.

- If $(G, \cdot)$ is a group, then both G and the trivial group $\{e\}$ are subgroups of $(G, \cdot)$
- $H = \{e, (012), (021)\}$ is a subgroup of S_3, but $H' = \{e, (01), (012)\}$ is not a subgroup of S_3
- Let $X = \{f | f : \mathbb{R} \longrightarrow \mathbb{R}\}$. Then $(X, +)$ the set X with the operation "addition of functions" is a group. And $X' = \{f : \mathbb{R} \to \mathbb{R} | f(0) = 0\}$ is subgroup of $(X, +)$. But $X'' = \{f : \mathbb{R} \to \mathbb{R} | f(0) = 1\}$ is not a subgroup of $(X, +)$.

The Dihedral Groups (P172-P173)

Definitions

1. *order of the set in a group*: the cardinality of the finite set of the group.
2. *the dihedral group D_n*: the subgroup of S_n of all symmetries of a regular n-gon. (Do the symmetry/rotation operation, do no damage to the n-gon itself)

e.g.

- The order of symmetric group S_n is $n!$ (P148).
- D_3 is the subgroup of S_3 of symmetries of an equilateral triangle and $D_3 = S_3$.
- $D_4 = \left\{ \begin{array}{c} e, (01)(23), (0123), (02)(13), (0321), \\ (01)(23)(0123), (01)(23)(02)(13), (01)(23)(0321) \end{array} \right\}$

The Dihedral Groups (P174)

Theorem

Let $n \geqslant 3$. The group D_n has order $2n$.

Proof.

Think about the symmetry/rotation operation. For n-gons, one can rotate the shape $\# = n - 1$ times and adding the initial condition, $\# = n$ choices in total. Then considering the case of symmetry, an n-gon has n symmetric lines, thus we can fold the n-gon in n ways, so $\# = n + n = 2n$ in total. $\square$

Lagrange's Theorem (P176)

Definitions Let $(G, \cdot)$ be a group, $H \leqslant G$ and $a \in G$.

1. *left coset*: $aH = \{a \cdot x | x \in H\}$
2. *right coset* : $Ha = \{x \cdot a | x \in H\}$

Theorem (Lagrange's Theorem)

Let $(G, \cdot)$ be a finite group. If $H \leq G$, then the order of H divides the order of G .

Proof.

P177-P179 □

Division Algorithm (P180)

Definition

exact division on $\mathbb{Z}$(the same way as exact division on $\mathbb{N}$)

Theorem (Division Algorithm)

Let $a \in \mathbb{Z}$ *and let* $b \in \mathbb{N}$ *with* $b \neq 0$. *There exists a unique* $q, r \in \mathbb{Z}$ *such that*

$$a = q \cdot b + r \text{ and } 0 \leq r < b$$

q: qoutient, r: remainder

Proof.

- Uniqueness(P181)
- Existence(P182)

$\square$