JOINT INSTITUTE
交大密西根学院

Discrete Mathematics Recitation Class

Tianyu Qiu

University of Michigan - Shanghai Jiaotong University

Joint Institute

Summer Term 2019

Contents

Generated Subgroups (P184)

Definition

Let $(G, \cdot)$ be a group and let $A \subseteq G$. We define the subgroup generated by A, denoted $\langle A \rangle_G$, to be the $\subseteq$ -least $H \subseteq G$ such that $A \cup \{e\} \subseteq H$ and for all $x, y \in H, x \cdot y^{-1} \in H$.

- $\langle A \rangle_G$ is a recursively defined set.
- The closure conditions (constructors) ensure that $\langle A \rangle_G \leq G$.
- Moreover, if $H \leq G$ with $A \subseteq H$, then $\langle A \rangle_G \subseteq H$ and so $\langle A \rangle_G \leq H$.
- If $A \subseteq G$ is finite with $A = \{a_1, \ldots, a_n\}$, then we will often write $\langle a_1, \ldots, a_n \rangle_G$ instead of $\langle A \rangle_G$.
- We will often write $\langle A \rangle$ or $\langle a_1, \ldots, a_n \rangle$ instead of $\langle A \rangle_G$ and $\langle a_1, \ldots, a_n \rangle_G$.

Examples for Generated Subgroups (P185-P186)

e.g.

- $\langle(01)(23),(0123)\rangle_{S_4}=D_4\leq S_4$.
- Consider $(\mathbb{Z},+)$,
$$\langle 2\rangle=2\mathbb{Z}\leq\mathbb{Z}$$
- Consider $(\mathbb{R}\setminus\{0\},\cdot)$,
$$\langle\mathbb{Z}\backslash\{0\}\rangle=\mathbb{Q}\backslash\{0\}\leq\mathbb{R}$$
- Consider S_n. If $A=\{\sigma\in S_n|\sigma \text{ is a 2 -cycle }\}$, then $\langle A\rangle=S_n$.

The Cyclic Groups

Definitions (P187)

1. *cyclic group of order n* C_n: $\langle a \rangle$ where $a \in G$ has order n.
2. *cyclic group of infinite order* C_∞: $\langle b \rangle$ where $b \in G$ has infinite order.

Lemma

Let $(G, \cdot)$ be a group. If $a \in G$, then

$$\langle a \rangle = \{a^m | m \in \mathbb{Z}\}$$

(Where, for all $k \in \mathbb{N}, a^{-k} = (a^{-1})^k$) (P188)

Proof.

P188 $\square$

The Cyclic Groups

Lemma

Let $n \in \mathbb{N} \setminus \{0\}$ or $n = \infty$. The group C_n is abelian. (P187)

Proof.

P188 □

Lemma

Let $(G, \cdot)$ be a group and let $n \in \mathbb{N} \setminus \{0\}$. If $a \in G$ has order n, then $|\langle a \rangle| = n$.

Proof.

P189 □

Cyclic Groups in the Symmetric Group (P190)

Lemma

Let $n \in \mathbb{N} \setminus \{0\}$ and let $m \le n$. Let $k_1, \dots, k_m \in [n]$ be distinct. The m-cycle $(k_1 \cdots k_m)$ has order m in S_n.

Proof.

P190 □

Theorem

Let $n \in \mathbb{N} \setminus \{0\}$. For all $0 < k \le n$, $C_k \le S_n$.

Theorem (Refinement of Lagrange's Theorem)

If $(G, \cdot)$ is a finite group and $x \in G$, then the order of x divides the order of G.

Proof.

P190 □

Group of order p (P191)

Theorem

Let p be prime. Let $(G, \cdot)$ be a finite group of order p. Then $(G, \cdot)$ is the the group C_p.

Proof.

P191 $\square$

Corollary

If $(G, \cdot)$ is a finite group with order p, then the only subgroups of G are the trivial group and G.

An Important Consequence of Lagrange's Theorem (P192)

Theorem

Let $(G, \cdot)$ be a group and let $g \in G$ have order n. If there exists $m, k \in \mathbb{N} \setminus \{0\}$ with $n = mk$, then the order of g^m is k.

Proof.

P192 □

Theorem

If $(G, \cdot)$ is a finite group with order n, then for all $g \in G, g^n = e$.

Proof.

P192 □

Examples for Lagrange's Theorem (P193)

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.

Converse to Lagrange's Theorem

Let $(G, \cdot)$ be a finite group. If a natural number k divides the order of G, then there exists $g \in G$ with order k.

e.g.

Let A_4 be the group of all even bijections in S_4. There is no $\sigma \in A_4$ with order 6. (This example indicates there is no converse to Lagrange's Theorem.)

Theorem

If $(G, \cdot)$ is a group of order 6, then there exists $g \in G$ with order 2.

Proof.

P194 $\square$

Isomorphisms & Homomorphisms (P195)

Definitions

1. *(group) homomorphism*: $(G, \cdot)$ and $(K, \star)$ are groups. $f : G \to K$ is a (group) homomorphism if $\forall a, b \in G, f(a \cdot b) = f(a) \star f(b)$.
2. *(group) isomorphism*: based on f is (group) homomorphism, f is a bijection.
3. *isomorphic*: $G \cong K$ $((G, \cdot) \cong (K, \star))$ if there exists an isomorphism between $(G, \cdot)$ and $(K, \star)$.

Theorem

Let $(G, \cdot)$ be a group. Let $g, h \in G$ both have order n. Then $\langle g \rangle \cong \langle h \rangle$. (P196)

Examples for Morphisms (P196-P197)

e.g.

- Let $(G, \cdot)$ be any group with $G \neq \{e\}$ and let $H = \{e\}$, i.e. H is the trivial subgroup of $(G, \cdot)$. The function $f : G \longrightarrow H$ defined by: for all $x \in G$, $f(x) = e$, is a homomorphism. The function $g : H \longrightarrow G$ defined by: $g(e) = e$, is also a homomorphism. The homomorphism f is surjective but not injective, and the homomorphism g is injective, but not surjective.
- Let $n \in \mathbb{N}$ with $n \geq 2$. Let $(G, \cdot)$ be a group and let $a \in G$ have order n. Let $H = \langle a \rangle$, i.e. H is (isomorphic to) C_n . Consider the group $(\mathbb{Z}, +)$. Define $f : \mathbb{Z} \longrightarrow H$ by: for all $x \in \mathbb{Z}, f(x) = a^x$. Then f is a homomorphism because for all $x, y \in \mathbb{Z}$,

$$f(x + y) = a^{x+y} = a^x \cdot a^y$$

Examples for Morphisms (P196)

Theorem

Consider the group $(Z, +)$. If $n \in \mathbb{N} \backslash \{0\}$, define

$$n\mathbb{Z} = \{m \in \mathbb{Z} | (\exists k \in \mathbb{Z})(m = nk)\}$$

Then $n\mathbb{Z} \leq \mathbb{Z}$ and $n\mathbb{Z} \cong \mathbb{Z}$

Proof.

Define $f : \mathbb{Z} \longrightarrow n\mathbb{Z}$ by: for all $x \in \mathbb{Z}, f(x) = nx$. Now, f is a bijection and for all $x, y \in \mathbb{Z}$,

$$f(x + y) = n(x + y) = nx + ny = f(x) + f(y)$$

$\square$