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

Proof.

P188 □

Lemma

Let $(G, \cdot)$ be a group and let $n \in \mathbb{N}\backslash\{0\}$. 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 $k_1, \ldots, k_m \in [n]$ be distinct. The m-cycle $(k_1 \cdots k_m)$ has order m in S_n.

Proof.

P190 $\square$

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 $\square$

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 □

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 $\square$

Theorem

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

Proof.

P192 $\square$

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 $x, y \in \mathbb{Z}$,

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

$\square$

Congruency

Definitions.(P199)

1. $a \equiv b(mod\ \ n)$ if and only if $n|(a-b)$
2. $\mathbb{Z}/n\mathbb{Z} = \{[a]_n | a \in \mathbb{Z}\}$
3. $\oplus_n : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$: $\forall a, b \in \mathbb{Z}$,
$$[a]_n \oplus_n [b]_n = [a+b]_n$$
4. $\otimes_n : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$: $\forall a, b \in \mathbb{Z}$,
$$[a]_n \otimes_n [b]_n = [ab]_n$$
5. *well-deifined*: A function is well-defined if it gives the same result when the representation of the input is changed without changing the value of the input.

Congruency

Theorem

Let $n \in \mathbb{N} \setminus \{0\}$. The operation $\oplus_n$ is well-defined. (P200)

Proof.

P200 $\square$

Theorem

Let $n \in \mathbb{N} \setminus \{0\}$. The operation $\otimes_n$ is well defined.(P201)

Proof.

P201 $\square$

Cayley Table

Lemma

If $n \in \mathbb{N} \setminus \{0\}$, then $(\mathbb{Z}/n\mathbb{Z}, \oplus_n)$ is group.(P202)

Take $(\mathbb{Z}/4\mathbb{Z}, \oplus_4)$ as an example, we construct Cayley Table:

$\oplus_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Lemma

If $n \in \mathbb{N} \setminus \{0\}$, then $(\mathbb{Z}/n\mathbb{Z}, \oplus_n)$ is abelian with order n. Moreover, $(\mathbb{Z}/n\mathbb{Z}, \oplus_n) = C_n$

Proof.

P203

Cayley Table (P203)

- $(\mathbb{Z}/n\mathbb{Z}, \otimes_n)$ is not group ($[0]_n$ does not have inverse).
- $(\mathbb{Z}/n\mathbb{Z} \setminus \{[0]_n\}, \otimes_n)$ is not group (operation is not close on $(\mathbb{Z}/n\mathbb{Z} \setminus \{[0]_n\}, \otimes_n)$ e.g. $[2]_6 \cdot [3]_6 = [6]_6 = [0]_6$)
- In order $(G_n, \otimes_n)$ to be group, $[1]_n$ must be the identity. For all $[k]_n \in G_n$, there must exist $[m]_n \in G_n$ such that

$$[k]_n \otimes_n [m]_n = [km]_n = [1]_n$$

I.e. for all $[k]_n \in G_n$, there must exists $x \in \mathbb{Z}$ such that

$$kx \equiv 1 (\bmod n)$$

Cayley Table

Definition.
$(\mathbb{Z}/n\mathbb{Z})^* = \{[k]_n \in \mathbb{Z}/n\mathbb{Z} | (\exists x \in \mathbb{Z})(kx \equiv 1 (\bmod\ n))\}$(P205)

Theorem
Let $n \in \mathbb{N}$ with $n \geq 2$. Then $((\mathbb{Z}/n\mathbb{Z})^*, \otimes_n)$ is a group.

Proof.
P206 $\square$

e.g. $[1]_6$ and $[5]_6$ are elements of $((\mathbb{Z}/6\mathbb{Z})^*, \otimes_6)$, moreover, $((\mathbb{Z}/6\mathbb{Z})^*, \otimes_6) \cong ((\mathbb{Z}/3\mathbb{Z})^*, \otimes_3) \cong C_2$. (P207)

$\otimes_6$	$[1]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[5]_6$
$[5]_6$	$[5]_6$	$[1]_6$

Cayley Table

Lemma

Let $n \in \mathbb{N}$ with $n \geq 2$. If $1 < m \leq n$ is such that there exists $1 < d \leq m$ with $d|m$ and $d|n$, then $[m]_n \notin (\mathbb{Z}/n\mathbb{Z})^*$. (P208)

Proof.

P208 $\square$

Greatest Common Divisor

Definitions

1. *gcd*(P209): Let $a, b \in \mathbb{Z}$ with $|a| + |b| \neq 0$. We say that $d \in \mathbb{N}$ is the greatest common divisor of a and b , and write this element gcd (a, b), if
   1.1 $d|a$ and $d|b$
   1.2 For all $c \in \mathbb{Z}$, if $c|$ a and $c|b$, then $c|d$
2. *linear Diophantine equation in two variables*(P210):

   $ax + by = c$ where $a, b, c \in \mathbb{Z}$ are constants with $|a| + |b| \neq 0$

3. *relatively prime*(P214): a, b are relatively prime if $gcd(a, b) = 1$

- A solution is a pair $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ with $ax_0 + by_0 = c$
- This means that in order to show that $[m]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, we show that the linear Diophantine equation $mx + ny = 1$ has a solution.

Bézout's Lemma

Theorem

Let $a, b \in \mathbb{Z}$ *with* $|a| + |b| \neq 0$. *Then there exists* $x, y \in \mathbb{Z}$ *such that* $\gcd(a, b) = ax + by$

Proof.

P211-P212 □

Corollary

(P212) Let $n \in \mathbb{N}$ *with* $n \geq 2$. *For all* $m \in \mathbb{Z}$ *,*

$$[m]_n \in (\mathbb{Z}/n\mathbb{Z})^* \text{ if and only if } \gcd(m, n) = 1$$

Corollary

(P213) Let $n \in \mathbb{N}$ *with* $n \geq 2$ *.*

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[m]_n | (m < n) \wedge (\gcd(m, n) = 1)\}$$

Bézout's Lemma

Lemma

Let $a \in \mathbb{Z}$ *and* $b \in \mathbb{N} \backslash \{0\}$. *If* $q, r \in \mathbb{Z}$ *with* $a = qb + r$, *then* $\gcd(a, b) = \gcd(b, r)$ *(P213)*

Proof.

P213 $\square$

Euler's Totient Function

Definition

Euler's Totient Function: $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$

Lemma

If $p \in \mathbb{N}$ is prime, then $\varphi(p) = p - 1$

Proof.

P216 $\square$

Theorem (Euler's Theorem)

Let $a, n \in \mathbb{N}$ with $n \geqslant 2$ and $gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 (mod\ n)$

Proof.

P217 $\square$

Euler's Totient Function

Theorem (Fermat's Little Theorem)

If $a, p \in \mathbb{N}$, *p is prime and* $gcd(a, p) = 1$, *then* $a^{p-1} \equiv 1(mod\ p)$.

Proof.

P217 □

Theorem (Euler's Product Formula)

$$\varphi(n) = n \cdot \prod_{p \in A} \left(1 - \frac{1}{p}\right)$$

Bézout's Lemma

Corollary

Let $a, b \in \mathbb{Z}$ *with* $|a| + |b| \neq 0$. *Then* $gcd\,(a, b) = 1$ *if and only if there exists a solution to the Diophantine equation* $ax + by = 1$

Proof.

P220 □

Corollary

Let $a, b \in \mathbb{Z}$ *with* $|a| + |b| \neq 0$. *If* $\gcd(a, b) = d$, *then*

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Proof.

P220 □

Fundamental Theorem of Arithmetic

Theorem

Let $a, b, c \in \mathbb{Z}$ *with* $\gcd(a, b) = 1$. *If* $a \mid c$ *and* $b \mid c$, *then* $ab \mid c$.

Proof.

P222 $\square$

Theorem (Euclid's Lemma)

Let $a, b, c \in \mathbb{Z}$ *with* $\gcd(a, b) = 1$. *If* $a \mid bc$, *then* $a \mid c$.

Proof.

P223 $\square$

Theorem

Let $p \in \mathbb{N}$ *and let* $a, b \in \mathbb{Z}$. *If* p *is prime and* $p \mid ab$, *then* $p \mid a$ *or* $p \mid b$.

Proof.

P223 $\square$

Fundamental Theorem of Arithmetic

Theorem

Let $p \in \mathbb{N}$ be prime. If $a_1, \ldots, a_n \in \mathbb{Z}$ and $p | a_1 \cdots a_n$, then there exists $1 \le k \le n$ such that $p | a_k$.

Proof.

P224 $\square$

Theorem

Let $p, q_1, \ldots, q_n \in \mathbb{N}$ be primes. If $p | q_1 \cdots q_n$, then there exists $1 \le k \le n$ such that $p = q_k$.

Proof.

P224 $\square$

Theorem (Fundamental Theorem of Arithmetic)

If $n \in \mathbb{N}$ with $n \ge 2$, then n can be uniquely factored into a product of primes.

Euclidean Algorithm

Definition(P228)

euclidean algorithm: Let $a, b \in \mathbb{N}\backslash\{0\}$ with $b < a$. Recursively define $F_{a,b}(0) = a$ and $F_{a,b}(1) = b$

$$F_{a,b}(n+2) = \begin{cases} 0 & \text{if } F_{a,b}(n+1) = 0 \\ r & \text{where } (\exists q \in \mathbb{Z}) \begin{pmatrix} F_{a,b}(n) = qF_{a,b}(n+1) + r \\ \wedge(0 \leqslant r < F_{a,b}(n+1)) \\ \text{and } F_{a,b}(n+1) \neq 0 \end{pmatrix} \end{cases}$$

Lemma

Let $a, b, n \in \mathbb{N}\backslash\{0\}$ with $b < a$. If $F_{a,b}(n) \neq 0$, then $F_{a,b}(n+1) < F_{a,b}(n)$. (P228)

Lemma

Let $a, b, n \in \mathbb{N}\backslash\{0\}$ with $b < a$. If $F_{a,b}(n) = 0$, then for all $m \geq n$, $F_{a,b}(m) = 0$ (P229)

Euclidean Algorithm

Lemma

Let $a, b \in \mathbb{N}\setminus\{0\}$ *with* $b < a$. *There exists* $n \in \mathbb{N}$ *such* $F_{a,b}(n) = 0$.

Proof.

Proof by Contradiction (P229) □

Lemma

Let $a, b \in \mathbb{N} \setminus \{0\}$ *with* $b < a$ *and let* $n \in \mathbb{N}$. *If* $F_{a,b}(n) \neq 0$, *then* $\gcd(a, b) = \gcd\left(F_{a,b}(n), F_{a,b}(n+1)\right)$

Proof.

P230 □

Euclidean Algorithm

Lemma

Let $a, b \in \mathbb{N} \backslash \{0\}$ *with* $b < a$. *Let* $n_0 \geq 2$ *be least such that* $F_{a,b}(n_0) = 0$ *Then* $\gcd(a, b) = F_{a,b}(n_0 - 1)$

Proof.

P231 $\square$

Linear Diophantine Equations

Definition

Diophantine equation in two variables(P210):

$$ax + by = c \text{ where } a, b, c \in \mathbb{Z} \text{ are constants with } |a| + |b| \neq 0$$

Theorem

Let $a, b, c \in \mathbb{Z}$. There exists a solution to the linear Diophantine equation $ax + by = c$ if and only if $\gcd(a, b) | c$.

Proof.

P238 □

Linear Diophantine Equations

Theorem

Let $a, b, c, d \in \mathbb{Z}$ *with* $d = \gcd(a, b)$ *and* $d \mid c$. *Let* (x_0, y_0) *be a solution to* $ax + by = c$. *For all* $t \in \mathbb{Z}, (x_t, y_t)$ *is a solution to* $ax + by = c$ *where*

$$x_t = x_0 + \frac{b}{d} t \text{ and } y_t = y_0 - \frac{a}{d} t$$

Moreover, if (x', y') *is a solution to* $ax + by = c$, *then there exists a* $t \in \mathbb{Z}$ *such that* $(x', y') = (x_t, y_t)$

Proof.

P239-P240 □

Procedure for solving LDEs

Given LDE: $ax + by = c$, with a, b, c are constants and x, y are unknowns, $|a| + |b| \neq 0$:

1. Use Euclidean algorithm to calculate $gcd(a, b)$.
2. Check whether this LDE has solutions (does $gcd(a, b)|c$?)
3. Apply euclidean algorithm in reverse direction to obtain one solution.
4. Write general solutions.

Linear Congruency Equations

Definition

linear congruence: an equation in the form

$$a \cdot x \equiv b \pmod{n}$$

Theorem

Let $a, b \in \mathbb{Z}$ *and let* $n \in \mathbb{N}\{0\}$*. The linear congruence equation*

$$ax \equiv b \pmod n$$

has a solution if and only if $\gcd(a, n) \mid b$*. Moreover, if* $\gcd(a, n) \mid b$*, then the linear congruence equation has exactly gcd* (a, n) *solutions that are mutually incongruent (mod* n*).*

Proof.

P247-P250

$\square$