Outline

① Order of element

② Lagrange theorem

③ cyclic group, generator

$(\mathbb{Z}_4, +)$ is a cyclic group generated 1.

$(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ is not a cyclic group.

$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ iff $\gcd(m,n) = 1$

Chinese Remainder Theorem

integer multiplication

④ Observation:

$(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ is a group

$(\mathbb{Z}_6 \setminus \{0\}, \cdot)$ is not a group

$\mathbb{Z}_6^* = \{1, 5\}$

$(\mathbb{Z}_6^*, \cdot)$ is a group.

$\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n \mid \underline{\gcd(a,n) = 1} \}$

$(\mathbb{Z}_n^*, \cdot)$ is a group

In $\mathbb{Z}_6$

$0 = 0$

$1+1+1+1+1+1 = 0$

$2+2+2 = 0$

$3+3 = 0$

$4+4+4 = 0$

$5+5+5+5+5 = 0$

How many times g operate on itself to reach identity?

In $\mathbb{Z}_2 \times \mathbb{Z}_3$

$(0,0) = (0,0)$

$(0,1)+(0,1)+(0,1) = (0,0)$

$(1,0)+(1,0) = (0,0)$

$(0,2)+(0,2)+(0,2) = (0,0)$

$(1,1)+(1,1)+(1,1)+(1,1)+(1,1)+(1,1) = (0,0)$

$(1,2)+(1,2)+(1,2)+(1,2)+(1,2)+(1,2) = (0,0)$

$\mathbb{Z}_6$ g	order / minimum # of times g operates on itself to get to e
0	x
1	6
2	3
3	2
4	3
5	6

$\mathbb{Z}_2 \times \mathbb{Z}_3$ g	order / minimum # of times g operates on itself to get to e
$(0,0)$	x
$(0,1)$	3
$(1,0)$	2
$(0,2)$	3
$(1,1)$	6
$(1,2)$	6

If f is an isomorphism map between $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$, then f should preserve the minimum # of times g operates on itself to get to e / order of g

f must map 3 to $(1,0)$ since 3 and $(1,0)$ are the only elements with order 3.

Write $(a,b) = a(1,0) + b(0,1)$

$$f((a,b)) = a f((1,0)) + b f((0,1))$$
$$= 3a + 2b \quad \text{or} \quad 3a + 4b$$

since $(0,1)$ is of order 3. and the only elements of order 2 in $\mathbb{Z}_6$ is 2 and 4.

Order of group element

Given a finite group G.

For all element $g \in G$, there exists integer d

such that $g^d = e$.

The smallest such d is called order of g.

Notations

$(G, \cdot)$ multiplicatively

$$g^d = \underbrace{g \cdot g \cdot g \cdot g \cdots g}_{d \text{ times}}$$

$(G, +)$ additively

$$d \cdot g = \underbrace{g + g + g + \cdots + g}_{d \text{ times}}$$

$(\mathbb{Z}, +)$ is a group.

$1 \in \mathbb{Z}$. $1+1+ \ldots \ldots \neq 0$

1 has no finite order

Existence of finite order for all $g \in G$ when G is finite

Let $g \in G$, we list down all elements of g^i

$$g, g^2, g^3, \ldots g^i \ldots$$

Since G is finite, there exits i and j such that

$$g^i = g^j$$

Let g^{-1} be the inverse of g.

$$g^{-j} = g^{-1} \cdot g^{-1} \cdot g^{-1} \ldots g^{-1} \quad (j \text{ times})$$

$$g^i \cdot g^{-j} = g^j \cdot g^{-j}$$

$$g^{i-j} = e$$

Hence, when G is finite, $\exists$ integer $d = i-j$ such that $g^d = e$.

Properties of group elements

Let G be a finite abelian group.

① Let d be the order of $g \in G$,

$g^f = e$ iff d divides f.

Lagrange ② d divides $|G|$.

---

① $\Rightarrow$ If d divides f, $f = dq$, $q \in \mathbb{Z}$

$$g^f = g^{dq} = (g^d)^q = e^q = e$$

$\Leftarrow$ Prove by contradiction. If $g^f = e$.

If $d \nmid f$, $f = dq + r$, $1 \le r \le d-1$

$$g^f = g^{dq+r} = g^{dq} \cdot g^r = g^r = e$$

But $g^r \neq e$ because d by def should be the smallest such integer. Contradiction.

② $G = \{g_1, g_2, \ldots, g_n\}$ $|G| = n$

Let $a \in G$

$aG = \{ag_1, ag_2, \ldots, ag_n\}$

Note that $aG = G$.

E.g. $3(\mathbb{Z}_6, +) = \{3+0, 3+1, 3+2, 3+3, 3+4, 3+5\}$

$= \{3, 4, 5, 0, 1, 2\}$

$= (\mathbb{Z}_6, +)$

Take the product of all element in aG and G respectively.

$g_1 g_2 \ldots g_n = ag_1 \cdot ag_2 \cdot \ldots \cdot ag_n$ } abelian

$g_1 g_2 \ldots g_n = a^n \underline{g_1 \ldots g_n}$

$a^n = e$ (multiplying both sides by $(g_1 \ldots g_n)^{-1}$)

By property ①, order of a must divides n

Cyclic group

Given a finite group G. If there exists an element $g \in G$ such that order of g is $|G|$, then G is a cyclic group.

g is called the generator of G.

In $(\mathbb{Z}_6, +)$, order of 1 is 6.

1 is a generator of $\mathbb{Z}_6$

$\mathbb{Z}_6$ is a cyclic group.

1, $1+1=2$, $1+1+1=3$, $1+1+1+1=4$,

$1+1+1+1+1=5$, $1+1+1+1+1+1=6$

In $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ is not a cyclic group.

	order
$(1,0)$	2
$(0,1)$	2
$(1,1)$	2
$(0,0)$	X

All non-identity elements have order 2.

Chinese Remainder Theorem

If N, m_1, m_2 such that m_1 and m_2 are coprime.
(no common divisors)

then there exist unique solution x to the following:

$$x \equiv x_1 \mod m_1$$
$$x \equiv x_2 \mod m_2$$

If $N = m_1 m_2$ where m_1 and m_2 are coprime
then $f : \mathbb{Z}_N \longleftrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$

$$x \longmapsto (x \bmod m_1, x \bmod m_2)$$

f is bijective.

(E.g) $f: \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$

$$1 \to (1, 1)$$
$$2 \to (0, 2)$$
$$3 \to (1, 0)$$
$$4 \to (0, 1)$$
$$5 \to (1, 2)$$
$$0 \to (0, 0)$$

Euler Totient function, φ

$\varphi(n)$ = number of integers between 1 to $n-1$ that are coprime with n.