Classification of Cyclic Subgroups with the Fundamental Theorem of Cyclic Groups

Larine Ouyang, Bang Tam Ngo, Irene Choi

May 21, 2024

Groups

Definition (Groups)

A group is defined as an ordered pair $(G, \star)$.

- Associativity: $(a \star b) \star c = a \star (b \star c)$.
- Existence of an identity: $a \star e = e \star a = a$.
- Existence of an inverse: $a \star a^{-1} = a^{-1} \star a = e$.

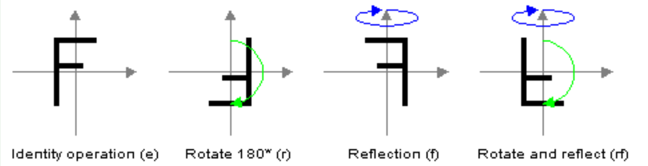
Examples of Groups

Example

- $\mathbb{Z}$: Group of all integers under addition
- $\mathbb{Z}_n$: The group of modulos, $\{0, 1, 2, ..., n-1\}$, under addition
- $(\mathbb{Z}_n)^\times$: The group of integers relatively prime to n under multiplication.
- S_n: A group of permutations

Example (Dihedral Group)

D_n: Group consisting of rotations and reflections



Cyclic Groups

Definition

1. For a group H, some element x is a generator if $H = \{g^k : k \in \mathbb{Z}\}$.
2. A group H is a cyclic group if there is some element $x \in H$ that is a generator of group H, i.e, $H = \langle x \rangle$
3. The order of an element X of a group H is defined as the least positive integer k, such that $x^k = x \cdot x \cdot \ldots \cdot x$ (k times) $= e$, where e is the identity of group H.(i.e. $k = \mathrm{ord}(x)$)

Example

$(\mathbb{Z}_5)^\times = \{1, 2, 3, 4\} = \{2^4, 2^1, 2^3, 2^2\}$

Subgroups

Definition (Subgroup)

Let G be a group. The subset H of G is a **subgroup** of G if H is nonempty and H is closed under products and inverses (i.e. $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leqslant G$.

Example

Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and the subgroup $\mathbb{Z}_2 = \{0, 2\}$.

- $\mathbb{Z}_2$ is closed under the group operation of $\mathbb{Z}_4$. i.e. For any $a, b \in \mathbb{Z}_2$, $a + b$ are still in $\mathbb{Z}_2$.
- Inverses: Each element $a \in \mathbb{Z}_2$ has an inverse in $\mathbb{Z}_2$.

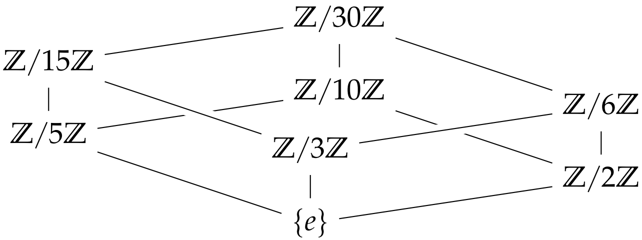
Lattice of Subgroups

Definition

Lattices of the subgroups of G are positioned in the following manner:

- Start at the bottom with the identity element e.
- Place the subgroups in ascending order with the increase in their orders until G is reached.
- Connect two subgroup vertices if $\exists$ subgroups between the two.

The lattice of subgroups of $\mathbb{Z}/30\mathbb{Z}$:



Fundamental Theorem of Cyclic Groups

Definition (Fundamental Theorem of Cyclic Groups)

For some cyclic group $G = \langle g \rangle$ of order n.

1. Every subgroup of G is cyclic.
2. If $|G| = n$, the order of all subgroups of G divides n.
3. $\forall\ k \mid n$, the subgroup $\langle g^{n/k} \rangle$ is a unique subgroup with order k.

Proof of the Fundamental Theorem of Cyclic Groups

Leading Questions and Steps Pt 1.

Q1. Can any subgroup H of G be written in the form $\langle g^d \rangle$? □

Proof.

1. Let d be the smallest positive integer such that $g^d \in H$.
2. Suffices to show that for any $g^k \in H$, that k is a multiple of d.
3. Write $k = dq + r$ so $g^k = (g^d)^q \cdot g^r$. Since $g^d, g^k \in H$, $g^r \in H$, so r must be 0 by our assumption.

□

Proof of the Fundamental Theorem of Cyclic Groups

Leading Questions and Steps Pt 2.

Q2. If $H = \langle g^d \rangle$, then does $d \mid n$? □

Proof.

1. Because $g^n = e$, and $g^{kd} \in H$, there exists an integer m such that $(g^d)^m = e$.
2. Therefore, $d \mid n$ and thus $m \mid n$.

□

Proof of the Fundamental Theorem of Cyclic Groups

Proof.

Q3. If $H = \langle g^l \rangle$, what would the order of H be? $\square$

Proof.

Letting $H = \langle g^l \rangle$, we have that the order of H is $\frac{n}{l} = k$ and therefore $l = \frac{n}{k}$. $\square$

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Let $n_1, n_2, \ldots, n_k \in \mathbb{Z}^+$ *be greater than 1 and pairwise coprime. Consider:*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ &\vdots \\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

There exists an integer x *that satisfies all these congruences simultaneously, and any two solutions* x, y *are congruent modulo* N*, where* $N = n_1 n_2 \cdots n_k$*.*

Theorem (Chinese Remainder Theorem Group Theory Version)

Let $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$*, where* $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z}^+$*. Then,*

1. $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \ldots \times \mathbb{Z}_{p_k^{\alpha_k}}$
2. $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$

Application 1 (Part I)

Theorem

The direct product $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ is a cyclic group if and only if the numbers $n_1, n_2, \ldots, nk$ are pairwise coprime.

Proof.

- Backward:
  Let $m = \text{lcm}(n_1, \ldots, n_k)$. Since $n_1, \ldots, n_k$ are pairwise coprime, $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Thus, $m = n_1 \cdot \ldots \cdot n_k$. Consider the element $g = (1, \ldots, 1)$ in $\mathbb{Z}n_1 \times \ldots \times \mathbb{Z}n_k$. By CRT, g generates the entire group, meaning every element in $\mathbb{Z}n_1 \times \ldots \times \mathbb{Z}n_k$ can be expressed as a power of g. Thus, the group is cyclic.

$\square$

Application 1 (Part II)

Theorem

The direct product $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ is a cyclic group if and only if the numbers $n_1, n_2, \ldots, n_k$ are pairwise coprime.

Proof.

- Forward:
  Let $g = (g_1, \ldots, g_k)$ be a generator of $\mathbb{Z}n_1 \times \ldots \times \mathbb{Z}_{n_k}$. Then the order of g must be the order of the group, which is $n_1 \cdot \ldots \cdot n_k$. Suppose $\exists\ n_i, n_j$ such that $\gcd(n_i, n_j) = d > 1$. Then the order of the identity element, is $n_1 \cdot \ldots \cdot n_k / d < n_1 \cdot \ldots \cdot n_k$, contradicting that g is a generator of the group. $n_1, \ldots, n_k$ must be pairwise coprime.

$\square$

Application 2

Theorem

$(\mathbb{Z}/n\mathbb{Z})^\times$ *is cyclic if and only if* $n \in \{1, 2, 4, p^k, 2p^k\}$

Application 2: Part 1

Proposition

$(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for $n > 2$.

Proof.

1. Find 2 subgroups of order 2
2. The first element:

$$(2^k - 1)^2 \equiv 1 \pmod{2^k}$$
$$= (2^k)^2 - 2(2^k) + 1 \equiv 1 \pmod{2^k}$$

3. The second element:

$$(2^{k-1} - 1)^2 \equiv 1 \pmod{2^k}$$
$$= (2^{k-1})^2 - 2(2^{k-1}) + 1 \equiv 1 \pmod{2^k}$$
$$= (2^{2k-2}) - 2^k + 1 \equiv 1 \pmod{2^k}$$

Application 2: Part 2

Proposition

For all odd $p \in \mathbb{P}$, $k \in \mathbb{Z}^+$, *there exists a generator* $u \in (\mathbb{Z}/p^k\mathbb{Z})^\times$. *That is,* $(\mathbb{Z}/p^k\mathbb{Z})^\times$ *is cyclic of order* $\varphi\left(p^k\right)$.

Application 2: Final Part

Proof.

1. We know that by Chinese Remainder Theorem, $(\mathbb{Z}/n\mathbb{Z})^\times = \prod_{i=0}^{k} (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times$.
2. So, All of the 'factors' of $(\mathbb{Z}/n\mathbb{Z})^\times$ must be cyclic as well by the Fundamental Theorem of Cyclic Groups.
3. By our previous application, no two factors, $(\mathbb{Z}/p_a^{k_a}\mathbb{Z})^\times$ and $(\mathbb{Z}/p_b^{k_b}\mathbb{Z})^\times$, for $a, b \leqslant i$ can have an even order, as it would imply $\gcd(p_a^{k_a}, p_b^{k_b}) > 1$

$\square$

Application 2: Final Part

Proof.

1. We know that $(\mathbb{Z}/p^k\mathbb{Z})^\times$ has size $\varphi\left(p^k\right) = (p-1)(p^k-1)$ which is an even number when p is odd.
2. This means that $(\mathbb{Z}/n\mathbb{Z})^\times$ can have at most a factor of one $(\mathbb{Z}/p^k\mathbb{Z})^\times$ multiplied with some $(\mathbb{Z}/2^n\mathbb{Z})^\times$.
3. We can check that $(\mathbb{Z}/2\mathbb{Z})^\times = 1$, so it is trivial, while $(\mathbb{Z}/4\mathbb{Z})^\times = 1, 3$ has an order of size 2. So the group is only cyclic when $n = 1, 2, 4, p^k, 2p^k$.

$\square$

Acknowledgements

We would like to thank the PRIMES CIRCLE program for giving us the opportunity to study this amazing topic, our mentor Zhao Yu Ma for teaching us (and making the sessions fun as well), and our parents.