
LECTURE 10 REVIEW SEP 23

Cosets

Author

Tom Jeong

September 23, 2024

Contents

1	Order of Element	3
---	------------------	---

1 Order of Element

Proposition 1.1. let G be a cyclic group

1. every subgroup of G is cyclic
2. suppose G is finite and d is a divisor of $|G|$, then there is a unique subgroup of G of order d
3. there are $\phi(d)$ elements of order d in G These are exactly the generators of the unique subgroup of order d

Corollary 2.7.6 Let N be a positive integer. Then

$$\sum_{d|N} \phi(d) = N$$

where the summ is over all divisors $d \in \text{div}(N)$

Proof.

let $G = \mathbb{Z}/N\mathbb{Z}$

$$N = \sum_{g \in G} 1 = \sum_{d|N} \underbrace{\sum_{\substack{g \in G \\ \phi(d)}} 1}_{\phi(d)} = \sum_{d|N} \phi(d) \quad \square$$

Theorem 1.2 (Euler 1.7.2). Let $a, n \in \mathbb{Z}$ be relatively prime and $n \in \mathbb{N}$ then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Proof.

Let $G = \mathbb{Z}/n\mathbb{Z}^*$ Then $|G| = \phi(n)$

Since $\gcd(a, n) = 1$ we have $[a] \in G$

By Proposition 2.6.3, $[1] = [a]^{|G|} = [a]^{\phi(n)}$ so $a^{\phi(n)} \equiv 1 \pmod{n}$

□

Take away: group can be a powerful tool for studying things that dont immediately seem to be about groups.

Definition 1.1.

Let G_1, G_2, \dots, G_n be a group; The Product of G_1, G_2, \dots, G_n is the group $G = G_1 \times G_2 \times \dots \times G_n = \{(g_1, g_2, \dots, g_n) | g_i \in G_i\}$ with the composition law $(g_1, g_2, \dots, g_n) \cdot (h_1, h_2, \dots, h_n) = (g_1 h_1, g_2 h_2, \dots, g_n h_n)$

exercise the composition is associative. identity: (e_1, e_2, \dots, e_n) inverse: $(g_1, g_2, \dots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$

ex: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\cong \mathbb{Z}/4\mathbb{Z}$ since every element in the lhs has order 2. NOte: if we have isomorphism $\phi_i : H \rightarrow G_i$ then we have an isomorphism $\phi : H \rightarrow G_1 \times G_2 \times \cdots \times G_n$ given by $\phi(h) = (\phi_1(h), \phi_2(h), \dots, \phi_n(h))$

Lemma 1.3 (cor 1.5.11 ii).

If $a, b, c \in \mathbb{Z}$ and $\gcd(a, b) = 1$ and $a|bc$ then $a|c$

Proposition 1.4 (2.8.2).

let $n_1, n_2, \dots, n_r \in \mathbb{Z}$ be pairwise relatively prime integers and let $N = n_1 n_2 \dots n_r$ then for any $a_1, a_2, \dots, a_r \in \mathbb{Z}$ we have the system of congruences

if ϕ_i denotes the canonical homomorphism $\phi_i : \mathbb{Z} \rightarrow \mathbb{Z}/n_i\mathbb{Z}$ with $\phi_i(x) = [x]$ then the map

$$\tilde{\phi} : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

given by $\tilde{\phi}([x]) = ([x], [x], \dots, [x])$ is an isomorphism.

Proof. claim $\text{Ker } \tilde{\phi} = N\mathbb{Z}$

$$x \in N\mathbb{Z} \iff x \equiv 0 \pmod{n_i} \text{ for all } i \iff [x] = ([0], [0], \dots, [0]) \iff \tilde{\phi}([x]) = ([0], [0], \dots, [0])$$

Thus, $\text{Ker } \tilde{\phi} = N\mathbb{Z}$

By the Isomorphism Theorem, $\tilde{\phi}$ is an isomorphism.

□

We'll state a big theorem about certain abelian groups .

Definition 1.2. Let G be a group and let $a_i \in G$ for $i \in I$ The smallest subgroup of G containing $\{a_i | i \in I\}$ is the subgroup generated by $\{a_i | i \in I\}$ and is denoted $\langle a_i | i \in I \rangle$ If this subgroup is all of G then we say that G is generated by $\{a_i | i \in I\}$ If there is a finite set $\{a_i | i \in I\}$ that generates G then we say that G is finitely generated.

Theorem 1.5. If G is a group and $a_i \in G$ for $i \in I$ then the subgroup H generated by $\{a_i | i \in I\}$ has elements precisely these elements that are finite products of integral powers of a_i where powers of a fixed a_i may occur several times in the product.

ex. D_3 is finitely generated by r_1, s_1 . ex. \mathbb{Z} is generated by 1. ex $\mathbb{Z} \times \mathbb{Z}$

Theorem 1.6 (fundamental Theorem of Finitely Generated Abelian groups).
every finitely generated abelian group is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}^{n_1} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

where $n_1, n_2, \dots, n_r \in \mathbb{N}$ and $n_1 | n_2 | \dots | n_r$. Where the p_i 's are prime not necessarily distinct and r_i are positive integers the direct product is unique up to reordering the factors.