Abelian finite groups

Definition: A group $\langle G, \cdot \rangle$ is a set G, closed under a binary operation $\cdot$, $(\cdot : G \times G \longrightarrow G)$ such that satisfies the following axioms:

1) $\forall\ a,b,c \in G$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

2) $\exists\ e \in G$, such that $\forall\ x \in G$

$$e \cdot x = x \cdot e = x \qquad \text{(Identity element)}$$

3) $\forall a \in G$, corresponds an element $a' \in G$, such that

$$a \cdot a' = a' \cdot a = e \qquad \text{(Inverse of } a\text{)}$$

Example:

- $\langle U, \cdot \rangle$, $\quad U = \{ z \in \mathbb{C} \ / \ |z| = 1 \{$
- $\langle U_n, \cdot \rangle$, $\quad U_n = \{ z \in \mathbb{C} \ / \ z^n = 1 \{$

Since the multiplication of complex numbers is associative, and U and U_n contains to 1.

And $e^{i\theta} \in U$, $e^{i\theta} \cdot e^{i(2\pi - \theta)} = e^{2\pi i} = 1$

proves that every element of U has inverse.

For $z \in U_n$

$$z \cdot z^{n-1} = z^n = 1$$

Shows that each $z \in U_n$, has an inverse.

- $\langle \mathbb{Z}_n, + \rangle$ $\quad \mathbb{Z}_n = \{ 0, 1, \ldots, n-1 \{$

Under the sum module n $a \equiv b \mod n$, if $a - b$ is multiple of n.

Example:

$$x + 5 = 3 \qquad \mathbb{Z}_8, \quad x = 6$$

$$5 +_8 6 = 11 \mod 8 = 3$$

Definition: A group G is Abelian if his binary operation is commutative (Abel - 1926)

Definition: If a subset H of a group G is closed under the binary operation of G and if H under the induced operation of G, is a group for itself, it is said that H is a subgroup of G, $H \leq G$.

$$\langle \mathbb{Z}, + \rangle \leq \langle \mathbb{R}, + \rangle$$

$$\langle \mathbb{Q}^+, + \rangle \not\leq \langle \mathbb{R}, + \rangle, \text{ even if } \mathbb{Q} \subseteq \mathbb{R}.$$

Theorem: Let G be a group and $a \in G$, then

$$H = \{ a^n / n \in \mathbb{Z} \}$$

is a subgroup of G and it is the smallest subgroup of G that contains to a.

Proof: To proof that $H \leq G$ it must be fulfilled that:

- H is closed under the binary operation of G.
- If $e \in G$, $e \in G$.
- $\forall\, a \in H$, $a^{-1} \in H$.

As $a^r \cdot a^s = a^{r+s}$, $r, s \in \mathbb{Z}$.

We can see that the product of two elements of H is back in H. So H is closed under the operation of G.

Also $a^0 = e$, thus $e \in H$

Furthermore, if $a^r \in H$, $a^{-r} \in H$

$a^r \cdot a^{-r} = a^{-r} \cdot a^r = e$, then $H \leq G$ ■

Definition: Let G be a group and $a \in G$. Then the subgroup $\{a^n | n \in \mathbb{Z}\}$ of G, it is called cyclic subgroup of G, generated by a and it denotes $\langle a \rangle$.

Definition: An element a, of a group G generates a G if $\langle a \rangle = G$. A group G is cyclic if there exist $a \in G$, such that $\langle a \rangle = G$.

Example:

- $\mathbb{Z}_4$, is cyclic since 1 and 3, both are generators.

$$\langle 1 \rangle \langle 3 \rangle = \mathbb{Z}_4$$

- $\langle \mathbb{Z}, + \rangle$ is cyclic since 1 and -1 are generators.

End of the introduction.

The Dual Group

Let A be a finite abelian group. The group A is called cyclic if it is generated by for an only one element, i.e., there is $\tau \in A$, called generator of A, such that

$$A = \{1, \tau, \tau^2, \ldots, \tau^{N-1}\},$$

with $N = |A|$, the cardinality of the set A.

Fundamental theorem of Finite Abelian Groups.

Any finite abelian group A, is isomorphic to the product

$$A_1 \times A_2 \times A_3 \times \ldots \times A_x$$

of cyclic groups.

(Lang, Algebra)

Let A be a finite abelian group. The character of A is a homomorphism of the group $\chi : A \longrightarrow \mathbb{T}$, to the unitary torus, i.e., χ is a map that satisfies

$$\chi(ab) = \chi(a)\chi(b)$$

$$\mathbb{T} = \{ z \in \mathbb{C} \mid |z| = 1 \}$$

Let $\hat{A}$ the set of all characters of A.

Lemma: The punctual product $(\chi, \eta) \longmapsto \chi\eta$ with

$$\chi\eta(a) = \chi(a)\eta(a)$$

makes $\hat{A}$ an abelian group. We call to $\hat{A}$ the dual group or Pontryagin's dual of A.

Proof: Let's proof that $\chi\eta$ is a character of A, when χ and η are characters..

Let $a, b \in A$.

$$\begin{aligned}(\chi\eta)(ab) &= \chi(ab)\eta(ab) \\ &= \chi(a)\chi(b)\eta(a)\eta(b) \\ &= (\chi\eta)(a)(\chi\eta)(b).\end{aligned}$$

In the same way, we can see that χ^{-1} is character of χ, where $\chi^{-1} = \chi(a)^{-1}$.

This proves that $\hat{A}$ is a subgroup of the group of all maps from A to $\mathbb{T}$. ■

Lemma: Let A be a cyclic group of order N. Let's set up a generator τ of A, i.e., $A = \{1, \tau, \tau^2, \dots, \tau^{N-1}\}$ y $\tau^N = 1$.

The characters of the characters of the group A are given by

$$\eta_\ell(\tau^k) = e^{2\pi i k \ell / N}, \quad k \in \mathbb{Z}$$

for $\ell = 0, 1, \dots, N-1$. The group $\hat{A}$ is cyclic of order N.

Proof: Let η be a character of A. Then $\eta(\tau)$ is an element $t \in \mathbb{T}$ satisfies $t^N = \eta(\tau^N) = 1$. Therefore, there exist an unique $\ell \in \{0, 1, \dots, N-1\}$ such that

$$\eta(\tau) = e^{2\pi i \ell / N}$$

Then, for all $k \in \mathbb{Z}$, we have

$$\eta_l(\tau^k) = \eta_l(\tau)^k = e^{2k\pi i l/N}$$

$a^n \quad \eta \cdot \eta \cdot \eta$

$\eta(a^n) = \eta(a \cdot \ldots \cdot a) = \eta(a)\eta(a)\ldots\eta(a) = \eta(a)^n$

which shows that every character is of the form

$$\eta_l, \text{ for some } l \in \{0, 1, \ldots, N-1\}$$

We have seen that for each finite cyclic group A, its dual $\hat{A}$ is cyclic and of the same order. This will imply that both "can" be isomorphic.

Theorem: Let A be a finite abelian group. There exist a canonical isomorphism to the bidual. $A \longmapsto \hat{\hat{A}}$ given $a \longmapsto \delta_a$ where δ_a, is the evaluation in a, i.e.,

$$\delta_a : \hat{A} \longrightarrow \mathbb{T}$$

$$\chi \longmapsto \chi(a)$$

Proof: The map $a \longmapsto \delta_a$ is a homomorphism, since

$$\delta_{ab}(\chi) = \chi(ab) = \chi(a)\chi(b) = \delta_a(\chi)\delta_b(\chi)$$

Lemma: Let A be a finite abelian group and let $a \in A$. Let's suppose that $\chi(a) = 1$, for all $\chi \in \hat{A}$, then $a = 1$.

Proof: The above lemma proves that this is true for cyclic groups. In view of the fundamental theorem of the abelian finite groups, only remains to be prove, that if the suposition is true for the groups A and B, then is valid for $A \times B$.

For this, let $(a_0, b_0) \in A \times B$, with $\eta(a_0, b_0) = 1 \ \forall \eta \in \widehat{A \times B}$, for all $\chi \in \hat{A}$ the map $\chi(a, b) = \chi(a)$ is a character of $A \times B$ and therefore $\chi(a_0) = 1$, which imply that $a_0 = 1$, and in the same way for b_0

The map $a \longmapsto \delta_a$ is an injective homomorphism from A to $\hat{\hat{A}}$.

Homework: Prove that $|A| = |\hat{A}|$.