Day 1 _ Ahmet BATAL

Group

$*: S\times S \longrightarrow S$ is a binary operation such that

- $*$ is associativity
- $*$ has identity element.
- $*$ has inverse element.

Thus $(S,*)$ is a group. $(S,*)$ is abelian if $\forall x,y \in S$,

$$x*y = y*x$$

$(S,*)$ is cyclic if every element of S can be written as a product of an element $a\in S$.

Theorem. Every cyclic group G is isomorphic to either $\mathbb{Z}_n$ or $\mathbb{Z}$.

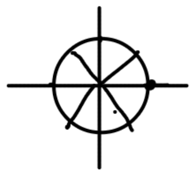
Remainder: Let $\varphi: G \to H$ and G, H be two groups. Then φ is homomorphism if $\quad \varphi(a\cdot b) = \varphi(a)\cdot\varphi(b) \quad \forall a,b\in G$.

If φ is bijection, φ is called isomorphism

$*$ $\mathcal{U}_n \subseteq \mathbb{C}^* =$ n^{th} roots of unity. $\quad (\mathbb{C}^* = \mathbb{C}\setminus\{0\})$

$$z^n = 1 = e^{2\pi k i}$$

$$z = \exp\left(\frac{2\pi k i}{n}\right), \quad 0 \le k \le n-1$$



Theorem. Every finite abelian group is isomorphic to some

$$\mathbb{Z}_{n_1}\times\dots\times\mathbb{Z}_{n_k}.$$

Here G_1, G_2 group, then

$$G_1\times G_2 = \{(a,b) \mid a\in G_1,\ b\in G_2\}$$

and $\cdot$ defined as:

$$(a,b)\cdot(c,d) = (ac, bd)$$

Definition. Let G be a group. We say χ as a character of G if it is an isomorphism from G to $\mathbb{C}^*$, i.e, $\varphi: G \longrightarrow \mathbb{C}^*$

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

Say $G^* :=$ the set of characters of G. Then G^* is an abelian group

$\varphi, \psi \in G^*$ $\quad (\varphi\psi)(a) = \varphi(a)\psi(a)$

We can also define χ_T : trivial character, i.e., for all $a\in G$,

$\chi_T(a) = 1.$

$$(\varphi\psi)(a) = \varphi(a)\cdot\underbrace{\varphi(a^{-1})}_{\psi(a)} = \varphi(a\cdot a^{-1}) = \varphi(1_G) = 1$$

Thus $\varphi\psi = \psi\varphi = \chi_T$, where $\psi(a) = \varphi(a^{-1})$

Now let G_1, G_2 be two groups and $h: G_1 \to G_2$ be an homomorphism and let χ be a character of G_2. Then $h^*\chi_2 := \chi_2 \circ h$ is an pullback of χ_2 w.r.t h

Theorem. $h^*\chi_2$ is a chacter of G_1.

$$\begin{tikzcd} G_1 \arrow[r, "h"] \arrow[dr, "\chi_2\circ h", "h^*\chi_2"'] & G_2 \arrow[d, "\chi_2"] \\ & \mathbb{C}^* \end{tikzcd}$$

Theorem. Let $G_1 \cong G_2$, then $G_1^* \cong G_2^*$

Proof. $G_1 \xrightarrow{h} G_2$ such that h is an isomorphism.

$G_1^* \xrightarrow{h^*} G_2^*$. Then h^* is an isomorphism

Let $\chi \in G_1^*$ let $\mathcal{J} = \chi \circ h^{-1}$

$\vdots$

$\square$

Tensor Product of Characters

G_1, G_2 be groups, and let χ_1, χ_2 be characters of G_1, G_2 respectively. Tensor product of $\chi_1 \otimes \chi_2 : G_1 \times G_2 \longrightarrow \mathbb{C}^*$ is defined as

$$(\chi_1 \otimes \chi_2)(ab) := \chi_1(a)\chi_2(b)$$

Theorem. All characters of $G_1 \times G_2$ is in the form $\chi_1 \otimes \chi_2$ where $\chi_1 \in G_1^*$ and $\chi_2 \in G_2^*$

Proof. Let $\chi \in (G_1 \times G_2)^*$.

Define $i_1 : G_1 \longrightarrow G_1 \times G_2$ and $i_2 : G_2 \longrightarrow G_1 \times G_2$

as $i_1(g_1) = (g_1, 1)$ and $i_2(g_2) = (1, g_2)$

Let $\chi_1 = i_1^*\chi$, $\chi_2 = i_2^*\chi$ where $\chi = \chi_1 \otimes \chi_2$

$$\begin{aligned}(\chi_1 \otimes \chi_2)^{(a,b)} &= (i_1^*\chi \otimes i_2^*\chi)^{(a,b)} = (\chi\circ i_1 \otimes \chi\circ i_2)^{(a,b)} \\ &= (\chi\circ i_1)(a)\,(\chi\circ i_2)(b) \\ &= \chi(a,1)\chi(1,b) \\ &= \chi((a,1)(1,b)), \text{ i.e., } (\chi_1 \otimes \chi_2)^{(a,b)} = \chi(a,b)\end{aligned}$$

$\square$

For finite abelian group G,

$$G \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$
$$\chi_1 \qquad \chi_k$$

For $z \in G^*$, $z = \chi_1 \otimes \cdots \otimes \chi_k$.

Characterization of Characters of $\mathbb{Z}_1$

Let $\chi \in \mathbb{Z}_n^*$ $\quad \chi(na) = \chi(a)^n$ for all $a \in \mathbb{Z}_n^*$ $an = 0$.

$$\chi(a) = 1 \in \mathbb{C}^*$$

Therefore, $\chi^n = \chi \ldots$. χ .... every a to an n^{th} rooth of unity.

$$\chi^{-1}(a) = \chi(a^{-1}) = 1/\chi(a) = \overline{\chi(a)}, \quad |\chi(a)| = 1$$
$$\bar{\chi}(a) = \overline{\chi(a)} \Rightarrow \chi^{-1} = \overline{\chi}$$

Day 2

→ $\chi : G \to \mathbb{C}^*$ homomorphism

→ G^*: the group of characters of G

→ $\chi \in (G_1 \times G_2)^* \iff \chi = \chi_1 \otimes \chi_2$, $\chi_1 \in G_1^*$ and $\chi_2 \in G_2^*$

$(G_1 \otimes G_2)^* \cong G_1^* \otimes G_2^* = \{\chi_1 \otimes \chi_2 \mid \chi_1 \in G_1^*, \chi_2 \in G_2^*\}$ G finite abelian group $G \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ for some $n_1, \ldots, n_k \in \mathbb{N}$

$G^* \simeq \mathbb{Z}_{n_1}^* \otimes \cdots \otimes \mathbb{Z}_{n_k}^*$

$\mathbb{Z}_n$, G finite cyclic, $G \simeq \mathbb{Z}_n$

$$U_n = \{\exp\left(\tfrac{2\pi i k}{n}\right) \mid 0 \leq k < n\}$$

$$U_n \simeq \mathbb{Z}_n \quad \Rightarrow \quad U_n^* \simeq \mathbb{Z}_n^*$$

Let $h \in U_n^*$, $h : U_n \to U_n$, say g be generator of U_n, i.e., $a \in G$, $a = g^i$ for some $i \in [0, n-1] \subseteq \mathbb{N}$

Thus $\quad h(a) = h(g^i) = h(g)^i$

There n distinct h since we associate g with n different element in U_n.

$i : U_n \to U_n$ $\quad U_n^*$, it is easy to show that this identity map is homomorphism, and bijective, i.e., i is isomorphism. Thus,

$$U_n^* := \{h : U_n \to U_n\} \simeq U_n \simeq \mathbb{Z}_n.$$

Therefore $\mathcal{U}_n^* \simeq \mathbb{Z}_n^* \simeq \mathbb{Z}_n \simeq \mathcal{U}_n$

Now let us characterise $\mathbb{Z}_n^*$

$$\chi_k(l) = \exp\left(2\pi i k l/n\right)$$

$$\chi_k(l)\,\chi_k(s) = \exp\left(2\pi i k(l+s)/n\right) = \chi_k(l+s)$$

It is easy to see that $\chi_k = \chi_l$ if and only if $k = l$

$$\mathbb{Z}_n^* = \left\{ \exp\left(2\pi i k/n\right) \mid 0 \leq k \leq n-1 \right\}$$

Example. $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$. Then

$$\chi_{\vec{k}} = \chi_{k_1} \otimes \cdots \otimes \chi_{k_m} \qquad \vec{k} = (k_1, \dots, k_m)$$

Let $\vec{y} \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m} \Rightarrow \chi_{\vec{k}}(\vec{y}) = \chi_{k_1}(y_1)\,\chi_{k_2}(y_2) \cdots \chi_{k_m}(y_m)$

This gives

$$\chi_{\vec{k}}(\vec{y}) = \exp\left[2\pi i \left(\frac{k_1 y_1}{m} + \cdots + \frac{k_m y_m}{m}\right)\right]$$

In particular, if all n_k's are equal let it be n $G = (\mathbb{Z}_n)^m$

$$\chi_{\vec{k}}(\vec{y}) = \exp\left[2\pi i/n\,(\vec{k}\cdot\vec{y})\right] \quad \text{where } \vec{k}\cdot\vec{y} = k_1 y_1 + \cdots + k_m y_m$$

Define

$$V_G = \{ f \mid f \text{ is a complex vector function on } G \}$$

and the operations

- $(\alpha f)(g) := \alpha f(g)$, scalar multiplication
- $(f+h)(g) := f(g) + h(g)$, addition.

$$\vec{z}\cdot\vec{w} = \sum_{i=1}^{n} z_i \overline{w_i} \qquad z \in \mathbb{C}^n \qquad z = (z_1, \dots, z_n)$$

Inner product : $\langle \cdot , \cdot \rangle = \mathbb{V} \times \mathbb{V} \to \mathbb{C}$

- $\langle \alpha v + u, z \rangle = \alpha \langle v, z \rangle + \langle u, z \rangle$
- $\langle u, v \rangle = \overline{\langle v, u \rangle}$
- $\langle v, v \rangle \geqslant 0$ and $\langle u, u \rangle = 0 \iff u = 0$

On a finite group G, V_G

$$\langle f, h \rangle := \sum_{g \in G} f(g)\,\overline{h(g)}$$

$\langle f,h\rangle = 0$, $f \perp g$ f & g are orthogonal. $|G|=n$ $\dim V_G = n$

$V_G \cong \mathbb{C}^n$. Let $\{e_1,\dots,e_n\}$ be an orthogonal basis of V_G let $f\in V_G$,

$$f=\sum_{i=1}^n \alpha_i e_i .$$

Take inner product both sides

$$\langle f,e_i\rangle = \langle \sum_{i=1}^n \alpha_i e_i , e_j\rangle$$

$$= \sum_1^n \alpha_i \langle e_i,e_j\rangle$$

$\langle f,e_j\rangle = \alpha_j\|e_j\|^2$, if $\|e_j\|=1$, then $\langle f,e_j\rangle=\alpha_j$.

$$\sum_{g\in G} f(g)\overline{h(g)} = \langle f,h\rangle$$

V_G $\delta_g: G\to\mathbb{C}$

$$\delta_g(s)=\begin{cases}1 & g=s\\ 0 & g\neq s\end{cases}$$

$$\langle\delta_g,\delta_s\rangle = \sum_{t\in G}\delta_g(t)\,\delta_s(s) = \dots \quad ?$$

$\{\delta_g \mid g\in G\}$: standart orthonormal basis

↳ abelian

$|G^*|=n$, $G=\{g_1,\dots,g_n\}$ and $G^*=\{\chi_{g_1},\dots,\chi_{g_n}\}$

Theorem. Let $\chi\in G^*$, then

$$\sum_{h\in G}\chi(h) = \begin{cases}|G|, & \chi=\chi_T\\ 0, & \text{otherwise}\end{cases}$$

If $\chi\neq\chi_T$, then $\exists g_0\in G$ such that $\chi(g_0)\neq 1$ / $\varphi_{g_0}(1)=g_0 h$

$\varphi: G - G$.

$$\sum_{h\in G}\chi(h)=\sum_{h\in G}\chi(g_0h)=\sum_{h\in G}\chi(g_0)\,\chi(h)$$

$$=\underbrace{\chi(g_0)}_{1}\underbrace{\sum_h\chi(h)}_{0}$$

Example. $G=\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k}$ and $\chi_{\vec k}(\vec y) = \exp\left[2\pi i\left(\frac{k_1y_1}{n_1}+\cdots+\frac{k_my_m}{n_m}\right)\right]$

$$\sum_{l=0}^{n-1}\exp(2\pi i k l/n) = \begin{cases} n & k=0\\ 0 & k\neq 0\end{cases}$$

net kuvvet $\vec{0}$

$$\langle \chi_g, \chi_s \rangle = 0 \quad \text{if} \quad g \neq s$$

$$\sum_{t\in G} \chi_g(t)\overline{\chi_s(t)} = \sum_{t\in G} \chi_g(t)\chi_s^{-1}(t) = \sum_{t\in G} (\chi_g \chi_s^{-1})(t)$$

These are orthogonal basis. Now, we make these orthonormal basis. Therefore,

$$\chi_g := \frac{1}{\sqrt{|G|}} \chi_g \,, \text{ then } \quad \|\chi_g\| = 1.$$

$$\Delta_G = \{ \delta_g \mid g \in G \} \qquad C_G = \{ \chi_g \mid g \in G \}$$

Fourier Transform

We will work with Fourier Transform on finite abelian G is the linear map on V_G which sends each χ_g to δ_g.

$$\hat{f}(s) = \langle f, \chi_s \rangle = \sum_t f(t)\overline{\chi_s(t)}$$

Special case : $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$

$$\chi_{\vec{s}}(x) = \exp\left[2\pi i\left(\frac{s_1 x_1}{n_1} + \cdots + \frac{s_m x_m}{n_m}\right)\right]$$

Thus $$\hat{f}(s) = \sum f(t) \exp\left[2\pi i\left(\frac{s_1 t_1}{n_1} + \cdots \frac{s_m t_m}{n_m}\right)\right]$$

Normalization : Multiply by $1/\sqrt{n_1 \cdots n_m}$

$(\mathbb{Z}_n)^m$

$$\hat{f}(s) = 1/n^{m/2} \sum_{t \in \mathbb{Z}_n^m} f(t_1, \dots, t_m) \cdot \exp\left[\frac{2\pi i}{n^m}(\vec{s} \cdot \vec{t}\,)\right)$$

Day 3.

$$\hat{f}(s) = F_f = \sum \langle f, \chi_g \rangle \delta_g \Rightarrow \hat{f}(s) = \langle f, \chi_s \rangle$$

Thus,

$$\hat{f}(s) = \sum_{g\in G} f(s) \overline{\chi_s(g)}$$
$$= 1/\sqrt{n} \sum_{t=0}^{n-1} f(t) \exp(-2\pi i s t/n) \quad \text{when } G = \mathbb{Z}_n$$

Remark. F is an isometry, also not only isomorphism and also preserves inner product, i.e.,

$$\langle F_{f_1}, F_{f_2} \rangle = \langle f_1, f_2 \rangle$$

Proof. $\langle F_{f_1}, F_{f_2} \rangle = \langle \hat{f}_1, \hat{f}_2 \rangle = \sum_{g\in G} \hat{f}_1(g) \overline{\hat{f}_2(g)}$

$$= \sum_{g\in G} \langle f_1, \chi_g \rangle \overline{\langle f_2, \chi_g \rangle}$$

and it is also

$$= \sum_{g\in G} \langle \langle f_1, \chi_g\rangle \chi_g, f_2 \rangle$$
$$= \langle \sum_{g\in G} \langle f_1, \chi_g\rangle \chi_g, f_2 \rangle$$
$$= \langle f_1, f_2 \rangle \quad \text{, i.e., } \langle \hat{f}_1, \hat{f}_2 \rangle = \langle f_1, f_2 \rangle$$

Plancheral Identity (Parseval's Identity)

$$\boxed{\sum_{g\in G} \hat{f}_1(g)\hat{f}_2(g) = \sum_{g\in G} f_1(g) f_2(g)}$$: Parseval's Identity

Take $f_1 = f_2 = f$, $\|\hat{f}\|^2 = \|f\|^2 \Rightarrow \|\hat{f}\| = \|f\|$

Thus we have $\boxed{\sum_{g\in G} |\hat{f}(g)|^2 = \sum_{g\in G} |f(g)|^2}$: Plancheral's Identity

Inverse Fourier Transform

$$F^{-1}: V_G \to V_G \quad \text{as } \delta_g \longmapsto \chi_g$$

$$F^{-1}(f) = F^{-1}\left(\sum_{g\in G} \langle f, \delta_g\rangle \delta_g\right) = \sum_{g\in G} \underbrace{\langle f, \delta_g\rangle}_{f(g)} \chi_g := \check{f}$$

Example. $G = \mathbb{Z}/n$

$$\check{f}(t) = 1/\sqrt{n} \sum_{k=0}^{n-1} f(k) \exp(2\pi i k t/n)$$
$$\hat{f}(t) = 1/\sqrt{n} \sum_{k=0}^{n-1} f(t) \exp(-2\pi i k t/n)$$

How can we write f according to $\hat{f}$?

$$f = \mathbb{1} f = F^{-1}(F_f) = F^{-1}(\hat{f})$$
$$f(t) = \sum_{g\in G} \hat{f}(g) \chi_g(t)$$
$$f(t) = 1/\sqrt{n} \sum_{k=0}^{n-1} \hat{f}(t) \exp(2\pi i k t/n).$$

Theorem. Let p be a prime and let $\mathbb{Z}_p$ be the field with p elements. Given any set $A \subseteq \mathbb{Z}_p$ of size at least $\overset{?}{100}\sqrt{p}$, we can find $x, y \in \mathbb{Z}_p$ such that

$$x+y \text{ and } xy$$

both belong to A.

Lemma. Let S be the set of squares on $\mathbb{Z}_p$. Then

$$|\hat{1}_S(r)| = \begin{cases} \frac{p+1}{2\sqrt{p}} & \text{if } r = 0 \\ 1/2 + O(1/\sqrt{p}) & \text{if } r \neq 0 \end{cases}$$

$$1_A := \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases} \quad \text{: characteristic function}$$

$$|S| = \frac{|\mathbb{Z}_p^*| + 1}{2} + 1 = p+1/2$$

Proof. $\hat{1}_S(0) = 1/\sqrt{p} \sum_{x=0}^{p-1} 1_S(x) \exp\left(\frac{2\pi i \cdot 0 \cdot x}{p}\right) = \frac{|S|}{\sqrt{p}} = \frac{p+1}{2\sqrt{p}}$

If $r \neq 0$,

$$\hat{1}_S(r) = 1/\sqrt{p} \sum_{x=0}^{p-1} 1_S(x) \exp\left(\frac{-2\pi i \cdot r \cdot x}{p}\right)$$

$$= 1/\sqrt{p} + \frac{1}{2\sqrt{p}} \underbrace{\sum_{x\neq 0} \exp(-2\pi i r x^2/p)}_{\text{Gauss Sum}-1 := Y}$$

counted doubly

$:z$

$$|z|^2 = \left| \sum_{x\in\mathbb{Z}_p} \exp\left(\frac{-2\pi i r x^2}{p}\right)\right|^2$$

$$= \sum_{x\in\mathbb{Z}_p} \exp\left(\frac{-2\pi i r x^2}{p}\right) \sum_{y\in\mathbb{Z}_p} \exp\left(\frac{2\pi i r y^2}{p}\right)$$

$$= \sum_{x,y\in\mathbb{Z}_p} \exp\left(-2\pi i r (x^2-y^2)/p\right)$$

$$= \sum_{x,y\in\mathbb{Z}_p} e^{-2\pi i r (x-y)(x+y)/p} \qquad \text{Say } \begin{matrix} \nu = x-y \\ \gamma = x+y \end{matrix}$$

$$= \sum_{\nu} \sum_{\gamma} \exp(-2\pi i r \nu \gamma/p) = \begin{cases} 0 & \nu \neq 0 \\ p & \nu = 0 \end{cases}$$

$a, b \in A$, $p(t) = t^2 - at + b$. Suppose there exist roots of $p(t)$ in $\mathbb{Z}_p$. $t^2 - at + b = (t-x)(t-y) = t^2 - (x+y)t + xy$

Now, Theorem says equivalently "$\exists a,b \in A$ $p(t) = t^2 - at + b$ has roots

$$x_{1,2} = 2^{-1}(a \pm \sqrt{a^2-4b}) \text{ in } \mathbb{Z}_p$$

$S = \sqrt{a^2-4b}$, $S^2 = a^2-4b$

and also equivalently $\equiv$ "$\exists a,b \in A$ such that a^2-4b is square in $\mathbb{Z}_p$.

$$\equiv \sum_{a,b\in A} 1_S(a^2-4ab) > 0, \quad p > 2.$$

Then we have

$$\sum_{r\in\mathbb{Z}_p} 1/\sqrt{p} \sum_{a,b\in\mathbb{Z}_p} 1_S(r) \exp(2\pi i r [a^2-4b]/p)$$

Say $M = 1/\sqrt{p} \sum_{a,b\in A} 1_S(0) = 1/\sqrt{p} \frac{p+1}{2\sqrt{p}} \sum_{a,b\in A} 1 = |A|^2(p+1)/2p > |A|^2/2$

$M_0 = M \quad \sum_r M_r \quad E = \sum_{r\neq} M_r$

$$E = \frac{1}{\sqrt{p}} \sum_{r\neq 0} \hat{1}_S(r) \sum_{a,b\in A} \exp(2\pi i r [a^2-4b]/p)$$

$$|E| \leq 1/\sqrt{p} \sum_{r\neq 0} |\hat{1}_S(r)| \left|\sum_{a,b\in A} \exp(2\pi i r [a^2-4ab]/2)\right| \qquad |\hat{1}_S(r)| \approx 1/2 + \dots \leq 1$$

$$|E| \leq 1/\sqrt{p} \sum_{r\neq 0} \left|\sum_{a\in A} \exp(2\pi i r a^2/p)\right| \left|\sum_{b} \exp(2\pi i r(-4b)/p)\right|$$

$$|E|^2 \leq 1/p \left(\sum_{r\neq 0} \left|\sum_{a\in A} \exp(2\pi i r a^2/p)\right|^2\right) \left(\sum_{r\neq 0} \underbrace{\left|\sum_{b\in A} \exp\left(2\pi i r(-4b)/p\right)\right|}_{\hat{1}_A(4r)}{}^2\right)$$

$$\hat{1}_A(s) = 1/\sqrt{p} \sum_{x \in \mathbb{Z}_p} 1_A(x) \exp\left(\frac{-2\pi i s x}{p}\right) = 1/\sqrt{p} \sum_{x \in A} \exp\left(\frac{-2\pi i 4 r x}{p}\right)$$

$$P_2 = p \sum_{r \in \mathbb{Z}_p} |\hat{1}_A(4r)|^2 = p \cdot \sum_{x \in \mathbb{Z}_p} |1_A(x)|^2 = p \cdot |A|.$$

$$\hat{f}(-r) = \sum_{a \in A} \exp\left(2\pi i r a^2/p\right) = \sum_{x \in \mathbb{Z}_p} \exp\left(2\pi i r x/p\right) \cdot f(x)$$

$$f(x) = |\{a \in A \mid a^2 = x\}|$$

$$P_1 = \sum_{r \in \mathbb{Z}_p} |\hat{f}(-r)|^2 = \sum_{x \in \mathbb{Z}_p} |f(x)|^2$$
$$\leq 4|A|$$

Thus,

$$|E|^2 \leq \frac{1}{p} 4|A| p \cdot p|A| = 4|A|^2 p \Rightarrow |E| \leq 2|A|\sqrt{p}$$

$M \geq |A|^2/2$ $\qquad$ $|E|/M \leq \frac{4|A|\sqrt{p}}{|A|^2} = \frac{4\sqrt{p}}{|A|} < 1$ if $|A| > 4\sqrt{p}$

$|E| < M$

Thus $|M+E| = |M-(-E)| \geq ||M| - |-E|| \geq |M| - |E| \geq M - |E|$
$> 0.$