INTRODUCTION TO HARMONIC ANALYSIS OVER FINITE FIELDS

ELAD ZELINGHER

1. Finite Abelian groups

Let G be a finite abelian group. We denote by $\hat{G}$ the collection of characters (i.e. homomorphisms) $\chi : G \to \mathbb{C}^{\times}$. $\hat{G}$ has a group structure by pointwise multiplication, and is called the character group of G. Note that since $\chi^{|G|} = 1$, we have that $|\chi(g)| = 1$ for every $g \in G$, and therefore $\chi(-g) = \chi(g)^{-1} = \overline{\chi(g)}$.

Example 1. Let $G = \mathbb{Z}/n\mathbb{Z}$. Then $\chi(1)^n = \chi(n) = \chi(0) = 1$, and therefore $\chi(1) = e^{\frac{2\pi i k}{n}}$ for some k, and then $\chi(j) = \chi(1)^j = e^{\frac{2\pi i k}{n} j}$. It can be verified that $\chi_k(j) = e^{\frac{2\pi i k}{n} j}$ is indeed a character of G. Therefore we have that $G \cong \hat{G}$ by $k \mapsto \chi_k$.

Example 2. Let G, H be two finite abelian groups. Then $\hat{G} \times \hat{H} \cong \widehat{G \times H}$ by $(\chi, \mu) \mapsto (g, h) \mapsto \chi(g)\mu(h)$.

Recall that if G is a finite abelian group, then G is isomorphic to a finite product of finite cyclic groups. Therefore we have

Corollary 3. $G \cong \hat{G}$.

This isomorphism is far from being canonical, it depends on the choice of generators for the cyclic groups.

We will now use the character group $\hat{G}$ in order to expand functions $f : G \to \mathbb{C}$ in terms of characters. Denote $S(G) = \{f : G \to \mathbb{C}\}$ the space of all functions from G to $\mathbb{C}$. We have an inner product defined on $S(G)$ by

$$\langle f_1, f_2 \rangle = \sum_{g \in G} f_1(g) \overline{f_2(g)} \qquad f_1, f_2 \in S(G).$$

Lemma 4. *Let* $\chi_1, \chi_2 \in S(G)$. *Then* $\langle \chi_1, \chi_2 \rangle = \begin{cases} 0 & \chi_1 \neq \chi_2 \\ |G| & \chi_1 = \chi_2 \end{cases}$.

Proof. If $\chi_1 = \chi_2 = \chi$ then $\langle \chi_1, \chi_2 \rangle = \sum_{g \in G} \chi(g) \overline{\chi(g)} = \sum_{g \in G} 1 = |G|$.

If $\chi_1 \neq \chi_2$, then there exists $g_0 \in G$ with $\chi_1(g_0) \neq \chi_2(g_0)$ and then

$$\begin{aligned} \langle \chi_1, \chi_2 \rangle &= \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} \\ &= \sum_{g \in G} \chi_1(g_0 + g) \overline{\chi_2(g_0 + g)} \\ &= \chi_1(g_0) \chi_2(g_0)^{-1} \langle \chi_1, \chi_2 \rangle, \end{aligned}$$

and since $\chi_1(g_0) \chi_2(g_0)^{-1} \neq 1$, we get $\langle \chi_1, \chi_2 \rangle = 0$. $\square$

Since we know that $S(G)$ is a vector space of dimension $|G|$ over $\mathbb{C}$, and since $\left|\hat{G}\right| = |G|$, we have that

Corollary 5. *The set* $\left(\frac{1}{\sqrt{|G|}}\chi\right)_{\chi\in\hat{G}}$ *forms an orthonormal basis for* $S(G)$.

Given a function $f \in S(G)$, we can write its expansion with respect to this basis by

$$f = \sum_{\chi\in\hat{G}} \left\langle f, \frac{1}{\sqrt{G}}\chi \right\rangle \frac{1}{\sqrt{G}}\chi.$$

We denote $\hat{f}(\chi) = \left\langle f, \frac{1}{\sqrt{G}}\chi^{-1}\right\rangle$. $\hat{f}$ is a function $\hat{f} : \hat{G} \to \mathbb{C}$, i.e. $\hat{f} \in S\left(\hat{G}\right)$. Then we have $f = \sum_{\chi\in\hat{G}} \hat{f}\left(\chi^{-1}\right) \frac{1}{\sqrt{G}}\chi$. From this expansion we get Plancherel's theorem:

Theorem 6 (Plancherel)**.** *The map* $f \mapsto \hat{f}$ *is unitary.*

Proof. Since $\left(\frac{1}{\sqrt{G}}\chi\right)_{\chi\in\hat{G}}$ is an orthonormal basis, we have that $\|f\|^2 = \sum_{\chi\in\hat{G}} \left|\hat{f}\left(\chi^{-1}\right)\right|^2 = \sum_{\chi\in\hat{G}} \left|\hat{f}(\chi)\right|^2 = \left\|\hat{f}\right\|^2$, and therefore $f \mapsto \hat{f}$ preserves length and is unitary. □

We have a canonical map $\varphi : G \to \hat{\hat{G}}$ by $\varphi(g)(\chi) = \chi(g)$. One can check that this is an isomorphism. By definition

$$\begin{aligned}\hat{f}(\chi) = \left\langle f, \chi^{-1}\right\rangle &= \sum_{g\in G} f(g) \frac{1}{\sqrt{|G|}}\chi(g) \\ &= \sum_{g\in G} f(g) \frac{1}{\sqrt{|G|}}\varphi(g)(\chi).\end{aligned}$$

Therefore the coefficient of $\varphi(g)^{-1} = \varphi(-g)$ in $\hat{f}(\chi)$ is $f(-g)$, and we get

Theorem 7 (Fourier Inversion formula)**.** $\hat{\hat{f}}(\varphi(g)) = f(-g)$. *If we write* g *for* $\varphi(g)$ *(identifying* $\hat{\hat{G}}$ *with* G *via* φ*), we have* $\hat{\hat{f}}(g) = f(-g)$.

2. Finite fields

Let $\mathbb{F}$ be a finite field. Then $\mathbb{F}$ is a finite extension of $\mathbb{F}_p$ for $p = \operatorname{char}\mathbb{F}$. Denote $k = [\mathbb{F} : \mathbb{F}_p]$. Let $\psi^0 : \mathbb{F}_p \to \mathbb{C}^\times$ be a nontrivial character. Denote $\psi = \psi^0 \circ \operatorname{Tr}_{\mathbb{F}/\mathbb{F}_p} \in \hat{\mathbb{F}}$. Consider the map $\mathbb{F} \to \hat{\mathbb{F}}$ defined by $a \mapsto \psi_a$, where $\psi_a(x) = \psi(ax) = \psi^0\left(\operatorname{Tr}_{\mathbb{F}/\mathbb{F}_p}(ax)\right)$. This is a homomorphism, and it is injective: let $b \in \mathbb{F}$ with $\operatorname{Tr}(b) \neq 0$ (such b exists because $\operatorname{Tr}_{\mathbb{F}/\mathbb{F}_p} b = 0 \iff b^{p^{k-1}} + b^{p^{k-1}} + \cdots + b = 0$, this is a polynomial of degree p^{k-1}, and therefore can has at most p^{k-1} roots. Therefore there exists an element of $\mathbb{F}$ with $\operatorname{Tr}_{\mathbb{F}/\mathbb{F}_p}(b) \neq 0$). Then if $a \neq 0$, $\psi_a\left(\frac{1}{\operatorname{Tr}(b)} ba^{-1}\right) = \psi^0(1) \neq 1$.

Since $|\mathbb{F}| = \left|\hat{\mathbb{F}}\right|$, the map $a \mapsto \psi_a$ is an isomorphism $\mathbb{F} \to \hat{\mathbb{F}}$.

Corollary 8. *Let* $\psi : (\mathbb{F}, +) \to \mathbb{C}^\times$ *be a non-trivial character. Then for every* $\psi' \in \hat{\mathbb{F}}$ *there exists a unique* $a \in \mathbb{F}$*, such that* $\psi'(x) = \psi(ax)$.

Recall that for $\mathbb{R}$, we have that every unitary character is of the form $x \mapsto e^{i\xi x}$, for some $\xi \in \mathbb{R}$.

For a non-trivial character $\psi : \mathbb{F} \to \mathbb{C}$, denote $\psi_a : \mathbb{F} \to \mathbb{C}$ by $\psi_a(x) = \psi(ax)$. We will denote the Fourier transform of $f \in S(\mathbb{F})$ with respect to the character ψ by $(\mathcal{F}_\psi f)(a) = \hat{f}(\psi_a)$, i.e.

$$(\mathcal{F}_\psi f)(a) = \hat{f}(\psi_a) = \left\langle f, \frac{1}{\sqrt{|\mathbb{F}|}} \psi_a^{-1} \right\rangle = \frac{1}{\sqrt{|\mathbb{F}|}} \sum_{x \in \mathbb{F}} f(x)\, \psi(ax).$$

Under this identification $(\mathcal{F}_\psi \mathcal{F}_\psi f)(x) = f(-x)$, and $\left(\mathcal{F}_{\psi^{-1}} \mathcal{F}_\psi f\right)(x) = f(x)$, where the latter follows from the relation $\left(\mathcal{F}_{\psi^{-1}} f\right)(a) = (\mathcal{F}_\psi f)(-a)$.

2.1. **Mellin transform.** Given a function $f : \mathbb{F}^\times \to \mathbb{C}$, its Mellin transform is the function $\mathcal{M}f : \widehat{\mathbb{F}^\times} \to \mathbb{C}$ defined by $(\mathcal{M}f)(\theta) = \frac{1}{|\mathbb{F}^\times|} \sum_{x \in \mathbb{F}^\times} f(x)\, \theta(x)$. This is exactly the Fourier transform of f with respect to the abelian group $\mathbb{F}^\times$.

Given a function $f : \mathbb{F} \to \mathbb{C}$, we can restrict it to $\mathbb{F}^\times$ and then take its Mellin transform. By abuse of notation denote this as $\mathcal{M}(f)$. A natural question to ask is what is the relation between $\mathcal{M}(f)$ and $\mathcal{M}(\mathcal{F}_\psi f)$.

Example 9 (Tate)**.** The characters on $\mathbb{R}^\times$ are of the form $x \mapsto |x|^s$ and $x \mapsto |x|^s \cdot \operatorname{sgn} x$ for $s \in \mathbb{C}$. The Mellin transform of a function $f : \mathbb{R} \to \mathbb{C}$ is the function

$$(\mathcal{M}f)(\theta) = \begin{cases} \int_{-\infty}^{\infty} f(x)\, |x|^s \frac{dx}{|x|} & \theta = |x|^s, \\ \int_{-\infty}^{\infty} f(x)\, |x|^s \operatorname{sgn} x \frac{dx}{|x|} & \theta = |x|^s \operatorname{sgn} x \end{cases}.$$

The Fourier transform of a function with respect to the character $\psi(x) = e^{-2\pi i x}$ is $(\mathcal{F}_\psi f)(y) = \int_{-\infty}^{\infty} f(x)\, e^{-2\pi i x y} dx$. We have the following relation

$$(\mathcal{M}f)(\theta) = \gamma(\theta, \psi)^{-1} \left(\mathcal{M}(\mathcal{F}_\psi f)\right)\left(\hat{\theta}\right),$$

where $\hat{\theta}(x) = \frac{|x|}{\theta(x)}$ and

$$\gamma(\theta, \psi)^{-1} = \begin{cases} 2^{1-s} \pi^{-s} \cos\left(\frac{\pi}{2} s\right) \Gamma(s) & \theta = |x|^s, \\ 2^{1-s} \pi^{-s} \sin\left(\frac{\pi}{2} s\right) \Gamma(s)\, i & \theta = |x|^s \operatorname{sgn} x \end{cases}.$$

Theorem 10 (Tate's local functional equation analog)**.** *Denote for $f \in S(\mathbb{F})$ and $\theta \in \widehat{\mathbb{F}^\times}$,*

$$Z(f, \theta) = \sum_{x \in \mathbb{F}^\times} f(x)\, \theta(x) = \sqrt{|\mathbb{F}^\times|}\, (\mathcal{M}f)(\theta).$$

Then

$$\frac{1}{\sqrt{|\mathbb{F}|}} f(0) \sum_{x \in \mathbb{F}^\times} \theta(x) + \gamma(\theta, \psi)\, Z(f, \theta) = Z\left(\mathcal{F}_\psi f, \theta^{-1}\right),$$

where $\gamma(\theta, \psi) = \frac{1}{\sqrt{|\mathbb{F}|}} \sum_{x \in \mathbb{F}^\times} \theta^{-1}(x)\, \psi(x)$.

Proof. If $\theta = 1$ then

$$\begin{aligned} Z\left(\mathcal{F}_\psi f, \theta^{-1}\right) &= \sum_{x\in\mathbb{F}^\times} \mathcal{F}_\psi f(x) \\ &= \frac{1}{\sqrt{|\mathbb{F}|}} \sum_{x\in\mathbb{F}^\times} \sum_{y\in\mathbb{F}} f(y)\,\psi(xy) \\ &= \frac{1}{\sqrt{|\mathbb{F}|}} \sum_{x\in\mathbb{F}^\times} \sum_{y\in\mathbb{F}^\times} f(y)\,\psi(xy) + \frac{1}{\sqrt{|\mathbb{F}|}} \sum_{x\in\mathbb{F}^\times} f(0)\cdot 1 \\ &= \frac{1}{\sqrt{\mathbb{F}}} \sum_{x\in\mathbb{F}^\times} \underbrace{\theta^{-1}(x)}_{=1}\psi(x) \sum_{y\in\mathbb{F}^\times} f(y) + \frac{f(0)}{\sqrt{|\mathbb{F}|}} \sum_{x\in\mathbb{F}^\times} \underbrace{\theta(x)}_{=1} \end{aligned}$$

If $\theta \neq 1$, then $\sum_{x\in\mathbb{F}^\times}\theta(x) = 0$. We prove that $Z(f_1,\theta)\,Z\left(\mathcal{F}_\psi f_2, \theta^{-1}\right) = Z(f_2,\theta)\,Z\left(\mathcal{F}_\psi f_1,\theta^{-1}\right)$, for every f_1, f_2. Then we choose a good substitution for f_2.

$$\begin{aligned} Z(f_1,\theta)\,Z\left(\mathcal{F}_\psi f_2,\theta^{-1}\right) &= \sum_{x\in\mathbb{F}^\times} f_1(x)\,\theta(x) \sum_{y\in\mathbb{F}^\times} \mathcal{F}_\psi f_2(y)\,\theta\left(y^{-1}\right) \\ &= \frac{1}{\sqrt{|\mathbb{F}|}} \sum_{x\in\mathbb{F}^\times}\sum_{y\in\mathbb{F}^\times}\sum_{z\in\mathbb{F}} f_1(x)\,f_2(z)\,\theta\left(xy^{-1}\right)\psi(zy) \end{aligned}$$

If $z = 0$, we get a sum $\sum_{y\in\mathbb{F}^\times}\theta\left(xy^{-1}\right) = 0$, as $\theta^{-1}\neq 1$. Therefore we have

$$\begin{aligned} Z(f_1,\theta)\,Z\left(\mathcal{F}_\psi f_2,\theta^{-1}\right) &= \frac{1}{\sqrt{|\mathbb{F}|}} \sum_{x\in\mathbb{F}^\times}\sum_{y\in\mathbb{F}^\times}\sum_{z\in\mathbb{F}^\times} f_1(x)\,f_2(z)\,\theta\left(xy^{-1}\right)\psi(zy) \\ &= \frac{1}{\sqrt{|\mathbb{F}|}} \sum_{x\in\mathbb{F}^\times}\sum_{y\in\mathbb{F}^\times}\sum_{z\in\mathbb{F}^\times} f_1(x)\,f_2(z)\,\theta\left(xzy^{-1}\right)\psi(y)\,. \end{aligned}$$

It is clear that the last sum is symmetric with respect to f_1, f_2, and therefore

$$Z(f_1,\theta)\,Z\left(\mathcal{F}_\psi f_2,\theta^{-1}\right) = Z(f_2,\theta)\,Z\left(\mathcal{F}_\psi f_1,\theta^{-1}\right).$$

Now take $f_2 = \delta_1$ the indicator function of 1, then $(\mathcal{F}_\psi f_2)(y) = \frac{1}{\sqrt{|\mathbb{F}|}}\psi(y)$. Therefore we have $Z(f_2,\theta) = 1$ and $Z\left(\mathcal{F}_\psi f_2,\theta^{-1}\right) = \frac{1}{\sqrt{|\mathbb{F}|}}\sum_{x\in\mathbb{F}^\times}\theta^{-1}(x)\,\psi(x) = \gamma(\theta,\psi)$, i.e. we proved that for every $f\in S(\mathbb{F})$, $Z(f,\theta)\,\gamma(\theta,\psi) = Z\left(\mathcal{F}_\psi f,\theta^{-1}\right)$. □

For $\theta \neq 1$ we have that

$$\begin{aligned} \gamma(\theta,\psi)\,Z(f,\theta) &= Z\left(\mathcal{F}_\psi f,\theta^{-1}\right) \\ Z(f,\theta) = Z\left(\mathcal{F}_{\psi^{-1}}\mathcal{F}_\psi f,\theta\right) &= \gamma\left(\theta^{-1},\psi^{-1}\right) Z\left(\mathcal{F}_\psi f,\theta^{-1}\right) \\ &= \gamma\left(\theta^{-1},\psi^{-1}\right)\gamma(\theta,\psi)\,Z(f,\theta)\,, \end{aligned}$$

and therefore $\gamma\left(\theta^{-1},\psi^{-1}\right)\gamma(\theta,\psi) = 1$. By definition $\overline{\gamma(\theta,\psi)} = \gamma\left(\theta^{-1},\psi^{-1}\right)$, and therefore $|\gamma(\theta,\psi)| = 1$, i.e. $\sum_{x\in\mathbb{F}^\times}\theta^{-1}(x)\,\psi(x)$ has norm $\sqrt{|\mathbb{F}|}$.

3. Quadratic reciprocity law

Let q be an odd prime. Let $\mathbb{F}_q$ be a field with q elements. A character $\theta_q : \mathbb{F}_q^\times \to \mathbb{C}^\times$ is a quadratic character if $\theta_q : \mathbb{F}_q^\times \to \{\pm 1\}$. Such a non-trivial character exists and is unique: let ξ be a generator of the cyclic group $\mathbb{F}_q^\times$. Then $\theta : \mathbb{F}_q^\times \to \mathbb{C}^\times$

is determined by the image of ξ. Therefore $\theta_q\left(\xi^k\right)=(-1)^k$ is the unique non-trivial quadratic character on $\mathbb{F}_q^\times$. Furthermore, recall that for every $a\in\mathbb{F}_q^\times$ we have $a^{q-1}=1$. Then $a^{\frac{q-1}{2}}\equiv\pm1$. Therefore we have a character $\mathbb{F}_q^\times\to\{\pm1\}\subseteq\mathbb{C}^\times$ by $a\mapsto a^{\frac{q-1}{2}}$. Note that $\xi^{\frac{q-1}{2}}\neq1$, as ξ is a generator of the cyclic group, and therefore $\xi^{\frac{q-1}{2}}=-1$, which implies that the above two characters agree, i.e. $\theta_q(a)\equiv a^{\frac{q-1}{2}}\ (\mod q)$. Finally note that if $a=b^2$, then $a^{\frac{q-1}{2}}=b^{q-1}=1$, now $\theta_q\left(\xi^k\right)=1$ if k is even (and then $\xi^k=\left(\xi^{\frac{k}{2}}\right)^2$ is a square), and $\theta_q\left(\xi^k\right)=-1$ if k is odd (and then ξ^k can't be a square). We denote $\theta_q(a)=\left(\frac{a}{q}\right)$ the Legendre symbol.

Let p,q be odd primes with $p\neq q$. Let $\psi:\mathbb{F}_q\to\mathbb{C}^\times$ be a non-trivial additive character, and let $\theta_q:\mathbb{F}_q^\times\to\mathbb{C}^\times$ be a non trivial quadratic character. Then $\theta_q^2=1$, which implies $\gamma\left(\theta_q^{-1},\psi^{-1}\right)=\gamma\left(\theta_q,\psi^{-1}\right)=\theta_q(-1)\gamma(\theta_q,\psi)$. Denote $\tau=\sum_{x\in\mathbb{F}_q^\times}\theta_q^{-1}(x)\psi(x)$, then $\tau^2=\theta_q(-1)\cdot q$. Note that since $\gcd(p,q)=1$,

$$\sum_{x\in\mathbb{F}_q^\times}\theta_q^{-1}(x)\psi(px)=\theta_q(p)\sum_{x\in\mathbb{F}_q^\times}\theta_q^{-1}(x)\psi(x)=\theta_q(p)\tau.$$

Now $\tau\in\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]$ is an algebraic integer. We claim that the map $\mathbb{Z}/p\mathbb{Z}\to\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]/p\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]$ is an inclusion: otherwise $j\in p\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]$ for some $0<j<p$, which implies that $\frac{j}{p}$ is an algebraic integer, which is a contradiction.

Passing to the quotient $\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]/p\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]$ we have that $\tau^2=\theta_q(-1)\cdot q$ implies that τ is invertible in the quotient, as q and $\theta_q(-1)$ are invertible modulo $p\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]$. Next we consider

$$\begin{aligned}\tau^p&\equiv\sum_{x\in\mathbb{F}_q^\times}\theta_q^{-p}(x)\psi(px)\left(\mod p\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]\right)\\&=\sum_{x\in\mathbb{F}_q^\times}\theta_q^{-1}(x)\psi(px)\left(\mod p\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]\right)\\&=\theta_q(p)\tau\left(\mod p\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]\right).\end{aligned}$$

Now $\tau^p=\tau\cdot\left(\tau^2\right)^{\frac{p-1}{2}}=\tau\cdot\theta_q(-1)^{\frac{p-1}{2}}\cdot q^{\frac{p-1}{2}}$, and on the other hand $\tau^p=\theta_q(p)\tau\left(\mod p\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]\right)$, therefore modulo $p\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]$ we get $\theta_q(p)\tau=\theta_q(-1)^{\frac{p-1}{2}}\cdot q^{\frac{p-1}{2}}\tau\left(\mod p\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]\right)$. Since τ is invertible modulo $p\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]$, we have $\theta_q(p)=\theta_q(-1)^{\frac{p-1}{2}}\cdot q^{\frac{p-1}{2}}\left(\mod p\mathbb{Z}\left[e^{\frac{2\pi i}{q}}\right]\right)$. Using the fact that $\left(\frac{q}{p}\right)=q^{\frac{p-1}{2}}\ (\mod p)$ and $\theta_q(a)=\left(\frac{a}{q}\right)$, $\theta_q(-1)=(-1)^{\frac{q-1}{2}}$, we get

$$\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right),$$

which implies $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.