Fourier Analysis on Finite Abelian Groups and Applications

Summer Course Sponsored by GSM

Tefjol Pllaha

July 22, 2018

Contents

The intent of these notes is to facilitate going through the first part of the book *"Fourier Analysis on Finite Groups and Applications"* by Audrey Terras. Please read with caution and be aware of typos as they are unedited.

1 Toolbox

This section will be roughly based on chapter one of the book. We will review the necessary machinery from modular arithmetic, and then give some motivation by drawing connections with analysis. Since we will be dealing almost exclusively with finite abelian groups, unless otherwise stated, any group will be finite and abelian.

Let $\mathbb{Z}$ be the ring of whole numbers. For any natural number $n \in \mathbb{N}$, denote $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$. That is, elements of $\mathbb{Z}_n$ are equivalence classes $\overline{a} := \{b \in \mathbb{Z} \mid n|(b-a)\}$. Two representatives of the same equivalence class are called *congruent* (modulo n), and in this case we will write $a \equiv b \bmod n$. Then $\mathbb{Z}_n = \{\overline{a} \mid 0 \leq a < n\}$ is again a ring with multiplication and addition given by

$$\overline{a} + \overline{b} := \overline{a+b} \text{ and } \overline{a} \cdot \overline{b} := \overline{a \cdot b}. \tag{1.1}$$

We will refer to the ring $\mathbb{Z}_n$ as the *finite circle*. Convince yourself that this is an appropriate name. Throughout we will pay special attention to the finite circle for two major reasons. The first one is that every cyclic group of order n is isomorphic with the additive group of $\mathbb{Z}_n$. The second reason is the following.

Theorem 1.1 (Fundamental Theorem of Finite Abelian Groups)**.** *Every finite abelian group is the direct product of some finite circles.*

We will denote $\mathbb{Z}_n^*$ the *group of units* of $\mathbb{Z}_n$, that is,

$$\mathbb{Z}_n^* := \{\overline{a} \in \mathbb{Z}_n \mid \exists\, \overline{b} \in \mathbb{Z}_n \text{ such that } \overline{a} \cdot \overline{b} = \overline{1}\}. \tag{1.2}$$

Proposition 1.2. $\overline{a} \in \mathbb{Z}_n^* \iff \gcd(a,n) = 1$.

Proof. By the very definition of the group of units, $\overline{a} \in \mathbb{Z}_n^*$ iff there exists $\overline{b} \in \mathbb{Z}_n$ such that $\overline{a \cdot b} = \overline{1}$. The latter happens precisely when $n|(1-ab)$. In other words, precisely when there exists $k \in \mathbb{Z}$ such that $1 = ab + kn$. But this is just the *Bézout's Identity*[1] for a and n. Thus $\gcd(a,n) = 1$. □

Theorem 1.3. *$\mathbb{Z}_n$ is a field iff n is prime.*

Proof. Since $\mathbb{Z}_n$ is a field, every nonzero element has a multiplicative inverse. That is $\mathbb{Z}_n^* = \mathbb{Z}_n - \{\overline{0}\}$. Thus for all $1 \leq a < n$, by Proposition 1.2 we have $\gcd(a,n) = 1$. This implies that n is prime. Now note that all the implications in the proof of the forward direction are actually equivalences. □

Remark 1.4. Let p be a prime. Then $\mathbb{Z}_p$ is a field by Theorem 1.3. In particular this implies that $\mathbb{Z}_p$ is a *domain*[2]. However this can also be seen directly as follows. Assume $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{0}$. Thus $p|ab$. Since p is prime it follows that $p|a$ or $p|b$. Thus $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.

A Sweet Little Trick 1.5. Many things get simplified a lot in a finite world. One of the reasons is Exercise 1.20. Let's see Exercise 1.20 in action. Let R be a finite commutative ring, which in addition is also a domain. Fix $0 \neq a \in R$. Define the map $m_a : R \longrightarrow R$, $x \longmapsto ax$. Note first that m_a is injective. Indeed $m_a(x) = m_a(y)$ iff $a(x-y) = 0$. Since R is a domain and $a \neq 0$ we may conclude $x = y$. But then m_a is also surjective. Thus, for $1 \in R$, there exists $b \in R$ such that $ab = m_a(b) = 1$. In other words, every nonzero element is a unit and thus R is a field.

[1] Bézout's Identity: $\gcd(a,b) = d \iff \exists r, s \in \mathbb{Z}$ such that $d = ra + sb$.

[2] $\overline{a} \cdot \overline{b} = \overline{0} \implies \overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.

Theorem 1.6 (Chinese Reminder Theorem)**.** *Let $n, m \in \mathbb{N}$ be two natural numbers such that* $\gcd(n, m) = 1$*. Then $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$*

Proof. See Dummit and Foote, along with the observation[3] that $\gcd(n, m) = 1$ iff the ideals $n\mathbb{Z}$ and $m\mathbb{Z}$ are comaximal. □

Definition 1.7. The map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}$ given by

$$\begin{aligned}\phi(n) &:= |\{a \mid 1 \le a \le n-1 \text{ and } \gcd(a, n) = 1\}| \\ &= |\mathbb{Z}_n^*| \qquad \text{(By Proposition 1.2)}\end{aligned}$$

is called *Euler's function.*

A useful tool for computing Euler's function is the following.

Theorem 1.8. *Euler's function is multiplicative. That is $\phi(nm) = \phi(n)\phi(m)$ for all $n, m \in \mathbb{N}$ such that* $\gcd(n, m) = 1$*.*

Proof. One can prove the statement using elementary counting arguments. However, this is an immediate consequence of the definition and Theorem 1.6. □

Example 1.9. By the very definition of ϕ we have $\phi(n) = n - 1$ iff n is prime; compare this with Theorem 1.3. Convince yourself that for any prime power we have

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right). \tag{1.3}$$

Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be written in its prime decomposition. Then $\gcd(p_i^{k_i}, p_j^{k_j}) = 1$ for all $i \ne j$, and thus by Theorem 1.8 we have

$$\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right). \tag{1.4}$$

The latter is called *Euler's product formula.*

Exercise 1.10. Show that Euler's function satisfies

$$\sum_{d|n} \phi(d) = \sum_{d|n} \phi\left(\frac{n}{d}\right), \tag{1.5}$$

and then use (1.5) to show that $\sum_{d|n} \phi(d) = n$.

Example 1.11 (Public Key Cryptography)**.** In here we will describe the RSA[4] cryptosystem. Think of your to be sent message as a number m. Assume $p \ne q$ are primes, and fix t such that $\gcd(t, \phi(pq)) = 1$ (where ϕ is Euler's function). The encryption of the message m is $m^t (\operatorname{mod} pq)$. Typically neither p nor q divide m. The pair (t, pq) is known to the entire world and that is why the name "public". So how can we recover m from $m^t (\operatorname{mod} pq)$? That is, we are looking for s such that

$$m^{ts} \equiv m (\operatorname{mod} pq). \tag{1.6}$$

[3] This follows easily from the Bézout Identity.

[4] RSA is the acronym for Rivest–Shamir–Adleman.

By making use of Exercise 1.21 it is not difficult to see that it suffices to find s such that

$$ts \equiv 1(\bmod \phi(pq)), \tag{1.7}$$

By making use of Exercise 1.21 once again, it suffices that s satisfies

$$s \equiv t^{\phi(\phi(pq))-1}(\bmod \phi(pq)). \tag{1.8}$$

So in oder to compute s one must have in hand (other than the publicly know t) $\phi(pq) = (p-1)(q-1)$ which practically impossible due to the difficulty of prime factorization. Knowing the product of two large primes doesn't say anything about the primes, and thus, knowing pq is harmless (as one must know p and q for the decryption).

Definition 1.12. The *Möbius function* is defined as

$$\mu(n) := \begin{cases} 1, & \text{if } n \text{ is the product of an even number of distinct primes,} \\ -1, & \text{if } n \text{ is the product of an odd number of distinct primes,} \\ 0, & \text{otherwise.} \end{cases}$$

Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be written in its prime decomposition. It follows directly by the definition that $\mu(n) = 0$ iff there exists i such that $k_i > 1$.

Theorem 1.13.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \textit{if } n\textit{=1,} \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be written in its prime decomposition. Then

$$\sum_{d|n} \mu(d) = \sum_{i=0}^{r} \binom{r}{i} (-1)^i = (1-1)^r = 0.$$

□

By making use of Theorem 1.13 we can relate Euler's and Möbius functions as follows. First, convince yourself of the following identity:

$$\prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = 1 - \sum_{i=1}^{r} \frac{1}{p_i} + \sum_{1 \le i < j \le r} \frac{1}{p_i p_j} - \cdots \tag{1.9}$$

Now combine (1.4) and (1.9), and apply Theorem 1.13 to obtain

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}. \tag{1.10}$$

Note that the right-hand-side of (1.10) gives the proportion of numbers smaller than n that are relatively prime with n, and has vast applications to number theory (especially with regards to the distributions of primes).

Theorem 1.14 (Möbius Inversion Formula)**.** *Let f and g be two functions defined for every natural number and assume that they satisfy $f(n) = \sum_{d|n} g(d)$. Then g satisfies*

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right). \tag{1.11}$$

Proof.

$$\begin{aligned}\sum_{d|n}\mu(d)f\left(\frac{n}{d}\right) &= \sum_{d|n}\mu\left(\frac{n}{d}\right)f(d) = \sum_{d|n}\mu\left(\frac{n}{d}\right)\sum_{d'|d}g(d')\\ &= \sum_{d'|n}g(d')\sum_{m|(n/d')}\mu(m)\\ &= g(n),\end{aligned}$$

since by Theorem 1.13 we have

$$\sum_{m|(n/d')}\mu(m) = \begin{cases}1, & \text{if } d' = n,\\ 0, & \text{otherwise.}\end{cases}$$

□

Definition 1.15. Let f and g be defined for any natural number. The *convolution* $f * g$ is defined by

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a)g(b). \tag{1.12}$$

Exercise 1.16. Show that the convolution is commutative and associative. Make use of associativity to deduce the Möbius Inversion Formula.

We now return to the study of $\mathbb{Z}_n$ (although, technically, we never left it). Let $\mathbb{F}_q$ be the[5] finite field with q elements. Then $q = p^k$ is a prime power. We know that the group of units $\mathbb{F}_q^*$ is cyclic, and thus, so is $\mathbb{Z}_p^*$ for every prime p (and of course it has order $p-1$). Assume $\mathbb{Z}_n^*$ is cyclic and write $\mathbb{Z}_n^* = \langle\overline{a}\rangle$ for some $\overline{a} \in \mathbb{Z}_n$. Such $\overline{a}$ is called a *primitive root*, and by definition it has multiplicative order $\mathrm{ord}(\overline{a}) = |\mathbb{Z}_n^*| = \phi(n)$. We have

$$\mathrm{ord}(\overline{a}^k) = \mathrm{ord}(\overline{a}) \iff \gcd(k, n) = 1. \tag{1.13}$$

The cyclicity of $\mathbb{Z}_n^*$ is determined by the following. See Theorem 5, page 25 from the book.

Theorem 1.17. *$\mathbb{Z}_n^*$ is cyclic iff $n \in \{2, 4, p^k, 2p^k \mid\ p$ is odd prime and $k \geq 1\}$.*

Back to finite fields. For $1 \leq \ell \leq k$, $\mathbb{F}_{p^\ell}$ is a vector space of dimension ℓ over $\mathbb{F}_p$. Yet $\mathbb{F}_{p^\ell} \subseteq \mathbb{F}_{p^k}$ is a subfield iff $\ell|k$. Next, $\mathbb{F}_p$ is called the *prime field* of $\mathbb{F}_{p^\ell}$. The group of automorphisms of $\mathbb{F}_{p^\ell}$, denoted $\mathrm{Aut}(\mathbb{F}_{p^\ell})$ (or $\mathrm{Gal}(\mathbb{F}_{p^\ell}|\mathbb{F}_p)$ if you have seen Galois theory), is a cyclic group of order ℓ generated by the *Frobenius automorphism* $x \longmapsto x^p$. It follows from this, and you should convince yourself (again, if you have seen Galois theory it should be trivial), that $\mathbb{F}_p = \{x \in \mathbb{F}_{p^\ell} \mid x^p = x\}$. The *trace* of $x \in \mathbb{F}_{p^k}$ over $\mathbb{F}_p$ is given by

$$\mathrm{tr}(x) \coloneqq \sum_{i=0}^{k-1} x^{p^i}. \tag{1.14}$$

Convince yourself that $\mathrm{tr}(x) \in \mathbb{F}_p$ for all $x \in \mathbb{F}_{p^k}$. Using the Frobenius automorphism it follows easily that the trace is $\mathbb{F}_p$ linear. Convince yourself that $\mathrm{tr}(x) = \mathrm{tr}(x^p)$ for all $x \in \mathbb{F}_{p^k}$, and as a consequence, for all $y \in \mathbb{F}_p$

$$|\mathrm{tr}^{-1}(y)| = |\{x \in \mathbb{F}_{p^k} \mid \mathrm{tr}(x) = y\}| = p^{k-1}. \tag{1.15}$$

In particular $\mathrm{tr} : \mathbb{F}_{p^k} \longrightarrow \mathbb{F}_p$ is surjective. What other $\mathbb{F}_p$-linear maps $\mathbb{F}_{p^k} \longrightarrow \mathbb{F}_p$ do we have? For all $x \in \mathbb{F}_{p^k}$ consider the map $\Phi_x : \mathbb{F}_{p^k} \longrightarrow \mathbb{F}_p, a \longmapsto \mathrm{tr}(ax)$. Since the trace is $\mathbb{F}_p$-linear so is Φ_x. Convince yourself that $x \neq x'$ implies $\Phi_x \neq \Phi_{x'}$.

[5] Recall that up to isomorphism there is a unique finite field with q elements.

Exercise 1.18. Show that $\{\Phi_x \mid x \in \mathbb{F}_{p^k}\}$ is the set of all $\mathbb{F}_p$-linear maps $\mathbb{F}_{p^k} \longrightarrow \mathbb{F}_p$. Next, denote this set with $\mathrm{Hom}(\mathbb{F}_{p^k}, \mathbb{F}_p)$. Show that, moreover, $\mathrm{Hom}(\mathbb{F}_{p^k}, \mathbb{F}_p) \cong \mathbb{F}_{p^k}$ as $\mathbb{F}_p$-vector spaces.

The *norm* of $x \in \mathbb{F}_{p^k}$ over $\mathbb{F}_p$ is given by

$$N(x) := \prod_{i=0}^{k-1} x^{p^i} = x^{(p^k-1)/(p-1)}. \tag{1.16}$$

As for the trace, we have $N(x) \in \mathbb{F}_p$ for all $x \in \mathbb{F}_{p^k}$ and $N : F_{p^k} \longrightarrow \mathbb{F}_p$ is surjective. In contrast, with the trace, however, the norm is multiplicative, that is, $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{F}_{p^k}$. We will denote $\Xi_k := \{x \in \mathbb{F}_{p^k} \mid N(x) = 1\}$. Since the norm is surjective we have $|\Xi_k| = (p^k - 1)(p - 1) =: d_k$.

Now it is time to connect all the above with notions from real analysis and what is known as (classical) Fourier analysis. Definition 1.15 should sound familiar with convolution from real analysis. That is, the *convolution* $f * g$ of two reasonably nice functions f and g is defined as

$$(f * g)(x) := \int_{\mathbb{R}} f(x)g(x-y)dy \tag{1.17}$$

Then one also defines the *Fourier transform* of a function f to be

$$(\mathcal{F}f)(x) := \int_{\mathbb{R}} f(y)e^{-2\pi ixy}dy. \tag{1.18}$$

Then the *Fourier Inversion Theorem* guaranties

$$f(y) = \int_{\mathbb{R}} (\mathcal{F}f)(x)e^{-2\pi ixy}dx = \int_{\mathbb{R}}\int_{\mathbb{R}} e^{2\pi i(x-z)y}f(z)dz\,dx. \tag{1.19}$$

If $f, g : \mathbb{R} \longrightarrow \mathbb{C}$ are two reasonably nice functions, one defines the *Hermitian inner product* as

$$\langle\, f \mid g \,\rangle := \int_{\mathbb{R}} f(x)\overline{g(x)}dx, \tag{1.20}$$

where $\bar{\bullet}$ now is the complex conjugate. Then the *norm* of f is given by

$$\|f\| := \langle\, f \mid f \,\rangle^{\frac{1}{2}} = \left(\int_{\mathbb{R}} |f(x)|^2 dx\right)^{\frac{1}{2}}. \tag{1.21}$$

Convince yourself that

$$\|\mathcal{F}f\| = \langle\, \mathcal{F}f \mid \mathcal{F}g \,\rangle = \langle\, f \mid g \,\rangle = \|f\|, \tag{1.22}$$

that is, the Fourier transform is an *isometry*. There is an extremely nice connection between the Fourier transform and convolution. Namely, Fourier transform transforms convolution to point-wise multiplication:

$$(\mathcal{F}(f * g))(x) = (\mathcal{F}f)(x)(\mathcal{F}g)(x). \tag{1.23}$$

Now, although historically the Fourier transform has been denoted with $\mathcal{F}$, the beauty of (1.23) is obscured by the heavy-looking notation. So from now on, we will denote the Fourier transform of f by $\widehat{f}$.

If we want to be all technical, we have been secretly working with the *Hilbert space* $L^2(\mathbb{R})$ of all square integrable complex valued functions. Hopefully by now it should be clear the connection between the discrete convolution and continuous convolution. What is missing for a complete picture is the notion of a discrete Fourier transform. The idea is to jump from $L^2(\mathbb{R})$ to the space

$$L^2(G) := \{f : G \longrightarrow \mathbb{C}\}, \tag{1.24}$$

attached to any given finite abelian group G. Note that we are putting no restrictions on the maps f.

Exercise 1.19. Show that $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$.

Exercise 1.20. Let A and B be two sets of the same cardinality. Show that $f : A \longrightarrow B$ is injective iff it is surjective.

Exercise 1.21. Let $n, m \in \mathbb{N}$ be such that $\gcd(n,m) = 1$. Show that $n^{\phi(m)} \equiv 1 \bmod m$, and use this to show that $n^{\phi(m)} + m^{\phi(n)} \equiv 1 \bmod nm$.

Exercise 1.22 (Fermat's Little Theorem)**.** Let p be a prime. Show that if a is not divisible by p then $a^{p-1} \equiv 1 \bmod p$.

Exercise 1.23. [Wilson's Theorem] Show that for any prime number p we have $(p-1)! \equiv -1 \bmod p$.

2 Characters of a Finite Abelian Group

Let G be a finite abelian group of order n, written additively. A *character* is a homomorphism from G to the multiplicative group of complex numbers $(\mathbb{C}^*, \cdot)$. We will denote $\widehat{G}$ the set of all characters of G. Note that $\widehat{G} \subset L^2(G)$. If $\chi \in \widehat{G}$ is a character then for all $g \in G$ we have $1 = \chi(0) = \chi(ng) = \chi(g)^n$. Thus all the character's values are roots of unity. So we can restrict the codomain to $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$. In $\widehat{G}$ we define addition as

$$(\chi + \psi)(g) := \chi(g)\psi(g) \text{ for all } \chi, \psi \in \widehat{G}, g \in G. \tag{2.1}$$

Convince yourself that (2.1) turns $\widehat{G}$ to an abelian group. We will refer to $\widehat{G}$ as the *character group*. The zero of $\widehat{G}$ is the *principal character* ε_G given by $\varepsilon_G(g) := 1$ for all $g \in G$ and the inverse of χ is given by $(-\chi)(g) := \chi(-g) = \overline{\chi(g)}$ (where $\overline{\bullet}$ is the complex conjugate).

Theorem 2.1. *(1)* $\widehat{\mathbb{Z}_n} \cong \mathbb{Z}_n$.
(2) $\widehat{G_1 \times G_2} \cong \widehat{G_1} \times \widehat{G_2}$.
As a consequence of the Fundamental Theorem of Finite Abelian Groups we have $\widehat{G} \cong G$ *for any finite abelian group.*

Proof. (1) Note that it suffices to show that $\widehat{\mathbb{Z}_n}$ is a cyclic group of order n. To that end, fix $\omega := e^{2\pi i/n}$. Then for $0 \le j < n$ define $\chi_j : \mathbb{Z}_n \longrightarrow \mathbb{C}^*$, $\overline{a} \longmapsto \omega^{ja}$. Convince yourself that χ_j is a character (that is, χ_j is well-defined and homomorphism). Thus $\{\chi_j \mid 0 \le j < n\} \subseteq \widehat{\mathbb{Z}_n}$. We show next the reverse inclusion. Let $\chi \in \widehat{\mathbb{Z}_n}$. Since ω is a primitive root of unity there exists j such that $\chi(\overline{1}) = \omega^j$. It follows that $\chi(\overline{a}) = \omega^{ja} = \chi_j(\overline{a})$. Thus $\widehat{\mathbb{Z}_n} = \{\chi_j \mid 0 \le j < n\} = \langle \chi_1 \rangle$.
(2) It is straightforward to show that the map

$$\Phi : \widehat{G_1} \times \widehat{G_2} \longrightarrow \widehat{G_1 \times G_2}, \quad (\chi_1, \chi_2) \longmapsto \left\{ \begin{array}{ccc} G_1 \times G_2 & \longrightarrow & \mathbb{C}^* \\ (g_1, g_2) & \longmapsto & \chi_1(g_1)\chi_2(g_2) \end{array} \right. \tag{2.2}$$

is a homomorphism. We show next that Φ is injective by showing that $\ker \Phi = \{(\varepsilon_{G_1}, \varepsilon_{G_2})\}$. Assume $\Phi(\chi_1, \chi_2)(g_1, g_2) = \chi_1(g_1)\chi_2(g_2) = 1$ for all $(g_1, g_2) \in G_1 \times G_2$. By using pairs of form $(x, 0) \in G_1 \times G_2$ we may conclude $\chi_1 = \varepsilon_{G_1}$. Similarly, $\chi_2 = \varepsilon_{G_2}$. Next, let $\chi \in \widehat{G_1 \times G_2}$. Then $\chi = \Phi(\chi_1, \chi_2)$ where $\chi_1(x) := \chi(x, 0)$ and $\chi_2(y) = \chi(0, y)$. $\square$

Remark 2.2. Consider the finite field with p^n elements $\mathbb{F}_{p^n}$. We know that $\mathbb{F}_{p^n} \cong \mathbb{F}_p^n$ as $\mathbb{F}_p$-vector spaces, and of course $\mathbb{F}_p = \mathbb{Z}_p$. Thus, by Theorem 2.1 we have $\widehat{\mathbb{F}_{p^n}} \cong \widehat{\mathbb{Z}_p} \times \cdots \times \widehat{\mathbb{Z}_p}$. In other words, we pretty much know $\widehat{\mathbb{F}_{p^n}}$; see also Remark 2.4 if necessary. However, later on we will need an explicit description of the characters of $\mathbb{F}_{p^n}$. Let $\omega := e^{2\pi i/p}$ be a p^{th} root of unity and recall the trace function from (1.14). We claim that $\widehat{\mathbb{F}_{p^n}} = \{\chi_x \mid x \in \mathbb{F}_{p^n}\}$, where $\chi_x(y) := \omega^{\mathrm{tr}(xy)}$. To prove the claim it is sufficient (due to cardinality reasons) to show that $\chi_x = \chi_{x'}$ implies $x = x'$. To this end, assume $\chi_x(y) = \chi_{x'}(y)$ for all $y \in \mathbb{F}_{p^n}$. This implies $\omega^{\mathrm{tr}((x-x')y)} = 1$ for all $y \in \mathbb{F}_{p^n}$, which in turn implies $\mathrm{tr}((x-x')y) = 0$ for all $y \in \mathbb{F}_{p^n}$. Now make use of Exercise 1.18 to show that the latter implies $x - x' = 0$.

Example 2.3 (Dirichlet characters). Theorem 2.1 gives the characters of the finite abelian group $(\mathbb{Z}_n, +)$. But $(\mathbb{Z}_n^*, \cdot)$ is as well a finite abelian group. Fix a character $\widetilde{\chi} \in \widehat{\mathbb{Z}_n^*}$, and consider $\chi : \mathbb{Z} \longrightarrow \mathbb{C}^*$ given by

$$\chi(a) = \begin{cases} \widetilde{\chi}(\overline{a}), & \text{if } \gcd(a,n) = 1, \\ 0, & \text{else.} \end{cases}$$

Such a map is called *Dirichlet character* and were used by Dirichlet to show that there are infinitely many primes congruent to any number n. It is easy to see that a Dirichlet character is *strongly multiplicative*, that is $\chi(nm) = \chi(n)\chi(m)$ for all $n, m \in \mathbb{Z}$. Then the *Dirichlet L-function* is defined

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \tag{2.3}$$

for any $s \in \mathbb{C}$. Note that the Dirichlet L-function associated to the trivial Dirichlet character ε is the Riemann ζ-function: $L(s,\varepsilon) = \zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. As such, L-functions play central role in analytical number theory. In fact one can associate a L-function to any strongly multiplicative map $f : \mathbb{Z} \longrightarrow \mathbb{C}$ by

$$L(s,f) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}. \tag{2.4}$$

For complex number $s \in \mathbb{C}$ such that $\mathrm{Re}(s) > 1$ the right-hand-side of (2.3) converges and admits the *Euler product formula*

$$L(s,\chi) = \prod_p \left(\sum_{j=1}^{\infty} \chi(p^j) p^{-js} \right) = \prod_p \frac{1}{1 - \chi(p)p^s}.$$

Remark 2.4. Inducting on Theorem 2.1(2) we obtain $\widehat{G^k} \cong \widehat{G}^k$, where $G^k = G \times \cdots \times G$. Similarly, the isomorphism is given by

$$\chi(g) := \prod_{i=1}^{k} \chi_i(g_i), \tag{2.5}$$

for all $\chi = (\chi_1, \dots, \chi_k) \in \widehat{G}^k, g = (g_1, \cdots, g_k) \in G^k$. Now consider $\mathbb{Z}_n$. In Theorem 2.1(1) we saw how the characters of $\mathbb{Z}_n$ look like. Fix $\overline{a} = (\overline{a_1}, \dots, \overline{a_k})$ and $\chi = (\chi_{i_1}, \dots, \chi_{i_k})$. Recall that $\chi_{i_k}(\overline{x}) = \omega^{i_k x}$. Thus, applying (2.5) to this specific case we obtain

$$\chi(\overline{a}) = \prod_{j=1}^{k} \chi_{i_j}(\overline{a_j}) = \prod_{j=1}^{k} \omega^{i_j a_j} = \omega^{i \cdot a}, \tag{2.6}$$

where $i \cdot a := \sum_{j=1}^{k} i_j a_j$ is the standard dot product modulo n.

Definition 2.5. Let $H \leq G$ and $K \leq \widehat{G}$ be two subgroups. Then
(1) $H^\perp := \{\chi \in \widehat{G} \mid \chi_{|H} = \varepsilon_H\} = \{\chi \in \widehat{G} \mid \chi(h) = 1 \text{ for all } h \in H\}$.
(2) $K^\perp := \{g \in G \mid \chi(g) = 1 \text{ for all } \chi \in K\}$.
$H^\perp$ and $K^\perp$ are called the *dual* groups of H and K respectively.

Since a character is a group homomorphism we have $\ker\chi := \{g \in G \mid \chi(g) = 1\}$ is a subgroup of G. With this notation we have

$$K^\perp = \bigcap_{\chi\in K} \ker\chi. \tag{2.7}$$

Theorem 2.6. *The map*

$$\Phi\colon H^\perp \longmapsto \widehat{G/H},\quad \chi \longmapsto \begin{cases} \Phi_\chi\colon G/H & \longrightarrow & \mathbb{C}^* \\ \quad g+H & \longmapsto & \chi(g) \end{cases} \tag{2.8}$$

is an isomorphism of groups. As a consequence $|H^\perp| = |G|/|H|$.

Proof. The only interesting part is to show that Φ is well-defined, that is, every $\chi \in H^\perp$ gives a well-defined map Φ_χ. Indeed, if $g - g' \in H$ then since $\chi \in H^\perp$ we obtain $\chi(g) = \chi(g')$. Thus $\Phi_\chi(g+H) = \Phi_\chi(g'+H)$. By Theorem 2.1 we have $|H^\perp| = |\widehat{G/H}| = |G/H| = |G|/|H|$. □

Theorem 2.7. *Let $H \leq G$ be a subgroup. Then every character of H can be extended to a character of G.*

Proof. Define the map $\pi : \widehat{G} \longrightarrow \widehat{H}$, $\chi \longmapsto \chi_{|H}$. Note first that it suffices to show that π is surjective. Convince yourself that $\ker\pi = H^\perp$. This yields

$$|\mathrm{im}\,\pi| = |\widehat{G}|/|H^\perp| = |H| = |\widehat{H}|,$$

where the middle equality follows by Theorem 2.6. Thus $\mathrm{im}\,\pi = \widehat{H}$ and as consequence π is surjective. □

Theorem 2.8. *Let $f : G \longrightarrow H$ be a surjective homomorphism of finite abelian groups. Then the map $f^* : \widehat{H} \longrightarrow \widehat{G}$, $\chi \longmapsto \chi\circ f$ is an injective homomorphism such that $f^*(\widehat{H}) = (\ker f)^\perp$. In particular, f is bijective iff f^* is bijective.*

Proof. Clearly f^* is a homomorphism. We prove first that f^* is injective. Let $\chi \in \ker f^*$. Then $\chi\circ f = \varepsilon_G$. We want to show that $\chi = \varepsilon_H$. To that end, fix $x \in H$ and write $x = f(y)$ for some $y \in G$ (since f is surjective). Thus $\chi(x) = \chi(f(y)) = 1$. Next, we show $f^*(\widehat{H}) \subseteq (\ker f)^\perp$, that is, $\chi(f(x)) = 1$ for all $\chi \in \widehat{H}$ and $x \in \ker f$. But the latter statement is clear. On the other hand, since f is surjective, we have $|\ker f| = |G|/|H|$. By Theorem 2.7 we have $|(\ker f)^\perp| = |G|/|\ker f| = |H| = |\widehat{H}| = |f^*(\widehat{H})|$, where the last equality is due to injectivity of f^*. □

Corollary 2.9. *Let G be a finite abelian group and fix $0 \neq g \in G$. Then there exists $\chi \in \widehat{G}$ such that $\chi(g) \neq 1$.*

Proof. Let $H := G/\langle g\rangle$ and let $\pi : G \longrightarrow H$ be the canonical projection. Thus $\ker\pi = \langle g\rangle$. By Theorem 2.8 we have

$$|\langle g\rangle^\perp| = |G/\langle g\rangle| < |G|,$$

where the last inequality follows by $g \neq 0$. But by the very definition we have $\langle g\rangle^\perp = \{\chi \in \widehat{G} \mid \chi(g) = 1\}$. Thus there exists $\chi \in \widehat{G}$ such that $\chi(g) \neq 1$. □

Example 2.10 (How to extend a character)**.** Let $H \leq G$ be a proper subgroup and fix $\chi \in \widehat{H}$. Let $0 \neq x \in G - H$ and let d be the smallest integers such that $0 \neq dx \in H$. Note that $d \neq 1$ and $nx \in H$ iff $d|n$. Fix $z \in \mathbb{C}^*$ such that $z^d = \chi(dx)$. Put $K := \{nx + h \mid h \in H\} \supsetneq H$. Define $\widetilde{\chi} : K \longrightarrow$

$\mathbb{C}^*$, $nx + h \longmapsto z^n \chi(h)$. $\widetilde{\chi}$ is well-defined because if $nx + h = mx + h'$ then $(n - m)x = h' - h \in H$. Thus $d|(n - m)$. Write $n = dk + m$. By minimality of d we have $kx = 0$. Now we compute

$$\widetilde{\chi}(nx + h) = z^n \widetilde{\chi}(h) = z^{dk+m} \widetilde{\chi}(h) = z^m \widetilde{\chi}(kx) \widetilde{\chi}(h) = z^m \widetilde{\chi}(h) = \widetilde{\chi}(mx + h)$$

$\widetilde{\chi}$ is clearly a group homomorphism and thus $\widetilde{\chi} \in \widehat{K}$. If $K = G$ we are done, otherwise repeat. The process will clearly end because G is finite.

Exercise 2.11. Let $H \leq G$. Show that every character of H extends to a character of G in $|G|/|H|$ different ways.

So far we have been studying the character group of a finite abelian group, which in turn is itself a finite abelian group. So what about its character group $\widehat{\widehat{G}}$? Let $\mathrm{ev}_g : \widehat{G} \longrightarrow \mathbb{C}^*, \chi \longmapsto \chi(g)$ be the *evaluation map*. Then

$$\zeta_G : G \longmapsto \widehat{\widehat{G}}, \quad g \longmapsto \left\{ \begin{array}{rcl} \mathrm{ev}_g : \widehat{G} & \longrightarrow & \mathbb{C}^* \\ \chi & \longmapsto & \chi(g) \end{array} \right. , \tag{2.9}$$

is an isomorphism[6] of groups. Then (9) should be read as $g(\chi) = \chi(g)$.

Theorem 2.12.

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} 0, & \text{if } g \neq 0 \\ |G|, & \text{if } g = 0 \end{cases} \quad \text{and} \quad \sum_{g \in G} \chi(g) = \begin{cases} 0, & \text{if } \chi \neq \varepsilon_G, \\ |G|, & \text{if } \chi = \varepsilon_G. \end{cases} \tag{2.10}$$

Proof. We prove the second equation. The first equation follows by the second and (9). If $\chi = \varepsilon_G$ then the equality is obvious. Now assume $\chi \neq \varepsilon_G$. Then there exists $x \in G$ such that $\chi(x) \neq 1$. Then

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g + x) = \chi(x) \sum_{g \in G} \chi(g),$$

which in turn implies

$$(1 - \chi(x)) \sum_{g \in G} \chi(g) = 0.$$

This concludes the proof. ∎

Corollary 2.13 (Orthogonality Relations)**.**

$$\sum_{g \in G} \chi(g) \overline{\psi(g)} = \left\{ \begin{array}{ll} |G|, & \text{if } \chi = \psi, \\ 0, & \text{else.} \end{array} \right. \quad \text{and} \quad \sum_{\chi \in \widehat{G}} \chi(x) \overline{\chi(y)} = \left\{ \begin{array}{ll} |G|, & \text{if } x = y, \\ 0, & \text{else.} \end{array} \right.$$

Corollary 2.14. *Let $H \leq G$ and $K \leq \widehat{G}$. Then*

$$\sum_{\chi \in K} \chi(g) = \left\{ \begin{array}{ll} |K|, & \text{if } g \in K^\perp, \\ 0, & \text{else.} \end{array} \right. \quad \text{and} \quad \sum_{h \in H} \chi(h) = \left\{ \begin{array}{ll} |H|, & \text{if } \chi \in H^\perp, \\ 0, & \text{else.} \end{array} \right. \tag{2.11}$$

Definition 2.15. Let $G = \{g_0, \ldots, g_{n-1}\}$ and $\widehat{G} = \{\chi_0, \ldots, \chi_{n-1}\}$. The *Fourier matrix*[7] of G is

$$F_G = \left(\chi_i(g_j)\right)_{i,j=0}^{n-1} \in \mathbb{C}^{n \times n}. \tag{2.12}$$

[6]Note that ζ_G does not involve any choice, which makes it a natural isomorphism. Compare this with Theorem 2.1 where the isomorphism involves the choice of a primitive root of unity.

[7]Group theorists refer to C_G as the *character table*.

Proposition 2.16. *The matrix $A = \frac{1}{\sqrt{n}} F_G$ is unitary.*

Proof. Let $A^\dagger$ the conjugate transpose of A. Then it is enough to show that $A^\dagger A = I$. Indeed

$$(A^\dagger A)_{i,j} = \frac{1}{n}\sum_{l=0}^{n-1} \overline{\chi_l(g_i)}\chi_l(g_j) = \frac{1}{n}\sum_{l=0}^{n-1} \chi_l(g_j - g_i) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

□

Example 2.17. It is easy to see that the Fourier matrix of $\mathbb{Z}_2$ is

$$F_{\mathbb{Z}_2} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The Fourier matrix of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ is given below. The computation is done by using (2.6). Note that $F_G = F_{\mathbb{Z}_2} \otimes F_{\mathbb{Z}_2}$.

$$F_G = \begin{array}{c} \\ (\chi_0,\chi_0) \\ (\chi_0,\chi_1) \\ (\chi_1,\chi_0) \\ (\chi_1,\chi_1) \end{array} \begin{array}{c} \begin{array}{cccc} (0,0) & (0,1) & (1,0) & (1,1) \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \end{array}.$$

Exercise 2.18. Let $G = G_1 \times G_2$. Show that $F_G = F_{G_1} \otimes F_{G_2}$.

Exercise 2.19. Let $H \leq G$ and $K \leq \widehat{G}$. Prove a similar result as in Theorem 2.6 for K, that is, show that $K^\perp \cong \widehat{G/K}$. In addition, show the following.
(1) $H = (H^\perp)^\perp$ and $K = (K^\perp)^\perp$.
(2) $G^\perp = \{\varepsilon_G\}$ and $\widehat{G}^\perp = \{0\}$.
(3) Make use of (2.7) to show that $\chi(x) = 1$ for all $\chi \in \widehat{G}$ implies $x = 0$.

Exercise 2.20. Let G be a finite abelian group. Denote $G_{(n)} \coloneqq \{g \in G \mid g^n = 1\}$ and $G^{(n)} = \{g^n \mid g \in G\}$. Show that $(G_{(n)})^\perp = \widehat{G}^{(n)}$ and $(G^{(n)})^\perp = \widehat{G}_{(n)}$.

Exercise 2.21 (Additive version of characters)**.** Consider the quotient group $\mathbb{Q}/\mathbb{Z}$ and let G be a finite abelian group. Denote $G^\# \coloneqq \{f : G \longrightarrow \mathbb{Q}/\mathbb{Z} \mid f \text{ is a group homomorphism}\}$. Define addition on $G^\#$ point-wise. Thus $G^\#$ is again abelian. Show that $\widehat{G} \cong G^\#$.

Exercise 2.22. In this exercise we will see $\widehat{\bullet} : A \longmapsto \widehat{A}$ as a *contravariant, exact, duality-preserving functor*. Let A, B, C be finite abelian groups, and suppose we have two group homomorphisms $A \xrightarrow{f} B \xrightarrow{g} C$. As in Theorem 2.8 we obtain $\widehat{C} \xrightarrow{g^*} \widehat{B} \xrightarrow{f^*} \widehat{A}$. Show the following.
(1) $(g \circ f)^* = f^* \circ g^*$.
(2) $\operatorname{im} f = \ker g \iff \operatorname{im} g^* = \ker f^*$.

3 The Space $L^2(G)$

Let G be a finite abelian group of order n. Write $G = \{g_0, \ldots, g_{n-1}\}$. Recall from (1.24) that $L^2(G) = \{f : G \longrightarrow \mathbb{C}\}$. Note that a map $f \in L^2(G)$ is completely determined by the vector $(f(g_0), \ldots, f(g_{n-1})) \in \mathbb{C}^n$. Conversely, every vector in $\mathbb{C}^n$ determines a map in $L^2(G)$. In other words, $L^2(G) \cong \mathbb{C}^n$ as complex vector spaces. Just to state the obvious, the scalar multiplication is given by $(z \cdot f)(g) = z(f(g))$ for all $z \in \mathbb{C}$. In particular, $\dim_{\mathbb{C}} L^2(G) = n = |G|$. The first goal is to find a nice basis of $L^2(G)$.

Theorem 3.1 (Linear Independence of Characters)**.** *For $1 \leq k \leq n$, any k distinct characters of G are linearly independent.*

Proof. We induct on the number of characters considered. First, convince yourself that a single character is linearly independent. Let $\chi_1, \dots, \chi_k$ be distinct characters, and assume

$$\sum_{i=1}^{k} a_i \chi_i = 0, \ a_i \in \mathbb{C}. \tag{3.1}$$

We want to show that $a_1 = \cdots = a_k = 0$. We have $\sum_{i=1}^{k} a_i \chi_i(g) = 0$ for all $g \in G$. Since $\chi_1 \neq \chi_k$, there exists $g' \in G$ such that $\chi_1(g') \neq \chi_k(g')$. Now we have

$$0 = \sum_{i=1}^{k} a_i \chi_i(g) = \sum_{i=1}^{k} a_i \chi_i(g + g') = \sum_{i=1}^{k} a_i \chi_i(g) \chi_i(g'). \tag{3.2}$$

Multiply (3.1) on both sides by $\chi_k(g') \in \mathbb{C}$, that is, for all $g \in G$ we have

$$0 = \chi_k(g') \sum_{i=1}^{k} a_i \chi_i(g). \tag{3.3}$$

Now combine (3.2) and (3.3) to obtain

$$\sum_{i=1}^{k-1} a_i (\chi_k(g') - \chi_i(g')) \chi_i(g) = 0 \tag{3.4}$$

for all $g \in G$. Note that (3.4) is a linear combination of $\chi_1, \dots, \chi_{k-1}$, and thus all the coefficients must be 0 by inductive hypothesis. Since $\chi_1(g') - \chi_k(g') \neq 0$, we conclude that $a_1 = 0$. Proceed similarly for $a_2, \dots, a_k$. □

Theorem 3.2. *$\widehat{G}$ is a basis for $L^2(G)$.*

Proof. Since $\widehat{G} \subseteq L^2(G)$ we have $\operatorname{span}_{\mathbb{C}} \widehat{G} \subseteq L^2(G)$. Now the statement follows by Theorem 3.1 and $|\widehat{G}| = n$. □

Exercise 3.3. Let $\chi_1, \dots, \chi_N$ and $\chi'_1, \dots, \chi'_M$ be characters of G that satisfy $\sum_{i=1}^{N} \chi_i = \sum_{j=1}^{M} \chi'_j$. Show that the multisets $\{\{\chi_1, \dots, \chi_N\}\}$ and $\{\{\chi'_1, \dots, \chi'_M\}\}$ coincide.

Definition 3.4. On $L^2(G)$ define the *Hermitian inner product* as

$$\langle f \mid g \rangle_G = \frac{1}{|G|} \sum_{x \in G} f(x) \overline{g(x)} \tag{3.5}$$

Remark 3.5. Note that (3.5) gives rise to a norm function via $\|f\| := \langle f \mid f \rangle_G^{1/2}$. Then clearly $\|f\| \geq 0$ and $\|f\| = 0$ iff $f = 0$. Convince yourself that the Hermitian inner product is non-degenerate, that is, if $\langle f \mid g \rangle_G = 0$ for all $g \in L^2(G)$ then $f = 0$ and if $\langle f \mid g \rangle_G = 0$ for all $f \in L^2(G)$ then $g = 0$. Note that viewing $f \in L^2(G)$ as a complex vector of length n, then (3.5) is nothing else but the usual Hermitian inner product in $\mathbb{C}^n$. In other words, $(L^2(G), \|\bullet\|)$ is isomorphic to $\mathbb{C}^n$ as Hilbert spaces, and thus it is itself a Hilbert space of dimension n.

Corollary 3.6. *$\widehat{G}$ is an orthonormal basis of $L^2(G)$.*

Exercise 3.7. Find a basis for $L^2(\widehat{G})$. Define an analogous inner product $\langle \bullet \mid \bullet \rangle_{\widehat{G}}$. Is the basis you found orthonormal with respect to $\langle \bullet \mid \bullet \rangle_{\widehat{G}}$?

Exercise 3.8. For $f_1, f_2 \in L^2(G)$ define their convolution as

$$(f_1 * f_2)(g) := \sum_{h \in G} f_1(h) f_2(g - h). \tag{3.6}$$

For all $g \in G$ denote the $\delta_g \in L^2(G)$ map $\delta_g(x) = 1$ if $x = g$ and $\delta_g(x) = 0$ if $x \neq g$. Show that $\delta_g * \delta_h = \delta_{g+h}$.

Exercise 3.9. Show that $\Delta_G := \{\delta_g \mid g \in G\}$ is basis for $L^2(G)$.

Exercise 3.10. Since $\widehat{G}$ is a basis, every $f \in L^2(G)$ can be expressed uniquely as

$$f = \sum_{\chi \in \widehat{G}} c_\chi \chi, \quad c_\chi \in \mathbb{C}. \tag{3.7}$$

Find c_χ in (3.7). Use this to find the change of basis matrix between Δ_G and $\widehat{G}$ for the case $G = \mathbb{Z}_4$.

4 The Discrete Fourier Transform

We first make use of the orthogonality relations 2.13 to motivate the Discrete Fourier Transform (DFT) and then we show some properties of DFT. Fix $f \in L^2(G)$. Then f can be expressed uniquely in terms of the basis Δ_G as

$$f = \sum_{g \in G} f(g) \delta_g. \tag{4.1}$$

The second orthogonality relation in (2.13) can be written in terms of Δ_G as

$$\sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi(x)} = |G| \delta_g(x) \implies \delta_g(x) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \overline{\chi(g)} \chi(x). \tag{4.2}$$

Substituting in (4.1) we obtain

$$\begin{aligned} f(x) &= \sum_{g \in G} f(g) \left(\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \overline{\chi(g)} \chi(x) \right) \\ &= \sum_{\chi \in \widehat{G}} \sum_{g \in G} \frac{1}{|G|} f(g) \overline{\chi(g)} \chi(x) \\ &= \sum_{\chi \in \widehat{G}} c_\chi \chi(x), \end{aligned}$$

where

$$c_\chi = \frac{1}{|G|} \sum_{g \in G} f(g) \overline{\chi(g)} = \langle f \mid \chi \rangle_G. \tag{4.3}$$

Definition 4.1. The *Discrete Fourier transform* of $f \in L^2(G)$ is the function $\widehat{f} \in L^2(\widehat{G})$ given by

$$\widehat{f}(\chi) = \sum_{g \in G} f(g) \overline{\chi(g)} = |G| \langle f \mid \chi \rangle_G = |G| c_\chi.$$

We have also proved the following

Theorem 4.2 (Fourier Inversion Formula). *For any $f \in L^2(G)$ we have*

$$f(x) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi(x).$$

Exercise 4.3. Find the DFT of a character. Find the DFT of δ_g. Find the DFT of a constant function.

Now we prove Theorem 2 on page 168.

Theorem 4.4. *(1) Show that the Fourier transform $\widehat{\bullet} : L^2(G) \longrightarrow L^2(\widehat{G})$ is an isomorphism of vector spaces.*
(2) $\widehat{f * g}(\chi) = \widehat{f}(\chi)\widehat{g}(\chi)$.
(3) $\langle f \,|\, f \rangle_G = (1/|G|)\langle \widehat{f} \,|\, \widehat{f} \rangle_{\widehat{G}}$, where the inner product on $L^2(\widehat{G})$ is given by

$$\langle F \,|\, H \rangle_{\widehat{G}} = \sum_{\chi \in \widehat{G}} F(\chi)\overline{H(\chi)}. \tag{4.4}$$

(4) Define for $g \in G$, $f^s(g) := f(g+s)$. Then $\widehat{f^s}(\chi) = \chi(s)\widehat{f}(\chi)$

Proof. (1) It is easy to check that the map

$$\widehat{\bullet}^{-1} : L^2(\widehat{G}) \longmapsto L^2(G), \quad f \longmapsto \begin{cases} G \longrightarrow & \mathbb{C} \\ g \longmapsto & \frac{1}{|G|}\sum_{\chi \in \widehat{G}} f(\chi)\chi(g) \end{cases}, \tag{4.5}$$

is the inverse of $\widehat{\bullet}$. See also Theorem 4.2.
(2) Lisa proved this one. See also page 38 of the book.
(3) Recall that Lisa showed the identity for characters. In fact this is sufficient because the Hermitian inner product is linear and characters form a basis for $L^2(G)$. However, bellow we use a slightly different approach. Recall from Definition 4.1 that $\widehat{f}(\chi) = |G|\langle f \,|\, \chi \rangle$. We have

$$\begin{aligned} \langle \widehat{f} \,|\, \widehat{f} \rangle_{\widehat{G}} &= |G|^2 \sum_{\chi \in \widehat{G}} \langle f \,|\, \chi \rangle \overline{\langle f \,|\, \chi \rangle} \\ &= \sum_{\chi \in \widehat{G}} \sum_{a \in G} \sum_{b \in G} f(a)\overline{\chi(a)}\chi(b)\overline{f(b)} \\ &= \sum_{a \in G} \sum_{b \in G} f(a)\overline{f(b)} \sum_{\chi \in \widehat{G}} \chi(a-b) \\ &= |G| \sum_{a \in G} \sum_{a \in G} f(a)\overline{f(a)} \\ &= |G|\langle f \,|\, f \rangle. \end{aligned}$$

(4)

$$\begin{aligned} \widehat{f^s}(\chi) &= \sum_{g \in G} f^s(g)\overline{\chi(g)} = \sum_{g \in G} f(g+s)\overline{\chi(g)} \\ &= \sum_{a \in G} f(a)\overline{\chi(a-s)} = \sum_{a \in G} f(a)\overline{\chi(a)}\chi(s) \\ &= \chi(s)\widehat{f}(\chi). \end{aligned}$$

□

Lemma 4.5. *Let $H \leq G$ and let $f \in L^2(G)$ be such that $f(g+h) = f(g)$ for all $g \in G$ (that is, f is constant in the cosets of H). Write G as disjoint union of its cosets: $G = \dot\bigcup_{i=1}^{l}(g_i + H)$. Then*

(1) $\widehat{f}(\chi) = \begin{cases} |H| \sum\limits_{i=1}^{l} f(g_i)\overline{\chi(g_i)}, & \text{if } \chi \in H^\perp \\ 0, & \text{if } \chi \notin H^\perp. \end{cases}$

(2) The map $\widetilde{f} \in \widehat{G/H}$, $a + H \longmapsto f(a)$ is well-defined, and for all $\chi \in \widehat{G/H} \cong H^\perp$ we have

$$\widehat{\widetilde{f}}(\chi) = \frac{1}{|H|}\widehat{f}(\chi).$$

Proof. (1) The statement follows by Corollary 2.14 and the following computation.

$$\begin{aligned}\widehat{f}(\chi) &= \sum_{g \in G} f(g)\overline{\chi(g)} = \sum_{i=1}^{l}\sum_{h\in H} f(g_i + h)\overline{\chi(g_i + h)} \\ &= \sum_{i=1}^{l} f(g_i)\overline{\chi(g_i)} \sum_{h \in H} \overline{\chi(h)}.\end{aligned}$$

(2) First of all, $\widetilde{f}$ is clearly well-defined. Next, recall from Theorem 2.6 that $H^\perp \cong \widehat{G/H}$ via $[\chi \longmapsto [\Phi_\chi : g + H \longmapsto \chi(g)]$. We have

$$\begin{aligned}\widehat{\widetilde{f}}(\chi) &= \sum_{g+H \in G/H} \widetilde{f}(g+H)\overline{\chi(g+H)} \\ &= \sum_{i=1}^{l} f(g_i)\overline{\chi(g_i)} \\ &\overset{(1)}{=} \frac{1}{|H|}\widehat{f}(\chi).\end{aligned}$$

□

Theorem 4.6 (Poisson Summation Formula)**.** *Let $H \leq G$ and fix $g \in G$, $f \in L^2(G)$. Then*

$$\sum_{h \in H} f(g + h) = \frac{1}{|H^\perp|}\sum_{\chi \in H^\perp} \widehat{f}(\chi)\chi(g). \tag{4.6}$$

In particular, for $g = 0$ we obtain

$$\sum_{h \in H} f(h) = \frac{1}{|H^\perp|}\sum_{\chi \in H^\perp} \widehat{f}(\chi). \tag{4.7}$$

Proof. Let $f' \in L^2(G)$ be given by $f'(g) \coloneqq \sum_{h \in H} f(g + H)$. Then $f'(g+h) = f'(g)$ for all $h \in H$. As in Lemma 4.5(2) we obtain $\widetilde{f} \in \widehat{G/H}$ given by $g + H \longmapsto f'(g)$. Thus, the left-hand-side of (4.6) equals $\widetilde{f}(g+H)$. On the other hand we have

$$\begin{aligned}
\sum_{\chi\in H^\perp}\widehat{f}(\chi)\chi(g) &= \sum_{\chi\in H^\perp}\sum_{b\in G} f(b)\overline{\chi(b)}\chi(g) \\
&= \sum_{\chi\in H^\perp}\sum_{i=1}^{l}\sum_{h\in H} f(g_i+h)\overline{\chi(g_i+h)}\chi(g) && \text{(as in Lemma 4.5)} \\
&= \sum_{\chi\in H^\perp}\sum_{i=1}^{l} f'(g_i)\overline{\chi(g_i)}\chi(g) && \text{(since } \chi\in H^\perp\text{)} \\
&= \sum_{\chi\in H^\perp}\frac{1}{|H|}\widehat{f'}(\chi)\chi(g) && \text{(by Lemma 4.5(1))} \\
&= \sum_{\chi\in\widehat{G/H}}\widehat{\widetilde{f}}(\chi)\chi(g+h) && \text{(by Lemma 4.5(2))} \\
&= \sum_{\chi\in\widehat{G/H}}\sum_{y+H}\widetilde{f}(y+H)\chi(y+H)\chi(g+H) \\
&= \sum_{y+H}\widetilde{f}(y+H)\sum_{\chi\in\widehat{G/H}}\chi(y+g+H) \\
&= \widetilde{f}(g+H)\cdot|G/H|. && \text{(by Orthogonality Relations in } G/H\text{)}
\end{aligned}$$

The result now follows because $|H^\perp|=|G/H|$ by Theorem 2.6. The case when $g=0$ is clear. □

Exercise 4.7. Let $G=G_1\times\cdots\times G_n$ and $f_i\in L^2(G_i)$. Define $f\in L^2(G)$ via $(g_1,\dots,g_n)\longmapsto\prod_{i=1}^n f_i(g_i)$. Show that $\widehat{f}=\prod_{i=1}^n\widehat{f_i}$. That is, show that for all $(\chi_1,\dots,\chi_n)\in\widehat{G}\cong\widehat{G_1}\times\cdots\times\widehat{G_n}$ we have

$$\widehat{f}(\chi_1,\dots,\chi_n)=\prod_{i=1}^n\widehat{f_i}(\chi_i).$$

Exercise 4.8. Let $f\in L^2(G)$. By using the natural identification $G\cong\widehat{\widehat{G}}$ show that for all $g\in G$ we have $\widehat{\widehat{f}}(g)=|G|f(-g)$.

Exercise 4.9. Convince yourself that for all $g\in G$ the following map gives a linear transformation of complex vector spaces.

$$T_g: L^2(G)\longrightarrow L^2(G),\quad f\longmapsto\left\{\begin{array}{rcl} T_gf: G & \longrightarrow & \mathbb{C}^* \\ x & \longmapsto & f(g+x)\end{array}\right. . \tag{4.8}$$

Now show the following.

(1) Show that characters are eigenvectors of T_g.

(2) Show that $\widehat{T_gf}=\chi(g)\widehat{f}$ and $\langle T_gf_1\,|\,T_gf_2\rangle_G=\langle f_1\,|\,f_2\rangle_G$ for any $f,f_1,f_2\in L^2(G)$.

(3) For any $f\in L^2(G)$ and $\chi\in\widehat{G}$ show that $\delta_g*f=T_{-g}f$ and $\chi*f=\widehat{f}(\chi)\chi$.

Exercise 4.10. Let $G=\mathbb{Z}_n$. Similarly as in Exercise 4.9 consider the linear transformation $D_g: L^2(G)\longrightarrow L^2(G)$ given by $(D_gf)(x)=f(gx)$ for all $f\in L^2(G)$ and $x\in G$. Show that $\widehat{D_gf}=D_{-g}\widehat{f}$.

4.1 Fast Fourier Transform

In this subsection we will consider the DFT for the very special case $G=\mathbb{Z}_n$. Let $\omega=\exp(2\pi i/n)$. Recall that in this case $\widehat{\mathbb{Z}_n}=\{\chi_x\,|\,\overline{x}\in\mathbb{Z}_n\}$, where $\chi_x(\overline{y})=\omega^{xy}$ as in the proof of Theorem 2.1(1). We will identify a character $\chi_x\in\widehat{\mathbb{Z}_n}$ with $\overline{x}\in\mathbb{Z}_n$ and think of the DFT as $\widehat{\bullet}: L^2(\mathbb{Z}_n)\longrightarrow L^2(\mathbb{Z}_n),\ f\longmapsto\widehat{f}$, where Definition 4.1 reads as

$$\widehat{f}(\overline{x})=\sum_{\overline{y}\in\mathbb{Z}_n} f(\overline{y})\omega^{-xy}. \tag{4.9}$$

To find the Fourier Transform of character χ_x we compute

$$\widehat{\chi_x}(\overline{z}) = \sum_{\overline{z}\in\mathbb{Z}_n} \chi_x(\overline{z})\omega^{-zy} = \sum_{\overline{z}\in\mathbb{Z}_n} \omega^{-z(x-y)},$$

and the Fourier matrix $F_n = F_{\mathbb{Z}_n}$ from Definition 2.15 reads as

$$F_n = (\omega^{xy})_{0\le x,\, y\le n-1} \tag{4.10}$$

In Section 3 we saw how a map $f \in L^2(G)$ can be thought as a vector $(f(g_1),\dots,f(g_n)) \in \mathbb{C}^n$ where $g_i \in G$. For the purposes of this subsection we will need column vectors. So for $f \in L^2(\mathbb{Z}_n)$ denote $f = (f(\overline{0}),\dots,f(\overline{n-1}))^{\mathsf{T}}$ and $g = (\widehat{f}(\overline{0}),\dots,\widehat{f}(\overline{n-1}))^{\mathsf{T}}$. Clearly we have $g = F_n f$, and thus, to compute the Fourier Transform are required n^2 multiplications. However, it is possible to compute the Fourier Transform much faster when n divisible by a high power of 2. Indeed, assume $n = 2m$ and write

$$f = (f', f''),\ \text{where}\ f' = (f(\overline{0}), f(\overline{2})\ \dots, f(\overline{n-2})),\ f' = (f(\overline{1}), f(\overline{3})\ \dots, f(\overline{n-1})).$$

Put $g' = F_m f'$ and $g'' = F_m f''$. It is straightforward to check that for $0 \le j \le n-1$ we have $g_j = g'_j + \omega^j g''_j$ and for $0 \le j \le m$ we have $g_{m+j} = (g')_j - \omega^j (g''))_j$. In other words, in order to compute the Fourier Transform when $n = 2m$ we will need $2m^2 + m$ multiplications instead of $n^2 = 4m^2$ (which is roughly half). If $n = 2^r$ then one need $\frac{n}{2}(r+2) < n\log(n) \ll n^2$. This is known as Cooley-Tukey algorithm; see also Theorem 1, page 153.

Remark 4.11. Assume $n, m \in \mathbb{Z}$ are coprime. By Theorem 1.6 we have $\mathbb{Z}_{nm} = \mathbb{Z}_n \times \mathbb{Z}_m$, and thus, by Exercise 2.18 we have $F_{nm} = F_n \otimes F_m$. This fact speeds up the computation of the Fourier Transform. Although less obvious, this applies to any $n, m \in \mathbb{Z}$. See also the discussion on page 155.

5 Discrete Uncertainty Principle

In this section we give a discrete version of the classical *uncertainty principle*, which says that if a function $f(x)$ is essentially zero in Δx and its Fourier transform (see (1.18)) $\widehat{f}(y)$ is essentially zero in Δy then

$$\Delta x \Delta y \ge 1 \tag{5.1}$$

Compare (5.1) with Theorem 5.1. The uncertainty principle was used by Heisenberg in 1927 to show that a particle's position and momentum cannot be simultaneously determined. In other words, the more you know about a particle's position the less you know about its momentum, and vice versa.

Recall that an inner product $\langle \bullet \,|\, \bullet \rangle$ gives rise to norm function $\|\bullet\|$ via $\|f\|^2 := \langle f \,|\, f \rangle$. We will make use of the Cauchy-Schwartz inequality

$$|\langle f \,|\, g \rangle|^2 \le \|f\|^2 \cdot \|g\|^2. \tag{5.2}$$

In Remark 3.5 we discussed the norm associated to the Hermitian inner product (3.5). In this case we will need a rescaled version, called the L^2*−norm* and denoted $\|\bullet\|_2$. Namely $\|f\|_2^2 := \sum_{x\in G} |f(x)|^2$. In addition, we will need the following norm in $L^2(G)$:

$$\|f\|_\infty := \max_{x\in G} |f(x)|. \tag{5.3}$$

For a map $f \in L^2(G)$, the *support of* f is given by $\operatorname{supp} f = \{x \in G \mid f(x) \neq 0\}$. It follows from the very definitions above that

$$\|f\|_2^2 = \sum_{x \in G} |f(x)|^2 \leq \|f\|_\infty^2 \cdot |\operatorname{supp} f|. \tag{5.4}$$

Define

$$\mathbb{1}(x) = \begin{cases} 1, & \text{if } x \in \operatorname{supp} f, \\ 0, & \text{if } x \notin \operatorname{supp} f, \end{cases} \tag{5.5}$$

and note that we have $f(x) = (f \cdot \mathbb{1})(x) = f(x) \cdot \mathbb{1}(x)$ for all $x \in G$. Of course $\|\bullet\|_2$, $\|\bullet\|_\infty$, supp, and $\mathbb{1}$ can be also defined over $L^2(\widehat{G})$, and we will use the same notation.

Theorem 5.1. *Let $f \in L^2(G)$ be not identically zero. Then*

$$|\operatorname{supp} f| \cdot |\operatorname{supp} \widehat{f}| \geq |G|.$$

Proof. By making use of the Fourier Inversion Formula and the fact that $|\chi(x)| \leq 1$ for all $x \in G$ (since $\chi(x)$ is a root of unity), we obtain

$$\|f\|_\infty \leq \frac{1}{|G|} \sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)|.$$

Now by making use of the Cauchy-Schwartz inequality we obtain

$$\begin{aligned}
\|f\|_\infty^2 &\leq \frac{1}{|G|^2} \left(\sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)| \right)^2 = \frac{1}{|G|^2} \left(\sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)| \cdot |\mathbb{1}(\chi)| \right)^2 \\
&\leq \frac{1}{|G|^2} \left(\sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)|^2 \right) \cdot \left(\sum_{\chi \in \operatorname{supp} \widehat{f}} |\mathbb{1}(\chi)|^2 \right) \\
&= \frac{1}{|G|^2} \|\widehat{f}\|_2^2 \cdot |\operatorname{supp} \widehat{f}| \\
&= \frac{1}{|G|} \|f\|_2^2 \cdot |\operatorname{supp} \widehat{f}|,
\end{aligned}$$

where the last equality follows by Theorem 4.4(3). Now (5.4) implies

$$\|f\|_\infty^2 \leq \frac{1}{|G|} \|f\|_\infty^2 \cdot |\operatorname{supp} f| \cdot |\operatorname{supp} \widehat{f}|.$$

Since f is not identically zero we have $\|f\|_\infty^2 \neq 0$ and thus the statement follows. ☐

Below we give two examples where Theorem 5.1 holds with equality.

Example 5.2. (1) Consider $f = \delta_0$, $0 \in G$ as in Exercise 3.8. Then $\operatorname{supp} f = \{0\}$. On the other hand $\widehat{\delta_0}(\chi) = 1$ for all $\chi \in \widehat{G}$. Thus $\operatorname{supp} \widehat{f} = \widehat{G}$, and $|\operatorname{supp} f| \cdot |\operatorname{supp} \widehat{f}| = |G|$.

(2) Let $T \subseteq G$ be a subset. Define

$$\delta_T(x) = \begin{cases} 1, & \text{if } x \in T, \\ 0, & \text{if } x \notin T. \end{cases}$$

In this case we say that δ *is supported in* T. Now let $H \leq G$ be a subgroup. For $f = \delta_H$ we clearly have $|\mathrm{supp} f| = |H|$. On the other hand by Corollary 2.14 we have

$$\widehat{f}(\chi) = \sum_{x \in G} f(x)\overline{\chi(x)} = \sum_{x \in H} \overline{\chi(x)} = \begin{cases} |H|, & \text{if } \chi \in H^{\perp}, \\ 0, & \text{if } \chi \notin H^{\perp}. \end{cases}$$

By Theorem 2.6 we have $|\mathrm{supp}\widehat{f}| = |H^{\perp}| = |G|/|H|$, and thus $|\mathrm{supp} f| \cdot |\mathrm{supp}\widehat{f}| = |G|$. The above argument also shows that $\widehat{\delta_H} = |H|\delta_{H^{\perp}}$.

Definition 5.3. Let $f \in L^2(G)$, and $T \subseteq G$, $W \subseteq \widehat{G}$.

(1) The *time-limiting operator* P_T is given by $P_T f := f \cdot \delta_T$, that is,

$$(P_T f)(x) = f(x)\delta_T(x) = \begin{cases} f(x), & \text{if } x \in T \\ 0, & \text{if } x \notin T. \end{cases} \tag{5.6}$$

(2) The *band-limiting operator* R_W is given by

$$(R_W f)(x) = \frac{1}{|G|} \sum_{\chi \in W} \widehat{f}(\chi)\chi(x). \tag{5.7}$$

Remark 5.4. What is the band-limiting operator of a time-limiting operator, or the other way around? For this we would need the Fourier transform of $P_T f$. We have

$$\widehat{P_T f}(\chi) = \sum_{x \in G} f(x)\delta_T(x)\overline{\chi(x)} = \sum_{x \in T} f(x)\overline{\chi(x)}.$$

Thus

$$(R_W P_T f)(x) = \frac{1}{|G|} \sum_{\chi \in W} \widehat{P_T f}(\chi)\chi(x) = \frac{1}{|G|} \sum_{\chi \in W} \sum_{y \in T} f(\chi)\chi(x - y)$$

Similarly, for $x \in T$ we have

$$(P_T R_W f)(x) = (R_W f)(x)\delta_T(x) = \frac{1}{|G|} \sum_{\chi \in W} \widehat{f}(\chi)\chi(x),$$

and $(P_T R_W f)(x) = 0$ if $x \notin T$.

Definition 5.5. Let $Q : L^2(G) \longrightarrow L^2(G)$ be a linear operator.

(1) The *operator norm* $\|Q\|$ *of* Q is defined as

$$\|Q\| = \max\left\{ \frac{\|Qf\|_2}{\|f\|_2} \;\middle|\; f \in L^2(G), f \neq 0 \right\}.$$

(2) Think of Q as the $n \times n$ complex matrix of Q with respect to the basis Δ_G. Then, the L^2*-norm of* Q is defined as $\|Q\|_2^2 = \mathrm{tr}(Q^{\dagger}Q)$ where the dagger means the conjugate transpose and tr is the trace of a matrix.

Exercise 5.6. Show that $\|\bullet\|$ and $\|\bullet\|_2$ satisfy the following axioms of a *matrix norm.*

(1) $\|Q\| \geq 0$.
(2) $\|Q\| = 0 \iff Q = 0$.
(3) $\|cQ\| = |c|\|Q\|$ for $c \in \mathbb{C}$.
(4) $\|Q_1 + Q_2\| \leq \|Q_1\| + \|Q_2\|$.

(5) $\|Q_1Q_2\| \le \|Q_1\|\|Q_2\|$.

Exercise 5.7. Recall the linear operator $T_g : L^2(G) \longrightarrow L^2(G)$ from Exercise 4.9. Show that $\|T_g\| = 1$.

Lemma 5.8. *(1)* $\|R_W\| = 1$.
(2) $\|P_T\| = 1$.

Proof. (1) Note that $\|R_W\| \le 1$ iff $\|R_W f\|_2^2 \le \|f\|_2^2$, $f \ne 0$. We have

$$\begin{aligned}
\|R_W f\|_2^2 &= \sum_{x\in G} |(R_W f)(x)|^2 = \frac{1}{|G|^2}\sum_{x\in G}\left|\sum_{\chi\in W}\widehat{f}(\chi)\chi(x)\right|^2 \\
&= \frac{1}{|G|^2}\sum_{x\in G}\left(\sum_{\chi\in W}\widehat{f}(\chi)\chi(x)\right)\left(\sum_{\psi\in W}\overline{\widehat{f}(\psi)}\,\overline{\psi(x)}\right) \\
&= \frac{1}{|G|}\sum_{\chi\in W}|\widehat{f}(\chi)|^2 \\
&\le \|f\|_2^2.
\end{aligned}$$

To finish the proof it is enough to find $f \in L^2(G)$ such that $\|R_W f\|_2^2 = \|f\|_2^2$. That is, we are looking for $f \in L^2(G)$ that satisfies $\widehat{f}(\chi) = \delta_W(\chi)$. Then making use of the Fourier Inversion Formula one finds

$$f(x) = \frac{1}{|G|}\sum_{\chi\in W}\delta_W(x)\chi(x) = (R_W\delta_W)(x).$$

(2) Let $0 \ne f \in L^2(G)$. Then

$$\|P_T f\|_2^2 = \sum_{x\in G}|(P_T f)(x)|^2 = \sum_{x\in T}|f(x)|^2 \le \|f\|_2^2.$$

The same computation shows that for $f = \delta_T$ we have $\|P_T f\|_2^2 = \|f\|_2^2$. The statement now follows.

□

Exercise 5.9. Let $Q : L^2(G) \longrightarrow L^2(G)$ be a linear operator. Then Q is an *orthogonal projection* if $Q^\dagger = Q$ and $Q^2 = Q$. Show the following.
(1) If Q_1, Q_2 are two orthogonal operators then $\|Q_1Q_2\| = \|Q_2Q_1\| \le 1$.
(2) Show that P_T and R_W are orthogonal projections[8].
(3) Let Ξ be the set of all eigenvalues (that is, the spectrum) of $Q^\dagger Q$ and the let λ be the maximal eigenvalue (note first that all the eigenvalues of $Q^\dagger Q$ are real and nonnegative). Show that

$$\|Q\|^2 = \lambda \text{ and } \|Q\|_2^2 = \sum_{\lambda\in\Xi}\lambda.$$

Theorem 5.10. *Let $Q = R_W P_T$. Then*

$$\sqrt{\frac{1}{|G|}}\|Q\|_2 \le \|Q\| \le \|Q\|_2 = \sqrt{\frac{|W||T|}{|G|}}.$$

[8] For $Q^\dagger = Q$, you can either think of them as matrices with respect to Δ_G, or recall that it is enough to show $\langle Qf \,|\, f\rangle_G = \langle f \,|\, Qf\rangle_G$.

Proof. The only interesting part is the last equality as the first two inequalities follow easily by Exercise 5.9(2). To do so we will need the matrix of $R_W P_T$ with respect to the basis Δ_G. By Remark 5.4 we have

$$(R_W P_T f)(x) = \sum_{y\in G} q_{T,W}(x,y) f(y),$$

where

$$q_{T,W}(x,y) = q(x,y) := \frac{1}{|G|}\delta_T(y) \sum_{\chi\in W} \chi(x-y), \quad x, y \in G.$$

Now we compute[9]

$$\begin{aligned}
\|R_W P_T\|_2^2 = \sum_{\substack{x\in G\\ y\in G}} |q(x,y)|^2 &= \frac{1}{|G|^2} \sum_{\substack{x\in G\\ y\in G}} \left|\delta_T(y) \sum_{\chi\in W} \chi(x-y)\right|^2 \\
&= \frac{1}{|G|^2} \sum_{\substack{x\in G\\ y\in T}} \sum_{\chi\in W} \chi(x-y) \sum_{\psi\in W} \overline{\psi(x-y)} \\
&= \frac{1}{|G|^2} \sum_{y\in T} \sum_{\substack{\chi\in W\\ \psi\in W}} \psi(y)\overline{\chi(y)} \sum_{x\in G} \chi(x)\overline{\psi(x)} \\
&= \frac{1}{|G|} \sum_{y\in T} \sum_{\chi\in W} \chi(y)\overline{\chi(y)} \\
&= \frac{|W||T|}{|G|}.
\end{aligned}$$

□

Definition 5.11. A map $f \in L^2(G)$ is called *ε-concentrated on $T \subseteq G$* if $\|f - \delta_T f\|_2 \le \varepsilon \|f\|_2$. A map $F \in L^2(\widehat{G})$ is called *η-concentrated on $W \subseteq \widehat{G}$* if $\|F - \delta_W F\|_2 \le \eta \|f\|_2$. $f \in L^2(G)$ is called *η-band-limited to W* if there exists $f_W \in L^2(G)$ such that $\operatorname{supp}\widehat{f_W} \subseteq W$ and $\|f - f_W\|_2 \le \eta \|f\|_2$.

Theorem 5.12. *Let $0 \ne f \in L^2(G)$ be ε-concentrated on T and η-band-limited to W. Then*

$$\sqrt{\frac{|T||W|}{|G|}} \ge \|P_T R_W\| \ge 1 - \varepsilon - \eta.$$

Proof. Note that the first inequality follows by Theorem 5.10 and Exercise 5.9. Let f_W be such that $\operatorname{supp}\widehat{f_W} \subseteq W$ and $\|f - f_W\|_2 \le \eta \|f\|_2$. It is easy to see that $R_W f_W = f_W$. Next, it follows (easily) by Exercise 5.9(3) that $\|P_T\|_2 = 1$. Also recall that $P_T f = \delta_T f$. Now we compute

$$\begin{aligned}
\|f\|_2 - \|P_T R_W f\|_2 &\le \|f - P_T R_W f\|_2 \\
&\le \|f - P_T f\|_2 + \|P_T f - P_T R_W f\|_2 \\
&\le \varepsilon \|f\|_2 + \|P_T\|_2 \|f - f_W\|_2 \\
&\le \varepsilon \|f\|_2 + \eta \|f\|_2.
\end{aligned}$$

To conclude the proof divide by $0 \ne \|f\|_2$. □

[9] Make sure to justify the very first equality.

6 Error-Correcting Codes: MacWilliams Theorem

It is now time to see the first application of the Fourier transform. In this section we will introduce basic notions from coding theory. Although we will focus on the binary case (that is, over the binary field $\mathbb{F}_2$) everything can be easily adapted over any finite field.

Before we give concise definitions let us explore a simple scenario to gain some intuition. Assume you need to answer a yes-or-no question you received. Think of 1 as "yes" and 0 as "no". You read the question and you want to respond "yes", that is, you send out 1. During transmission an error may occur. The errors in this case are *bit-flip* erros: $1 \longmapsto 0$ or $0 \longmapsto 1$. Assume that a bit flips with probability[10] p. Thus, with probability $1-p$ no error will occur. Now instead of sending 1, send out the string 111. Errors may occur during transmission, and assume now the string is abc. It seems reasonable to *decode* the corrupted string abc as 1 if there are at least two 1 in it, that is, if at most one error has occurred. The options are:

(1) No error happens during transmission. The probability of this event is $(1-p)^3$.
(2) One error occurs during transmission. The probability of this event is $3p(p-1)^2$.
(3) Two errors occur during transmission. The probability of this event is $3p^2(p-1)$.
(4) Three errors occur during transmission. The probability of this event is p^3.

Thus, the probability that at most one error occurs is $(1-p)^3 + 3p(1-p)^2$, which approaches one as p gets smaller. In this way we have drastically increased the likelihood of decoding correctly. However, be aware that in the less likely event that two errors occur, the decoding will be incorrect.

A *binary linear code of length* n is a vector space $\mathcal{C} \subseteq \mathbb{F}_2^n$. Elements of $\mathcal{C}$ are called *codewords*. If the dimension of $\mathcal{C}$ is k we say that $\mathcal{C}$ is an $[n,k]$-code. The *Hamming distance* of $x, y \in \mathbb{F}_2^n$ is

$$\mathrm{d_H}(x,y) := |\{i \mid x_i \neq y_i\}|. \tag{6.1}$$

The Hamming distance is indeed a distance function as it satisfies the following:

(1) $\mathrm{d_H}(x,y) \geq 0$.
(2) $\mathrm{d_H}(x,y) = 0$ iff $x = y$.
(3) $\mathrm{d_H}(x,y) = \mathrm{d_H}(y,x)$.
(4) $\mathrm{d_H}(x,y) \leq \mathrm{d_H}(x,z) + \mathrm{d_H}(z,y)$.

Exercise 6.1. Show that the Hamming distance is *translation invariant*, that is, for all $z \in \mathbb{F}_2^n$ we have $\mathrm{d_H}(x+z, y+z) = \mathrm{d_H}(x,y)$.

The Hamming distance gives rise to the *Hamming weight* $\mathrm{wt_H}(x) := \mathrm{d_H}(x,0) = |\{i \mid x_i \neq 0\}|$. The *minimum distance* of $\mathcal{C}$ is

$$\mathrm{dist}(\mathcal{C}) := \min_{\substack{x,y\in\mathcal{C}\\ x\neq y}}\{\mathrm{d_H}(x,y)\} = \min_{\substack{x\in\mathcal{C}\\ x\neq 0}}\{\mathrm{wt_H}(x)\}, \tag{6.2}$$

where the last equality follows by the linearity of $\mathcal{C}$ and Exercise 6.1. If $\mathrm{dist}(\mathcal{C}) = d$ we say that $\mathcal{C}$ is an $[n,k,d]$-code.

Remark 6.2. Let $\mathcal{C}$ be and $[n,k,d]$-code. Since $\mathcal{C}$ is a subspace, it is the row space of a $k \times n$ matrix G (pick a basis of $\mathcal{C}$ and use the basis codewords as rows of G). Note that G has rank k. We call G *generating matrix*. In other words we have $\mathcal{C} = \{xG \mid x \in \mathbb{F}_2^k\}$. We say that $x \in \mathbb{F}_2^k$ is the *message* and $xG \in \mathcal{C}$ is its *encoding*. By performing row and column operations we may assume (without loss of generality, which needs a little bit of "convince yourself") that a generating matrix

[10] Of course the smaller p is the better the *channel* is. Obtaining high quality channels is an engineering task.

is of the *standard* form $G = [I_k \mid A]$. With a generating matrix in standard form, x is encoded as $xG = (x,y)$ where $y = xA \in \mathbb{F}_2^{n-k}$. Thus the transmitted word x appears in the first k bits of its encoding. Similarly, $\mathcal{C}$ is the kernel[11] of a $(n-k)\times n$ matrix H. Such a matrix is called *parity check matrix*. In other words $\mathcal{C} = \{x \in \mathbb{F}_2^n \mid Hx^\mathsf{T} = 0\}$. If $G = [I_k \mid A]$ is a generating matrix then $H = [A^\mathsf{T} \mid I_{n-k}]$ is a parity check matrix in standard form.

Definition 6.3. Let $\mathcal{C} \subseteq \mathbb{F}_2^n$ be a linear code. The *dual code* is

$$\mathcal{C}^\perp := \{x \in \mathbb{F}_2^n \mid x\cdot c = \sum_{i=1}^n x_i c_i = 0 \text{ for all } c \in \mathcal{C}\}.$$

Exercise 6.4. Let $\mathcal{C}$ be an $[n,k]$-code. Show the following.

(1) Since $\mathcal{C}$ is a vector space it is in particular a finite abelian group. We used the perp notation to denote the dual group as in Definition 2.5(1). Show that the dual group and the dual code are isomorphic[12].

(2) G is a generating matrix of $\mathcal{C}$ iff G is the parity check matrix of $\mathcal{C}^\perp$ and H is the parity check matrix of $\mathcal{C}$ iff H is the generating matrix of $\mathcal{C}^\perp$. Conclude that $\mathcal{C}^\perp$ is an $[n, n-k]$-code.

Example 6.5 (The Hamming code)**.** In this example we will see in action one of the most famous error-correcting codes - the Hamming $[7,4,3]$-code. Let $\mathcal{C}$ be the $[7,4]$-code given by the following generating matrix in standard form

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Then $\mathcal{C}$ has $2^4 = 16$ codewords. By going through all the codewords you will verify that $\operatorname{dist}(\mathcal{C}) = 3$. A parity check matrix for $\mathcal{C}$ is

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Note that the columns of H are all the elements of $\mathbb{F}_2^3$ and they are ordered in such a way that the i^{th} column of H is the binary expansion of i. The Hamming code can correct one error. Assume that for the message $x \in \mathbb{F}_2^4$ at most one error occurred in xG during transmission. Of course if no error occurred we're happy. So assume that a single error occurred. Denote r the word received, that is xG with an error occurred somewhere. Since a single error has occurred we may write $r = xG + e_i$ where e_i is the i^{th} standard basis vector. Since H is a parity check matrix we have $H(xG)^\mathsf{T} = (HG^\mathsf{T})x^\mathsf{T} = 0$. The column vector $z := Hr^\mathsf{T} = He_i^\mathsf{T} \in \mathbb{F}_2^3$ is called the *error syndrome*. The error syndrome tells us where the error occurred. After we spot the index i where the error occurred we easily correct it by *flipping* the bit i.

We now turn to the main purpose of this section.

Definition 6.6. Let $\mathcal{C}$ be an $[n,k]$-code. Let $A_i := |\{x \in \mathcal{C} \mid \mathrm{wt_H}(x) = i\}|$. The *weight enumerator polynomial of* $\mathcal{C}$ is given by

$$w_{\mathcal{C}}(x,y) = \sum_{i=0}^n A_i x^{n-i} y^i.$$

[11] We are talking about the right kernel because it is customary in coding theory to use row vectors.

[12] Thus the usage of the perp notation in Definition 6.3 is justified. We will think of $\mathcal{C}^\perp$ as a dual code and as dual group interchangeably, and it should be clear from context what we mean.

Theorem 6.7 (MacWilliams Theorem). *Let $\mathcal{C}$ be an $[n,k]$-linear code. Then the weight enumerator polynomial of the dual code $\mathcal{C}^\perp$ is*

$$w_{\mathcal{C}^\perp}(x,y) = \frac{1}{|\mathcal{C}|} w_{\mathcal{C}}(x+y, x-y).$$

Proof. Consider the function $f : \mathcal{C} \longrightarrow \mathbb{C}$, $c \longmapsto x^{n-\mathrm{wt}_{\mathrm{H}}(c)} y^{\mathrm{wt}_{\mathrm{H}}(c)}$. Note first that $w_{\mathcal{C}}(x,y) = \sum_{c\in\mathcal{C}} f(c)$. Since $\mathbb{F}_2 = \mathbb{Z}_2$ we can make use of (4.9) and Remark 2.4 to compute $\widehat{f}$. Since -1 is a second root of unity we have

$$\begin{aligned}
\widehat{f}(c) &= \sum_{v\in\mathcal{C}} x^{n-\mathrm{wt}_{\mathrm{H}}(v)} y^{\mathrm{wt}_{\mathrm{H}}(v)} (-1)^{\sum_{i=1}^n v_i c_i} \\
&= \prod_{i=1}^n \left(\sum_{v_i=0}^1 (-1)^{c_i v_i} x^{1-v_i} y^{v_i} \right) \\
&= (x+y)^{n-\mathrm{wt}_{\mathrm{H}}(c)} (x-y)^{\mathrm{wt}_{\mathrm{H}}(c)}.
\end{aligned}$$

By Theorem 4.6 we have

$$\begin{aligned}
w_{\mathcal{C}^\perp}(x,y) &= \sum_{a\in\mathcal{C}^\perp} f(a) = \frac{1}{|\mathcal{C}|} \sum_{c\in\mathcal{C}} \widehat{f}(c) \\
&= \frac{1}{|\mathcal{C}|} \sum_{c\in\mathcal{C}} (x+y)^{n-\mathrm{wt}_{\mathrm{H}}(c)} (x-y)^{\mathrm{wt}_{\mathrm{H}}(c)} \\
&= \frac{1}{|\mathcal{C}|} w_{\mathcal{C}}(x+y, x-y).
\end{aligned}$$

□

Example 6.8. Consider again the Hamming code from Example 6.5. It is easy to see that its weight enumerator polynomial is

$$w_{\mathcal{C}}(x,y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7. \tag{6.3}$$

By making use of Theorem 6.7 one computes

$$w_{\mathcal{C}^\perp}(x,y) = x^7 + 7x^3y^4. \tag{6.4}$$

Note that (6.4) implies $\mathrm{dist}(\mathcal{C}^\perp) = 4$, and thus the dual of the Hamming $[7,4,3]$-code is an $[7,3,4]$-code. In literature the dual of the Hamming code is know as the *shortened Hadamard code* or as a *simplex code*.

7 Quadratic Reciprocity Law

Throughout this section p will be an odd prime and we will work with the field $\mathbb{Z}_p$. Recall that $\mathbb{Z}_p^*$ is cyclic. Fix $\overline{g}$ a generator. In particular $\overline{g}^{p-1} = \overline{1}$ and $\overline{g}^{(p-1)/2} = -\overline{1}$. Denote $\mathcal{Q}_p = \{\overline{x}^2 \mid \overline{x} \in \mathbb{Z}_p^*\}$. Elements of $\mathcal{Q}_p$ are called *quadratic residues*. Note that $\overline{0}$ is not (considered) a quadratic residue. Put $\mathcal{N}_p := \mathbb{Z}_p^* - \mathcal{Q}_p$. Elements of $\mathcal{N}_p$ are called *quadratic nonresidues*.

Remark 7.1. Let $f : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^*$, $\overline{x} \longmapsto \overline{x}^2$. Clearly f is a homomorphism and $\operatorname{im} f = \mathcal{Q}_p$. Thus $\mathcal{Q}_p$ is a cyclic subgroup. In fact $\mathcal{Q}_p = \{\overline{g}^{2i} \mid 0 \le i < (p-1)/2\}$. It follows that $|\mathcal{Q}_p| = (p-1)/2$ and $|\mathcal{Q}_p| = |\mathcal{N}_p|$. Moreover it is not difficult to see that $\mathcal{Q}_p\mathcal{Q}_p = \mathcal{Q}_p$, $\mathcal{N}_p\mathcal{Q}_p = \mathcal{N}_p$, and $\mathcal{N}_p\mathcal{N}_p = \mathcal{Q}_p$.

Definition 7.2. Let $a \in \mathbb{Z}$ be not divisible by p. The *Legendre symbol* is

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } \overline{a} \in \mathcal{Q}_p, \\ -1, & \text{if } \overline{a} \in \mathcal{N}_p. \end{cases}$$

That is, the Legendre symbol is a map $\mathbb{Z} - p\mathbb{Z} \longrightarrow \mathbb{C}$.

.

Lemma 7.3 (Euler's Criterion)**.** *Suppose that p does not divide a. Then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} (\operatorname{mod} p).$$

As an immediate consequence we have

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Proof. Since p does not divide a we have $\overline{a} \in \mathbb{Z}_p^*$. Recall that we have fixed a generator $\overline{g}$ of $\mathbb{Z}_p^*$. Thus, there exists t such that $\overline{a} = \overline{g}^t$. Clearly $\overline{a} \in \mathcal{Q}_p$ iff t is even. It follows that $\left(\frac{a}{p}\right) = (-1)^t$. We mentioned that $\overline{g}^{(p-1)/2} \equiv -\overline{1}$. Thus

$$a^{(p-1)/2} \equiv (-1)^t \equiv \left(\frac{a}{p}\right) (\operatorname{mod} p).$$

□

Corollary 7.4. *With a slight abuse of notation, the map*

$$\left(\frac{\bullet}{p}\right) : \mathbb{Z}_p^* \longrightarrow \mathbb{C},\ \overline{a} \longrightarrow \left(\frac{a}{p}\right),$$

is a (multiplicative, of course) homomorphism, and thus a Dirichlet character (see Example 2.3).

Proof. Immediate consequence of the proof of Lemma 7.3. □

Definition 7.5.

$$\chi_p(\overline{x}) = \begin{cases} \left(\frac{x}{p}\right), & \text{if } \overline{x} \neq \overline{0}, \\ 0, & \text{if } \overline{x} = \overline{0}. \end{cases}$$

Note that by Corollary 7.4 we have $\chi_p \in \widehat{\mathbb{Z}_p}$.

Lemma 7.6. $\widehat{\chi_p}(-\overline{x}) = \chi_p(\overline{x}) \widehat{\chi_p}(-\overline{1})$.

Proof. Note that if $\overline{x} = \overline{0}$ the statement is trivial. Assume now that $\overline{x} \neq \overline{0}$. We have

$$\begin{aligned} \widehat{\chi_p}(-\overline{x}) &= \sum_{\overline{a} \in \mathbb{Z}_p} \chi_p(\overline{a}) \exp\left(\frac{2\pi i x a}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \exp\left(\frac{2\pi i x a}{p}\right) \\ &= \sum_{b=0}^{p-1} \left(\frac{b x^{-1}}{p}\right) \exp\left(\frac{2\pi i b}{p}\right) = \left(\frac{x^{-1}}{p}\right) \widehat{\chi_p}(-\overline{1}) \\ &= \chi_p(\overline{x}) \widehat{\chi_p}(-\overline{1}), \end{aligned}$$

where by x^{-1} we denote a representative of $\overline{x}^{-1}$. The very last equality follows from $\chi_p(\overline{x}^{-1}) = (\chi_p(\overline{x}))^{-1} = \chi_p(\overline{x})$. □

Lemma 7.6 implies that χ_p is a constant multiple of its own Fourier transform because

$$\widehat{\chi_p}(\overline{x}) = \chi_p(-\overline{x})\widehat{\chi_p}(-\overline{1}) = \chi_p(\overline{x})[\underbrace{\chi_p(-\overline{1})\widehat{\chi_p}(-\overline{1})}_{\text{constant}}]. \tag{7.1}$$

Definition 7.7. The *Gauss sum* of $\overline{a} \in \mathbb{Z}_p^*$ and $\chi \in \widehat{\mathbb{Z}_p^*}$ is

$$\mathfrak{g}(\overline{a}, \chi) := \widehat{\chi}(-\overline{x}) = \sum_{\overline{x} \in \mathbb{Z}_p^*} \chi(\overline{x}) \exp\left(\frac{2\pi i a x}{p}\right).$$

Exercise 7.8. Show that $\mathfrak{g}(\overline{a}, \chi) = \overline{\chi(g)}\mathfrak{g}(\overline{1}, \chi)$.

Throughout we will denote $\mathfrak{g} := \mathfrak{g}(\overline{1}, \chi_p) = \widehat{\chi_p}(-\overline{1})$.

Lemma 7.9. $\mathfrak{g}^2 = (-1)^{(p-1)/2} p$.

Proof. Apply the Fourier transform to Lemma 7.6 and use Exercise 4.8 to obtain

$$p\chi_p(\overline{x}) = \widehat{\chi_p}(\overline{x})\widehat{\chi_p}(-\overline{1}). \tag{7.2}$$

Evaluate (7.2) at $\overline{x} = -\overline{1}$ to obtain $\mathfrak{g}^2 = p\chi_p(-\overline{1})$. Making use of Euler's criterion we have

$$\mathfrak{g}^2 = p\chi_p(-\overline{1}) = \left(\frac{-1}{p}\right)p = (-1)^{(p-1)/2}p.$$

$\square$

Lemma 7.10. *Let $q \neq p$ be an odd prime. Then*

$$\mathfrak{g}^{q-1} \equiv \left(\frac{\mathfrak{g}^2}{q}\right) (\operatorname{mod} q).$$

Proof. Since q is odd, by Euler's Criterion we have

$$\left(\frac{\mathfrak{g}^2}{q}\right) \equiv (\mathfrak{g}^2)^{(q-1)/2} (\operatorname{mod} q) = \mathfrak{g}^{q-1} (\operatorname{mod} q).$$

$\square$

Note that for an odd prime $q = 2k+1$, by Lemma 7.9 we have $\mathfrak{g}^{q-1} = p^k \in \mathbb{Z}$, which is not a priori clear from the definition of $\mathfrak{g}$. Clearly $\mathfrak{g} \notin \mathbb{Z}$. Let $\omega = \exp(2\pi i/p)$. Then $\mathfrak{g} \in \mathbb{Z}[\omega]$, where

$$\mathbb{Z}[\omega] = \left\{ \sum_{i=0}^{r} a_i \omega^i \;\middle|\; a_i \in \mathbb{Z}, r \geq 0 \right\}, \tag{7.3}$$

is the polynomial ring with variable ω and integer coefficients.

Exercise 7.11. Show the following.
(1) $\mathbb{Z}[\omega] \cap \mathbb{Q} = \mathbb{Z}$. (**Hint:** Use the fact that the minimal polynomial of ω is $x^{p-1} + \cdots + x + 1$.)
(2) For any prime q and $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}[\omega]$ we have

$$\left(\sum_{i=1}^{k} \alpha_i\right)^q \equiv \left(\sum_{i=1}^{k} \alpha_i^q\right) (\operatorname{mod} q).$$

Lemma 7.12. *Let $q \neq p$ be an odd prime. Then $(\widehat{\chi_p}(\overline{x}))^q \equiv \widehat{\chi_p}(q\overline{x}) (\operatorname{mod} q)$.*

Proof. We have

$$\begin{aligned}(\widehat{\chi_p}(\overline{x}))^q &= \left(\sum_{\overline{a}\in\mathbb{Z}_p} \left(\frac{a}{p}\right) \exp\left(\frac{-2\pi iax}{p}\right)\right)^q \\ &\equiv \sum_{\overline{a}\in\mathbb{Z}_p} \left(\frac{a}{p}\right) \exp\left(\frac{-2\pi iqax}{p}\right) \\ &= \widehat{\chi_p}(q\overline{x}),\end{aligned}$$

where the congruence follows by Exercise 7.11(2). □

Theorem 7.13 (Quadratic Reciprocity Law)**.** *Let $q \neq p$ be an odd prime. Then*

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

Proof. Evaluate Lemma 7.12 at $\overline{x} = -\overline{1}$ and make use of Lemma 7.6 to obtain

$$\mathfrak{g}^q \equiv \widehat{\chi_p}(-\overline{q}) \equiv \left(\frac{q}{p}\right)\mathfrak{g} \,(\operatorname{mod} q). \tag{7.4}$$

Multiply (7.4) by $\mathfrak{g}$ and make use of Lemma 7.10 to obtain

$$\left(\frac{q}{p}\right)\mathfrak{g}^2 \equiv \mathfrak{g}^{q-1}\mathfrak{g}^2 \equiv \left(\frac{\mathfrak{g}^2}{q}\right)\mathfrak{g}^2 \equiv \,(\operatorname{mod} q). \tag{7.5}$$

By Lemma 7.9 we have

$$(-1)^{(p-1)/2}p\left(\frac{\mathfrak{g}^2}{q}\right) \equiv (-1)^{(p-1)/2}p\left(\frac{q}{p}\right) (\operatorname{mod} q). \tag{7.6}$$

Since $\gcd(p,q) = 1$ we can cancel out p in (7.6) and the equivalence becomes equality. Since the Legendre symbol is multiplicative, and by Lemmas 7.9 and 7.3 we obtain

$$\left(\frac{q}{p}\right) = \left(\frac{\mathfrak{g}^2}{q}\right) = \left(\frac{(-1)^{(p-1)/2}p}{q}\right) = \left(\frac{(-1)^{(p-1)/2}}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2}\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right). \tag{7.7}$$

□

Exercise 7.14. Show that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Why does the proof of Theorem 7.13 fall apart for the case $q = 2$?

8 Graphs over Finite Abelian Groups

We start with some terminology and notation. Let X be a graph. We will denote $V(X) = \{x_1, \ldots, x_n\}$ the set of vertices of X and $E(X)$ the set of edges. A graph is called *k-regular* if each vertex is adjacent to exactly k vertices, that is, if the *degree* of each vertex is k. The *distance* between two vertices is the number of edges in the shortest path that connects the two. We will denote d the *diameter* of a graph, that is, the greatest distance between any pair of vertices. On the other hand, the *girth* of a graph, denoted g, is the number of edges in a shortest cycle contained in the graph. The *adjacency matrix of X* is an $n \times n$ matrix $A(X) = (a_{i,j})$ where

$$a_{i,j} = \begin{cases} 1, & \text{if } (x_i, x_j) \in E(X), \\ 0, & \text{else.} \end{cases}$$

As usual, we put $L^2(V(X)) = \{f : V(X) \longrightarrow \mathbb{C}\}$. Then $A(X)$ acts on $L^2(V(X))$ via

$$(A \cdot f)(x) = \sum_{y \text{ adjacent to } x} f(y), \quad \text{for any } x \in V(X). \tag{8.1}$$

Thus we may think of the adjacency matrix $A : L^2(V(X)) \longrightarrow L^2(V(X))$ as an *adjacency operator*.

Let G be a finite abelian group. In this section we will consider graphs whose vertices are labeled by G, that is, $V(X) = G$. A subset $S \subseteq G$ is called *symmetric* if $-x \in S$ for all $x \in S$. Note that a subgroup of G constitutes a symmetric set (with the additional property that $0 \in S$). The *Cayley graph over G associated to S*, denoted $X = X(G,S)$, is the graph where $V(X) = G$ and $E(X) = \{(x, x+s) \mid x \in V(X), s \in S\}$. Then (8.1) reads as

$$Af(x) = \sum_{s \in S} f(x+s) = (\delta_S * f)(x). \tag{8.2}$$

Note that $X(G,S)$ is a $|S|$-regular graph. It is easy to see that $\langle\, Af \mid g \,\rangle_G = \langle\, f \mid Ag \,\rangle_G$, and thus A is a *self-adjoint* operator. In particular A is diagonalizable. We will pay special attention to the case $G = \mathbb{Z}_n$ associated to the *shell* $S(r) := \{\pm r (\operatorname{mod} n)\}$ and the *ball* $B(r) := \{0, \pm 1, \ldots, \pm r (\operatorname{mod} n)\}$.

Theorem 8.1 (Spectra of Cayley graphs)**.** *The set of eigenvalues (that is, the* spectrum*) of $A(X)$, where $X = X(G,S)$, is $\{\widehat{\delta_S}(\chi) \mid \chi \in \widehat{G}\}$.*

Proof. As in (8.2) we have $Af = \delta_S * f$. By Theorem 4.4(2) we have $\widehat{Af}(\chi) = \widehat{\delta_S * f}(\chi) = \widehat{\delta_S}(\chi)\widehat{f}(\chi)$. Note that the latter gives a diagonalization of A. To point out this let us use the old notation of the Fourier transform $\mathcal{F}f := \widehat{f}$. Thus for $h = \mathcal{F}f = \widehat{f}$ we have

$$[(\mathcal{F}A\mathcal{F}^{-1})(h)](\chi) = (\mathcal{F}\delta_S(\chi)) \cdot h(\chi).$$

Now the statement follows by the Spectral Theorem for self-adjoint operators. □

Example 8.2. Theorem 8.1 tells us that the eigenvalues of $A(X)$ are precisely

$$\widehat{\delta_S}(\chi) = \sum_{s \in S} \overline{\chi(s)} = \sum_{s \in S} \chi(s), \quad \chi \in \widehat{G}. \tag{8.3}$$

For the case $G = \mathbb{Z}_n$, recall that, as in (4.9), the Fourier transform takes values in $\mathbb{Z}_n$ rather that in $L^2(\mathbb{Z}_n)$. In this case the eigenvalues of $A(X)$ are precisely

$$\widehat{\delta_S}(\overline{x}) = \sum_{\overline{s} \in S} \exp\left(\frac{2\pi i x s}{n}\right), \quad \overline{x} \in \mathbb{Z}_n. \tag{8.4}$$

Let us consider now two special cases. The Cayley graph $X = X(\mathbb{Z}_n, S(1))$, that is, the cycle on n vertices. By Theorem 8.1, the eigenvalues of X are

$$\widehat{\delta_S}(\overline{x}) = \sum_{\overline{s}\in S(1)} \exp\left(\frac{2\pi i x s}{n}\right) = \exp\left(\frac{-2\pi i x}{n}\right) + \exp\left(\frac{2\pi i x}{n}\right) = 2\cos\left(\frac{2\pi x}{n}\right),$$

where the last equality follows by *Euler's formula* $\exp(ix) = \cos(x) + i\sin(x)$. Similarly, if we consider the Cayley graph $X = X(\mathbb{Z}_n, B(r))$, we find that the eigenvalues of $A(X)$ are

$$\widehat{\delta_S}(\overline{x}) = \sum_{k=-r}^{r} \exp\left(\frac{2\pi i k x}{n}\right) = 1 + 2\cos\left(\frac{2\pi x}{n}\right) + \cdots + 2\cos\left(\frac{2\pi r x}{n}\right), \quad \overline{x} \in \mathbb{Z}_n. \tag{8.5}$$

Note that for $\overline{x} \neq \overline{0}$, that is, n doesn't divide x, we can rewrite[13] (8.5) as

$$\widehat{\delta_S}(\overline{x}) = \frac{\sin(\pi x(2r+1)/n)}{\sin(\pi x/n)}. \tag{8.6}$$

Remark 8.3. By making use of (8.2) and (8.3) it follows easily that $\chi \in G$ is an eigenfunction[14] of $A(X)$ corresponding to the eigenvalue $\widehat{\delta_S}(\chi)$. That is $(A \cdot \chi) = \widehat{\delta_S}(\chi)\chi$ holds for all $\chi \in \widehat{G}$.

8.1 Four Questions about Cayley Graphs

Here we will discuss questions of interests about Cayley graphs. We will focus to finite abelian groups G and symmetric sets S for which the questions are somewhat easy.

Question 8.4. Let $X = X(G, S)$ be the Cayley graph over G associated to S.
(1) Is X *Ramanujan*[15], that is, if $\lambda \in \mathrm{Spec}(A(X))$, $|\lambda| < k$, does λ satisfy $|\lambda| \le 2\sqrt{k-1}$?
(2) Is[16] $0 \in \mathrm{Spec}(A(X))$?
(3) Can we bound the diameter d?
(4) Can we bound the girth g?

Example 8.5. (1) Consider the cycle $X(\mathbb{Z}_n, S(1)\})$. By (8.4) we know the spectrum of $A(X)$, namely,

$$\mathrm{Spec}(A(X)) = \left\{ 2\cos\left(\frac{2\pi x}{n}\right) \,\middle|\, \overline{x} \in \mathbb{Z}_n \right\}.$$

Thus X is clearly Ramanujan and $0 \in \mathrm{Spec}(A(X))$ iff n is divisible by 4. Since X is a cycle with n vertices, it follows that $d = \lfloor n/2 \rfloor$ and $g = n$.

(2) Consider the Cayley graph $X(\mathbb{Z}_n, B(r))$. It is easy to see that due to (8.6) we have X is not Ramanujan for large values of n and that $0 \notin \mathrm{Spec}(A(X))$ iff $\gcd(n, 2r+1) = 1$. On the other hand, X has loops since $\overline{0} \in B(r)$. Thus $g = 1$. Computing the diameter is trickier. See Theorem 1, page 77 for an upper bound.

Exercise 8.6. Show that for any prime p and any symmetric set $\{\overline{0}\} \neq S \subsetneq \mathbb{Z}_p$, $0 \notin \mathrm{Spec}(A(X))$ where $X = X(\mathbb{Z}_p, S)$.

[13] This is a nice little trigonometric trick.
[14] Since $A(X)$ is an operator on the function space $L^2(G)$ the "vectors" are functions and thus the word "eigenfunction".
[15] See also Theorem 1, page 54 for facts on the spectra of k-regular graphs to gain some intuition.
[16] By the Spectral Theorem, the determinant of a matrix is equal to the product of its eigenvalues, and thus the question is equivalent with whether or not $A(X)$ is invertible.

Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements. Recall the norm function from (8.12). Recall also the notation $d_n := (p^n - 1)/(p-1) = |\Xi_n|$ where $\Xi_n = \{x \in \mathbb{F}_{p^n} \mid N(x) = 1\}$. Note that Ξ_n is symmetric iff n is even, and thus in what follows we restrict ourselves to even n.

Definition 8.7. Let n be even. The graph $X = X(\mathbb{F}_{p^n}, \Xi_n)$, that is, $V(X) = \mathbb{F}_{p^n}$ and $E(X) = \{(x, x+s) \mid x \in \mathbb{F}_{p^k}, s \in \Xi_n\}$, is called *Winnie Li's graph.*

Example 8.8. Consider the field on four elements $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, where $\alpha^2 = \alpha + 1$, that is, $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$. Since $|\Xi_2| = (4-1)/(2-1) = 3$ and $N(0) = 0$ we have $\Xi_2 = \{1, \alpha, \alpha^2\}$. Note that by definition $(x, y) \in E(X)$ iff $x - y \in \Xi_2 = \{1, \alpha, \alpha^2\}$ iff $x \neq y$. In other words, there is an edge between every two different vertices. That is $X = X(\mathbb{F}_{2^2}, \Xi_2)$ is the complete graph in four vertices. In particular, X has diameter 1 and girth 3.

Remark 8.9. In order to attempt answering Question 8.4(1)-(2) for the Winnie Li's graph one needs a complete description of $\widehat{\mathbb{F}_{p^n}}$. But we covered this in Remark 2.2. Namely, we have $\widehat{\mathbb{F}_{p^n}} = \{\chi_x \mid x \in \mathbb{F}_{p^n}\}$, where $\chi_x(y) := \omega^{\operatorname{tr}(xy)}$ and $\omega = \exp(2\pi i/p)$. By Remark 8.3 it follows that χ_x is an eigenfunction corresponding to the eigenvalue

$$\widehat{\delta_{\Xi_n}}(\chi_x) = \sum_{s \in \Xi_n} \chi_x(s) = \sum_{s \in \Xi_n} \omega^{\operatorname{tr}(sx)} = \sum_{\substack{s \in \mathbb{F}_{p^n} \\ N(s)=1}} \exp\left(\frac{2\pi i(\operatorname{tr}(sx))}{p}\right).$$

For a discussion for the case $n = 2$ see page 75 and the references therein.

Exercise 8.10. Let K_n denote the complete graph on n vertices. Show that K_n is a Cayley graph and compute $\operatorname{Spec}(A(K_n))$. Is K_n Ramanujan?

8.2 Random Walks in Cayley Graphs

Consider the Cayley graph $X = X(\mathbb{Z}_n, S)$ with $|S| = k$. Then X is a k-regular graph. Throughout we will assume that X is not bipartite. Assume that a person is standing in vertex $\overline{x} \in V(X)$ and that the person walks along the edges of X. Thus the person can walk from $\overline{x}$ to $\overline{x+s}$ for any $\overline{s} \in S$. We assume that all the events occur with equal probability $1/k$, which makes the event a *random walk*. A random walk gives rise to the *Markov transition matrix*

$$T = (p_{i,j})_{0 \le i,j \le n} = \frac{1}{k} A(X), \tag{8.7}$$

where $A(X)$ is the adjacency matrix of X. Similarly as $A(X)$, T can be viewed as a *transition operator* by acting on $L^2(\mathbb{Z}_n)$ (as in (8.1)). Clearly T is self-adjoint.

Remark 8.11. Since $T = (1/k)A(X)$ we have $\operatorname{Spec}(T) = (1/k)\operatorname{Spec}(A(X))$. By making use of Theorem 1, page 54 we conclude that $\operatorname{Spec}(T)$ is of the form

$$\lambda_1 = 1 > \lambda_2 \ge \cdots \ge \lambda_n > -1. \tag{8.8}$$

It follows that

$$\beta := \max\{|\lambda| \mid \lambda \in \operatorname{Spec}(T), \lambda \neq 1\} < 1. \tag{8.9}$$

Since T is self-adjoint we will fix a orthonormal basis of eigenfunctions $\mathcal{B} = \{\phi_1, \ldots, \phi_n\}$. Of course the basis satisfies

$$T\phi_i = \lambda_i \phi_i, 1 \le i \le n, \text{ and } \langle \phi_i \,|\, \phi_j \rangle = \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases}$$

It is easy to verify that to eigenvalue $\lambda_1 = 1$ corresponds the eigenfunction $\phi_1(\overline{x}) := 1/\sqrt{n}$ for all $\overline{x} \in \mathbb{Z}_n$.

A *probability density on* $\mathbb{Z}_n$ is a function $p \in L^2(\mathbb{Z}_n)$ that satisfies

$$p(\overline{x}) \geq 0 \text{ for all } \overline{x} \in \mathbb{Z}_n, \text{ and } \sum_{\overline{x} \in \mathbb{Z}_n} p(\overline{x}) = 1.$$

If the probability density depends on time we will write $p^{(t)}(\overline{x})$ and interpret it as the probability the person is at vertex $\overline{x}$ at time t. We have

$$p^{(t+1)}(\overline{x}) = Tp^{(t)}(\overline{x}) = T^{t+1}p^{(0)}(\overline{x}).$$

The probability density $u(\overline{x}) := 1/n$ for all $\overline{x} \in \mathbb{Z}_n$ is called *uniform density.*

Theorem 8.12. *Let X be a connected nonbipartite k-regular graph with n vertices. For any probability density p we have*

$$\lim_{t \to \infty} T^t p = u.$$

Proof. Using the basis $\mathcal{B}$ from Remark 8.11, we may write

$$p(x) = \sum_{i=1}^{n} \langle p \,|\, \phi_i \rangle \phi_i(x). \tag{8.10}$$

Then applying T^t to (8.10) and using the fact that ϕ_i is an eigenfunction corresponding to λ_i we obtain

$$T^t p(x) = \sum_{i=1}^{n} \langle p \,|\, \phi_i \rangle \lambda_i^t \phi_i(x). \tag{8.11}$$

Now by making use of (8.8) and the fact that $\sum_{x \in X} p(x) = 1$ we obtain

$$\lim_{t \to \infty} T^t p = \langle p \,|\, \phi_1 \rangle \phi_1 = u.$$

□

Recall the L^2-norm form Section 5. For $f \in L^2(V(X))$ we define the L^1-*norm* as $\|f\|_1 := \sum_{x \in V(X)} |f(x)|$. The two norms satisfy

$$\|f\|_2 \leq \|f\|_1 \leq |V(X)|^{1/2} \|f\|_2. \tag{8.12}$$

Exercise 8.13. Let $\mathcal{B}$ be as in Remark 8.11. Show that for any $f \in L^2(V(X))$ we have

$$\sum_{i=1}^{n} |\langle f \,|\, \phi_i \rangle|^2 = \|f\|_2^2.$$

We have the following.

Theorem 8.14. *Let X be a connected nonbipartite k-regular graph with n vertices and let β be as in (8.9). For any probability density p we have*

$$\|T^m p - u\|_1 \leq \sqrt{n} \|T^m p - u\|_2 \leq \sqrt{n} \beta^m.$$

Proof. Note that the first inequality is an immediate consequence of (8.12). So we focus on the second inequality. We make use of the orthonormal basis $\mathcal{B}$ from Remark 8.11 yet again. Recall that $\phi_1(\overline{x}) = 1/\sqrt{n}$ for all $\overline{x} \in V(X)$. Since p is a probability density and $\lambda_1 = 1$ if follows that $\langle\, p \,|\, \phi_1 \,\rangle \lambda_1 \phi_1(\overline{x}) = u(\overline{x})$ for all $\overline{x} \in V(X)$. Now we have

$$\|T^m p - u\|_2^2 = \left\| \sum_{i=2}^{n} \langle\, p \,|\, \phi_i \,\rangle \lambda_i^m \phi_i \right\|_2^2 = \sum_{i=2}^{n} |\langle\, p \,|\, \phi_i \,\rangle|^2 |\lambda_i|^{2m}.$$

By the definition of β we have $|\lambda_i| \le \beta$ for $2 \le i \le n$. Thus

$$\|T^m p - u\|_2^2 \le \beta^{2m} \sum_{i=2}^{n} |\langle\, p \,|\, \phi_i \,\rangle|^2 \le \beta^{2m} \sum_{i=1}^{n} |\langle\, p \,|\, \phi_i \,\rangle|^2 = \beta^{2m} \|p\|_2^2,$$

where the last equality follows by Exercise 8.13. Since p is a probability density it follows that $\|p\|_2^2 \le 1$, and thus the statement follows. □

Conclusion 8.15. Since $\beta < 1$, of course β^m approaches zero as m gets larger. In Theorem 8.14, m represents the number of walks from a vertex to another (adjacent vertex). It is clear then that the number of steps needed to guarantee a truly random walk depends on how small β is. For instance, consider the Winnie Li's graph $X = X(\mathbb{F}_{p^2}, \Xi_2)$. In this case we have $n = p^2, k = p+1$, and $\beta = 2\sqrt{p}/(p+1)$. Taking $m = 3$, Theorem 8.14 reads[17] as

$$\|T^3 p - u\|_1 \le \frac{8}{\sqrt{p-1}}.$$

In other words, in this case, after only three steps (for large p) the walk looks pretty random.

8.3 Hamming graphs

In Section 6 we defined the Hamming distance. In this section we make use of it to define (and then study) a class of Cayley graphs commonly called *Hamming graphs*. In here we will discuss only the binary case, though the general case is extremely similar. Let S_n denote that standard basis of $\mathbb{F}_2^n$, that is, $S_n = \{e_1, \ldots, e_n\}$ where e_i has 1 in position i and 0 else. Then, a binary Hamming graph on n vertices is the Cayley graph $X_n := X(\mathbb{F}_2^n, S_n)$. Thus, by definition, $V(X_n) = \mathbb{F}_2^n$ and $(x, y) \in E(X_n)$ iff $\mathrm{d_H}(x, y) = 1$. For $n = 3$ the binary Hamming graph X_3 is given in Figure 1. Note

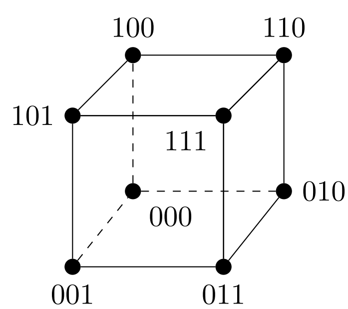

Figure 1: Binary Hamming graph X_3.

that $\mathrm{d_H}(x, y)$ equals the number of edges in the shortest path between $x, y \in \mathbb{F}_2^n$.

[17] Be aware of the probability density p and the prime number p.

We start by determining the spectrum of $A(X_n)$. Since we are considering the binary case, the second primitive root of unity is $\omega = -1$. By Theorem 8.1 (see also Example 8.2 and Remark 2.4) it follows that $\operatorname{Spec}(A(X_n)) = \{\lambda_x \mid x \in \mathbb{F}_2^n\}$ where

$$\lambda_x = \sum_{i=1}^{n} (-1)^{x \cdot e_i} = \sum_{i=1}^{n} (-1)^{x_i} = n - 2\mathrm{wt}_{\mathrm{H}}(x). \tag{8.13}$$

Theorem 8.16. *As an immediate consequence of* (8.13)*, the following hold.*
(1) $-n \in \operatorname{Spec}(A(X_n))$*, and thus* X_n *is bipartite.*
(2) X_n *is Ramanujan iff* $2 \le n \le 6$*.*
(3) $0 \in \operatorname{Spec}(A(X_n))$ *iff* n *is even.*

We now discuss a generalization of Hamming graphs. Consider the Cayley graph $X_{n,r} = X(\mathbb{F}_2^n, S_{\mathrm{H}}(r))$ where as a symmetric set we use the *Hamming sphere* $S_{\mathrm{H}}(r) := \{x \in \mathbb{F}_2^n \mid \mathrm{wt}_{\mathrm{H}}(x) = r\}$. Then $\operatorname{Spec}(A(X_{n,r})) = \{\lambda_x \mid x \in \mathbb{F}_2^n\}$ where $\lambda_x = \sum_{y \in S_{\mathrm{H}}(r)} (-1)^{x \cdot y}$. To have a full description of the eigenvalues assume $\mathrm{wt}_{\mathrm{H}}(x) = k$. We have

$$\lambda_x = \sum_{y \in S_{\mathrm{H}}(r)} (-1)^{x \cdot y} = \sum_{i=0}^{k} \binom{k}{i} \binom{n-k}{r-i} (-1)^i. \tag{8.14}$$

Clearly $\lambda_x = \lambda_y$ iff $\mathrm{wt}_{\mathrm{H}}(x) = \mathrm{wt}_{\mathrm{H}}(y)$.

Example 8.17. Consider $X_{3,2}$, that is, the graph with vertex set labeled by $\mathbb{F}_2^3$ and (x,y) is an edge iff $\mathrm{d}_{\mathrm{H}}(x,y) = 2$. The graph is given in Figure 2. Clearly $X_{3,2}$ is disconnected. Using (8.14) one computes

$$\begin{aligned}
&\lambda_{000} = 1,\\
&\lambda_{100} = \lambda_{010} = \lambda_{001} = -1,\\
&\lambda_{110} = \lambda_{101} = \lambda_{011} = -1,\\
&\lambda_{111} = 1.
\end{aligned}$$

It follows (as one can also see from Figure 2) that $X_{3,2}$ is not bipartite. It also follows that $X_{3,2}$ is Ramanujan.

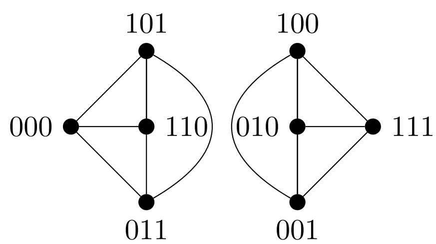

Figure 2: The graph $X_{3,2}$.

Exercise 8.18. Determine whether or not $A(X_{5,2})$ is invertible. Determine the maximum r for which $A(X_{19,r})$ is invertible.

9 Solutions to Selected Exercises

In this section we will sketch solutions of some selected exercises. The aim is to give step-by-step hints that will lead to a guided solution. Occasionally we will give complete solutions.

Exercise 1.19. It is straightforward to check that the following map

$$\Phi : \mathbb{Z}_n^* \longrightarrow \mathrm{Aut}(\mathbb{Z}_n), \quad \overline{u} \longmapsto \left\{ \begin{array}{cccc} f_u : & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & \overline{x} & \longmapsto & \overline{ux} \end{array} \right. ,$$

is an injective homomorphism. Thus it suffices to show that Φ is surjective. To that end, let $f \in \mathrm{Aut}(\mathbb{Z}_n)$. Then $f(\overline{1}) =: \overline{x}$ must be a unit in $\mathbb{Z}_n$. Thus the map f is of type f_x for $\overline{x} \in \mathbb{Z}_n^*$, that is, $\Phi(\overline{x}) = f$.

Exercise 1.23. Since $\mathbb{Z}_p$ is a domain $\overline{0}$ and $\overline{1}$ are inverses of themselves, and they are the only elements with this property. Thus, every element of the set $\{\overline{2}, \overline{3}, \ldots, \overline{p-2}\}$ can be paired up with its inverse (again from the set). In other words $\overline{2} \cdots \overline{p-2} = \overline{1}$. It follows that $(p-1)! \equiv p-1 \equiv -1 (\bmod p)$.

Exercise 2.19. Consider the following map

$$\Phi : K^\perp \longrightarrow \quad \widehat{\widehat{G}/K}, \quad g \longmapsto \left\{ \begin{array}{ccc} \Phi_g : \widehat{G}/K & \longrightarrow & \mathbb{C}^* \\ \chi + K & \longmapsto & \chi(g) \end{array} \right. .$$

You will verify that Φ_g is well-defined iff $g \in K^\perp$. It also follows easily that Φ is injective. Now by Theorem 2.6 we have $|\widehat{\widehat{G}/K}| = |\widehat{G}/K| = K^\perp$. The statement now follows by Exercise 1.20.

(1) It is straightforward to verify that $H \subseteq (H^\perp)^\perp$ and $K \subseteq (K^\perp)^\perp$. Equality follows again by Theorem 2.6.

(2) By Theorem 2.6 we have $|G^\perp| = |\widehat{G}^\perp| = 1$. The statement now follows.

(3) This is an immediate consequence of $\widehat{G}^\perp = \{0\}$ from part (2) above.

Exercise 2.22.

(1) This follows immediately from the definition and associativity of composition.

(2) We will show only the forward direction. The backward direction follows from the forward direction and the duality (9). However, you are encouraged to prove the backward direction directly. We will show first that $\mathrm{im}\, f \subseteq \ker g \implies \mathrm{im}\, g^* \subseteq \ker f^*$. You will verify first that $\ker f \subseteq \mathrm{im}\, g$ iff $g \circ f = 0$. Thus, by assumption, we have $f^* \circ g^* = (g \circ f)^* = 0^* = 0$, which in turn yields the claim. Next, we show $\ker g \subseteq \mathrm{im}\, f \implies \ker f^* \subseteq \mathrm{im}\, g^*$. Assume $\chi \in \ker f^*$, that is, $\chi \circ f = \varepsilon_B$. We are seeking $\psi \in \widehat{B}$ such that $\psi = \chi \circ g$. The latter implies $\chi(b) = \psi(g(b))$ for all $b \in B$. Define $\psi : \mathrm{im}\, g \longrightarrow \mathbb{C}$, $g(b) \longmapsto \chi(b)$. We show first that ψ is well-defined. Assume $g(b) = g(b')$. By the assumption $\ker g \subseteq \mathrm{im}\, f$, it follows that there exists $a \in A$ such that $b - b' = f(a)$. Now the well-definednesss follows by $\chi \circ f = \varepsilon_B$. To conclude the argument use Theorem 2.7.

Exercise 4.7. We compute

$$\begin{aligned}\widehat{f}(\chi_1,\dots,\chi_n) &= \sum_{(g_1,\dots,g_n)} f(g_1,\dots,g_n)\overline{(\chi_1,\dots,\chi_n)(g_1,\dots,g_n)}\\ &= \sum_{(g_1,\dots,g_n)} \prod_{i=1}^{n} f_i(g_i)\overline{\chi_i(g_i)}\\ &= \prod_{i=1}^{n}\sum_{g_i\in G_i} f_i(g_i)\overline{\chi_i(g_i)}\\ &= \prod_{i=1}^{n}\widehat{f_i}(\chi_i).\end{aligned}$$

Exercise 4.8. Recall that we identify g with the evaluation map ev_g. With this identification we have

$$\begin{aligned}\widehat{\widehat{f}}(g) = \widehat{\widehat{f}}(\mathrm{ev}_g) &= \sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\overline{\mathrm{ev}_g(\chi)}\\ &= \sum_{\chi\in\widehat{G}}\sum_{x\in G} f(x)\overline{\chi(x+g)}\\ &= \sum_{x\in G} f(x)\sum_{\chi\in\widehat{G}}\overline{\chi(x+g)}\\ &= |G|f(-g),\end{aligned}$$

where the last equality follows from (2.10).

Exercise 4.9.

(1) We need to show that for each character there exists an eigenvalue $\lambda\in\mathbb{C}$ such that $T_g\chi = \lambda\chi$. But for all $x\in G$ we have $T_g\chi(x) = \chi(x+g) = \chi(g)\chi(x)$. In other words χ is an eigenvector corresponding to the eigenvalue $\chi(g)\in\mathbb{C}$.

(2) The second part should be obvious. For the first part we have

$$\begin{aligned}\widehat{T_g f}(\chi) &= \sum_{x\in G} T_g f(x)\overline{\chi(x)} = \sum_{x\in G} f(x+g)\overline{\chi(x)}\\ &= \sum_{y\in G} f(y)\overline{\chi(y-g)} = \sum_{y\in G} f(y)\overline{\chi(y)}\chi(g)\\ &= \chi(g)\widehat{f}.\end{aligned}$$

(3) This follows immediately from the definition of convolution and T_g.

Exercise 6.4.

(1) **Hint:** Use Remark 2.4 along with the definitions of the dual group and dual code.

(2) By definition, G is a generating matrix for $\mathcal{C}$ iff $\mathcal{C} = \{xG \mid x\in\mathbb{F}_2^k\}$. Also by definition, H is a parity check matrix for $\mathcal{C}$ iff $\mathcal{C} = \{x\in\mathbb{F}_2^n \mid Hx^\mathsf{T} = 0\}$. But by the definition of the dual code

$$\begin{aligned}\mathcal{C}^\perp &= \{x\in F_2^n \mid c\cdot x = 0 \text{ for all } c\in\mathcal{C}\}\\ &= \{x\in\mathbb{F}_2^n \mid Gx^\mathsf{T} = 0\},\end{aligned}$$

and thus G is a parity check matrix for $\mathcal{C}^\perp$. To show that H is a generating matrix for $\mathcal{C}^\perp$ it suffices to show $\mathcal{C}^\perp = \{xH \mid x \in \mathbb{F}_2^{n-k}\}$. Note that " $\supseteq$ " follows easily. Now equality follows by part (1) along with Theorem 2.6.

Exercise 7.11.

(1) Using the fact that the minimal polynomial of ω is $x^{p-1} + \cdots + x + 1$ it follows easily that

$$\mathbb{Z}[\omega] = \left\{ \sum_{i=0}^{p-2} a_i \omega^i \;\middle|\; a_i \in \mathbb{Z} \right\}.$$

Now take $x \in \mathbb{Z}[\omega] \cap \mathbb{Q}$, that is, $x = n/m$, $m \neq 0$ and $x = \sum_{i=0}^{p-2} a_i \omega^i$. This implies

$$(ma_0 - n) + (ma_1)\omega + \cdots + (ma_{p-2})\omega^{p-2} = 0.$$

It follows that $ma_i = 0$ for $i = 1, \ldots, p-2$. Since $m \neq 0$ we conclude that $x = a_0 \in \mathbb{Z}$.

(2) Use binomial expansion and observe that the "middle" coefficients are divisible by q.

Exercise 7.14. Recall that we solved this exercise by following the hints of the book. In here we give an alternative solutions that uses Gauss Lemma (that you encouraged to prove).

Gauss Lemma (in number theory). Let p be an odd prime and assume a is not divisible by p. Consider the least residues modulo p of the integers $a, 2a, \ldots, ((p-1)/2)a$. Then

$$\left(\frac{a}{p}\right) = (-1)^n,$$

where n is the number of residues (from above) greater than $p/2$.

Back to the solution. We first distinguish two cases: $p \equiv \pm 1 (\bmod 8)$ and $p \pm 3 (\bmod 8)$. We focus on the first case. The second follows similarly. Note first that if $p \equiv \pm 1 (\bmod 8)$ then $(p^2-1)/8$ is even. So in this case we need to show $\left(\frac{2}{p}\right) = 1$. We now focus on the subcase $p \equiv 1 (\bmod 8)$, that is, $p = 8k+1$. Apply Gauss Lemma for $a = 2$. Thus we look at the least residues modulo p of $2, 4, \cdots, p-1$. It is easy to see that in this case there are $2k$ of such numbers greater than $p/2$. Thus the result follows. The other (three) cases are extremely similar.

Exercise 8.10. The complete graph in n vertices K_n is the Cayley graph $X(\mathbb{Z}_n, \mathbb{Z}_n - \{\overline{0}\})$. Note that $A(K_n) = J - I$ where J is the all-one matrix. It is easy to see that the eigenvalues of $A(K_n)$ are $n-1$ with multiplicity 1 and -1 with multiplicity $n-1$. Clearly K_n is Ramanujan for $n \geq 3$.

10 Written Assignment

Instructions: The assignment is due Tuesday, July 24. You should provide well-written, complete, and detailed answers. You may use additional resources, both human or electronic. However, you must have your own write-up and acknowledge any help used. You are encouraged to use a word-processing software.

Preamble: In this written assignment we will focus on the kernel of some "special" characters, called *generating characters*. For the curious reader, behind the scenes we will be considering some special instances of *finite Frobenius rings* using a character-theoretic approach. In particular, we will focus on finite abelian groups that arise as the additive group of a finite ring.

Exercise 10.1. Consider $\mathbb{Z}_8$. Recall that $\widehat{\mathbb{Z}_8} = \{\chi_0, \dots, \chi_7\}$, where χ_i's are as in the proof of Theorem 2.1(1). Then do the following.

(1) Compute $\ker \chi_i$ for $0 \le i \le 7$. Verify that $\ker \chi_0 \cap \cdots \cap \ker \chi_7 = \{\overline{0}\}$; see also equation (2.7) and Exercise 2.19.

(2) For what i's do we have $\ker \chi_i = \{0\}$? What can you say about $\overline{i} \in \mathbb{Z}_8$?

(3) Generalize (and prove) your findings to $\mathbb{Z}_n$ for any n.

Exercise 10.2. Let G be the additive group of the ring of two-by-two matrices over $\mathbb{Z}_2$. For $A = (a_{ij}) \in G$, let $\mathrm{tr}(A) = a_{11} + a_{22}$ denote the trace of A. For each $A \in G$, define

$$\chi_A : G \longrightarrow \mathbb{C}^*,\ B \longmapsto (-1)^{\mathrm{tr}(AB^{\mathsf{T}})},$$

where B^{T} is the transpose of B. Do the following.

(1) Show that $\chi_A \in \widehat{G}$ and $\widehat{G} = \{\chi_A \mid A \in G\}$.

(2) Compute $\ker \chi_I$, where I is the identity matrix.

(3) In $\widehat{G}$ define a "scalar-multiplication" by $(A \cdot \chi)(B) := \chi(BA)$ for all $A \in G$ and $\chi \in \widehat{G}$. For each $M \in G$ define $\Phi_M : G \longrightarrow \widehat{G},\ A \longmapsto A \cdot \chi_M$. Do the following.

   (i) Show that Φ_M is a *module homomorphism*, that is, Φ_M satisfies

$$\Phi_M(A_1 + A_2) = \Phi_M(A_1) + \Phi_M(A_2)$$
$$\Phi_M(A_1 A_2) = A_1 \cdot \Phi_M(A_2)$$

   for all $A_1, A_2 \in G$.

   (ii) Show that Φ_I is bijective. (**Hint**: You might find it useful to show first that if $\mathrm{tr}(AB) = 0$ for all $B \in G$ then $A = 0$.)

   (iii) Show that if A is invertible then Φ_A is bijective.

   (iv) **A tiny challenge (optional)**: Is the converse of (iii) true?