Finite Fourier Analysis Lecture Note

专业 数学与应用数学专业

学号 xxxxxxxx

姓名 WenMuke

2024 年 12 月 7 日

目录

Preliminary: group

0.1 Definition of group

Def 0.1 (Group). *A group is a set G associated with a binary operation $\circ$ such that:*

1. ***Association:*** $(a \circ b) \circ c = a \circ (b \circ c)$ *for all* $a, b, c \in G$
2. ***Identity:*** $\exists\, e \in G$ *s.t.* $e \circ a = a \circ e = a \quad \forall\, a \in G$
3. ***Inverse:*** $\forall\, a \in G \quad \exists\, b \in G$ *s.t.* $a \circ b = b \circ a = e$

   If the binary operation also satisfies:
4. ***Commutativity:*** $\forall\, a\, b \in G\, a \circ b = b \circ a$

   we call G is a abelian group / commutative group.

Example 0.2 ($(\mathbb{Z}(N)\,, +)$). *The set of N^{th} root of unity is denoted as $\mathbb{Z}(N) = \left\{e^{2k\pi i/N} | k \in \mathbb{Z}\right\}$ is called the set of all N^{th} roots of unity.*

Actually, $\mathbb{Z}(N) = \left\{1\,, e^{2\pi i/N}\,, e^{2\pi 2i/N}\,, \ldots\,, e^{2\pi i(2N-1)/N}\right\}$.

*$\mathbb{Z}(N)$ is an **abelian group** under complex multiplication.*

Example 0.3 ($(\mathbb{Z}/N\mathbb{Z}\,, \oplus)$). *Before introduce an important concept before we define this group.*

*Two integers x and y are **congruent module N** if the difference $x - y$ is divisible by N, and we write $x \equiv y \pmod N$.*

The above defines an equivalence relation on $\mathbb{Z}$. Let $R(x)$ denote the equivalence class of integer x.

$\oplus$ is defined as the additive over this equivalence class: $R(x) \oplus R(y) = R(x + y)$

With the function $f : R(k) \to e^{2\pi ik/N}$, we see that $(\mathbb{Z}(N)\,, +)$ and $(\mathbb{Z}/N\mathbb{Z}\,, \oplus)$ are actually the "same".

Def 0.4. *inner product*

1. ***Positive*** $(X, X) \geq 0$ *and* $= \Leftrightarrow X = 0$
2. ***Symmetric*** $(X, Y) = \overline{(Y, X)}$
3. ***Linear*** $(\alpha X + \beta Y, Z) = \alpha\,(X, Z) + \beta\,(Y, Z) \Rightarrow (X, \alpha Y + \beta Z) = \overline{\alpha}\,(X, Y) + \overline{\beta}\,(X, Z)$

1 Fourier analysis on $\mathbb{Z}(N)$

1.1 Fourier inversion theorem and Plancherel identity

Do the similar things on $\mathbb{Z}(N)$, find a "basis" of function defined on $\mathbb{Z}(N)$ and repeat the procedure we have done for several times. We denote the vector space V consisted of all the complex-number functions defined on $\mathbb{Z}(N)$. That's is

$$V = \{F : \mathbb{Z}(N) \to \mathbb{C}\}$$

Obviously, the dimension of V is N. So we need at most N function to span this vector space.

We define a basis similarly on the $\mathbb{Z}(N)$

$$\begin{aligned} e_l : \mathbb{Z}(N) &\to \mathbb{C} \\ k &\mapsto e^{2\pi i l k/N} \end{aligned}$$
$$\text{that is } e_l(k) = \zeta^{lk} = e^{2\pi i l k/N}$$

for $l = 0, \ldots, N-1$ and $k = 0, \ldots, N-1$ where $\zeta = e^{2\pi i/N}$ The inner product (Hermitian inner product) on V is defined as follow:

$$(F, G) = \sum_{k=0}^{N-1} F(k)\overline{G(k)} \tag{1}$$

associated norm

$$\|F\|^2 = \sum_{k=0}^{N-1} |F(k)|^2 \tag{2}$$

Lemma 1.1. *The family* $\{e_0, \ldots, e_{N-1}\}$ *is orthogonal.*

$$(e_m, e_l) = \begin{cases} N & if\, m = l, \\ 0 & if\, m \neq l. \end{cases} \tag{3}$$

proof:

$$(e_m, e_l) = \sum_{k=0}^{N-1} \zeta^{mk}\zeta^{-lk} = \sum_{k=0}^{N-1} \zeta^{(m-l)k}$$

If $m = l$, $\zeta^{(m-l)k} = 1 \Rightarrow (e_m, e_l) = N$. If $m \neq l$, the inner product is a geometric series, we have $(e_m, e_l) = \frac{1-\zeta^{(m-l)N}}{1-\zeta^{m-l}}$. Obviously, $\zeta^{(m-l)N} = \left(\zeta^N\right)^{(m-l)} = 1$ □

Orthogonal ⇒ linearly independent. So we conclude $\{e_0, \ldots, e_{N-1}\}$ **is an orthogonal basis for** V.

By lemma 1.1, the norm of each vector e_l is $\sqrt{N}$. Normalize the basis and we have

$$e_l^* = \frac{1}{\sqrt{N}} e_l$$

then$\left\{e_0^*, \ldots, e_{N-1}^*\right\}$ is an unit orthogonal basis.

Hence for any $F \in V$ we have

$$F = \sum_{n=0}^{N-1} (F, e_n^*)\, e_n^* \tag{4}$$

as well as

$$\|F\|^2 = \sum_{n=0}^{N-1} |(F, e_n^*)|^2 \tag{5}$$

So we define the n^{th} **Fourier coefficient** of F by

$$a_n = \sum_{k=0}^{N-1} F(k)\, e^{-2\pi ikn/N} \tag{6}$$

Then we have the version of Fourier inversion and the Parseval-Plancherel formulas on $\mathbb{Z}(N)$.

Theorem 1.2. *If F is a function on $\mathbb{Z}(N)$, then*

$$F(k) = \sum_{n=0}^{N-1} a_n\, e^{2\pi ink/N} \tag{7}$$

Moreover,

$$\sum_{n=0}^{N-1} |a_n|^2 = \frac{1}{N} \sum_{k=0}^{N-1} |F(k)|^2 \tag{8}$$

proof: the proof is straight forward by (4).

1.2 The fast Fourier transform(FFT)

Goal: calculating efficiently the Fourier coefficients of a function F on $\mathbb{Z}(N)$.

1.2.1 Naive approach

Fix N, and suppose we are given $F(0), \ldots, F(N-1)$ and $\omega_N = e^{-2\pi i/N}$. If we denote the k^{th} Fourier coefficient of F on $\mathbb{Z}(N)$ by $a_k^N(F)$, then by the definition of Fourier coefficients (6):

$$a_k^N(F) = \frac{1}{N} \sum_{r=0}^{N-1} F(r)\, \omega_N^{kr} \tag{9}$$

Compute $\omega_N^k \quad k = 2, 3, \ldots, N-1$. This step needs $N-2$ multiplications. Once we have $\omega_N^k \quad k = 2, 3, \ldots, N-1$, we use (9) to compute a_k^N which needs $N-1$ additions and $N+1$ multiplications. So the total calculations needed is $2N^2 + N - 2$. （书上没有-2，但是我计算的结果依然满足书上的式子，仍然不大于 $2N^2 + N$）

Calculating the Fourier coefficients in this way takes $O(N^2)$ operations.

1.2.2 Introduction to DFT matrix

The DFT matrix, denoted as F, is an $N \times N$ matrix with elements defined as:

$$F_{k,r} = \omega_N^{kr}$$

where $\omega_N = e^{-2\pi i/N}$ is the N-th root of unity, and k and r are the row and column indices, respectively, with $0 \leq k, r < N$.

According to the Fourier coefficients defined earlier in equation (9), we can derive the DFT matrix .

$$\begin{bmatrix} a_0^N(F) \\ a_1^N(F) \\ \vdots \\ a_{N-1}^N(F) \end{bmatrix} = \frac{1}{N} \begin{bmatrix} \omega_N^{0\cdot 0} & \omega_N^{0\cdot 1} & \cdots & \omega_N^{0\cdot(N-1)} \\ \omega_N^{1\cdot 0} & \omega_N^{1\cdot 1} & \cdots & \omega_N^{1\cdot(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_N^{(N-1)\cdot 0} & \omega_N^{(N-1)\cdot 1} & \cdots & \omega_N^{(N-1)\cdot(N-1)} \end{bmatrix} \begin{bmatrix} F(0) \\ F(1) \\ \vdots \\ F(N-1) \end{bmatrix}$$

Simplifying, we obtain:

$$\begin{bmatrix} a_0^N(F) \\ a_1^N(F) \\ \vdots \\ a_{N-1}^N(F) \end{bmatrix} = \frac{1}{N} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \cdots & \omega_N^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \cdots & \omega_N^{(N-1)(N-1)} \end{bmatrix} \begin{bmatrix} F(0) \\ F(1) \\ \vdots \\ F(N-1) \end{bmatrix}$$

This provides a matrix representation of the discrete Fourier transform, but we never use it in practical operations because of its computational complexity is $O(N^2)$.

1.2.3 FFT algorithm

Now we present the **fast Fourier transform(FFT)**, which improved this algorithm in the case where the partition of the circle is dyadic, that is $N = 2^n$.

Theorem 1.3. *Given $\omega_N = e^{-2\pi i/N}$ with $N = 2^n$, it is possible to calculate the Fourier coefficients of a function on $\mathbb{Z}(N)$ with at most*

$$4 \cdot 2^n n = 4N \log_2 N = O(N \ln N) \tag{10}$$

operations.

We are going to prove the theorem 1.3 through the following lemma, which gives the key procedure of the fast Fourier transform**(FFT)** algorithm.

Lemma 1.4. *If we are given $\omega_{2M} = e^{-2\pi i/2M}$, then*

$$\#(2M) \leq 2\#(M) + 8M \tag{11}$$

Where $\#(M)$ denotes the minimum number of operations needed to calculate all the Fourier coefficients of any function on $\mathbb{Z}(M)$.

proof of lemma:

Main idea: for any given function F on $\mathbb{Z}(2M)$, we consider two functions F_0 and F_1 on $\mathbb{Z}(2M)$ defined by

$$F_0(n) = F(2n) \quad \text{and} \quad F_1(n) = F(2n+1)$$

Then we use the Fourier coefficients corresponding to the groups $\mathbb{Z}(M)$ to construct the Fourier coefficients corresponding to the groups $\mathbb{Z}(2M)$.

Step 1 Calculation of $\omega_{2M}, \ldots, \omega_{2M}^{2M}$

This step requires no more than $2M$ operations.

Step 2 Calculation of Fourier coefficients of F_0 and F_1

Calculation of Fourier coefficients of F_0 and F_1 needs no more than $\#(M)$ operations.

This step requires no more than $2\#(M)$ operations.

Step 3 Calculation of Fourier coefficients of F

We denote the Fourier coefficients corresponding to the groups $\mathbb{Z}(M)$ and $\mathbb{Z}(2M)$ by a_k^{2M} and a_k^M, respectively, thereby:

$$a_k^{2M}(F) = \frac{1}{2}\left(a_k^M(F_0) + a_k^M(F_1)\,\omega_{2M}^k\right) \tag{12}$$

To prove (12), we start by the definition of Fourier coefficients.

$$\begin{aligned} a_k^{2M}(F) &= \frac{1}{2M}\sum_{r=0}^{2M-1} F(r)\,\omega_{2M}^{kr} \\ &= \frac{1}{2}\left(\frac{1}{M}\sum_{l=0}^{M-1} F(2l)\,\omega_{2M}^{k(2l)} + \frac{1}{M}\sum_{m=0}^{M-1} F(2m+1)\,\omega_{2M}^{k(2m+1)}\right) \\ &= \frac{1}{2}\left(\frac{1}{M}\sum_{l=0}^{M-1} F_0(l)\,\omega_M^{kl} + \frac{1}{M}\sum_{m=0}^{M-1} F_1(m)\,\omega_M^{km}\omega_{2M}^{k}\right) \\ &= \frac{1}{2}\left(a_k^M(F_0) + a_k^M(F_1)\,\omega_{2M}^k\right) \end{aligned}$$

Using (12), there are two multiplications and a additions when calculating single a_k^{2M}.

The total operations required in this step is $3 \times 2M$

Through 3 steps above, we have the total operation required in this algorithm.

$$\#(2M) \le 2M + 2\#(M) + 3 \times 2M = 2\#(M) + 8M \quad \square$$

Now we go back to the theorem 1.3, considering the lemma 1.4, it is nature to using the induction to prove the theorem.

- when $n = 1$, there are two coefficients to calculate.

$$a_0^N(F) = \frac{1}{2}(F(0) + F(1)) \quad \text{and} \quad a_1^N(F) = \frac{1}{2}(F(0) + (-1)F(1))$$

  So $\#(2) \leq 5 < 4 \times 2 \times 1 = 8$(equation (10)).

- we suppose the theorem holds when $n = k - 1$, that is $\#\left(2^{k-1}\right) \leq 4 \cdot 2^{k-1}(k-1)$.

- we now consider $n = k$. Use lemma 1.4 and we have $\#\left(2^k\right) \leq 2\#\left(2^{k-1}\right) + 8 \times 2^{k-1} = 2 \times 4 \cdot 2^{k-1}(k-1) + 8 \times 2^{k-1} = 4 \cdot 2^k k$.

- That is $\#(N) \leq 4N \log_2 N$.

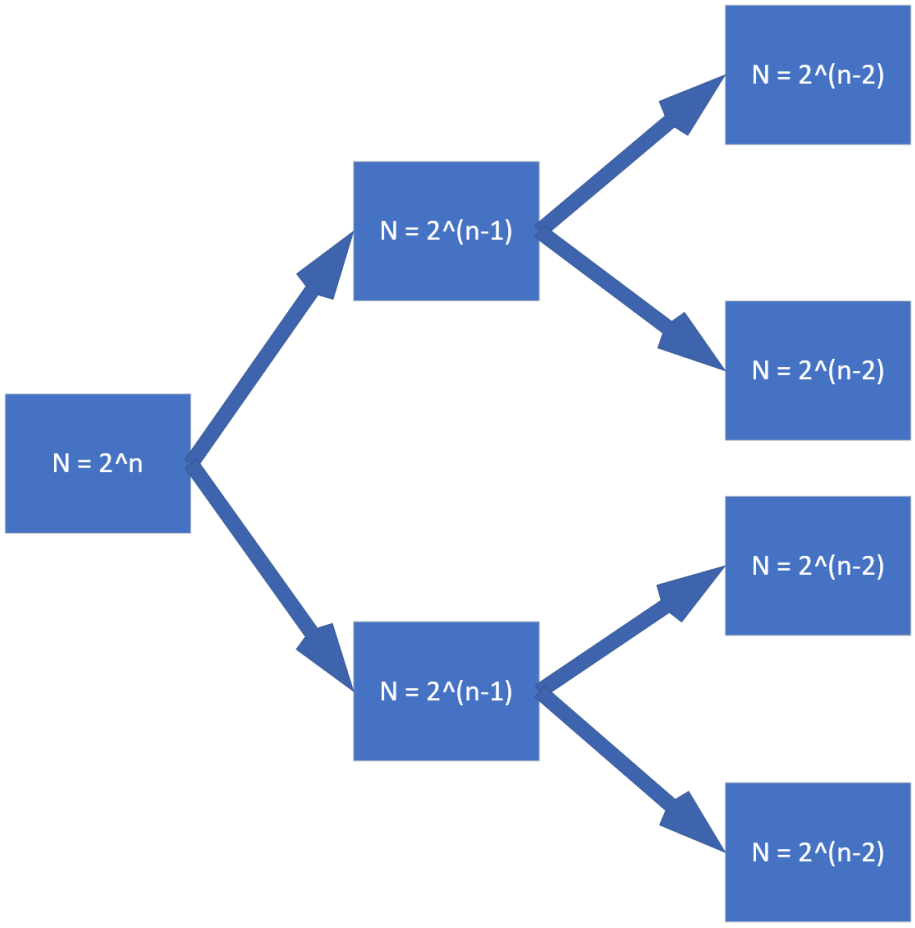

图 1: FFT process

1.3 More than $N = 2^n$

One can compute the Fourier coefficients of a function on $\mathbb{Z}(N)$ when $N = 3^n$ with at most $6N \log_3 N$ operations.

To show that one can compute the Fourier coefficients of a function on $\mathbb{Z}(N)$ when $N = 3^n$ with at most $6N \log_3 N$ operations, we can follow a reasoning similar to the FFT algorithm for $N = 2^n$, but adjusted for base 3.

1. **Base 3 FFT Algorithm:**

- Split the input sequence into three subsequences: F_0, F_1, F_2, where F_j contains elements of the original sequence with indices $3m + j$.

- Recursively apply the FFT to each subsequence, each of size $\frac{N}{3}$.

- Use the combination of the three FFTs to construct the FFT of the original sequence.

$$a_k^{3N}(F) = \frac{1}{3}\left(a_k^N(F_0) + a_k^N(F_1)\,\omega_{3N}^k + a_k^N(F_2)\,\omega_{3N}^{2k}\right) \tag{13}$$

2. **Computational Complexity:**

- Each recursive step requires $\frac{N}{3}$ FFT computations, along with some additional multiplications and additions to combine the results.

- The total number of operations for the FFT can be expressed as:

$$\#(3N) \leq 3\#(N) + 5 \times 3N + 3N = 3\#(N) + 18N \tag{14}$$

3. **Induction:**

- When $n = 1$, compute three Fourier coefficients needs 13 operations, which is less than $18 = 6 \times 1 \times 3^1$

- When $n = k - 1$, we assume the statement holds.

- When $n = k$, using equation (14) we have our conclusion.

$$\begin{aligned}
&\#\left(3^k\right) \leq 6 \cdot 3^k \cdot (k-1) + 18 \cdot 3^{k-1} = 6 \cdot 3^k \cdot k \\
&\#(N) \leq 6N \log_3 N
\end{aligned}$$

4. **Generalize:**

More general, one can compute the Fourier coefficients of a function on $\mathbb{Z}(N)$ when $N = a^n$ with at most $2aN \log_a N$ operations.

Claims:

$$\#(aN) \leq a\#(N) + (2a-1) \times aN + aN = a\#(N) + 2a^2N \tag{15}$$

By induction:

$$\begin{aligned}
&\#\left(a^k\right) \leq 2a \cdot a^k \cdot (k-1) + 2a^2 \cdot a^{k-1} = 2a \cdot a^k \cdot k \\
&\#(N) \leq 2aN \log_a N
\end{aligned}$$

2 Fourier analysis on finite abelian groups

2.1 Abelian groups

First, we give some further introduction about group.

A **homomorphism** between two abelian groups G and H is a map $f : G \to H$ which satisfies the property

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

where the dot on the LHS is the operation in G, and the dot on the RHS the operation in H.

We say the two group G and H are **isomorphic**, and write $G \approx H$, if there is a bijective homomorphism from G to H.

Example 2.1. $\mathbb{Z}(N) \approx \mathbb{Z}/N\mathbb{Z}$

Example 2.2. $\{R, +\} \approx \{R^+, \times\}$

We forces on the finite groups. In this case, we denote by $|G|$ the number of elements in G, and call $|G|$ the **order** of the group.

If G_1 and G_2 are two finite abelian groups, their **direct product** $G_1 \times G_2$ is a group if the operation in $G_1 \times G_2$ is defined by:

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2')$$

Theorem 2.3. *Every finite abelian group G is isomorphic to a direct product of cyclic groups. (Problem 2)*

Furthermore, a finite abelian group is direct product of cyclic subgroups of prime-power orders, and the order is unique.

The group $\mathbb{Z}^*(q)$

Notice that $m \equiv m' \pmod{q}$ and $n \equiv n' \pmod{q}$ then $m \times n \equiv m' \times n' \pmod{q}$. With this observation, it is natural to define the multiplication on $\mathbb{Z}(q)$. An integer $n \in \mathbb{Z}(q)$ is a **unit** if there exists an integer $m \in \mathbb{Z}(q)$ so that $nm \equiv 1 \pmod{q}$.

Obviously, $(\mathbb{Z}(q), \times)$ is not a group, since 0 has no inverse in $(\mathbb{Z}(q), \times)$. If we want to define a multiplication group on $\mathbb{Z}(q)$, we need to delete some elements. The set of all units in $\mathbb{Z}(q)$ is denoted by $\mathbb{Z}^*(q)$, and it is clear from our definition that $\mathbb{Z}^*(q)$ is an abelian group under *multiplication* modulo q.

Example 2.4. $q = 4$

$Z^*(4) = \{1, 3\} \approx Z(2)$

Example 2.5. $q = 5$

$Z^*(5) = \{1, 2, 3, 4\} \approx Z(4)$

Example 2.6. $q = 8$

$Z^*(8) = \{1, 3, 5, 7\} \approx Z(2) \times Z(2)$

2.2 Characters

Let G be a finite abelian group (with the multiplicative notation) and S^1 the unit circle in the complex plane. A **character** on G is a complex-valued function $e : G \to S^1$ which satisfies the following condition:

$$e(a \cdot b) = e(a) \cdot e(b) \quad \forall a, b \in G. \tag{16}$$

In other words, a character is a homomorphism from G to the circle group. The **trivial** or **unit character** is defined by $e(a) = 1 \, \forall \, a \in G$

Example 2.7. *Exponential functions on the circle and the law*

$$e_l(k + m) = e_l(k) + e_l(m) \quad \textit{where } e_l(k) = \zeta^{lk} = e^{2\pi i l k/N}$$

which held for the exponentials $e_0, \cdots, e_{N-1}$ *used in the Fourier theory on* $\mathbb{Z}(N)$*. So the exponential functions are the characters of the group* $\mathbb{Z}(N)$*.*

Lemma 2.8. *The set* $\widehat{G}$ *is an abelian group under mulitiplication defined by*

$$(e_1 \cdot e_2)(a) = e_1(a) e_2(a) \quad \forall \, a \in G$$

We call $\widehat{G}$ *the* ***dual group*** *of* G*.*

Lemma 2.9. *Let* G *be a finite abelian group, and* $e : G \to \mathbb{C} - \{0\}$ *a multiplicative function, namely* $e(a \cdot b) = e(a) \cdot e(b) \quad \forall a, b \in G$*. Then* e *is a character.*

proof of lemma 2.9

Notice that we only need to check the range of e is the subset of S^1. G is finite group, so the range is finite. That is $e(a)$ is bounded above and below.

$$\exists M_1, M_2 \in \mathbb{R}^+ \Rightarrow 0 < M_2 < |e(a)| < M_1$$

For any element $a \in G$, $|e(a^n)| = |e(a)|^n$ is bounded for all $n \in \mathbb{N}^*$, so we conclude that $|e(a)| = 1$ for all $a \in G$. □

2.3 The orthogonality relations

Let V denote the vector space of complex-valued functions defined on the finite abelian group G. Note that the dimension of V is $|G|$, the order of G. We define a **Hermitian inner product** on V by

$$(f,g) = \frac{1}{|G|}\sum_{a\in G} f(a)\,\overline{g(a)}, \quad \text{whenever } f,g \in V \tag{17}$$

It is easy to check the (17) is a inner product. (Hermitian symmetric, linear, positive-definite)

Theorem 2.10. *The characters of G form an orthonormal family with respect to the inner product defined in (17).*

proof of the theorem 2.10

Since $|e(a)| = 1$ for any character, we find that

$$(e,e) = \frac{1}{|G|}\sum_{a\in G} e(a)\,\overline{e(a)} = \frac{1}{|G|}\sum_{a\in G} |e(a)|^2 = 1$$

If $e \neq e'$ and both are characters, we must prove the $(e,e') = 0$. We write this in the following lemma.

Lemma 2.11. *If e is a non-trivial character of the group G, then $\sum_{a\in G} e(a) = 0$.*

proof of the lemma 2.11

Choose $b \in G$ such that $e(b) \neq 1$. Then we have

$$e(b)\sum_{a\in G} e(a) = \sum_{a\in G} e(b)\,e(a) = \sum_{a\in G} e(ab) = \sum_{a\in G} e(a)$$

The last equality because an simple observation: if $ab = cb$, we multiply both sides by b^{-1} which gives us $a = c$. So as a ranges over the group, ab ranges over G as well. Since $e(b) \neq 1$, our claim is true.

(continue) proof of the theorem 2.10

Suppose e' is a character distinct from e. $\exists a \in G$ s.t. $ee'^{-1}(a) \neq 1$. So the character ee'^{-1} is non-trivial. The lemma implies that

$$(e,e') = \sum_{a\in G} e(a)\,\overline{e'(a)} = \sum_{a\in G} \left(ee'^{-1}\right)(a) = 0$$

Since $e'^{-1}(a) = \overline{e'(a)}$, we can conclude that the inner product defined by (17) of e and e' equals to 0 which says they are orthonormal.

As a consequence of the theorem, we see that distinct characters are linearly independent.

2.4 Characters as a total family

Since the dimension of $V = \{f : G \to \mathbb{C}\}$ over $\mathbb{C}$ is $|G|$, we conclude that the order of $\widehat{G}$ is finite and $\leq |G|$. The main result to which we now turn is that, in fact, $|\widehat{G}| = |G|$.

Theorem 2.12. *The characters of a finite abelian group G form a basis for the vector space of functions on G.*

An easy approach is using the decomposition of the abelian group. Using the structure theorem for finite abelian groups we have mentioned earlier, which states that any such group is the direct product of cyclic groups, that is, such groups is the direct product of cyclic groups ($\mathbb{Z}(N)$). And cyclic groups are **self-dual**, using this fact we would conclude that $|\widehat{G}| = |G|$.

2.5 Fourier inversion and Plancherel formula

Given a function f on G and character e of G, we define the **Fourier coefficient** of f with respect to e, by

$$\widehat{f}(e) = (f, e) = \frac{1}{|G|} \sum_{a \in G} f(a) \overline{e(a)} \tag{18}$$

and the **Fourier series** of f as

$$f = \sum_{e \in \widehat{G}} \widehat{f}(e)\, e \tag{19}$$

We use a theorem to summarize our results.

Theorem 2.13. *Let G be a finite abelian group. The characters of G form an orthonormal basis for the vector space V of functions on G equipped with the inner product*

$$(f, g) = \frac{1}{|G|} \sum_{a \in G} f(a) \overline{g(a)} \tag{20}$$

*In particular, **any** function f on G is equal to its Fourier series*

$$f = \sum_{e \in \widehat{G}} \widehat{f}(e)\, e \tag{21}$$

.

Finally, we have the Parseval-Plancherel formula for finite abelian groups.

Theorem 2.14. *If f is a function on G, then $\|f\|^2 = \sum_{e \in \widehat{G}} \left|\widehat{f}(e)\right|^2$*

proof of theorem 2.14

Since the characters of G form an orthonormal basis for the vector space V, and $(f, e) = \widehat{f}(e)$, we have that

$$\|f\|^2 = (f, f) = \sum_{e \in \widehat{G}} \left|\widehat{f}(e)\right|^2. \quad \square$$

The second equation is because (19)