DIRICHLET'S THEOREM

ANG LI

Abstract. Abstract here.

Contents

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

1.1. The group $\mathbb{Z}(N)$.

Definition 1.1. A complex number z is an N^{th} **root of unity** if $z^N = 1$. We denote the set of all N^{th} roots of unity by $\mathbb{Z}(N)$

Definition 1.2. Two integers x and y are **congruent modulo** N if the difference $x - y$ is divisible by N, and we write $x \equiv y \mod N$.

- $x \equiv x \mod N$ for all integers x
- If $x \equiv y \mod N$, then $y \equiv x \mod N$
- If $x \equiv y \mod N$, and $y \equiv z \mod N$, then $x \equiv z \mod N$

Thus the relation $\equiv$ on $\mathbb{Z}$ is an equivalence relation. Let $R(x)$ denote the equivalence class, or residue class, of integer x. There are N equivalence classes and each class has a unique representative between 0 and $N - 1$

Definition 1.3. The group of integers modulo N, sometimes denoted by $\mathbb{Z}/N\mathbb{Z}$, is $\{0, 1, 2.....N - 1\}$.

1.2. **Fourier inversion theorem and Plancherel identity on $\mathbb{Z}(N)$.** Let $e_n(x) = e^{2\pi inx}$

$e_n(x+y) = e_n(x) + e_n(y)$
On $\mathbb{Z}(N)$, the appropriate analogues are the N functions $e_0,...,e_{N-1}$ defined by

$$e_l(k) = \zeta^{lk} = e^{2\pi lk/N} \text{ for } l = 0,...,N-1 \text{ and } k = 0,...N-1,$$

where $\zeta = e^{2\pi ilk/N}$

Definition 1.4. The **Hermitian inner product** over a vector space is defined by

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

and associated norm

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

Lemma 1.5. *The family $\{e_0, ...e_{N-1}\}$ is orthogonal. In fact,*

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

Proof. We have

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

If $m = l$, $\zeta^{(m-l)k} = 1$ for each k, and $(e_m, e_l) = N$. If $m \neq n$ then $q = \zeta^{m-l}$ is not equal to 1, and

$$1 + q + q^2 + ... + q^{N-1} = \tfrac{1-q^N}{1-q} = 0$$

because $q^N = \zeta^{(m-l)N = e^{2(m-l)\pi}} = 1$ $\square$

Definition 1.6. The n^{th} **Fourier coefficient** of F by

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

Theorem 1.7. If F is a function on $\mathbb{Z}(N)$, then

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

Moreover,

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

Proof. We define $e_l^* = \frac{1}{\sqrt{N}}e_l$. Since the vector space V of all complex-valued functions on $\mathbb{Z}(N)$ is N-dimensional, and from the lemma $\{e_0, ...e_{N-1}\}$ is orthogonal, $\{e_0^*, ..., e_{N-1}^*\}$ is an orthonormal basis for V. Hence for any $F \in V$ we have

$$F = \textstyle\sum_{n=0}^{N-1}(F, e_n^*)e_n^* \quad \text{and} \quad \|F\| = \sum_{n=0}^{N-1} |(F, e_n^*)|^2$$

We also have

$$(F, e_n^*) = \sqrt{N} \sum_{k=0}^{N-1} F(k) e^{-2\pi i n k/N} = \sqrt{N} a_n$$

Then

$$F(k) = \sum_{n=0}^{N-1} \sqrt{N} a_n e_n^*(k) = \sum_{n=0}^{N-1} a_n e^{2\pi i n k/N}$$

Moreover,

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

□

2. Fourier analysis on finite abelian groups

2.1. **Abelian groups.**

Definition 2.1. An **abelian group** (or commutative group) is a set Gn together with a binary operation on pairs of elements of G, $(a, b) \longmapsto a \cdot b$, that satsfies the following conditions

(1) *Associativity* : $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad$ for all $a, b, c \in G$.
(2) *Identity* : There exists an element $u \in G$(often written as either 1 or 0) such that $a \cdot u = u \cdot a = a \quad$ for all $a \in G$.
(3) *Inverses* : For every $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = u$.
(4) *Commutativity* : For $a, b \in G$, we have $a \cdot b = b \cdot a$.

Definition 2.2. 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 left-hand side is the operation in G, and the dot on the right-hand side the operation in H.

Definition 2.3. Two groups G and H are **isomorphic**, and write $G \approx H$, if there is a bijective homomorphism from G to H.

Definition 2.4. In finite abelian group G, the **order** of G is the number of elements in G, denoted by $|G|$.

Definition 2.5. If G_1 and G_2 are two finite abelian groups, their **direct product** $G_1 \times G_2$ is the group whose elements are pairs (g_1, g_2) with $g_1 \in G_1$ and $g_2 \in G_2$. The operation in $G_1 \times G_2$ is them defined by

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

Clearly, if G_1 and G_2 are two finite abelian groups, then so is $G_1 \times G_2$

Definition 2.6. An integer $n \in \mathbb{Z}(q)$ is a **unit** if there exists an integer $m \in \mathbb{Z}(q)$ so that

$$nm \equiv 1 \mod q.$$

The set of all units in $\mathbb{Z}(q)$ is denoted by $\mathbb{Z}^*(q)$.

2.2. **Characters.**

Definition 2.7. Let G be a finite abelian group 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:

$$e(a \cdot b) = e(a) \cdot e(b) \qquad \text{fro all } a, b \in G$$

The **trivial** or **unit character** is defined by $e(a) = 1$ for all $a \in G$

If G is a finite abelian group, we denote by $\hat{G}$ the set of all characters of G.

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

$$(e_1 \cdot e_2)(a) = e_1(a) \cdot e_2(a) \quad \textit{for all } a \in G.$$

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

Proof. The group G is finite, then $|e(a)|$ is bounded above and below as as a ranges over G. Since $|e(b^n)| = |e(b)|^n$, $|e(b)| = 1$ for all $b \in G$ □

2.3. **The orthogonality relations.**

Lemma 2.10. *If e is a non-trivial character of the group G, then $\sum_{a \in G} e(a) = 0$.*

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

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

Therefore $\sum_{a \in G} e(a) = 0$. □

Theorem 2.11. *The characters of G form an orthonormal family with respect to the Hermitian inner product.*

Proof. Since $|e(a)| = 1$ for any character, we have

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

If $e \neq e'$ and both e and e' are characters, we must prove that $(e, e') = 0$. $e \neq e'$ implies that $e(e')^{-1}$ is non-trivial. The lemma shows that

$$\sum_{a\in G} e(a)(e'(a))^{-1} = 0.$$

Since $(e'(a))^{-1} = \overline{e'(a)}$, the theorem is proved. □

2.4. **Characters as a total family.**

Definition 2.12. A linear transformation $T : V \to V$ is **unitary** if it preserves the inner product, $(Tv, Tw) = (v, w)$ for all $v, w \in V$

Theorem 2.13. *(spectral theorem)*
Any unitary transformation on a finite-dimensional space is diagonalizable. In other words, there exists a basis $\{v_1, ..., v_d\}$(eigenvectors) of V such that $T(v_i) = \lambda_i v_i$, where $\lambda_i \in \mathbb{C}$ is the eigenvalue attached to v_i.

Lemma 2.14. *Suppose $\{T_1, ..., T_k\}$ is a commuting family of unitary transformations on the finite-dimensional inner product space V; that is,*

$$T_iT_j = T_jT_i \quad \textit{for all } i, j.$$

Then $T_1, ..., T_k$ are simultaneously diagonalizable. In other words, there exists a basis for V which consists of eigenvectors for every T_i.

Theorem 2.15. *The characters of a finite abelian group G form a basis for the vector space of functions on G.*

2.5. **Fourier inversion and Plancherel formula.**

Definition 2.16. Given a finite abelian group G and a function f on G, define the **Fourier coefficient** of f with respect to character e of G, by

$$\hat{f}(e) = (f, e) = \tfrac{1}{|G|}\sum_{a\in G} f(a)\overline{e(a)},$$

and the **Fourier series** of f as

$$f \sim \sum_{e\in\hat{G}} \hat{f}(e)e$$

Theorem 2.17. *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 Hermitian inner product.In particular, any function f on G is equal to its Fourier series*

$$f = \sum_{e\in G} \hat{f}(e)e.$$

Proof. Since the characters of the finite abelian group G forms an orhtonormal basis for the vector space V of functions on G, then

$$f = \sum_{e\in\hat{G}} c_e e$$

for some set of constants c_e. Also, by because the orthogonality, we have

$$(f, e) = c_e = \hat{f}(e).$$

Therefore, $f = \sum_{e \in \hat{G}} \hat{f}(e)e$. □

Theorem 2.18. *(the Parseval-Plancherel formula) If f is a function on G, then $\|f\|^2 = \sum_{e \in \hat{G}} |\hat{f}()e|^2$.*

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

$$\|f\|^2 = (f, f) = \sum_{e \in \hat{G}} (f, e)\overline{\hat{f}()e} = \sum_{e \in \hat{G}} |\hat{f}(e)|^2$$

□

3. Elementary number theory

3.1. The fundamental theorem of arithmetic.

Theorem 3.1. *(Euclid's algorithm) For any integers a and b with $b > 0$, there exists unique integers q and r with $0 \leq r < b$ such that*

$$a = qb + r.$$

Definition 3.2. An integer a **divides** b if there exists another integer c such that $ac = b$; we then write $a|b$ and say that a is a **divisor** of b. A **prime number** is a positive integer greater than 1 that has no positive divisors besides 1 and itself.

Definition 3.3. The **greatest common divisor** of two positive integers a and b is the largest integer that divides both a and b. Two positive integers are **relatively prime** if their greatest common divisor is 1.

Theorem 3.4. *If $gcd(a, b) = d$, then there exist integers x and y such that*

$$ax + by = d$$

Proof. Consider the set S of all positive integers of the form $ax+by$ where $x, y \in \mathbb{Z}$, and let s be the smallest element in S. Claim that $s = d$. There exists integers x and y such that

$$ax + by = s$$

Clearly, any divisor of a and b divides s, so we have $d \leq s$. BY Euclid's algorithm, we can write $a = qr + r$ with $0 \leq r < s$. By $ax + by = s$, we have $qax + qby = qs = a - r$. Hence, $r = a(1 - qx) + b(-qy)$. Since s is the minimal in S, we have $r = 0$. Therefore, $s|a$ and similarly $s|b$. Then $s = d$. □