Fourier Analysis, Stein and Shakarchi
Chapter 7 Finite Fourier Analysis

Yung-Hsiang Huang*

2018.06.14

Abstract

I finish this solution file when I am a teaching assistant of the course "Analysis II" in NTU 2018 Spring. Some exercises are discussed with Jing-Wen Chen and Wei-Ning Deng.

The following students contribute the Problem section:

Problem 2,3: Chin-Bin Hsu, Zi-Li Lim.

Exercises

1. Let f be a function on the circle. For each $N \geq 1$ the discrete Fourier coefficients of f are defined by

$$a_N(n) = \frac{1}{N}\sum_{k=1}^{N} f(e^{2\pi ik/N})e^{-2\pi ikn/N}, \text{ for } n \in \mathbb{Z}.$$

We also let

$$a(n) = \int_0^1 f(e^{2\pi ix})e^{-2\pi inx}\,dx$$

denote the ordinary Fourier coefficients of f.

Then it's easy to show that $a_N(n) = a_N(n+N)$. Furthermore, if f is continuous, then one can deduce $a_N(n) \to a(n)$ as $N \to \infty$ from the Riemann sum approximation. Does $a_N \to a$ uniformly in n? (Note that this is true if $f \in C^1$ by the next exercise.)

2. **If f is a C^1 function on the circle, prove that $|a_N(n)| \leq c/|n|$ whenever $0 < |n| \leq N/2$.**

*Department of Math., National Taiwan University. Email: d04221001@ntu.edu.tw

Proof. The hint is easy to prove. So $|a_N(n)||1-e^{2\pi iln/N}| \le M_f|1-e^{2\pi il/N}|$ where M_f is the Lipschitz constant of f. Choose the integer l such that $|l-\frac{N}{2n}| \le \frac{1}{2}$. Then $|\frac{ln}{N}-\frac{1}{2}| \le \frac{|n|}{2N} \le \frac{1}{4}$ and so $\frac{1}{4} \le \frac{ln}{N} \le \frac{3}{4}$. Therefore,

$$|a_N(n)| \le \frac{M_f|1-e^{2\pi il/N}|}{|1-e^{2\pi iln/N}|} \le CM_f\frac{l}{N} \le CM_f(\frac{1}{2|n|}+\frac{1}{2N}) \le CM_f\frac{1}{|n|}.$$

$\square$

3. **By a similar method, show that if f is a C^2 function on the circle, then $|a_N(n)| \le c/|n|^2$, whenever $0<|n|\le N/2$. As a result, prove the inversion formula for $f \in C^2$,**

$$f(e^{2\pi ix}) = \sum_{n=-\infty}^{\infty} a(n)e^{2\pi inx}$$

from its finite version.

Proof. Use the hint for Exercise 2 twice (for $\pm l$), we have

$$|a_N||2-e^{2\pi iln/N}-e^{-2\pi iln/N}| \le M_f|e^{2\pi il/N}-1|^2.$$

The quadratic decay rate can be proved similarly as Exercise 2 with a constant independent of N. Note that $a(n)$ also decays quadratically.

For the second part, let N be odd, one write the inversion formula as

$$\sum_{|n|<\frac{N}{2}} a_N(n)e^{2\pi ikn/N} = \frac{1}{N}\sum_{j=0}^{N-1} f(e^{2\pi ij/N})\sum_{|n|<\frac{N}{2}} e^{-2\pi ijn/N}e^{2\pi ikn/N} = f(e^{2\pi ik/N})$$

Given $\epsilon>0$, let $\delta>0$ be the uniform modulus of f associated with ϵ. Let $N_0(\epsilon)>\delta^{-1}$. Then for each $J>N_0(\epsilon)$ and $x\in[0,1]$, one can pick $k(x,J)\in\mathbb{Z}$ such that $|x-\frac{k(x,J)}{J}|<\frac{1}{J}<\frac{1}{N_0(\epsilon)}<\delta$. Note that

$$\begin{aligned}|f(e^{2\pi ix})-\sum_{|n|\le J/2} a(n)e^{2\pi inx}| \le |f(e^{2\pi ix})-f(e^{2\pi i\frac{k(x,J)}{J}})|+|f(e^{2\pi i\frac{k(x,J)}{J}})-\sum_{|n|\le J/2} a_J(n)e^{2\pi in\frac{k(x,J)}{J}}|\\ +|\sum_{|n|\le J/2}[a_J(n)-a(n)]e^{2\pi in\frac{k(x,J)}{J}}|+|\sum_{|n|\le J/2} a(n)[e^{2\pi in\frac{k(x,J)}{J}}-e^{2\pi inx}]|\end{aligned} \tag{1}$$

Note that the first term $<\epsilon$ by uniform continuity of f. The last term is less than a generic multiple of $\sum_{|n|\le J/2}\frac{1}{n^2}\frac{n}{J}=\frac{\log J}{J}$ and then turns to be less than ϵ if $J>N_1(\epsilon)$ for some $N_1(\epsilon)>0$. For the third term, one use the quadratic decay as follows: there is $N_2(\epsilon)$ such that $\sum_{|n|>N_2(\epsilon)}\frac{1}{n^2}<\epsilon$. So for $J>2N_2(\epsilon)$, we decompose this sum into two parts, $|n|<N_2(\epsilon)$ and $J/2\ge|n|>N_2(\epsilon)$.

For the second part, it's bounded by a multiple of $\sum_{|n|>N_2(\epsilon)} \frac{1}{n^2} < \epsilon$. For the first part, we use Exercise 1 to conclude that this part is less than a multiple of $2N_2(\epsilon) \cdot \frac{\epsilon}{N_2(\epsilon)}$ whenever $J > N_3(\epsilon)$ for some $N_3(\epsilon) \in \mathbb{N}$.

If J is odd, then the second term vanishes. If J is even, then we modify (1) as follows:

$$\begin{aligned}
&|f(e^{2\pi ix}) - \sum_{|n|\le \frac{J}{2}} a(n)e^{2\pi inx}| = |f(e^{2\pi ix}) - \sum_{|n|\le \frac{J+1}{2}} a(n)e^{2\pi inx}| \\
&\le |f(e^{2\pi ix}) - f(e^{2\pi i\frac{k(x,J+1))}{J+1}})| + |f(e^{2\pi i\frac{k(x,J+1)}{J+1}}) - \sum_{|n|\le \frac{J+1}{2}} a_{J+1}(n)e^{2\pi in\frac{k(x,J+1)}{J+1}}| \\
&+ |\sum_{|n|\le \frac{J+1}{2}} [a_{J+1}(n) - a(n)]e^{2\pi in\frac{k(x,J+1)}{J+1}}| + |\sum_{|n|\le \frac{J+1}{2}} a(n)[e^{2\pi in\frac{k(x,J+1)}{J+1}} - e^{2\pi inx}]|.
\end{aligned}$$

Consequently, one see that if $J > N(\epsilon) := \max\{N_0(\epsilon), N_1(\epsilon), N_2(\epsilon), N_3(\epsilon)\}$, then

$\sup_x |f(e^{2\pi ix}) - \sum_{|n|\le \frac{J}{2}} a(n)e^{2\pi inx}|$ is less than a generic multiple of ϵ. □

4. **Let e be a character on $G = \mathbb{Z}(N)$, the additive group of integers modulo N. Show that there exists a unique $0 \le l \le N-1$ so that $e(k) = e_l(k) = e^{2\pi ilk/N}$ for all $k \in \mathbb{Z}(N)$. Conversely, every function of this type is a character on $\mathbb{Z}(N)$. Deduce that $e^l \mapsto l$ defines an isomorphism from $\widehat{G}$ to G.**

Proof. By definition, $e(1) = e^{2\pi i\tilde{l}}$ for some $\tilde{l} \in [0,1)$. Let $l = N\tilde{l} \in [0,N)$. By multiplicative property of e. One has $1 = e(N) = e(1)^N = e^{2\pi iN\tilde{l}}$. So $N\tilde{l} \in \mathbb{Z}$ and hence $0 \le l \le N-1$. The uniqueness and converse part are easy to prove. This implies the map $\phi : e^l \mapsto l$ is bijective. It's also trivial that ϕ is a homomorphism. □

5. **Show that all characters on $S^1 = [0,1]$ are given by**

$$e_n(x) = e^{2\pi inx} \quad \textbf{with} \quad n \in \mathbb{Z},$$

and check that $e_n \mapsto n$ defines an isomorphism from $\widehat{S^1}$ to $\mathbb{Z}$.

Proof. Given $e \in \widehat{S^1}$. We verify e is differentiable at first. The multiplicative property of e implies e is continuous. The continuity of e and the fact $e(0) = 1$ imply $c := \int_0^\delta e(y)\,dy \ne 0$ for some small $\delta > 0$. So $ce(x) = \int_x^{x+\delta} e(y)\,dy$, which implies e is differentiable.

Then $e(x+h) = e(x)e(h)$ for all $x \in [0,1)$ and $h \in [0,1-x)$, then $\frac{e(x+h)-e(x)}{h} = \frac{e(h)-e(0)}{h}e(x) \to \dot{e}(0)e(x)$ as $h \to 0^+$ for all $x \in (0,1)$. On the other hand, $\frac{e(x-h)-e(x)}{-h} = \frac{e(0)-e(h)}{-h}e(x-h) \to \dot{e}(0)e(x)$ as $h \to 0^+$ for all $x \in (0,1)$. So e satisfies $\dot{e}(x) = e(x)\dot{e}(0)$. So $e(x) = e^{x\dot{e}(0)}$. In particular $1 = e(0) = e(1) = e^{\dot{e}(0)}$ implies that $\dot{e}(0) = 2\pi in$ for some n. □

Remark 1. This technique is standard in the theory of semigroups. See [2, Chapter 1] for some settings in Banach spaces. (There is some difficulty for $x-h$ part to be overcame by uniform boundedness principle). $\dot{e}(0)$ is called the infinitesimal generator.

6. **Prove that all characters on $\mathbb{R}$ take the form**

$$e_\xi(x) = e^{2\pi i \xi x} \quad \textbf{with} \quad \xi \in \mathbb{R},$$

and that $e_\xi \mapsto \xi$ defines an isomorphism from $\widehat{\mathbb{R}}$ to $\mathbb{R}$. The argument in Exercise 5 applies here as well.

Proof. Same argument as the previous argument implies $e(x) = e^{(a+ib)x}$ for some $a, b \in \mathbb{R}$. Note that the boundary conditions $|e(x)| \equiv 1$ on $x = \pm\infty$ imply $a = 0$. □

7. **Let $\zeta = e^{2\pi i/N}$. Define the $N \times N$ matrix $M = (a_{jk})_{1 \le j,k \le N}$ by $a_{jk} = N^{-1/2}\zeta^{jk}$.**

(a) Show that M is unitary. (b) Interpret the identity $(Mu, Mv) = (u, v)$ and the fact that $M^* = M^{-1}$ in terms of Fourier series on $\mathbb{Z}(N)$.

Proof. (a) One notes that $(M^*M)_{ij} = \sum_{k=1}^N (M^*)_{ik} M_{kj} = N^{-1} \sum_{k=1}^N \zeta^{-ki}\zeta^{kj} = \delta_{ij}$, the Kronecker delta. Argument for showing $(MM^*)_{ij} = \delta_{ij}$ is almost the same .

(b) Given $u, v \in \mathbb{C}^N$, we define the function U on $\mathbb{Z}(N)$ by $U(j) = u_j$, the j-th component of u. By Parseval's identity,

$$(Mu, Mv) = \sum_{j=1}^N \widehat{U}(-j)\widehat{\overline{V}}(j) = \sum_{j=1}^N \overline{\widehat{\overline{U}}(j)}\widehat{\overline{V}}(j) = \sum_{j=1}^N \overline{\overline{U(j)}}\overline{V}(j) = (u, v).$$

Similarly, by Fourier inversion formula on $\mathbb{Z}(N)$, $U(n) = \sum_j \widehat{U}(j)\zeta^{jn} = N^{\frac{1}{2}}(M\widehat{U})(n) = (MM^*)U(n)$. So $M^* = M^{-1}$. □

8. **Suppose that $P(x) = \sum_{n=1}^N a_n e^{2\pi i n x}$.**

(a) Show by using the Parseval identities for the circle and $\mathbb{Z}(N)$, that

$$\int_0^1 |P(x)|^2 \, dx = \frac{1}{N}\sum_{j=1}^N |P(j/N)|^2.$$

(b) Prove the reconstruction formula

$$P(x) = \sum_{j=1}^N P(j/N) K(x - (j/N))$$

where

$$K(x) = \frac{e^{2\pi i x}}{N}\frac{1-e^{2\pi i N x}}{1-e^{2\pi i x}} = \frac{1}{N}(e^{2\pi i x} + e^{2\pi i 2x} + \cdots + e^{2\pi i N x}).$$

Observe that P is completely determined by the values $P(j/N)$ for $1 \le j \le N$. Note also that $K(0) = 1$, and $K(j/N) = 0$ whenever j is not congruent to 0 modulo N.

Remark 2. Compare with Exercise 5.20.

Proof. (a) Using the Parseval identities, one has

$$\int_0^1 |P(x)|^2\,dx = \sum_{j=1}^N |a_j|^2 = \frac{1}{N}\sum_{j=1}^N |P(j/N)|^2.$$

(b) Let $Q(z) = \sum_{n=1}^N a_n z^{n-1}$ and $\{z_j\}_{j=1}^N := \{e^{2\pi i \frac{j}{N}}\}_{j=1}^N$ be the N-th root of unity.

Using the Lagrange interpolation polynomials, one can derive that $Q(z) = \sum_{j=1}^N \frac{Q(z^j)}{N z_j^{N-1}}\frac{z^N-1}{z-z_j}$

Then

$$P(x) = e^{2\pi i x}Q(e^{2\pi i x}) = e^{2\pi i x}\sum_{j=1}^N \frac{P(\frac{j}{N})e^{-2\pi i \frac{j}{N}}}{N}\frac{e^{2\pi i N x}-1}{e^{2\pi i (x-\frac{j}{N})}-1} = \sum_{j=1}^N P(\frac{j}{N})K(x-\frac{j}{N}).$$

□

9. One can prove the following assertions by modifying the argument given in the text.

(a) 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.

(b) Generalize this to $N = \alpha^n$ where α is an integer > 1.

10. **A group G is cyclic if there exists $g \in G$ that generates all of G, that is, if any element in G can be written as g^n for some $n \in \mathbb{Z}$. Prove that a finite abelian group is cyclic if and only if it is isomorphic to $\mathbb{Z}(N)$ for some N.**

Remark 3. (1) Cyclic $\not\Leftrightarrow$ Abelian. (2) See Problem 2 for a more precise formulation for structure theorem for finite abelian groups.

Proof. If $G \cong_\phi \mathbb{Z}(N)$, then G is cyclic with $g = \phi(0)$. Conversely, if G has a generator g, then we define $\phi : G \to \mathbb{Z}(|G|)$ by $\phi(g^n) = n$ for every $0 \le n \le |G|-1$. Now it's easy to check ϕ is an isomorphism. □

11. **Write down the multiplicative tables for the groups $\mathbb{Z}^*(3), \mathbb{Z}^*(4), \mathbb{Z}^*(5), \mathbb{Z}^*(6), \mathbb{Z}^*(8)$, and $\mathbb{Z}^*(9)$. Which of these groups are cyclic?**

Proof. It's standard to see that $\mathbb{Z}^*(3), \mathbb{Z}^*(4), \mathbb{Z}^*(6)$ are all isomorphic to $\mathbb{Z}(2)$, and hence cyclic; $\mathbb{Z}^*(5) \cong \mathbb{Z}(4)$ is also cyclic; $\mathbb{Z}^*(8) \cong \mathbb{Z}(2) \times \mathbb{Z}(2)$ is not cyclic; $\mathbb{Z}^*(9) \cong \mathbb{Z}(6)$ is cyclic. □

12. **Suppose that G is a finite abelian group and $e : G \to \mathbb{C}$ is a function that satisfies $e(x \cdot y) = e(x)e(y)$ for all $x, y \in G$. Prove that either e is identically 0, or e never vanishes. In the second case, show that for each x, $e(x) = e^{2\pi i r}$ for some $r \in \mathbb{Q}$ of the form $r = p/q$, where $q = |G|$.**

Proof. Let 0_G be the identity of G. The multiplicative property implies $e(0_G) = 1$ or 0. If $e(0_G) = 0$, then the multiplicative property implies $e \equiv 0$. On the other hand, $e(a)e(a^{-1}) = e(0_G) = 1$ implies $e(a) \neq 0$ for all $a \in G$.

Note that for each x, $|G|x = x + x + \cdots + x = 0_G$ (Lagrange's theorem in group theory). So $e(x)^{|G|} = 1$, which implies $e(x) = e^{2\pi i \frac{r_x}{|G|}}$ for some $r_x \in \mathbb{Z}$. □

13. **In analogy with ordinary Fourier series, one may interpret finite Fourier expansions using convolutions as follows. Suppose G is a finite abelian group, 1_G its unit, and V the vector space of complex-valued functions on G.**

(a) The convolution of two functions f and g in V is defined for each $a \in G$ by

$$(f * g)(a) = \frac{1}{|G|} \sum_{b \in G} f(b) g(a \cdot b^{-1}).$$

Show that for all $e \in \widehat{G}$ one has $\widehat{(f * g)}(e) = \widehat{f}(e)\widehat{g}(e)$.

(b) Use Theorem 2.5 to show that

$$\sum_{e \in \widehat{G}} e(c) = 0 \quad \textbf{whenever} \quad c \in G \quad \textbf{and} \quad c \neq 1_G.$$

(c) As a result of (b), show that the Fourier series $Sf(a) = \sum_{e \in \widehat{G}} \widehat{f}(e) e(a)$ of a function $f \in V$ takes the form

$$Sf = f * D,$$

where D is defined by

$$D(c) = \sum_{e \in \widehat{G}} e(c) = \begin{cases} |G| & \textbf{if} \quad c = 1_G, \\ 0 & \textbf{otherwise}. \end{cases} \tag{2}$$

Since $f * D = f$, we recover the fact that $Sf = f$. Loosely speaking, D corresponds to a "Dirac delta function"; it has unit mass

$$\frac{1}{|G|} \sum_{c \in G} D(c) = 1,$$

and (2) says that this mass is concentrated at the unit element in G. Thus D has the same interpretation as the "limit" of a family of good kernels. (See Section 4, Chapter 2.)

Note. The function D reappears in the next chapter as $\delta_1(n)$.

Proof. (a) Note that $G \cdot b^{-1} = G$ for all $b \in G$. So

$$\widehat{(f * g)}(e) = \frac{1}{|G|} \sum_{a \in G} (f * g)(a) e(a) = \frac{1}{|G|^2} \sum_{a,b \in G} f(b) g(a \cdot b^{-1}) e(a \cdot b^{-1}) e(b)$$
$$= \frac{1}{|G|^2} \sum_{b \in G} f(b) e(b) \sum_{a \in G} g(a \cdot b^{-1}) e(a \cdot b^{-1}) = \frac{1}{|G|} \sum_{b \in G} f(b) e(b) \widehat{g}(e) = \widehat{f}(e) \widehat{g}(e)$$

(b) Note that $f\widehat{G} = \widehat{G}$ for each $f \in \widehat{G}$. If there is $e' \in \widehat{G}$ such that $e'(c) \neq 1$, then we see that $\sum_{e \in \widehat{G}} e(c) = 0$ since

$$e'(c) \sum_{e \in \widehat{G}} e(c) = \sum_{e \in \widehat{G}} (e'e)(c) = \sum_{f \in \widehat{G}} f(c).$$

The existence of e' (which looks like the group version of Hahn-Banach theorem) can be proved as follows:

Let H be the cyclic group generated by c. Then $|H| > 1$ and hence $|G/H| < |G|$, where $G/H = \{bH : b \in G\}$ is the quotient group. Suppose $e(c) = 1$ for all $e \in \widehat{G}$. Then each character e induces a character e_H on G/H defined by $e_H(bH) = e(b)$ (we verify this is well-defined by the hypothesis $e \equiv 1$ on H). So $e_H \neq f_H$ provided $e \neq f$ and hence we have a contradiction that $|G/H| < |G| = |\widehat{G}| = |\widehat{G/H}| = |G/H|$.

(c)

$$Sf(a) = \sum_{e \in \widehat{G}} \widehat{f}(e) e(a) = \sum_{e \in \widehat{G}} \frac{1}{|G|} \sum_{b \in G} f(b) \overline{e(b)} e(a) = \sum_{e \in \widehat{G}} \frac{1}{|G|} \sum_{b \in G} f(b) e(b^{-1}) e(a) = \frac{1}{|G|} \sum_{b \in G} f(b) D(b^{-1}a).$$

$\square$

Problems

1. **Prove that if n and m are two positive integers that are relatively prime, then**

$$\mathbb{Z}(nm) \cong \mathbb{Z}(n) \times \mathbb{Z}(m).$$

Proof. As hint, we consider the map $\phi : k \mapsto (k \bmod n, k \bmod m) =: (\phi_1(k), \phi_2(k))$.

Given $(a, b) \in \mathbb{Z}(n) \times \mathbb{Z}(m)$. Since m, n are relatively prime, there is $x, y \in \mathbb{Z}$ such that $mx + ny = 1$ (see Corollary 1.3 of Chapter 8). Then $k = amx + bny$ is a modulo n and is b modulo m, that is, $\phi(k) = (a, b)$.

If $\phi(k_1) = \phi(k_2)$, then $k_1 - k_2 = (p_1 - p_2)n$ for some $p_1, p_2 \in \mathbb{Z}$. Since m, n are relatively prime, $k_1 - k_2 = (q_1 - q_2)mn$. So $k_1 = k_2$ in $\mathbb{Z}(nm)$.

Finally, since $AB = (p_A n + \phi_1(A))(p_B n + \phi_1(B)) = (p_A p_B + p_A \phi_1(B) + p_B \phi_1(A))n + \phi_1(A)\phi_1(B)$, $\phi_1(AB) = \phi_1(A)\phi_1(B)$ for any $A, B \in \mathbb{Z}(nm)$. Similar for $\phi_2(AB) = \phi_2(A)\phi_2(B)$. □

2. **Every finite abelian group G is isomorphic to a direct product of cyclic groups. Here are two more precise formulations of this theorem.**

   - **If $p_1, \cdots, p_s$ are the distinct primes appearing in the factorization of the order of G, then**

   $$G \cong G(p_1) \times \cdots \times G(p_s),$$

   where each $G(p)$ is of the form $G(p) = \mathbb{Z}(p^{r_1}) \times \cdots \times \mathbb{Z}(p^{r_l})$, with $0 \le r_1 \le \cdots \le r_l$ (this sequence of integers depends on p of course). This decomposition is unique.

   - **There exist unique integers $d_1, \cdots, d_k$ such that**

   $$d_1 | d_2, d_2 | d_3, \cdots, d_{k-1} | d_k$$

   and

   $$G \cong \mathbb{Z}(d_1) \times \cdots \times \mathbb{Z}(d_k).$$

   Deduce the second formulation from the first.

   Proof. □

3. **Let $\widehat{G}$ denote the collection of distinct characters of the finite abelian group G.**

   (a) Note that if $G = \mathbb{Z}(N)$, then $\widehat{G}$ is isomorphic to G.

   (b) Prove that $\widehat{G_1 \times G_2} = \widehat{G_1} \times \widehat{G_2}$.

   (c) Prove using Problem 2 that if G is a finite abelian group, then $\widehat{G}$ is isomorphic to G.

   Remark 4. The results in this problem give another proof to Theorem 2.5.

   Proof. □

4. **When p is prime, the group $\mathbb{Z}^*(p)$ is cyclic and $\mathbb{Z}^*(p) \cong \mathbb{Z}(p-1)$.**

Proof. One way to prove this is through Euclidean algorithm (Corollary 1.3 of Chapter 8, also see page 244). The authors also refer this problem to [1, Chapter 7]. □

References

[1] Andrews, George E. Number theory. Courier Corporation, 1994.

[2] Engel, Klaus-Jochen, and Rainer Nagel. One-parameter semigroups for linear evolution equations. Vol. 194. Springer Science & Business Media, 1999.

[3] Herstein, Israel Nathan. Abstract algebra. Prentice Hall, 1996.