Homework 14 Solution

Yikun Zhang[1]

Chapter 7. Ex.5 *Show that all characters on S^1 are given by*

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

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

Proof. Suppose that F is a character on S^1. Then by definition at the bottom of Page 231, F is continuous on S^1, $F(0) \neq 0$, and $F(x+y) = F(x)F(y)$.
With the continuity of F and $F(0) \neq 0$, we can choose an appropriate δ such that $c = \int_0^\delta F(y)dy \neq 0$.
Then we have

$$cF(x) = \int_0^\delta F(x)F(y)dy = \int_0^\delta F(x+y)dy = \int_x^{x+\delta} F(u)du. \tag{1}$$

Differentiating (1) on both sides yields that $cF'(x) = F(x+\delta) - F(x) = [F(\delta) - 1]F(x)$.
If $F(\delta) = 1$, then $F(x) \equiv constant$. Together with the fact that $F(0) = 1$, we only obtain a trivial character.
If $F(\delta) \neq 1$, we conclude that $F(x) = e^{Ax}$ for some A, since $F(0) = 1$.
Since $|F(x)| = 1$, we know that $|F(1)| = e^{Re(A)} = 1$ and thus A is purely imaginary, which, on the other hand, means that $F(x) = e^{ipx}$ for some $p \in \mathbb{R}$.
Note that S^1 is isomorphic to $\mathbb{R}\, modulo\, 2\pi$, we can derive that $F(\pi)F(\pi) = F(2\pi) = F(0) = 1$ and therefore $e^{2\pi ip} = 1$, showing that $p \in \mathbb{Z}$.
Hence all the characters on S^1 are given by $e^{2\pi inx}$, with $n \in \mathbb{Z}$.
Define $\phi : \widehat{S^1} \to \mathbb{Z}$ by taking the reciprocal of the minimal period of e_n, i.e., $e_n \mapsto n$. This definition is well-defined because the minimal period of a character is unique.
Subjection: For any $n \in \mathbb{Z}$, by definition of the character on S^1, there exists a character of the form $e_n(x) = e^{2\pi inx}$.
Injection: If $m = n$, it is by no means that e_n and e_m have any difference.
Therefore, ϕ is an isomorphism from $\widehat{S^1}$ to $\mathbb{Z}$. □

Chapter 7. Ex.8 *Suppose that $P(x) = \sum_{n=1}^{N} a_n e^{2\pi inx}$.*
(a) Show by using the Parseval identities for the circle and $\mathbb{Z}(N)$, that

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

[1]School of Mathematics, Sun Yat-sen University

(b) Prove the reconstruction formula

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

where

$$K(x) = \frac{e^{2\pi ix}}{N}\frac{1 - e^{2\pi iNx}}{1 - e^{2\pi ix}} = \frac{1}{N}(e^{2\pi ix} + e^{2\pi i2x} + \cdots + e^{2\pi iNx}).$$

Observe that P is completely determined by the values $P(\frac{j}{N})$ for $1 \leq j \leq N$. Note also that $K(0) = 1$, and $K(\frac{j}{N}) = 0$ whenever j is not congruent to 0 module N.

Proof. (a) On one hand, by the Parseval identity for the circle, we have

$$\int_0^1 |P(x)|^2 dx = \sum_{n=1}^{N} |a_n|^2. \tag{2}$$

On the other hand, $P(\frac{j}{N}) = \sum_{n=1}^{N} a_n e^{\frac{2\pi inj}{N}}$. As a function on $\mathbb{Z}(N)$, the norm of P is

$$\begin{aligned} ||P||^2 &= \frac{1}{N}\sum_{j=1}^{N} P(\frac{j}{N}) \cdot \overline{P(\frac{j}{N})} \\ &= \frac{1}{N}\sum_{j=1}^{N}(\sum_{n=1}^{N} a_n e^{\frac{2\pi inj}{N}}) \cdot (\sum_{k=1}^{N} \bar{a_k} e^{-\frac{2\pi ikj}{N}}) \\ &= \frac{1}{N}\sum_{j=1}^{N}\sum_{n=1}^{N}\sum_{k=1}^{N} a_n \bar{a_k} e^{\frac{2\pi i(n-k)j}{N}} \\ &= \sum_{n=1}^{N} |a_n|^2, \end{aligned} \tag{3}$$

since

$$\sum_{j=1}^{N} e^{\frac{2\pi i(n-k)j}{N}} = \begin{cases} N & \text{if } n = k, \\ 0 & n \neq k. \end{cases}$$

With the Parseval identity on $\mathbb{Z}(N)$, we obtain that

$$\begin{aligned} ||P||^2 &= \sum_{e \in \widehat{\mathbb{Z}(N)}} |\hat{P}(e)|^2 \\ &= \sum_{l=1}^{N}(\frac{1}{N}\sum_{j=1}^{N} P(\frac{j}{N}) e^{\frac{2\pi ilj}{N}}) \cdot (\frac{1}{N}\sum_{k=1}^{N} \overline{P(\frac{k}{N})} e^{-\frac{2\pi ilk}{N}}) \\ &= \frac{1}{N}\sum_{j=1}^{N} |P(\frac{j}{N})|^2, \end{aligned} \tag{4}$$

Combining the equations (2), (3), and (4), the result follows.

(b) Note that $K(x) = \sum_{k=1}^{N} e^{2\pi ikx}$ satisfies $K(0) = 1$ and $K(\frac{j}{N}) = 0$ whenever j is not congruent to 0 modulo N.
Therefore, we have

$$\begin{aligned}\sum_{j=1}^{N} P(\frac{j}{N})K(x-\frac{j}{N}) &= \sum_{j=1}^{N}(\sum_{n=1}^{N} a_n e^{\frac{2\pi inj}{N}}) \cdot (\frac{1}{N}\sum_{k=1}^{N} e^{2\pi ikx}e^{-\frac{2\pi ikj}{N}}) \\ &= \frac{1}{N}\sum_{j=1}^{N}(\sum_{n=1}^{N}\sum_{k=1}^{N} a_n e^{2\pi ikx}e^{\frac{2\pi i(n-k)j}{N}}) \\ &= \sum_{n=1}^{N} a_n e^{2\pi inx} \\ &= P(x),\end{aligned} \tag{5}$$

where we again use the fact that $\{e^{\frac{2\pi ikl}{N}}\}_{l=1}^{N}, k = 1, ..., N$ is an orthogonal family on $\mathbb{Z}(N)$. □

Chapter 7. Ex.9 *To prove the following assertions, modify 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.

Proof. We only present the proof for (b) because (a) is just a special case of (b).
Given $\omega_N = e^{-\frac{2\pi i}{N}}$ with $N = \alpha^n$, we aim to prove that it is possible to calculate the Fourier coefficients of a function on $\mathbb{Z}(N)$ with at most

$$2\alpha N \log_\alpha N$$

operations.
Let $\#(M)$ denote the minimum number of operations needed to calculate all the Fourier coefficients of any functions on $\mathbb{Z}(M)$. We first prove a lemma.
Lemma. If we are given $\omega_{\alpha M} = e^{-\frac{2\pi i}{\alpha M}}$, then

$$\#(\alpha M) \leq \alpha\#(M) + 2\alpha^2 M.$$

Proof. The calculation of $\omega_{\alpha M}, ..., \omega_{\alpha M}^{\alpha M}$ requires no more than αM operations. Note that in particular we get $\omega_M = e^{-\frac{2\pi i}{M}} = \omega_{\alpha M}^{\alpha}$. The main idea is that for any given function F on $\mathbb{Z}(\alpha M)$, we consider α functions on $\mathbb{Z}(M)$ defined by

$$F_j(n) = F(\alpha n + j), 0 \leq j \leq \alpha - 1.$$

We assume that it is possible to calculate the Fourier coefficients of F_j in no more than $\#(M)$ operations each. If we denote the Fourier coefficients corresponding to the groups $\mathbb{Z}(\alpha M)$ and $\mathbb{Z}(M)$ by $a_k^{\alpha M}$ and a_k^M, respectively, then we have

$$a_k^{\alpha M}(F) = \frac{1}{\alpha}[a_k^M(F_0) + a_k^M(F_1)\omega_{\alpha M}^k + \cdots + a_k^M(F_{\alpha-1})\omega_{\alpha M}^{(\alpha-1)k}]$$

with some similar arguments in the text.
As a result, knowing $a_k^M(F_j), j = 0, ..., \alpha - 1$, and $\omega_{\alpha M}^k$, we see that each $a_k^{\alpha M}(F)$ can be computed via no more than $(2\alpha - 1)$ operations. So

$$\#(\alpha M) \leq \alpha M + \alpha\#(M) + (2\alpha - 1)\alpha M \leq \alpha\#(M) + 2\alpha^2 M,$$

and the proof of the lemma is complete.
An induction on n, where $N = \alpha^n$, will conclude the proof of the theorem. The initial step $n = 1$ is subtle, since we have to separate the case $k = 0$ from others in order to deduce a more precise upper bound.
If $n = 1$, i.e., $N = \alpha$, $a_k^N(F) = \frac{1}{N}\sum_{r=0}^{N-1} F(r)\omega_N^{kr}$. When $k = 0$ there are totally α operations ($(\alpha-1)$ additions and one multiplication). As for the rest, there are $(\alpha-1)$ additions and $(\alpha+1)$ multiplications for each $k \neq 0$. Together with $(\alpha - 1)$ operations for $\omega_N^{kr}, r = 0, ..., N - 1$, the total operations for the Fourier coefficients when $N = \alpha$ are $\alpha-1+\alpha+2\alpha(\alpha-1) = 2\alpha^2-1 \leq 2\alpha^2$. Suppose the result is true up to $N = \alpha^{n-1}$ so that $\#(N) \leq 2\alpha(n-1)\alpha^{n-1}$. By the lemma we must have

$$\#(\alpha N) \leq \alpha[2\alpha(n-1)\alpha^{n-1}] + 2\alpha^2 \cdot \alpha^{n-1},$$

which concludes the inductive step. □
Remark. This exercise generalizes Theorem 1.3 in the text and their proofs are also similar. However, some attentions still have to be paid when we inherit the argument from the text.