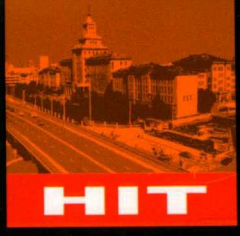
Number Theory with Applications



HIT

国外优秀数学著作
原 版 系 列

数论新应用

[美] 李文卿 (W.C.Winnier Li) 著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

Number Theory with Applications

数论新应用

国外优秀数学著作
原版系列

数论新应用

Number Theory with Applications

·[美]李文卿(W.C.Winnier Li)著

HITP
哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

黑版贸审字 08-2017-077 号

图书在版编目(CIP)数据

数论新应用:英文/(美)李文卿(W. C. Winnie Li)著.
—哈尔滨:哈尔滨工业大学出版社,2018.1
书名原文:Number theory with applications
ISBN 978-7-5603-6908-2

Ⅰ.①数… Ⅱ.①李… Ⅲ.①数论-研究-英文
Ⅳ.①O156

中国版本图书馆 CIP 数据核字(2017)第 207711 号

策划编辑 刘培杰
责任编辑 张永芹 杜莹雪
封面设计 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 哈尔滨市工大节能印刷厂
开 本 787mm×1092mm 1/16 印张 15.75 字数 295 千字
版 次 2018 年 1 月第 1 版 2018 年 1 月第 1 次印刷
书 号 ISBN 978-7-5603-6908-2
定 价 68.00 元

Preface

In the past decade, there have been important applications of number theory to network communications and computation complexity through explicit constructions of the so-called Ramanujan graphs. These are regular graphs whose nontrivial eigenvalues are small. (See Chapter 9 for more details.) All the known constructions are number-theoretic: one based on the estimates of Fourier coefficients of modular forms, namely, the former Ramanujan-Petersson conjecture established by Deligne, and one based on the estimates of certain character sums, which can be derived as consequences of the Riemann hypothesis for curves over finite fields proved by Weil. The common thread of both theoretic backgrounds is the celebrated Weil conjectures settled by Deligne in 1973. This is our starting point. The purpose of this book is to explain in detail the material in number theory involved in the applications discussed above, with the ultimate goal of giving the explicit constructions. In fact, this simple-minded goal serves as the guideline of the selection and the exposition of the material in this book. The reader will be amazed to find, as we take the journey along this line, how far and deep in mathematics we have gone through when we arrive at the destination.

The style of this book is semi-formal. It is written for advanced undergraduate students, graduate students and people interested in number theory and its applications. While it is desirable that the reader has some background in algebra and basic number theory, I try to make this book as self-contained as possible. More emphasis is given on basic concepts and results, while complicated proofs of hard theorems are only sketched in order to give the reader some flavor and idea of the approach. Occasionally statements without proofs are asserted for the sake of completeness and exposition. The reader can find the missing details and many untreated topics from the references listed at the end of each chapter. Exercises are scattered throughout the text, and sometimes used to prove theorems.

The material in this book is organized as follows. After reviewing the basic facts about finite fields in Chapter 1, we discuss in Chapter 2 the celebrated Weil conjectures on zeta functions attached to projective varieties over finite fields. We'll see how Weil arrived at his conjectures from computing the number of solutions of an equation over extensions of a finite field, and the ideas involved in the proof of these conjectures will also be sketched. Local and global fields are introduced and studied in Chapter 3. In this book adèlic language is employed for global fields. Chapters 4 and 5 concern function fields, where the Riemann-Roch theorem is proved and the analytic behaviour of the zeta and L-functions attached to idèle class characters is shown. By appealing to some results in class field theory (which we review briefly) and combining the results on L-functions and the Riemann hypothesis for curves over finite fields established in Chapters 5 and 2, we derive in Chapter 6 many character sum estimates, some of which will be used to construct Ramanujan graphs in Chapter 9. Chapter 7 deals with classical modular forms, which are a very rich subject, deeply intertwined with many branches of mathematics. We give a summary of the development of the theory, including Hecke operators, L-functions, converse theorems, and the theory of newforms. We also discuss main conjectures and consequences in this area, some of which are still outstanding and would have far-reaching consequences in number theory. One such example is the Taniyama-Shimura conjecture, which is recently established for semistable elliptic curves by Wiles and Taylor and Wiles. This result together with earlier works of Frey and Ribet implies the truth of Fermat's Last Theorem! Automorphic forms and representations are discussed in Chapter 8. There we give an adèlic interpretation of the classical modular forms, which naturally leads to the adèlic definition of automorphic forms and representations for $GL(2)$. Then we survey the Jacquet-Langlands theory of local and global representation theory for $GL(2)$ and quaternion groups. In particular, we show how the local representations of these groups are determined by the attached L- and ε- factors, from which correspondences of local representations of these two groups follow immediately. Finally in chapter 9 we see the interplay between number theory and combinatorics. On one hand, we apply what we have learned to give explicit constructions of Ramanujan graphs; on the other hand, we obtain some information on the distribution of eigenvalues of a Hecke operator from considering the limit of the measures attached to certain family of graphs arising from quaternion groups.

This book grew out of the one year graduate course in number theory I gave at the National Taiwan University during the year 1992-93. An outline of the material was given as a special one month summer course for graduate students in Sichuan University in the summer of 1992. I would like to thank both universities for their hospitality and support. The positive feedback from the audience has been a great source of encouragement to me. The main part of this book was written while I was spending my sabbatical year, 1992-93, visiting the National Taiwan University. Special thanks are due to the National Science Council in Taiwan and the National Security Agency in USA for their financial support, and to Ms. Shirley Wang for her superb typing job. The final part of the book was completed in the spring of

1995 while I was visiting the Mathematical Sciences Research Institute at Berkeley, California, to which I would like to express my sincere gratitude for its hospitality and support.

Wen-Ching Winnie Li
Berkeley, California
Spring, 1995

Contents

CHAPTER 1

Finite Fields

§1 The structure of a finite field

A finite field k is a finite commutative ring in which all nonzero elements have multiplicative inverse. Its characteristic, i.e., the smallest positive integer n such that $1+1+\cdots+1(n \text{ times}) = 0$, is a prime number p. Thus it contains $\mathbf{Z}/p\mathbf{Z}$ as a subfield, and it is a finite-dimensional vector space over $\mathbf{Z}/p\mathbf{Z}$. Its cardinality $|k| = q = p^d$ is a power of p, with exponent being the dimension of k over $\mathbf{Z}/p\mathbf{Z}$. This also indicates that the additive group of k is a direct sum of d copies of cyclic group of order p.

Next consider the multiplicative group $k^\times$, it has order $q-1$. So every nonzero element in k satisfies

$$x^{q-1} = 1,$$

and the order of an element in $k^\times$ divides $q-1$. For each positive divisor r of $q-1$, let

$$\Omega(r) = \{x \in k^\times : \text{ the order of } x \text{ is } r\}.$$

Then $k^\times$ is a disjoint union of $\Omega(r)$ as r runs through all positive divisors of $q-1$. We want to show that $\Omega(q-1)$ is nonempty, in other words,

Theorem 1. *$k^\times$ is cyclic of order $q-1$.*

To prove this theorem, observe first the general fact :

Lemma 1. *A polynomial $f(x)$ of degree n over a field F has at most n distinct roots in F.*

Proof. Let α be a root of $f(x)$ in F. Then $f(\alpha) = 0$, and

$$f(x) = f(x) - f(\alpha) = (x-\alpha)g(x)$$

for a polynomial $g(x)$ of degree $n-1$ over F. If β is a root of $f(x)$ in F different from α, then $0 = f(\beta) = (\beta-\alpha)f(\beta)$ and $\beta - \alpha \neq 0$ imply $g(\beta) = 0$. By induction,

$g(x)$ has at most $n-1$ distinct roots in F, so $f(x)$ has at most n distinct roots in F. □

It follows from Lemma 1 that if $\Omega(r)$ is nonempty, say, contains y, then y generates a cyclic subgroup of order r consisting of all solutions of $x^r = 1$ in k and $\Omega(r)$ is the set of generators in the cyclic group $< y >$. That is, $\Omega(r) = \{y^i : 1 \le i \le r,\ \gcd(i,r) = 1\}$. This shows that the cardinality of $\Omega(r)$ is either 0 or $\phi(r)$, where $\phi(n)$ is the Euler function which denotes the number of integers between 1 and n which are prime to n. We have

$$|k^\times| = q - 1 = \sum_{r|q-1} |\Omega(r)| \le \sum_{r|q-1} \phi(r).$$

To continue, we note another fact.

Lemma 2. *For every positive integer m, $\sum_{r|m} \phi(r) = m$.*

Granting Lemma 2, we conclude immediately from the above inequality that $|\Omega(r)| = \phi(r)$ for all $r \mid q-1$, and in particular, $|\Omega(r)| = \phi(r) \ge 1$, and the theorem follows.

To show Lemma 2, we partition the set $\{1, 2, \cdots, m\}$ as a disjoint union of

$$Y(r) = \{1 \le i \le m : \gcd(i,m) = \frac{m}{r}\}$$

as r runs through all positive divisors of m. For $i \in Y(r)$, write $i = j\frac{m}{r}$. Then $1 \le j \le r$ and $\gcd(i,m) = \gcd(j\frac{m}{r}, m) = \frac{m}{r}\gcd(j,r) = \frac{m}{r}$ implies $\gcd(j,r) = 1$. Hence $|Y(r)| = \phi(r)$. This proves

$$m = \sum_{r|m} |Y(r)| = \sum_{r|m} \phi(r).$$

□

Some immediate consequences of the above arguments are

Corollary 1. *The field k consists of the solutions to $x^q - x = 0$ in an algebraic closure of $\mathbf{Z}/p\mathbf{Z}$ containing k.*

Corollary 2. *There is an element $\xi \in k$ such that $k = (\mathbf{Z}/p\mathbf{Z})(\xi)$, that is, k is a simple extension of the prime field $\mathbf{Z}/p\mathbf{Z}$.*

Corollary 3. *For each positive divisor r of $q-1 (= |k^\times|)$ there are exactly $\phi(r)$ elements in $k^\times$ of order r.*

Corollary 4. *Given a positive integer n, there is a unique field extension of $\mathbf{Z}/p\mathbf{Z}$ of degree n within an algebraic closure of $\mathbf{Z}/p\mathbf{Z}$.*

Proof. Corollary 1 shows that a degree n extension of $\mathbf{Z}/p\mathbf{Z}$, if exists, is unique, namely, it should consist of the roots of $x^{p^n} = x$ in the algebraic closure. On the other hand, one checks easily that if α, β are solutions to $x^{p^n} = x$, then so are $\alpha - \beta$ and $\alpha\beta^{-1}$ (for $\beta \neq 0$), so the solutions to $x^{p^n} = x$ do form a field. □

Corollary 5. *Given any positive integer n, there exists an irreducible polynomial of degree n over $\mathbf{Z}/p\mathbf{Z}$.*

Proof. Let k be a finite field of degree n over $\mathbf{Z}/p\mathbf{Z}$. Then $k = (\mathbf{Z}/p\mathbf{Z})(\xi)$ by Corollary 2. Let $f(x)$ be the irreducible polynomial of ξ over $\mathbf{Z}/p\mathbf{Z}$. Then $k = (\mathbf{Z}/p\mathbf{Z})(\xi) = (\mathbf{Z}/p\mathbf{Z})[\xi] \cong (\mathbf{Z}/p\mathbf{Z})[x]/(f(x))$ shows $\deg f = [k : \mathbf{Z}/p\mathbf{Z}] = n$. □

---

§2 Extensions of a finite field

Let k be a finite field with q elements and let k_n be a degree n field extension of k. If k_m is an intermediate field of degree m over k, then k_n is a vector space over k_m, so m divides n. Conversely, any degree m extension of k within an algebraic closure of k_n with $m \mid n$ is a subfield of k_n by Corollary 1.

For an extension E of a field F, denote by $Gal(E/F)$ the group of automorphisms of E leaving F elementwise fixed. Consider the map σ on k_n which sends x to x^q. From

$$\sigma(x+y) = (x+y)^q = x^q + y^q = \sigma(x) + \sigma(y)$$

and

$$\sigma(xy) = (xy)^q = x^q y^q = \sigma(x)\sigma(y)$$

we see that σ is an endomorphism. Further, $\sigma(x) = x^q = 1$ together with $x^{q^n} = x$ implies $x = 1$. So σ is $1-1$. As k_n is finite, we have shown that σ is an automorphism of k_n. Finally, $\sigma(x) = x^q = x$ for $x \in k$, this shows that $\sigma \in Gal(k_n/k)$, called the Frobenius automorphism. Let r be the order of σ. Then

$$\sigma^r(x) = x^{q^r} = x \text{ for all } x \in k_n$$

implies $r = n$ since $k_n^\times$ is cyclic of order $q^n - 1$. Hence $Gal(k_n/k)$ contains the cyclic group $< \sigma >$ of order n. To determine $Gal(k_n/k)$ we notice following facts.

Each automorphism in $Gal(E/F)$ can be viewed as an F–linear transformation on E.

Lemma 3. *The automorphisms in $Gal(E/F)$ are E–linearly independent F–linear transformations.*

Proof. Suppose otherwise. Let $a_1\tau_1 + \cdots + a_r\tau_r = 0$ be a shortest nontrivial linear relation with $a_1, \cdots, a_r \in E^\times$ and $\tau_1, \cdots, \tau_r \in Gal(E/F)$. Then $r \geq 2$ and τ_i are distinct. Let $y \in E$ be such that $\tau_1(y) \neq \tau_2(y)$. From $\sum_{i=1}^r a_i\tau_i = 0$ we get $\sum_{i=1}^r a_i\tau_i(yx) = \sum_{i=1}^r a_i\tau_i(y)\tau_i(x) = 0$ for all $x \in k_n$, so $\sum_{i=1}^r a_i\tau_i(y)\tau_i = 0$. This yields another nontrivial relation

$$\sum_{i=1}^r a_i\tau_i(y)\tau_i - \tau_1(y)\sum_{i=1}^r a_i\tau_i = \sum_{i=2}^r a_i(\tau_i(y) - \tau_1(y))\tau_i = 0,$$

which is shorter than the relation we started with, a contradiction. □

Lemma 4. *Let E be a degree n extension of a field F. Then there are at most n distinct automorphisms in $Gal(E/F)$.*

Proof. Suppose otherwise. Let $\tau_1, \cdots, \tau_m$, $m > n$, be distinct automorphisms in $Gal(E/F)$. Let $\{v_1, \cdots, v_n\}$ be a basis of E over F. Let $(a_1, \cdots, a_m)$ be a nontrivial solution in E to the $n \times m$ system of linear equations

$$\begin{pmatrix} \tau_1(v_1) & \tau_2(v_1) & \cdots & \tau_m(v_1) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_1(v_n) & \cdots & \cdots & \tau_m(v_n) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Consider $\sum_{i=1}^m a_i\tau_i$. By construction, we have $\sum_{i=1}^m a_i\tau_i(v_j) = 0$ for $j = 1, \cdots, n$, hence $\sum_{i=1}^m a_i\tau_i(x) = 0$ for all $x \in E$. In other words, $\tau_1, \cdots, \tau_m$ are linearly dependent over E. This is impossible by Lemma 3. □

Therefore $|Gal(k_n/k)| = |<\sigma>| = n = [k_n : k]$, which is the maximal possible. In this case we say that the field k_n is Galois over k. We record this in

Theorem 2. *The field k_n is Galois over k with $Gal(k_n/k)$ cyclic of order n, generated by the Frobenius automorphism σ.*

Note that an element $x \in k_n$ lies in k if and only if it satisfies $x^q = x$, in other words, if and only if it is fixed by the Frobenius automorphism, or equivalently, by the group $Gal(k_n/k)$.

Using $G = Gal(k_n/k)$, we define two important maps, called trace and norm, denoted by $\mathrm{Tr}_{k_n/k}$ and $\mathrm{N}_{k_n/k}$, respectively, from k_n to k as follows:

$$\mathrm{Tr}_{k_n/k} : x \longmapsto \sum_{\tau \in G} \tau(x) = \sum_{i=1}^n \sigma^i(x),$$

$$\mathrm{N}_{k_n/k} : x \longmapsto \prod_{\tau \in G} \tau(x) = \prod_{i=1}^n \sigma^i(x).$$

One checks easily that the images of trace and norm maps are in k. It is clear that $\mathrm{Tr}_{k_n/k}$ is a homomorphism from the additive group k_n to the additive group k, and $\mathrm{N}_{k_n/k}$ is a homomorphism from $k_n^\times$ to $k^\times$. Next we study their images.

Theorem 3. *(Hilbert Theorem 90) The norm map $\mathrm{N}_{k_n/k}$ from $k_n^\times$ to $k^\times$ is surjective with the kernel consisting of $x/\sigma(x)$, $x \in k_n^\times$.*

Proof. Since $\mathrm{N}_{k_n/k}(\sigma(x)) = \sum_{i=1}^n \sigma^{i+1}(x) = \sum_{i=1}^n \sigma(x) = \mathrm{N}_{k_n/k}(x)$, so $x/\sigma(x)$ lies in the kernel of the norm map for all $x \in k_n^\times$. Further, $x/\sigma(x) = y/\sigma(y)$ if and only if $xy^{-1} \in k^\times$, hence the elements $x/\sigma(x)$ with $x \in k_n^\times$ form a subgroup of $k_n^\times$ of order $(q^n-1)/(q-1)$. Thus it is equal to the whole kernel if and only if the norm map is surjective. To see the surjectiveness of $\mathrm{N}_{k_n/k}$, observe that $\mathrm{N}_{k_n/k}(x) = \prod_{i=1}^n \sigma^i(x) = x \cdot x^q \cdot x^{q^2} \cdots x^{q^{n-1}} = x^{1+q+q^2+\cdots+q^{n-1}} = x^{(q^n-1)/(q-1)}$ for all $x \in k_n^\times$. Thus any generator x of $k_n^\times$ has $\mathrm{N}_{k_n/k}(x)$ of order $q-1$. □

Theorem 4. *(Hilbert Theorem 90) The trace map $\mathrm{Tr}_{k_n/k}$ from k_n to k is surjective with the kernel consisting of $x - \sigma(x)$, $x \in k_n$.*

Proof. As elements in $Gal(k_n/k)$ are k-linear maps, the image of $\mathrm{Tr}_{k_n/k}$ is a vector space over k, hence $\mathrm{Tr}_{k_n/k}(k_n) = 0$ or k. If $\mathrm{Tr}_{k_n/k}(k_n) = 0$, then $\sum_{i=1}^n \sigma^i = 0$, which is a nontrivial linear relation among elements of $Gal(k_n/k)$, hence impossible by Lemma 3. Therefore $\mathrm{Tr}_{k_n/k}$ is surjective. Then its kernel has order q^{n-1}. Clearly, $\mathrm{Tr}_{k_n/k}(\sigma(x)) = \mathrm{Tr}_{k_n/k}(x)$ so that kernel contains $x - \sigma(x)$ for all $x \in k_n$. Further, $x - \sigma(x) = y - \sigma(y)$ if and only if $x - y \in k$, so the group $\{x - \sigma(x) : x \in k_n\}$ has order q^n/q, thus is equal to the kernel. □

Remark. The Hilbert theorem 90 for norm and trace maps is usually proved using first cohomology group of the Galois group (à la Noether). When the base field is finite, we may use counting argument, as shown above.

Exercise 1. Let k be a finite field with finite extensions k_m and k_{mn} of degree m, mn, respectively. Show that

$$\mathrm{Tr}_{k_{mn}/k} = \mathrm{Tr}_{k_m/k} \circ \mathrm{Tr}_{k_{mn}/k_m} \quad \text{and} \quad \mathrm{N}_{k_{mn}/k} = \mathrm{N}_{k_m/k} \circ \mathrm{N}_{k_{mn}/k_m}.$$

Given $z \in k_n$, it defines a k-linear transformation L_z on k_n by $x \mapsto zx$, that is, multiplication by z. The trace and determinant of L_z are defined as the trace and determinant of any $n \times n$ matrix representing L_z. They are in fact given by $\mathrm{Tr}_{k_{mn}/k}$ and $\mathrm{N}_{k_{mn}/k}$ of z. More precisely, we have

Theorem 5. *Let $z \in k_n$ and define L_z as above. Then*

(1) $\operatorname{Tr} L_z = \operatorname{Tr}_{k_n/k}(z)$ *and* $\det L_z = \mathrm{N}_{k_n/k}(z)$

(2) *Suppose $k(z) = k_n$. Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ be the irreducible polynomial of z over k. Then*

$$a_1 = -\operatorname{Tr}_{k_n/k}(z) \quad \textit{and} \quad a_n = (-1)^n \mathrm{N}_{k_n/k}(z).$$

Proof. We shall prove (1) and (2) under the assumption (2) and leave (1) for the case $k(z)$ being a proper subfield of k_n as an exercise. For each τ in $Gal(k_n/k)$, $0 = \tau(f(z)) = f(\tau(z))$, hence $\tau(z)$ is also a root of $f(x)$. Further, if τ and τ' are two different elements in $Gal(k_n/k)$, then $\tau(z) \neq \tau'(z)$ (otherwise they would agree on $k(z) = k_n$). This shows that z has n distinct images under $Gal(k_n/k)$ and they are the roots of $f(x)$. Therefore,

$$-a_1 = \text{ the sum of roots of } f(x) = \operatorname{Tr}_{k_m/k}(z)$$

and

$$(-1)^n a_n = \text{ the product of roots of } f(x) = \mathrm{N}_{k_n/k}(z).$$

This proves (2). For (1), we know that L_z satisfies $f(x) = 0$. As $f(x)$ is irreducible over k and $[k_n : k] = n$, $f(x)$ is the characteristic polynomial of L_z. The companion matrix attached to L_z is

$$\begin{pmatrix} 0 & & & -a_n \\ 1 & 0 & & -a_{n-1} \\ & 1 & \cdot & \cdot \\ & & \cdot & \cdot \\ & & 0 & \cdot \\ & & 1 & -a_1 \end{pmatrix},$$

which has trace $= -a_1$ and determinant $= (-1)^n a_n$. This proves (1). □

Exercise 2. Let $z \in k_n$. Suppose $k(z) = k_m$ is a proper subfield of k_n. Prove that $\operatorname{Tr} L_z = \operatorname{Tr}_{k_n/k}(z) = \frac{n}{m} \operatorname{Tr}_{k_m/k}(z)$ and $\det L_z = \mathrm{N}_{k_m/k}(z)^{n/m}$.

Exercise 3. (1) (Normal Basis Theorem) There exists an element $z \in k_n$ such that $\{\tau(z) : \tau \in Gal(k_n/k)\}$ is basis of k_n over k. (Hint : Consider the minimal polynomial of the Frobenius automorphism σ.)

(2) For z in (1) we have $\operatorname{Tr}_{k_n/k}(z) \neq 0$. (Hint : Express an element in k_n as a k-linear combination of $\{\tau(z)\}$. Then show $\operatorname{Tr}_{k_n/k}(k_n) = k \operatorname{Tr}_{k_n/k}(z)$.)

§3 Characters

A character of a topological group G is a continuous homomorphism from G to the unit circle S^1 in the complex plane. If G is a finite group, then it is endowed with the discrete topology so that a character is simply a homomorphism from G to S^1. As S^1 is commutative, any character of G factors through the quotient of G by its commutator subgroup. The character sending G to 1 is called the trivial character of G.

All characters of G form an abelian group under pointwise multiplication, called the dual group of G and denoted by $\widehat{G}$.

Example 1. Compute $\widehat{G}$ for a finite cyclic group G.

Suppose G has order n. Let g be a generator of G and ζ be a primitive nth root of 1. The homomorphism η from G to S^1 sending g to ζ is a charactor of G of order n. Hence $\widehat{G}$ contains the cyclic group $< \eta >$. On the other hand, any character χ of G is determined by its value $\chi(g)$ at g, which is an nth root of 1. Thus $\chi(g) = \zeta^k$ for some integer k, and this shows that $\chi = \eta^k$. So $G =< \eta >$ is also a cyclic group of order n. We see that $\widehat{G}$ is isomorphic to G.

Proposition 1. *If G is a finite abelian group, then G is isomorphic to its dual group $\widehat{G}$.*

Proof. By the fundamental theorem of finite abelian groups, we may decompose G as a product of cyclic groups

$$G = G_1 \times \cdots \times G_r.$$

For a character χ of G, denote by χ_i its restriction to G_i. Thus χ is the product of $\chi_1, \cdots, \chi_r$ and $\widehat{G} = \widehat{G_1} \times \cdots \times \widehat{G_r}$. We have seen that each $\widehat{G_i}$ is isomorphic to G_i, hence $\widehat{G}$ is isomorphic to G. □

Remark. The above isomorphism $G \cong \widehat{G}$ is not canonical since it depends on the decomposition of G into a product of cyclic groups and for each cyclic group, the isomorphism depends on the choice of generators. However, the dual of $\widehat{G}$, namely, $\hat{\widehat{G}}$, is naturally isomorphic to G. This follows from the non-degeneracy of the pairing

$$\xi : G \times \widehat{G} \longrightarrow S^1$$

given by

$$\xi(g, \chi) = \chi(g).$$

(When we fix one variable, ξ is a homomorphism with respect to the other variable.)

Exercise 4. (1) Show that ξ defined above is nondegenerate, that is,

(i) If g is not the identity element of G, then there is a character χ of G such that $\chi(g) \neq 1$.

(ii) If χ is a nontrivial character of G, then there exists an element g of G such that $\chi(g) \neq 1$.

(2) Show that the nondegeneracy of ξ implies that G and $\hat{\hat{G}}$ are naturally isomorphic.

For a closed subgroup H of G, denote by $H^{\perp} = \{\chi \in \widehat{G} : \chi(H) = 1\}$. When G is an abelian group, $H^{\perp}$ is canonically identified with $\widehat{G/H}$.

Theorem 6. *(Pontrjagin duality) Let G be an abelian topological group. The map $H \mapsto H^{\perp}$ establishes a bijection from the closed subgroups of G to those of $\widehat{G}$. Further, $H^{\perp\perp}$ is naturally isomorphic to H.*

We examine this theorem for the case where G is a finite abelian group, thus topology plays no role. Again, by the fundamental theorem of finite abelian groups, we may assume that G is cyclic of order n. The subgroups H of G are indexed by the positive divisors d of n such that $d =$ the order of H. Then $\widehat{G}$ is cyclic of order n and $H^{\perp}$ has order $\frac{n}{|H|}$. The bijection $H \mapsto H^{\perp}$ is obvious. Under the canonical isomorphism $\hat{\hat{G}} \cong G$, we may identity $H^{\perp\perp}$ with the group $\widetilde{H} = \{g \in G : \chi(g) = 1$ for all $\chi \in H^{\perp}\}$. Since every $\chi \in H^{\perp}$ is trivial on H, the group $\widetilde{H}$ contains H. On the other hand, $|\widetilde{H}| = |\widehat{G}|/|H^{\perp}|$ and $|H^{\perp}| = |G|/|H|$ imply $|\widehat{H}| = |H|$. Hence $\widehat{H} = H$, i.e., $H^{\perp\perp} \cong H$ naturally. □

Define an inner product $<,>$ on the space $\mathbf{C}[G]$ of complex-valued functions on a finite abelian group G by

$$< f, g >= \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}.$$

Proposition 2. *Let G be a finite abelian group. Then the characters of G form an orthonormal basis of $\mathbf{C}[G]$.*

To prove this, we shall need

Lemma 5. *Let G be a finite abelian group, $g \in G$ and $\chi \in$ hat$G$. Then*

$$(1) \sum_{x \in G} \chi(x) = \begin{cases} 0 & \text{if } \chi \text{ is nontrivial,} \\ |G| & \text{if } \chi \text{ is trivial.} \end{cases}$$

$$(2) \sum_{\eta \in \widehat{G}} \eta(g) = \begin{cases} 0 & \text{if } g \text{ is not the identity of } G, \\ |G| & \text{if } g \text{ is the identity of } G. \end{cases}$$