Introduction to Analytic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Definitions

Group Axioms

Definition (Postulates for a Group)

A **group** G is a nonempty set of elements together with a binary operation, which we denote by $\cdot$, such that the following postulates are satisfied:

(a) **Closure** For every a and b in G, $a \cdot b$ is also in G.

(b) **Associativity** For every a, b, c in G, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(c) **Existence of Identity** There is a unique element e in G, called the **identity**, such that $a \cdot e = e \cdot a = a$, for every a in G.

(d) **Existence of Inverses** For every a in G, there is a unique element b in G such that $a \cdot b = b \cdot a = e$. This b is denoted by a^{-1} and is called the **inverse** of a.

- We usually omit the dot and write ab for $a \cdot b$.

Abelian and Finite Groups and Subgroups

Definition

A group G is called **abelian** if every pair of elements commute, i.e., if

$$ab = ba, \quad \text{for all } a \text{ and } b \text{ in } G.$$

Definition

A group G is called **finite** if G is a finite set. In this case the number of elements in G is called the **order** of G and is denoted by $|G|$.

Definition

A nonempty subset G' of a group G which is itself a group, under the same operation, is called a **subgroup** of G.

Subsection 2

Examples of Groups and Subgroups

Examples

- **Trivial Subgroups** Every group G has at least two subgroups, G itself and the set $\{e\}$ consisting of the identity element alone.
- **Integers under Addition** The set of all integers is an abelian group with $+$ as the operation and 0 as the identity. The inverse of n is $-n$.
- **Complex Numbers under Multiplication** The set of all non-zero complex numbers is an abelian group with ordinary multiplication of complex numbers as the operation and 1 as the identity. The inverse of z is the reciprocal $\frac{1}{z}$.

  The set of all complex numbers of absolute value 1 is a subgroup.
- **The n-th Roots of Unity** An example of a finite group is the set $\{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}\}$, where $\varepsilon = e^{2\pi i/n}$ and the operation is ordinary multiplication of complex numbers. This group, of order n, is called the **group of n-th roots of unity**.

  It is a subgroup of both groups in the preceding example.

Subsection 3

Elementary Properties of Groups

Cancelation Laws

- Unless otherwise stated, G is an arbitrary group, not required to be abelian nor finite.

Theorem (Cancelation Laws)

For all elements a, b, c in G,

$$ac = bc \quad \text{or} \quad ca = cb \quad \text{implies} \quad a = b.$$

- In the first case multiply each member on the right by c^{-1} and use associativity:

$$\begin{aligned} ac = bc \quad & \Rightarrow \quad (ac)c^{-1} = (bc)c^{-1} \\ & \Rightarrow \quad a(cc^{-1}) = b(cc^{-1}) \\ & \Rightarrow \quad ae = be \\ & \Rightarrow \quad a = b. \end{aligned}$$

In the second case multiply on the left by c^{-1}.

Properties of Inverses

Theorem (Properties of Inverses)

In any group G we have:

(a) $e^{-1} = e$;
(b) For every a in G, $(a^{-1})^{-1} = a$;
(c) For all a and b in G, $(ab)^{-1} = b^{-1}a^{-1}$;
(d) For all a and b in G the equation $ax = b$ has the unique solution $x = a^{-1}b$; the equation $ya = b$ has the unique solution $y = ba^{-1}$.

(a) We have $ee = ee^{-1}$. Cancel e to obtain $e = e^{-1}$.
(b) Since $aa^{-1} = e$ and inverses are unique, a is the inverse of a^{-1}.
(c) By associativity, $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. So $b^{-1}a^{-1}$ is the inverse of ab.
(d) By associativity, $a(a^{-1}b) = (aa^{-1})b = b$ and $(ba^{-1})a = b(a^{-1}a) = b$. The solutions are unique because of the cancelation laws.

Powers of an Element

Definition (Powers of an Element)

If $a \in G$, we define a^n for any integer n by the following relations:

$$a^0 = e, \quad a^n = aa^{n-1}, \quad a^{-n} = (a^{-1})^n, \quad \text{for } n > 0.$$

Theorem

If $a \in G$, any two powers of a commute, and for all integers m and n we have

$$a^m a^n = a^{m+n} = a^n a^m \quad \text{and} \quad (a^m)^n = a^{nm} = (a^n)^m.$$

Moreover, if a and b commute, we have $a^n b^n = (ab)^n$.

- These laws of exponents can be proved by induction.

The Subgroup Criterion

Theorem (Subgroup Criterion)

If G' is a nonempty subset of a group G, then G' is a subgroup if, and only if, G' satisfies group postulates (a) and (d):

(a) **Closure** If $a, b \in G'$, then $ab \in G'$.

(d) **Existence of Inverse** if $a \in G'$, then $a^{-1} \in G'$.

- Every subgroup G' certainly has these properties.

  Conversely, if G' satisfies (a) and (d) it is easy to show that G' also satisfies postulates (b) and (c).

  (b) Associativity holds in G' because it holds for all elements in G.

  (c) Existence of identities holds in G'.
  Since G' is nonempty, there exists an element a in G'.
  By (d), $a^{-1} \in G'$. By (a), $e = aa^{-1} \in G'$.

Subsection 4

Construction of Subgroups

Cyclic Subgroups

- A subgroup of a given group G can always be constructed stating from a specific element of G.
- Choose any element a in G.
- Form the set of all its powers

$$a^n, \quad n = 0, \pm 1, \pm 2, \ldots.$$

- This set clearly satisfies postulates (a) and (d), closure under the operation and under inverses.
- So it is a subgroup of G.
- It is called the **cyclic subgroup generated** by a, denoted by $\langle a \rangle$.
- Note that $\langle a \rangle$ is abelian, even if G is not.

The Order of an Element

- Let G be a group.
- Let a be an element of G.
- Suppose $a^n = e$, for some positive integer n.
- Then there will be a smallest $n > 0$ with this property.
- The subgroup $\langle a \rangle$ is a finite group of order n,

$$\langle a \rangle = \{a, a^2, \ldots, a^{n-1}, a^n = e\}.$$

- The integer n is also called the **order of the element** a.

  Example: A cyclic subgroup of order n is the group of n-th roots of unity.

Order of Elements in a Finite Group

- Every element of a finite group has finite order.

Theorem

If G is finite and $a \in G$, then there is a positive integer n such that $a^n = e$.

- Let $g = |G|$.

  At least two of the following $g + 1$ elements of G must be equal,

$$e, a, a^2, \ldots, a^g.$$

  Suppose that $a^r = a^s$, where $0 \leq s < r \leq g$.

  Then we have

$$e = a^r (a^s)^{-1} = a^{r-s}.$$

  This proves the theorem with $n = r - s$.

Indicator of an Element in a Subgroup

Claim: If G' is a subgroup of a finite group G, then for any element a in G, there is an integer n, such that $a^n \in G'$.

If a is already in G' we simply take $n = 1$.

If $a \notin G'$, we can take n to be the order of a, since $a^n = e \in G'$.

- However, there may be a smaller positive power of a which lies in G'.
- By the well-ordering principle there is a smallest positive integer n, such that
$$a^n \in G'.$$
- We call this integer the **indicator of a in G'**.

Augmenting a Subgroup

Theorem

Let G' be a subgroup of a finite abelian group G, where $G' \neq G$. Choose an element a in G, $a \notin G'$, and let h be the indicator of a in G'. Then the set of products

$$G'' = \{xa^k : x \in G' \text{ and } k = 0, 1, 2, \ldots, h-1\}$$

is a subgroup of G which contains G'. Moreover, the order of G'' is h times that of G',

$$|G''| = h|G'|.$$

- To show G'' is a subgroup we use the subgroup criterion.

Augmenting a Subgroup (Cont'd)

- First we test closure.

  Choose two elements in G''.

  They have the form xa^k and ya^j, where $x, y \in G'$ and $0 \leq k, j < h$.

  Since G is abelian, their product is $(xy)a^{k+j}$.

  Now $k + j = qh + r$, where $0 \leq r < h$.

  Hence,

$$a^{k+j} = a^{qh+r} = a^{qh}a^r = za^r,$$

  where $z = a^{qh} = (a^h)^q \in G'$, since $a^h \in G'$.

  Therefore,

$$(xy)a^{k+j} = (xyz)a^r = wa^r,$$

  where $w \in G'$ and $0 \leq r < h$.

  This proves that G'' satisfies the closure postulate.

Augmenting a Subgroup (Cont'd)

- Next we show that the inverse of each element in G'' is also in G''.
  Choose an arbitrary element in G'', say xa^k.
  - If $k = 0$, then the inverse is x^{-1} which is in G''.
  - If $0 < k < h$, the inverse is the element
  $$(xa^k)^{-1} = x^{-1}(a^h)^{-1}a^h a^{-k} = (x^{-1}(a^h)^{-1})a^{h-k}.$$
  This is again in G'', since $a^h \in G'$ and $0 < h - k < h$.

  This shows that G'' is indeed a subgroup of G.

  Clearly G'' contains G'.

Augmenting a Subgroup (Cont'd)

- Next we determine the order of G''.

  Let $m = |G'|$.

  Let x run through the m elements of G'.

  Let k run through the h integers $0, 1, 2, \ldots, h-1$.

  Then we obtain mh products xa^k.

  If we show that all these are distinct, then G'' has order mh.

  Consider two of these products, say xa^k and ya^j.

  Assume that

  $$xa^k = ya^j, \quad 0 \le j \le k < h.$$

  Then $a^{k-j} = x^{-1}y$ and $0 \le k-j < h$.

  Since $x^{-1}y \in G'$, we must have a^{k-j} in G'.

  So $k = j$. Hence $x = y$.

Subsection 5

Characters of Finite Abelian Groups

Characters of Groups

Definition

Let G be an arbitrary group. A complex-valued function f defined on G is called a **character** of G if f has the multiplicative property

$$f(ab) = f(a)f(b),$$

for all a, b in G, and if $f(c) \neq 0$, for some c in G.

A Property of Characters

Theorem

If f is a character of a finite group G with identity element e, then

$$f(e) = 1.$$

Moreover, each function value $f(a)$ is a root of unity. In fact, if $a^n = e$, then

$$f(a)^n = 1.$$

- Choose c in G, such that $f(c) \neq 0$.
  Since $ce = c$, we have $f(c)f(e) = f(c)$. So $f(e) = 1$.
  Now suppose $a^n = e$.
  Then
  $$f(a)^n = f(a^n) = f(e) = 1.$$

Existence of Characters

- Every group G has at least one character.

  The function which is identically 1 on G is a character.

  This is called the **principal character**.
- The next theorem tells us that there are further characters if G is abelian and has finite order > 1.

Theorem

A finite abelian group G of order n has exactly n distinct characters.

- In a previous theorem we saw how to construct, from a given subgroup $G' \neq G$, a new subgroup G'' containing G' and at least one more element a not in G'.

  Let $\langle G'; a\rangle = \{xa^k : x \in G', 0 \leq k < h\}$ be the subgroup G'' thus constructed, where h is the indicator of a in G'.

Proof of the Theorem (Setup)

- Now we apply this construction repeatedly, starting with the subgroup $\{e\}$ which we denote by G_1.
  If $G_1 \neq G$, let a_1 be an element of G other than e.
  Define $G_2 = \langle G_1; a_1 \rangle$.
  If $G_2 \neq G$, let a_2 be an element of G which is not in G_2.
  Define $G_3 = \langle G_2; a_2 \rangle$.
  Continue the process to obtain a finite set of elements $a_1, a_2, \ldots, a_t$ and a corresponding set of subgroups $G_1, G_2, \ldots, G_{t+1}$, such that $G_{r+1} = \langle G_r; a_r \rangle$, with $G_1 \subset G_2 \subset \cdots \subset G_{t+1} = G$.
  By hypothesis, the given group G is finite.
  Moreover, each G_{r+1} contains more elements than its predecessor G_r.
  So the process must terminate in a finite number of steps.
  We fix such a chain of subgroups.
  We prove the theorem by induction, showing that if it is true for G_r, it must also be true for G_{r+1}.

Proof of the Theorem (Sketch of Induction)

- It is clear that there is only one character for G_1.

  This is the function which is identically 1.

  Now assume that:

  - G_r has order m;
  - There are exactly m distinct characters for G_r.

  Consider $G_{r+1} = \langle G_r; a_r \rangle$ and let h be the indicator of a_r in G_r.

  This is the smallest positive integer such that $a_r^h \in G_r$.

  We shall show that:

  - There are exactly h different ways to extend each character of G_r to obtain a character of G_{r+1};
  - Each character of G_{r+1} is the extension of some character of G_r.

  This will prove that G_{r+1} has exactly mh characters.

  Since mh is also the order of G_{r+1} this will complete the induction.

Proof of the Theorem (Induction Step)

- An element in G_{r+1} has the form xa_r^k, where $x \in G_r$ and $0 \leq k < h$.
  Suppose that it is possible to extend a character f of G_r to G_{r+1}.
  Call this extension $\widetilde{f}$ and let us see what can be said about $\widetilde{f}(xa_r^k)$.
  The multiplicative property requires $\widetilde{f}(xa_r^k) = \widetilde{f}(x)\widetilde{f}(a_r)^k$.
  Since $x \in G_r$, we have $\widetilde{f}(x) = f(x)$.
  So we get $\widetilde{f}(xa_r^k) = f(x)\widetilde{f}(a^r)^k$.
  This tells us that $\widetilde{f}(xa_r^k)$ is determined as soon as $\widetilde{f}(a_r)$ is known.
  What are the possible values for $\widetilde{f}(a_r)$?
  Let $c = a_r^h$. Since $c \in G_r$ we have $\widetilde{f}(c) = f(c)$.
  Since $\widetilde{f}$ is multiplicative, we also have $\widetilde{f}(c) = \widetilde{f}(a_r)^h$.
  Hence, $\widetilde{f}(a_r)^h = f(c)$. So $\widetilde{f}(a_r)$ is one of the h-th roots of $f(c)$.
  Therefore, there are at most h choices for $\widetilde{f}(a_r)$.

Proof of the Theorem (Step Cont'd)

- These observations tell us how to define $\widetilde{f}$.
  If f is a given character of G_r, we choose one of the h-th roots of $f(c)$, where $c = a_r^h$, and define $\widetilde{f}(a_r)$ to be this root.
  Then we define $\widetilde{f}$ on the rest of G_{r+1} by the equation
  $$\widetilde{f}(xa_r^k) = f(x)\widetilde{f}(a_r)^k.$$
  The h choices for $\widetilde{f}(a_r)$ are all different.
  So this gives us h different ways to define $\widetilde{f}(xa_r^k)$.
  We verify that $\widetilde{f}$ satisfies the multiplicative property.
  $$\begin{array}{rcl} \widetilde{f}(xa_r^k \cdot ya_r^j) & = & \widetilde{f}(xy \cdot a_r^{k+j}) \\ & = & f(xy)\widetilde{f}(a_r)^{k+j} \\ & = & f(x)f(y)\widetilde{f}(a_r)^k\widetilde{f}(a_r)^j \\ & = & \widetilde{f}(xa_r^k)\widetilde{f}(ya_r^j). \end{array}$$
  So $\widetilde{f}$ is a character of G_{r+1}.

Proof of the Theorem (Conclusion)

- No two of the extensions $\widetilde{f}$ and $\widetilde{g}$ can be identical on G_{r+1}.

  This follows because the functions f and g which they extend would then be identical on G_r.

  Therefore, each of the m characters of G_r can be extended in h different ways to produce a character of G_{r+1}.

  Moreover, if φ is any character of G_{r+1}, then its restriction to G_r is also a character of G_r.

  So the extension process produces all the characters of G_{r+1}.

Subsection 6

The Character Group

The Characters of a Finite Abelian Group

- Let G be a finite abelian group of order n.
- The principal character of G is denoted by f_1.
- The other characters, denoted by

$$f_2, f_3, \ldots, f_n,$$

  are called **nonprincipal characters**.
- They have the property that

$$f(a) \neq 1, \quad \text{for some } a \text{ in } G.$$

The Character Group

Theorem

If multiplication of characters is defined by the relation

$$(f_i f_j)(a) = f_i(a) f_j(a),$$

for each a in G, then the set of characters of G forms an abelian group of order n. We denote this group by $\widehat{G}$. The identity element of $\widehat{G}$ is the principal character f_1. The inverse of f_i is the reciprocal $\frac{1}{f_i}$.

- Verification of the group postulates is straightforward.

Note on Inverses

- For each character f we have $|f(a)| = 1$.
- Hence the reciprocal $\frac{1}{f(a)}$ is equal to the complex conjugate $\overline{f(a)}$.
- Thus, the function $\overline{f}$ defined by
$$\overline{f}(a) = \overline{f(a)}$$
is also a character of G.
- Moreover, we have, for every a in G,
$$\overline{f}(a) = \frac{1}{f(a)} = f(a^{-1}).$$

Subsection 7

The Orthogonality Relations for Characters

The Matrix $A(G)$

- Let G be a finite abelian group of order n, with elements

$$a_1, a_2, \ldots, a_n.$$

- Let

$$f_1, f_2, \ldots, f_n$$

be the characters of G, with f_1 the principal character.

- We denote by $A = A(G)$ the $n \times n$ matrix $[a_{ij}]$ whose element a_{ij} in the i-th row and j-th column is

$$a_{ij} = f_i(a_j).$$

Sums of Rows of the Matrix $A(G)$

Theorem

The sum of the entries in the i-th row of A is given by

$$\sum_{r=1}^{n} f_i(a_r) = \begin{cases} n, & \text{if } f_i \text{ is the principal character} \\ 0, & \text{otherwise} \end{cases}$$

- Let S denote the sum.
  - If $f_i = f_1$, each term of the sum is 1. So $S = n$.
  - If $f_i \neq f_1$, there is an element b in G for which $f(b) \neq 1$.
    As a_r runs through the elements of G so does the product ba_r.
    Hence
    $$S = \sum_{r=1}^{n} f_i(ba_r) = f_i(b) \sum_{r=1}^{n} f_i(a_r) = f_i(b)S.$$
    Therefore, $S(1 - f_i(b)) = 0$.
    Since $f_i(b) \neq 1$, it follows that $S = 0$.

The Inverse of $A(G)$

Theorem

Let A^* denote the conjugate transpose of the matrix A. Then we have

$$AA^* = nI,$$

where I is the $n \times n$ identity matrix. Hence $n^{-1}A^*$ is the inverse of A.

- Let $B = AA^*$.

  The entry b_{ij} in the i-th row and j-th column of B is

$$b_{ij} = \sum_{r=1}^{n} f_i(a_r)\overline{f}_j(a_r) = \sum_{i=1}^{n} (f_i\overline{f}_j)(a_r) = \sum_{r=1}^{n} f_k(a_r),$$

  where $f_k = f_i\overline{f}_j = \frac{f_i}{f_j}$.

The Inverse of $A(G)$ (Cont'd)

- For $B = AA^*$, we found

$$b_{ij} = \sum_{r=1}^{n} f_k(a_r),$$

where $f_k = f_i \overline{f}_j = \frac{f_i}{f_j}$.

Now we have $\frac{f_i}{f_j} = f_1$, if, and only if, $i = j$.

Hence, by the preceding theorem,

$$b_{ij} = \begin{cases} n, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

In other words, $B = nI$.

Orthogonality Relations for Characters

Theorem (Orthogonality Relations for Characters)

We have

$$\sum_{r=1}^{n} \overline{f}_r(a_i) f_r(a_j) = \begin{cases} n, & \text{if } a_i = a_j \\ 0, & \text{if } a_i \neq a_j \end{cases}.$$

- The relation $AA^* = nI$ implies $A^*A = nI$.

  The element in the i-th row and j-th column of A^*A is the sum

$$\sum_{r=1}^{n} \overline{f}_r(a_i) f_r(a_j).$$

Comments

- Note that
$$\overline{f}_r(a_i) = f_r(a_i)^{-1} = f_r(a_i^{-1}).$$
- So the general term of the sum $\sum_{r=1}^{n} \overline{f}_r(a_i) f_r(a_j)$ is equal to
$$f_r(a_i^{-1}) f_r(a_j) = f_r(a_i^{-1} a_j).$$
- Therefore, the orthogonality relations can also be expressed as
$$\sum_{r=1}^{n} f_r(a_i^{-1} a_j) = \begin{cases} n, & \text{if } a_i = a_j \\ 0, & \text{if } a_i \neq a_j \end{cases}.$$

Sums of the Characters

- Consider the sum

$$\sum_{r=1}^{n} f_r(a_i^{-1}a_j) = \begin{cases} n, & \text{if } a_i = a_j \\ 0, & \text{if } a_i \neq a_j \end{cases}.$$

- Let a_i be the identity element e in the sum.

Theorem

The sum of the entries in the j-th column of A is given by

$$\sum_{r=1}^{n} f_r(a_j) = \begin{cases} n, & \text{if } a_j = e \\ 0, & \text{otherwise} \end{cases}.$$

Subsection 8

Dirichlet Characters

Residue Classes Modulo k

- Let k be a fixed positive integer.
- Let G be the group of reduced residue classes modulo k.
- Recall that this is a set of $\varphi(k)$ integers $\{a_1, a_2, \ldots, a_{\varphi(k)}\}$ incongruent modulo k, each of which is relatively prime to k.
- For each integer a the corresponding residue class $\widehat{a}$ is the set of all integers congruent to a modulo k:

$$\widehat{a} = \{x : x \equiv a \pmod{k}\}.$$

- Multiplication of residue classes is defined by the relation

$$\widehat{a} \cdot \widehat{b} = \widehat{ab}.$$

- So the product of two residue classes $\widehat{a}$ and $\widehat{b}$ is the residue class of the product ab.

Group of Reduced Residue Classes

Theorem

With multiplication $\widehat{a} \cdot \widehat{b} = \widehat{ab}$ the set of reduced residue classes modulo k is a finite abelian group of order $\varphi(k)$. The identity is the residue class $\widehat{1}$. The inverse of $\widehat{a}$ is the residue class $\widehat{b}$, where $ab \equiv 1 \pmod{k}$.

- The closure property is automatically satisfied because of the way multiplication of residue classes was defined.

  The class $\widehat{1}$ is clearly the identity element.

  If $(a, k) = 1$, there is a unique b, such that $ab \equiv 1 \pmod{k}$.

  Hence the inverse of $\widehat{a}$ is $\widehat{b}$.

  Finally, it is clear that the group is abelian and that its order is $\varphi(k)$.

Dirichlet Characters

Definition (Dirichlet Characters)

Let G be the group of reduced residue classes modulo k. Suppose f is a character of G. Define an arithmetical function $\chi = \chi_f$ as follows:

$$\chi(n) = \begin{cases} f(\widehat{n}), & \text{if } (n,k) = 1, \\ 0, & \text{if } (n,k) > 1. \end{cases}$$

The function χ is called a **Dirichlet character modulo** k.

The **principal character** χ_1 is the one corresponding to f_1, i.e., that which has the properties

$$\chi_1(n) = \begin{cases} 1, & \text{if } (n,k) = 1 \\ 0, & \text{if } (n,k) > 1 \end{cases}$$

Properties of Dirichlet Characters

Theorem

There are $\varphi(k)$ distinct Dirichlet characters modulo k, each of which is completely multiplicative and periodic with period k. That is, we have:

- $\chi(mn) = \chi(m)\chi(n)$, for all m, n;
- $\chi(n+k) = \chi(n)$, for all n.

Conversely, if χ is completely multiplicative and periodic with period k, and if $\chi(n) = 0$, if $(n,k) > 1$, then χ is one of the Dirichlet characters mod k.

- There are $\varphi(k)$ characters f for the group G of reduced residue classes modulo k. Hence, there are $\varphi(k)$ characters χ_f modulo k.

  The multiplicative property of χ_f follows from that of f when both m and n are relatively prime to k.

  If one of m or n is not relatively prime to k then neither is mn. Hence, both $\chi(mn)$ and $\chi(m)\chi(n)$ are zero.

Properties of Dirichlet Characters (Cont'd)

- The periodicity property is a consequence of the following facts:
  - $a \equiv b \pmod{k}$ implies $(a, k) = (b, k)$;
  - $\chi_f(n) = f(\widehat{n})$.

  Conversely, suppose that:
  - χ is completely multiplicative;
  - χ is periodic with period k;
  - $\chi(n) = 0$, if $(n, k) > 1$.

  Let f be the function defined on the group G by the equation

  $$f(\widehat{n}) = \chi(n), \quad \text{if } (n, k) = 1.$$

  Then f is a character of G.

  Consequently, χ is a Dirichlet character mod k.

Examples: $k = 3$ and $k = 4$

- When $k = 1$ or $k = 2$ then $\varphi(k) = 1$.

  So the only Dirichlet character is the principal character χ_1.
- For $k \geq 3$, there are at least two Dirichlet characters since $\varphi(k) \geq 2$.

  The following tables display all the Dirichlet characters for $k = 3, 4$.

n	1	2	3
$\chi_1(n)$	1	1	0
$\chi_2(n)$	1	-1	0

n	1	2	3	4
$\chi_1(n)$	1	0	1	0
$\chi_2(n)$	1	0	-1	0

  To fill these tables we use:
  - $\chi(n)^{\varphi(k)} = 1$, if $(n, k) = 1$. So $\chi(n)$ is a $\varphi(k)$-th root of unity.
  - If χ is a character mod k so is the complex conjugate $\overline{\chi}$.

  This information suffices to complete the tables for k = 3 and k = 4.

Examples: $k = 5$

- The following table displays all the Dirichlet characters for $k = 5$.

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	-1	-1	1	0
$\chi_3(n)$	1	i	$-i$	-1	0
$\chi_4(n)$	1	$-i$	i	-1	0

When $k = 5$ we have:

- $\varphi(5) = 4$. So $\chi(n)$ equals ± 1 or $\pm i$ when $(n, 5) = 1$.
- Also, $\chi(2)\chi(3) = \chi(6) = \chi(1) = 1$.
  So $\chi(2)$ and $\chi(3)$ are reciprocals.
- Finally, $\chi(4) = \chi(2)^2$.

This information suffices to fill the table for $k = 5$.

- As a check we can use the previous theorems which tell us that the sum of the entries is 0 in each row and column except for the first.

Examples: $k = 6$ and $k = 7$

- The following tables display all the Dirichlet characters mod 6 and 7, where $\omega = e^{\pi i/3}$.

n	1	2	3	4	5	6
$\chi_1(n)$	1	0	0	0	1	0
$\chi_2(n)$	1	0	0	0	-1	0

n	1	2	3	4	5	6	7
$\chi_1(n)$	1	1	1	1	1	1	0
$\chi_2(n)$	1	1	-1	1	-1	-1	0
$\chi_3(n)$	1	ω^2	ω	$-\omega$	$-\omega^2$	-1	0
$\chi_4(n)$	1	ω^2	$-\omega$	$-\omega$	ω^2	1	0
$\chi_5(n)$	1	$-\omega$	ω^2	ω^2	$-\omega$	1	0
$\chi_6(n)$	1	$-\omega$	$-\omega^2$	ω^2	ω	-1	0

Orthogonality for Characters Modulo k

Theorem

Let $\chi_1, \ldots, \chi_{\varphi(k)}$ denote the $\varphi(k)$ Dirichlet characters modulo k. Let m and n be two integers, with $(n, k) = 1$. Then we have

$$\sum_{r=1}^{\varphi(k)} \chi_r(m)\overline{\chi}_r(n) = \begin{cases} \varphi(k), & \text{if } m \equiv n \pmod{k} \\ 0, & \text{if } m \not\equiv n \pmod{k} \end{cases}$$

- Suppose, first, $(m, k) = 1$.
  Take $a_i = \widehat{n}$ and $a_j = \widehat{m}$ in the orthogonality relations
  $$\sum_{r=1}^{\varphi(k)} \overline{\chi}_r(\widehat{n})\chi_r(\widehat{m}) = \begin{cases} \varphi(k), & \text{if } \widehat{m} = \widehat{n}, \\ 0, & \text{if } \widehat{m} \neq \widehat{n}. \end{cases}$$
  Suppose, next, that $(m, k) > 1$.
  Then $\chi_r(\widehat{m}) = 0$, for all r, and $m \not\equiv n \pmod{k}$.

Subsection 9

Sums Involving Dirichlet Characters

Sums Involving Dirichlet Characters

Theorem

Let χ be any nonprincipal character modulo k. Let f be a nonnegative function which has a continuous negative derivative $f'(x)$, for all $x \geq x_0$. Then, if $y \geq x \geq x_0$, we have

$$\sum_{x<n\leq y} \chi(n)f(n) = O(f(x)).$$

If, in addition, $f(x) \to 0$ as $x \to \infty$, then the infinite series

$$\sum_{n=1}^{\infty} \chi(n)f(n)$$

converges. Moreover, we have, for $x \geq x_0$,

$$\sum_{n\leq x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + O(f(x)).$$

Sums Involving Dirichlet Characters (Cont'd)

- Let $A(x) = \sum_{n \le x} \chi(n)$.
  By hypothesis, χ is nonprincipal.
  So $A(k) = \sum_{n=1}^{k} \chi(n) = 0$.
  By periodicity, $A(nk) = 0$, for $n = 2, 3, \ldots$.
  Hence, $|A(x)| < \varphi(k)$, for all x.
  So we have $A(x) = O(1)$.

Sums Involving Dirichlet Characters (Cont'd)

- Now we use Abel's Identity to express $\sum_{x<n\leq y}\chi(n)f(n)$ as an integral:

$$\begin{aligned}\sum_{x<n\leq y}\chi(n)f(n) &= f(y)A(y)-f(x)A(x)-\int_x^y A(t)f'(t)dt\\ &= O(f(y))+O(f(x))+O\left(\int_x^y(-f'(t))dt\right)\\ &= O(f(x)).\end{aligned}$$

If $f(x)\to 0$ as $x\to\infty$, by the preceding relation and the Cauchy Convergence Criterion, the series $\sum_{n=1}^{\infty}\chi(n)f(n)$ converges.

To prove the last relation we simply note that

$$\sum_{n=1}^{\infty}\chi(n)f(n)=\sum_{n\leq x}\chi(n)f(n)+\lim_{y\to\infty}\sum_{x<n\leq y}\chi(n)f(n).$$

Since the limit on the right is $O(f(x))$, this completes the proof.

Applications of the Sums

- We apply the preceding theorem successively with $f(x) = \frac{1}{x}$, $f(x) = \frac{\log x}{x}$, and $f(x) = \frac{1}{\sqrt{x}}$, for $x \geq 1$ to obtain:

Theorem

If x is any nonprincipal character mod k and if $x \geq 1$, we have

$$\begin{aligned}
\sum_{n \leq x} \frac{\chi(n)}{n} &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + O\left(\frac{1}{x}\right), \\
\sum_{n \leq x} \frac{\chi(n) \log n}{n} &= \sum_{n=1}^{\infty} \frac{\chi(n) \log n}{n} + O\left(\frac{\log x}{x}\right), \\
\sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} &= \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}}\right).
\end{aligned}$$

Subsection 10

The Nonvanishing of $L(1,\chi)$ for Real Nonprincipal χ

Divisor Sum of Real Characters

- We denote by $L(1,\chi)$ the sum

$$L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}.$$

Theorem

Let χ be any real-valued character mod k and let

$$A(n) = \sum_{d|n} \chi(d).$$

Then $A(n) \geq 0$, for all n, and $A(n) \geq 1$ if n is a square.

Divisor Sum of Real Characters (Cont'd)

- For prime powers we have

$$A(p^a) = \sum_{t=0}^{a} \chi(p^t) = 1 + \sum_{t=1}^{a} \chi(p)^t.$$

By hypothesis, χ is real-valued.

So the only possible values for $\chi(p)$ are 0, 1 and -1.

  - If $\chi(p) = 0$ then $A(p^a) = 1$.
  - If $\chi(p) = 1$ then $A(p^a) = a + 1$.
  - If $\chi(p) = -1$, then $A(p^a) = \begin{cases} 0, & \text{if } a \text{ is odd} \\ 1, & \text{if } a \text{ is even} \end{cases}$.

In any case, $A(p^a) \geq 1$ if a is even.

Divisor Sum of Real Characters (Cont'd)

- We showed $A(p^a) \geq 1$, if a is even.

  Now if $n = p_1^{a_1} \cdots p_r^{a_r}$, by multiplicativity,

  $$A(n) = A(p_1^{a_1}) \cdots A(p_r^{a_r}).$$

  Each factor $A(p_i^{a_i}) \geq 0$.

  Hence $A(n) \geq 0$.

  If n is a square then each exponent a_i is even.

  So each factor $A(p_i^{a_i}) \geq 1$.

  Hence $A(n) \geq 1$.

  This proves the theorem.

Value of $L(1,\chi)$

Theorem

For any real-valued nonprincipal character x mod k, let

$$A(n) = \sum_{d|n} \chi(d) \quad \text{and} \quad B(x) = \sum_{n \le x} \frac{A(n)}{\sqrt{n}}.$$

Then we have:

(a) $B(x) \to \infty$ as $x \to \infty$.

(b) $B(x) = 2\sqrt{x} L(1,\chi) + O(1)$, for all $x \ge 1$.

Therefore, $L(1,\chi) \neq 0$.

Value of $L(1,\chi)$ (Parts (a) and (b))

(a) Use the preceding theorem to write

$$B(x) \geq \sum_{\substack{n \leq x \\ n=m^2}} \frac{1}{\sqrt{n}} = \sum_{m \leq \sqrt{x}} \frac{1}{m}.$$

The last sum tends to ∞ as $x \to \infty$ since the series $\sum \frac{1}{m}$ diverges.

(b) We write

$$B(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} \sum_{d|n} \chi(d) = \sum_{\substack{q,d \\ qd \leq x}} \frac{\chi(d)}{\sqrt{dq}}.$$

Value of $L(1,\chi)$ (Part (b) Cont'd)

- Use generalized partial sums of Dirichlet products,

$$\sum_{\substack{q,d \\ qd\le x}} f(d)g(q) = \sum_{n\le a} f(n)G\left(\frac{x}{n}\right) + \sum_{n\le b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b),$$

  where $ab=x$, $F(x)=\sum_{n\le x} f(n)$ and $G(x)=\sum_{n\le x} g(n)$.

  Take $a=b=\sqrt{x}$ and let:
  - $f(n)=\frac{\chi(n)}{\sqrt{n}}$;
  - $g(n)=\frac{1}{\sqrt{n}}$.

  We obtain

$$\begin{array}{rcl} B(x) & = & \sum_{\substack{q,d \\ qd\le x}} \frac{\chi(d)}{\sqrt{qd}} \\ & = & \sum_{n\le\sqrt{x}} \frac{\chi(n)}{\sqrt{n}} G(\frac{x}{n}) + \sum_{n\le\sqrt{x}} \frac{1}{\sqrt{n}} F(\frac{x}{n}) - F(\sqrt{x})G(\sqrt{x}). \end{array}$$

Value of $L(1,\chi)$ (Part (b) Cont'd)

- We know that
  - $G(x)=\sum_{n\le x}\frac{1}{\sqrt{n}}=2\sqrt{x}+A+O(\frac{1}{\sqrt{x}})$, where A is a constant;
  - $F(x)=\sum_{n\le x}\frac{\chi(n)}{\sqrt{n}}=B+O(\frac{1}{\sqrt{x}})$, where $B=\sum_{n=1}^{\infty}\frac{\chi(n)}{\sqrt{n}}$.

  Since $F(\sqrt{x})G(\sqrt{x})=2Bx^{1/4}+O(1)$, we now get

$$\begin{aligned}
B(x) &= \sum_{n\le\sqrt{x}}\frac{\chi(n)}{\sqrt{n}}\{2\sqrt{\frac{x}{n}}+A+O(\sqrt{\frac{n}{x}})\} \\
&\qquad +\sum_{n\le\sqrt{x}}\frac{1}{\sqrt{n}}\{B+O(\sqrt{\frac{n}{x}})\}-2Bx^{1/4}+O(1) \\
&= 2\sqrt{x}\sum_{n\le\sqrt{x}}\frac{\chi(n)}{n}+A\sum_{n\le\sqrt{x}}\frac{\chi(n)}{\sqrt{n}}+O(\frac{1}{\sqrt{x}}\sum_{n\le\sqrt{x}}|\chi(n)|) \\
&\qquad +B\sum_{n\le\sqrt{x}}\frac{1}{\sqrt{n}}+O(\frac{1}{\sqrt{x}}\sum_{n\le\sqrt{x}}1)-2Bx^{1/4}+O(1) \\
&= 2\sqrt{x}L(1,\chi)+O(1).
\end{aligned}$$

  Parts (a) and (b) together imply that $L(1,\chi)\neq 0$.