Analytic Number Theory
Lecture 6

Mariusz Mirek
Rutgers University

Padova, March 27, 2025.

Supported by the NSF grant DMS-2154712,
and the CAREER grant DMS-2236493.

Index with respect to the primitive roots

Example

The following table lists the primitive roots for the first six primes.

p	$\varphi(p-1)$	primitive roots
2	1	1
3	1	2
5	2	2,3
7	2	3,5
11	4	2, 6, 7, 8
13	4	2, 6, 7, 11

Index with respect to the primitive roots

- Let $p \in \mathbb{P}$ be a prime, and let g be a primitive root modulo p. If $a \in \mathbb{Z}$ is not divisible by p, then there is a unique $k \in \{0, 1, \ldots, p-2\}$ so that

$$a \equiv g^k \pmod{p}.$$

- This integer k is called the index of a with respect to the primitive root g, and is denoted by $k = \operatorname{ind}_g(a)$.

Properties of the index

- If $k_1, k_2 \in \mathbb{Z}$ are such that $k_1 \leq k_2$ and
$$a \equiv g^{k_1} \equiv g^{k_2} \pmod{p},$$
then
$$g^{k_2 - k_1} \equiv 1 \pmod{p},$$
and since g is a primitive root and $\varphi(p) = p - 1$, thus
$$k_1 \equiv k_2 \pmod{p-1}.$$
- If $a \equiv g^k \pmod{p}$ and $b \equiv g^l \pmod{p}$, then
$$ab \equiv g^k g^l = g^{k+l} \pmod{p}$$
and so
$$\mathrm{ind}_g(ab) \equiv k + l \equiv \mathrm{ind}_g(a) + \mathrm{ind}_g(b) \pmod{p-1}.$$
- The index map ind_g is also called the discrete logarithm to the base g modulo p.

Example

- For example, 2 is a primitive root modulo 13. Here is a table of $\mathrm{ind}_2(a)$ for $a \in [12]$:

a	$\mathrm{ind}_2(a)$	a	$\mathrm{ind}_2(a)$
1	0	7	11
2	1	8	3
3	4	9	8
4	2	10	10
5	9	11	7
6	5	12	6

- By the structure theorem of subgroups in cyclic groups, if g is a primitive root modulo p, then g^k is a primitive root iff $(k, p-1) = 1$.
- For example, for $p = 13$ there are $\varphi(12) = 4$ integers k such that $0 \leq k \leq 11$ and $(k, 12) = 1$, namely, $k = 1, 5, 7, 11$, and so the four pairwise incongruent primitive roots modulo 13 are

$$2^1 \equiv 2 \pmod{13},$$
$$2^5 \equiv 6 \pmod{13},$$
$$2^7 \equiv 11 \pmod{13},$$
$$2^{11} \equiv 7 \pmod{13}.$$

Power residues

- Let $a, k, m \in \mathbb{Z}$ be integers such that $m \geq 2, k \geq 2$, and $(a, m) = 1$. We say that a is a k-th power residue modulo m if there exists an $x \in \mathbb{Z}$ such that
$$x^k \equiv a \pmod{m}.$$
- If this congruence has no solution, then a is called a k-th power nonresidue modulo m.
- Let $k = 2$ and $(a, m) = 1$. If the congruence $x^2 \equiv a \pmod{m}$ is solvable, then a is called a quadratic residue modulo m. Otherwise, a is called a quadratic nonresidue modulo m.
- For example, the quadratic residues modulo 7 are $1, 2$, and 4; the quadratic nonresidues are $3, 5$, and 6. The only quadratic residue modulo 8 is 1, and the quadratic nonresidues modulo 8 are $3, 5, 4$ and 7.
- Let $k = 3$ and $(a, m) = 1$. If the congruence $x^3 \equiv a \pmod{m}$ is solvable, then a is called a cubic residue modulo m. Otherwise, a is called a cubic nonresidue modulo m.
- For example, the cubic residues modulo 7 are 1 and 6; the cubic nonresidues are $2, 3, 4$, and 5. The cubic residues modulo 5 are $1, 2, 3$, and 4; there are no cubic nonresidues modulo 5.

Power residues modulo primes

Theorem

Let $p \in \mathbb{P}$ be a prime number, $k \geq 2$, and $d = (k, p-1)$. Let $a \in \mathbb{Z}$ be not divisible by p. Let g be a primitive root modulo p.

- *Then a is a k-th power residue modulo p if and only if*

  $$\mathrm{ind}_g(a) \equiv 0 \pmod{d},$$

  if and only if

  $$a^{(p-1)/d} \equiv 1 \pmod{p}.$$

- *If a is a k-th power residue modulo p, then the congruence*

  $$x^k \equiv a \pmod{p} \tag{*}$$

  has exactly d solutions that are pairwise incongruent modulo p.

- *Moreover, there are exactly $(p-1)/d$ pairwise incongruent k-th power residues modulo p.*

Proof

- Let $l = \mathrm{ind}_g(a)$, where g is a primitive root modulo p. Congruence (*) is solvable if and only if there exists $y \in \mathbb{Z}$ such that
$$g^y \equiv x \pmod{p} \quad \text{and} \quad g^{ky} \equiv x^k \equiv a \equiv g^l \pmod{p}.$$
- This is equivalent to $ky \equiv l \pmod{p-1}$, since $\mathrm{ord}_p(g) = p - 1$.
- This linear congruence in y has a solution if and only if
$$\mathrm{ind}_g(a) = l \equiv 0 \pmod{d}, \quad \text{where} \quad d = (k, p-1).$$
- Thus, the k-th power residues modulo p are precisely the integers in the $(p-1)/d$ congruence classes $g^{id} + p\mathbb{Z}$ for $i \in \{0, 1, \dots, (p-1)/d - 1\}$.
- Moreover,
$$a^{(p-1)/d} \equiv g^{(p-1)l/d} \equiv 1 \pmod{p}$$
if and only if
$$\frac{(p-1)l}{d} \equiv 0 \pmod{p-1} \quad \iff \quad \mathrm{ind}_g(a) = l \equiv 0 \pmod{d}$$
- Finally, if the linear congruence $ky \equiv l \pmod{p-1}$ is solvable, then it has exactly d solutions y that are pairwise incongruent modulo $p - 1$, and so (*) has exactly d solutions $x = g^y$ that are pairwise incongruent modulo p. This completes the proof. □

Examples

- For example, let $p = 19$ and $k = 3$. Then $d = (k, p-1) = (3, 18) = 3$.
- We can check that 2 is a primitive root modulo 19, and so a is a cubic residue modulo 19 if and only if 3 divides $\operatorname{ind}_2(a)$.
- Since $-1 \equiv 2^9 \pmod{3}$ and $\operatorname{ind}_2(-1) = 9$, it follows that -1 is a cubic residue modulo 19.
- The solutions of the congruence $x^3 \equiv -1 \pmod{19}$ are of the form $x \equiv 2^y \pmod{19}$, where $0 \leq y \leq 17$ and $3y \equiv 9 \pmod{18}$. Then $y \equiv 3 \pmod{6}$, and so $y = 3, 9,$ and 15. These give the following three cube roots of -1 modulo 19:

$$
\begin{aligned}
8 &\equiv 2^3 \pmod{19}, \\
18 &\equiv 2^9 \pmod{19}, \\
12 &\equiv 2^{15} \pmod{19}.
\end{aligned}
$$

Corollary

Let $p \in \mathbb{P}$ be an odd prime number, and let $k \geq 2$ be an integer such that $(k, p-1) = 1$. If $(a, p) = 1$, then a is a k-th power residue modulo p, and the congruence $x^k \equiv a \pmod{p}$ has a unique solution modulo p.

Quadratic residues

- Let $p \in \mathbb{P}$ be an odd prime and $a \in \mathbb{Z}$ not divisible by p. Then a is called a quadratic residue modulo p if there exists $x \in \mathbb{Z}$ such that
$$x^2 \equiv a \pmod{p}. \tag{*}$$
- If this congruence has no solution, then a is called a quadratic nonresidue modulo p. Thus, an integer a is a quadratic residue modulo p if and only if $(a, p) = 1$ and a has a square root modulo p. By the previous theorem, exactly half the congruence classes relatively prime to p have square roots modulo p.
- We define the Legendre symbol for the odd prime p as follows: For any integer a we set
$$(a \mid p) = \begin{cases} 1 \text{ if } (a,p) = 1 \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1 \text{ if } (a,p) = 1 \text{ and } a \text{ is a quadratic nonresidue modulo } p, \\ 0 \text{ if } p \text{ divides } a. \end{cases}$$
- The solvability of congruence (*) depends only on the congruence class of $a \pmod{p}$, that is,
$$(a \mid p) = (b \mid p) \quad \text{if} \quad a \equiv b \pmod{p},$$
and so the Legendre symbol is a well-defined function on the congruence classes $\mathbb{Z}/p\mathbb{Z}$.

Legendre symbol: simple calculations

- We observe that if $p \in \mathbb{P}$ is an odd prime, then, the only solutions of the congruence $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1 \pmod{p}$.
- If $\varepsilon, \varepsilon' \in \{-1, 0, 1\}$ and $\varepsilon \equiv \varepsilon' \pmod{p}$, then $p \mid (\varepsilon - \varepsilon')$, and so $\varepsilon = \varepsilon'$. In particular, if $(a \mid p) \equiv \varepsilon \pmod{p}$, then $(a \mid p) = \varepsilon$.

Theorem

Let $p \in \mathbb{P}$ be an odd prime. For every integer $a \in \mathbb{Z}$, we have

$$(a \mid p) \equiv a^{(p-1)/2} \pmod{p}.$$

Proof.

- If $p \mid a$, then both sides of the congruence are 0.
- If p does not divide a, then, by Fermat's theorem, we have $\left(a^{(p-1)/2}\right)^2 \equiv a^{p-1} \equiv 1 \pmod{p}$ and so $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.
- Applying the previous theorem with $k = 2$, we have

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \text{if and only if} \quad (a \mid p) = 1,$$

  and consequently we must have

$$a^{(p-1)/2} \equiv -1 \pmod{p} \quad \text{if and only if} \quad (a \mid p) = -1.$$

This completes the proof. □

Legendre symbol is completely multiplicative

Theorem

Let $p \in \mathbb{P}$ be an odd prime, and let $a, b \in \mathbb{Z}$. Then $(ab \mid p) = (a \mid p)(b \mid p)$.

Proof.

- If p divides a or b, then p divides ab, and

$$(ab \mid p) = 0 = (a \mid p)(b \mid p).$$

- If p does not divide ab, then, by the previous theorem, we obtian

$$\begin{aligned} (ab \mid p) &\equiv (ab)^{(p-1)/2} \pmod{p} \\ &\equiv a^{(p-1)/2} b^{(p-1)/2} \pmod{p} \\ &(a \mid p)(b \mid p) \pmod{p}. \end{aligned}$$

- The result follows immediately from the observation that each side of this congruence is ± 1. See the remark before the previous theorem.

This completes the proof of the theorem. □

Legendre symbol: specific calculations for $(-1 \mid p)$

- Previous theorem implies that the Legendre symbol $(\cdot \mid p)$ is completely determined by its values at $-1, 2$, and odd primes q.
- If a is an integer not divisible by p, then we can write

  $$a = \pm 2^{r_0} q_1^{r_1} q_2^{r_2} \cdots q_k^{r_k},$$

  where $q_1, \ldots, q_k$ are distinct odd primes not equal to p. Then

  $$(a \mid p) = (\pm 1 \mid p)(2 \mid p)^{r_0}(q_1 \mid p)^{r_1} \cdots (q_k \mid p)^{r_k}.$$

Theorem

Let $p \in \mathbb{P}$ be an odd prime number. Then

$$(-1 \mid p) = \begin{cases} 1 & \textit{if} \quad p \equiv 1 \pmod 4, \\ -1 & \textit{if} \quad p \equiv 3 \pmod 4. \end{cases}$$

Equivalently,

$$(-1 \mid p) = (-1)^{(p-1)/2}.$$

Legendre symbol: specific calculations for $(2 \mid p)$

Proof.

- We observe that

$$(-1)^{(p-1)/2} = \begin{cases} 1 & \text{if} \quad p \equiv 1 \pmod 4, \\ -1 & \text{if} \quad p \equiv 3 \pmod 4. \end{cases}$$

- By the previous theorem with $a = -1$, we obtain

$$(-1 \mid p) \equiv (-1)^{(p-1)/2} \pmod p.$$

This completes the proof, since both sides of this congruence are ± 1. □

Theorem

Let $p \in \mathbb{P}$ be an odd prime. Then

$$(2 \mid p) = \begin{cases} 1 & \textit{if } p \equiv \pm 1 \pmod 8, \\ -1 & \textit{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Equivalently,

$$(2 \mid p) = (-1)^{(p^2-1)/8}.$$

Proof

- Consider the following congruences:

$$\begin{aligned} p-1 &\equiv 1(-1)^1 \pmod{p}, \\ 2 &\equiv 2(-1)^2 \pmod{p}, \\ p-3 &\equiv 3(-1)^3 \pmod{p}, \\ 4 &\equiv 4(-1)^4 \pmod{p}, \\ &\vdots \\ r &\equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \pmod{p}, \end{aligned}$$

  where $r = p - \frac{p-1}{2}$ or $r = \frac{p-1}{2}$.

- Multiply both sides by each integer on the left, which is even. Then

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+\ldots+\frac{(p-1)}{2}} \pmod{p},$$

  or equivalently $2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{\frac{(p^2-1)}{8}} \pmod{p}$.

- Since $\left(\frac{p-1}{2}\right)! \not\equiv 0 \pmod{p}$ we obtain $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{(p^2-1)}{8}} \pmod{p}$

- By Euler's criterion, $(2 \mid p) = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{(p^2-1)}{8}} \pmod{p}$ as desired. □

Gaussian sets modulo p

- Let $p \in \mathbb{P}$ be an odd prime, and let S be a set of $(p-1)/2$ integers. We call S a Gaussian set modulo p if $S \cup -S = S \cup \{-s : s \in S\}$ is a reduced system of residues modulo p.
- Equivalently, S is a Gaussian set if for every integer a not divisible by p, there exist unique $s \in S$ and $\varepsilon \in \{1, -1\}$ such that $a \equiv \varepsilon s \pmod{p}$.
- For example, the sets $\{1, 2, \ldots, (p-1)/2\}$ and $\{2, 4, 6, \ldots, p-1\}$ are Gaussian sets modulo p for every odd prime $p \in \mathbb{P}$.
- If S is a Gaussian set, $s, s' \in S$, and $s \equiv \pm s' \pmod{p}$, then $s = s'$.

Lemma (Gauss lemma)

Let $p \in \mathbb{P}$ be an odd prime, and let $a \in \mathbb{Z}$ be not divisible by p. Let S be a Gaussian set modulo p. For every $s \in S$ there exist unique integers $u_a(s) \in S$ and $\varepsilon_a(s) \in \{1, -1\}$ such that

$$as \equiv \varepsilon_a(s) u_a(s) \pmod{p}.$$

Moreover,

$$(a \mid p) = \prod_{s \in S} \varepsilon_a(s) = (-1)^m,$$

where m is the number of $s \in S$ such that $\varepsilon_a(s) = -1$.

Proof

- Since S is a Gaussian set, for every $s \in S$ there exist unique integers $u_a(s) \in S$ and $\varepsilon_a(s) \in \{1, -1\}$ such that $as \equiv \varepsilon_a(s) u_a(s) \pmod{p}$.
- We show that $s \mapsto u_a(s)$ is one-to-one. Indeed, if $u_a(s) = u_a(s')$ for some $s, s' \in S$, then

$$\begin{aligned} as' &\equiv \varepsilon_a(s') u_a(s') \equiv \varepsilon_a(s') u_a(s) \pmod{p} \\ &\equiv \varepsilon_a(s') \varepsilon_a(s) \varepsilon_a(s) u_a(s) \pmod{p} \equiv \pm as \pmod{p}. \end{aligned}$$

- Dividing by a, we obtain $s' \equiv \pm s \pmod{p}$ and so $s' = s$. It follows that the map $u_a : S \to S$ is a permutation of S, and so $\prod_{s \in S} s = \prod_{s \in S} u_a(s)$.
- Therefore,

$$\begin{aligned} a^{(p-1)/2} \prod_{s \in S} s \equiv \prod_{s \in S} as \pmod{p} &\equiv \prod_{s \in S} \varepsilon_a(s) u_a(s) \pmod{p} \\ &\equiv \prod_{s \in S} \varepsilon_a(s) \prod_{s \in S} u_a(s) \pmod{p} \\ &\equiv \prod_{s \in S} \varepsilon_a(s) \prod_{s \in S} s \pmod{p} \end{aligned}$$

- Dividing by $\prod_{s \in S} s$, the proof follows, as we obtain

$$(a \mid p) \equiv a^{(p-1)/2} \equiv \prod_{s \in S} \varepsilon_a(s) \pmod{p}. \qquad \square$$

Example

- We shall use Gauss's lemma to compute the Legendre symbol $(3 \mid 11)$.
- Let S be the Gaussian set $\{2, 4, 6, 8, 10\}$. We have

$$\begin{aligned}
3 \cdot 2 &\equiv 6 \pmod{11}, \\
3 \cdot 4 &\equiv (-1)10 \pmod{11}, \\
3 \cdot 6 &\equiv (-1)4 \pmod{11}, \\
3 \cdot 8 &\equiv 2 \pmod{11}, \\
3 \cdot 10 &\equiv 8 \pmod{11}.
\end{aligned}$$

- The number of $s \in S$ with $\varepsilon_3(s) = -1$ is $m = 2$, and so

$$(3 \mid 11) = (-1)^2 = 1,$$

  that is, 3 is a quadratic residue modulo 11.
- There are exactly two incongruent solutions of $x^2 \equiv 3 \pmod{11}$, namely

$$5^2 \equiv 6^2 \equiv 3 \pmod{11}.$$

  and so 5 and 6 are the square roots of 3 modulo 11.

Basic definitions

- Let $\mathbb{G}$ be a finite abelian group, written additively, and let $A_1, \ldots, A_k \subseteq \mathbb{G}$. The sum of these sets is the set

  $$A_1 + \cdots + A_k = \{a_1 + \cdots + a_k : a_i \in A_i \text{ for } i \in [k]\} .$$

- If $\mathbb{G}_1, \ldots, \mathbb{G}_k$ are subgroups of $\mathbb{G}$, then the sumset $\mathbb{G}_1 + \cdots + \mathbb{G}_k$ is a subgroup of $\mathbb{G}$.
- We say that $\mathbb{G}$ is the direct sum of the subgroups $\mathbb{G}_1, \ldots, \mathbb{G}_k$, written $\mathbb{G} = \mathbb{G}_1 \oplus \cdots \oplus \mathbb{G}_k$, if every element $g \in \mathbb{G}$ can be written uniquely in the form $g = g_1 + \cdots + g_k$, where $g_i \in \mathbb{G}_i$ for $i \in [k]$.
- If $\mathbb{G} = \mathbb{G}_1 \oplus \cdots \oplus \mathbb{G}_k$, then $|\mathbb{G}| = |\mathbb{G}_1| \cdots |\mathbb{G}_k|$.
- The order of an element g in an additive group is the smallest positive integer $d \in \mathbb{Z}_+$ such that $dg = 0$. We know that d divides $|\mathbb{G}|$.
- Let $p \in \mathbb{P}$ be a prime number. A p-group is a group each of whose elements has an order that is a power of p.
- For every prime number $p \in \mathbb{P}$, let

  $$\mathbb{G}(p) := \{g \in \mathbb{G} : \mathrm{ord}_{\mathbb{G}}(g) = p^l \text{ for some } l \in \mathbb{Z}_+\}.$$

  Then $\mathbb{G}(p)$ is a subgroup of the abelian group $\mathbb{G}$.

The structure of finite Abelian groups

Theorem (Structure theorem for finite Abelian groups)

Every finite abelian group is a direct sum of cyclic groups.

This result will be a consequence of the next two theorems.

Theorem

Let $\mathbb{G}$ be a finite abelian group, written additively, and let $|\mathbb{G}| = m$. For every prime number $p \in \mathbb{P}$, let $\mathbb{G}(p)$ be the set of all elements $g \in \mathbb{G}$ whose order is a power of p. Then

$$\mathbb{G} = \bigoplus_{p|m} \mathbb{G}(p).$$

Proof.

- Let $m = \prod_{i\in[k]} p_i^{r_i}$, and define $m_i = mp_i^{-r_i}$ for $i \in [k]$.
- Then $(m_1, \ldots, m_k) = 1$, and by the GCD theorem there exist $u_1, \ldots, u_k \in \mathbb{Z}$ such that $m_1u_1 + \cdots + m_ku_k = 1$.
- Let $g \in \mathbb{G}$, and define $g_i = m_iu_ig \in \mathbb{G}$ for $i \in [k]$. Since $p_i^{r_i} g_i = mu_ig = 0$, it follows that $g_i \in \mathbb{G}(p_i)$. Moreover,

$$\begin{aligned} g &= (m_1u_1 + \cdots + m_ku_k)\, g = m_1u_1g + \cdots + m_ku_kg \\ &= g_1 + \cdots + g_k \in \mathbb{G}(p_1) + \cdots + \mathbb{G}(p_k). \end{aligned}$$

Proof

- Thus we have proved that $\mathbb{G} = \mathbb{G}\left(p_1\right) + \cdots + \mathbb{G}\left(p_k\right)$.
- Suppose that
$$g_1 + \cdots + g_k = 0,$$
where $g_i \in \mathbb{G}\left(p_i\right)$ for $i \in [k]$.
- There exist $r_1, \ldots, r_k \in \mathbb{N}$ such that g_i has order $p_i^{r_i}$ for $i \in [k]$. Let
$$d_j = \prod_{\substack{i \in [k] \\ i \neq j}} p_i^{r_i}.$$
- Since $d_j g_i = 0$ for $i \in [k]$ with $i \neq j$, it follows that
$$0 = d_j\left(g_1 + \cdots + g_k\right) = d_j g_j.$$
- We proved that $d_j g_j = 0$ for all $j \in [k]$, thus $p_j^{r_j} \mid d_j$, but $\left(p_j^{r_j}, d_j\right) = 1$, which is only possible when $r_1 = \ldots = r_k = 0$
- Hence, $g_j = 0$ for all $j \in [k]$.
- Thus, 0 has no nontrivial representation in $\mathbb{G} = \mathbb{G}\left(p_1\right) + \cdots + \mathbb{G}\left(p_k\right)$.
- We conclude that $\mathbb{G}$ is the direct sum of the subgroups $\mathbb{G}\left(p_i\right)$. □

Useful lemma

Lemma

Let $\mathbb{G}$ be a finite abelian p-group. Let $g_1 \in \mathbb{G}$ be an element of maximum order p^{r_1}, and let $\mathbb{G}_1 = \langle g_1 \rangle$ be the cyclic subgroup generated by g_1. Let $h \in \mathbb{G}$ and suppose that $h + \mathbb{G}_1 \in \mathbb{G}/\mathbb{G}_1$ has order p^r, then there exists an element $g \in \mathbb{G}$ such that $g + \mathbb{G}_1 = h + \mathbb{G}_1$ and g has order p^r in $\mathbb{G}$.

Proof.

- If $h + \mathbb{G}_1$ has order p^r in $\mathbb{G}/\mathbb{G}_1$, then the order of h in $\mathbb{G}$ is at most p^{r_1} (since p^{r_1} is the maximum order in $\mathbb{G}$) and at least p^r.
- Since $\mathbb{G}_1 = p^r\left(h + \mathbb{G}_1\right) = p^r h + \mathbb{G}_1$, it follows that $p^r h \in \mathbb{G}_1$, and so $p^r h = u g_1$ for some positive integer $u \leq p^{r_1}$ (since g_1 has order p^{r_1}).
- Write $u = p^s v$, where $(p, v) = 1$ and $0 \leq s \leq r_1$. Then $v g_1$ also has order p^{r_1}, and so $p^s v g_1$ has order $p^{r_1 - s}$ in $\mathbb{G}$. Then $p^r h = p^s v g_1$ has order $p^{r_1 - s}$ in $\mathbb{G}$, and so h has order $p^{r_1 + r - s} \leq p^{r_1}$. It follows that $r \leq s$, and

$$p^r h = p^s v g_1 = p^r\left(p^{s-r} v g_1\right) = p^r g_1',$$

  where $g_1' = p^{s-r} v g_1 \in \mathbb{G}_1$. Taking $g = h - g_1'$, we see $g + \mathbb{G}_1 = h + \mathbb{G}_1$.
- Moreover, $p^r g = p^r h - p^r g_1' = 0$, and so the order of g is at most p^r. On the other hand, $g + \mathbb{G}_1$ has order p^r in the quotient group $\mathbb{G}/\mathbb{G}_1$, and so the order of g is at least p^r. Therefore, g has order p^r as desired. □

Structure of finite abelian p-groups

Theorem

Every finite abelian p-group is a direct sum of cyclic groups.

Proof.

- The proof is by induction on the cardinality of $\mathbb{G}$. Let $\mathbb{G}$ be a finite abelian p-group. If $\mathbb{G}$ is cyclic, we are done. If $\mathbb{G}$ is not cyclic, let $g_1 \in \mathbb{G}$ be an element of maximum order p^{r_1}, and let $\mathbb{G}_1 := \langle g_1 \rangle$.
- The quotient group $\mathbb{G}/\mathbb{G}_1$ is a finite abelian p-group, and

$$1 < |\mathbb{G}/\mathbb{G}_1| = \frac{|\mathbb{G}|}{p^{r_1}} < |\mathbb{G}|$$

- Therefore, the induction hypothesis holds for $\mathbb{G}/\mathbb{G}_1$, and so

$$\mathbb{G}/\mathbb{G}_1 = \mathbb{H}_2 \oplus \cdots \oplus \mathbb{H}_k$$

  where $\mathbb{H}_i$ is a cyclic subgroup of $\mathbb{G}/\mathbb{G}_1$ of order p^{r_i} for $i \in [k] \setminus \{1\}$.
- Moreover,

$$\frac{|\mathbb{G}|}{p^{r_1}} = |\mathbb{G}/\mathbb{G}_1| = \prod_{i=2}^{k} p^{r_i}$$

Proof

- By the previous lemma, for each $i \in [k] \setminus \{1\}$ there exists $g_i \in \mathbb{G}$ such that $g_i + \mathbb{G}_1$ generates $\mathbb{H}_i$ and $\operatorname{ord}_{\mathbb{G}}(g_i) = p^{r_i}$. Let $\mathbb{G}_i := \langle g_i \rangle$.
- Then $|\mathbb{G}_i| = p^{r_i}$ for $i \in [k]$. We shall prove that $\mathbb{G} = \mathbb{G}_1 \oplus \cdots \oplus \mathbb{G}_k$.
- We begin by showing that $\mathbb{G} = \mathbb{G}_1 + \cdots + \mathbb{G}_k$. If $g \in \mathbb{G}$, then $g + \mathbb{G}_1 \in \mathbb{G}/\mathbb{G}_1$, and there exist $u_2, \ldots, u_k \in \mathbb{Z}$ such that $0 \leq u_i \leq p^{r_i} - 1$ for each $i \in [k] \setminus \{1\}$, and

  $$g+\mathbb{G}_1 = u_2\left(g_2 + \mathbb{G}_1\right)\oplus\cdots\oplus u_k\left(g_k + \mathbb{G}_1\right) = \left(u_2 g_2 + \cdots + u_k g_k\right)+\mathbb{G}_1.$$

- It follows that we can find $u_1 \in \mathbb{Z}$ such that $0 \leq u_1 \leq p^{r_1} - 1$ and

  $$g - \left(u_2 g_2 + \cdots + u_k g_k\right) = u_1 g_1 \in \mathbb{G}_1,$$

  and so

  $$g = u_1 g_1 + u_2 g_2 + \cdots + u_k g_k \in \mathbb{G}_1 + \cdots + \mathbb{G}_k.$$

- Therefore, $\mathbb{G} = \mathbb{G}_1 + \cdots + \mathbb{G}_k$. Since

  $$|\mathbb{G}| = |\mathbb{G}_1 + \cdots + \mathbb{G}_k| \leq |\mathbb{G}_1| \cdots |\mathbb{G}_k| = \prod_{i=1}^{k} p^{r_i} = |\mathbb{G}|$$

  it follows that every element of $\mathbb{G}$ has a unique representation as an element in the sumset $\mathbb{G}_1 + \cdots + \mathbb{G}_k$, and so $\mathbb{G} = \mathbb{G}_1 \oplus + \cdots + \oplus \mathbb{G}_k$.
- This completes the proof. □

Characters of finite Abelian groups

- Let $\mathbb{G}$ be a finite abelian group, written additively. A group character is a homomorphism $\chi : \mathbb{G} \to \mathbb{C}^\times$, where $\mathbb{C}^\times$is the multiplicative group of nonzero complex numbers.
- Then $\chi(0) = 1$ and $\chi\left(g_1 + g_2\right) = \chi\left(g_1\right)\chi\left(g_2\right)$ for all $g_1, g_2 \in \mathbb{G}$.
- If χ is a character of a multiplicative group $\mathbb{G}$, then $\chi(1) = 1$ and $\chi\left(g_1 g_2\right) = \chi\left(g_1\right)\chi\left(g_2\right)$ for all $g_1, g_2 \in \mathbb{G}$.
- We define the character χ_0 on $\mathbb{G}$ by $\chi_0(g) = 1$ for all $g \in \mathbb{G}$. If $\mathbb{G}$ is an additive group of order n and if $g \in \mathbb{G}$ has order d, then

  $$\chi(g)^d = \chi(dg) = \chi(0) = 1,$$

  and so $\chi(g)$ is a d-th root of unity, and also $\chi(g)$ is an n-th root of unity for every $g \in \mathbb{G}$, since $d \mid n$. Hence, we have $|\chi(g)| = 1$ for all $g \in \mathbb{G}$.
- We define the product of two characters χ_1 and χ_2 by

  $$\chi_1\chi_2(g) = \chi_1(g)\chi_2(g) \quad \text{for all} \quad g \in \mathbb{G}.$$

  In is not difficult to see that this product is associative and commutative.
- The character χ_0 is a multiplicative identity, since

  $$\chi_0\chi(g) = \chi_0(g)\chi(g) = \chi(g)$$

  for every character χ and $g \in \mathbb{G}$.

Characters of finite Abelian groups

- The inverse of the character χ is the character χ^{-1} defined by
$$\chi^{-1}(g) = \chi(-g),$$
and indeed we have $\chi\chi^{-1} = \chi_0$, since
$$\begin{aligned}\chi\chi^{-1}(g) &= \chi(g)\chi^{-1}(g) = \chi(g)\chi(-g) \\ &= \chi(g-g) = \chi(0) = 1 \\ &= \chi_0(g).\end{aligned}$$
- The complex conjugate of a character χ is the character $\bar{\chi}$ defined by
$$\overline{\chi}(g) = \overline{\chi(g)}.$$
Since $|\chi(g)| = 1$ for all $g \in \mathbb{G}$, we have
$$\chi\overline{\chi}(g) = \chi(g)\overline{\chi}(g) = |\chi(g)|^2 = 1 = \chi_0(g),$$
and so for every character χ and all $g \in \mathbb{G}$ we have
$$\chi^{-1}(g) = \overline{\chi}(g).$$
- It follows that the set $\widehat{\mathbb{G}}$ of all characters of a finite abelian group $\mathbb{G}$ is an abelian group, called the dual group or character group of $\mathbb{G}$.
- We prove that $\mathbb{G}$ is isomorphic to $\widehat{\mathbb{G}}$ for every finite abelian group $\mathbb{G}$.

The dual group of a cyclic group

Theorem

The dual of a cyclic group of order n is also a cyclic group of order n.

Proof.

- Recall that $e(x) = e^{2\pi ix}$ for any $x \in \mathbb{R}$ and we will write $e_n(x) = e(x/n)$.
- The nth roots of unity are the complex numbers $1, e_n(1), \ldots, e_n(n-1)$.
- Let $\mathbb{G} = \{jg_0 : j \in \mathbb{N}_{<n}\}$ be a cyclic group of order n with generator g_0.
- For every $a \in \mathbb{Z}$, we define $\psi_a \in \widehat{\mathbb{G}}$ by $\psi_a\left(jg_0\right) := e_n(aj)$.
- We can easily verify that $\psi_a\psi_b = \psi_{a+b}$, and $\psi_a^{-1} = \psi_{-a}$, and $\psi_a = \psi_b$ if and only if $a \equiv b \pmod{n}$. It follows that $\psi_a = \psi_1^a$ for any $a \in \mathbb{Z}$.
- If $\chi \in \widehat{\mathbb{G}}$, then χ is completely determined by its value on g_0. Since $\chi\left(g_0\right)$ is an n-th root of unity, we have $\chi\left(g_0\right) = e_n(a)$ for some $a \in \mathbb{N}_{<n}$, and so $\chi\left(jg_0\right) = e_n(aj)$ for all $j \in \mathbb{Z}$. Thus, $\chi = \psi_a$ and

  $$\widehat{\mathbb{G}} = \{\psi_a : a \in \mathbb{N}_{<n}\} = \{\psi_1^a : a \in \mathbb{N}_{<n}\}$$

  is also a cyclic group of order n, and the map $\mathbb{G} \ni a \mapsto \psi_q \in \widehat{\mathbb{G}}$ defines the isomorphism between $\mathbb{G}$ and $\widehat{\mathbb{G}}$.
- It is a simple but critical observation that if g is a nonzero element of a cyclic group $\mathbb{G}$, then $\psi_1(g) \neq 1$.

The dual group of a finite abelian group

Theorem

Let $\mathbb{G}$ be a finite abelian group and let $\mathbb{G}_1, \ldots, \mathbb{G}_k$ be subgroups of $\mathbb{G}$ such that $\mathbb{G} = \mathbb{G}_1 \oplus \cdots \oplus \mathbb{G}_k$. For every character $\chi \in \widehat{\mathbb{G}}$ there exist unique characters $\chi_i \in \widehat{\mathbb{G}_i}$ such that if $g \in \mathbb{G}$ and $g = g_1 + \cdots + g_k$ with $g_i \in \mathbb{G}_i$ for $i \in [k]$, then

$$\chi(g) = \chi_1(g_1) \cdots \chi_k(g_k). \tag{*}$$

Moreover, $\widehat{\mathbb{G}}$ and $\widehat{\mathbb{G}_1} \times \cdots \times \widehat{\mathbb{G}_k}$ are isomorphic.

Proof.

- If $\chi_i \in \widehat{\mathbb{G}_i}$ for $i \in [k]$, then we can construct a map $\chi : \mathbb{G} \to \mathbb{C}^\times$ as follows. For each $g \in \mathbb{G}$ there exist unique elements $g_i \in \mathbb{G}_i$ such that $g = g_1 + \cdots + g_k$. Define

$$\chi(g) = \chi(g_1 + \cdots + g_k) = \chi_1(g_1) \cdots \chi_k(g_k). \tag{**}$$

- Then χ is a character in $\widehat{\mathbb{G}}$, and this construction induces a map

$$\Psi : \widehat{\mathbb{G}_1} \times \cdots \times \widehat{\mathbb{G}_k} \to \widehat{\mathbb{G}},$$

defined by $\Psi(\chi_1, \ldots, \chi_k) := \chi$, where χ is given as in (**).

The dual group of a finite abelian group

- If is easy to see that Ψ is a one-to-one homomorphism. Indeed, if $(\chi_1, \ldots, \chi_k) \neq (\chi'_1, \ldots, \chi'_k)$, then without loss of generality we can assume that $\chi_1 \neq \chi'_1$. This means that there exists $g_1 \in \mathbb{G}_1$ such that $\chi_1(g_1) \neq \chi'_1(g_1)$. It suffices to take $g = g_1 + 0 + \ldots + 0$ to see that $\Psi(\chi_1, \ldots, \chi_k)(g) = \chi_1(g_1) \neq \chi'_1(g_1) = \Psi(\chi'_1, \ldots, \chi'_k)(g)$.
- We shall show that the map Ψ is onto. Let $\chi \in \widehat{\mathbb{G}}$. We define the function χ_i on $\mathbb{G}_i$ by

$$\chi_i\left(g_i\right) = \chi\left(g_i\right) \quad \text{for all} \quad g_i \in \mathbb{G}_i.$$

- Then χ_i is a character in $\widehat{\mathbb{G}_i}$. If $g \in \mathbb{G}$ and $g = g_1 + \cdots + g_k$ with $g_i \in \mathbb{G}_i$, then

$$\chi(g) = \chi\left(g_1 + \cdots + g_k\right) = \chi\left(g_1\right) \cdots \chi\left(g_k\right) = \chi_1\left(g_1\right) \cdots \chi_k\left(g_k\right).$$

- It follows that

$$\Psi\left(\chi_1, \ldots, \chi_k\right) = \chi$$

and so Ψ is onto. □

Duality theorem for finite Abelian groups

Theorem (Separation points property)

Let $\mathbb{G}$ be a finite abelian group. If $0 \neq g \in \mathbb{G}$, then there is $\chi \in \widehat{\mathbb{G}}$ so that $\chi(g) \neq 1$.

Proof.

- We write $\mathbb{G} = \mathbb{G}_1 \oplus \cdots \oplus \mathbb{G}_k$ as a direct product of cyclic groups.
- If $g \neq 0$, then there exist $g_1 \in \mathbb{G}_1, \ldots, g_k \in \mathbb{G}_k$ such that $g = g_1 + \cdots + g_k$, and $g_j \neq 0$ for some $j \in [k]$.
- Since the group $\mathbb{G}_j$ is cyclic, there is $\chi_j \in \widehat{\mathbb{G}_j}$ such that $\chi_j\left(g_j\right) \neq 1$. For $i \in [k] \setminus \{j\}$, let $\chi_i \in \widehat{\mathbb{G}_i}$ be the character defined by $\chi_i\left(g_1\right) = 1$ for all $g_i \in \mathbb{G}_i$. If $\chi = \Psi\left(\chi_1, \ldots, \chi_k\right) \in \widehat{\mathbb{G}}$, then $\chi(g) = \chi_j\left(g_j\right) \neq 1$.

This completes the proof of the theorem. □

Theorem (Duality theorem)

A finite abelian group $\mathbb{G}$ is isomorphic to its dual, that is, $\mathbb{G} \equiv \widehat{\mathbb{G}}$.

Proof.

- We know the dual of a finite cyclic group of order n is also a finite cyclic group of order n. We also know that a finite abelian group $\mathbb{G}$ has cyclic subgroups $\mathbb{G}_1, \ldots, \mathbb{G}_k$ such that $\mathbb{G} = \mathbb{G}_1 \oplus \cdots \oplus \mathbb{G}_k$. Finally we see that

$$\widehat{\mathbb{G}} \equiv \widehat{\mathbb{G}_1} \times \cdots \times \widehat{\mathbb{G}_k} \equiv \mathbb{G}_1 \times \cdots \times \mathbb{G}_k \equiv \mathbb{G}_1 \oplus \cdots \oplus \mathbb{G}_k = \mathbb{G}.$$

□

Pairing

- Let $\mathbb{G}$ be a finite abelian group of order n, and Γ_n be the group of nth roots of unity. There is a pairing map $\langle \cdot, \cdot \rangle : \mathbb{G} \times \widehat{\mathbb{G}} \to \Gamma_n$ defined by

$$\langle a, \chi \rangle = \chi(a).$$

- This map is nondegenerate in the sense that:
  - $\langle a, \chi \rangle = 1$ for all group elements $a \in \mathbb{G}$ if and only if $\chi = \chi_0$;
  - $\langle a, \chi \rangle = 1$ for all characters $\chi \in \widehat{\mathbb{G}}$ if and only if $a = 0$ by the separation points property.
- For each $a \in \mathbb{G}$, the function $\langle a, \cdot \rangle$ is a character of the dual group $\widehat{\mathbb{G}}$, that is, $\langle a, \cdot \rangle \in \widehat{\widehat{\mathbb{G}}}$. The map $\Delta : \mathbb{G} \to \widehat{\widehat{\mathbb{G}}}$ defined by $a \mapsto \langle a, \cdot \rangle$ or, equivalently,

$$\Delta(a)(\chi) = \langle a, \chi \rangle = \chi(a),$$

  is a homomorphism of the group $\mathbb{G}$ into its double dual $\widehat{\widehat{\mathbb{G}}}$.
- Since the pairing is nondegenerate, this homomorphism is one-to-one.
- Since $|\mathbb{G}| = |\widehat{\mathbb{G}}| = |\widehat{\widehat{\mathbb{G}}}|$, it follows that Δ is a natural isomorphism of $\mathbb{G}$ onto $\widehat{\widehat{\mathbb{G}}}$.

Orthogonality relations

Theorem

Let $\mathbb{G}$ be a finite abelian group of order n, and let $\widehat{\mathbb{G}}$ be its dual group.

- *If $\chi \in \widehat{\mathbb{G}}$, then*

$$\sum_{a \in \mathbb{G}} \chi(a) = \begin{cases} n & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

- *If $a \in \mathbb{G}$, then*

$$\sum_{\chi \in \widehat{\mathbb{G}}} \chi(a) = \begin{cases} n & \text{if } a = 0, \\ 0 & \text{if } a \neq 0. \end{cases}$$

Proof.

- *For $\chi \in \widehat{\mathbb{G}}$, let*

$$S(\chi) = \sum_{a \in \mathbb{G}} \chi(a).$$

If $\chi = \chi_0$, then $S(\chi_0) = |\mathbb{G}| = n$. If $\chi \neq \chi_0$, then $\chi(b) \neq 1$ for some $b \in \mathbb{G}$, and so $S(\chi) = 0$, since

$$\chi(b)S(\chi) = \chi(b) \sum_{a \in \mathbb{G}} \chi(a) = \sum_{a \in \mathbb{G}} \chi(ba) = \sum_{a \in \mathbb{G}} \chi(a) = S(\chi).$$

Proof

- For $a \in \mathbb{G}$, let
$$T(a) = \sum_{\chi \in \widehat{\mathbb{G}}} \chi(a)$$
- If $a = 0$, then $T(a) = |\widehat{\mathbb{G}}| = n$. If $a \neq 0$, then $\chi'(a) \neq 1$ for some $\chi' \in \widehat{\mathbb{G}}$ (by the separation point property), hence
$$\begin{aligned}\chi'(a)T(a) &= \chi'(a) \sum_{\chi \in \widehat{\mathbb{G}}} \chi(a) \\ &= \sum_{\chi \in \widehat{\mathbb{G}}} \chi'\chi(a) \\ &= \sum_{\chi \in \widehat{\mathbb{G}}} \chi(a) \\ &= T(a)\end{aligned}$$

and so $T(a) = 0$. This completes the proof. □

Orthogonality relations

Theorem

Let $\mathbb{G}$ be a finite abelian group of order n, and let $\widehat{\mathbb{G}}$ be its dual group.

- *If $\chi_1, \chi_2 \in \widehat{\mathbb{G}}$, then*

$$\sum_{a \in \mathbb{G}} \chi_1(a)\overline{\chi_2}(a) = \begin{cases} n & \text{if } \chi_1 = \chi_2, \\ 0 & \text{if } \chi_1 \neq \chi_2. \end{cases}$$

- *If $a, b \in \mathbb{G}$, then*

$$\sum_{\chi \in \widehat{\mathbb{G}}} \chi(a)\overline{\chi}(b) = \begin{cases} n & \text{if } a = b, \\ 0 & \text{if } a \neq b. \end{cases}$$

Proof.

- These identities follow immediately from the previous theorem, since

$$\chi_1(a)\overline{\chi_2}(a) = \chi_1\chi_2^{-1}(a), \quad \text{and} \quad \chi(a)\overline{\chi}(b) = \chi(a-b).$$

This completes the proof. □

Examples

- The character table for a group has one column for each element of the group and one row for each character of the group.
- For example, if C_4 is the cyclic group of order 4 with generator g_0, then the characters of C_4 are the functions

$$\psi_a(jg_0) = e_4(aj) = i^{aj}$$

for $a \in \{0, 1, 2, 3\}$, and the character table is the following:

	0	g_0	$2g_0$	$3g_0$
ψ_0	1	1	1	1
ψ_1	1	i	-1	$-i$
ψ_2	1	-1	1	-1
ψ_3	1	$-i$	-1	i

- Note the that sum of the numbers in the first row is equal to the order of the group, and the sum of the numbers in each of the other rows is 0.
- Similarly, the sum of the numbers in the first column is the order of the group, and the sum of the numbers in each of the other columns is 0. This is a special case of the orthogonality relations.