Chapter 4

Characters and Gauss sums

4.1 Characters on finite abelian groups

In what follows, abelian groups are multiplicatively written, and the unit element of an abelian group A is denoted by 1. We denote the order (number of elements) of A by $|A|$.

Let A be a finite abelian group. A *character* on A is a group homomorphism $\chi : A \to \mathbb{C}^*$ (i.e., $\mathbb{C} \setminus \{0\}$ with multiplication).

If $|A| = n$ then $a^n = 1$, hence $\chi(a)^n = 1$ for each $a \in A$ and each character χ on A. Therefore, a character on A maps A to the roots of unity.

The product $\chi_1\chi_2$ of two characters χ_1, χ_2 on A is defined by $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$ for $a \in A$. With this product, the characters on A form an abelian group, the so-called *character group of* A, which we denote by $\widehat{A}$ (or $\mathrm{Hom}(A, \mathbb{C}^*)$). The unit element of $\widehat{A}$ is the trivial character $\chi_0^{(A)}$ that maps A to 1. Since any character on A maps A to the roots of unity, the inverse $\chi^{-1} : a \mapsto \chi(a)^{-1}$ of a character χ is equal to its complex conjugate $\overline{\chi} : a \mapsto \overline{\chi(a)}$.

It would have been possible to develop the theory of characters using the fact that every finite abelian groups is the direct sum of cyclic groups, but we prefer to start from scratch.

Let B be a subgroup of A and χ a character on B. By an *extension* of χ to A we mean a character χ' on A such that $\chi'|_B = \chi$, i.e., $\chi'(b) = \chi(b)$ for $b \in B$.

Lemma 4.1. *Let A be a finite abelian group, B a subgroup of A such that A/B is cyclic, and χ a character on B. Then χ has precisely $|A|/|B|$ extensions to A.*

Proof. The order of A/B is precisely $t := |A|/|B|$. Let $g \in A$ be such that $\overline{g} := gB$ is a generator of A/B. Then $h := g^t \in B$. If χ' is an extension of χ to A, then necessarily $\chi'(g)^t = \chi(h)$. We show that conversely, for each of the t roots ρ of $\rho^t = \chi(h)$ there is a unique extension χ_ρ of χ to A such that $\chi_\rho(g) = \rho$; this clearly implies our lemma.

Notice that $A = \{bg^k : b \in B, k \in \mathbb{Z}\}$. The character χ_ρ, if it exists, necessarily has to satisfy $\chi_\rho(bg^k) = \chi(b)\rho^k$, for $b \in B$, $k \in \mathbb{Z}$. We now define χ_ρ in this way and show that it is well-defined, i.e., independent of the choice of b and k. Indeed, suppose that $b_1 g^{k_1} = b_2 g^{k_2}$, with $b_1, b_2 \in B$ and $k_1, k_2 \in \mathbb{Z}$, i.e. $g^{k_1-k_2} = b_1^{-1} b_2$. Then $\overline{g}^{k_1-k_2} = \overline{1}$, so $q := (k_2 - k_1)/t \in \mathbb{Z}$, hence $h^q = b_1^{-1} b_2$. This implies $\rho^{k_1-k_2} = \chi(h)^q = \chi(b_1)^{-1}\chi(b_2)$, hence $\chi(b_2)\rho^{k_2} = \chi(b_1)\rho^{k_1}$. This shows that indeed χ_ρ is well-defined. It is easily shown to be a character. □

Proposition 4.2. *Let A be a finite abelian group, B a subgroup of A, and χ a character on B. Then χ has precisely $|A|/|B|$ extensions to A.*

Proof. We proceed by induction on $|A|/|B|$. If $|A|/|B| = 1$ we are done. Assume that $|A|/|B| > 1$. Choose $g \in A \setminus B$ and define $B' := B\langle g \rangle$. Then B'/B is cyclic, so by Lemma 4.1, the character χ has precisely $|B'|/|B|$ extensions to B'. Since $|B'| > |B|$, we can apply the induction hypothesis and infer that each of these extensions to B' has precisely $|A|/|B'|$ extensions to A. Thus it follows that χ has precisely $|A|/|B|$ extensions to A. □

Corollary 4.3. *Let A be a finite abelian group. Then $|\widehat{A}| = |A|$.*

Proof. Apply Proposition 4.2 with $B = \{1\}$. □

Corollary 4.4. *Let A be a finite abelian group, and $g \in A$ with $g \neq 1$. Then there is a character χ on A with $\chi(g) \neq 1$.*

Proof. Assume g has order $r > 1$. A character on $\langle g \rangle$ is uniquely determined by its value in g, so there is precisely one character χ_0 on $\langle g \rangle$ with $\chi_0(g) = 1$. By Proposition 4.2, this character has precisely $|A|/|\langle g \rangle| = |A|/r$ extensions to A. Hence there are characters χ on A that do not extend χ_0, i.e., for which $\chi(g) \neq 1$. □

For a finite abelian group A, let $\widehat{\widehat{A}}$ denote the character group of $\widehat{A}$. Each element $a \in A$ gives rise to a character $\widehat{a}$ on $\widehat{A}$, given by $\widehat{a}(\chi) := \chi(a)$.

Theorem 4.5 (Duality)**.** *Let A be a finite abelian group. Then the map $a \mapsto \widehat{a}$ defines an isomorphism from A to $\widehat{\widehat{A}}$.*

Proof. The map $\varphi : a \mapsto \widehat{a}$ obviously defines a group homomorphism from A to $\widehat{\widehat{A}}$. We show that it is injective. Let $a \in \mathrm{Ker}(\varphi)$; then $\widehat{a}(\chi) = 1$ for all $\chi \in \widehat{A}$, i.e., $\chi(a) = 1$ for all $\chi \in \widehat{A}$, which by Corollary 4.4 implies that $a = 1$. So indeed, φ is injective. But then φ is surjective as well, since by Corollary 4.3, $|\widehat{\widehat{A}}| = |\widehat{A}| = |A|$. Hence φ is an isomorphism. □

Theorem 4.6 (Orthogonality relations for characters)**.** *Let A be a finite abelian group.*

(i) For any two characters χ_1, χ_2 on A we have

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

(ii) For any two elements a, b of A we have

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

Proof. Part (ii) follows by applying part (i) with $\widehat{A}$ instead of A, and using Theorem 4.5 and Corollary 4.3. So we prove only (i). Let $\chi_1, \chi_2 \in \widehat{A}$ and put $S := \sum_{a \in A} \chi_1(a)\overline{\chi_2(a)}$. Let $\chi := \chi_1\overline{\chi_2} = \chi_1\chi_2^{-1}$. Then $S = \sum_{a \in A} \chi(a)$. Clearly, if $\chi_1 = \chi_2$ then $\chi = \chi_0^{(A)}$, hence $S = |A|$. Let $\chi_1 \neq \chi_2$. Then $\chi \neq \chi_0^{(A)}$, hence there is $g \in A$ with $\chi(g) \neq 1$. Further,

$$\chi(g)S = \sum_{a \in A} \chi(ga) = S,$$

since ga runs through the elements of A. Hence $S = 0$. □

This will not be needed later, but for completeness we show that there is also an isomorphism from a finite abelian group A to its character group $\widehat{A}$. But unlike the isomorphism in Theorem 4.5 this is not canonical, since it will depend on a choice of generators for A.

Lemma 4.7. *Let A be a cyclic group of order n. Then $\widehat{A}$ is also a cyclic group of order n.*

Proof. Let $A = \langle g \rangle$. Then $A = \{1, g, \dots, g^{n-1}\}$ and $g^n = 1$. A character χ on A is determined by $\chi(g)$. Let ρ_1 be a primitive n-th root of unity. It is easy to see that there is a character χ_1 on A with $\chi_1(g) = \rho_1$, that $\chi_0^{(A)}, \chi_1, \dots, \chi_1^{n-1}$ are distinct, and $\chi_1^n = \chi_0^{(A)}$. Further, if χ is any character on A, then $\chi(g)^n = 1$, which implies that χ is a power of χ_1. So $\widehat{A} = \langle \chi_1 \rangle$ is a cyclic group of order n. $\square$

Lemma 4.8. *Let $A = A_1 \times \cdots \times A_r$ be the direct product of finite abelian groups $A_1, \dots, A_r$. Then $\widehat{A}$ is isomorphic to $\widehat{A_1} \times \cdots \times \widehat{A_r}$.*

Proof. It suffices to prove this for $r = 2$; then the proof of the lemma can be completed by induction on r. Denote by 1 the unit element of A. Let $A = A_1 \times A_2 = \{g_1 g_2 : g_1 \in A_1, g_2 \in A_2\}$ where $g_1 g_2 = 1$ if and only if $g_1 = g_2 = 1$. Define a map

$$\varphi : \widehat{A_1} \times \widehat{A_2} \to \widehat{A} : (\chi_1, \chi_2) \mapsto \chi_1 \chi_2,$$

where $\chi_1\chi_2(g_1 g_2) := \chi_1(g_1)\chi_2(g_2)$ for $g_1 \in A_1, g_2 \in A_2$. It is easy to see that φ is a group homomorphism. Substituting $g_1 = 1$, respectively $g_2 = 1$, we see that χ_2, χ_1 are uniquely determined by $\chi_1\chi_2$. Hence φ is injective. Since $\widehat{A_1} \times \widehat{A_2}$ and $\widehat{A}$ have the same cardinality, it follows also that φ is surjective. $\square$

Proposition 4.9. *Every finite abelian group is a direct product of cyclic groups.*

Proof. See S. Lang, Algebra, Chap.1, §10. $\square$

Theorem 4.10. *Let A be a finite abelian group. Then there exists an isomorphism from A to $\widehat{A}$.*

Proof. By Proposition 4.9, A is a direct product $C_1 \times \cdots \times C_r$ of finite cyclic groups. By Lemmas 4.8, 4.7, $\widehat{A}$ is isomorphic to $\widehat{C_1} \times \cdots \times \widehat{C_r}$, where $\widehat{C_i}$ is a cyclic group of the same order as C_i, for $i = 1, \dots, r$. Now the isomorphism from A to $\widehat{A}$ can be established by mapping a generator of C_i to one of $\widehat{C_i}$, for $i = 1, \dots, r$. $\square$

Remark. The isomorphism constructed above depends on choices for generators of C_i, $\widehat{C_i}$, for $i = 1, \dots, r$. So it is not canonical.

4.2 Dirichlet characters

Let $q \in \mathbb{Z}_{\geqslant 2}$. Denote the residue class of a mod q by $\overline{a}$. Recall that the prime residue classes mod q, $(\mathbb{Z}/q\mathbb{Z})^* = \{\overline{a} : \gcd(a,q) = 1\}$ form a group of order $\varphi(q)$ under multiplication of residue classes. We can lift any character $\widetilde{\chi}$ on $(\mathbb{Z}/q\mathbb{Z})^*$ to a map $\chi : \mathbb{Z} \to \mathbb{C}$ by setting

$$\chi(a) := \begin{cases} \widetilde{\chi}(\overline{a}) & \text{if } \gcd(a,q) = 1; \\ 0 & \text{if } \gcd(a,q) > 1. \end{cases}$$

Notice that χ has the following properties:

(i) $\chi(1) = 1$;
(ii) $\chi(ab) = \chi(a)\chi(b)$ for $a, b \in \mathbb{Z}$;
(iii) $\chi(a) = \chi(b)$ if $a \equiv b \pmod{q}$;
(iv) $\chi(a) = 0$ if $\gcd(a,q) > 1$.

Any map $\chi : \mathbb{Z} \to \mathbb{C}$ with properties (i)–(iv) is called a *(Dirichlet) character modulo q*. Conversely, from a character χ mod q one easily obtains a character $\widetilde{\chi}$ on $(\mathbb{Z}/q\mathbb{Z})^*$ by setting $\widetilde{\chi}(\overline{a}) := \chi(a)$ for $a \in \mathbb{Z}$ with $\gcd(a,q) = 1$.

Let $G(q)$ be the set of characters modulo q. We define the product $\chi_1\chi_2$ of $\chi_1, \chi_2 \in G(q)$ by $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$ for $a \in \mathbb{Z}$. With this operation, $G(q)$ becomes a group, with unit element the *principal character modulo q* given by

$$\chi_0^{(q)}(a) = \begin{cases} 1 & \text{if } \gcd(a,q) = 1; \\ 0 & \text{if } \gcd(a,q) > 1. \end{cases}$$

The inverse of $\chi \in G(q)$ is its complex conjugate

$$\overline{\chi} : a \mapsto \overline{\chi(a)}.$$

It is clear, that this makes $G(q)$ into a group that is isomorphic to the character group of $(\mathbb{Z}/q\mathbb{Z})^*$.

One of the advantages of viewing characters as maps from $\mathbb{Z}$ to $\mathbb{C}$ is that this allows to multiply characters of different moduli: if χ_1 is a character mod q_1 and χ_2 a character mod q_2, then their product $\chi_1\chi_2$ is a character mod $\operatorname{lcm}(q_1, q_2)$.

We can easily translate the orthogonality relations for characters of $(\mathbb{Z}/q\mathbb{Z})^*$ into orthogonality relations for Dirichlet characters modulo q. Recall that a *complete* *residue system modulo* q is a set, consisting of precisely one integer from every residue class modulo q, e.g., $\{3, 5, 11, 22, 104\}$ is a complete residue system modulo 5.

Theorem 4.11. *Let $q \in \mathbb{Z}_{\geqslant 2}$, and let S_q be a complete residue system modulo q.*
(i) Let $\chi_1, \chi_2 \in G(q)$. Then

$$\sum_{a \in S_q} \chi_1(a)\overline{\chi_2(a)} = \begin{cases} \varphi(q) & \text{if } \chi_1 = \chi_2; \\ 0 & \text{if } \chi_1 \neq \chi_2. \end{cases}$$

(ii) Let $a, b \in \mathbb{Z}$. Then

$$\sum_{\chi \in G(q)} \chi(a)\overline{\chi(b)} = \begin{cases} \varphi(q) & \text{if } \gcd(ab, q) = 1,\ a \equiv b \pmod q; \\ 0 & \text{if } \gcd(ab, q) = 1,\ a \not\equiv b \pmod q; \\ 0 & \text{if } \gcd(ab, q) > 1. \end{cases}$$

Proof. Exercise. □

Let χ be a character mod q and d a positive divisor of q.

We say that q is *induced* by a character χ' mod d if $\chi(a) = \chi'(a)$ for every $a \in \mathbb{Z}$ with $\gcd(a, q) = 1$. Here we define the principal character mod 1 by $\chi_0^{(1)}(a) = 1$ for $a \in \mathbb{Z}$. For instance, $\chi_0^{(q)}$ is induced by $\chi_0^{(1)}$. Notice that if $\gcd(a, d) = 1$ and $\gcd(a, q) > 1$, then $\chi'(a) \neq 0$ but $\chi(a) = 0$.

The character χ is called *primitive* if there is no divisor $d < q$ of q such that χ is induced by a character mod d.

Theorem 4.12. *Let $q \in \mathbb{Z}_{\geqslant 2}$ and χ a character mod q. Then there are a unique divisor f of q, and a unique primitive character χ_0 mod f, such that χ is induced by χ_0.*

The integer f from Theorem 4.12 is called the *conductor* of χ.

To prove this, we need some lemmas.

Lemma 4.13. *Let a be an integer with $\gcd(a, d) = 1$. Then there is $b \in \mathbb{Z}$ with $a \equiv b \pmod d$, $\gcd(b, q) = 1$.*

Proof. Write $q = q_1 q_2$, where q_1 is composed of the primes occurring in the factorization of d, and where q_2 is composed of primes not dividing d. By the Chinese Remainder Theorem, there is $b \in \mathbb{Z}$ with

$$b \equiv a \,(\mathrm{mod}\, d), \quad b \equiv 1 \,(\mathrm{mod}\, q_2).$$

This integer b is coprime with d, hence with q_1, and also coprime with q_2, so it is coprime with q. □

Lemma 4.14. *Let d be a divisor of q. Then there is at most one character mod d that induces χ.*

Proof. Suppose that χ is induced by the character χ_1 mod d. Let $a \in \mathbb{Z}$ with $\gcd(a, d) = 1$ and choose b with $a \equiv b \,(\mathrm{mod}\, d)$ and $\gcd(b, q) = 1$. Then $\chi_1(a) = \chi_1(b) = \chi(b)$. Hence χ_1 is uniquely determined by χ. □

The next lemma gives a method to verify if a character χ is induced by a character mod d.

Lemma 4.15. *Let χ be a character mod q, and d a divisor of q. Then the following assertions are equivalent:*
(i) χ is induced by a character mod d;
(ii) $\chi(a) = \chi(b)$ for all $a, b \in \mathbb{Z}$ with $a \equiv b \,(\mathrm{mod}\, d)$ and $\gcd(ab, q) = 1$;
(iii) $\chi(a) = 1$ for all $a \in \mathbb{Z}$ with $a \equiv 1 \,(\mathrm{mod}\, d)$ and $\gcd(a, q) = 1$.

Proof. The implications (i)⇒(ii)⇒(iii) are trivial.

(iii) ⇒ *(ii)*. Let $a, b \in \mathbb{Z}$ with $a \equiv b \,(\mathrm{mod}\, d)$ and $\gcd(ab, q) = 1$. There is $c \in \mathbb{Z}$ with $\gcd(c, q) = 1$ such that $a \equiv bc \,(\mathrm{mod}\, q)$. For this c we have $c \equiv 1 \,(\mathrm{mod}\, d)$. Now by (iii) we have $\chi(a) = \chi(b)\chi(c) = \chi(b)$.

(ii) ⇒ *(i)*. We define a character χ' mod d as follows. For $a \in \mathbb{Z}$ with $\gcd(a, d) > 1$ put $\chi'(a) := 0$. For $a \in \mathbb{Z}$ with $\gcd(a, d) = 1$, choose $b \in \mathbb{Z}$ such that $a \equiv b \,(\mathrm{mod}\, d)$ and $\gcd(b, q) = 1$ (which is possible by Lemma 4.13), and put $\chi'(a) := \chi(b)$. By (ii) this gives a well-defined character mod d that clearly induces χ. □

Lemma 4.16. *Let χ be a character mod q. Assume that χ is induced by characters χ_1 mod d_1, χ_2 mod d_2, where d_1, d_2 are divisors of q. Then χ is induced by a character mod $\gcd(d_1, d_2)$ which in turn induces χ_1, χ_2.*

Proof. Let $d = \gcd(d_1, d_2)$, $d_0 := \text{lcm}(d_1, d_2)$. We first show that χ_1 is induced by a character mod d. We apply criterion (iii) of the previous lemma. That is, we have to show that if a is an integer with $\gcd(a, d_1) = 1$ and $a \equiv 1 \pmod{d}$, then $\chi_1(a) = 1$.

Take such a. Then $a = 1 + td$ with $t \in \mathbb{Z}$. There are $x, y \in \mathbb{Z}$ with $xd_1 + yd_2 = d$. Hence $a = 1 + txd_1 + tyd_2$. The number $c := 1 + tyd_2$ is coprime with d_1 since a is coprime with d_1, and also coprime with d_2, hence it is coprime with d_0. By Lemma 4.13, there is b with $b \equiv c \pmod{d_0}$ and $\gcd(b, q) = 1$. We have $b \equiv a \pmod{d_1}$, $b \equiv 1 \pmod{d_2}$, hence $\chi_1(a) = \chi(b) = \chi_2(1) = 1$.

It follows that χ_1 is induced by a character, say χ_3 mod d. Similarly, χ_2 is induced by a character χ_3' mod d. Both χ_3, χ_3' induce χ. So by Lemma 4.14, $\chi_3 = \chi_3'$. □

Proof of Theorem 4.12. Let f be the smallest divisor of q such that χ is induced by a character mod f. This character, say χ_0, is necessarily primitive. Assume there is another primitive character χ_0' mod f' that induces χ. By the previous lemma, χ is induced by a character χ_0'' mod $\gcd(f, f')$ that in turn induces χ_0 and χ_0'. But this is possible only if $f = f'$. By Lemma 4.14 it follows that also $\chi_0 = \chi_0'$. □

4.3 Computation of $G(q)$

We give a method to compute the character group modulo q. We first make a reduction to prime powers.

Theorem 4.17. *Let $q = p_1^{k_1} \cdots q_t^{k_t}$, where $p_1, \ldots, p_t$ are distinct primes and $k_1, \ldots, k_t$ positive integers. Then the map*

$$G(p_1^{k_1}) \times \cdots \times G(p_t^{k_t}) \to G(q) : \ (\chi_1, \ldots, \chi_t) \mapsto \chi_1 \cdots \chi_t$$

is a group isomorphism.

Proof. Let f denote the map under consideration. Then f is a homomorphism. We show that it is injective. Let $\chi_i \in G(p_i^{k_i})$ $(i = 1, \ldots, t)$ be such that $\chi_1 \cdots \chi_t = \chi_0^{(q)}$. Let $i \in \{1, \ldots, t\}$ and choose $a \in \mathbb{Z}$ with $\gcd(a, p_i) = 1$. By the Chinese Remainder Theorem, there is $b \in \mathbb{Z}$ such that

$$b \equiv a \pmod{p_i^{k_i}}, \quad b \equiv 1 \pmod{p_j^{k_j}} \text{ for } j \neq i.$$

Then with this b we have

$$\chi_i(a) = \prod_{j=1}^{t} \chi_j(b) = \chi_0^{(q)}(b) = 1.$$

Hence $\chi_i = \chi_0^{(p_i^{k_i})}$. This holds for $i = 1, \ldots, t$, so f is injective.

Now since $G(p_1^{k_1}) \times \cdots \times G(p_t^{k_t})$ and $G(q)$ have the same order $\varphi(q)$, the map f is also surjective. □

To compute $G(p^k)$ for a prime power p^k, we need some information about the structure of $(\mathbb{Z}/p^k\mathbb{Z})^*$. This is provided by the following theorem.

Theorem 4.18. *(i) Let p be a prime $\geqslant 3$. Then the group $(\mathbb{Z}/p^k\mathbb{Z})^*$ is cyclic of order $p^{k-1}(p-1)$.*
(ii) $(\mathbb{Z}/4\mathbb{Z})^*$ is cyclic of order 2.
Further, if $k \geqslant 3$ then $(\mathbb{Z}/2^k\mathbb{Z})^* =< \overline{-1} > \times < \overline{5} >$ is the direct product of a cyclic group of order 2 and a cyclic group of order 2^{k-2}.

We skip the proof of $k = 1$ of (i), which belongs to a basic algebra course. For the proof of the remaining parts, we need a lemma.

For a prime number p, and for $a \in \mathbb{Z} \setminus \{0\}$, we denote by $\mathrm{ord}_p(a)$ the largest integer k such that p^k divides a.

Lemma 4.19. *Let p be a prime number and a an integer such that* $\mathrm{ord}_p(a-1) \geqslant 1$ *if $p \geqslant 3$ and* $\mathrm{ord}_p(a-1) \geqslant 2$ *if $p = 2$. Then*

$$\mathrm{ord}_p(a^{p^k} - 1) = \mathrm{ord}_p(a-1) + k.$$

Proof. We prove the assertion only for $k = 1$; then the general statement follows easily by induction on k. Our assumption on a implies that $a = 1 + p^t b$, where $t \geqslant 1$ if $p \geqslant 3$, $t \geqslant 2$ if $p = 2$, and where b is an integer not divisible by p. Now by the binomial formula,

$$a^p - 1 = \sum_{j=1}^{p} \binom{p}{j} (p^t b)^j = p^{t+1} b^j + p^{t+2}(\cdots).$$

Here we have used that all binomial coefficients $\binom{p}{j}$ are divisible by p except the last. But the last term $(p^t b)^p$ is divisible by p^{pt}, and the exponent pt is larger than

$t+1$ (the assumption $t \geqslant 2$ for $p=2$ is needed to ensure this). This shows that $\mathrm{ord}_p(a^p-1)=t+1$. □

Proof of Theorem 4.18. (i). We take for granted that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$, and assume that $k \geqslant 2$. We construct a generator for $(\mathbb{Z}/p^k\mathbb{Z})^*$. Let g be an integer such that $g \pmod p$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. We show that we can choose g such that $\mathrm{ord}_p(g^{p-1}-1)=1$. Indeed, assume that $\mathrm{ord}_p(g^{p-1}-1) \geqslant 2$ and take $g+p$. Then

$$\begin{aligned}(g+p)^{p-1}-1 &= \sum_{j=1}^{p-1}\binom{p-1}{j} g^{p-1-j}p^j = (p-1)g^{p-2}p + p^2(\cdots)\\ &= -g^{p-2}p + p^2(\cdots)\end{aligned}$$

hence $\mathrm{ord}_p((g+p)^{p-1}-1)=1$. So, replacing g by $g+p$ if need be, we get an integer g such that $g \pmod p$ generates $(\mathbb{Z}/p\mathbb{Z})^*$ and $\mathrm{ord}_p(g^{p-1}-1)=1$.

We show that $\overline{g} := g \pmod{p^k}$ generates $(\mathbb{Z}/p^k\mathbb{Z})^*$. Let n be the order of $\overline{g}$ in $(\mathbb{Z}/p^k\mathbb{Z})^*$; that is, n is the smallest positive integer with $g^n \equiv 1 \pmod{p^k}$. On the one hand, $g^n \equiv 1 \pmod p$, hence $p-1$ divides n. On the other hand, n divides the order of $(\mathbb{Z}/p^k\mathbb{Z})^*$, that is, $p^{k-1}(p-1)$. So $n = p^s(p-1)$ with $s \leqslant k-1$. By Lemma 4.19 we have

$$\mathrm{ord}_p(g^n-1) = \mathrm{ord}_p(g^{p-1}-1)+s = s+1.$$

This has to be equal to k, so $s=k-1$. Hence $n=p^{k-1}(p-1)$ is equal to the order of $(\mathbb{Z}/p^k\mathbb{Z})^*$. It follows that $(\mathbb{Z}/p^k\mathbb{Z})^* = \langle \overline{g} \rangle$.

(ii). Assume that $k \geqslant 3$. Define the subgroup of index 2,

$$H := \{\overline{a} \in (\mathbb{Z}/2^k\mathbb{Z})^* : \ a \equiv 1 \pmod 4\}.$$

Then

$$(\mathbb{Z}/2^k\mathbb{Z})^* = H \cup (-H) = \{(\overline{-1})^k\overline{a} : \ k \in \{0,1\}, \ \overline{a} \in H\}$$

and $(\overline{-1})^k\overline{a} = \overline{1}$ if and only if $k=0$ and $\overline{a}=\overline{1}$. Hence $(\mathbb{Z}/2^k\mathbb{Z})^* =< \overline{-1} > \times H$. Similarly as above, one shows that H is cyclic of order 2^{k-2}, and that $H = \langle \overline{5} \rangle$. □

Corollary 4.20. *Let p be a prime and $k \geqslant 1$.*
(i) If $p=2$, $k=1,2$ or $p>2$ then $G(p^k)$ is cyclic of order $p^{k-1}(p-1)$.
(ii) If $p=2$, $k \geqslant 3$, then $G(p^k)$ is the direct product of a cyclic group of order 2 and a cyclic group of order 2^{k-2}.

Proof. Immediate consequence of Theorem 4.18 and Lemmas 4.7 and 4.8. □

Following the proofs of Lemmas 4.7, 4.8, we can give an explicit description for the groups $G(p^k)$.

Clearly, $G(2) = \{\chi_0^{(2)}\}$ and $G(4) = \{\chi_0^{(4)}, \chi_4\}$, where $\chi_4(a) = 1$ if $a \equiv 1 \pmod 4$, $\chi_4(a) = -1$ if $a \equiv 3 \pmod 4$, $\chi_4(a) = 0$ if a is even.

If $p > 2$, choose $g \in \mathbb{Z}$ such that $g \pmod{p^k}$ generates $(\mathbb{Z}/p^k\mathbb{Z})^*$, and choose a primitive $p^{k-1}(p-1)$-th root of unity ρ. Then $G(p^k) = \langle \chi_1 \rangle$ where χ_1 is the Dirichlet character determined by $\chi_1(g) = \rho$.

As for 2^k with $k \geqslant 3$, choose a primitive 2^{k-2}-th root of unity ρ. Then $G(2^k) = \langle \chi_1 \rangle \times \langle \chi_2 \rangle$, where χ_1, χ_2 are given by

$$\chi_1(-1) = -1,\ \chi_1(5) = 1; \quad \chi_2(-1) = 1,\ \chi_2(5) = \rho.$$

4.4 Gauss sums

Let $q \in \mathbb{Z}_{\geqslant 2}$. For a character χ mod q and for $b \in \mathbb{Z}$, we define the Gauss sum

$$\tau(b, \chi) := \sum_{x \in S_q} \chi(x) e^{2\pi i b x/q},$$

where S_q is a full system of representatives modulo q. This does not depend on the choice of S_q. The Gauss sum $\tau(1, \chi)$ occurs for instance in the functional equation for the L-function $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$ (later).

We prove some basic properties of Gauss sums.

Theorem 4.21. *Let $q \in \mathbb{Z}_{\geqslant 2}$ and let χ be a character mod q. Further, let $b \in \mathbb{Z}$.*
(i) If $\gcd(b, q) = 1$, then $\tau(b, \chi) = \overline{\chi(b)} \cdot \tau(1, \chi)$.
(ii) If $\gcd(b, q) > 1$ and χ is primitive, then $\tau(b, \chi) = \overline{\chi(b)} \cdot \tau(1, \chi) = 0$.

Proof. (i) Suppose $\gcd(b, q) = 1$. If x runs through a complete residue system S_q mod q, then bx runs to another complete residue system S'_q mod q. Write $y = bx$. Then $\chi(y) = \chi(b)\chi(x)$, hence $\chi(x) = \overline{\chi(b)}\chi(y)$. Therefore,

$$\begin{aligned} \tau(b, \chi) &= \sum_{x \in S_q} \chi(x) e^{2\pi i b x/q} = \sum_{y \in S'_q} \overline{\chi(b)} \chi(y) e^{2\pi i y/q} \\ &= \overline{\chi(b)} \tau(1, \chi). \end{aligned}$$

(ii) We use the following observation: if q_1 is any divisor of q with $1 \leqslant q_1 \leqslant q$, then there is $c \in \mathbb{Z}$ such that $c \equiv 1 \pmod{q_1}$, $\gcd(c, q) = 1$, and $\chi(c) \neq 1$. Indeed, this is obvious if $q_1 = q$. If $q_1 < q$, then Lemma 4.15 implies that if there is no such integer c then χ is induced by a character mod q_1, contrary to our assumption that χ is primitive.

Now let $d := \gcd(b, q)$, put $b_1 := b/d$, $q_1 := q/d$, and choose c according to the observation. Then

$$\chi(c)\tau(b, \chi) = \sum_{x \in S_q} \chi(cx) e^{2\pi i bx/q}.$$

If x runs through a complete residue system S_q mod q, then $y := cx$ runs through another complete residue system S'_q mod q. Further, since $c \equiv 1 \pmod{q_1}$ we have

$$e^{2\pi i x b/q} = e^{2\pi i x b_1/q_1} = e^{2\pi i c x b_1/q_1} = e^{2\pi i y b/q}.$$

Hence

$$\chi(c)\tau(b, \chi) = \sum_{y \in S_q} \chi(y) e^{2\pi i b y/q} = \tau(b, \chi).$$

Since $\chi(c) \neq 1$ this implies that $\tau(b, \chi) = 0$. □

Theorem 4.22. *Let $q \in \mathbb{Z}_{\geqslant 2}$ and let χ be a primitive character mod q. Then*

$$|\tau(1, \chi)| = \sqrt{q}.$$

Proof. We have by Theorem 4.21,

$$\begin{aligned}
|\tau(1, \chi)|^2 &= \overline{\tau(1, \chi)} \cdot \tau(1, \chi) = \sum_{x=0}^{q-1} \overline{\chi(x)} e^{-2\pi i x/q} \tau(1, \chi) \\
&= \sum_{x=0}^{q-1} e^{-2\pi i x/q} \tau(x, \chi) = \sum_{x=0}^{q-1} e^{-2\pi i x/q} \left(\sum_{y=0}^{q-1} \chi(y) e^{2\pi i x y/q} \right) \\
&= \sum_{x=0}^{q-1} \left(\sum_{y=0}^{q-1} \chi(y) e^{2\pi i x(y-1)/q} \right) \\
&= \sum_{y=0}^{q-1} \chi(y) \left(\sum_{x=0}^{q-1} e^{2\pi i x(y-1)/q} \right) = \sum_{y=0}^{q-1} \chi(y) S(y), \text{ say.}
\end{aligned}$$

If $y = 1$, then $S(y) = \sum_{x=0}^{q-1} 1 = q$, while if $y \neq 1$, then

$$S(y) = \frac{e^{2\pi i(y-1)} - 1}{e^{2\pi i(y-1)/q} - 1} = 0.$$

Hence $|\tau(1,\chi)|^2 = \chi(1)q = q$. $\square$

For later purposes we need the following variation on this result. A *real* character mod q is one which assumes only real values. This implies that $\chi(a) \in \{\pm 1\}$ if $\gcd(a,q) = 1$.

Theorem 4.23. *Let χ be a primitive real character mod q. Then $\tau(1,\chi)^2 = \chi(-1)q$.*

Proof. Similarly as in the proof of Theorem 4.22 we have

$$\tau(1,\chi)^2 = \sum_{x=0}^{q-1} \chi(x) e^{2\pi i x/q} \tau(1,\chi)$$

and by following the same reasoning,

$$\tau(1,\chi)^2 = \sum_{y=0}^{q-1} \chi(y) \left(\sum_{x=0}^{q-1} e^{2\pi i x(y+1)/q} \right) = \sum_{y=0}^{q-1} \chi(y) T(y),$$

say. As is easily seen, $T(q-1) = q$, while $T(y) = 0$ for $y = 0, \ldots, q-2$. This implies Theorem 4.23. $\square$

Remark. Theorem 4.22 implies that $\varepsilon_\chi := \tau(1,\chi)/\sqrt{q}$ lies on the unit circle. Gauss gave an explicit expression for ε_χ in the case that ε_χ is a primitive real character mod q. There is no general method known to compute ε_χ for non-real characters χ modulo large values of q.

4.5 Quadratic reciprocity

We give a proof of Gauss' Quadratic Reciprocity Theorem using Gauss sums. This section requires a little bit more algebraic background.

Let $p > 2$ be a prime number. An integer a is called a *quadratic residue modulo p* if $x^2 \equiv a \pmod{p}$ is solvable in $x \in \mathbb{Z}$ and $p \nmid a$, and a *quadratic non-residue modulo*

p if $x^2 \equiv a \pmod p$ is not solvable in $x \in \mathbb{Z}$. Further, a quadratic (non-)residue class modulo p is a residue class modulo p represented by a quadratic (non-)residue.

We define the *Legendre symbol*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p; \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p; \\ 0 & \text{if } p|a. \end{cases}$$

Lemma 4.24. *Let p be a prime > 2.*
(i) $\left(\frac{\cdot}{p}\right)$ is a primitive character mod p.
(ii) There are precisely $\frac{1}{2}(p-1)$ quadratic residue classes, and precisely $\frac{1}{2}(p-1)$ quadratic non-residue classes modulo p.
(iii) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$ for $a \in \mathbb{Z}$.

Proof. (i) The group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$. Let $g(\text{mod } p)$ be a generator of this group. Take $a \in \mathbb{Z}$ with $\gcd(a,p) = 1$. Then there is $t \in \mathbb{Z}$ such that $a \equiv g^t \pmod p$. Now clearly, $x^2 \equiv a \pmod p$ is solvable in $x \in \mathbb{Z}$ if and only if t is even. Hence $\left(\frac{a}{p}\right) = (-1)^t$. This shows that $\left(\frac{\cdot}{p}\right)$ is a character mod p.

(ii) The group $(\mathbb{Z}/p\mathbb{Z})^*$ consists of $g^t \pmod p$ $(t = 0, \ldots, p-1)$. Clearly, the quadratic residue classes are those with t even, and the quadratic non-residue classes those with t odd. This implies (ii). This shows also that $\left(\frac{\cdot}{p}\right)$ is not the principal character mod p, and so, since p is a prime, it must be primitive.

(iii) The assertion is clearly true if $p|a$. Assume that $p \nmid a$. Then there is $t \in \mathbb{Z}$ with $a \equiv g^t \pmod p$. Note that $(g^{(p-1)/2})^2 \equiv 1 \pmod p$, hence $g^{(p-1)/2} \equiv \pm 1 \pmod p$. But $g^{(p-1)/2} \not\equiv 1 \pmod p$ since g (mod p) is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Hence $g^{(p-1)/2} \equiv -1 \pmod p$. As a consequence,

$$a^{(p-1)/2} \equiv (-1)^t \equiv \left(\frac{a}{p}\right) \pmod p.$$

□

The following is immediate:

Corollary 4.25. *Let p be a prime > 2. Then*

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

Gauss' Quadratic Reciprocity Theorem is as follows:

Theorem 4.26. *Let p, q be distinct primes > 2. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 \pmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

Furthermore, as a supplement we have:

Theorem 4.27. *Let p be a prime > 2. Then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8, \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Example. Check if $x^2 \equiv 33 \pmod{97}$ is solvable.

$$\begin{aligned} \left(\frac{33}{97}\right) &= \left(\frac{3}{97}\right) \cdot \left(\frac{11}{97}\right) = \left(\frac{97}{3}\right) \cdot \left(\frac{97}{11}\right) \\ &= \left(\frac{1}{3}\right) \cdot \left(\frac{-2}{11}\right) = \left(\frac{1}{3}\right) \cdot \left(\frac{-1}{11}\right) \cdot \left(\frac{2}{11}\right) = 1 \cdot (-1) \cdot (-1) = 1. \end{aligned}$$

We prove only Theorem 4.26 and leave Theorem 4.27 as an exercise. We first make some preparations and then prove some lemmas.

Let $\mathbb{Q}[X]$ denote the ring of polynomials with coefficients in $\mathbb{Q}$. A number $\alpha \in \mathbb{C}$ is called *algebraic* if there is a non-zero polynomial $f \in \mathbb{Q}[X]$ such that $f(\alpha) = 0$. Among all non-zero polynomials from $\mathbb{Q}[X]$ having α as a zero, we choose one of minimal degree. By multiplying such a polynomial with a suitable constant, we obtain one which is *monic*, i.e., of which the coefficient of the highest power of X is 1. There is only one monic polynomial in $\mathbb{Q}[X]$ of minimal degree having α as a zero, for if there were two, their difference would give a non-zero polynomial in $\mathbb{Q}[X]$ of smaller degree having α as a zero. This unique monic polynomial in $\mathbb{Q}[X]$ of minimal degree having α as a zero is called the *minimal polynomial* of α, denoted by f_α.

We observe that f_α must be irreducible in $\mathbb{Q}[X]$, that is, not a product of two non-constant polynomials from $\mathbb{Q}[X]$. For otherwise, α would be a zero of one of these polynomials, which has degree smaller than that of f_α.

Let q be a prime number > 2. We write $\zeta_q := e^{2\pi i/q}$. Define

$$R_q := \mathbb{Z}[\zeta_q] = \left\{ \sum_{i=0}^{r} a_i \zeta_q^i : \ a_i \in \mathbb{Z},\, r \geqslant 0 \right\}.$$

This set is closed under addition and multiplication, hence it is a ring.

Lemma 4.28. *$R_q \cap \mathbb{Q} = \mathbb{Z}$.*

Proof. We use without proof, that the minimal polynomial of ζ_q is $(X^q-1)/(X-1) = X^{q-1} + \cdots + X + 1$. Hence $\zeta_q^{q-1} = -\sum_{j=0}^{q-2} \zeta_q^j$. By repeatedly substituting this into an expression $\sum_{i=0}^{r} a_i \zeta_q^i$ with $a_i \in \mathbb{Z}$, we eventually get an expression $\sum_{j=0}^{q-2} b_j \zeta_q^j$ with $b_j \in \mathbb{Z}$ for all j. Hence all elements of R_q can be expressed in this form. Now if $\alpha \in R_q \cap \mathbb{Q}$, we get

$$\alpha = \sum_{j=0}^{q-2} b_j \zeta_q^j$$

with $\alpha \in \mathbb{Q}$ and $b_j \in \mathbb{Z}$ for all j. This implies that ζ_q is a zero of the polynomial $b_{q-2}X^{q-2} + \cdots + b_0 - \alpha$. Since the minimal polynomial of ζ_q has degree $q-1$, this is possible only if $b_0 = \alpha$ and $b_1 = \cdots = b_{q-2} = 0$. Hence $\alpha \in \mathbb{Z}$. $\square$

Given $\alpha, \beta \in R_q$ and $n \in \mathbb{Z}_{>0}$, we write $\alpha \equiv \beta \pmod{n}$ in R_q if $(\alpha - \beta)/n \in R_q$. Further, we write $\alpha \equiv \beta \pmod{n}$ in $\mathbb{Z}$ if $(\alpha - \beta)/n \in \mathbb{Z}$. By the Lemma we just proved, for $\alpha, \beta \in \mathbb{Z}$ we have that $\alpha \equiv \beta \pmod{n}$ in R_q if and only if $\alpha \equiv \beta \pmod{n}$ in $\mathbb{Z}$.

Lemma 4.29. *Let p be any prime number. Then for $\alpha_1, \ldots, \alpha_r \in R_q$ we have*

$$(\alpha_1 + \cdots + \alpha_r)^p \equiv \alpha_1^p + \cdots + \alpha_r^p \pmod{p} \quad \text{in } R_q.$$

Proof. By the multinomial theorem,

$$(\alpha_1 + \cdots + \alpha_r)^p = \sum_{i_1 + \cdots + i_r = p} \frac{p!}{i_1! \cdots i_r!} \alpha_1^{i_1} \cdots \alpha_r^{i_r}.$$

All multinomial coefficients are divisible by p, except those where one index $i_j = p$ and the others are 0. $\square$

Proof of Theorem 4.26. We use Gauss sums. For notational convenience we write χ_q for $\left(\frac{\cdot}{q}\right)$. We work in the ring R_q.

Notice that by Theorem 4.23 and Corollary 4.25,

$$\tau(1,\chi_q)^2 = \chi_q(-1)q = (-1)^{(q-1)/2}q. \tag{4.1}$$

Further, by Lemma 4.29 and Theorem 4.21,

$$\tau(1,\chi_q)^p \equiv \sum_{x=0}^{q-1} \chi_q(x)^p \zeta_q^{px} \equiv \sum_{x=0}^{q-1} \chi_q(x)\zeta_q^{px} \equiv \tau(p,\chi_q) \equiv \left(\frac{p}{q}\right)\tau(1,\chi_q) \pmod{p} \text{ in } R_q.$$

On multiplying with $\tau(1,\chi_q)$ and applying (4.1), we obtain

$$\tau(1,\chi_q)^{p+1} \equiv (-1)^{(q-1)/2}q\cdot\left(\frac{p}{q}\right) \pmod{p} \text{ in } R_q.$$

On the other hand, by (4.1) and Lemma 4.28,

$$\begin{aligned}\tau(1,\chi_q)^{p+1} &= (-1)^{(q-1)(p+1)/4}q^{(p+1)/2} = (-1)^{(q-1)/2}q\cdot(-1)^{(q-1)(p-1)/4}q^{(p-1)/2}\\ &\equiv (-1)^{(q-1)/2}q\cdot(-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right) \pmod{p} \text{ in } R_q.\end{aligned}$$

As a consequence,

$$(-1)^{(q-1)/2}q\cdot\left(\frac{p}{q}\right) \equiv (-1)^{(q-1)/2}q\cdot(-1)^{(q-1)(p-1)/4}\left(\frac{q}{p}\right) \pmod{p} \text{ in } \mathbb{Z}.$$

Since q is coprime with p, this gives

$$\left(\frac{p}{q}\right) \equiv (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right) \pmod{p} \text{ in } \mathbb{Z}.$$

Since integers equal to ± 1 can be congruent modulo p only if they are equal, this implies Theorem 4.26. □

Exercise 4.1. *Prove Theorem 4.27.*
Hint. *You have to follow the proof of Theorem 4.26, but instead of R_q, χ_q, you have to use the ring $R_8 = \mathbb{Z}[\zeta_8]$ where $\zeta_8 = e^{2\pi i/8}$, and the character χ_8 mod 8, given by*

$$\chi_8(a) = \begin{cases} 1 & \text{if } a \equiv \pm 1 \pmod{8},\\ -1 & \text{if } a \equiv \pm 3 \pmod{8},\\ 0 & \text{if } a \equiv 0 \pmod{2}.\end{cases}$$

Use that ζ_8 has minimal polynomial X^4+1.