Chapter 4

Dirichlet Characters

In this chapter we develop a systematic theory for computing with Dirichlet characters, which are extremely important to computations with modular forms for (at least) two reasons:

1. To compute the Eisenstein subspace $E_k(\Gamma_1(N))$ of $M_k(\Gamma_1(N))$ we explicitly write down Eisenstein series attached to pairs of Dirichlet characters (see Chapter 5).

2. To compute $S_k(\Gamma_1(N))$, we instead compute a decomposition

$$M_k(\Gamma_1(N)) = \bigoplus M_k(\Gamma_1(N), \varepsilon)$$

then compute each factor. Here the sum is over all Dirichlet characters ε modulo N.

Of course Dirichlet characters are also extremely important in much of number theory. For example, they are the one-dimensional characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so are important in studying Galois representations and class field theory for $\mathbb{Q}$.

Example 4.0.1. Expanding on the second enumerated point above, the spaces $M_k(\Gamma_1(N), \varepsilon)$ are frequently much easier to compute with than the full $M_k(\Gamma_1(N))$. As we will see, if $\varepsilon = 1$ is the trivial character, then $M_k(\Gamma_1(N), 1) = M_k(\Gamma_0(N))$, which has much smaller dimension than $M_k(\Gamma_1(N))$. For example, $M_2(\Gamma_1(100))$ has dimension 370, whereas $M_2(\Gamma_1(100), 1)$ has dimension only 24, and $M_2(\Gamma_1(389))$ has dimension 6499, whereas $M_2(\Gamma_1(389), 1)$ has dimension only 33.

```
sage: dimension_modular_forms(Gamma1(100),2)
370
sage: dimension_modular_forms(Gamma0(100),2)
24
sage: dimension_modular_forms(Gamma1(389),2)
6499
sage: dimension_modular_forms(Gamma0(389),2)
33
```

4.1 The Definition

Fix an integral domain R and a root ζ of unity in R.

Definition 4.1.1 (Dirichlet Character)**.** A *Dirichlet character* modulo N over R is a map $\varepsilon : \mathbb{Z} \to R$ such that there is a homomorphism $f : (\mathbb{Z}/N\mathbb{Z})^* \to \langle\zeta\rangle$ for which

$$\varepsilon(a) = \begin{cases} 0 & \text{if } \gcd(a, N) > 1, \\ f\,(a \bmod N) & \text{if } \gcd(a, N) = 1. \end{cases}$$

We denote the group of such Dirichlet characters by $D(N, R)$. Note that elements of $D(N, R)$ are in bijection with homomorphisms $(\mathbb{Z}/N\mathbb{Z})^* \to \langle\zeta\rangle$.

One familiar example of a Dirichlet character is the Legendre symbol $\left(\frac{a}{p}\right)$ that appears in quadratic reciprocity theory. It is a Dirichlet character modulo p that takes the value 1 on integers that are congruent to a nonzero square modulo p, the value -1 on integers that are congruent to a nonzero non-square modulo p, and 0 on integers divisible by p.

4.2 Dirichlet Characters in SAGE

To create a Dirichlet character in SAGE you first create the group $D(N, R)$ of Dirichlet characters, then construct elements of that group. First we make $D(11, \mathbb{Q})$:

```
sage: G = DirichletGroup(11, RationalField()); G
Group of Dirichlet characters of modulus 11 over Rational Field
```

A Dirichlet character prints as a matrix that gives the values of the character on canonical generators of $(\mathbb{Z}/N\mathbb{Z})^*$ (as discussed below).

```
sage: list(G)
[[1], [-1]]
sage: eps = G.0      # 0th generator for Dirichlet group
sage: eps
[-1]
```

The character ε takes the value -1 on the unit generator.

```
sage: G.unit_gens()
[2]
sage: eps(2)
-1
sage: eps(3)
1
```

It is 0 on any integer not coprime to 11:

```
sage: [eps(11*n) for n in range(10)]   # values on 0,11,22,33, ...
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```

We can also create groups of Dirichlet characters taking values in other rings or fields. For example, we create the cyclotomic field $\mathbb{Q}(\zeta_4)$.

```
sage: R = CyclotomicField(4)
sage: CyclotomicField(4)
Cyclotomic Field of order 4 and degree 2
```

Then we define $G = D(15, \mathbb{Q}(\zeta_4)$.

```
sage: G = DirichletGroup(15, R)
sage: G
Group of Dirichlet characters of modulus 15 over Cyclotomic Field
of order 4 and degree 2
```

And we list each of its elements.

```
sage: list(G)
[[1, 1], [-1, 1], [1, zeta_4], [-1, zeta_4], [1, -1], [-1, -1],
 [1, -zeta_4], [-1, -zeta_4]]
```

Now lets evaluate the second generator of G on various integers:

```
sage: e = G.1
sage: e(4)
-1
sage: e(-1)
-1
sage: e(5)
0
```

Finally we list all the values of e.

```
sage: [e(n) for n in range(15)]
[0, 1, zeta_4, 0, -1, 0, 0, zeta_4, -zeta_4,
    0, 0, 1, 0, -zeta_4, -1]
```

We can also compute with groups of Dirichlet characters with values in a finite field.

```
sage: G = DirichletGroup(15, GF(5)); G
Group of Dirichlet characters of modulus 15 over Finite Field of size 5
```

We list all the elements of G, again represented by matrices that give the images

of each unit generator, as an element of $\mathbb{F}_5$.

```
sage: list(G)
  [[1, 1], [4, 1], [1, 2], [4, 2], [1, 4], [4, 4], [1, 3], [4, 3]]
```

We evaluate the second generator of G on several integers.

```
sage: e = G.1
sage: e(-1)
4
sage: e(2)
2
sage: e(5)
0
sage: print [e(n) for n in range(15)]
[0, 1, 2, 0, 4, 0, 0, 2, 3, 0, 0, 1, 0, 3, 4]
```

4.3 Representing Dirichlet Characters

Lemma 4.3.1. *The groups $(\mathbb{Z}/N\mathbb{Z})^*$ and $D(N,\mathbb{C})$ are non-canonically isomorphic.*

Proof. This follows from the more general fact that for any finite abelian group G, we have that $G \approx \mathrm{Hom}(G,\mathbb{C}^*)$. To deduce this latter non-canonical isomorphism, first reduce to the case when G is cyclic of order n, in which case the statement follows because $\mathbb{C}^*$ contains the nth root of unity $e^{2\pi i/n}$, so $\mathrm{Hom}(G,\mathbb{C}^*)$ is also cyclic of order n. □

Corollary 4.3.2. *We have $\#D(N,R) \mid \varphi(N)$, with equality if and only if the order of our choice of $\zeta \in R$ is a multiple of the exponent of the group $(\mathbb{Z}/N\mathbb{Z})^*$.*

Proof. This is because $\#(\mathbb{Z}/N\mathbb{Z})^* = \varphi(N)$. □

Example 4.3.3. The group $D(5,\mathbb{C})$ has elements $\{[1],[i],[-1],[-i]\}$, so is cyclic of order $\varphi(5) = 4$. In contrast, the group $D(5,\mathbb{Q})$ has only the two elements $[1]$ and $[-1]$ and order 2. In SAGE the command `DirichletGroup(N)` with no second argument create the group of Dirichlet characters with values in the cyclotomic field $\mathbb{Q}(\zeta_n)$, where n is the exponent of the group $(\mathbb{Z}/N\mathbb{Z})^*$. Every element in $D(N,\mathbb{C})$ takes values in $\mathbb{Q}(\zeta_n)$, so $D(N,\mathbb{Q}(\zeta_n)) \cong D(N,\mathbb{C})$.

```
sage: list(DirichletGroup(5))
[[1], [zeta_4], [-1], [-zeta_4]]
sage: list(DirichletGroup(5, Q))
[[1], [-1]]
```

Fix a positive integer N, and write $N = \prod_{i=0}^{n} p_i^{e_i}$ where $p_0 < p_1 < \cdots < p_n$ are the prime divisors of N. By Exercise 4.1, each factor $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ is a cyclic

group $C_i = \langle g_i \rangle$, except if $p_0 = 2$ and $e_0 \geq 3$, in which case $(\mathbb{Z}/p_0^{e_0}\mathbb{Z})^*$ is a product of the cyclic subgroup $C_0 = \langle -1 \rangle$ of order 2 with the cyclic subgroup $C_1 = \langle 5 \rangle$. In all cases we have

$$(\mathbb{Z}/N\mathbb{Z})^* \cong \prod_{0 \leq i \leq n} C_i = \prod_{0 \leq i \leq n} \langle g_i \rangle.$$

For i such that $p_i > 2$, choose the generator g_i of C_i to be the element of $\{2, 3, \ldots, p_i^{e_i} - 1\}$ that is smallest and generates. Finally, use the Chinese Remainder Theorem (see [Coh93, §1.3.3])) to lift each g_i to an element in $(\mathbb{Z}/N\mathbb{Z})^*$, also denoted g_i, that is 1 modulo each $p_j^{e_j}$ for $j \neq i$.

Algorithm 4.3.4 (Minimal generator for $(\mathbb{Z}/p^r\mathbb{Z})^*$)**.** *Given an odd prime power p^r, this algorithm computes the minimal generator for $(\mathbb{Z}/p^r\mathbb{Z})^*$.*

1. [Factor Group Order] Factor $n = \phi(p^r) = p^{r-1} \cdot 2 \cdot ((p-1)/2)$ as a product $\prod p_i^{e_i}$ of primes. This is equivalent in difficulty to factoring $(p-1)/2$. (See, e.g., [Coh93, Ch.8, Ch. 10] for an excellent discussion of factorization algorithms, though of course much progress has been made since then.)
2. [Initialize] Set $g = 2$.
3. [Generator?] Using the binary powering algorithm (see [Coh93, §1.2]), compute $g^{n/p_i} \pmod{p^r}$, for each prime divisor p_i of n. If any of these powers are 1, then g is not a generator, so set $g = g + 1$ and go to Step 2. If no powers are 1, output g and terminate.

See Exercise 4.2 for a proof that this algorithm is correct.

Example 4.3.5. A minimal generator for $(\mathbb{Z}/49\mathbb{Z})^*$ is 3. We have $n = \varphi(49) = 42 = 2 \cdot 3 \cdot 7$, and

$$2^{n/2} \equiv 1, \qquad 2^{n/3} \equiv 18, \qquad 2^{n/7} \equiv 15 \pmod{49}.$$

so 2 is not a generator for $(\mathbb{Z}/49\mathbb{Z})^*$. (We see this just from $2^{n/2} \equiv 1 \pmod{49}$.) However 3 is since

$$3^{n/2} \equiv 48, \qquad 3^{n/3} \equiv 30, \qquad 3^{n/7} \equiv 43 \pmod{49}.$$

Example 4.3.6. In this example we compute minimal generators for $N = 25$, 100, and 200:

1. The minimal generator for $(\mathbb{Z}/25\mathbb{Z})^*$ is 2.
2. Minimal generators for $(\mathbb{Z}/100\mathbb{Z})^*$, lifted to numbers modulo 100, are $g_0 = 51$ and $g_1 = 77$. Notice that $g_0 \equiv -1 \pmod 4$ and $g_0 \equiv 1 \pmod{25}$, and $g_1 \equiv 2 \pmod{25}$ is the minimal generator modulo 25.
3. Minimal generators for $(\mathbb{Z}/200\mathbb{Z})^*$, lifted to numbers modulo 200, are $g_0 = 151$, $g_1 = 101$, and $g_2 = 177$. Note that $g_0 \equiv -1 \pmod 4$, that $g_1 \equiv 5 \pmod 8$, and $g_2 \equiv 2 \pmod{25}$.

In SAGE, the command `Integers(N)` creates $\mathbb{Z}/N\mathbb{Z}$.

```
sage: R = Integers(49)
sage: R
Ring of integers modulo 49
```

The `unit_gens()` command computes the unit generators as defined above.

```
sage: R.unit_gens()
[3]
sage: Integers(25).unit_gens()
[2]
sage: Integers(100).unit_gens()
[51, 77]
sage: Integers(200).unit_gens()
[151, 101, 177]
sage: Integers(2005).unit_gens()
[402, 1206]
sage: Integers(200000000).unit_gens()
[174218751, 51562501, 187109377]
```

Fix an element ζ of finite multiplicative order in a ring R, and let $D(N, R)$ denote the group of Dirichlet characters modulo N over R, with image in $\langle\zeta\rangle \cup \{0\}$. We specify an element $\varepsilon \in D(N, R)$ by giving the list

$$[\varepsilon(g_0), \varepsilon(g_1), \ldots, \varepsilon(g_n)] \tag{4.3.1}$$

of images of the generators of $(\mathbb{Z}/N\mathbb{Z})^*$. (Note if N is even, the number of elements of the list (4.3.1) does *not* depend on whether or not $8 \mid N$—there are always two factors corresponding to 2.) This representation completely determines ε and is convenient for arithmetic operations with Dirichlet characters. It is analogous to representing a linear transformation by a matrix. See Section 4.7 for a discussion of alternative ways to represent Dirichlet characters.

4.4 Evaluation of Dirichlet Characters

This section is about how to compute $\varepsilon(n)$, where ε is a Dirichlet character and n is an integer. We begin with an example.

Example 4.4.1. If $N = 200$, then $g_0 = 151$, $g_1 = 101$ and $g_2 = 177$, as we saw in Example 4.3.6. The exponent of $(\mathbb{Z}/200\mathbb{Z})^*$ is 20, since that is the least common multiple of the exponents of $4 = \#(\mathbb{Z}/8\mathbb{Z})^*$ and $20 = \#(\mathbb{Z}/25\mathbb{Z})^*$. The orders of g_0, g_1 and g_2 are 2, 2, and 20. Let $\zeta = \zeta_{20}$ be a primitive 20th root of unity in $\mathbb{C}$. Then the following are generators for $D(200, \mathbb{C})$:

$$\varepsilon_0 = [-1, 1, 1], \qquad \varepsilon_1 = [1, -1, 1], \qquad \varepsilon_2 = [1, 1, \zeta],$$

and $\varepsilon = [1, -1, \zeta^5]$ is an example element of order 4. To evaluate $\varepsilon(3)$, we write 3 in terms of g_0, g_1, and g_2. First, reducing 3 modulo 8, we see that $3 \equiv g_0 \cdot g_1 \pmod 8$. Next reducing 3 modulo 25, and trying powers of $g_2 = 2$, we find that $e \equiv g_2^7 \pmod{25}$. Thus

$$\begin{aligned}\varepsilon(3) &= \varepsilon(g_0 \cdot g_1 \cdot g_2^7) \\ &= \varepsilon(g_0)\varepsilon(g_1)\varepsilon(g_2)^7 \\ &= 1 \cdot (-1) \cdot (\zeta^5)^7 \\ &= -\zeta^{35} = -\zeta^{15}.\end{aligned}$$

We next illustrate the above computation of $\varepsilon(3)$ in SAGE. First we make the group $D(200, \mathbb{Q}(\zeta_8))$, and list its generators.

```
sage: G = DirichletGroup(200)
sage: G
Group of Dirichlet characters of modulus 200 over Cyclotomic Field
      of order 20 and degree 8
sage: G.exponent()
20
sage: G.gens()
([-1, 1, 1], [1, -1, 1], [1, 1, zeta_20])
```

We construct ε.

```
sage: K.<zeta> = G.base_ring()
sage: eps = G([1,-1,zeta^5])
sage: eps
[1, -1, zeta_20^5]
```

Finally, we evaluate ε at 3.

```
sage: eps(3)
zeta_20^5
sage: -zeta^15
zeta_20^5
```

Example 4.4.1 illustrates that if ε is represented using a list as described above, evaluation of ε is inefficient without extra information; it requires solving the discrete log problem in $(\mathbb{Z}/N\mathbb{Z})^*$. In fact, for a general character ε calculation of ε will probably be at least as hard as finding discrete logarithms no matter what representation we use (quadratic characters are easier—see Algorithm 4.4.5).

Algorithm 4.4.2 (Evaluate ε)**.** *Given a Dirichlet character ε modulo N, represented by a list $[\varepsilon(g_0), \varepsilon(g_1), \ldots, \varepsilon(g_n)]$, and an integer a, this algorithm computes $\varepsilon(a)$.*

1. [GCD] Compute $g = \gcd(a, N)$. If $g > 1$, output 0 and terminate.

2. [Discrete Log] For each i, write $a \pmod{p_i^{e_i}}$ as a power m_i of g_i using some algorithm for solving the discrete log problem (see below). If $p_i = 2$, write $a \pmod{p_i^{e_i}}$ as $(-1)^{m_0} \cdot 5^{m_1}$. (This step is analogous to writing a vector in terms of a basis.)
3. [Multiply] Compute and output $\prod \varepsilon(g_i)^{m_i}$ as an element of R, and terminate. (This is analogous to multiplying a matrix times a vector.)

4.4.1 The Discrete log problem

By Exercise 4.3 we have an isomorphism of groups

$$(1 + p^{n-1}(\mathbb{Z}/p^n\mathbb{Z}),\ \times) \cong (\mathbb{Z}/p\mathbb{Z},\ +),$$

so one sees by induction that Step 2 is "about as difficult" as finding a discrete log in $(\mathbb{Z}/p\mathbb{Z})^*$. There is an algorithm called "baby-step giant-step", which solves the discrete log problem in $(\mathbb{Z}/p\mathbb{Z})^*$ in time $O(\sqrt{\ell})$, where ℓ is the largest prime factor of $p - 1 = \#(\mathbb{Z}/p\mathbb{Z})^*$ (note that the discrete log problem in $(\mathbb{Z}/p\mathbb{Z})^*$ reduces to a series of discrete log problems in each prime-order cyclic factor). This is unfortunately still exponential in the number of digits of ℓ; it also uses $O(\sqrt{\ell})$ memory. We now describe this algorithm without any specific optimizations.

Algorithm 4.4.3 (Baby-Step Giant Step Discrete Log)**.** *Given a prime p, a generator g of $(\mathbb{Z}/p\mathbb{Z})^*$, and an element $a \in (\mathbb{Z}/p\mathbb{Z})^*$, this algorithm finds an n such that $g^n = a$. (Note that this algorithm works in any cyclic group, not just $(\mathbb{Z}/p\mathbb{Z})^*$.)*

1. [Make Lists] Let $m = \lceil \sqrt{p} \rceil$ be the ceiling of $\sqrt{p}$, and construct two lists

$$g,\ g^m,\ \ldots,\ g^{(m-1)m}, g^{m^2} \qquad \text{(giant steps)}$$

and

$$ag,\ ag^2,\ \ldots,\ ag^{m-1}, ag^m \qquad \text{(baby steps)}.$$

2. [Find Match] Sort the two lists and find a match $g^{im} = ag^j$. Then $a = g^{im-j}$.

Proof. We prove that there will always be a match. Since we know that $a = g^k$ for some k with $0 \le k \le p-1$ and any such k can be written in the form $im - j$ for $0 \le i, j \le m - 1$, we will find such a match. □

Algorithm 4.4.3 uses nothing special about $(\mathbb{Z}/p\mathbb{Z})^*$, so it works in a generic group. It is a theorem that there is no faster algorithm to find discrete logs in a "generic group" (see [Sho97, Nec94]). Fortunately there are much better subexponential algorithms for solving the discrete log problem in $(\mathbb{Z}/p\mathbb{Z})^*$, which use the special structure of this group. They use the number field sieve (see e.g., [Gor93]), which is also the best known algorithm for factoring integers. This class of algorithms has been very well studied by cryptographers;

though sub-exponential, solving discrete log problems when p is large is still extremely difficult. For a more in-depth survey see [Gor04]. These algorithms are particularly relevant when p is large, and their development is motivated mainly by their application to breaking cryptosystems. For computing Dirichlet characters in our context, p is not too large, so Algorithm 4.4.3 works well.

4.4.2 Enumeration of all values

The applications of Dirichlet characters in this book involve computing modular forms, and for these applications N will be fairly small, e.g., $N < 10^6$. Also we will evaluate ε on a *huge* number of random elements, inside inner loops of algorithms. Thus for our purposes it will often be better to make a table of all values of ε, so that evaluation of ε is extremely fast. The following algorithm computes a table of all values of ε, and it does not require computing any discrete logs since we are computing *all* values.

Algorithm 4.4.4 (Values of ε)**.** *Given a Dirichlet character ε represented by the list of values of ε on the minimal generators g_i of $(\mathbb{Z}/N\mathbb{Z})^*$, this algorithm creates a list of all the values of ε.*

1. [Initialize] For each minimal generator g_i, set $a_i = 0$. Let $n = \prod g_i^{a_i}$, and set $z = 1$. Create a list v of N values, all initially set equal to 0. When this algorithm terminates the list v will have the property that
$$v\,[x \pmod N] = \varepsilon(x).$$
Notice that we index v starting at 0.
2. [Add Value to Table] Set $v[n] = z$.
3. [Finished?] If each a_i is one less than the order of g_i, output v and terminate.
4. [Increment] Set $a_0 = a_0 + 1$, $n = n \cdot g_0 \pmod N$, and $z = z \cdot \varepsilon(g_0)$. If $a_0 \geq \mathrm{ord}(g_0)$, set $a_0 \to 0$, then set $a_1 = a_1 + 1$, $n = n \cdot g_1 \pmod N$, and $z = z \cdot \varepsilon(g_1)$. If $a_1 \geq \mathrm{ord}(g_1)$, do what you just did with a_0, but with all subscripts replaced by 1. Etc. (Imagine a car odometer.) Go to Step 2.

4.4.3 Quadratic characters

Frequently people describe quadratic characters in terms of the Kronecker symbol. The following algorithm gives a way to go between the two representations.

Algorithm 4.4.5 (Kronecker Symbol)**.** *Given an integer N, this algorithm computes a representation of the Kronecker symbol $\left(\frac{a}{N}\right)$ as a Dirichlet character.*

1. Compute the minimal generators g_i of $(\mathbb{Z}/N\mathbb{Z})^*$ using Algorithm 4.3.4.
2. Compute $\left(\frac{g_i}{N}\right)$ for each g_i using one of the algorithms of [Coh93, §1.1.4].

Remark 4.4.6. The algorithms in [Coh93, §1.1.4] for computing the Kronecker symbol run in time quadratic in the number of digits of the input, so they do not require computing discrete logarithms. (They use, e.g., that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$, when p is an odd prime.) If N is very large and we are only interested in evaluating $\varepsilon(a) = \left(\frac{a}{N}\right)$ for a few a, then viewing ε as a Dirichlet character in the sense of this chapter leads to a less efficient way to compute with ε. The algorithmic discussion of characters in this chapter is most useful for working with the full group of characters, and non-quadratic characters.

Example 4.4.7. We compute the Dirichlet character associated to the Kronecker symbol $\left(\frac{a}{200}\right)$. We find that $\left(\frac{g_i}{200}\right)$, for $i = 0, 1, 2$, where the g_i are as in Example 4.4.1:

```
sage: kronecker(151,200)
1
sage: kronecker(101,200)
-1
sage: kronecker(177,200)
1
```

Thus the corresponding character is defined by $[1, -1, 1]$.

Example 4.4.8. We compute the character associated to $\left(\frac{a}{420}\right)$. We have $420 = 4 \cdot 3 \cdot 5 \cdot 7$, and minimal generators are

$$g_0 = 211, \quad g_1 = 1, \quad g_2 = 281, \quad g_3 = 337, \quad g_4 = 241.$$

We have $g_0 \equiv -1 \pmod{4}$, $g_2 \equiv 2 \pmod{3}$, $g_3 \equiv 2 \pmod{5}$ and $g_4 \equiv 3 \pmod{7}$. Using SAGE again we find $\left(\frac{g_0}{420}\right) = \left(\frac{g_1}{420}\right) = 1$ and $\left(\frac{g_2}{420}\right) = \left(\frac{g_3}{420}\right) = \left(\frac{g_4}{420}\right) = -1$, so the corresponding character is $[1, 1, -1, -1, -1]$.

4.5 Conductors of Dirichlet characters

The following algorithm for computing the order of ε reduces the problem to computing the orders of powers of ζ in R.

Algorithm 4.5.1 (Order of Character)**.** *This algorithm computes the order of a Dirichlet character $\varepsilon \in D(N, R)$.*

1. Compute the order r_i of each $\varepsilon(g_i)$, for each minimal generator g_i of $(\mathbb{Z}/N\mathbb{Z})^*$. Since the order of $\varepsilon(g_i)$ is divisor of $n = \#(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$, we can compute its order by factoring n and considering the divisors of n.
2. Compute and output the least commmon multiple of the integers r_i.

Remark 4.5.2. Computing the order of $\varepsilon(g_i) \in R$ is potentially difficult and tedious. Using a different (simultaneous) representation of Dirichlet characters avoids having to compute the order of elements of R. See Section 4.7.

The next algorithm factors ε as a product of "local" characters, one for each prime divisor of N. It is useful for other algorithms, e.g., for explicit computations with trace formuls (see [Hij74]). This factorization is easy to compute because of how we represent ε.

Algorithm 4.5.3 (Factorization of Character)**.** *Given a Dirichlet character $\varepsilon \in D(N, R)$, with $N = \prod p_i^{e_i}$, this algorithm finds Dirichlet characters ε_i modulo $p_i^{e_i}$, such that for all $a \in (\mathbb{Z}/N\mathbb{Z})^*$, we have $\varepsilon(a) = \prod \varepsilon_i(a \pmod{p_i^{e_i}})$. If $2 \mid N$, the steps are as follows:*

1. Let g_i be the minimal generators of $(\mathbb{Z}/N\mathbb{Z})^*$, so ε is given by a list
$$[\varepsilon(g_0), \ldots, \varepsilon(g_n)].$$
2. For $i = 2, \ldots, n$, let ε_i be the element of $D(p_i^{e_i}, R)$ defined by the singleton list $[\varepsilon(g_i)]$.
3. Let ε_1 be the element of $D(2^{e_1}, R)$ defined by the list $[\varepsilon(g_0), \varepsilon(g_1)]$ of length 2. Output the ε_i and terminate.

If $2 \nmid N$, then omit Step 3, and include all i in Step 2.

The factorization of Algorithm 4.5.3 is unique since each ε_i is determined by the image of the canonical map $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ in $(\mathbb{Z}/N\mathbb{Z})^*$, which sends $a \pmod{p_i^{e_i}}$ to the element of $(\mathbb{Z}/N\mathbb{Z})^*$ that is $a \pmod{p_i^{e_i}}$ and $1 \pmod{p_j^{e_j}}$ for $j \neq i$.

Example 4.5.4. If $\varepsilon = [1, -1, \zeta^5] \in D(200, \mathbb{C})$, then $\varepsilon_1 = [1, -1] \in D(8, \mathbb{C})$ and $\varepsilon_2 = [\zeta^5] \in D(25, \mathbb{C})$.

Definition 4.5.5 (Conductor)**.** The *conductor* of a Dirichlet character $\varepsilon \in D(N, R)$ is the smallest positive divisor $c \mid N$ such that there is a character $\varepsilon' \in D(c, R)$ for which $\varepsilon(a) = \varepsilon'(a)$ for all $a \in \mathbb{Z}$ with $(a, N) = 1$. A Dirichlet character is *primitive* if its modulus equals its conductor. The character ε' associated to ε with modulus equal to the conductor of ε is called the *primitive character associated to* ε.

We will be interested in conductors later, when computing new subspaces of spaces of modular forms with character. Also certain formulas for special values of L functions are only valid for primitive characters.

Algorithm 4.5.6 (Conductor)**.** *This algorithm computes the conductor of a Dirichlet character $\varepsilon \in D(N, R)$.*

1. [Factor Character] Using Algorithm 4.5.3, find characters ε_i whose product is ε.
2. [Compute Orders] Using Algorithm 4.5.1, compute the orders r_i of each ε_i.
3. [Conductors of Factors] For each i, either set $c_i \to 1$ if ε_i is the trivial character (i.e., of order 1), or set $c_i = p_i^{\mathrm{ord}_{p_i}(r_i)+1}$, where $\mathrm{ord}_p(n)$ is the largest power of p that divides n.

4. [Adjust at 2?] If $p_1 = 2$ and $\varepsilon_1(5) \neq 1$, set $c_1 = 2c_1$.
5. [Finished] Output $c = \prod c_i$ and terminate.

Proof. Let ε_i be the local factors of ε, as in Step 1. We first show that the product of the conductors f_i of the ε_i is the conductor f of ε. Since ε_i factors through $(\mathbb{Z}/f_i\mathbb{Z})^*$, the product ε of the ε_i factors through $(\mathbb{Z}/\prod f_i\mathbb{Z})^*$, so the conductor of ε divides $\prod f_i$. Conversely, if $\mathrm{ord}_{p_i}(f) < \mathrm{ord}_{p_i}(f_i)$ for some i, then we could factor ε as a product of local (prime power) characters differently, which contradicts that this factorization is unique.

It remains to prove that if ε is a nontrivial character modulo p^n, where p is a prime, and r is the order of ε, then the conductor of ε is $p^{\mathrm{ord}_p(r)+1}$, except possibly if $8 \mid p^n$. Since the order and conductor of ε and of the associated primitive character ε' are the same, we may assume ε is primitive, i.e., that p^n is the conductor of ε; note that $n > 0$, since ε is nontrivial.

First suppose p is odd. Then the abelian group $D(p^n, R)$ splits as a direct sum $D(p, R) \oplus D(p^n, R)'$, where $D(p^n, R)'$ is the p-power torsion subgroup of $D(p^n, R)$. Also ε has order $u \cdot p^m$, where u, which is coprime to p, is the order of the image of ε in $D(p, R)$ and p^m is the order of the image in $D(p^n, R)'$. If $m = 0$, then the order of ε is coprime to p, so ε is in $D(p, R)$, which means that $n = 1$, so $n = m + 1$, as required. If $m > 0$, then $\zeta \in R$ must have order divisible by p, so R has characteristic not equal to p. The conductor of ε does not change if we adjoin roots of unity to R, so in light of Lemma 4.3.1 we may assume that $D(N, R) \approx (\mathbb{Z}/N\mathbb{Z})^*$. It follows that for each $n' \leq n$, the p-power subgroup $D(p^{n'}, R)'$ of $D(p^{n'}, R)$ is the $p^{n'-1}$-torsion subgroup of $D(p^n, R)'$. Thus $m = n - 1$, since $D(p^n, R)'$ is by assumption the smallest such group that contains the projection of ε. This proves the formula of Step 3. We leave the argument when $p = 2$ as an exercise (see Exercise 4.4). □

Example 4.5.7. If $\varepsilon = [1, -1, \zeta^5] \in D(200, \mathbb{C})$, then as we saw in Example 4.5.4, ε is the product of $\varepsilon_1 = [1, -1]$ and $\varepsilon_2 = [\zeta^5]$. Because $\varepsilon_1(5) = -1$, the conductor of ε_1 is 8. The order of ε_2 is 4 (since ζ is a 20th root of unity), so the conductor of ε_2 is 5. Thus the conductor of ε is $40 = 8 \cdot 5$.

4.6 Restriction, Extension, and Galois Orbits

The following two algorithms restrict and extend characters to a compatible modulus. Using them it is easy to define multiplication of two characters $\varepsilon \in D(N, R)$ and $\varepsilon' \in D(N', R')$, as long as R and R' are subrings of a common ring. To carry out the multiplication, just extend both characters to a common base ring, then extend them to characters modulo $\mathrm{lcm}(N, N')$, then multiply.

Algorithm 4.6.1 (Restriction of Character)**.** *Given a Dirichlet character $\varepsilon \in D(N, R)$ and a divisor N' of N that is a multiple of the conductor of ε, this algorithm finds a characters $\varepsilon' \in D(N', R)$, such that $\varepsilon'(a) = \varepsilon(a)$, for all $a \in \mathbb{Z}$ with $(a, N) = 1$.*

1. [Conductor] Compute the conductor of ε using Algorithm 4.5.6, and verify that indeed N' is divisible by the conductor and divides N.
2. [Minimal Generators] Compute the minimal generators g_i for $(\mathbb{Z}/N'\mathbb{Z})^*$.
3. [Values of Restriction] For each i, compute $\varepsilon'(g_i)$ as follows. Find a multiple aN' of N' such that $(g_i + aN',\ N) = 1$; then $\varepsilon'(g_i) = \varepsilon(g_i + aN')$.
4. [Output Character] Output the Dirichlet character modulo N' defined by $[\varepsilon'(g_0), \ldots, \varepsilon'(g_n)]$.

Proof. The only part that is not clear is that in Step 3 there is an a such that $(g_i + aN', N) = 1$. If we write $N = N_1 \cdot N_2$, with $(N_1, N_2) = 1$, and N_1 divisible by all primes that divide N', then $(g_i, N_1) = 1$ since $(g_i, N') = 1$. By the Chinese Remainder Theorem, there is an $x \in \mathbb{Z}$ such that $x \equiv g_i \pmod{N_1}$ and $x \equiv 1 \pmod{N_2}$. Then $x = g_i + bN_1 = g_i + (bN_1/N') \cdot N'$ and $(x, N) = 1$, which completes the proof. □

Algorithm 4.6.2 (Extension of Character)**.** *Given a Dirichlet character $\varepsilon \in D(N, R)$ and a multiple N' of N, this algorithm finds a characters $\varepsilon' \in D(N', R)$, such that $\varepsilon'(a) = \varepsilon(a)$, for all $a \in \mathbb{Z}$ with $(a, N') = 1$.*

1. [Minimal Generators] Compute the minimal generators g_i for $(\mathbb{Z}/N'\mathbb{Z})^*$.
2. [Evaluate] Compute $\varepsilon(g_i)$ for each i. Since $(g_i, N') = 1$, we also have $(g_i, N) = 1$.
3. [Output Character] Output the character defined by $[\varepsilon(g_0), \ldots, \varepsilon(g_n)]$.

We finish with an algorithm that computes the Galois orbit of an element in $D(N, R)$. This can be used to divide $D(N, R)$ up into Galois orbits, which is useful for modular forms computations, because, e.g., the spaces $M_k(\Gamma_1(N))(\varepsilon)$ and $M_k(\Gamma_1(N))(\varepsilon')$ are canonically isomorphic if ε and ε' are conjugate.

Algorithm 4.6.3 (Galois Orbit)**.** *Given a Dirichlet character $\varepsilon \in D(N, R)$, this algorithm computes the orbit of ε under the action of $G = \mathrm{Gal}(\overline{F}/F)$, where F is the prime subfield of* $\mathrm{Frac}(R)$*, so $F = \mathbb{F}_p$ or $\mathbb{Q}$.*

1. [Order of ζ] Let n be the order of the chosen root $\zeta \in R$.
2. [Nontrivial Automorphisms] If $\mathrm{char}(R) = 0$, let
$$A = \{a : 2 \le a < n \text{ and } (a, n) = 1\}.$$
If $\mathrm{char}(R) = p > 0$, compute the multiplicative order r of p modulo n, and let
$$A = \{p^m : 1 \le m < r\}.$$
3. [Compute Orbit] Compute and output the *set* of unique elements ε^a for each $a \in A$ (there could be repeats, so we output unique elements only).

Proof. We prove that the nontrivial automorphisms of $\langle\zeta\rangle$ in characteristic p are as in Step 2. It is well-known that every automorphism in characteristic p on $\zeta \in \overline{\mathbb{F}}_p$ is of the form $x \mapsto x^{p^s}$, for some s. The images of ζ under such automorphisms are

$$\zeta, \zeta^p, \zeta^{p^2}, \ldots.$$

Suppose $r > 0$ is minimal such that $\zeta = \zeta^{p^r}$. Then the orbit of ζ is $\zeta, \ldots, \zeta^{p^{r-1}}$. Also $p^r \equiv 1 \pmod{n}$, where n is the multiplicative order of ζ, so r is the multiplicative order of p modulo n, which completes the proof. □

Example 4.6.4. The Galois orbits of characters in $D(20, \mathbb{C}^*)$ are as follows:

$$\begin{aligned}
G_0 &= \{[1,1,1]\},\\
G_1 &= \{[-1,1,1]\},\\
G_2 &= \{[1,1,\zeta_4],\ [1,1,-\zeta_4]\}\\
G_3 &= \{[-1,1,\zeta_4],\ [-1,1,-\zeta_4]\}\\
G_4 &= \{[1,1,-1]\},\\
G_5 &= \{[-1,1,-1]\}
\end{aligned}$$

The conductors of the characters in orbit G_0 are 1, in order G_1 are 4, in orbit G_2 they are 5, in G_3 they are 20, in G_4 the conductor is 5, and in G_5 the conductor is 20. (You should verify this.)

SAGE computes Galois orbits as follows:

```
sage: G = DirichletGroup(20)
sage: G.galois_orbits()
[[[1, 1]], [[-1, 1]],
 [[1, zeta4], [1, -zeta4]],
 [[-1, zeta4], [-1, -zeta4]],
 [[1, -1]], [[-1, -1]]]
```

4.7 Alternative Representations of Characters

Let N be a positive integer and R an integral domain, with fixed root of unity ζ order n, and let $D(N,R) = D(N,R,\zeta)$. As in the rest of this chapter, write $N = \prod p_i^{e_i}$, and let $C_i = \langle g_i\rangle$ be the corresponding cyclic factors of $(\mathbb{Z}/N\mathbb{Z})^*$. In this section we discuss other ways to represent elements $\varepsilon \in D(N,R)$. Each representation has advantages and disadvantages, and no single representation is best. It emerged while writing this chapter that simultaneously using more than one representation of elements of $D(N,R)$ would be best. It is easy to convert between them, and some algorithms are much easier using one representation, than when using another. In this section we present two other representations, each which has advantages and disadvantages. But, we emphasize that there is frequently no reason to restrict to only one representation!

We could represent ε by giving a list $[b_0, \ldots, b_n]$, where each $b_i \in \mathbb{Z}/n\mathbb{Z}$ and $\varepsilon(g_i) = \zeta^{b_i}$. Then arithmetic in $D(N, R)$ is arithmetic in $(\mathbb{Z}/n\mathbb{Z})^{n+1}$, which is very efficient. A drawback to this approach is that it is easy to accidently consider sequences that do not actually correspond to elements of $D(N, R)$, though it is not really any easier to do this than with the representation we use elsewhere in this chapter. Also the choice of ζ is less clear, which can cause confusion. Finally, the orders of the local factors is more opaque, e.g., compare $[-1, \zeta_{40}]$ with $[20, 1]$. Overall this representation is not too bad, and is more like representing a linear transformation by a matrix. It has the *advantage* over the representation discussed earlier in this chapter that arithmetic in $D(N, R)$ is very efficient, and doesn't require any operations in the ring R; such operations could be quite slow, e.g., if R were a large cyclotomic field.

Another way to represent ε would be to give a list $[b_0, \ldots, b_n]$ of integers, but this time with $b_i \in \mathbb{Z}/\gcd(s_i, n)\mathbb{Z}$, where s_i is the order of g_i. Then

$$\varepsilon(g_i) = \zeta^{b_i \cdot n/(\gcd(s_i,n))},$$

which is already complicated enough to ring warning bells. With this representation we set up an identification

$$D(N, R) \cong \bigoplus_i \mathbb{Z}/\gcd(s_i, n)\mathbb{Z},$$

and arithmetic is efficient. This approach is seductive because every sequence of integers determines a character, and the sizes of the integers in the sequence nicely indicate the local orders of the character. However, giving analogues of many of the algorithms discussed in this chapter that operate on characters represented this way is tricky. For example, the representation depends very much on the order of ζ, so it is difficult to correctly compute natural maps $D(N, R) \to D(N, S)$, for $R \subset S$ rings, whereas for the representation elsewhere in this chapter such maps are trivial to compute. This was the representation the author (Stein) implemented in MAGMA.

The PARI documentation says the following (where we have preserved the incorrect typesetting):

> "A *character* on the Abelian group $\oplus(\mathbb{Z}/N_i\mathbb{Z})g_i$ is given by a row vector $\chi = [a_1, \ldots, a_n]$ such that $\chi(\prod g_i^{n_i}) = \exp(2i\pi \sum a_i n_i/N_i)$."

This means that the abelian group has independent generators g_i of order N_i. This definition says that, e.g., the value of the character on g_1 is

$$\chi(g_1) = (e^{2\pi i/N_1})^{a_1}.$$

Thus the integers a_i are integers modulo N_i, and this representation is basically the same as the one we described in the previous paragraph (and which the author does not like).

4.8 Exercises

4.1 This exercise is about the structure of the units of $\mathbb{Z}/p^n\mathbb{Z}$.

(a) If p is odd and n is a positive integer, prove that $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic.

(b) If $n \geq 3$ prove that $(\mathbb{Z}/2^n\mathbb{Z})^*$ is a direct sum of the cylclic subgroups $\langle -1 \rangle$ and $\langle 5 \rangle$, of orders 2 and 2^{n-2}, respectively.

4.2 Prove that Algorithm 4.3.4 works, i.e., that if $g \in (\mathbb{Z}/p^r\mathbb{Z})^*$ and $g^{n/p_i} \neq 1$ for all $p_i \mid n = \varphi(n)$, then g is a generator of $(\mathbb{Z}/p^r\mathbb{Z})^*$.

4.3 Let p be an odd prime and $n \geq 2$ an integer, and prove that

$$(1 + p^{n-1}(\mathbb{Z}/p^n\mathbb{Z}),\ \times) \cong (\mathbb{Z}/p\mathbb{Z},\ +).$$

Use this to show that solving the discrete log problem in $(\mathbb{Z}/p^n\mathbb{Z})^*$ is "not much harder" than solving the discrete log problem in $(\mathbb{Z}/p\mathbb{Z})^*$.

4.4 Suppose ε is a nontrivial Dirichlet character modulo 2^n of order r over the complex numbers $\mathbb{C}$. Prove that the conductor of ε is

$$c = \begin{cases} 2^{\mathrm{ord}_2(r)+1} & \text{if } \varepsilon(5) = 1 \\ 2^{\mathrm{ord}_2(r)+2} & \text{if } \varepsilon(5) \neq 1. \end{cases}$$

4.5 (a) Find an irreducible quadratic polynomial f over $\mathbb{F}_5$.

(b) Then $\mathbb{F}_{25} = \mathbb{F}_5[x]/(f)$. Find an element with multiplicative order 5 in $\mathbb{F}_{25}$.

(c) Make a list of all Dirichlet characters in $D(25, \mathbb{F}_{25}, \zeta)$.

(d) Divide these characters up into orbits for the action of $\mathrm{Gal}(\overline{\mathbb{F}}_5/\mathbb{F}_5)$.