Chapter 6

The Dirichlet Unit Theorem

As usual, we will be working in the ring B of algebraic integers of a number field L. Two factorizations of an element of B are regarded as essentially the same if one is obtained from the other by multiplication by a unit. Our experience with the integers, where the only units are ± 1, and the Gaussian integers, where the only units are ± 1 and $\pm i$, suggests that units are not very complicated, but this is misleading. The Dirichlet unit theorem gives a complete description of the structure of the multiplicative group of units in a number field.

6.1 Preliminary Results

6.1.1 Lemma

Let B^* be the group of units of B. An element $x \in B$ belongs to B^* if and only if $N(x) = \pm 1$.

Proof. If $xx^{-1} = 1$, then $1 = N(1) = N(xx^{-1}) = N(x)N(x^{-1})$, so the integer $N(x)$ must be ± 1. Conversely, if the norm of x is ± 1, then the characteristic equation of x has the form $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x \pm 1 = 0$, with the $a_i \in \mathbb{Z}$ [see (2.1.3) and (2.2.2)]. Thus $x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2 x + a_1) = \mp 1$. ♣

6.1.2 The Logarithmic Embedding

Let $\sigma : L \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = \mathbb{R}^n$ be the canonical embedding defined in (5.3.1). The *logarithmic embedding* is the mapping $\lambda : L^* \to \mathbb{R}^{r_1+r_2}$ given by

$$\lambda(x) = (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1+r_2}(x)|).$$

Since the σ_i are monomorphisms, $\lambda(xy) = \lambda(x) + \lambda(y)$, so λ is a homomorphism from the multiplicative group of L^* to the additive group of $\mathbb{R}^{r_1+r_2}$.

6.1.3 Lemma

Let C be a bounded subset of $\mathbb{R}^{r_1+r_2}$, and let $C' = \{x \in B^* : \lambda(x) \in C\}$. Then C' is a finite set.

Proof. Since C is bounded, all the numbers $|\sigma_i(x)|, x \in B^*, i = 1, \dots, n$, will be confined to some interval $[a^{-1}, a]$ with $a > 1$. Thus the elementary symmetric functions of the $\sigma_i(x)$ will also lie in some interval of this type. But by (2.1.6), the elementary symmetric functions are the coefficients of the characteristic polynomial of x, and by (2.2.2), these coefficients are integers. Thus there are only finitely many possible characteristic polynomials of elements $x \in C'$, hence by (2.1.5), only finitely many possible roots of minimal polynomials of elements $x \in C'$. We conclude that x can belong to C' for only finitely many x. ♣

6.1.4 Corollary

The kernel G of the homomorphism λ restricted to B^* is a finite group.

Proof. Take $C = \{0\}$ in (6.1.3). ♣

The following result gives additional information about G.

6.1.5 Proposition

Let H be a finite subgroup of K^*, where K is an arbitrary field. Then H consists of roots of unity and is cyclic.

Proof. Let z be an element of H whose order n is the exponent of H, that is, the least common multiple of the orders of all the elements of H. Then $y^n = 1$ for every $y \in H$, so H consists of roots of unity. Since the polynomial $X^n - 1$ has at most n distinct roots, we have $|H| \leq n$. But $1, z, \dots, z^{n-1}$ are distinct elements of H, because z has order n. Thus H is cyclic. ♣

For our group G, even more is true.

6.1.6 Proposition

The group G consists exactly of all the roots of unity in the field L.

Proof. By (6.1.5), every element of G is a root of unity. Conversely, suppose $x^m = 1$. Then x is an algebraic integer (it satisfies $X^m - 1 = 0$) and for every i,

$$|\sigma_i(x)|^m = |\sigma_i(x^m)| = |1| = 1.$$

Thus $|\sigma_i(x)| = 1$ for all i, so $\log|\sigma_i(x)| = 0$ and $x \in G$. ♣

6.1.7 Proposition

B^* is a finitely generated abelian group, isomorphic to $G \times \mathbb{Z}^s$ where $s \leq r_1 + r_2$.

Proof. By (6.1.3), $\lambda(B^*)$ is a discrete subgroup of $\mathbb{R}^{r_1+r_2}$. ["Discrete" means that any bounded subset of $\mathbb{R}^{r_1+r_2}$ contains only finitely many points of $\lambda(B^*)$.] It follows that

$\lambda(B^*)$ is a lattice in $\mathbb{R}^s$, hence a free $\mathbb{Z}$-module of rank s, for some $s \leq r_1 + r_2$. The proof of this is outlined in the exercises. Now by the first isomorphism theorem, $\lambda(B^*) \cong B^*/G$, with $\lambda(x)$ corresponding to the coset xG. If $x_1G, \ldots, x_sG$ form a basis for B^*/G and $x \in B^*$, then xG is a finite product of powers of the x_iG, so x is an element of G times a finite product of powers of the x_i. Since the $\lambda(x_i)$ are linearly independent, so are the x_i, provided we translate the notion of linear independence to a multiplicative setting. The result follows. ♣

We can improve the estimate of s.

6.1.8 Proposition

In (6.1.7), we have $s \leq r_1 + r_2 - 1$.

Proof. If $x \in B^*$, then by (6.1.1) and (2.1.6),

$$\pm 1 = N(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=r_1+1}^{r_1+r_2} \sigma_j(x)\overline{\sigma_j(x)}.$$

Take absolute values and apply the logarithmic embedding to conclude that $\lambda(x) = (y_1, \ldots, y_{r_1+r_2})$ lies in the hyperplane W whose equation is

$$\sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_1+r_2} y_j = 0.$$

The hyperplane has dimension $r_1 + r_2 - 1$, so as in the proof of (6.1.7), $\lambda(B^*)$ is a free $\mathbb{Z}$-module of rank $s \leq r_1 + r_2 - 1$. ♣

In the next section, we will prove the Dirichlet unit theorem, which says that s actually equals $r_1 + r_2 - 1$.

Problems For Section 6.1

We will show that if H is a discrete subgroup of $\mathbb{R}^n$, in other words, for every bounded set $C \subseteq \mathbb{R}^n$, $H \cap C$ is finite, then H is a lattice in $\mathbb{R}^r$ for some $r \leq n$. Choose $e_1, \ldots, e_r \in H$ such that the e_i are linearly independent over $\mathbb{R}$ and r is as large as possible. Let $\overline{T}$ be the closure of the fundamental domain determined by the e_i, that is, the set of all $x = \sum_{i=1}^{r} a_i e_i$, with $0 \leq a_i \leq 1$. Since H is discrete, $H \cap \overline{T}$ is a finite set.

Now let x be any element of H. By choice of r we have $x = \sum_{i=1}^{r} b_i e_i$ with $b_i \in \mathbb{R}$.

1. If j is any integer, set $x_j = jx - \sum_{i=1}^{r} \lfloor jb_i \rfloor e_i$, where $\lfloor y \rfloor$ is the maximum of all integers $z \leq y$. Show that $x_j \in H \cap T$.
2. By examining the above formula for x_j with $j = 1$, show that H is a finitely generated $\mathbb{Z}$-module.
3. Show that the b_i are rational numbers.
4. Show that for some nonzero integer d, dH is a free $\mathbb{Z}$-module of rank at most r.
5. Show that H is a lattice in $\mathbb{R}^r$.

6.2 Statement and Proof of Dirichlet's Unit Theorem

6.2.1 Theorem

The group B^* of units of a number field L is isomorphic to $G \times \mathbb{Z}^s$, where G is a finite cyclic group consisting of all the roots of unity in L, and $s = r_1 + r_2 - 1$.

Proof. In view of (6.1.4)-(6.1.8), it suffices to prove that $s \geq r_1 + r_2 - 1$. Equivalently, by the proof of (6.1.7), the real vector space $V = \lambda(B^*)$ contains $r_1 + r_2 - 1$ linearly independent vectors. Now by the proof of (6.1.8), V is a subspace of the $(r_1 + r_2 - 1)$-dimensional hyperplane W, so we must prove that $V = W$. To put it another way, every linear form f that vanishes on V must vanish on W. This is equivalent to saying that if f does not vanish on W, then it cannot vanish on V, that is, for some unit $u \in B^*$ we have $f(\lambda(u)) \neq 0$.

Step 1. We apply Minkowski's convex body theorem (5.1.3b) to the set

$$S = \{(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : |y_i| \leq a_i, |z_j| \leq a_{r_1+j}\}$$

where i ranges from 1 to r_1 and j from 1 to r_2. We specify the a_i as follows. Fix the positive real number $b \geq 2^{n-r_1}(1/2\pi)^{r_2}|d|^{1/2}$. Given arbitrary positive real numbers $a_1, \dots, a_r$, where $r = r_1 + r_2 - 1$, we choose the positive real number a_{r+1} such that

$$\prod_{i=1}^{r_1} a_i \prod_{j=r_1+1}^{r_1+r_2} a_j^2 = b.$$

The set S is compact, convex, and symmetric about the origin, and its volume is

$$\prod_{i=1}^{r_1} 2a_i \prod_{j=r_1+1}^{r_1+r_2} \pi a_j^2 = 2^{r_1}\pi^{r_2} b \geq 2^{n-r_2}|d|^{1/2}.$$

We apply (5.1.3b) with S as above and $H = \sigma(B)$ [see (5.3.3)], to get $S \cap (H \setminus \{0\}) \neq \emptyset$. Thus there is a nonzero algebraic integer $x = x_a,\ a = (a_1, \dots, a_r)$, such that $\sigma(x_a) \in S$, and consequently,

$$|\sigma_i(x_a)| \leq a_i,\ i = 1, \dots, n,$$

where we set $a_{j+r_2} = a_j,\ j = r_1 + 1, \dots, r_1 + r_2$.

Step 2. We will show that the norms of the x_a are bounded by b in absolute value, and

$$0 \leq \log a_i - \log|\sigma_i(x_a)| \leq \log b.$$

Using step 1, along with (2.1.6) and the fact that the norm of an algebraic integer is a rational integer [see (2.2.2)], we find

$$1 \leq |N(x_a)| = \prod_{i=1}^{n} |\sigma_i(x_a)| \leq \prod_{i=1}^{r_1} a_i \prod_{j=r_1+1}^{r_1+r_2} a_j^2 = b.$$

But for any i,

$$|\sigma_i(x_a)| = |N(x_a)| \prod_{j \neq i} |\sigma_j(x_a)|^{-1} \geq \prod_{j \neq i} a_j^{-1} = a_i b^{-1}.$$

Thus $a_i b^{-1} \leq |\sigma_i(x_a)| \leq a_i$ for all i, so $1 \leq a_i/|\sigma_i(x_a)| \leq b$. Take logarithms to obtain the desired chain of inequalities.

Step 3. Completion of the proof. In the equation of the hyperplane W, $y_1, \ldots, y_r$ can be specified arbitrarily and we can solve for y_{r+1}. Thus if f is a nonzero linear form on W, then f can be expressed as $f(y_1, \ldots, y_{r+1}) = c_1 y_1 + \cdots + c_r y_r$ with not all c_i's zero. By definition of the logarithmic embedding [see (6.1.2)], $f(\lambda(x_a)) = \sum_{i=1}^r c_i \log |\sigma_i(x_a)|$, so if we multiply the inequality of Step 2 by c_i and sum over i, we get

$$|\sum_{i=1}^r c_i \log a_i - f(\lambda(x_a))| = |\sum_{i=1}^r c_i (\log a_i - \log |\sigma_i(x_a)|)| \leq \sum_{i=1}^r |c_i| \log b.$$

Choose a positive real number t greater than the right side of this equation, and for every positive integer h, choose positive real numbers $a_{ih}, i = 1, \ldots, r$, such that $\sum_{i=1}^r c_i \log a_{ih}$ coincides with $2th$. (This is possible because not all c_i's are zero.) Let $a(h) = (a_{1h}, \ldots, a_{rh})$, and let x_h be the corresponding algebraic integer $x_{a(h)}$. Then by the displayed equation above and the choice of t to exceed the right side, we have $|f(\lambda(x_h)) - 2th| < t$, so

$$(2h-1)t < f(\lambda(x_h)) < (2h+1)t.$$

Since the open intervals $((2h-1)t, (2h+1)t)$ are (pairwise) disjoint, it follows that the $f(\lambda(x_h)), h = 1, 2, \ldots$, are all distinct. But by Step 2, the norms of the x_h are all bounded in absolute value by the same positive constant, and by (4.2.13), only finitely many ideals can have a given norm. By (4.2.6), there are only finitely many distinct ideals of the form Bx_h, so there are distinct h and k such that $Bx_h = Bx_k$. But then x_h and x_k are associates, hence for some unit u we have $x_h = ux_k$, hence $\lambda(x_h) = \lambda(u) + \lambda(x_k)$. By linearity of f and the fact that $f(\lambda(x_h)) \neq f(\lambda(x_k))$, we have $f(\lambda(u)) \neq 0$. ♣

6.2.2 Remarks

The unit theorem implies that there are $r = r_1 + r_2 - 1$ units $u_1, \ldots, u_r$ in B such that every unit of B can be expressed uniquely as

$$u = z\, u_1^{n_1} \cdots u_r^{n_r}$$

where the u_i are algebraic integers and z is a root of unity in L. We call $\{u_1, \ldots, u_r\}$ a *fundamental system of units* for the number field L.

As an example, consider the cyclotomic extension $L = \mathbb{Q}(z)$, where z is a primitive p^{th} root of unity, p an odd prime. The degree of the extension is $\varphi(p) = p - 1$, and an embedding σ_j maps z to $z^j, j = 1, \ldots, p-1$. Since these z^j's are never real, we have $r_1 = 0$ and $2r_2 = p - 1$. Therefore $r = r_1 + r_2 - 1 = (p-3)/2$.

6.3 Units in Quadratic Fields

6.3.1 Imaginary Quadratic Fields

First, we look at number fields $L = \mathbb{Q}(\sqrt{m})$, where m is a square-free negative integer. There are no real embeddings, so $r_1 = 0$ and $2r_2 = n = 2$, hence $r_2 = 1$. But then $r_1 + r_2 - 1 = 0$, so the only units in B are the roots of unity in L. We will use (6.1.1) to determine the units.

Case 1. Assume $m \not\equiv 1 \mod 4$. By (2.3.11), an algebraic integer has the form $x = a+b\sqrt{m}$ for integers a and b. By (6.1.1) and (2.1.10), x is a unit iff $N(x) = a^2 - mb^2 = \pm 1$. Thus if $m \leq -2$, then $b = 0$ and $a = \pm 1$. If $m = -1$, we have the additional possibility $a = 0, b = \pm 1$.

Case 2. Assume $m \equiv 1 \mod 4$. By (2.3.11), $x = a + b(1 + \sqrt{m})/2$, and by (2.1.10), $N(x) = (a + b/2)^2 - mb^2/4 = [(2a + b)^2 - mb^2]/4$. Thus x is a unit if and only if $(2a + b)^2 - mb^2 = 4$. We must examine $m = -3, -7, -11, -15, \ldots$. If $m \leq -7$, then $b = 0, a = \pm 1$. If $m = -3$, we have the additional possibilities $b = \pm 1, (2a \pm b)^2 = 1$, that is, $a = 0, b = \pm 1;\ a = 1, b = -1;\ a = -1, b = 1$.

To summarize, if B is the ring of algebraic integers of an imaginary quadratic field, then the group G of units of B is $\{1, -1\}$, except in the following two cases:
1. If $L = \mathbb{Q}(i)$, then $G = \{1, i, -1, -i\}$, the group of 4^{th} roots of unity in L.
2. If $L = \mathbb{Q}(\sqrt{-3})$, then $G = \{[(1 + \sqrt{-3})/2]^j,\ j = 0, 1, 2, 3, 4, 5\}$, the group of 6^{th} roots of unity in L. We may list the elements $x = a + b/2 + b\sqrt{-3}/2 \in G$ as follows:
$j = 0 \Rightarrow x = 1 \quad (a = 1, b = 0)$
$j = 1 \Rightarrow x = (1 + \sqrt{-3})/2 \quad (a = 0, b = 1)$
$j = 2 \Rightarrow x = (-1 + \sqrt{-3})/2 \quad (a = -1, b = 1)$
$j = 3 \Rightarrow x = -1 \quad (a = -1, b = 0)$
$j = 4 \Rightarrow x = -(1 + \sqrt{-3})/2 \quad (a = 0, b = -1)$
$j = 5 \Rightarrow x = (1 - \sqrt{-3})/2 \quad (a = 1, b = -1).$

6.3.2 Remarks

Note that G, a finite cyclic group, has a generator, necessarily a primitive root of unity. Thus G will consist of all t^{th} roots of unity for some t, and the field L will contain only finitely many roots of unity. This is a general observation, not restricted to the quadratic case.

6.3.3 Real Quadratic Fields

Now we examine $L = \mathbb{Q}(\sqrt{m})$, where m is a square-free positive integer. Since the $\mathbb{Q}$-automorphisms of L are the identity and $a + b\sqrt{m} \to a - b\sqrt{m}$, there are two real embeddings and no complex embeddings. Thus $r_1 = 2, r_2 = 0$, and $r_1 + r_2 - 1 = 1$. The only roots of unity in $\mathbb{R}$ are ± 1, so by (6.2.1) or (6.2.2), the group of units in the ring of algebraic integers is isomorphic to $\{-1, 1\} \times \mathbb{Z}$. If u is a unit and $0 < u < 1$, then $1/u$ is a unit and $1/u > 1$. Thus the units greater than 1 are $h^n, n = 1, 2, \ldots$, where h, the unique generator greater than 1, is called the *fundamental unit* of L.

Case 1. Assume $m \not\equiv 1 \mod 4$. The algebraic integers are of the form $x = a + b\sqrt{m}$ with $a, b \in \mathbb{Z}$. Thus we are looking for solutions for $N(x) = a^2 - mb^2 = \pm 1$. Note that if $x = a + b\sqrt{m}$ is a solution, then the four numbers $\pm a \pm b\sqrt{m}$ are $x, -x, x^{-1}, -x^{-1}$ in some order. Since a number and its inverse cannot both be greater than 1, and similarly for a number and its negative, it follows that exactly one of the four numbers is greater than 1, namely the number with a and b positive. The fundamental unit, which is the smallest unit greater than 1, can be found as follows. Compute mb^2 for $b = 1, 2, 3, \ldots$, and stop at the first number mb_1^2 that differs from a square a_1^2 by ± 1. Then $a_1 + b_1\sqrt{m}$ is the fundamental unit.

There is a more efficient computational technique using the continued fraction expansion of $\sqrt{m}$. Details are given in many texts on elementary number theory.

Case 2. Assume $m \equiv 1 \mod 4$. It follows from (2.2.6) that the algebraic integers are of the form $x = \frac{1}{2}(a + b\sqrt{m})$, where a and b are integers of the same parity, both even or both odd. Since the norm of x is $\frac{1}{4}(a^2 - mb^2)$, x is a unit iff $a^2 - mb^2 = \pm 4$. Moreover, if a and b are integers satisfying $a^2 - mb^2 = \pm 4$, then a and b must have the same parity, hence $\frac{1}{2}(a + b\sqrt{m})$ is an algebraic integer and therefore a unit of B. To calculate the fundamental unit, compute $mb^2, b = 1, 2, 3, \ldots$, and stop at the first number mb_1^2 that differs from a square a_1^2 by ± 4. The fundamental unit is $\frac{1}{2}(a_1 + b_1\sqrt{m})$.

Problems For Section 6.3

1. Calculate the fundamental unit of $\mathbb{Q}(\sqrt{m})$ for $m = 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17$.

In Problems 2-5, we assume $m \equiv 1 \mod 4$. Suppose that we look for solutions to $a^2 - mb^2 = \pm 1$ (rather than $a^2 - mb^2 = \pm 4$). We get units belonging to a subring $B_0 = \mathbb{Z}[\sqrt{m}]$ of the ring B of algebraic integers, and the positive units of B_0 form a subgroup H of the positive units of B. Let $u = \frac{1}{2}(a + b\sqrt{m})$ be the fundamental unit of the number field L.

2. If a and b are both even, for example when $m = 17$, show that H consists of the powers of u, in other words, $B_0^* = B^*$.
3. If a and b are both odd, show that $u^3 \in B_0$.
4. Continuing Problem 3, show that $u^2 \notin B_0$, so H consists of the powers of u^3.
5. Verify the conclusions of Problems 3 and 4 when $m = 5$ and $m = 13$.