DIRICHLET'S UNIT THEOREM

KEITH CONRAD

1. Introduction

Dirichlet's unit theorem describes the structure of the unit group of any order in a number field.

Theorem 1.1 (Dirichlet, 1846)**.** *Let K be a number field with r_1 real embeddings and $2r_2$ pairs of complex conjugate embeddings. The unit group of any order in K is finitely generated with $r_1 + r_2 - 1$ independent generators of infinite order.*

More precisely, letting $r = r_1 + r_2 - 1$, any order $\mathcal{O}$ in K contains multiplicatively independent units $\varepsilon_1, \ldots, \varepsilon_r$ of infinite order such that every unit in $\mathcal{O}$ can be written uniquely in the form

$$\zeta \varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r},$$

where ζ is a root of unity in $\mathcal{O}$ and the m_i's are in $\mathbf{Z}$. Abstractly, $\mathcal{O}^\times \cong \mu(\mathcal{O}) \times \mathbf{Z}^{r_1+r_2-1}$, where $\mu(\mathcal{O})$ is the finite cyclic group of roots of unity in $\mathcal{O}$.

Units $u_1, \ldots, u_k$ are called *multiplicatively independent*, or just independent, when they satisfy no multiplicative relations except the trivial one: $u_1^{m_1} \cdots u_k^{m_k} = 1 \Rightarrow m_i = 0$ for all i. It then follows that exponents in such a product are unique: if $u_1^{m_1} \cdots u_k^{m_k} = u_1^{n_1} \cdots u_k^{n_k}$ then $m_i = n_i$ for all i. This looks like linear independence, and that is exactly what it is: when we view $\mathcal{O}^\times$ as a $\mathbf{Z}$-module using its group law, multiplicative independence means $\mathbf{Z}$-linear independence.

If $r_1 > 0$ then $\mu(\mathcal{O}) = \{\pm 1\}$ since ± 1 are the only roots of unity in $\mathbf{R}$. If $r_1 = 0$ we might also have $\mu(\mathcal{O}) = \{\pm 1\}$, *e.g.*, $\mathcal{O} = \mathbf{Z}[\sqrt{d}]$ for $d < -1$.

It is important that the unit groups of all orders in K have the same number of independent generators of infinite order: $r_1 + r_2 - 1$. Therefore $[\mathcal{O}_K^\times : \mathcal{O}^\times]$ is finite. A choice of generators $\varepsilon_1, \ldots, \varepsilon_r$ for $\mathcal{O}^\times$ (really, for the quotient group $\mathcal{O}^\times/\mu(\mathcal{O})$) is called a system of *fundamental units*. We call $r_1 + r_2 - 1$ the rank of the unit group.

The unit groups of orders in number fields were, historically, the first important examples of finitely generated abelian groups. Finding algorithms to produce explicit generators for unit groups is one of the tasks of computational number theory.

In Section 2 we will look at some examples of the unit theorem. The theorem will be proved in Section 3.

2. Examples

Example 2.1. For $\mathbf{Q}(\sqrt{2})$ we have $r_1 + r_2 - 1 = 1$, so the unit group of any order in $\mathbf{Q}(\sqrt{2})$ has the form $\pm\varepsilon^{\mathbf{Z}}$ for some unit ε. In particular, $\mathbf{Z}[\sqrt{2}]^\times = \pm(1+\sqrt{2})^{\mathbf{Z}}$ and $\mathbf{Z}[3\sqrt{2}]^\times = \pm(17+12\sqrt{2})^{\mathbf{Z}}$.

Table 1 describes unit groups in the full ring of integers in several number fields. The unit ε in the row for $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)$ is

$$\varepsilon = \frac{-1 + 2\sqrt[3]{2} + \sqrt[3]{4}}{3} + \frac{1 - \sqrt[3]{2} + \sqrt[3]{4}}{3}\zeta_3.$$

K	r_1	r_2	$r_1 + r_2 - 1$	$\mu(\mathcal{O}_K)$	$\mathcal{O}_K^\times$
$\mathbf{Q}(\sqrt{3})$	2	0	1	± 1	$\pm(2+\sqrt{3})^{\mathbf{Z}}$
$\mathbf{Q}(\sqrt{5})$	2	0	1	± 1	$\pm(\frac{1+\sqrt{5}}{2})^{\mathbf{Z}}$
$\mathbf{Q}(\zeta_5)$	0	2	1	μ_{10}	$\mu_{10}(\frac{1+\sqrt{5}}{2})^{\mathbf{Z}}$
$\mathbf{Q}(\sqrt[3]{2})$	1	1	1	± 1	$\pm(1+\sqrt[3]{2}+\sqrt[3]{4})^{\mathbf{Z}}$
$\mathbf{Q}(\sqrt[3]{6})$	1	1	1	± 1	$\pm(1-6\sqrt[3]{6}+3\sqrt[3]{36})^{\mathbf{Z}}$
$\mathbf{Q}(\sqrt[4]{2})$	2	1	2	± 1	$\pm(1+\sqrt[4]{2})^{\mathbf{Z}}(1+\sqrt{2})^{\mathbf{Z}}$
$\mathbf{Q}(\sqrt[3]{2}, \zeta_3)$	0	3	2	μ_6	$\mu_6 \cdot \varepsilon^{\mathbf{Z}}\overline{\varepsilon}^{\mathbf{Z}}$
$\mathbf{Q}(\sqrt{2}, \sqrt{3})$	4	0	3	± 1	$\pm(1+\sqrt{2})^{\mathbf{Z}}(\sqrt{2}+\sqrt{3})^{\mathbf{Z}}(\frac{\sqrt{2}+\sqrt{6}}{2})^{\mathbf{Z}}$

TABLE 1. Unit Group of $\mathcal{O}_K$

Example 2.2. The unit group of an order is finite if and only if $r_1 + r_2 - 1 = 0$. This means (r_1, r_2) is $(1, 0)$ or $(0, 1)$, so K is $\mathbf{Q}$ or an imaginary quadratic field. Moreover, the unit group of any order in an imaginary quadratic field is $\{\pm 1\}$ except for the maximal orders $\mathbf{Z}[i]$ and $\mathbf{Z}[\zeta_3]$, whose units groups have size 4 and 6, respectively. There are a number of important results in algebraic number theory which have a simpler form for $\mathbf{Q}$ and imaginary quadratic fields than for other number fields, precisely because in these (and only these) cases the unit group is finite.

Example 2.3. We have $r_1 + r_2 - 1 = 1$ if and only if $(r_1, r_2) = (2, 0)$, $(1, 1)$, or $(0, 2)$, *i.e.*, K is real quadratic (*e.g.*, $\mathbf{Q}(\sqrt{2})$), a cubic field with only one real embedding (*e.g.*, $\mathbf{Q}(\sqrt[3]{2})$), or a totally complex quartic field (*e.g.*, $\mathbf{Q}(\zeta_5)$).

Example 2.4. If K is a totally real cubic field then $r_1 + r_2 - 1 = 2$, so any order in K has unit group of the form $\pm\varepsilon_1^{\mathbf{Z}}\varepsilon_2^{\mathbf{Z}}$.

Example 2.5. We always have $r_1 + r_2 - 1 \leq n - 1$, where $n = [K : \mathbf{Q}] = r_1 + 2r_2$. Easily $r_1 + r_2 - 1 = n - 1$ if and only if $r_2 = 0$, *i.e.*, K is a totally real number field.

Example 2.6. Let's look at a unit group with rank greater than 1 and see how to find multiplicative relations between units numerically, by using logarithms to discover them as linear relations. Set $K = \mathbf{Q}(\alpha)$ where $\alpha^3 - 3\alpha - 1 = 0$. The polynomial $f(T) = T^3 - 3T - 1$ has 3 real roots, so $\mathcal{O}_K^\times$ has rank $r_1 + r_2 - 1 = 3 - 1 = 2$.

Before looking at $\mathcal{O}_K^\times$, let's show $\mathcal{O}_K = \mathbf{Z}[\alpha]$. Since $\mathrm{disc}(\mathbf{Z}[\alpha]) = -4(-3)^3 - 27(-1)^2 = 81 = 3^4$, $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ divides 9. Therefore elements of $\mathcal{O}_K$ when written in the basis $\{1, \alpha, \alpha^2\}$ have coefficients with denominator dividing 9. Since $f(T+1) = T^3 + 3T^2 - 3$ is Eisenstein at 3 with $\alpha - 1$ as a root, elements of $\mathcal{O}_K$ when written in the basis $\{1, \alpha - 1, (\alpha - 1)^2\}$ have coefficients with denominator prime to 3. This carries over to $\{1, \alpha, \alpha^2\}$, so $\mathcal{O}_K = \mathbf{Z}[\alpha]$. (The Minkowski bound is exactly 2, and there is no prime ideal with norm 2 since $T^3 - 3T - 1$ is irreducible modulo 2, so $h(K) = 1$: $\mathbf{Z}[\alpha]$ is a PID.)

We now write down several units in $\mathbf{Z}[\alpha]$. For any $a, b \in \mathbf{Q}$, $\mathrm{N}_{K/\mathbf{Q}}(a\alpha+b) = -a^3 f(-b/a)$. Check with this formula that $\alpha, \alpha+1, \alpha-2$, and $2\alpha+3$ all have norm ± 1, so they are all in $\mathbf{Z}[\alpha]^\times$. The three roots of $f(T)$ are α, $2-\alpha^2$, and $\alpha^2-\alpha-2$, so $2-\alpha^2$ and $\alpha^2-\alpha-2$ are in $\mathbf{Z}[\alpha]^\times$. The product of all three roots of $f(T)$ is $-f(0) = 1$.

Since $\mathbf{Z}[\alpha]^\times$ has rank 2, the nontrivial units we just wrote down must admit some nontrivial multiplicative relations. How can we find such relations? We will use the three different embeddings $K \to \mathbf{R}$. Call them σ_1, σ_2, and σ_3. The real roots of $f(T)$ are $\sigma_1(\alpha), \sigma_2(\alpha)$, and $\sigma_3(\alpha)$. Arranging the roots in increasing order,

$$\sigma_1(\alpha) = -1.532\ldots, \quad \sigma_2(\alpha) = -.347\ldots, \quad \sigma_3(\alpha) = 1.879\ldots.$$

For $\gamma \in K$, $\mathrm{N}_{K/\mathbf{Q}}(\gamma) = \sigma_1(\gamma)\sigma_2(\gamma)\sigma_3(\gamma)$. For $u \in \mathcal{O}_K^\times$, $|\sigma_1(u)\sigma_2(u)\sigma_3(u)| = 1$. Taking logarithms,

$$u \in \mathcal{O}_K^\times \Longrightarrow \log|\sigma_1(u)| + \log|\sigma_2(u)| + \log|\sigma_3(u)| = 0. \tag{2.1}$$

Define the logarithmic mapping $L\colon K^\times \to \mathbf{R}^3$ by

$$L(\gamma) = (\log|\sigma_1(\gamma)|, \log|\sigma_2(\gamma)|, \log|\sigma_3(\gamma)|).$$

We will use such a map L in the proof of the general unit theorem; here we will see how this map is useful computationally. Easily L is a group homomorphism and by (2.1), $L(\mathcal{O}_K^\times)$ is in the hyperplane $\{(x,y,z) \in \mathbf{R}^3 : x+y+z = 0\}$. The kernel of L on $\mathcal{O}_K^\times$ is $\{\pm 1\}$ (why?). Table 2 gives numerical approximations to the images of units under the logarithmic mapping.

γ	$L(\gamma)$ (approx.)
α	$(.4266, -1.0575, .6309)$
$\alpha+1$	$(-.6309, -.4266, 1.0575)$
$\alpha-2$	$(1.2618, .8532, -2.1151)$
$2\alpha+3$	$(-2.7460, .8352, 1.9108)$
$2-\alpha^2$	$(-1.0575, .6309, .4266)$
$\alpha^2-\alpha-2$	$(.6309, .4266, -1.0575)$

TABLE 2. Log Images of Units

From the table, it appears that $L(\alpha-2) = -2L(\alpha+1) = L(1/(\alpha+1)^2)$, so $\alpha - 2 = \pm 1/(\alpha+1)^2$. You can check that it is the minus sign which holds. Using a computer algebra package, the 3×3 matrix $(L(\alpha)\ \ L(\alpha+1)\ \ L(2\alpha+3))$ has $(2,-3,1)$ in its kernel, so $\alpha^2(\alpha+1)^{-3}(2\alpha+3)$ has L-value 0. Therefore $2\alpha+3 = \pm\alpha^{-2}(\alpha+1)^3$. Check that the plus sign holds. Since it looks like $L(2-\alpha^2) = L(\alpha+1) - L(\alpha)$, $2-\alpha^2 = \pm(\alpha+1)/\alpha$ and it is the minus sign which holds. Then, since the three roots of $f(T)$ multiply to 1, $\alpha^2-\alpha-2 = 1/(\alpha(2-\alpha^2)) = (1/\alpha)(-\alpha/(\alpha+1)) = -1/(\alpha+1)$.

This evidence suggests that α and $\alpha+1$ are a system of fundamental units for $\mathbf{Z}[\alpha]^\times$.

3. Proof of the unit theorem

Our proof of the unit theorem is adapted from [1, pp. 214–215] (see also [2, p. 5]), which interprets the unit theorem as a compactness theorem. That is, the unit theorem is connected to a certain group being compact.

We will use Minkowski's convex-body theorem in our proof. This is a standard tool for proofs of the unit theorem, although by comparison with typical applications of Minkowski's

theorem we will be able to get by with a crudely chosen convex body: any sufficiently large ball will work.

Dirichlet did not have Minkowski's theorem available; he proved the unit theorem in 1846, while Minkowski developed the geometry of numbers only near the end of the 19th century. His substitute for the convex-body theorem was the pigeonhole principle. Dirichlet did not state the unit theorem for all orders, but only those of the form $\mathbf{Z}[\alpha]$, since at the time these were the kinds of rings that people considered. The main idea for the proof came to him while attending a concert in the Sistine Chapel.

Lemma 3.1. *For any $a \neq 0$ in $\mathcal{O}$, $[\mathcal{O} : (a)] = |\mathrm{N}_{K/\mathbf{Q}}(a)|$.*

Proof. This follows from $\mathcal{O}$ being a free $\mathbf{Z}$-module of rank $[K : \mathbf{Q}]$. □

Lemma 3.2. *There are only finitely many ideals in $\mathcal{O}$ with any given index.*

Proof. If $\mathfrak{a} \subset \mathcal{O}$ is an ideal with index m then $m\mathcal{O} \subset \mathfrak{a} \subset \mathcal{O}$. Ideals of index m in $\mathcal{O}$ are in bijection with $\mathcal{O}$-submodules of index m in $\mathcal{O}/m\mathcal{O}$. Since $\mathcal{O}/m\mathcal{O}$ is finite, there are only finitely many such ideals. □

We set some notation. Let $n = [K : \mathbf{Q}]$ and $V = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ with K embedded in V using its real and complex embeddings (using only one complex embedding from each conjugate pair). We view V as a commutative ring. Give V its natural topology and all subsets of V will be given the subspace topology. A particular subset we will care about is $V^\times = (\mathbf{R}^\times)^{r_1} \times (\mathbf{C}^\times)^{r_2}$.

Denote the image of $\mathcal{O}^\times$ in $V^\times$ as U (for "units"). Let $\mathrm{N}\colon V \to \mathbf{R}$ be the analogue on V of the norm map $\mathrm{N}_{K/\mathbf{Q}}\colon K \to \mathbf{Q}$ (so $\mathrm{N}(\theta_K(\alpha)) = \mathrm{N}_{K/\mathbf{Q}}(\alpha)$ for $\alpha \in K$.) Then since $\mathcal{O}^\times = \{\alpha \in \mathcal{O} : |\mathrm{N}_{K/\mathbf{Q}}(\alpha)| = 1\}$,

$$v \in U \Longrightarrow |\mathrm{N}(v)| = 1.$$

Set

$$G = \{v \in V^\times : |\mathrm{N}(v)| = 1\}.$$

This subgroup of $V^\times$ is closed in V since it's the inverse image of the point 1 under the continuous map $v \mapsto |\mathrm{N}(v)|$. Since the embedding of $\mathcal{O}$ into V has a discrete image, U is a discrete subset of $V^\times$ and thus U is a discrete subgroup of G too. We will be interested in the quotient group G/U.

Example 3.3. Let $K = \mathbf{Q}(\sqrt{2})$ and $\mathcal{O} = \mathcal{O}_K = \mathbf{Z}[\sqrt{2}]$. Then $V = \mathbf{R}^2$ and $\mathrm{N}\colon V \to \mathbf{R}$ by $\mathrm{N}(x, y) = xy$. The Euclidean embedding $\theta\colon \mathbf{Q}(\sqrt{2}) \to \mathbf{R}^2$ places $\mathbf{Z}[\sqrt{2}]^\times$ on the curve $G = \{(x, y) \in \mathbf{R}^2 : |xy| = 1\}$, a union of two hyperbolas. It is a discrete subset of G ("equally spaced" in a multiplicative sense). See Figure 1.

Multiplication on G by an element of U moves the arcs between consecutive points of U to other such arcs, and exchanges the hyperbolas $y = 1/x$ and $y = -1/x$ if the unit has norm -1. Multiplication by $\theta(-1) = (-1, -1)$ exchanges the two branches on each hyperbola. Since we know $\mathbf{Z}[\sqrt{2}]^\times = \pm(1 + \sqrt{2})^{\mathbf{Z}}$, modulo U any $(x, y) \in G$ is congruent to a point on the arc between $\theta(1)$ and $\theta((1 + \sqrt{2})^2)$. So the map $[1, (1 + \sqrt{2})^2] \to G/U$ given by $x \mapsto (x, 1/x)U$ is surjective and continuous, which implies G/U is compact.

In the previous example we used knowledge of the unit group of $\mathbf{Z}[\sqrt{2}]$ to see G/U is compact. The key to proving the unit theorem is showing this compactness holds without knowing the structure of the unit group in advance:

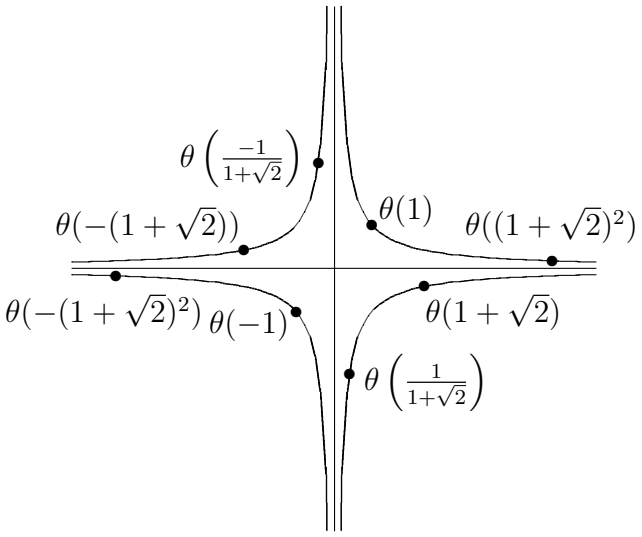


FIGURE 1. Units in $\mathbf{Z}[\sqrt{2}]$ on $G = \{(x, y) \in \mathbf{R}^2 : |xy| = 1\}$.

Theorem 3.4. *The group G/U is compact in the quotient topology.*

Proof. We will show every sequence in G/U has a convergent subsequence, so G/U is sequentially compact and thus compact. (Usually G itself is not compact. See Figure 1.)

We begin with a remark about volumes. For $v \in V^\times$, multiplication of $V = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ by v is an $\mathbf{R}$-linear map (hence continuous) given by a matrix with determinant $\mathrm{N}(v)$, so for any region $R \subset V$ with finite volume, the volume of vR is $|\mathrm{N}(v)|$ times the volume of R. In particular, if $v \in G$ then $\mathrm{vol}(vR) = \mathrm{vol}(R)$ because $|\mathrm{N}(v)| = 1$. When R is compact so is vR, by continuity of multiplication.

Choose a sequence $\overline{g}_j = g_j U$ in G/U. We want to show there is a convergent subsequence in G/U. We will show that there is a subsequence of $\{\overline{g}_j\}$ admitting coset representatives which converge in V (and thus their limit is in G since G is closed in V). The reduction map $G \to G/U$ is continuous because we are giving G/U the quotient topology, so a convergent sequence in G turns into a convergent sequence when reduced modulo U, hence the $\overline{g}_j$'s will have a convergent subsequence in G/U.

Pick a compact, convex, centrally symmetric region $C \subset V$ with $\mathrm{vol}(C) > 2^n \mathrm{vol}(\theta_K(\mathcal{O}))$. (for instance, C could be a large ball). For *any* $g \in G$, gC is also compact and centrally symmetric. It is convex too, since multiplication by g on V is an invertible linear transformation, and invertible linear transformations send convex sets to convex sets. Therefore Minkowski's convex body theorem applies to gC and the lattice $\mathcal{O} \subset V$ (we identify $\mathcal{O}$ with $\theta_K(\mathcal{O})$):

$$gC \cap (\mathcal{O} - \{0\}) \neq \emptyset.$$

So we can write $g_j c_j = a_j$ for some $c_j \in C$ and $a_j \in \mathcal{O} - \{0\}$.

By Lemma 3.1, $[\mathcal{O} : (a_j)] = |\mathrm{N}_{K/\mathbf{Q}}(a_j)| = |\mathrm{N}(a_j)|$. Since

$$\mathrm{N}(a_j) = \mathrm{N}(g_j)\mathrm{N}(c_j) = \pm \mathrm{N}(c_j),$$

and the numbers $|\mathrm{N}(c_j)|$ are bounded above (N is continuous and C is compact), the ideals (a_j) in $\mathcal{O}$ have bounded index. Therefore by Lemma 3.2, infinitely many of the ideals (a_j)

must be the same, so by passing to a subsequence we may assume all these ideals are equal: $a_k\mathcal{O} = a_1\mathcal{O}$ for all k, so $a_k = a_1u_k$ for some u_k in $\mathcal{O}^\times$, which we identify with its Euclidean image U. (We have just "produced" units in $\mathcal{O}$!) Thus

$$g_k = c_k^{-1}a_k = c_k^{-1}a_1u_k \equiv c_k^{-1}a_1 \bmod U.$$

We will show the sequence $\{c_k^{-1}a_1\}$ in $V^\times$ has a convergence subsequence.

Since the c_k's lie in a compact subset of V, they have a convergent subsequence. So by passing to yet another subsequence we may assume the c_k's converge in V, say $c_k \to \ell$. Is $\ell \in V^\times$? Since $|\mathrm{N}(c_k)| = |\mathrm{N}(a_k)| = |\mathrm{N}(a_1)\mathrm{N}(u_k)| = |\mathrm{N}(a_1)|$ is constant, by continuity of N we have $|\mathrm{N}(\ell)| = |\mathrm{N}(a_1)| > 0$, so $\ell \in V^\times$. Therefore the sequence c_k^{-1} converges (to ℓ^{-1}) in $V^\times$, so $c_k^{-1}a_1$ converges in $V^\times$ as $k \to \infty$. Thus $g_kU = c_k^{-1}a_1U$ converges in G/U (to $\ell^{-1}a_1U$), so we're done. □

Now we prove the unit theorem. Recall that we set $G = \{v \in V : |\mathrm{N}(v)| = 1\}$. Any element of $V = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ can be written in the form $(x_1, \dots, x_{r_1}, z_{r_1+1}, \dots, z_{r_1+r_2})$. Define the logarithmic mapping $L\colon V^\times \to \mathbf{R}^{r_1+r_2}$ by

$$L(x_1, \dots, z_{r_1+r_2}) := (\dots, \log|x_i|, \dots, 2\log|z_j|, \dots),$$

so L is a continuous group homomorphism and, for $g \in G$, $L(g)$ lies in the hyperplane

$$H = \{(y_1, \dots, y_{r_1+r_2}) \in \mathbf{R}^{r_1+r_2} : \sum_i y_i = 0\}.$$

It is easy to show $L(G) = H$, so $L(G)$ has dimension $r_1 + r_2 - 1$ over $\mathbf{R}$. What we really care about is $L(U)$, which provides a linearized geometric picture for U (once we determine the kernel of $L|_U$). The basic plan is to show $L(U)$ is a "full" lattice in the hyperplane $L(G)$ and the kernel of L on U is finite cyclic (coming from roots of unity in U).

First we treat the **kernel** of L on U. As a map out of $V^\times$, the kernel of L is compact:

$$\ker L = \{\pm 1\}^{r_1} \times (S^1)^{r_2}.$$

Any root of unity in U gets sent to 0 by L. Let's check these are the only elements of $U = \mathcal{O}^\times$ in $\ker L$. Since U is closed in $V^\times$ (any discrete set is closed), the kernel of $L|_U$ is closed and thus (as a subset of $\{\pm 1\}^{r_1} \times (S^1)^{r_2}$) is compact. Since $\mathcal{O}$ is discrete in V (it's a lattice), U is discrete in $V^\times$, so the kernel of $L|_U$ is also discrete (any subset of a discrete set is discrete), so $\ker(L|_U)$ is compact and discrete: it is finite! A subgroup of U with finite order can only contain roots of unity. Therefore the elements of $\ker(L|_U)$ are the roots of unity in $U = \mathcal{O}^\times$, which form a finite cyclic group since any finite subgroup of $K^\times$ is a cyclic group. (Warning: it is *false* that the kernel of L as a map out of $K^\times$ is only the roots of unity in K. Any element of $K^\times$ which has all of its $\mathbf{Q}$-conjugates lying on the unit circle is in the kernel of L. An example is $3/5 + (4/5)i$, or more generally any $a/c + (b/c)i$ where (a, b, c) is a Pythagorean triple. But these are not algebraic *integers*, so they don't belong to U.)

Now we look at the **image** $L(U)$ in the hyperplane $L(G) \subset \mathbf{R}^{r_1+r_2}$. We have already seen (and used) that the group U is discrete in $V^\times$, so also in G. The image of a discrete set under a continuous map need not be discrete (consider $\mathbf{Z}^2 \to \mathbf{R}$ by $(m, n) \mapsto m + n\sqrt{2}$), but $L(U)$ is discrete in $L(G)$ since there are only finitely many elements in $L(U)$ that lie in any bounded region of $\mathbf{R}^{r_1+r_2}$. Indeed, consider the box

$$\{(y_1, \dots, y_{r_1+r_2}) \in \mathbf{R}^{r_1+r_2} : |y_i| \le b\}.$$

Suppose $L(u)$ is in this box for some $u \in U$. The real embeddings[1] of u have absolute value at most e^b and the complex embeddings of u have absolute value at most $e^{b/2}$. That puts an upper bound in terms of b (and $n = [K : \mathbf{Q}]$) on the coefficients of the polynomial $\prod_\sigma (T - \sigma(u)) \in \mathbf{Z}[T]$. The coefficients have only finitely many possibilities, since there are finitely many integers with absolute value below a given bound, so there are finitely many such polynomials. As u is a root of such a polynomial, there are finitely many choices for u. This shows $L(U)$ is discrete.

Since $L(U)$ is a discrete subgroup of $L(G) \cong \mathbf{R}^{r_1+r_2-1}$, $L(U) \cong \mathbf{Z}^{r'}$ where $r' \leq r_1 + r_2 - 1$. Since $L\colon G \to L(G)$ is a continuous and surjective group homomorphism, the induced map $G/U \to L(G)/L(U)$ is also continuous and surjective where both quotient groups get the quotient topology. From Theorem 3.4, G/U is compact so $L(G)/L(U)$ is compact. Since $L(G)$ is an (r_1+r_2-1)-dimensional over $\mathbf{R}$ and $L(U)$ has $\mathbf{Z}$-rank $r' \leq r_1+r_2-1$, compactness of $L(G)/L(U)$ forces $r' = r_1+r_2-1$: Euclidean space modulo a discrete subgroup is compact *only* when the subgroup has rank equal to the dimension of the space (*e.g.*, $\mathbf{R}^2/(\mathbf{Z} \times \{(0,0)\})$ is a non-compact infinite cylinder). That proves $L(U) \cong \mathbf{Z}^{r_1+r_2-1}$ and $L(U)$ is a lattice in the hyperplane H.

We're now basically done. Let $\varepsilon_1, \ldots, \varepsilon_r$ $(r = r_1 + r_2 - 1)$ be elements of $\mathcal{O}^\times$ whose Euclidean embeddings in U provide a $\mathbf{Z}$-basis of $L(U)$. The ε_i's are multiplicatively independent, since their L-images are $\mathbf{Z}$-linearly independent. For any $\varepsilon \in \mathcal{O}^\times$, $L(\varepsilon) = m_1 L(\varepsilon_1) + \cdots + m_r L(\varepsilon_r)$ for some integers m_i, so $L(\varepsilon) = L(\varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r})$. Since $\ker(L|_U)$ is the Euclidean image of the roots of unity in $\mathcal{O}^\times$, $\varepsilon = \zeta \varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r}$ for some $\zeta \in \mu(\mathcal{O})$. This concludes the proof of the unit theorem.

The most difficult part of the proof of the unit theorem is showing there are $r_1 + r_2 - 1$ independent units of infinite order. For instance, using the logarithmic map it was not hard for us to show $L(U)$ is a discrete subgroup of $L(G) \cong \mathbf{R}^{r_1+r_2-1}$, so $\mathcal{O}^\times \cong U \cong W \times \mathbf{Z}^{r'}$ where $r' \leq r_1 + r_2 - 1$ and W is the group of roots of unity in $\mathcal{O}^\times$. Thus $\mathcal{O}^\times$ has *at most* $r_1 + r_2 - 1$ independent units of infinite order. Showing the bound is reached is hard, and that is also the only part of the proof which shows there are any units at all other than roots of unity if $r_1 + r_2 - 1 > 0$.

4. Fundamental Unit in the Rank 1 Case

As noted already in Example 2.3, an order $\mathcal{O}$ in number field K has a rank 1 unit group precisely when K is real quadratic, a cubic with 1 real embedding (that is, a cubic field which is not totally real), or a totally complex quartic field. In the first two cases, the only roots of unity in K are ± 1, which are always in $\mathcal{O}$, so $\mathcal{O}^\times = \pm\varepsilon^{\mathbf{Z}}$. Viewing K in $\mathbf{R}$, the choice of $\varepsilon > 1$ is called *the* fundamental unit of $\mathcal{O}$.

Example 4.1. Since $\mathbf{Z}[\sqrt{2}]^\times = \pm(1+\sqrt{2})^{\mathbf{Z}}$, the fundamental unit of $\mathbf{Z}[\sqrt{2}]$ is $1 + \sqrt{2}$.

Example 4.2. Since $\mathbf{Z}[3\sqrt{2}]^\times = \pm(17 + 12\sqrt{2})^{\mathbf{Z}}$, the fundamental unit of $\mathbf{Z}[3\sqrt{2}]$ is $17 + 12\sqrt{2}$.

Example 4.3. Since $\mathbf{Z}[\sqrt[3]{6}]^\times = \pm(1 - 6\sqrt[3]{6} + 3\sqrt[3]{36})^{\mathbf{Z}}$ and $1 - 6\sqrt[3]{6} + 3\sqrt[3]{36} \approx .00305$, the fundamental unit is the reciprocal $109 + 60\sqrt[3]{6} + 33\sqrt[3]{36} \approx 326.990$.

[1]We are identifying $U = \theta_K(\mathcal{O}^\times)$ with $\mathcal{O}^\times$ when we speak of real embeddings of u. If we did not make that identification, and wrote $u = \theta_K(\alpha)$, then we would speak instead of real embeddings of α, which are the initial coordinates of u.

In a real quadratic field, one way to find the fundamental unit in an order is by brute force: if we write a unit greater than 1 as $a+b\sqrt{d}$ or $a+b(1+\sqrt{d})/2$ with $a, b \in \mathbf{Z}$, necessarily $a \geq 0$ and $b \geq 1$ (check!). This allows one to systematically search for the smallest unit greater than 1 by sifting through pairs of integers in the first quadrant by increasing values of a and b. (There is a more efficient method, using continued fractions.)

To give some examples of fundamental unit computations in the cubic case, we will work out an inequality due to Artin.

Theorem 4.4 (Artin)**.** *Let $\mathcal{O}$ be an order in a cubic field K with $r_1 = 1$. Viewing K in $\mathbf{R}$, if $v > 1$ is a unit of $\mathcal{O}^\times$ then $|\operatorname{disc}(\mathcal{O})| < 4v^3 + 24$.*

Proof. This is a tedious calculation. The reader may want to read the corollary and its applications first, then return to this proof.

Since v is a unit and is not ± 1, $v \notin \mathbf{Q}$. Thus $\mathbf{Q}(v) = K$, so $\mathbf{Z}[v]$ is an order inside $\mathcal{O}$. From $\mathbf{Z}[v] \subset \mathcal{O}$, $|\operatorname{disc}(\mathcal{O})| \leq |\operatorname{disc}(\mathbf{Z}[v])|$. We will show $|\operatorname{disc}(\mathbf{Z}[v])| < 4v^3 + 24$.

Let $\sigma\colon K \to \mathbf{C}$ be one of the non-real embeddings of K. Then $\mathrm{N}_{K/\mathbf{Q}}(v) = v\sigma(v)\overline{\sigma}(v) = v|\sigma(v)|^2 > 0$, so u has norm 1. Let $x = \sqrt{v}$ (as a positive real number), so $1 = x^2|\sigma(v)|^2$. Therefore $|\sigma(v)| = 1/x$, so in polar form $\sigma(v) = x^{-1}e^{it}$ for some real number t. Then

$$\begin{aligned}
\operatorname{disc}(\mathbf{Z}[v]) &= ((\sigma(v)-v)(\overline{\sigma}(v)-v)(\sigma(v)-\overline{\sigma}(v)))^2 \\
&= ((x^{-1}e^{it}-x^2)(x^{-1}e^{-it}-x^2)(x^{-1}e^{it}-x^{-1}e^{-it}))^2 \\
&= ((x^{-2}+x^4-2x\cos t)(-2ix^{-1}\sin t))^2 \\
&= -4(\sin^2 t)(x^3+x^{-3}-2\cos t)^2,
\end{aligned}$$

so

$$\begin{aligned}
\frac{1}{4}|\operatorname{disc}(\mathbf{Z}[v])| &= (\sin^2 t)(x^3+x^{-3}-2\cos t)^2 \\
&= (1-\cos^2 t)(x^3+x^{-3}-2\cos t)^2.
\end{aligned}$$

Set $c = \cos t$, so $c \in [-1,1]$, and $a = x^3 + x^{-3}$, so $a > 2$ since $x > 0$. Then $(1/2)\operatorname{disc}(\mathbf{Z}[u]) = (1-c^2)(a-2c)^2$. Set $f(y) = (1-y^2)(a-2y)^2$. What is its maximal value on $[-1,1]$? On this interval f takes nonnegative values and vanishes at the endpoints, so we check where f' vanishes in $[-1,1]$. By calculus, $f'(y) = 2(a-2y)(4y^2-ay-2)$, where the linear factor vanishes at $a/2 > 1$ and the quadratic factor has roots $(a \pm \sqrt{a^2+32})/8$; since $a > 2$, the root with the $+$ sign is greater than 1 and the other root is in $(-1,0)$. Call this root y_0. It is the only root of f' in $[-1,1]$, so $f(y_0)$ is the maximum value of f on $[-1,1]$. Thus

$$\begin{aligned}
\frac{1}{4}\operatorname{disc}(\mathbf{Z}[v]) &= f(c) \\
&\leq f(y_0) \\
&= (1-y_0^2)(a-2y_0)^2.
\end{aligned}$$

Expanding the square and using the equation $ay_0 = 4y_0^2 - 2$ (since y_0 is a root of the quadratic factor of f'), we get

$$(1-y_0^2)(a-2y_0)^2 = a^2 - 4y_0^4 - 4y_0^2 + 4.$$

Substituting $a = x^3 + x^{-3}$,

$$(1-y_0^2)(a-2y_0)^2 = x^6 + 6 + (x^{-6} - 4y_0^4 - 4y_0^2).$$

We will show $x^{-6} < 4y_0^2$, so the right side is less than $x^6 + 6 = v^3 + 6$. Then $|\operatorname{disc}(\mathbf{Z}[v])| < 4v^3 + 24$, as desired.

Since $y_0 \in (-1, 0)$ while $x^{-1} \in (0, 1)$, the inequality $x^{-6} < 4y_0^2$ is the same as $1 < 4|y_0|x^3$. To prove this inequality, let's write down formulas for y_0 and x in terms of a. Since y_0 is the smaller root of $4y^2 - ay - 2$, $y_0 = (a - \sqrt{a^2 + 32})/8$. Since $x^3 + x^{-3} = a$, multiplying by x^3 and using the quadratic formula shows $x^3 = (a + \sqrt{a^2 - 4})/2$. Therefore we want to show

$$1 < \frac{(\sqrt{a^2 + 32} - a)(a + \sqrt{a^2 - 4})}{4}.$$

It is left to the reader to check by calculus that the expression on the right is an increasing function of a for $a \geq 2$. At 2 the right side is 2, so since $a = x^3 + x^{-3} > 2$ we are done. □

Remark 4.5. It would be nice if one could give a less tedious proof of this inequality.

Corollary 4.6. *Let $\mathcal{O}$ be an order in a cubic field K with $r_1 = 1$. Viewing K in $\mathbf{R}$, if $u > 1$ is a unit of $\mathcal{O}^\times$ and $4u^{3/2} + 24 < |\operatorname{disc}(\mathcal{O})|$ then u is the fundamental unit of $\mathcal{O}^\times$.*

Proof. Let ε be the fundamental unit, so $u = \varepsilon^n$ with $n \geq 1$. We want to show $n = 1$. If $n \geq 2$ then Artin's inequality with $v = \varepsilon$ says

$$|\operatorname{disc}(\mathcal{O})| < 4\varepsilon^3 + 24 = 4u^{3/n} + 24 \leq 4u^{3/2} + 24,$$

which contradicts the inequality in the statement of the corollary. □

Example 4.7. Let $K = \mathbf{Q}(\sqrt[3]{2})$, so $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{2}]$ and $\operatorname{disc}(\mathcal{O}_K) = \operatorname{disc}(T^3 - 2) = -108$. Since

$$1 = \sqrt[3]{2}^3 - 1 = (\sqrt[3]{2} - 1)(\sqrt[3]{4} + \sqrt[3]{2} + 1),$$

we have a unit $u = 1 + \sqrt[3]{2} + \sqrt[3]{4} \approx 3.847$. Since $4u^{3/2} + 24 \approx 54.185 < 108$, u is the fundamental unit of $\mathcal{O}_K$.

Example 4.8. Let $K = \mathbf{Q}(\alpha)$, where $\alpha^3 + 2\alpha + 1 = 0$. The polynomial is irreducible modulo 3, so $K/\mathbf{Q}$ is cubic. It has one real root, approximately $-.45$. Since $\operatorname{disc}(T^3 + 2T + 1) = -59$, $\mathcal{O}_K = \mathbf{Z}[\alpha]$. Clearly α is a unit. We view K in $\mathbf{R}$. Since $\alpha \approx -.45$, we get a unit greater than 1 using

$$u = -\frac{1}{\alpha} \approx 2.205.$$

Since $4u^{3/2} + 24 \approx 37.10 < 59$, u is the fundamental unit of $\mathcal{O}_K$.

Now we look at some cubic examples with rank 1 where the method of Artin's inequality is insufficient to find the fundamental unit.

Example 4.9. Let $K = \mathbf{Q}(\alpha)$ where $\alpha^3 - \alpha - 1 = 0$. The polynomial $T^3 - T - 1$ is irreducible mod 5, so $K/\mathbf{Q}$ is cubic. The polynomial has one real root (approximately 1.324), so $r_1 = 1$. Since $\operatorname{disc}(T^3 - T - 1) = -23$ is squarefree, $\mathcal{O}_K = \mathbf{Z}[\alpha]$. Clearly α is a unit in $\mathcal{O}_K$. It is natural to wonder if α is the fundamental unit, since it is so close to 1 in the real embedding. We can't use Artin's inequality because $|\operatorname{disc}(\mathcal{O}_K)| < 24$, so $|\operatorname{disc}(\mathcal{O}_K)| < 4u^{3/2} + 24$ for all units $u > 1$.

Since we know the unit group (modulo ± 1) is infinite cyclic, to show α is the fundamental unit we show α is the smallest unit greater than 1: no unit $u \in \mathbf{Z}[\alpha]^\times$ satisfies $1 < u < \alpha$. Let $\sigma\colon K \to \mathbf{C}$ be one of the complex embeddings of K, so $\mathrm{N}_{K/\mathbf{Q}}(u) = u\sigma(u)\overline{\sigma}(u) =$

$u|\sigma(u)|^2 > 0$. Therefore $\mathrm{N}_{K/\mathbf{Q}}(u) = 1$. Since $u \notin \mathbf{Q}$, the minimal polynomial of u over $\mathbf{Q}$ is $T^3 + aT^2 + bT - 1$ for some integers a and b. The roots are $u, \sigma(u)$, and $\overline{\sigma}(u)$, so

$$a = -(u + \sigma(u) + \overline{\sigma}(u)), \quad b = u\sigma(u) + u\overline{\sigma}(u) + \sigma(u)\overline{\sigma}(u).$$

Then

$$|a| \leq u + 2|\sigma(u)|, \quad |b| \leq 2u|\sigma(u)| + |\sigma(u)|^2.$$

Since $1 = u|\sigma(u)|^2$, the bound $1 \leq u$ implies $|\sigma(u)| \leq 1$, so from $1 < u < \alpha$ we get

$$|a| < \alpha + 2 \approx 3.3, \quad |b| \leq 2\alpha + 1 \approx 3.6.$$

Thus a and b both lie in $\{0, \pm 1, \pm 2, \pm 3\}$. Among all $T^3 + aT^2 + bT - 1$ with a and b in this set, any such polynomial which has a unit of $\mathcal{O}_K$ as a root must have discriminant equal to a nonzero square multiple of $\mathrm{disc}(\mathcal{O}_K) = -23$ (because, with r being a root, $\mathrm{disc}(\mathbf{Z}[r]) = [\mathcal{O}_K : \mathbf{Z}[r]]^2 \mathrm{disc}(\mathcal{O}_K)$). Several polynomials have this feature, include $T^3 - T - 1$ itself, but aside from $T^3 - T - 1$, the real root of such a polynomial is always larger than α. Therefore α is the fundamental unit of $\mathcal{O}_K$.

Example 4.10. Let $K = \mathbf{Q}(\sqrt[3]{6})$. The reader can check $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{6}]$, so $\mathrm{disc}(\mathcal{O}_K) = \mathrm{disc}(T^3 - 6) = -972$. Let's find a nontrivial unit in $\mathcal{O}_K$. Since $T^3 - 6$ is Eisenstein at 2, the prime 2 is totally ramified in $\mathcal{O}_K$: $(2) = \mathfrak{p}^3$ for some prime ideal $\mathfrak{p}$ of norm 2. The element $2 - \sqrt[3]{6} > 0$ is a root of $(T-2)^3 + 6 = T^3 - 6T^2 + 12T - 2$, so the ideal $(2 - \sqrt[3]{6})$ has norm 2. Therefore $\mathfrak{p} = (2 - \sqrt[3]{6})$. Since $(2) = \mathfrak{p}^3 = (2 - \sqrt[3]{6})^3$, the ratio

$$\frac{(2 - \sqrt[3]{6})^3}{2} \approx .00306$$

is a unit in $\mathbf{Z}[\sqrt[3]{6}]$. It is quite small, so its inverse

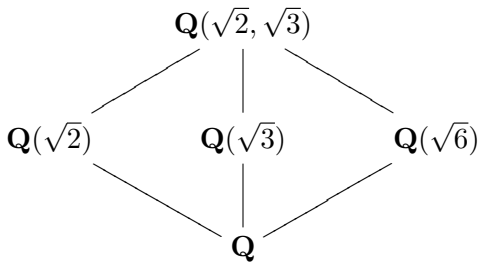
$$u = \frac{2}{(2 - \sqrt[3]{6})^3} = 109 + 60\sqrt[3]{6} + 33\sqrt[3]{36} \approx 326.9908$$

is a unit greater than 1. Since $4u^{3/2} + 24 \approx 23675.75 > 972$, Artin's inequality does not help us prove u is the fundamental unit of $\mathbf{Z}[\sqrt[3]{6}]$, but it really is. In principle, this could be shown by adapting the technique used in the previous example. We omit the details.

5. Units in a multiquadratic field

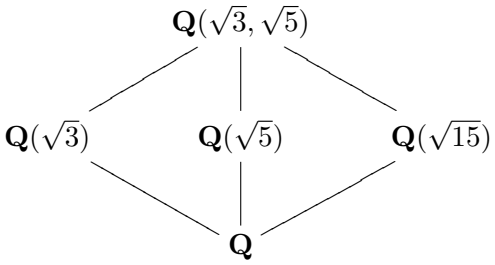
A real quadratic field has unit rank 1. A biquadratic field $\mathbf{Q}(\sqrt{m}, \sqrt{n})$, where m, n, and mn are not squares, has unit rank $4 - 1 = 3$. There are three quadratic subfields, $\mathbf{Q}(\sqrt{m})$, $\mathbf{Q}(\sqrt{n})$, and $\mathbf{Q}(\sqrt{mn})$, and each has a fundamental unit. A choice of one unit from each quadratic subfield need not provide a set of fundamental units for the biquadratic field.

Example 5.1. In the field $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, a system of fundamental units is $1 + \sqrt{2}$, $\sqrt{2} + \sqrt{3}$, and $\frac{\sqrt{2}+\sqrt{6}}{2}$ (see Table 1).



Fundamental units for the three quadratic subfields are $1+\sqrt{2}$, $2+\sqrt{3}$, and $5+2\sqrt{6}$. The units $2+\sqrt{3}$ and $5+2\sqrt{6}$ can't be part of a system of fundamental units for $\mathbf{Q}(\sqrt{2},\sqrt{3})$ since $2+\sqrt{3} = \left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^2$ and $5+2\sqrt{6} = (\sqrt{2}+\sqrt{3})^2$.

Example 5.2. In the field $\mathbf{Q}(\sqrt{3},\sqrt{5})$, a system of fundamental units is $v_1 = \frac{1+\sqrt{5}}{2}$, $v_2 = \frac{3+\sqrt{3}+\sqrt{5}+\sqrt{15}}{2}$, and $v_3 = \frac{3-\sqrt{3}-\sqrt{5}+\sqrt{15}}{2}$.



Fundamental units of the quadratic subfields are $u_1 = 2+\sqrt{3}$, $u_2 = \frac{1+\sqrt{5}}{2}$, and $u_3 = 4+\sqrt{15}$. Every unit in $\mathbf{Q}(\sqrt{3},\sqrt{5})$ has the form $\pm v_1^{a_1}v_2^{a_2}v_3^{a_3}$, which we can coordinatize by the integral vector (a_1,a_2,a_3) if we think about units up to sign. Using PARI, we find $u_1 = v_2/v_3$ and $u_3 = v_2v_3$, so the exponent coordinates of u_1, u_2, u_3 are $(0,1,-1)$, $(1,0,0)$, and $(0,1,1)$, respectively. This is not a basis of $\mathbf{Z}^3$, so the u_i's do not together form a system of fundamental units for $\mathbf{Q}(\sqrt{3},\sqrt{5})$. But each u_i is part of a system of fundamental units, such as $\{v_1,v_2,u_1\}$, $\{u_2,v_2,v_3\}$, and $\{v_1,v_2,u_3\}$.

Since $(0,1,-1)$, $(1,0,0)$, and $(0,1,1)$ span a subgroup of $\mathbf{Z}^3$ with index 2, the index of $\langle u_1,u_2,u_3\rangle$ in $\langle v_1,v_2,v_3\rangle$ is 2, so the index of $\langle u_1,u_2,u_3\rangle$ in the unit group of $\mathbf{Q}(\sqrt{3},\sqrt{5})$ is 4 (having ±1 in the unit group doubles the index).

More generally, consider a multiquadratic field

$$K = \mathbf{Q}(\sqrt{d_1},\ldots,\sqrt{d_k}),$$

where the d_i's are nonsquare integers which are multiplicatively independent modulo squares (that is, they are independent in $\mathbf{Q}^\times/(\mathbf{Q}^\times)^2$). By Galois theory and induction, $[K:\mathbf{Q}] = 2^k$ and $\mathrm{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^k$ by making sign changes on every $\sqrt{d_i}$. The unit rank of K is $r_1 - 1 = 2^k - 1$, and this is also the number of quadratic subfields: such subfields are of the form $\mathbf{Q}(\sqrt{d_I})$, where $I = \{i_1,\ldots,i_m\}$ is a nonempty subset of $\{1,2,\ldots,k\}$ and $d_I = d_{i_1}\cdots d_{i_m}$. Since each $\mathbf{Q}(\sqrt{d_I})$ has unit rank 1, it is natural to suspect that choosing one unit (besides ±1) from each quadratic subfield of K should give us a multiplicatively independent set of units in K.

Theorem 5.3. *With notation as above, let u_I be a unit in $\mathbf{Q}(\sqrt{d_I})$ other than ±1. These units are multiplicatively independent: if $\prod_I u_I^{a_I} = 1$, where the exponents a_I are in $\mathbf{Z}$, then each a_I is 0.*

Proof. Our argument is taken from [3, Lemma 2] (which includes some extraneous hypotheses on the d_i's). The special feature of a unit in a real quadratic field is that its $\mathbf{Q}$-conjugate is, up to sign, its inverse: $u' = \pm u^{-1}$. This fact will interact well with multiplication relations.

A $\mathbf{Q}$-basis of K is all the square roots $\sqrt{d_I}$ together with 1 (we could set $d_\emptyset = 1$ and $1 = \sqrt{d_\emptyset}$). For any nonempty subset J in $\{1,2,\ldots,k\}$, there is a $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ such that

$\sigma(\sqrt{d_J}) = -\sqrt{d_J}$ and $\sigma(\sqrt{d_I}) = \sqrt{d_I}$ for all $I \neq J$. Since σ is the identity on $\mathbf{Q}(\sqrt{d_I})$ and is nontrivial on $\mathbf{Q}(\sqrt{d_J})$, $\sigma(u_I) = u_I$ while $\sigma(u_J) = \pm u_J^{-1}$.

Applying σ to $\prod_I u_I^{a_I} = 1$ turns it into $\prod_{I \neq J} u_I^{a_I} \cdot (\pm u_J^{-1})^{a_J} = 1$. Dividing one multiplicative relation by the other, $(\pm u_J^2)^{a_J} = 1$. Since u_J has infinite order, $a_J = 0$. □

Corollary 5.4. *The units u_I generate a subgroup of $\mathcal{O}_K^\times$ with finite index.*

Proof. By their multiplicative independence, the u_I's generate a group of rank $2^k - 1$, which is the rank of $\mathcal{O}_K^\times$. □

References

[1] E. Kleinert, *Units of Classical Orders: A Survey*, L'Enseignement Math. **40** (1994), 205–248.
[2] E. Kleinert, "Units in Skew Fields," Birkhaüser, Basel, 2000.
[3] F. Luca and I. E. Shparlinski, "On the Square-free Parts of $\lfloor en! \rfloor$," Glasgow Math. J. **49** (2007), 391–403.