DIRICHLET'S UNIT THEOREM

KEITH CONRAD

1. Introduction

Dirichlet's unit theorem describes the structure of the unit group of orders 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 an order in K is finitely generated with $r_1 + r_2 - 1$ independent generators of infinite order.*

More precisely, letting $r = r_1 + r_2 - 1$, each 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 could still have $\mu(\mathcal{O}) = \{\pm 1\}$, *e.g.*, if $\mathcal{O} = \mathbf{Z}[\sqrt{d}]$ for $d < -1$. (Note $\mathbf{Z}[\sqrt{-1}]$ has units $\{\pm 1, \pm i\}$.)

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 and some more examples are described in Sections 4, 5, and 6.

2. Examples

Example 2.1. For $\mathbf{Q}(\sqrt{2})$ we have $r_1 + r_2 - 1 = 1$, so the unit group of each 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 the unit group in the ring of integers of several number fields.

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	$\pm(1+\sqrt[4]{2})^{\mathbf{Z}}(1+\sqrt{2})^{\mathbf{Z}}$
$\mathbf{Q}(\alpha)$	3	0	2	± 1	$\pm\alpha^{\mathbf{Z}}(\alpha+1)^{\mathbf{Z}}$
$\mathbf{Q}(\sqrt{2},\sqrt{3})$	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 $\mathcal{O}_K$. In row 7, $\alpha^3-3\alpha-1=0$.

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 each 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 that 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 each 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. For a unit group with rank greater than 1 let's see how to find multiplicative relations between units numerically, by discovering linear relations with logarithms first. Set $K=\mathbf{Q}(\alpha)$ where $\alpha^3-3\alpha-1=0$. This is in Table 1. 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 $a,b\in\mathbf{Q}$, $\mathrm{N}_{K/\mathbf{Q}}(a\alpha+b)=-a^3f(-b/a)$. 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 6 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 L 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 in $\mathcal{O}_K^\times$ is $\{\pm 1\}$ (why?). Table 2 gives numerical approximations to the images of some units under the mapping L.

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

The table suggests that $L(\alpha-2) = -2L(\alpha+1) = L(1/(\alpha+1)^2)$, so $\alpha - 2 = \pm 1/(\alpha+1)^2$. The minus sign is needed since you can check purely algebraically that $(\alpha-2)(\alpha+1)^2 = -1$. By 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 the plus sign holds. It looks like $L(2-\alpha^2) = L(\alpha+1) - L(\alpha)$, so $2-\alpha^2 = \pm(\alpha+1)/\alpha$. Check the minus sign holds. Since it looks like $L(\alpha^2-\alpha-2) = -L(\alpha+1)$, $\alpha^2-\alpha-2 = \pm 1/(\alpha+1)$. Check the minus sign holds.

We suspect $\{\alpha, \alpha+1\}$ is a system of fundamental units for $\mathbf{Z}[\alpha]^\times$ and will prove this in Example 5.10.

3. Proof of the unit theorem

Our proof of the unit theorem is based on [5, Sect. 1.5] and [6, pp. 214–215] (see also [7, p. 5]), and is deduced from a compactness theorem: the unit theorem is a consequence of 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: a sufficiently large ball will work.

Dirichlet did not use Minkowski's theorem; he proved the unit theorem in 1846 while Minkowski's theorem appeared in 1889. Dirichlet's substitute for the convex-body theorem was the pigeonhole principle. (An account of Dirichlet's proof in German is in [4, Sect. 183] and in English is in [8, Sect. 2.8–2.10].) Dirichlet did not state the unit theorem for all orders, but only those of the form $\mathbf{Z}[\alpha]$, since at that time these were the only kinds of

orders that were considered. According to an oft-repeated story, the main idea for the proof of the unit theorem came to Dirichlet while he attended a concert in the Sistine Chapel.[1]

We set some notation. As in the statement of the unit theorem, K is a number field of degree n, r_1 is the number of real embeddings of K and $2r_2$ is the number of complex embeddings of K (that is, embeddings $K \to \mathbf{C}$ whose image is not in $\mathbf{R}$), so $n = r_1 + 2r_2$. Set $V = \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$, so $\dim_{\mathbf{R}}(V) = n$. The *Euclidean embedding* $\theta_K \colon K \to V$ is defined using the real and complex embeddings of K, as follows. Let the real embeddings of K be $\sigma_1, \ldots, \sigma_{r_1}$ and let the complex embeddings of K be $\sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}$, where we collect the complex embeddings into conjugate pairs $\sigma_j, \overline{\sigma}_j$. For $\alpha \in K$, we set[2]

$$\theta_K(\alpha) = (\sigma_1(\alpha), \cdots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \cdots, \sigma_{r_1+r_2}(\alpha)) \in V.$$

Algebraically, V is a commutative ring using component wise operations. Give V its natural topology as a Euclidean space and *all subsets of V will be given the subspace topology.* A particular subset we will care about is $V^\times = (\mathbf{R}^\times)^{r_1} \times (\mathbf{C}^\times)^{r_2}$.

Let $\mathrm{N} \colon V \to \mathbf{R}$ by

$$\mathrm{N}(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) = x_1 \cdots x_{r_1} |z_1|^2 \cdots |z_{r_2}|^2 = x_1 \cdots x_{r_1} z_1 \overline{z}_1 \cdots z_{r_2} \overline{z}_{r_2}.$$

On the image of K in V, N looks like the norm: $\mathrm{N}(\theta_K(\alpha)) = \mathrm{N}_{K/\mathbf{Q}}(\alpha)$ for all $\alpha \in K$. Set

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

This is a subgroup of $V^\times$, and it is closed in V since G is the inverse image of $\{1\}$ under the continuous map $V \to \mathbf{R}$ given by $v \mapsto |\mathrm{N}(v)|$. Thus G is a closed subgroup of $V^\times$.

Let $\mathcal{O}$ be an order in K and set

$$U = \theta_K(\mathcal{O}^\times) = G \cap \theta_K(\mathcal{O}).$$

(Think "U = units".) We have $U \subset G$ since $\mathcal{O}^\times = \{\alpha \in \mathcal{O} : |\mathrm{N}_{K/\mathbf{Q}}(\alpha)| = 1\}$. Since we give G the subspace topology from V and the image of $\mathcal{O}$ in V under the Euclidean embedding is discrete, U is discrete in G. We will be interested in the quotient group G/U.

Example 3.1. 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. We know $\mathbf{Z}[\sqrt{2}]^\times = \pm(1 + \sqrt{2})^{\mathbf{Z}}$ and $U = \theta_K(\mathbf{Z}[\sqrt{2}]^\times)$ is a discrete subset of G ("equally spaced" in a multiplicative sense). See Figure 1.

Let's see how the subgroup U moves G around by multiplication in Figure 1. Multiplying G by some $u \in U$ moves the arcs between consecutive points of U in Figure 1 to other arcs between consecutive point, and it exchanges the hyperbolas $y = 1/x$ and $y = -1/x$ if

[1]For instance, in 1905 Minkowski [11, pp. 156–7] wrote "Es wird erzählt, da nach langjährigen vergeblichen Bemühungen um das schwierige Problem Dirichlet die Lösung in Rom in der Sixtinischen Kapelle während des Anhörens der Ostermusik ergründet hat. Inwieweit dieses Faktum für die von manchen behauptete Wahlverwandtschaft zwischen Mathematik und Musik spricht, wage ich nicht zu erörtern." (*translation*: "People say that, after many years of unsuccessful efforts in trying to solve this difficult problem, Dirichlet found the solution in Rome in the Sistine Chapel while listening to Easter music. I do not dare to discuss to what extent this fact confirms the conjectured (by some people) relationship between mathematics and music.")

[2]The Euclidean embedding of K, as defined here, depends on the ordering of the different real and complex embeddings as well as on the choice of one complex embedding from each conjugate pair. A coordinate-free way of defining the Euclidean embedding uses tensor products: the natural mapping $K \to \mathbf{R} \otimes_{\mathbf{Q}} K$ where $\alpha \mapsto 1 \otimes \alpha$ is a ring homomorphism into a finite-dimensional real vector space of dimension n, just like V.

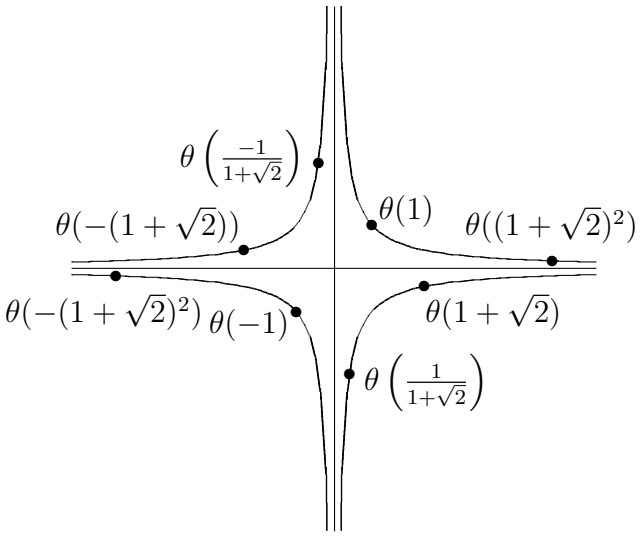


FIGURE 1. Units in $\mathbf{Z}[\sqrt{2}]$ on $G = \{(x, y) \in \mathbf{R}^2 : |xy| = 1\}$.

$\mathrm{N}(u) = -1$. Multiplication by $\theta(-1) = (-1, -1)$ on G exchanges the two branches on each hyperbola.

Modulo U each $(x, y) \in G$ 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 Example 3.1 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 the compactness of G/U without knowing the structure of the unit group in advance.

Lemma 3.2. *For nonzero a 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 3.3. *For each positive integer N, finitely many $a \in \mathcal{O}$ satisfy $|\mathrm{N}_{K/\mathbf{Q}}(a)| = N$ up to multiplication by $\mathcal{O}^\times$. That is, there are $a_1, \ldots, a_k \in \mathcal{O}$, where k depends on N, such that $|\mathrm{N}_{K/\mathbf{Q}}(a_i)| = N$ and each $a \in \mathcal{O}$ satisfying $|\mathrm{N}_{K/\mathbf{Q}}(a)| = N$ is a unit multiple of an a_i.*

Proof. If $|\mathrm{N}_{K/\mathbf{Q}}(a)| = N$ then $[\mathcal{O} : (a)] = N$ by Lemma 3.2, so $N\mathcal{O} \subset (a) \subset \mathcal{O}$. Since $\mathcal{O}/N\mathcal{O}$ is finite, there are only finitely many principal ideals between $N\mathcal{O}$ and $\mathcal{O}$. Let $(a_1), \ldots, (a_k)$ be those ideals. Then $(a) = (a_i)$ for some i, so a and a_i are unit multiples. □

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

Proof. We will find a compact subset S of G that represents all cosets in G/U. The continuous map $S \to G/U$ is onto and thus G/U is 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 a 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.

Pick a compact, convex, centrally symmetric region $C \subset V$ with $\mathrm{vol}(C) > 2^n \mathrm{vol}(\theta_K(\mathcal{O}))$, where the "volume" of the lattice $\theta_K(\mathcal{O})$ means the volume of a fundamental domain for this lattice as a subset of V. For instance, C could be a large ball in V centered at the origin. For *each* $g \in G$, 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. Using g^{-1} instead of g, Minkowski's convex body theorem applies to $g^{-1}C$ and the lattice $\mathcal{O} \subset V$ (we identify $\mathcal{O}$ with $\theta_K(\mathcal{O})$):

$$g^{-1}C \cap (\mathcal{O} - \{0\}) \neq \emptyset.$$

Let a be a nonzero element of $\mathcal{O}$ lying in $g^{-1}C$. Then $|\mathrm{N}_{K/\mathbf{Q}}(a)| = |\mathrm{N}(a)| \in |\mathrm{N}(g^{-1}C)| = |\mathrm{N}(C)|$, which is a bounded subset of $\mathbf{R}$ since C is compact. Note $|\mathrm{N}(C)|$ is independent of g. The number $|\mathrm{N}_{K/\mathbf{Q}}(a)|$ is also an integer, so $|\mathrm{N}_{K/\mathbf{Q}}(a)|$ lies in a *finite set* (a bounded set of integers is finite). Combining that with Lemma 3.3, there is a finite set $\{a_1, \ldots, a_m\}$ of nonzero elements of $\mathcal{O}$ such that every $g^{-1}C$ meets some $a_i\mathcal{O}^\times = a_iU$, which implies every gU meets some $a_i^{-1}C$.

We have shown the quotient group G/U is represented by $G \cap \bigcup_{i=1}^m a_i^{-1}C$. The union $\bigcup_{i=1}^m a_i^{-1}C$ is a compact subset of V, since each $a_i^{-1}C$ is compact, and since G is closed in V the intersection $G \cap \bigcup_{i=1}^m a_i^{-1}C$ is compact in G. Hence G/U has a compact set of representatives in G, so G/U is compact in the quotient topology. □

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

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

where the coefficients 2 in this formula are related to the exponents 2 in the definition of N. The function L is a continuous group homomorphism and, for each $g \in G$, $L(g)$ lies in the hyperplane

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

It is easy to see that $L(G) = H$, 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 restricted to U is finite cyclic (coming from roots of unity in U).

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

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

Every 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 $V^\times$ (all discrete subsets are 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 (a 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 every finite subgroup of $K^\times$ is a cyclic group. (Warning: it is *false* that the kernel of L as a map out of $K^\times$, not U, is only the roots of unity in K. An element of $K^\times$ that has all of its $\mathbf{Q}$-conjugates lying on

the unit circle is in the kernel of L. An example in $\mathbf{Q}(i)$ is $3/5 + (4/5)i$, or more generally $a/c + (b/c)i$ where (a, b, c) is a Pythagorean triple. These are not algebraic *integers* if they are not ± 1 or $\pm i$, 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 it is also discrete 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 a bounded region of $\mathbf{R}^{r_1+r_2}$. Indeed, consider the box

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

Suppose $L(u)$ is in this box for some $u \in U$. The real embeddings[3] 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 (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.*, $\mathbf{R}^2/(\mathbf{Z} \times \{0\})$ 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 $\varepsilon \in \mathcal{O}^\times$, $L(\varepsilon) = m_1 L(\varepsilon_1) + \cdots + m_r L(\varepsilon_r)$ 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, but this alone doesn't tell us there are units of infinite order in $\mathcal{O}^\times$. The place in the proof where saw there are units of infinite order (if $r_1 + r_2 - 1 > 0$) is when we went from $r' \leq r_1 + r_2 - 1$ to $r' = r_1 + r_2 - 1$. This happened two paragraphs up and relied on G/U being compact.

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, cubic with 1 real embedding (that is, a cubic field that

[3]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.

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 $\mathcal{O}^\times = \pm\varepsilon^{\mathbf{Z}}$.[4] 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 $\mathbf{Z}[3\sqrt{2}]^\times = \pm(17+12\sqrt{2})^{\mathbf{Z}}$, $\mathbf{Z}[3\sqrt{2}]$ has fundamental unit $17+12\sqrt{2}$.

Example 4.3. In Example 4.9 we will show $\mathbf{Z}[\sqrt[3]{6}]^\times = \pm(109 + 60\sqrt[3]{6} + 33\sqrt[3]{36})^{\mathbf{Z}}$, so $109 + 60\sqrt[3]{6} + 33\sqrt[3]{36} \approx 326.990$ is the fundamental unit of $\mathbf{Z}[\sqrt[3]{6}]$.

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 examples of fundamental unit computations in the cubic case, we will use an inequality due to Artin [1, pp. 169–170]. Mordell [12], near the end of his review of [1] in 1962, described Artin's inequality as a "surprise" since "one would have thought that there was not much opportunity for new results on cubic units".

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 argument is similar to Artin's in [1] and may look like a messy calculation. Consider reading the corollary and its applications first, and 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 v 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

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

Since $x > 1$, $x^3 + x^{-3} > 2$. Set $a = (x^3+x^{-3})/2$, so $a > 1$ and by taking absolute values,

$$\begin{aligned}
|\operatorname{disc}(\mathbf{Z}[v])| &= 4(\sin^2 t)(2a-2\cos t)^2 \\
&= 16(1-\cos^2 t)(a-\cos t)^2. \qquad (4.1)
\end{aligned}$$

Set $y = \cos t$, so $y \in [-1,1]$. Then (4.1) is

$$f(y) = 16(1-y^2)(a-y)^2$$

and we want to maximize this on $[-1,1]$. Let a maximum occur at y_0. Since $f(y) \geq 0$ on $[-1,1]$ with $f(1) = f(-1) = 0$ and $f(0) = 16a^2 > 0$, we have $y_0 \in (-1,1)$ and $f'(y_0) = 0$.

By the product rule, $\boxed{f'(y) = 32(a-y)(2y^2-ay-1)}$ and the root of the linear factor is a, with $a > 1 > y_0$, so from $f'(y_0) = 0$ we have $2y_0^2 - ay_0 - 1 = 0$. Rewrite this as

$$ay_0 = 2y_0^2 - 1. \qquad (4.2)$$

[4] Don't confuse $\pm\varepsilon^{\mathbf{Z}}$ with $\varepsilon^{\pm\mathbf{Z}}$; the latter is just $\varepsilon^{\mathbf{Z}}$.

Thus

$$|\operatorname{disc}(\mathbf{Z}[v])| = f(\cos t) \leq f(y_0) = 16(1-y_0^2)(a-y_0)^2. \tag{4.3}$$

Expanding $(a-y_0)^2$ and using the relation (4.2) a couple of times, we get

$$16(1-y_0^2)(a-y_0)^2 = 16(a^2+1-y_0^4-y_0^2).$$

Substituting $a = (x^3+x^{-3})/2$ into this,

$$\begin{aligned} f(y_0) &= 16\left(\frac{x^6}{4} + \frac{3}{2} + \left(\frac{x^{-6}}{4} - y_0^4 - y_0^2\right)\right) \\ &= 4x^6 + 24 + 4(x^{-6} - 4y_0^4 - 4y_0^2) \\ &= 4v^3 + 24 + 4(x^{-6} - 4y_0^4 - 4y_0^2). \end{aligned}$$

We will show $x^{-6} < 4y_0^2$, so $f(y_0) < 4v^3 + 24$. Then by (4.3), $|\operatorname{disc}(\mathbf{Z}[v])| < 4v^3 + 24$, as desired.

Let $h(y) = 2y^2 - ay - 1$, the quadratic factor of $f'(y)$, so $h'(y_0) = 0$. Since $h(-1) = 1 + a > 0$ and $h(0) = -1 < 0$, $h(y)$ has a root in $(-1, 0)$. And since $h(1) = 1 - a < 0$ and $h(y) > 0$ for large y, $h(y)$ also has a root in $(1, \infty)$. Thus $-1 < y_0 < 0$. Since $x > 1$, the desired inequality $x^{-6} < 4y_0^2$ is the same as $y_0 < -1/(2x^3)$. The graph of $h(y)$ is a concave up parabola and y_0 is the smaller root of $h(y)$, so to prove $y_0 < -1/(2x^3)$ it is enough to show $h(-1/(2x^3)) < 0$:

$$h\left(\frac{-1}{2x^3}\right) = \frac{2}{4x^6} + \frac{a}{2x^3} - 1 = \frac{1}{2x^6} + \frac{1}{2x^3}\frac{x^3+x^{-3}}{2} - 1 = \frac{3}{4x^6} - \frac{3}{4} = \frac{3}{4}\left(\frac{1}{x^6} - 1\right) < 0$$

since $x > 1$. □

Remark 4.5. The condition on v in Theorem 4.4 is $v > 1$, *not* $v > 0$. If we could use $0 < v < 1$ in Artin's inequality, then replacing v with a high power of itself would imply $|\operatorname{disc}(\mathcal{O})| < 24$, which is false for all cubic orders with one exception. See Footnote 8 below.

Corollary 4.6. *Let $\mathcal{O}$ be an order in a cubic field K with $r_1 = 1$. Viewing K inside $\mathbf{R}$, let $\varepsilon > 1$ be the fundamental unit of $\mathcal{O}$. For each unit $u > 1$ in $\mathcal{O}^\times$, if $4u^{3/m} + 24 \leq |\operatorname{disc}(\mathcal{O})|$ for an integer $m \geq 2$ then $u = \varepsilon^k$ where $1 \leq k < m$. In particular, if $4u^{3/2} + 24 \leq |\operatorname{disc}(\mathcal{O})|$ then $u = \varepsilon$.*

Proof. The group $\mathcal{O}^\times$ is $\pm\varepsilon^{\mathbf{Z}}$, so $u = \varepsilon^k$ for some positive integer k. Artin's inequality using $v = \varepsilon$ says

$$|\operatorname{disc}(\mathcal{O})| < 4\varepsilon^3 + 24 = 4u^{3/k} + 24.$$

If $k \geq m$ then $|\operatorname{disc}(\mathcal{O})| < 4u^{3/k} + 24 \leq 4u^{3/m} + 24 \leq |\operatorname{disc}(\mathcal{O})|$, so we have a contradiction. Thus $k < m$. □

Example 4.7. Let $K = \mathbf{Q}(\sqrt[3]{2})$, so $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{2}]$[5] 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 $4u^{3/2} + 24 \approx 54.185 \leq 108$, u is the fundamental unit of $\mathcal{O}_K$.

[5]See Example 2.4 in https://kconrad.math.uconn.edu/blurbs/gradnumthy/totram.pdf.

Example 4.8. Let $K = \mathbf{Q}(\alpha)$, where $\alpha^3 + 2\alpha + 1 = 0$. The polynomial $T^3 + 2T + 1$ is irreducible modulo 3, so $K/\mathbf{Q}$ is cubic. Since $\mathrm{disc}(T^3 + 2T + 1) = -59$, which is squarefree, $\mathcal{O}_K = \mathbf{Z}[\alpha]$. Clearly α is a unit. Since $T^3 + 2T + 1$ has one real root, approximately $-.45$, which we identify with α using the real embedding of K, a unit greater than 1 is

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

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

Example 4.9. Let $K = \mathbf{Q}(\sqrt[3]{6})$, so $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{6}]$.[6] This will be an example where a unit u we find will satisfy $4u^{3/2} + 24 > |\mathrm{disc}(\mathcal{O}_K)|$, so we will have to be more creative to prove u is the fundamental unit of $\mathcal{O}_K$.

To find units in $\mathcal{O}_K$, we seek two different descriptions of a principal ideal in $\mathcal{O}_K$: if $(\alpha) = (\beta)$ then $\alpha = \beta u$ where u is a unit. Here is a table of how the first few primes p decompose in $\mathcal{O}_K$, based on how $T^3 - 6 \bmod p$ decomposes.

p	$T^3 - 6 \bmod p$	(p)
2	T^3	$\mathfrak{p}_2^3$
3	T^3	$\mathfrak{p}_3^3$
5	$(T-1)(T^2+T+1)$	$\mathfrak{p}_5\mathfrak{p}_{25}$
7	$(T-3)(T-5)(T-6)$	$\mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7''$

The only ideal of norm 2 is $\mathfrak{p}_2$. We will prove $\mathfrak{p}_2$ is principal by finding an element of absolute norm 2. For $c \in \mathbf{Z}$, $\mathrm{N}_{K/\mathbf{Q}}(\sqrt[3]{6} + c) = c^3 + 6$. Therefore $\mathrm{N}_{K/\mathbf{Q}}(\sqrt[3]{6} - 2) = -2$, so the ideal $(\sqrt[3]{6} - 2)$ has norm 2 and must be $\mathfrak{p}_2$. We have the equality of principal ideals

$$(2) = \mathfrak{p}_2^3 = (\sqrt[3]{6} - 2)^3 = ((\sqrt[3]{6} - 2)^3),$$

so the numbers 2 and $(\sqrt[3]{6} - 2)^3$ are equal up to a unit multiple in $\mathcal{O}_K$. Since $(\sqrt[3]{6} - 2)^3 \approx -.0061$, to get a unit greater than 1 we use the ratio[7]

$$u = -\frac{2}{(\sqrt[3]{6} - 2)^3} \approx 326.9908.$$

Since $\mathrm{disc}(\mathcal{O}_K) = \mathrm{disc}(\mathbf{Z}[\sqrt[3]{6}]) = \mathrm{disc}(T^3 - 6) = -972$ and $4u^{3/2} + 24 \approx 23675.75 > 972$, we can't say right away that u is the fundamental unit of $\mathcal{O}_K$ from Corollary 4.6.

Let $\varepsilon > 1$ be the unknown fundamental unit of $\mathbf{Z}[\sqrt[3]{6}]$. Does $u = \varepsilon$? Since $u > 1$, the unit theorem implies $u = \varepsilon^k$ for some $k \geq 1$ and we want to show $k = 1$. Artin's inequality with $v = \varepsilon$ says that in $\mathbf{R}$,

$$|\mathrm{disc}(\mathcal{O}_K)| < 4\varepsilon^3 + 24 \Longrightarrow 972 < 4u^{3/k} + 24.$$

For large k this inequality fails, since the left side is 972 and the right side tends to $4+24 = 28$ as $k \to \infty$. More precisely, since $4u^{3/4} + 24 \approx 331.5 < 972$, k is either 1, 2, or 3. How do we rule out $u = \varepsilon^2$ and $u = \varepsilon^3$ in order to know $u = \varepsilon$?

Here's a great idea: to prove an algebraic integer is not a square or cube, prove it is not a square or cube modulo $\mathfrak{p}$ for some prime ideal $\mathfrak{p}$. Looking at the above table of prime ideal factorizations, we will use the ideals $\mathfrak{p}_5$ and $\mathfrak{p}_7$.

In $\mathcal{O}_K/\mathfrak{p}_5 \cong \mathbf{Z}/(5)$ we have $\sqrt[3]{6} \equiv 1 \bmod \mathfrak{p}_5$, so $u \equiv 2/(2-1)^3 \equiv 2 \bmod \mathfrak{p}_5$. The nonzero squares in $\mathbf{Z}/(5)$ are 1 and 4, so u is not a square in $\mathcal{O}_K/\mathfrak{p}_5$ and thus is not a square in $\mathcal{O}_K$.

[6] See Example 2.10 in https://kconrad.math.uconn.edu/blurbs/gradnumthy/totram.pdf.

[7] Explicitly, $u = 109 + 60\sqrt[3]{6} + 33\sqrt[3]{36}$, but this representation will not be needed.

In $\mathcal{O}_K/\mathfrak{p}_7 \cong \mathbf{Z}/(7)$ we have $\sqrt[3]{6} \equiv 3 \bmod \mathfrak{p}_7$, so $u \equiv 2/(2-3)^3 \equiv -2 \equiv 5 \bmod \mathfrak{p}_7$. The nonzero cubes in $\mathbf{Z}/(7)$ are 1 and 6, so u is not a cube in $\mathcal{O}_K$. (Using $\mathfrak{p}_7'$ or $\mathfrak{p}_7''$ would have led to the same conclusion.)

We have shown $k = 1$, so $u = \varepsilon$ is the fundamental unit of $\mathbf{Z}[\sqrt[3]{6}]$.

Example 4.10. 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 $\alpha \approx 1.324$, 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 of $\mathcal{O}_K$ since it is so close to 1 in the real embedding. We can't use Artin's inequality because $|\operatorname{disc}(\mathcal{O}_K)| < 24$,[8] so for every unit $u > 1$ and positive integer m, $|\operatorname{disc}(\mathcal{O}_K)| < 4u^{3/m} + 24$.

Since we know $\mathcal{O}_K^\times/\{\pm 1\}$ 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

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

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

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

Thus a and b both lie in $\{0, \pm 1, \pm 2, \pm 3\}$. There are 49 polynomials $T^3 + aT^2 + bT - 1$ with a and b in that set. Such a polynomial having a unit $u > 1$ in $\mathcal{O}_K$ as a root must have discriminant of the form $-23m^2$ because $\operatorname{disc}(\mathbf{Z}[u]) = [\mathcal{O}_K : \mathbf{Z}[u]]^2 \operatorname{disc}(\mathcal{O}_K)$. There are four such polynomials, shown in the table below, including $T^3 - T - 1$ itself. Each of these polynomials has one real root that turns out to be a small power of α.[9]

Polynomial	Discriminant	Real Root
$T^3 - T - 1$	-23	$\alpha \approx 1.324$
$T^3 - 2T^2 + T - 1$	-23	$\alpha^2 \approx 1.754$
$T^3 - 3T^2 + 2T - 1$	-23	$\alpha^3 \approx 2.324$
$T^3 - 2T^2 - 3T - 1$	-23	$\alpha^4 \approx 3.079$

Since α is the smallest root in this list, it is the fundamental unit of $\mathcal{O}_K$.

Example 4.11. Let $K = \mathbf{Q}(\alpha)$ where $\alpha^3 - \alpha - 5 = 0$. The polynomial $T^3 - T - 5$ is irreducible mod 3, so $K/\mathbf{Q}$ is cubic. The polynomial has one real root $\alpha \approx 1.904$, so $r_1 = 1$. Since $\operatorname{disc}(T^3 - T - 5) = -671 = -11 \cdot 61$ is squarefree, $\mathcal{O}_K = \mathbf{Z}[\alpha]$. An example of a unit is $\alpha - 2$: it is a root of

$$(T+2)^3 - (T+2) - 5 = T^3 + 6T^2 + 11T + 1,$$

so $\mathrm{N}_{K/\mathbf{Q}}(\alpha - 2) = -1$. In $\mathbf{R}$, $\alpha - 2 \approx -.095$, so a unit greater than 1 is $u := -1/(\alpha - 2) \approx 10.43$. Since $4u^{3/2} + 24 \approx 158.81 \le 671$, u is the fundamental unit of $\mathcal{O}_K$.

[8] This field K is the only cubic field, up to isomorphism, with absolute discriminant less than 24, so $\mathcal{O}_K$ is the only cubic order with absolute discriminant less than 24.

[9] All the polynomials in the table have discriminant -23, but this is not true for the minimal polynomials of all powers of α, *e.g.*, α^6 has minimal polynomial $T^3 - 5T^2 - 2T - 1$ with discriminant $-575 = -23 \cdot 5^2$.

Example 4.12. We will show for all $a \in \mathbf{Z}^+$ that $f(T) = T^3 + aT - 1$ is irreducible over $\mathbf{Q}$ with a unique real root α and $\mathbf{Z}[\alpha]^\times = \pm\alpha^{\mathbf{Z}}$ (even if $\mathbf{Z}[\alpha]$ is not the integers of $\mathbf{Q}(\alpha)$).

By the rational roots theorem, a rational root of $f(T)$ must be ± 1, and $f(1) = a \neq 0$ and $f(-1) = -a - 2 \neq 0$. Thus $f(T)$ is cubic with no rational root, so it is irreducible over $\mathbf{Q}$. From $f(0) = -1 < 0$ and $f(1) = a > 0$, $f(T)$ has a real root α in $(0, 1)$. This is the only real root, either because $\mathrm{disc}(f(T)) = -4a^3 - 27 < 0$ or because $f'(x) = 3x^2 + a > 0$ for $x \in \mathbf{R}$, so f is increasing on $\mathbf{R}$.[10]

Set $u = 1/\alpha$, a unit in $\mathbf{Z}[\alpha]$ with $u > 1$, so $\pm\alpha^{\mathbf{Z}} = \pm u^{\mathbf{Z}}$. To prove $\mathbf{Z}[\alpha]^\times = \pm u^{\mathbf{Z}}$ we will try to check $4u^{3/2} + 24 \leq |\mathrm{disc}(\mathbf{Z}[\alpha])|$ so we can apply Corollary 4.6:

$$4u^{3/2} + 24 \leq |\mathrm{disc}(\mathbf{Z}[\alpha])| \iff 4\left(\frac{1}{\alpha}\right)^{3/2} + 24 \stackrel{?}{\leq} 4a^3 + 27 \iff 1 \stackrel{?}{\leq} (a^2\alpha)^{3/2} + \frac{3}{4}\alpha^{3/2}. \tag{4.4}$$

This inequality turns out to be true for $a \geq 2$: $1/a - 1/a^4 < \alpha < 1/a$ since $f(1/a) = 1/a^3 > 0$ and $f(1/a - 1/a^4) = -(3(a^6 - a^3) + 1)/a^{12} < 0$, so

$$(a^2\alpha)^{3/2} + \frac{3}{4}\alpha^{3/2} > (a^2\alpha)^{3/2} > \left(a - \frac{1}{a^2}\right)^{3/2} > 1$$

since $x - 1/x^2$ is increasing for $x > 0$. This verifies (4.4), so $\mathbf{Z}[\alpha]^\times = \pm(1/\alpha)^{\mathbf{Z}} = \pm\alpha^{\mathbf{Z}}$.

What if $a = 1$? In that case, $1/\alpha \approx 1.4655$, so $4(1/\alpha)^{3/2} + 24 \approx 31.096 > 4a^3 + 27$. Since $4(1/\alpha)^{3/3} + 24 \approx 29.862 < 4a^3 + 27$, we have $1/\alpha = \varepsilon$ or ε^2 where ε is the fundamental unit of $\mathbf{Z}[\alpha]$. To rule out $1/\alpha = \varepsilon^2$ we will show $1/\alpha$ is not a square in $\mathbf{Z}[\alpha]$ by showing it's not a square mod $\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ in $\mathbf{Z}[\alpha]$. Since $\mathrm{disc}(f(T)) = -31$ is squarefree, $\mathbf{Z}[\alpha]$ is the ring of integers of $\mathbf{Q}(\alpha)$.[11] From $f(T) = T^3 + T - 1 \equiv (T - 2)(T^2 + 2T + 2) \bmod 3$, $(3) = \mathfrak{p}_3\mathfrak{p}_9$ with $\alpha \equiv 2 \bmod \mathfrak{p}_3$. Thus $1/\alpha \equiv 2 \bmod \mathfrak{p}_3$, which isn't a square in $\mathbf{Z}[\alpha]/\mathfrak{p}_3 \cong \mathbf{F}_3$.

Remark 4.13. We can use the family of rings $\mathbf{Z}[\alpha]$ in the previous examples to show that in Artin's inequality $|\mathrm{disc}(\mathcal{O})| < 4v^3 + 24$, the coefficient 4 and exponent 3 are "optimal". Suppose we always have $|\mathrm{disc}(\mathcal{O})| < Av^B + C$ for universal constants A, B, and C. Take $\mathcal{O} = \mathbf{Z}[\alpha]$ where α is a root of $T^3 + aT - 1$ for $a \in \mathbf{Z}^+$. Then the inequality for the unit $1/\alpha$ that's bigger than 1 becomes $4a^3 + 27 < A(1/\alpha)^B + C$. Dividing through by $4a^3$,

$$1 + \frac{27}{4a^3} < \frac{A}{4}\frac{1}{a^3\alpha^B} + \frac{C}{4a^3} = \frac{A}{4}\frac{a^{B-3}}{(a\alpha)^B} + \frac{C}{4a^3}. \tag{4.5}$$

When $a \to \infty$, the left side of (4.5) tends to 1. From the bounds $1/a - 1/a^4 < \alpha < 1/a$ in the previous example, $a\alpha \to 1$ as $a \to \infty$,[12] so the right side of (4.5) tends to 0 if $B < 3$, to $A/4$ if $B = 3$, and to ∞ if $B > 3$. Therefore $B \geq 3$, and if $B = 3$ then $A/4 \geq 1$, so $A \geq 4$.

If Artin's inequality were changed to $|\mathrm{disc}(\mathcal{O})| < 4v^3 + C$, must $C \geq 24$? An example showing C is at least above 20 is $\mathcal{O} = \mathbf{Z}[\beta]$ where β is a root of $T^3 - 2T^2 - T - 1$: the polynomial has discriminant -87 and $\beta \approx 2.546$ is the fundamental unit of $\mathbf{Z}[\beta]$, so $C > |-87| - 4\beta^3 \approx 20.92$. I don't know any larger lower bound on C.

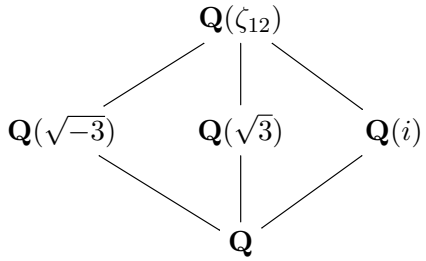
[10] $f(T)$ is irreducible when a is not 0 or -2. It has three real roots for $a \leq -3$. The case $a = -1$ was treated in Example 4.10.

[11] For $a \geq 2$, the ring of integers of $\mathbf{Q}(\alpha)$ is $\mathbf{Z}[\alpha]$ when $4a^3 + 27$ is squarefree, but also many times when $4a^3 + 27$ is not squarefree: $a = 3, 6, 12, 15, 21, 24, 30, 39, \ldots$.

[12] With a bit more care, the upper bound on α can be reduced from $1/a$ to $1/a - (1/2)/a^4$ when $a \geq 2$.

We now consider rank 1 unit groups in two totally complex quartic fields: $\mathbf{Q}(\zeta_{12})$ and $\mathbf{Q}(\zeta_5)$. Each field has a real quadratic subfield (the fixed field of complex conjugation) and norms down to that subfield will help us determine a fundamental unit in the quartic field.

Example 4.14. Let $K = \mathbf{Q}(\zeta_{12}) = \mathbf{Q}(\zeta_3, \zeta_4) = \mathbf{Q}(\sqrt{-3}, i) = \mathbf{Q}(\sqrt{3}, i)$. It has three quadratic subfields, as shown in the diagram below. In particular, K has the real quadratic subfield $\mathbf{Q}(\sqrt{3})$, which has unit rank 1 with fundamental unit $2 + \sqrt{3}$.



Since complex conjugation on $\mathbf{Q}(\zeta_{12})$ is an automorphism with order 2, $\mathbf{Q}(\zeta_{12})$ has degree 2 over the fixed field of complex conjugation. That fixed field has to be $\mathbf{Q}(\sqrt{3})$, either because $\mathbf{Q}(\sqrt{-3})$ and $\mathbf{Q}(i)$ are not fixed by complex conjugation or because (using $\zeta_{12} = e^{2\pi i/12}$) we have $\zeta_{12} + \zeta_{12}^{-1} = 2\cos(2\pi/12) = 2\cos(\pi/6) = \sqrt{3}$.

For each $u \in \mathcal{O}_K^\times$, $\overline{u}$ is also in $\mathcal{O}_K^\times$, so $u\overline{u} \in \mathcal{O}_K^\times \cap \mathbf{R} = \mathcal{O}_K^\times \cap \mathbf{Q}(\sqrt{3}) = \mathbf{Z}[\sqrt{3}]^\times$. Conversely, if $t \in \mathcal{O}_K$ then $t\bar{t} \in \mathbf{Z}[\sqrt{3}]$, so if $t\bar{t} \in \mathbf{Z}[\sqrt{3}]^\times$ with inverse $\alpha \in \mathbf{Z}[\sqrt{3}]$, then $t \in \mathcal{O}_K^\times$ because $t(\bar{t}\alpha) = 1$ in $\mathcal{O}_K$.

In particular, $\zeta_{12} - 1$ is a unit in $\mathcal{O}_K$ because

$$(\zeta_{12} - 1)\overline{(\zeta_{12} - 1)} = (\zeta_{12} - 1)(\zeta_{12}^{-1} - 1) = 1 - (\zeta_{12} + \zeta_{12}^{-1}) + 1 = 2 - (\zeta_{12} + \zeta_{12}^{-1}) = 2 - \sqrt{3},$$

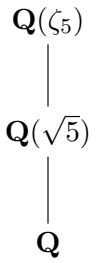
which is a unit in $\mathbf{Z}[\sqrt{3}]$.

Setting $u = \zeta_{12} - 1$, we'll show u is a fundamental unit of K. The roots of unity of K are the powers of ζ_{12}, and the unit theorem tells us there is a fundamental unit v in K, so $u = \zeta_{12}^j v^k$ for some integers j and k. Taking complex conjugates of both sides, $\overline{u} = \zeta_{12}^{-j}\overline{v}^k$, so

$$2 - \sqrt{3} = u\overline{u} = (v\overline{v})^k.$$

The product $v\overline{v}$ is a positive unit in $\mathbf{Q}(\sqrt{3})$, and $2 - \sqrt{3} = 1/(2 + \sqrt{3})$ is a generator of the positive units of $\mathbf{Q}(\sqrt{3})$, so $v\overline{v} = (2 - \sqrt{3})^\ell$ for some $\ell \in \mathbf{Z}$. Thus $2 - \sqrt{3} = (2 - \sqrt{3})^{k\ell}$, so $k = \pm 1$. Therefore u is $\zeta_{12}^j v$ or $\zeta_{12}^j v^{-1}$, so u is a fundamental unit of K.

Example 4.15. Let $K = \mathbf{Q}(\zeta_5)$. It is cyclic over $\mathbf{Q}$ with one quadratic subfield, $\mathbf{Q}(\sqrt{5})$.



A fundamental unit of $\mathbf{Q}(\sqrt{5})$ is $u = (1 + \sqrt{5})/2$. We will show u is also a fundamental unit of K. The roots of unity in K are the 10th roots of unity: powers of $-\zeta_5$. Let v be

a fundamental unit of K, so $u = (-\zeta_5)^j v^k$ for some $j, k \in \mathbf{Z}$. Taking complex conjugates of both sides, $u = (-\zeta_5)^{-j}\overline{v}^k$ since u is real, so $u^2 = (v\overline{v})^k$. Since $v\overline{v}$ is a positive unit in $\mathbf{Q}(\sqrt{5})$, $v\overline{v} = u^\ell$ for some $\ell \in \mathbf{Z}$, so $u^2 = (u^\ell)^k = u^{k\ell}$, so $k\ell = 2$. Thus k is ± 1 or ± 2. If $k = \pm 1$ then u is a fundamental unit of K. We will show $k \neq \pm 2$.

Suppose $k = \pm 2$, so $u = (-\zeta_5)^j v^2$. That means $u(-\zeta_5)^{-j}$ is a square in $\mathcal{O}_K$, so it is also a square in the residue fields $\mathcal{O}_K/\mathfrak{p}$ for all prime ideals $\mathfrak{p}$. We'll get a contradiction by using $\mathfrak{p} = (1 - \zeta_5)$, which is the unique prime in $\mathcal{O}_K$ that lies over 5. In $\mathcal{O}_K/(\zeta_5 - 1)$ we have $\zeta_5 \equiv 1$ and $5 \equiv 0$, so $u(-\zeta_5)^{-j} \equiv \pm u$ and $u = (1 + \sqrt{5})/2 \equiv 3$. The field $\mathcal{O}_K/(\zeta_5 - 1)$ has order 5, so it is (uniquely) isomorphic to $\mathbf{Z}/5\mathbf{Z}$ and ± 3 are not squares in $\mathbf{Z}/5\mathbf{Z}$. Thus u is not a square in $\mathcal{O}_K/(\zeta_5 - 1)$, so u can't be a square in $\mathcal{O}_K$. We have reached a contradiction.

Remark 4.16. Not all totally complex quartic fields can be treated like in the previous two examples since some totally complex quartic fields have no (real) quadratic subfield. An example is $K = \mathbf{Q}(\alpha)$ where $\alpha^4 + 8\alpha + 12$. The polynomial $T^4 + 8T + 12$ is irreducible over $\mathbf{Q}$ with no real roots and its Galois group over $\mathbf{Q}$ is isomorphic to A_4. A quadratic subfield of K would correspond by Galois theory to an index-2 subgroup of A_4, and A_4 has no such subgroup. Using a computer, a fundamental unit of K is $\frac{1}{2}\alpha^3 + \alpha^2 - 1$.

5. The regulator and some rank 2 unit groups

For an order $\mathcal{O}$ in a totally real cubic field K, the rank of $\mathcal{O}^\times$ is 2 and the roots of unity in K are ± 1, so $\mathcal{O}^\times = \pm\varepsilon_1^{\mathbf{Z}}\varepsilon_2^{\mathbf{Z}}$, where ε_1 and ε_2 are multiplicatively independent (Example 2.4). We will address two topics in this section:

- how to show units in $\mathcal{O}$ are multiplicatively independent,
- how to show two independent units in $\mathcal{O}$ generate $\mathcal{O}^\times/\{\pm 1\}$.

Both of these will use an important numerical invariant of $\mathcal{O}^\times$ called its regulator.

Let $\sigma_1, \sigma_2, \sigma_3$ be the different real embeddings of K. From the proof of the unit theorem, the mapping $\mathcal{O}^\times \to \mathbf{R}^3$ where

$$u \to (\log|\sigma_1(u)|, \log|\sigma_2(u)|, \log|\sigma_3(u)|) \tag{5.1}$$

has kernel ± 1 and image of rank 2 in the hyperplane $H = \{(x, y, z) \in \mathbf{R}^3 : x + y + z = 0\}$.

Theorem 5.1. *Multiplicative independence of u and v in $\mathcal{O}^\times$ is equivalent to $\mathbf{R}$-linear independence of $(\log|\sigma_1(u)|, \log|\sigma_2(u)|, \log|\sigma_3(u)|)$ and $(\log|\sigma_1(v)|, \log|\sigma_2(v)|, \log|\sigma_3(v)|)$.*

Proof. We will prove multiplicative *dependence* in $\mathcal{O}^\times$ is equivalent to linear *dependence* of the corresponding vectors in $\mathbf{R}^3$.

Set $\mathbf{u} = (\log|\sigma_1(u)|, \log|\sigma_2(u)|, \log|\sigma_3(u)|)$ and $\mathbf{v} = (\log|\sigma_1(v)|, \log|\sigma_2(v)|, \log|\sigma_3(v)|)$. If u or v is ± 1 then $\mathbf{u}$ or $\mathbf{v}$ is $\mathbf{0}$, so we have multiplicative dependence of units and linear dependence of vectors. Now we may assume u and v are not ± 1.

If u and v are multiplicatively dependent, then $u^a v^b = 1$ for integers a and b that are not both 0. Feeding both sides of the equation into (5.1), we get the $\mathbf{Z}$-linear relation $a\mathbf{u} + b\mathbf{v} = \mathbf{0}$, so $\mathbf{u}$ and $\mathbf{v}$ are $\mathbf{R}$-linearly dependent.

Now assume $\mathbf{u}$ and $\mathbf{v}$ are $\mathbf{R}$-linearly dependent. Since neither vector is $\mathbf{0}$, $\mathbf{v} = c\mathbf{u}$ for some $c \in \mathbf{R}^\times$. We will show c is in fact *rational*. Then $c = m/n$ for nonzero integers m and n, which means $n\mathbf{v} = m\mathbf{u}$, so $u^m = \pm v^n$ and thus $u^{2m}v^{-2n} = 1$: u and v are multiplicatively dependent. The rationality of c is subtle: $\mathbf{R}$-linear dependence of vectors does not normally imply $\mathbf{Q}$-linear dependence. What makes this happen for $\mathbf{u}$ and $\mathbf{v}$ is that the image of $\mathcal{O}^\times$ in H is a discrete subgroup and this image contains $\mathbf{u}$ and $\mathbf{v}$.

Since the image of $\mathcal{O}^\times$ in the hyperplane H is a discrete subgroup, $\mathbf{Z}\mathbf{u}+\mathbf{Z}\mathbf{v}$ is a discrete subgroup of H (subgroups of discrete groups are discrete). Writing $\mathbf{v}$ as $c\mathbf{u}$,

$$\mathbf{Z}\mathbf{u}+\mathbf{Z}\mathbf{v} = \mathbf{Z}\mathbf{u}+\mathbf{Z}c\mathbf{u} = (\mathbf{Z}+\mathbf{Z}c)\mathbf{u}.$$

This is a subgroup of the linear subspace $\mathbf{R}\mathbf{u}$ in H. A difference between rational and irrational c is that $\mathbf{Z}+\mathbf{Z}c$ is discrete in $\mathbf{R}$ when $c \in \mathbf{Q}$ and it is dense in $\mathbf{R}$ if $c \notin \mathbf{Q}$. (Explicitly, if $c = m/n$ then $\mathbf{Z}+\mathbf{Z}c = \frac{1}{n}(\mathbf{Z}n+\mathbf{Z}m) = \mathbf{Z}(d/n)$ where $d = \gcd(m,n)$.) So if c is irrational, $(\mathbf{Z}+\mathbf{Z}c)\mathbf{u}$ has infinitely many elements on the segment from $\mathbf{0}$ to $\mathbf{u}$, and that contradicts the discreteness of $(\mathbf{Z}+\mathbf{Z}c)\mathbf{u}$ in H. Hence c is rational and we're done. □

Example 5.2. Let α be a root of T^3-3T-1, so $\alpha+1$ is a root of $(T-1)^3-3(T-1)-1 = T^3-3T^2+1$: they are both units in $\mathbf{Z}[\alpha]$. We met these units in Example 2.6. The real roots of T^3-3T-1 are approximately -1.532, $-.3472$, and 1.879. That makes the vectors in $\mathbf{R}^3$ associated to α and $\alpha+1$ approximately

$$(\log(1.532), \log(.3472), \log(1.879)) \approx (.42, -1.05, .63)$$

and

$$(\log(.532), \log(.6527), \log(2.879)) \approx (-.63, -.42, 1.05).$$

These vectors are linearly independent just from comparing the signs of the coordinates in each vector. Therefore α and $\alpha+1$ are multiplicatively independent units.

The linear independence of two vectors (x,y,z) and (x',y',z') in $\mathbf{R}^3$ is equivalent to the nonvanishing of the determinant of some 2×2 submatrix of

$$\begin{pmatrix} x & y & z \\ x' & y' & z' \end{pmatrix}. \tag{5.2}$$

When the two rows lie in the hyperplane of vectors in $\mathbf{R}^3$ with coordinate sum 0, all three 2×2 determinants in (5.2) are *equal up to sign*. For example,

$$xz'-zx' = x(-x'-y')+(x+y)x' = -xy'+yx' = -(xy'-yx').$$

Similarly, $yz'-zy' = xy'-yx'$. Therefore the absolute value of the determinants of all the 2×2 submatrices in (5.2) are equal.

Definition 5.3. The *regulator* of two units u and v in $\mathcal{O}$ is the absolute value of any 2×2 determinant in (5.2) where the rows are the vectors associated u and v. This number is denoted $\mathrm{Reg}(u,v)$.

The value of $\mathrm{Reg}(u,v)$ is independent of the ordering of the units since we are using the absolute value of determinants. In terms of regulators, Theorem 5.1 says u and v are multiplicatively independent if and only if $\mathrm{Reg}(u,v) \neq 0$.

Remark 5.4. The two rows in (5.2) span a parallelogram in H with area $\sqrt{3}|xy'-yx'|$. That gives $\mathrm{Reg}(u,v)$ a geometric meaning: it's the area of the parallelogram spanned by the vectors in H associated to u and v, up to the scaling factor $\sqrt{3}$.

Example 5.5. Let α be a root of T^3-3T-1. By Example 2.6, α and $\alpha+1$ are units in $\mathbf{Z}[\alpha]$. Writing the real roots of T^3-3T-1 as $\sigma_1(\alpha) \approx -1.532$, $\sigma_2(\alpha) \approx -.3472$, and $\sigma_3(\alpha) \approx 1.879$,

$$\mathrm{Reg}(\alpha, \alpha+1) = \left|\det \begin{pmatrix} \log|\sigma_1(\alpha)| & \log|\sigma_2(\alpha)| \\ \log|\sigma_1(\alpha)+1| & \log|\sigma_2(\alpha)+1| \end{pmatrix}\right| \approx .8492 \neq 0.$$

This is a second proof (after Example 5.2) that α and $\alpha+1$ are independent units.

We have shown how to decide if two units in $\mathcal{O}$ are multiplicatively independent. Now we develop a method of deciding if a pair of independent units in $\mathcal{O}^\times$ is fundamental.

Theorem 5.6. *Let $\mathcal{O}$ be an order in a totally real cubic field and ε_1 and ε_2 be fundamental units of $\mathcal{O}$. For a pair of units u_1 and u_2 in $\mathcal{O}^\times$, write $u_1 = \pm\varepsilon_1^a\varepsilon_2^b$ and $u_2 = \pm\varepsilon_1^c\varepsilon_2^d$ for some choice of signs. Then $\mathrm{Reg}(u_1, u_2) = |ad - bc|\,\mathrm{Reg}(\varepsilon_1, \varepsilon_2)$, and if u_1 and u_2 are independent units then $|ad - bc| = [\mathcal{O}^\times : \langle -1, u_1, u_2\rangle]$.*

Proof. Let $\mathbf{v}_1 = (x, y, z)$ and $\mathbf{v}_2 = (x', y', z')$ be the vectors in H associated to ε_1 and ε_2, and $\mathbf{u}_1$ and $\mathbf{u}_2$ be the vectors in H associated to u_1 and u_2, so $\mathbf{u}_1 = a\mathbf{v}_1 + b\mathbf{v}_2$ and $\mathbf{u}_2 = c\mathbf{v}_1 + d\mathbf{v}_2$ in $\mathbf{R}^3$. Then we have an equation of 2×3 matrices:

$$\begin{pmatrix}\mathbf{u}_1\\ \mathbf{u}_2\end{pmatrix} = \begin{pmatrix}a\mathbf{v}_1 + b\mathbf{v}_2\\ c\mathbf{v}_1 + d\mathbf{v}_2\end{pmatrix} = \begin{pmatrix}ax + bx' & ay + by' & az + bz'\\ cx + dx' & cy + dy' & cz + dz'\end{pmatrix}$$

The first 2×2 determinant is $(ad - bc)(xy' - x'y)$, so $\mathrm{Reg}(u_1, u_2) = |ad - bc|\,\mathrm{Reg}(\varepsilon_1, \varepsilon_2)$.

To show $|ad - bc| = [\mathcal{O}^\times : \langle -1, u_1, u_2\rangle]$, we will compare quotient groups $\mathcal{O}^\times/\langle -1, u_1, u_2\rangle$ and $(\mathbf{Z}\mathbf{v}_1 + \mathbf{Z}\mathbf{v}_2)/(\mathbf{Z}\mathbf{u}_1 + \mathbf{Z}\mathbf{u}_2)$. The homomorphism (5.1) gives an isomorphism $\mathcal{O}^\times/\{\pm 1\} \to \mathbf{Z}\mathbf{v}_1 + \mathbf{Z}\mathbf{v}_2$ that identifies the subgroup $\langle -1, u_1, u_2\rangle/\{\pm 1\}$ with $\mathbf{Z}\mathbf{u}_1 + \mathbf{Z}\mathbf{u}_2$. Therefore we have a group isomorphism

$$(\mathcal{O}^\times/\{\pm 1\})/(\langle -1, u_1, u_2\rangle/\{\pm 1\}) \cong (\mathbf{Z}\mathbf{v}_1 + \mathbf{Z}\mathbf{v}_2)/(\mathbf{Z}\mathbf{u}_1 + \mathbf{Z}\mathbf{u}_2).$$

The index $[\mathbf{Z}\mathbf{v}_1 + \mathbf{Z}\mathbf{v}_2 : \mathbf{Z}\mathbf{u}_1 + \mathbf{Z}\mathbf{u}_2]$ is the absolute value of the determinant of the matrix expressing $\mathbf{u}_1$ and $\mathbf{u}_2$ in terms of $\mathbf{v}_1$ and $\mathbf{v}_2$.[13] Therefore from $\left(\begin{smallmatrix}\mathbf{u}_1\\ \mathbf{u}_2\end{smallmatrix}\right) = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\left(\begin{smallmatrix}\mathbf{v}_1\\ \mathbf{v}_2\end{smallmatrix}\right)$, the index is $|ab - bc|$, so

$$|ad - bc| = [\mathcal{O}^\times/\{\pm 1\} : \langle -1, u_1, u_2\rangle/\{\pm 1\}] = [\mathcal{O}^\times : \langle -1, u_1, u_2\rangle]. \qquad \square$$

Rewriting the conclusion of Theorem 5.6 as $\mathrm{Reg}(u_1, u_2) = [\mathcal{O}^\times : \langle -1, u_1, u_2\rangle]\,\mathrm{Reg}(\varepsilon_1, \varepsilon_2)$ makes it resemble the discriminant-index formula $\mathrm{disc}(A) = [\mathcal{O}_K : A]^2\,\mathrm{disc}(\mathcal{O}_K)$ where A is an order in $\mathcal{O}_K$. While discriminants are integers, regulators are expected to be transcendental (when they are nonzero). That doesn't prevent their ratios from being integers.

Corollary 5.7. *In the notation of Theorem 5.6, all pairs of fundamental units in $\mathcal{O}$ have the same regulator.*

Proof. If u_1 and u_2 are fundamental units then $|ad - bc| = 1$, so $\mathrm{Reg}(u_1, u_2) = \mathrm{Reg}(\varepsilon_1, \varepsilon_2)$. $\square$

This corollary is analogous to all $\mathbf{Z}$-bases of $\mathcal{O}$ having the same discriminant, which is therefore called the discriminant of $\mathcal{O}$. For similar reasons, we can now define $\mathrm{Reg}(\mathcal{O})$ to be the regulator of any pair of fundamental units of $\mathcal{O}$. Also we set $\mathrm{Reg}(K)$ to be $\mathrm{Reg}(\mathcal{O}_K)$, just as $\mathrm{disc}(K)$ is defined to be $\mathrm{disc}(\mathcal{O}_K)$.

For a pair of independent units u_1 and u_2 in $\mathcal{O}$ to be fundamental units means the index $[\mathcal{O}^\times : \langle -1, u_1, u_2\rangle]$ is 1, or equivalently $\mathrm{Reg}(u_1, u_2)/\mathrm{Reg}(\varepsilon_1, \varepsilon_2) = 1$. Since that regulator ratio is in $\mathbf{Z}^+$, it is 1 as soon as we know it is less than 2:

$$\mathcal{O}^\times = \langle -1, u_1, u_2\rangle \iff \frac{\mathrm{Reg}(u_1, u_2)}{\mathrm{Reg}(\varepsilon_1, \varepsilon_2)} < 2.$$

Using the inequality on the right to prove u_1 and u_2 are fundamental units might seem hopeless if we don't already know a pair of fundamental units ε_1 and ε_2. To make that

[13] See Theorem 5.19 in https://kconrad.math.uconn.edu/blurbs/linmultialg/modulesoverPID.pdf.

inequality practical, we want an *upper bound* on the regulator ratio by using a *lower bound* on $\mathrm{Reg}(\varepsilon_1, \varepsilon_2)$ that doesn't use fundamental units. Here is such a lower bound, due to Cusick [3, Theorem 1]. You might want to skip the proof first and read later examples.

Theorem 5.8. *Let K be a totally real cubic field. If an order $\mathcal{O}$ in K has discriminant D and regulator R, then*

$$R \geq \frac{1}{16}(\log(D/4))^2.$$

Proof. There are 3 real embeddings of K. Identify K with one of them, so $K \subset \mathbf{R}$. Write the other two real embeddings of K as $\alpha \mapsto \alpha'$ and $\alpha \mapsto \alpha''$. Pick a unit $u \in \mathcal{O}^\times$ with $u \neq \pm 1$. Label the $\mathbf{Q}$-conjugates u, u', u'' as u_0, u_1, u_2 so that $\boxed{|u_0| \geq |u_1| \geq |u_2|}$.

Since $u \in \mathcal{O}^\times - \{\pm 1\}$ we have $u \notin \mathbf{Q}$, so $\mathbf{Z}[u]$ has finite index in $\mathcal{O}$ and

$$\mathrm{disc}(\mathbf{Z}[u]) = [\mathcal{O} : \mathbf{Z}[u]]^2 \,\mathrm{disc}(\mathcal{O}) = [\mathcal{O} : \mathbf{Z}[u]]^2 D \geq D. \tag{5.3}$$

Since $\mathrm{disc}(\mathbf{Z}[u])$ equals the discriminant of the minimal polynomial of u over $\mathbf{Q}$,

$$\mathrm{disc}(\mathbf{Z}[u]) = (u-u')^2(u-u'')^2(u'-u'')^2 = \left(1 - \frac{u_1}{u_0}\right)^2 \left(1 - \frac{u_2}{u_0}\right)^2 \left(1 - \frac{u_2}{u_1}\right)^2 u_0^4 u_1^2, \tag{5.4}$$

where $|u_1/u_0| \leq 1$ and $|u_2/u_1| \leq 1$ by our convention on the ordering of $|u_0|$, $|u_1|$, and $|u_2|$. Set $v = u_1/u_0$ and $w = u_2/u_1$, so $\mathrm{disc}(\mathbf{Z}[u]) = (1-v)^2(1-vw)^2(1-w)^2 u_0^4 u_1^2$. From $|v| \leq 1$ and $|w| \leq 1$, $0 \leq (1-v)(1-w)(1-vw) \leq 2$ by calculus. Feeding this and (5.4) into (5.3),

$$0 < D \leq \mathrm{disc}(\mathbf{Z}[u]) \leq 4u_0^4 u_1^2.$$

Dividing through by 4 and taking absolute values and then logarithms,

$$\log\left(\frac{D}{4}\right) \leq 4\log|u_0| + 2\log|u_1|.$$

Set $\boxed{y_0 = \log|u_0|, y_1 = \log|u_1|, y_2 = \log|u_2|}$, so $y_0 \geq y_1 \geq y_2$ and $y_0 + y_1 + y_2 = 0$. Therefore

$$\begin{aligned}
\log\left(\frac{D}{4}\right) &\leq 4y_0 + 2y_1 \\
&= 2(2y_0 + y_1) = 2(-y_1 - 2y_2) \\
&= 2(\lambda y_0 + (\lambda - 1)y_1 + (\lambda - 2)y_2) \quad \text{for all } \lambda \\
&\leq 2\sqrt{\lambda^2 + (\lambda-1)^2 + (\lambda-2)^2}\sqrt{y_0^2 + y_1^2 + y_2^2} \quad \text{by Cauchy}-\text{Schwarz} \\
&= 2\sqrt{3\lambda^2 - 6\lambda + 5}\sqrt{y_0^2 + y_1^2 + y_2^2} \\
&= 2\sqrt{3\lambda^2 - 6\lambda + 5}\sqrt{(\log|u_0|)^2 + (\log|u_1|)^2 + (\log|u_2|)^2} \\
&= 2\sqrt{3\lambda^2 - 6\lambda + 5}\sqrt{(\log|u|)^2 + (\log|u'|)^2 + (\log|u''|)^2}.
\end{aligned}$$

The second square root doesn't depend on λ, so to optimize this inequality use the minimal value of $3\lambda^2 - 6\lambda + 5$, which is 2 (at $\lambda = 1$):

$$\log\left(\frac{D}{4}\right) \leq 2\sqrt{2}\sqrt{(\log|u|)^2 + (\log|u'|)^2 + (\log|u''|)^2}. \tag{5.5}$$

Let ε_1 and ε_2 be a pair of fundamental units of $\mathcal{O}$. We will express the right side of (5.5) in terms of these units and then bound it above using $R = \mathrm{Reg}(\varepsilon_1, \varepsilon_2)$.

Since $|uu'u''| = 1$, on the right side of (5.5)

$$\begin{aligned}(\log|u|)^2 + (\log|u'|)^2 + (\log|u''|)^2 &= (\log|u|)^2 + (\log|u'|)^2 + (\log|u| + \log|u'|)^2 \\ &= 2(\log|u|)^2 + 2(\log|u|)(\log|u'|) + 2(\log|u'|)^2. \end{aligned} \tag{5.6}$$

We can write $u = \pm\varepsilon_1^x\varepsilon_2^y$ for some integers x and y that are not both 0. For another real embedding of K, $u' = \pm(\varepsilon_1')^x(\varepsilon_2')^y$ with the same exponents. Set $L_1 = \log|\varepsilon_1|$, $L_2 = \log|\varepsilon_2|$, $M_1 = \log|\varepsilon_1'|$, and $M_2 = \log|\varepsilon_2'|$, so $\log|u| = xL_1 + yL_2$ and $\log|u'| = xM_1 + yM_2$. In (5.6) some algebra shows

$$2(\log|u|)^2 + 2(\log|u|)(\log|u'|) + 2(\log|u'|)^2 = Ax^2 + 2Bxy + Cy^2,$$

where $A = 2(L_1^2 + L_1M_1 + M_1^2)$, $B = 2L_1L_2 + L_1M_2 + L_2M_1 + 2M_1M_2$, and $C = 2(L_2^2 + L_2M_2 + M_2^2)$, so (5.5) becomes

$$\log\left(\frac{D}{4}\right) \leq 2\sqrt{2}\sqrt{Ax^2 + 2Bxy + Cy^2}. \tag{5.7}$$

The values of $Ax^2 + 2Bxy + Cy^2$ for $(x, y) \in \mathbf{Z}^2 - \{(0,0)\}$ are positive. In fact these values for $(x, y) \in \mathbf{R}^2 - \{(0,0)\}$ are all positive since the discriminant $(2B)^2 - 4AC = 4(B^2 - AC)$ is negative: check by tedious algebra that $AC - B^2 = 3(L_1M_2 - L_2M_1)^2$, and $L_1M_2 - L_2M_1$ is nonzero since $L_1M_2 - L_2M_1 = \left|\begin{smallmatrix} L_1 & M_1 \\ L_2 & M_2 \end{smallmatrix}\right| = \left|\begin{smallmatrix} \log|\varepsilon_1| & \log|\varepsilon_1'| \\ \log|\varepsilon_2| & \log|\varepsilon_2'| \end{smallmatrix}\right| = \pm R \neq 0$, so $AC - B^2 > 0$.

We derived (5.7) for all integers x and y that are not both 0. Since $AC - B^2 > 0$, it can be shown (see Theorem A.1) that for some $x, y \in \mathbf{Z}$ that are not both 0, $Ax^2 + Bxy + Cy^2 \leq \sqrt{(4/3)(AC - B^2)} = \sqrt{(4/3)(3R^2)} = 2R$. Using that x and y in (5.7),

$$\log\left(\frac{D}{4}\right) \leq 2\sqrt{2}\sqrt{2R} = 4\sqrt{R},$$

so $R \geq (1/16)(\log(D/4))^2$. □

Corollary 5.9. *Let K be a totally real cubic field and $\mathcal{O}$ be an order in K with discriminant D and regulator R. If u_1 and u_2 are independent units in $\mathcal{O}$ such that*

$$\frac{16\,\mathrm{Reg}(u_1, u_2)}{(\log(D/4))^2} < m$$

then $[\mathcal{O}^\times : \langle -1, u_1, u_2\rangle] < m$. In particular, if $16\,\mathrm{Reg}(u_1, u_2)/(\log(D/4))^2 < 2$ then u_1 and u_2 are fundamental units of $\mathcal{O}$.

This is an analogue of Corollary 4.6 for totally real cubic fields.

Proof. We can bound the index $[\mathcal{O}^\times : \langle -1, u_1, u_2\rangle]$ above by m:

$$[\mathcal{O}^\times : \langle -1, u_1, u_2\rangle] = \frac{\mathrm{Reg}(u_1, u_2)}{R} \leq \frac{\mathrm{Reg}(u_1, u_2)}{(\log(D/4))^2/16} < m.$$ □

Example 5.10. Let $K = \mathbf{Q}(\alpha)$ where $\alpha^3 - 3\alpha - 1 = 0$. We have $\mathcal{O}_K = \mathbf{Z}[\alpha]$, $\mathrm{disc}(\mathcal{O}_K) = 81$, and α and $\alpha + 1$ are independent units in $\mathcal{O}_K$ with $\mathrm{Reg}(\alpha, \alpha + 1) \approx .8492$ by Examples 2.6 and 5.5. Since

$$\frac{16\,\mathrm{Reg}(u_1, u_2)}{(\log(81/4))^2} \approx 1.5 < 2,$$

α and $\alpha + 1$ are fundamental units of $\mathcal{O}_K$ by Corollary 5.9.

Example 5.11. Let $K = \mathbf{Q}(\alpha)$, where $\alpha^3 - 4\alpha - 1 = 0$. The polynomial $T^3 - 4T - 1$ has discriminant 229, a prime, so $\mathcal{O}_K = \mathbf{Z}[\alpha]$. There are three real roots of the polynomial, so $\mathcal{O}_K^\times$ has rank 2. Obviously α is a unit in $\mathcal{O}_K$. Another unit is $\alpha + 2$, since it is a root of

$$(T-2)^3 - 4(T-2) - 1 = T^3 - 6T^2 + 8T - 1.$$

We'll show α and $\alpha + 2$ are fundamental units of $\mathcal{O}_K$.

The real roots of $T^3 - 4T - 1$ are $\sigma_1(\alpha) \approx -1.8608$, $\sigma_2(\alpha) \approx -.2541$, and $\sigma_3(\alpha) \approx 2.1149$, so

$$\mathrm{Reg}(\alpha, \alpha+2) = \left|\det \begin{pmatrix} \log|\sigma_1(\alpha)| & \log|\sigma_2(\alpha)| \\ \log|\sigma_1(\alpha)+2| & \log|\sigma_2(\alpha)+2| \end{pmatrix}\right| \approx 2.3554 \neq 0.$$

Since $\mathrm{disc}(\mathcal{O}_K) = 229$, we have

$$\frac{16\,\mathrm{Reg}(\alpha, \alpha+2)}{(\log(D/4))^2} \approx 2.3 < 3,$$

so $[\mathcal{O}_K^\times : \langle -1, \alpha, \alpha+2\rangle] \leq 2$. We'll show by contradiction the index is not 2, so it is 1.

Let's look at $\mathcal{O}_K^\times/\{\pm 1\} \cong \mathbf{Z}^2$ and its subgroup $\langle \pm\alpha, \pm(\alpha+2)\rangle/\{\pm 1\}$ of index at most 2. The subgroups of $\mathbf{Z}^2$ with index 2 lie between $\mathbf{Z}^2$ and $(2\mathbf{Z})^2$. Since $\mathbf{Z}^2/(2\mathbf{Z})^2 \cong (\mathbf{Z}/2\mathbf{Z})^2$ has three subgroups of index 2, there are three subgroups of $\mathbf{Z}^2$ with index 2: $\langle (2,0), (0,1)\rangle$, $\langle (0,2), (1,0)\rangle$, and $\langle (1,1), (2,0)\rangle = \langle (1,1), (0,2)\rangle$. Using the basis $\{(1,0), (0,1)\}$ of $\mathbf{Z}^2$, each subgroup of index 2 in $\mathbf{Z}^2$ has the double of $(1,0)$ or $(0,1)$ as a member of some basis. Translating this into $\mathcal{O}_K^\times/\{\pm 1\}$, if its subgroup $\boxed{U := \langle \pm\alpha, \pm(\alpha+2)\rangle/\{\pm 1\}}$ has index 2 then the square of some fundamental unit of $\mathcal{O}_K$ is a member of some (multiplicative) basis of U. Which elements of U can be in a basis of U, and can it be a square in $\mathcal{O}_K^\times$?

In $\mathbf{Z}^2$, the vectors $\binom{a}{b}$ that can be part of a basis must be primitive (have relatively prime coordinates). Therefore an element of U that is part of a (multiplicative) basis of U must be $\pm\alpha^a(\alpha+2)^b$ where $\gcd(a,b) = 1$. Thus a or b must be odd, so if $\pm\alpha^a(\alpha+2)^b$ is a square in $\mathcal{O}_K^\times$ then $\pm\alpha$ or $\pm(\alpha+2)$ or $\pm\alpha(\alpha+2)$ is a square in $\mathcal{O}_K^\times$ (corresponding to odd a and even b, even a and odd b, and odd a and b, respectively). We're going to show none of those three units is a square in $\mathcal{O}_K^\times$ by finding prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ such that those three units are not squares mod $\mathfrak{p}$. To handle the ambiguity of the $\pm$ signs, we'll use $\mathfrak{p}$ whose norm is 1 mod 4 which makes -1 a square mod $\mathfrak{p}$.

Since $\mathcal{O}_K = \mathbf{Z}[\alpha] \cong \mathbf{Z}[T]/(T^3 - 4T - 1)$, we'll factor $p = 5, 13, 17, \ldots$ to find suitable $\mathfrak{p}$. From Table 3 below, there is a prime $\mathfrak{p}_{13}$ of norm 13 and $\mathfrak{p}_{29}$ of norm 29, with $\alpha \equiv 5 \bmod \mathfrak{p}_{13}$ and $\alpha \equiv 16 \bmod \mathfrak{p}_{29}$.

p	$T^3 - 4T - 1 \bmod p$	(p)
5	irred.	(5)
13	$(T-5)(T^2+5T+8)$	$\mathfrak{p}_{13}\mathfrak{p}_{169}$
17	irred.	(17)
29	$(T-16)(T^2+16T+20)$	$\mathfrak{p}_{29}\mathfrak{p}_{29^2}$

TABLE 3. Factoring primes in $\mathcal{O}_K$.

In $\mathcal{O}_K/\mathfrak{p}_{13} \cong \mathbf{Z}/13\mathbf{Z}$, $\alpha \equiv 5$ and $\alpha + 2 \equiv 7$. Since 5 and 7 are not squares in $\mathbf{Z}/13\mathbf{Z}$ while -1 is, neither $\pm\alpha$ nor $\pm(\alpha+2)$ are squares in $\mathcal{O}_K^\times$. Since $5 \cdot 7 = 35 \equiv 9 \bmod 13$ is a square, this doesn't show $\pm\alpha(\alpha+2)$ isn't a unit square. To show that, we use the prime $\mathfrak{p}_{29}$:

$\pm\alpha(\alpha+2) \equiv \pm 16(18) \equiv \pm(4\cdot 3)^2 \cdot 2 \bmod \mathfrak{p}_{29}$. In $\mathbf{Z}/29\mathbf{Z}$, ± 2 are not squares, so $\pm\alpha(\alpha+2)$ is not a square in $\mathcal{O}_K^\times$.

We have proved the index $[\mathcal{O}_K^\times/\{\pm 1\} : U]$, which is at most 2, is not 2 and thus it is 1. Therefore $\mathcal{O}_K^\times/\{\pm 1\} = U$, so α and $\alpha+2$ are fundamental units of $\mathcal{O}_K$.

Our next theorem gives us an infinite family of examples of fundamental units in totally real cubic orders.

Theorem 5.12. *Fix an integer a. The polynomial $f_a(T) = T^3 - aT^2 - (a+3)T - 1$ is irreducible over $\mathbf{Q}$, and if α is a root of $f_a(T)$ then $\mathbf{Z}[\alpha]^\times = \pm\alpha^{\mathbf{Z}}(\alpha+1)^{\mathbf{Z}}$.*

The fields $\mathbf{Q}(\alpha)$ where $f_a(\alpha) = 0$ are called the "simplest cubic fields" (terminology of Dan Shanks [13]). The ring $\mathbf{Z}[\alpha]$ is often, but not always, the ring of integers of $\mathbf{Q}(\alpha)$.[14]

Theorem 5.12 is due to Thomas [15, Theorem 3.10] (a special case was pointed out earlier by Shanks [13, p. 1138]) using methods different from our approach based on Corollary 5.9.

Proof. By the rational roots theorem, a rational root of $f_a(T)$ must be ± 1, and $f_a(1) = -2a - 3 \neq 0$ and $f_a(-1) = 1 \neq 0$, so $f_a(T)$ is irreducible over $\mathbf{Q}$.

Let $K_a = \mathbf{Q}(\alpha)$. Clearly α is a unit in $\mathbf{Z}[\alpha]$. Since $\alpha+1$ is a root of

$$f_a(T-1) = T^3 - (a+3)T^2 + aT + 1,$$

$\alpha+1$ is also a unit in $\mathbf{Z}[\alpha]$. Check that $\boxed{\mathrm{disc}(f_a) = (a^2+3a+9)^2}$, a perfect square, so $K_a/\mathbf{Q}$ is Galois. The roots of $f_a(T)$ are α, $-1/(\alpha+1)$, and $-1/(-1/(\alpha+1)+1) = -1-1/\alpha$, which are all in $\mathbf{Z}[\alpha]$ even if this is not the full ring of integers of K_a.

Step 1: The units α and $\alpha+1$ are multiplicatively independent.

We have

$$\begin{aligned}\mathrm{Reg}(\alpha, \alpha+1) &= \det\begin{pmatrix} \log|\alpha| & \log|-1/(\alpha+1)| \\ \log|\alpha+1| & \log|-1/(\alpha+1)+1|\end{pmatrix} \\ &= \det\begin{pmatrix} \log|\alpha| & -\log|\alpha+1| \\ \log|\alpha+1| & \log|\alpha/(\alpha+1)|\end{pmatrix} \\ &= (\log|\alpha|)^2 - \log|\alpha|\log|\alpha+1| + (\log|\alpha+1|)^2.\end{aligned}$$

For real x and y, $x^2 - xy + y^2 > 0$ unless $x = y = 0$. So from $\log|\alpha| \neq 0$, $\mathrm{Reg}(\alpha, \alpha+1) \neq 0$.

Step 2: $\mathbf{Z}[\alpha]$ is invariant under $\mathrm{Gal}(K_a/\mathbf{Q})$.

Let $\sigma \in \mathrm{Gal}(K_a/\mathbf{Q})$ be determined by $\sigma(\alpha) = -1/(\alpha+1) \in \mathbf{Z}[\alpha]$, so $\mathrm{Gal}(K_a/\mathbf{Q}) = \{1, \sigma, \sigma^2\}$ and $\sigma(\mathbf{Z}[\alpha]) \subset \mathbf{Z}[\alpha]$. Applying σ to this containment twice, $\mathbf{Z}[\alpha] \subset \sigma(\sigma(\mathbf{Z}[\alpha])) \subset \sigma(\mathbf{Z}[\alpha])$. Therefore $\sigma(\mathbf{Z}[\alpha]) = \mathbf{Z}[\alpha]$, so also $\sigma^2(\mathbf{Z}[\alpha]) = \mathbf{Z}[\alpha]$.

Step 3: The group $\langle -1, \alpha, \alpha+1\rangle$ is invariant under $\mathrm{Gal}(K_a/\mathbf{Q})$.

It suffices to show this group is preserved by σ from Step 2:

$$\sigma\langle -1, \alpha, \alpha+1\rangle = \left\langle -1, -\frac{1}{\alpha+1}, -\frac{1}{\alpha+1}+1\right\rangle = \left\langle -1, \alpha+1, \frac{\alpha}{\alpha+1}\right\rangle = \langle -1, \alpha, \alpha+1\rangle.$$

Step 4: Reduce to the case $a \geq -1$.

Check $f_{-a-3}(T) = -f_a(-T-1)$, so $K_a = K_{-a-3}$. One root of $f_{-a-3}(T)$ is $\beta := -\alpha - 1 = -(\alpha+1)$, and $\beta + 1 = -\alpha$. Therefore $\mathbf{Z}[\beta] = \mathbf{Z}[\alpha]$ and

$$\langle -1, \beta, \beta+1\rangle = \langle -1, -(\alpha+1), -\alpha\rangle = \langle -1, \alpha, \alpha+1\rangle,$$

[14] For $0 \leq a \leq 10$, the ring of integers of $\mathbf{Q}(\alpha)$ is $\mathbf{Z}[\alpha]$ except when $a = 3$ and 5.

so if we prove the theorem for an integer a then it is also true with $-a-3$ in place of a. The involution $a \leftrightarrow -a-3$ on $\mathbf{R}$ fixes $-3/2$ and exchanges integers greater than and less than $-3/2 = -1.5$, so we may assume $a \geq -1$.

Step 5: Prove the theorem when $a \geq -1$.

First we'll treat $a = -1$. Then $\mathrm{disc}(\mathbf{Z}[\alpha]) = 49$ and $\mathrm{Reg}(\alpha, \alpha+1) \approx .5254$ by Step 1, so

$$\frac{16\,\mathrm{Reg}(\alpha, \alpha+1)}{(\log(\mathrm{disc}(\mathbf{Z}[\alpha])/4))^2} \approx \frac{16(.5254)}{(\log(49/4))^2} \approx 1.3 < 2,$$

so α and $\alpha+1$ are fundamental units of $\mathbf{Z}[\alpha]$ by Corollary 5.9.

We may now assume $a \geq 0$.

The roots of $f_a(T)$ are in the disjoint intervals $(-2,-1)$, $(-1,0)$, and $(a+1, a+2)$ when $a \geq 0$ since f_a has opposite signs at the endpoints: $f_a(-2) = -(2a+3) < 0$, $f_a(-1) = 1 > 0$, $f_a(0) = -1 < 0$, $f_a(a+1) = -(2a+3) < 0$, and $f_a(a+2) = a^2+3a+1 = (a+1)^2 + a > 0$ (that would be incorrect for $a = -1$).

By Steps 2 and 3 we can let α be the largest real root of $f_a(T)$, so $a+1 < \alpha < a+2$. Using the regulator formula in Step 1,

$$\begin{aligned}
\frac{16\,\mathrm{Reg}(\alpha, \alpha+1)}{(\log(\mathrm{disc}(\mathbf{Z}[\alpha])/4))^2} &= \frac{16\,\mathrm{Reg}(\alpha, \alpha+1)}{(\log((a^2+3a+9)^2/2^2))^2} \\
&= \frac{16((\log|\alpha|)^2 - \log|\alpha|\log|\alpha+1| + (\log|\alpha+1|)^2)}{4(\log((a^2+3a+9)/2))^2} \\
&= \frac{4((\log\alpha)(\log\alpha - \log(\alpha+1)) + (\log(\alpha+1))^2)}{(\log((a^2+3a+9)/2))^2}.
\end{aligned}$$

Since $\log\alpha < \log(\alpha+1)$ and $\alpha < a+2$,

$$\frac{16\,\mathrm{Reg}(\alpha, \alpha+1)}{(\log(\mathrm{disc}(\mathbf{Z}[\alpha])/4))^2} < \frac{4(\log(\alpha+1))^2}{(\log((a^2+3a+9)/2))^2} < \frac{4(\log(a+3))^2}{(\log((a^2+3a+9)/2))^2}. \tag{5.8}$$

For large a the right side of (5.8) is asymptotic to $4(\log a)^2/(\log(a^2))^2 = 4(\log a)^2/4(\log a)^2 = 1$, so it is less than 2 for large a. That proves the theorem for large a. We will now check more carefully if the right side of (5.8) is less than 2 for all $a \geq 0$.

Since

$$\begin{aligned}
\frac{4(\log(a+3))^2}{(\log((a^2+3a+9)/2))^2} < 2 &\iff \frac{\log(a+3)}{\log((a^2+3a+9)/2)} < \frac{1}{\sqrt{2}} \\
&\iff \frac{a^2+3a+9}{2} > (a+3)^{\sqrt{2}},
\end{aligned}$$

we consider where $F(x) := (x^2+3x+9)/2 - (x+3)^{\sqrt{2}}$ is positive. Its graph looks positive and increasing for $x \geq 2.5$. Numerically, $F(3) = 13.5 - 6^{\sqrt{2}} \approx .897 > 0$. With calculus we'll show $F(x)$ is increasing for $x \geq 3$, so $F(x) > 0$ for all $x \geq 3$:

$$\begin{aligned}
F'(x) &= x + \frac{3}{2} - \sqrt{2}(x+3)^{\sqrt{2}-1} \\
&= \frac{x}{2} + \frac{x+3}{2} - \sqrt{2}(x+3)^{\sqrt{2}-1} \\
&= \frac{x}{2} + (x+3)^{\sqrt{2}-1}\left(\frac{(x+3)^{2-\sqrt{2}}}{2} - \sqrt{2}\right),
\end{aligned}$$

which is positive for $x \geq 3$ if $(1/2)(x+3)^{2-\sqrt{2}} - \sqrt{2} > 0$, which is equivalent to $x > (2\sqrt{2})^{1/(2-\sqrt{2})} - 3 \approx 2.899$, so $F'(x) > 0$ for $x \geq 3$. We have proved the theorem for $a \geq 3$.

For $a = 0$, 1, and 2, we return to (5.8) and focus on the middle term to show

$$\frac{4(\log(\alpha+1))^2}{(\log((a^2+3a+9)/2))^2} < 2. \tag{5.9}$$

where α is the largest root of $f_a(T)$. By Table 4 below, (5.9) holds for $a = 0$, 1, and 2.

a	α	Ratio
0	1.879	1.97
1	2.651	1.91
2	3.507	1.78

TABLE 4. Left side of (5.9) for $a = 0, 1, 2$.

That completes the proof of the theorem. □

Cusick [3, Sect. 3] observed that the family of rings in the previous theorem shows the constant 16 in the lower bound of Theorem 5.8 can't be made smaller, as follows.

Corollary 5.13. *Using the notation of Theorem 5.8, if $\mathcal{O} = \mathbf{Z}[\alpha]$ from Theorem 5.12 and $a \to \infty$ in $\mathbf{Z}^+$, then $R/(\log(D/4))^2 \to 1/16$.*

Proof. Let α be the largest root of $f_a(T)$. Since $a+1 < \alpha < a+2$ for $a \geq 0$, $\alpha \sim a$ as $a \to \infty$. As $a \to \infty$, check $R = \mathrm{Reg}(\alpha, \alpha+1) \sim (\log a)^2$ and $(\log(D/4))^2 \sim 4(\log(a^2))^2 \sim 16(\log a)^2$. □

This ends our treatment of rank 2 units groups in the cubic case.[15]

For a set of units $u_1, \ldots, u_r$ in a number field K ($r = r_1 + r_2 - 1$), its regulator is defined in the following way. Write the real and complex embeddings of K as $\sigma_1, \ldots, \sigma_{r_1+r_2}$ where for complex embeddings we include only one of each complex conjugate pair of complex embeddings. Consider the $r \times (r+1)$ matrix

$$\begin{pmatrix} N_1 \log|\sigma_1(u_1)| & \cdots & N_{r_1+r_2}\log|\sigma_{r_1+r_2}(u_1)| \\ \vdots & \ddots & \vdots \\ N_1 \log|\sigma_1(u_r)| & \cdots & N_{r_1+r_2}\log|\sigma_{r_1+r_2}(u_r)| \end{pmatrix} \tag{5.10}$$

where $N_j = 1$ if σ_j is a real embedding of K and $N_j = 2$ if σ_j is a complex (non-real) embedding of K. (If K is totally real then all N_j's are 1 and we don't notice them.) The purpose of including the factors N_j is that it makes the row sums all equal to 0: the ith row sum is $\log|\mathrm{N}_{K/\mathbf{Q}}(u_i)| = \log|\pm 1| = 0$. The matrix (5.10) does not depend on which embedding of K from a pair of conjugate complex embeddings σ or $\overline{\sigma}$ is used for some σ_j since $|\sigma(\alpha)| = |\overline{\sigma(\alpha)}|$ for $\alpha \in K^\times$.

Definition 5.14. The *regulator* $\mathrm{Reg}(u_1, \ldots, u_r)$ is the absolute value of the determinant of an $r \times r$ submatrix of (5.10).

[15] We do not discuss other rank 2 unit cases: quartic with $r_1 = 2$ (like $\mathbf{Q}(\sqrt[4]{2})$), quintic with $r_1 = 1$ (like $\mathbf{Q}(\sqrt[5]{2})$), and sextic with $r_1 = 0$ (like $\mathbf{Q}(\zeta_7)$).

Because all row sums equal 0, every $r \times r$ submatrix in (5.10) has the same determinant up to sign. That makes $\mathrm{Reg}(u_1, \ldots, u_r)$ well-defined and independent of the ordering of the units. The only time this definition makes no sense is when $r = 0$ (what's a 0×0 submatrix?), which only occurs if K is $\mathbf{Q}$ or imaginary quadratic. In that case the regulator is set to be 1.

Example 5.15. If K has unit rank 1 and u is a unit in K then $\mathrm{Reg}(u) = |\log |u||$. Note this is unaffected if we change the sign of u or replace u with $1/u$.

As in the totally real cubic case, $\mathrm{Reg}(u_1, \ldots, u_r) \neq 0$ if and only if $u_1, \ldots, u_r$ are multiplicatively independent, and if we have two sets of independent units $u_1, \ldots, u_r$ and $v_1, \ldots, v_r$ where $\langle \zeta, u_1, \ldots, u_r\rangle \subset \langle \zeta, v_1, \ldots, v_r\rangle$ for some root of unity ζ, then

$$\frac{\mathrm{Reg}(u_1, \ldots, u_r)}{\mathrm{Reg}(v_1, \ldots, v_r)} = [\langle \zeta, v_1, \ldots, v_r\rangle : \langle \zeta, u_1, \ldots, u_r\rangle].$$

In particular, two sets of r independent units in K that generate the same group with some roots of unity have equal regulators. That gives meaning to the next concept.

Definition 5.16. The *regulator* of an order $\mathcal{O}$ in K is the regulator of a set of fundamental units of $\mathcal{O}$ and it is denoted $\mathrm{Reg}(\mathcal{O})$.

Example 5.17. The regulator of $\mathbf{Z}[\sqrt{2}]$ is $\log(1 + \sqrt{2})$.

Example 5.18. By Example 4.7, $\mathrm{Reg}(\mathbf{Z}[\sqrt[3]{2}]) = \log(1 + \sqrt[3]{2} + \sqrt[4]{2})$.

Example 5.19. For a cubic order $\mathcal{O}$ with one real embedding, Artin's inequality $|\mathrm{disc}(\mathcal{O})| < 4v^3+24$ can be rewritten as $\log v > (1/3)\log((|D|-24))/4)$ where $D = \mathrm{disc}(\mathcal{O})$ and $|D| > 24$. (There's only one cubic order with $|D| \leq 24$: see Example 4.10.) Taking for v the fundamental unit of $\mathcal{O}$ that's greater than 1, $\mathrm{Reg}(\mathcal{O}) = \log v$, so

$$\mathrm{Reg}(\mathcal{O}) > \frac{1}{3}\log\left(\frac{|D| - 24}{4}\right), \tag{5.11}$$

which is analogous to Cusick's lower bound $R > (1/16)(\log(D/4))^2$ in Theorem 5.8. Remark 4.13 tells us the denominator 3 in (5.11) can't be made smaller.

Example 5.20. Two units in $\mathbf{Z}[\sqrt[4]{2}]$ arre $1+\sqrt{2}$ and $1+\sqrt[4]{2}$. There are two real embeddings and one pair of complex embeddings. Using the two real embeddings,

$$\mathrm{Reg}(\mathbf{Z}[\sqrt[4]{2}]) = \left|\det\begin{pmatrix} \log|1+\sqrt{2}| & \log|1+\sqrt{2}| \\ \log|1+\sqrt[4]{2}| & \log|1-\sqrt[4]{2}| \end{pmatrix}\right| \approx 2.158 \neq 0,$$

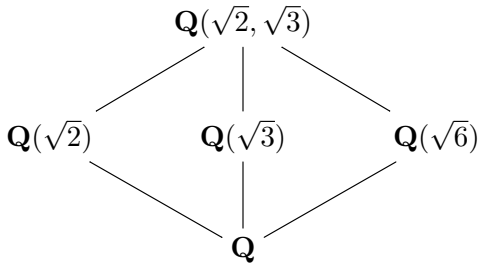
so $1 + \sqrt{2}$ and $1 + \sqrt[4]{2}$ are multiplicatively independent. These turn out to be a pair of fundamental units for $\mathbf{Z}[\sqrt[4]{2}]$, but we don't discuss a proof. It was first proved by Berwick [2, p. 372] in 1932.

Silverman [14] proved for number fields $K \neq \mathbf{Q}$ that there is a lower bound $\mathrm{Reg}(\mathcal{O}_K) > a(\log(b|D_K|))^{r-r_0}$, where $r = r_1+r_2-1$, r_0 is the maximum unit rank of the proper subfields of K (so $r_0 = 0$ if $\mathbf{Q}$ is the only proper subfield of K), $D_K = \mathrm{disc}(K)$, and a and b are constants depending only on the degree of K over $\mathbf{Q}$. The exponent $r - r_0$ is expected to be optimal. For cubic fields, $r - r_0 = r$, which is consistent with the regulator lower bounds in Example 5.19.

6. Units in a multiquadratic field

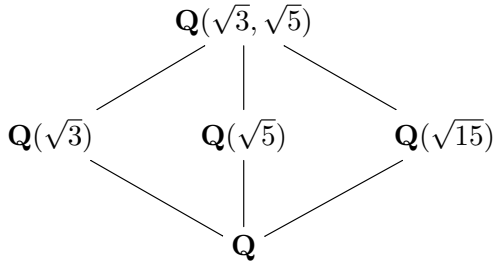
A biquadratic field $\mathbf{Q}(\sqrt{m}, \sqrt{n})$, where m, n, and mn are positive integers and not squares, has unit rank $4 - 1 = 3$. There are three real quadratic subfields, $\mathbf{Q}(\sqrt{m})$, $\mathbf{Q}(\sqrt{n})$, and $\mathbf{Q}(\sqrt{mn})$, and each has unit rank 1. A choice of one unit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

Example 6.1. 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 $u_1 = 1 + \sqrt{2}$, $u_2 = 2 + \sqrt{3}$, and $u_3 = 5 + 2\sqrt{6}$. In terms of the fundamental units of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, $u_2 = \left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^2$ and $u_3 = (\sqrt{2} + \sqrt{3})^2$. In terms of the fundamental units of the quadratic subfields, the fundamental units we listed for $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ are $u_1, \sqrt{u_3}, \sqrt{u_2}$.

Example 6.2. In the field $\mathbf{Q}(\sqrt{3}, \sqrt{5})$, a system of fundamental units is $\frac{1+\sqrt{5}}{2}$, $4 + \sqrt{15}$, and $\frac{3+\sqrt{3}+\sqrt{5}+\sqrt{15}}{2}$.



Fundamental units of the quadratic subfields are $u_1 = 2+\sqrt{3}$, $u_2 = \frac{1+\sqrt{5}}{2}$, and $u_3 = 4+\sqrt{15}$. In terms of the fundamental units of $\mathbf{Q}(\sqrt{3}, \sqrt{5})$, $u_1 = (4 + \sqrt{15})^{-1}\left(\frac{3+\sqrt{3}+\sqrt{5}+\sqrt{15}}{2}\right)^2$ by PARI. In terms of the fundamental units of the quadratic subfields, the fundamental units we listed for $\mathbf{Q}(\sqrt{3}, \sqrt{5})$ are $u_2, u_3, \sqrt{u_1 u_3}$.

Kuroda [9] showed that for every real biquadratic field $\mathbf{Q}(\sqrt{m}, \sqrt{n})$, with fundamental units u_1, u_2, u_3 for its 3 quadratic subfields, a set of fundamental units for the biquadratic field is one of the following 7 lists up to relabeling the u_i's:

$$\{u_1, u_2, u_3\}, \{\sqrt{u_1}, u_2, u_3\}, \{\sqrt{u_1 u_2}, u_2, u_3\}, \{\sqrt{u_1 u_2 u_3}, u_2, u_3\},$$
$$\{\sqrt{u_1}, \sqrt{u_2}, u_3\}, \{\sqrt{u_1 u_2}, \sqrt{u_3}, u_2\}, \{\sqrt{u_1 u_2}, \sqrt{u_2 u_3}, \sqrt{u_3 u_1}\}.$$

Examples 6.1 and 6.2 illustrate two of these possibilities and the list shows $\langle -1, u_1, u_2, u_3\rangle$ has index 1, 2, 4, or 8 in the unit group of the biquadratic field.

Consider now a general real multiquadratic field

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

where the d_i's are nonsquare *positive* integers that 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 6.3. *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 [10, 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.

One $\mathbf{Q}$-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 each nonempty subset J of $\{1, 2, \ldots, k\}$, there is a $\sigma_J \in \mathrm{Gal}(K/\mathbf{Q})$ such that $\sigma_J(\sqrt{d_J}) = -\sqrt{d_J}$ and $\sigma_J(\sqrt{d_I}) = \sqrt{d_I}$ for all $I \neq J$. Since σ_J is the identity on $\mathbf{Q}(\sqrt{d_I})$ and is nontrivial on $\mathbf{Q}(\sqrt{d_J})$, $\sigma_J(u_I) = u_I$ while $\sigma_J(u_J) = \pm u_J^{-1}$.

Applying σ_J 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 6.4. *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 $\mathcal{O}_K^\times$. □

Appendix A. Minimal nonzero value of a quadratic form

The following theorem is used near the end of the proof of Theorem 5.8.

Theorem A.1. *Let $Q(x, y) = Ax^2 + 2Bxy + Cy^2 = (x\ y)\left(\begin{smallmatrix} A & B \\ B & C \end{smallmatrix}\right)\binom{x}{y}$ be a positive-definite integral binary quadratic form with an even middle coefficient, and set $\det(Q) := AC - B^2 > 0$. There is a nonzero vector $(x_0, y_0) \in \mathbf{Z}^2$ such that $0 < Q(x_0, y_0) \leq \sqrt{(4/3)\det(Q)}$.*

Proof. Since $AC - B^2 > 0$, we have $A = Q(1, 0) > 0$ and $C = Q(0, 1) > 0$. In fact, all values of Q on $\mathbf{R}^2 - \{(0, 0)\}$ are positive since

$$\begin{aligned} Q(x, y) &= A\left(x^2 + \frac{2B}{A}xy + \frac{C}{A}y^2\right) \\ &= A\left(\left(x + \frac{B}{A}y\right)^2 + \frac{AC - B^2}{A^2}y^2\right) \\ &= A\left(\left(x + \frac{B}{A}y\right)^2 + \frac{\det(Q)}{A^2}y^2\right) > 0, \end{aligned}$$

so the polynomial $Q(x,y)$ on $\mathbf{Z}^2 - \{(0,0)\}$ has a minimum value in $\mathbf{Z}^+$. First assume A is the minimum value of Q on $\mathbf{Z}^2 - \{(0,0)\}$. Then we'll reduce the general case to that case.

Step 1: $A = \min Q(x,y)$ where (x,y) runs over $\mathbf{Z}^2 - \{(0,0)\}$.

Pick an integer x within $1/2$ of $-B/A$: $|x + B/A| \leq 1/2$. Then $Q(x,1) \leq A(1/2)^2 + \det(Q)/A$. From the minimality assumption on A,

$$A \leq Q(x,1) \leq \frac{A}{4} + \frac{\det(Q)}{A},$$

so $(3/4)A^2 \leq \det(Q)$. Therefore $Q(1,0) = A \leq \sqrt{(4/3)\det(Q)}$.

Step 2: General Q.

Let $\min Q(x,y) = Q(x_0,y_0) > 0$, where (x,y) runs over $\mathbf{Z}^2 - \{(0,0)\}$. The integers x_0 and y_0 are relatively prime: setting $d = \gcd(x_0,y_0)$ and writing $x_0 = dx_0'$ and $y_0 = dy_0'$, $Q(x_0,y_0) = Q(dx_0', dy_0') = d^2Q(x_0',y_0') \geq Q(x_0',y_0')$, so if $d > 1$ then the minimality of Q at (x_0,y_0) is violated. Thus $d = \gcd(x_0,y_0) = 1$.

There are x_1 and y_1 in $\mathbf{Z}$ such that $x_0y_1 - y_0x_1 = 1$, so the integral matrix $M = \left(\begin{smallmatrix} x_0 & x_1 \\ y_0 & y_1 \end{smallmatrix}\right)$ is invertible as an integral matrix with determinant 1. Note $M\binom{1}{0} = \binom{x_0}{y_0}$.

Now we'll make an invertible integral change of variables in $Q(x,y)$. Set

$$\widetilde{Q}(x,y) = Q\left(M\begin{pmatrix} x \\ y \end{pmatrix}\right) = \left(M\begin{pmatrix} x \\ y \end{pmatrix}\right)^\top \begin{pmatrix} A & B \\ B & C \end{pmatrix} M\begin{pmatrix} x \\ y \end{pmatrix} = (x\ y)M^\top \begin{pmatrix} A & B \\ B & C \end{pmatrix} M\begin{pmatrix} x \\ y \end{pmatrix}.$$

The product $M^\top \left(\begin{smallmatrix} A & B \\ B & C \end{smallmatrix}\right) M$ is symmetric (it equals its transpose) and has integral entries since M does. Its determinant is $AC - B^2 = \det(Q)$ since $\det(M) = 1$. Therefore if we write $M^\top \left(\begin{smallmatrix} A & B \\ B & C \end{smallmatrix}\right) M$ as $\left(\begin{smallmatrix} \widetilde{A} & \widetilde{B} \\ \widetilde{B} & \widetilde{C} \end{smallmatrix}\right)$, we have $\widetilde{Q}(x,y) = \widetilde{A}x^2 + 2\widetilde{B}xy + \widetilde{C}y^2$ where $\det(\widetilde{Q}) = \det(Q)$.

By Step 1, $\widetilde{Q}(1,0) = \widetilde{A} \leq \sqrt{(4/3)\det(\widetilde{Q})} = \sqrt{(4/3)\det(Q)}$. Since $\widetilde{Q}(1,0) = Q(M\binom{1}{0}) = Q(x_0,y_0)$, we have $0 < Q(x_0,y_0) \leq \sqrt{(4/3)\det(Q)}$. □

References

[1] E. Artin, *Theory of Algebraic Numbers*, George Striker, Schildweg 12, Göttingen, 1959.

[2] W. E. H. Berwick, "Algebraic number-fields with two independent units," Proc. London Math. Soc. **34** (1932), 360–378.

[3] T. Cusick, "Lower bounds for regulators," pp. 63–73 in *Number Theory, Noordwijkerhout 1983*, LNM 1068, Springer, Berlin 1984.

[4] P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, 4th ed., Vieweg und Sohn, Braunschweig, 1894. Online at https://archive.org/details/vorlesungenberz02dirigoog.

[5] R. Godement, *Introduction à la Théorie des Groups de Lie*, Springer–Verlag, Berlin, 2003.

[6] E. Kleinert, "Units of Classical Orders: A Survey," L'Enseignement Math. **40** (1994), 205–248.

[7] E. Kleinert, *Units in Skew Fields*, Birkhaüser, Basel, 2000.

[8] H. Koch, *Number Theory: Algebraic Numbers and Functions*, Amer. Math. Society, Providence, 2000.

[9] S. Kuroda, "Über den Dirichletschen Körper," J. Fac. Sci. Imp. Univ. Tokyo Sect. I **4** (1943), 383–406.

[10] F. Luca and I. E. Shparlinski, "On the Square-free Parts of $\lfloor en! \rfloor$," Glasgow Math. J. **49** (2007), 391–403.

[11] H. Minkowski, "Peter Gustav Lejeune Dirichlet und seine Bedeutung für die heutige Mathematik," Jahresbericht der Deutschen Mathematiker-Vereinigung **14** (1905), 149–163.

[12] L. J. Mordell, Review of E. Artin's "Theory of Algebraic Numbers", Bull. Amer. Math. Soc. **3** (1962), 162–166.

[13] D. Shanks, "The Simplest Cubic Fields," Math. Comp. **28** (1974), 1137–1152.

[14] J. H. Silverman, "An inequality relating the regulator and the discriminant of a number field," J. Number Theory **19** (1984), 437–442.

[15] E. Thomas, "Fundamental units for orders in certain cubic number fields," J. Reine Angew. Math. **310** (1979), 33–55.