

## THE UNIT GROUP OF A REAL QUADRATIC FIELD

While the unit group of an imaginary quadratic field is very simple, the unit group of a real quadratic field has nontrivial structure. Its study involves some geometry and analysis, but also it relates to Pell's equation and continued fractions, topics from elementary number theory.

### 1. REVIEW

Let  $F = \mathbf{Q}(\sqrt{n})$  be a real quadratic field. Thus  $n > 1$  is not a square, and we take  $n$  squarefree. Recall various facts about  $F$ .

- The nontrivial automorphism of  $F$  is the conjugation function,

$$\bar{\phantom{x}} : F \longrightarrow F, \quad \overline{a + b\sqrt{n}} = a - b\sqrt{n}.$$

- The trace function of  $F$  is the abelian group homomorphism

$$\text{tr} : F \longrightarrow \mathbf{Q}, \quad \text{tr}(x) = x + \bar{x}.$$

Specifically,

$$\text{tr}(a + b\sqrt{n}) = (a + b\sqrt{n}) + (a - b\sqrt{n}) = 2a.$$

The norm function of  $F$  is the homomorphism

$$N : F^\times \longrightarrow \mathbf{Q}^\times, \quad N(x) = x\bar{x}.$$

Specifically,

$$N(a + b\sqrt{n}) = (a + b\sqrt{n})(a - b\sqrt{n}) = a^2 - b^2n.$$

Sometimes we also define  $N(0) = 0$ .

- The unit group  $\mathcal{O}_F^\times$  of  $F^\times$  consists precisely of the elements of  $F^\times$  such that  $N(x) = \pm 1$ .
- The discriminant of  $F$  is

$$D_F = \begin{cases} n & \text{if } n \equiv 1 \pmod{4}, \\ 4n & \text{if } n \equiv 2, 3 \pmod{4}, \end{cases}$$

and the integer ring of  $F$  is

$$\mathcal{O}_F = \mathbf{Z} \left[ \frac{D_F + \sqrt{D_F}}{2} \right].$$

- An ideal of  $\mathcal{O}_F$  is a subset  $\mathfrak{a} \subset \mathcal{O}_F$  that forms an abelian group and is closed under multiplication by  $\mathcal{O}_F$ . The norm of a nonzero ideal  $\mathfrak{a}$  of  $\mathcal{O}_F$ , denoted  $N(\mathfrak{a})$ , is characterized by the conditions

$$\mathfrak{a}\bar{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}_F, \quad N(\mathfrak{a}) \in \mathbf{Z}^+.$$

We quickly show that for any positive integer  $m$ , only finitely many ideals  $\mathfrak{a}$  of  $\mathcal{O}_F$  have norm  $m$ . Indeed, for any such ideal,

$$\mathcal{O}_F \supset \mathfrak{a} \supset \mathfrak{a}\bar{\mathfrak{a}} = m\mathcal{O}_F.$$

Thus  $\mathcal{O}_F/m\mathcal{O}_F \supset \mathfrak{a}/m\mathcal{O}_F$ . But  $|\mathcal{O}_F/m\mathcal{O}_F| = m^2$  is finite, so there are only finitely many possibilities for  $\mathfrak{a}/m\mathcal{O}_F$  and hence only finitely many possibilities for  $\mathfrak{a} \cong \mathfrak{a}/m\mathcal{O}_F \oplus m\mathcal{O}_F$  (isomorphism of abelian groups).

- In consequence of the previous bullet, we have:

*Let  $\{x_h\}_{h \in \mathbf{Z}^+}$  be a sequence in  $\mathcal{O}_F$  all of whose elements satisfy  $|\mathbf{N}(x_h)| \leq \alpha$  for some constant  $\alpha$ . Then for some pair of distinct positive integers  $h$  and  $h'$ ,*

$$x_{h'} = ux_h, \quad u \in \mathcal{O}_F^\times.$$

The proof is that there are only finitely many ideals  $(x_h)$ .

## 2. GEOMETRIC RESULTS

**Lemma 2.1.** *Let  $\Lambda$  be a lattice in  $\mathbf{R}^2$ , and let  $E$  be a measurable subset of  $\mathbf{R}^2$  such that  $\mu(E) > \mu(\mathbf{R}^2/\Lambda)$ . Then there exist distinct points  $x, x' \in E$  such that  $x' - x \in \Lambda$*

*Proof.* Let  $(e, f)$  be a  $\mathbf{Z}$ -basis of  $\Lambda$ , so that corresponding fundamental parallelogram of  $\mathbf{R}^2/\Lambda$  is

$$\Pi = \{\xi e + \eta f : \xi, \eta \in [0, 1]\}.$$

Thus

$$\text{area}(\Pi) < \mu(E) = \sum_{\lambda \in \Lambda} \mu(E \cap (\lambda + \Pi)) = \sum_{\lambda \in \Lambda} \mu((\lambda + E) \cap \Pi).$$

Consequently, the intersection  $(\lambda + E) \cap (\lambda' + E) \cap \Pi$  must be nonempty for some distinct  $\lambda, \lambda' \in \Lambda$ . In particular,

$$\lambda + x = \lambda' + x' \quad \text{for some } x, x' \in E.$$

Thus  $x' - x = \lambda - \lambda' \in \Lambda - \{0\}$  as desired.  $\square$

**Proposition 2.2.** *Let  $\Lambda$  be a lattice in  $\mathbf{R}^2$ , and let  $E$  be a compact measurable subset of  $\mathbf{R}^2$  that is symmetric about 0 and convex and such that  $\mu(E) \geq 4\mu(\mathbf{R}^2/\Lambda)$ . Then  $E$  contains a nonzero point of  $\Lambda$ .*

*Proof.* The lemma says that for any  $\varepsilon > 0$ , the set

$$E' = \frac{1+\varepsilon}{2}E.$$

contains distinct points  $x$  and  $x'$  such that  $x' - x \in \Lambda$ . But also, using symmetry about 0, the nonzero difference  $x' - x = (2x' + 2(-x))/2$  is a convex linear combination of points of  $(1 + \varepsilon)E$ . That is, letting  $\Lambda' = \Lambda - \{0\}$ ,

$$\Lambda' \cap (1 + \varepsilon)E \neq \emptyset.$$

Note that  $\Lambda' \cap (1 + \varepsilon)E$  is compact (finite, for that matter) since it is the intersection of a discrete set and a compact set. Thus the nested intersection over all  $\varepsilon$  remains nonempty,

$$\bigcap_{\varepsilon > 0} (\Lambda' \cap (1 + \varepsilon)E) \neq \emptyset.$$

(The *finite intersection property* of compact sets rephrases the definition of compactness. If  $\bigcap_{\alpha} K_{\alpha} = \emptyset$  then  $\bigcup_{\alpha} K_{\alpha}^c = K_o$  gives an open cover of  $K_o$ , hence

$K_\alpha^c = K_o$  for some  $\alpha$  by the nestedness, hence  $K_\alpha = \emptyset$ , contradiction.) But the nonempty intersection is (again using the compactness of  $E$  at the last step)

$$\bigcap_{\varepsilon > 0} (\Lambda' \cap (1 + \varepsilon)E) = \Lambda' \cap \bigcap_{\varepsilon > 0} (1 + \varepsilon)E = \Lambda' \cap \overline{E} = \Lambda' \cap E.$$

This completes the argument.  $\square$

The lemma and the proposition are special cases of results due to Minkowski about the *geometry of numbers*.

### 3. THE CANONICAL EMBEDDING

**Definition 3.1.** *The canonical embedding of  $F$  is the ring homomorphism*

$$\iota : F \longrightarrow \mathbf{R}^2, \quad x \longmapsto (x, \bar{x}).$$

Recall that our real quadratic field is  $F = \mathbf{Q}(\sqrt{n})$ , and that the discriminant of  $F$  is

$$D_F = \begin{cases} n & \text{if } n \equiv 1 \pmod{4}, \\ 4n & \text{if } n \equiv 2, 3 \pmod{4}, \end{cases}$$

The abelian group structure of the integer ring of  $F$  is a direct sum,

$$\mathcal{O}_F = \frac{D_F + \sqrt{D_F}}{2} \mathbf{Z} \oplus \mathbf{Z}.$$

The images of the basis elements under the fundamental embedding are

$$\begin{aligned} \iota(1) &= (1, 1), \\ \iota\left(\frac{D_F + \sqrt{D_F}}{2}\right) &= \left(\frac{D_F + \sqrt{D_F}}{2}, \frac{D_F - \sqrt{D_F}}{2}\right). \end{aligned}$$

Thus  $\iota(\mathcal{O}_F)$  is a lattice in  $\mathbf{R}^2$  whose fundamental parallelogram has area

$$\left| \det \begin{bmatrix} 1 & 1 \\ \frac{D_F + \sqrt{D_F}}{2} & \frac{D_F - \sqrt{D_F}}{2} \end{bmatrix} \right| = \sqrt{D_F}.$$

That is,  $\mu(\mathbf{R}^2 / \iota(\mathcal{O}_F)) = \sqrt{D_F}$ . Consequently, Proposition 2.2 says that any compact box  $B$  that is symmetric about the origin and such that  $\text{area}(B) \geq 4\sqrt{D_F}$  contains a nonzero point of  $\iota(\mathcal{O}_F)$ . We will quote this fact later.

### 4. THE LOGARITHMIC EMBEDDING

**Definition 4.1.** *The logarithmic embedding of  $\mathcal{O}_F^\times$  is the group homomorphism*

$$\ell : \mathcal{O}_F^\times \longrightarrow \mathbf{R}^2, \quad x \longmapsto (\log |x|, \log |\bar{x}|).$$

Thus the logarithmic embedding takes the form

$$\ell = h \circ \iota|_{\mathcal{O}_F^\times}$$

where  $h$  is the continuous group homomorphism

$$h : (\mathbf{R}^\times)^2 \longrightarrow \mathbf{R}^2, \quad (u, v) \longmapsto (\log |u|, \log |v|).$$

Note that  $\iota|_{\mathcal{O}_F^\times}$  is also a homomorphism of multiplicative groups. Because  $x\bar{x} = N(x)$  for  $x \in \mathcal{O}_F^\times$ , the image  $\iota(\mathcal{O}_F^\times)$  lies in the ‘‘hyperbola’’

$$H = \{(u, v) \in (\mathbf{R}^\times)^2 : uv = \pm 1\}.$$

Also note that the calculation

$$uv = \pm 1 \implies \log |u| + \log |v| = \log |uv| = \log 1 = 0$$

shows that  $h$  restricts to a continuous homomorphism from the hyperbola  $H$  to the line of slope  $-1$ ,

$$L = \{(w, z) \in \mathbf{R}^2 : w + z = 0\}.$$

That is,

$$\iota(\mathcal{O}_F^\times) \subset H, \quad \ell(\mathcal{O}_F^\times) \subset L.$$

Also, direct inspection shows that

$$\ker(\ell) = \{\pm 1\},$$

and thus

$$\mathcal{O}_F^\times \cong \{\pm 1\} \times \ell(\mathcal{O}_F^\times).$$

## 5. UNIT GROUP STRUCTURE

**Lemma 5.1.** *For any nonnegative number  $r \in \mathbf{R}_{\geq 0}$ ,  $\ell^{-1}([-r, r]^2) \subset \mathcal{O}_F^\times$  is finite.*

(Setting  $r = 0$  in the lemma shows that  $\ker(\ell)$  is finite. Since  $\ker(\ell) = \{\pm 1\}$  in the real quadratic field case, we obtain nothing new here, but for number fields other than real quadratic fields, with the lemma modified accordingly, the result is of interest.)

*Proof.* Let  $r \geq 0$  and suppose that some element  $x \in \mathcal{O}_F^\times$  satisfies

$$\ell(x) \cap [-r, r]^2.$$

That is,  $(\log |x|, \log |\bar{x}|) \in [-r, r]^2$ , so that

$$|x|, |\bar{x}| \in [e^{-r}, e^r].$$

Consequently

$$|x + \bar{x}| \leq 2e^r \quad \text{and} \quad |x\bar{x}| \leq e^{2r}.$$

But the characteristic relation of  $x$  over  $\mathbf{Z}$  is

$$x^2 - ax + b = 0, \quad \begin{cases} a = \text{tr}(x) = x + \bar{x} \in \mathbf{Z}, \\ b = \text{N}(x) = x\bar{x} \in \mathbf{Z}. \end{cases}$$

Thus there are only finitely many possibilities for the characteristic polynomial, and hence there are only finitely many possibilities for  $x$ .  $\square$

Recall that  $\mathcal{O}_F^\times \cong \{\pm 1\} \times \ell(\mathcal{O}_F^\times)$ . The lemma shows that

$$\ell(\mathcal{O}_F^\times) \text{ is a discrete subgroup of } L.$$

Since  $L \cong \mathbf{R}$ , the question now is whether  $\ell(\mathcal{O}_F^\times) = \{0\}$  or  $\ell(\mathcal{O}_F^\times) \cong \mathbf{Z}$ .

**Proposition 5.2.**  $\ell(\mathcal{O}_F^\times) \cong \mathbf{Z}$ .

*Proof.* We will show that for any given nonzero linear functional

$$f : L \longrightarrow \mathbf{R},$$

there is a unit  $u \in \mathcal{O}_F^\times$  such that  $f(\ell(u)) \neq 0$ .

Since  $L = \{(w, z) \in \mathbf{R}^2 : w + z = 0\}$ , we have

$$f(w, z) = cw \quad \text{for some nonzero } c \in \mathbf{R}.$$

Introduce notation to make the proof run smoothly later by fixing a real number

$$\alpha \geq \sqrt{D_F},$$

and fixing a real number

$$\beta > |c| \log \alpha.$$

For any positive real number  $\lambda$ , let  $\mu = \alpha/\lambda$  so that  $\lambda\mu = \alpha$ . The compact box

$$B = [-\lambda, \lambda] \times [-\mu, \mu]$$

thus is symmetric about the origin, and its area is  $\text{area}(B) = 4\alpha \geq 4\sqrt{D_F}$ . As explained in section 3, the geometry of numbers shows that there exists a nonzero integer  $x_\lambda \in \mathcal{O}_F$  such that  $\iota(x_\lambda) \in B$ . The fact that  $\iota(x_\lambda) \in B$  says that

$$|\mathbf{N}(x_\lambda)| \leq \alpha.$$

Also, the condition  $|\mathbf{N}(x_\lambda)| \geq 1$  holds because  $x_\lambda \in \mathcal{O}_F$ , so

$$|x_\lambda| = |\mathbf{N}(x_\lambda)|/|\overline{x_\lambda}| \geq 1/\mu = \lambda/\alpha.$$

Thus  $1 \leq \lambda/|x_\lambda| \leq \alpha$ , and so

$$0 \leq \log \lambda - \log |x_\lambda| \leq \log \alpha.$$

Returning to the linear form  $f(w, z) = cw$ , we now have an estimate of  $f(\ell(x_\lambda))$ ,

$$|f(\ell(x_\lambda)) - c \log \lambda| = |c \log |x_\lambda| - c \log \lambda| \leq |c| \log \alpha < \beta.$$

The procedure of the previous paragraph works for any positive real number  $\lambda$ . For each positive integer  $h$  choose a corresponding  $\lambda_h$  such that

$$c \log \lambda_h = 2\beta h.$$

Thus  $\lambda_h = \exp(2\beta h/c)$ , so that our boxes grow horizontally and shrink vertically at a rate exponential in  $h$ . Consequently the logarithm of the absolute value of the first coordinate of a typical point in the box grows linearly in  $h$ . Quantitatively we have, by the previous two displays,

$$|f(\ell(x_{\lambda(h)})) - 2\beta h| < \beta \quad \text{for } h = 1, 2, 3, \dots,$$

and opening up the absolute value gives

$$(2h - 1)\beta < f(\ell(x_{\lambda(h)})) < (2h + 1)\beta \quad \text{for } h = 1, 2, 3, \dots,$$

showing that the values  $f(\ell(x_{\lambda(h)}))$  are all distinct. On the other hand, recall that

$$|\mathbf{N}(x_{\lambda(h)})| \leq \alpha \quad \text{for } h = 1, 2, 3, \dots,$$

so that (as explained at the end of the review section), for some pair of distinct positive integers  $h$  and  $h'$  we have

$$x_{\lambda(h')} = u x_{\lambda(h)}, \quad u \in \mathcal{O}_F^\times.$$

And so finally, since the logarithmic embedding  $\ell$  is a multiplicative-to-additive homomorphism, and since the functional  $f$  is linear, and since the values  $f(\ell(x_{\lambda(h)}))$  and  $f(\ell(x_{\lambda(h')}))$  are distinct,

$$\begin{aligned} f(\ell(u)) &= f(\ell(x_{\lambda(h')}/x_{\lambda(h)})) \\ &= f(\ell(x_{\lambda(h')}) - \ell(x_{\lambda(h)})) \\ &= f(\ell(x_{\lambda(h')})) - f(\ell(x_{\lambda(h)})) \neq 0. \end{aligned}$$

Thus  $\ell(\mathcal{O}_F^\times) \neq \{0\}$  and consequently  $\ell(\mathcal{O}_F^\times) \cong \mathbf{Z}$  as desired.  $\square$

## 6. THE FUNDAMENTAL UNIT

**Definition 6.1.** *The unique element  $u_1 \in \mathcal{O}_F^\times$  such that*

$$\mathcal{O}_F^\times = \{\pm 1\} \times \langle u_1 \rangle = \{\pm 1\} \times \{u_1^i : i \in \mathbf{Z}\}, \quad u_1 > 1.$$

*is the fundamental unit of  $F$ .*

The fundamental unit  $u_1$  is one of four generators of the infinite part of  $\mathcal{O}_F^\times$ , the other three being  $-u_1$  and  $\pm u_1^{-1}$ . If the fundamental unit is

$$u_1 = a + b\sqrt{n}, \quad a, b \in \mathbf{Q}$$

then since  $N(g) = \pm 1$ , the four generators are altogether

$$\pm a \pm b\sqrt{n}.$$

Since the fundamental unit is the largest of the four generators, in fact

$$u_1 = a + b\sqrt{n}, \quad a, b \in \mathbf{Q}^+,$$

and  $u_1$  is the *smallest* such element  $a + b\sqrt{n}$  of  $\mathcal{O}_F$ . The units  $u > 1$  are overall

$$u_k = u_1^k = (a + b\sqrt{n})^k, \quad k = 1, 2, 3, \dots$$

We now proceed by cases.

If  $n = 2, 3 \pmod{4}$  then

$$\mathcal{O}_F = \{a + b\sqrt{n} : a, b \in \mathbf{Z}\},$$

and so the fundamental unit takes the form

$$u_1 = a_1 + b_1\sqrt{n}, \quad a_1, b_1 \in \mathbf{Z}^+, \quad a_1^2 - nb_1^2 = \pm 1.$$

Its positive powers are

$$u_1^k = a_k + b_k\sqrt{n} = (a_1 + b_1\sqrt{n})^k.$$

Since  $b_{k+1} = a_k b_1 + b_k a_1$ , the sequence  $\{b_k\}$  is strictly increasing. Thus, an algorithm to find the fundamental unit for  $n = 2, 3 \pmod{4}$  is:

*Test  $b_1 = 1, 2, 3, \dots$  until either of  $nb_1^2 \pm 1$  is a perfect square. Let  $a_1$  be the positive integer such that  $a_1^2 - nb_1^2 = \pm 1$ . Then  $u_1 = a_1 + b_1\sqrt{n}$ .*

If  $n = 1 \pmod{4}$  then

$$\mathcal{O}_F = \left\{ \frac{1}{2}(a + b\sqrt{n}) : a, b \in \mathbf{Z}, a \equiv b \pmod{2} \right\},$$

and so the fundamental unit takes the form

$$u_1 = \frac{1}{2}(a_1 + b_1\sqrt{n}), \quad a_1, b_1 \in \mathbf{Z}^+, \quad a_1 \equiv b_1 \pmod{2}, \quad a_1^2 - nb_1^2 = \pm 4.$$

Its positive powers are

$$u_1^k = \frac{1}{2^k}(a_k + b_k\sqrt{n}) = \frac{1}{2^k}(a_1 + b_1\sqrt{n})^k.$$

Since  $b_{k+1} = a_k b_1 + b_k a_1$ , the sequence  $\{b_k\}$  is strictly increasing. Thus, an algorithm to find the fundamental unit for  $n = 1 \pmod{4}$  is:

*Test  $b_1 = 1, 2, 3, \dots$  until either of  $nb_1^2 \pm 4$  is a perfect square. Let  $a_1$  be the positive integer such that  $a_1^2 - nb_1^2 = \pm 4$ . Then  $u_1 = \frac{1}{2}(a_1 + b_1\sqrt{n})$ .*

$n$	$u_1$
2	$1 + \sqrt{2}$
3	$2 + \sqrt{3}$
5	$\frac{1}{2}(1 + \sqrt{5})$
6	$5 + 2\sqrt{6}$
7	$8 + 3\sqrt{7}$
10	$3 + \sqrt{10}$
11	$10 + 3\sqrt{11}$
13	$\frac{1}{2}(3 + \sqrt{13})$
14	$15 + 4\sqrt{14}$
15	$4 + \sqrt{15}$
17	$4 + \sqrt{17}$
19	$170 + 39\sqrt{19}$
21	$\frac{1}{2}(5 + \sqrt{21})$

FIGURE 1. Table of fundamental units

Some fundamental units are shown in table 1.

A more efficient method for finding the fundamental unit uses *continued fractions*.

#### 7. THE CONTINUED FRACTION OF A RATIONAL NUMBER

Let  $c$  and  $d$  be integers, with  $d > 0$ . The Euclidean algorithm gives

$$\begin{aligned} \frac{c}{d} &= q_0 + \frac{r_0}{d}, & q_0 \in \mathbf{Z}, & & 0 < r_0 < d, \\ \frac{d}{r_0} &= q_1 + \frac{r_1}{r_0}, & q_1 > 0, & & 0 < r_1 < r_0, \\ \frac{r_0}{r_1} &= q_2 + \frac{r_2}{r_1}, & q_2 > 0, & & 0 < r_2 < r_1, \\ & \vdots \\ \frac{r_{m-2}}{r_{m-1}} &= q_m, & q_m > 1 & \text{(note)}. \end{aligned}$$

Thus

$$\frac{c}{d} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots + \frac{1}{q_m}}}}.$$

Working productively with the notation of the previous display is hopeless. The standard remedy is to write instead

$$\frac{c}{d} = q_0 + \frac{1}{q_1 +} \frac{1}{q_2 +} \dots \frac{1}{q_m}.$$

Note that also (using the fact that  $q_m > 1$ )

$$\frac{c}{d} = q_0 + \frac{1}{q_1 +} \frac{1}{q_2 +} \dots \frac{1}{(q_m - 1) +} \frac{1}{1}.$$

The expression in the previous three displays is the **continued fraction** expression of  $c/d$ .

Symbolically, the first few continued fractions are

$$\begin{aligned} q_0 &= \frac{q_0}{1}, \\ q_0 + \frac{1}{q_1} &= \frac{q_0 q_1 + 1}{q_1}, \\ q_0 + \frac{1}{q_1 + \frac{1}{q_2}} &= q_0 + \frac{q_2}{q_1 q_2 + 1} = \frac{q_0 q_1 q_2 + q_0 + q_2}{q_1 q_2 + 1}, \\ q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3}}} &= q_0 + \frac{q_2 q_3 + 1}{q_1 q_2 q_3 + q_1 + q_3} = \frac{q_0 q_1 q_2 q_3 + q_0 q_1 + q_0 q_3 + q_2 q_3 + 1}{q_1 q_2 q_3 + q_1 + q_3}. \end{aligned}$$

The numerator of the continued fraction has a standard symbol,

$$q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \dots \frac{1}{q_m}}} = \frac{[q_0, q_1, \dots, q_m]}{d}.$$

Thus, for example,

$$\begin{aligned} [q_0] &= q_0, \\ [q_0, q_1] &= q_0 q_1 + 1, \\ [q_0, q_1, q_2] &= q_0 q_1 q_2 + q_0 + q_2, \\ [q_0, q_1, q_2, q_3] &= q_0 q_1 q_2 q_3 + q_0 q_1 + q_0 q_3 + q_2 q_3 + 1. \end{aligned}$$

The denominator requires no symbol of its own because, as the small examples have shown, it is simply  $[q_1, \dots, q_m]$ . To show this in general, note that the equality

$$q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \dots \frac{1}{q_m}}} = q_0 + \frac{1}{q_1 + \frac{1}{\frac{1}{\frac{1}{q_3 + \dots \frac{1}{q_m}}}}}$$

rewrites as

$$\frac{[q_0, q_1, \dots, q_m]}{d} = q_0 + \frac{d'}{[q_1, \dots, q_m]} = \frac{q_0 [q_1, \dots, q_m] + d'}{[q_1, \dots, q_m]},$$

showing that indeed

$$q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \dots \frac{1}{q_m}}} = \frac{[q_0, q_1, \dots, q_m]}{[q_1, \dots, q_m]}.$$

This calculation also shows the recurrence

$$[q_0, q_1, q_2, \dots, q_m] = q_0 [q_1, \dots, q_m] + [q_2, \dots, q_m],$$

which makes computation with these symbols quick.

Euler gave the explicit formula

$$[q_0, \dots, q_m] = q_0 \cdots q_m + \sum_i \frac{q_0 \cdots q_m}{q_i q_{i+1}} + \sum_{i,j} \frac{q_0 \cdots q_m}{q_i q_{i+1} q_j q_{j+1}} + \cdots.$$

That is,

- multiply all the  $q$ 's together,
- then multiply them together omitting *consecutive* pairs,
- then multiply them together omitting *pairs* of consecutive pairs,
- and so on.

Euler's formula demands extending the numerator-symbol to include the case

$$[\ ] = 1.$$

A consequence of Euler's formula is symmetry,

$$[q_0, q_1, \dots, q_m] = [q_m, \dots, q_1, q_0],$$

so that the recurrence is also

$$[q_0, q_1, q_2, \dots, q_m] = [q_0, \dots, q_{m-1}]q_m + [q_0, \dots, q_{m-2}].$$

For any  $k \geq 0$ , let

$$A_k = [q_0, q_1, \dots, q_k] \quad \text{and} \quad B_k = [q_1, \dots, q_k].$$

Then the  $k$ th **convergent** is  $A_k/B_k$ . Since

$$\begin{bmatrix} A_k \\ B_k \end{bmatrix} = q_k \begin{bmatrix} A_{k-1} \\ B_{k-1} \end{bmatrix} + \begin{bmatrix} A_{k-2} \\ B_{k-2} \end{bmatrix},$$

the convergents are easy to compute. Also,

$$\begin{vmatrix} A_k & A_{k-1} \\ B_k & B_{k-1} \end{vmatrix} = - \begin{vmatrix} A_{k-1} & A_{k-2} \\ B_{k-1} & B_{k-2} \end{vmatrix}$$

and

$$\begin{vmatrix} A_1 & A_0 \\ B_1 & B_0 \end{vmatrix} = \begin{vmatrix} [q_0, q_1] & [q_0] \\ [q_1] & [\ ] \end{vmatrix} = (q_0 q_1 + 1) \cdot 1 - q_0 q_1 = 1,$$

so that

$$\begin{vmatrix} A_{k+1} & A_k \\ B_{k+1} & B_k \end{vmatrix} = (-1)^k, \quad k \geq 0.$$

In particular,  $\gcd(A_k, B_k) = 1$  for all  $k \geq 0$ , showing that the  $k$ th convergent is in lowest terms.

Since

$$\frac{A_{k+1}}{B_{k+1}} - \frac{A_k}{B_k} = \frac{(-1)^k}{B_k B_{k+1}},$$

it follows that the sequence  $\{A_k/B_k\}$  is Leibniz.

## 8. THE CONTINUED FRACTION OF AN IRRATIONAL NUMBER

Let  $\alpha$  be an irrational number. Similarly to before, we have

$$\alpha = q_0 + 1/\alpha_1, \quad q_0 \in \mathbf{Z}, \quad \alpha_1 > 1,$$

$$\alpha_1 = q_1 + 1/\alpha_2, \quad q_1 > 0, \quad \alpha_2 > 1,$$

$$\alpha_2 = q_2 + 1/\alpha_3, \quad q_2 > 0, \quad \alpha_3 > 1,$$

$\vdots$

$$\alpha_m = q_m + 1/\alpha_{m+1}, \quad q_m > 0, \quad \alpha_{m+1} > 1$$

(specifically, each  $q_i = \lfloor \alpha_i \rfloor$  where  $\alpha_0 = \alpha$ ), but now the process doesn't terminate. Still, as before,

$$\alpha = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \dots + \frac{1}{q_m + \frac{1}{\alpha_{m+1}}}}}$$

Also as before,

$$\alpha = \frac{[q_0, \dots, q_m, \alpha_{m+1}]}{[q_1, \dots, q_m, \alpha_{m+1}]},$$

and we have the recurrence

$$[q_0, \dots, q_m, \alpha_{m+1}] = [q_0, \dots, q_m] \alpha_{m+1} + [q_0, \dots, q_{m-1}] = \alpha_{m+1} A_m + A_{m-1}.$$

Similarly

$$[q_1, \dots, q_m, \alpha_{m+1}] = \alpha_{m+1} B_m + B_{m-1},$$

and so

$$\alpha = \frac{\alpha_{m+1} A_m + A_{m-1}}{\alpha_{m+1} B_m + B_{m-1}}.$$

A little algebra gives

$$\alpha - \frac{A_m}{B_m} = \pm \frac{1}{B_m(\alpha_{m+1} B_m + B_{m+1})},$$

and since  $\alpha_{m+1} > q_{m+1}$  it follows that

$$\left| \alpha - \frac{A_m}{B_m} \right| < \frac{1}{B_m B_{m+1}}.$$

Thus

$$\alpha = \lim_m \frac{A_m}{B_m} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_m + \dots}}}.$$

When the continued fraction context is clear, we write more concisely

$$\alpha = q_0, q_1, q_2, \dots, q_m, \dots.$$

**Definition 8.1.** A quadratic irrational number is a real number of the form

$$\alpha = a + b\sqrt{n}, \quad a, b \in \mathbf{Q}, \quad n \in \mathbf{Z}^+ \text{ squarefree.}$$

The **conjugate** of such a number is

$$\alpha' = a - b\sqrt{n}.$$

A quadratic irrational number is **normalized** if  $\alpha > 1$  and  $-1 < \alpha' < 0$ .

**Proposition 8.2.** Let  $\alpha$  be an irrational number. Then  $\alpha$  is quadratic and normalized if and only if its continued fraction is periodic.

*Proof of the easy direction.* Suppose that

$$\alpha = q_0, \dots, q_m, q_0, \dots, q_m, q_0, \dots, q_m, \dots = \overline{q_0, \dots, q_m}.$$

Since  $q_0$  repeats as the term of the continued fraction, it is a positive integer, giving  $\alpha > 1$ . Next, the characteristic relation of  $\alpha$ ,

$$\alpha = \frac{A_m \alpha + A_{m-1}}{B_m \alpha + B_{m-1}},$$

rewrites as the characteristic equation

$$B_m \alpha^2 + (B_{m-1} - A_m) \alpha - A_{m-1} = 0,$$

showing that  $\alpha$  is quadratic. Now consider the reverse-order periodic continued fraction,

$$\beta = \overline{q_m, \dots, q_0}.$$

Note that  $\beta > 1$  since  $q_m$  is a positive integer, and note that the characteristic relation of  $\beta$  is almost the same as that of  $\alpha$ ,

$$\beta = \frac{A_m \beta + B_m}{A_{m-1} \beta + B_{m-1}}.$$

Consequently, the characteristic relation of  $-1/\beta$  is

$$-1/\beta = \frac{B_{m-1}(-1/\beta) - A_{m-1}}{-B_m(-1/\beta) + A_m},$$

so that the characteristic equation of  $-1/\beta$  is

$$B_m(-1/\beta)^2 + (B_{m-1} - A_m)(-1/\beta) - A_{m-1} = 0.$$

That is,  $\alpha$  and  $-1/\beta$  satisfy the same quadratic equation, so  $-1/\beta$  is one of  $\alpha, \alpha'$ . Since  $\alpha > 1$  and  $-1 < -1/\beta < 0$ , we see that  $-1/\beta = \alpha'$  and consequently  $-1 < \alpha' < 0$ . That is,  $\alpha$  is normalized.

The proof of the other direction isn't much more difficult, but it is a bit more painstaking.  $\square$

Now consider a positive integer  $n$  that is not a perfect square. Let

$$q_0 = \lfloor \sqrt{n} \rfloor, \quad \alpha = q_0 + \sqrt{n}.$$

Then  $\alpha' = q_0 - \sqrt{n} \in (-1, 0)$ , showing that  $\alpha$  is normalized. Note also that

$$\alpha' = -\alpha + 2q_0.$$

By the (unproved direction of the) previous proposition,

$$\alpha = \overline{2q_0, q_1, \dots, q_m},$$

so that

$$\frac{1}{\alpha - 2q_0} = \overline{q_1, \dots, q_m, 2q_0}.$$

Also, by the proof of the proposition,

$$-1/\alpha' = \overline{q_m, \dots, q_1, 2q_0}.$$

But since  $\alpha' = q_0 - \sqrt{n}$ , the left sides of the two previous displays are equal, hence so are the right sides, and thus

$$q_1, \dots, q_m \text{ is palindromic.}$$

Thus  $\sqrt{n} = \alpha - q_0$  has continued fraction

$$\boxed{\sqrt{n} = q_0, \overline{q_1, q_2, \dots, q_2, q_1, 2q_0}}.$$

For example,

$$\sqrt{2} = 1, \overline{2},$$

$$\sqrt{3} = 1, \overline{1, 2},$$

$$\sqrt{13} = 3, \overline{1, 1, 1, 1, 6},$$

$$\sqrt{31} = 5, \overline{1, 1, 3, 5, 3, 1, 1, 10}.$$

Rewrite the continued fraction representation of  $\sqrt{n}$  in a fashion that forgets its palindromic aspect,

$$\sqrt{n} = q_0, \overline{q_1, q_2, \dots, q_{m-1}, q_m, 2q_0}.$$

Then

$$\sqrt{n} = \frac{\alpha_{m+1}A_m + A_{m-1}}{\alpha_{m+1}B_m + B_{m-1}}$$

where

$$\alpha_{m+1} = 2q_0, \overline{q_1, \dots, q_m, 2q_0} = \sqrt{n} + q_0.$$

The previous two displays give

$$\sqrt{n} = \frac{(\sqrt{n} + q_0)A_m + A_{m-1}}{(\sqrt{n} + q_0)B_m + B_{m-1}},$$

or

$$\sqrt{n}((\sqrt{n} + q_0)B_m + B_{m-1}) = (\sqrt{n} + q_0)A_m + A_{m-1},$$

or, after equating rational and irrational components,

$$A_{m-1} = -q_0A_m + nB_m,$$

$$B_{m-1} = A_m - q_0B_m.$$

Recall that

$$\begin{vmatrix} A_m & A_{m-1} \\ B_m & B_{m-1} \end{vmatrix} = (-1)^{m-1}.$$

The previous two displays give

$$\begin{vmatrix} A_m & -q_0A_m + nB_m \\ B_m & A_m - q_0B_m \end{vmatrix} = (-1)^{m-1},$$

or

$$A_m^2 - nB_m^2 = (-1)^{m-1}.$$

That is,

$$\boxed{A_m + B_m\sqrt{n} \text{ is a unit of } \mathbf{Q}(\sqrt{n}).}$$