In this example we consider the polynomial

$$f(X) = X^4 + 6X^2 - 3X - 6.$$

Since it is Eisenstein with respect to the prime 3, it is irreducible in $\mathbf{Q}[X]$. Let α denote a zero of f. In this note we prove the following theorem.

Theorem. *Let $F = \mathbf{Q}(\alpha)$. Then we have the following.*
(a) The ring of integers O_F of F is equal to $\mathbf{Z}[\alpha]$.
(b) The ideal class group of O_F is cyclic of order 4.
(c) the unit group O_F^* is generated by -1 and the units

$$1 - \alpha^2 + \alpha^3 \quad \textit{and} \quad 7 - 6\alpha + \alpha^2 - \alpha^3.$$

1. Discriminant, ring of integers and quadratic form.

Proposition 1. *The ring of integers O_F of F is equal to $\mathbf{Z}[\alpha]$ and the discriminant of F is equal to $-402219 = -3^3 14897$.*

Proof. In general, if α is a zero of an irreducible polynomial of the form $x^4 - a_3X^3 + a_2X^2 - a_1X + a_0$, Newton's formulas imply that $\mathrm{Tr}(\alpha^k) = 4, a_3, a_3^2 - 2a_2$ and $a_3^3 - 3a_2a_3 - 3a_2$ for $k = 0, 1, 2, 3$ respectively. In this case, we find that $\mathrm{Tr}(\alpha^k) = 4, 0, -12$ and 9 for $k = 0, 1, 2, 3$ respectively. We use the relation $\alpha^k = -6\alpha^{k-2} + 3\alpha^{k-3} + 6\alpha^{k-4}$ to compute the trace of α^k for $k \geq 4$. This gives $\mathrm{Tr}(\alpha^k) = 96, -90$ and -621 for $k = 4, 5$ and 6 respectively. Therefore the discriminant of the ring $\mathbf{Z}[\alpha]$ is given by

$$\det \begin{pmatrix} 4 & 0 & -12 & 9 \\ 0 & -12 & 9 & 96 \\ -12 & 9 & 96 & -90 \\ 9 & 96 & -90 & -621 \end{pmatrix} = -402219 = -3^3 14897.$$

Since f is Eisenstein at 3 and since 14897 is prime, the ring $\mathbf{Z}[\alpha]$ is integrally closed. Therefore the ring of integers O_F of F is equal to $\mathbf{Z}[\alpha]$. This proves the Lemma.

The second derivative of f is $12X^2 + 12$. Since it has no zeroes, the derivative of f has only one zero and hence f has only one minimum. Since $f(0) = -6$ is negative, f has precisely two real zeroes. They are approximately equal to -0.7542 and 1.1359. Let ϕ_1 and ϕ_2 denote the corresponding embeddings $F \hookrightarrow \mathbf{R}$. The non-real zeroes are $-0.1908 \pm 2.6393i$. Let $\phi_3 : F \hookrightarrow \mathbf{C}$ be the embedding that maps α to $-0.1908 + 2.6393i$ and ϕ_4 its complex conjugate.

The natural scalar product on the 4-dimensional $\mathbf{R}$-algebra $F_{\mathbf{R}}$ gives rise to the following formula for the length of an element $x \in F \hookrightarrow F_{\mathbf{R}}$:

$$\|x\|^2 = \sum_{i=1}^{4} |\phi_i(x)|^2.$$

For the computation of the unit group, it is useful to make this explicit. Since $1, \alpha, \alpha^2, \alpha^3$ is a $\mathbf{Z}$-basis of O_F, any $x \in O_F$ can be written as $\lambda_1 + \lambda_2\alpha + \lambda_3\alpha^2 + \lambda_4\alpha^3$ with $\lambda_i \in \mathbf{Z}$. It follows that $\|x\|^2$ is the value of the quadratic form

$$Q(X_1, X_2, X_3, X_4) = \sum_{i,j=1}^{4} a_{ij} X_i X_j, \quad \text{with } a_{ij} = \textstyle\sum_{k=1}^{4} \phi_k(\alpha^{i-1})\overline{\phi_k(\alpha^{j-1})}$$

in $(\lambda_1, \lambda_2\lambda_3, \lambda_4)$. The determinant of the matrix (a_{ij}) is $|\Delta_F|$. Numerically, we have

$$\begin{aligned} Q(X_1, X_2, X_3, X_4) =& 4X_1^2 - 24X_1X_3 + 18X_1X_4 + 15.8644\, X_2^2 - 3.2722\, X_2X_3 \\ & - 190.1235\, X_2X_4 + 100.0599\, X_3^2 - 34.1395\, X_3X_4 + 689.0786\, X_4^2 \end{aligned}$$

$$\begin{aligned} = \quad & 4(X_1 - 3X_3 + \tfrac{9}{4}X_4)^2 \\ & + 15.8644(X_2 - 0.1031\, X_3 - 5.9921\, X_4)^2 \\ & + 63.8911(X_3 + 0.0019\, X_4)^2 \\ & + 99.2057\, X_4^2. \end{aligned}$$

2. The class group.

We compute the Minkowski constant of F. It is given by

$$\frac{4!}{4^4}\frac{4}{\pi}\sqrt{402219} = 75.7029.$$

It follows that the class group of O_F is generated by the prime ideals of norm ≤ 73. Generators of these prime ideals can be computed by factoring the polynomial f modulo the prime numbers $p \leq 73$. Prime ideals of characteristic p that have norm p^k with $k \geq 2$ necessarily satisfy $p \leq \sqrt{73}$. We list these primes in Table I.

Table I.

p		
2	$\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_4$	$\mathfrak{p}_2 = (\alpha, 2)$, $\mathfrak{p}_2' = (\alpha+1, 2)$, $\mathfrak{p}_4 = (2, 1+\alpha+\alpha^2)$
3	$\mathfrak{p}_3^4$	$\mathfrak{p}_3 = (\alpha, 3)$
5	$\mathfrak{p}_5\mathfrak{p}_{125}$	$\mathfrak{p}_5 = (5, \alpha+2)$
7	$\mathfrak{p}_7\mathfrak{p}_{343}$	$\mathfrak{p}_7 = (7, \alpha-2)$

The remaining prime ideals of norm ≤ 73 are of the form $(p, \alpha - z)$, where p is a prime ≤ 73 and z is a root of the polynomial f in $\mathbf{F}_p$. We list these prime ideals in Table II. Note that the ring O_F does not possess any prime ideals whose norm is between 47 and 73.

Table II.

p	
13	$\mathfrak{p}_{13} = (13, \alpha - 5)$
19	$\mathfrak{p}_{19} = (19, \alpha + 9)$
23	$\mathfrak{p}_{23} = (23, \alpha + 3)$, $\mathfrak{p}'_{23} = (23, \alpha + 16)$
29	$\mathfrak{p}_{29} = (29, \alpha - 7)$, $\mathfrak{p}'_{29} = (29, \alpha - 5)$
31	$\mathfrak{p}_{31} = (31, \alpha + 9)$, $\mathfrak{p}'_{31} = (31, \alpha - 6)$
41	$\mathfrak{p}_{41} = (41, \alpha - 17)$
43	$\mathfrak{p}_{43} = (43, \alpha + 11)$, $\mathfrak{p}'_{43} = (43, \alpha + 20)$
47	$\mathfrak{p}_{47} = (47, \alpha + 24)$

Proposition 2. *The class group of O_F is generated by $\mathfrak{p}_2$. Moreover, $\mathfrak{p}_2^4$ is principal.*

Proof. To see this, we factor a few "small" principal ideals. It is convenient to consider principal ideals generated by elements of the form $a + b\alpha$ for $a, b \in \mathbf{Z}$, because their norms are equal to $b^4 f(-a/b)$ and are easy to compute. We computed the norms of $a + b\alpha$ for $a, b \in \mathbf{Z}$ satisfying $-5 \leq a, b \leq 5$. There are 39 such numbers with $\gcd(a, b) = 1$. In Table III we have listed the factorizations of $a + b\alpha$ all of whose prime ideal factors have norm ≤ 47.

Table III.

$a + b\alpha$	$\lvert N(a + b\alpha)\rvert$	
$1 + 2\alpha$	47	$\mathfrak{p}_{47}$
$1 + 4\alpha$	$29 \cdot 43$	$\mathfrak{p}_{29}\mathfrak{p}_{43}$
$3 - 2\alpha$	$3 \cdot 43$	$\mathfrak{p}_3\mathfrak{p}'_{43}$
$3 - 5\alpha$	$2^2 \cdot 3 \cdot 7 \cdot 41$	$\mathfrak{p}_2'^2\mathfrak{p}_3\mathfrak{p}_7\mathfrak{p}_{41}$
$4 - 3\alpha$	$2^2 \cdot 5 \cdot 31$	$\mathfrak{p}_2^2\mathfrak{p}_5\mathfrak{p}_{31}$
$1 + 5\alpha$	$2^3 \cdot 13 \cdot 31$	$\mathfrak{p}_2'^2\mathfrak{p}_{13}\mathfrak{p}'_{31}$
$5 - \alpha$	$2 \cdot 13 \cdot 29$	$\mathfrak{p}'_2\mathfrak{p}_{13}\mathfrak{p}'_{29}$
$3 + \alpha$	$2 \cdot 3 \cdot 23$	$\mathfrak{p}'_2\mathfrak{p}_3\mathfrak{p}_{23}$
$2 + 3\alpha$	$2^2 \cdot 23$	$\mathfrak{p}_2^2\mathfrak{p}'_{23}$
$1 - 2\alpha$	$5 \cdot 19$	$\mathfrak{p}_5\mathfrak{p}_{19}$
$2 - 3\alpha$	$2^5 \cdot 13$	$\mathfrak{p}_2^5\mathfrak{p}_{13}$
$2 - \alpha$	$2^2 \cdot 7$	$\mathfrak{p}_2^2\mathfrak{p}_7$
$2 + \alpha$	$2^5 \cdot 5$	$\mathfrak{p}_2^5\mathfrak{p}_5$
2	2^4	$\mathfrak{p}_2\mathfrak{p}'_2\mathfrak{p}_4$
α	$2 \cdot 3$	$\mathfrak{p}_2\mathfrak{p}_3$
$1 - \alpha$	2	$\mathfrak{p}'_2$

All prime ideals of prime norm ≤ 47 appear as a divisor of one of the numbers in the table. The only exceptions are $\mathfrak{p}_{29} = (29, \alpha - 7)$ and $\mathfrak{p}_4$. For $\mathfrak{p}_{29}$ we observe that $\alpha - 7$ has norm $2^2 \cdot 23 \cdot 29$. For $\mathfrak{p}_4$ we remark that it divides the ideal (2). This leads to the factorizations

$$(\alpha - 7) = \mathfrak{p}_2'^2\mathfrak{p}'_{23}\mathfrak{p}_{29},$$
$$(2) = \mathfrak{p}_2\mathfrak{p}'_2\mathfrak{p}_4.$$

These factorizations together with the ones listed in Table III show inductively that the class of each of the prime ideals $\mathfrak{p}$ with $3 \leq N(\mathfrak{p}) \leq 47$ is in fact contained in the subgroup of ideal classes generated by primes of smaller norm. It follows that the ideal class group of O_F is generated by the primes of norm 2. Since $\mathfrak{p}_2'$ is principal, Cl_F is actually generated by the class of $\mathfrak{p}_2$ alone. Since $\mathfrak{p}_2\mathfrak{p}_3$ is equal to the principal ideal generated by α, the class group is also generated by $\mathfrak{p}_3$. The fact that $(3) = \mathfrak{p}_3^4$, implies that $\mathfrak{p}_2^4$ is principal. Indeed, we have $\mathfrak{p}_2^4 = (\frac{1}{3}\alpha^4) = (2\alpha^2 - \alpha - 2)$. This proves the proposition.

It follows that the class group is cyclic of order dividing 4. Attempts to find additional relations turn out to fail. This leads to the suspicion that the class group *is* actually cyclic of order 4 generated by $\mathfrak{p}_2$ or, equivalently, by $\mathfrak{p}_3$. In other words, we wonder whether

$$Cl_F \cong \mathbf{Z}/4\mathbf{Z}?$$

This is likely, but to *prove* this we need some information about the unit group O_F^*. Indeed, if the order of the class group were a proper divisor of 4, then $\mathfrak{p}_3^2$ would be principal, generated by $\beta \in O_F$ say. Since $\mathfrak{p}_3^4 = (3)$, this would mean that $\beta^2 = 3\varepsilon$ for some $\varepsilon \in O_F^*$. In order to be able to check this, we need to know something about ε. Fortunately, we do not need to know the full unit group O_F^*. It suffices to know generators for the unit group modulo squares. In section 4 we explain how to compute O_F^* modulo p-th powers for small primes p. As an application we prove in section 5 that the class group has order 4.

3. The unit group.

By Dirichlet's Unit Theorem, the rank of the unit group O_F^* is 2. Since F can be embedded into $\mathbf{R}$, the subgroup of roots of unity is equal to $\{\pm 1\}$. Our method to find other units, is to look for principal ideals (x) and (y) that have the same factorization into prime ideals. Then we know that x/y is in O_F^*. From our list of factored elements of the form $a + b\alpha$ with $a, b \in \mathbf{Z}$, we single out the following factorizations.

Table IV.

$a + b\alpha$	$N(a + b\alpha)$	
$1 - \alpha$	-2	$\mathfrak{p}_2'$
$1 + \alpha$	2^2	$\mathfrak{p}_2'^2$
$1 - 3\alpha$	-2^9	$\mathfrak{p}_2'^9$

We see that the principal ideal generated by $(1 - \alpha)^2$ has the same factorization as the ideal $(1 + \alpha)$. Therefore the quotient is a unit. Put

$$\varepsilon_1 = (1 - \alpha)^2/(1 + \alpha) = 7 - 6\alpha + \alpha^2 - \alpha^3.$$

Similarly, the principal ideal generated by $(1 + \alpha)^4(1 - \alpha)$ has the same factorization as the ideal $(1 - 3\alpha)$. A second unit is therefore given by

$$\varepsilon_2 = (1 + \alpha)^4(1 - \alpha)/(1 - 3\alpha) = 1 - \alpha^2 + \alpha^3.$$

Subsequent attempts to find more units always lead to units that are in the group U generated by -1, ε_1 and ε_2. For instance, the factorizations

$$(3+4\alpha) = \mathfrak{p}_3\mathfrak{p}_5, \qquad (3-\alpha) = {\mathfrak{p}_2'}^3\mathfrak{p}_3\mathfrak{p}_5, \qquad (1-\alpha) = \mathfrak{p}_2'$$

give rise to the unit $(1-\alpha)^3(3+4\alpha)/(3-\alpha)$ which turns out to be equal to $-\varepsilon_1\varepsilon_2$. Therefore, we wonder

$$O_F^* = U?$$

We suspect that the answer is yes, but proving rigorously that O_F^* is equal to U is not so easy. We do so in section 6. Solving the problem of section 2, i.e. proving that the class group of F is cyclic of order 4 is easier. We do this in section 5. The following computer calculation may convince us that indeed $O_F^* = U$ and $h_F = 4$, but it is not a proof.

Remark 3. If it were true that $U = O_F^*$, then the regulator R_F is given by

$$R_F \;=\; |\det\begin{pmatrix}\log|\phi_1(\epsilon_1)| & \log|\phi_2(\epsilon_1)|\\ \log|\phi_1(\epsilon_2)| & \log|\phi_2(\epsilon_2)|\end{pmatrix}| \;=\; 29.202215268966053595676604 81\ldots,$$

which is equal to the covolume of the unit lattice $L(O_F^*)$ divided by $\sqrt{2}$. If it also were true that $h_F = \#Cl(O_F)$ is equal to 4, then we can compute the residue of te zeta function of F in $s = 1$. It would be equal to

$$\frac{2^2\cdot 2\pi\cdot h_F R_F}{2\sqrt{402219}} \;=\; 2.31448495737317400142070565 5\ldots$$

On the other hand, if either U is a proper subgroup of O_F^* or if h_F is a proper divisor of 4, then the residue is k times smaller for some integer $k \geq 2$.

This is very unlikely. Indeed, we have

$$\frac{\zeta_F(s)}{\zeta(s)} = \frac{\prod_{\mathfrak{p}}(1-\frac{1}{N(\mathfrak{p})^s})}{\prod_p(1-\frac{1}{p^s})} = \prod_p \frac{\prod_{\mathfrak{p}|p}(1-\frac{1}{N(\mathfrak{p})^s})}{1-\frac{1}{p^s}}$$

and the Euler product converges for $s = 1$. Its limit is the residue of $\zeta_F(s)$ in $s = 1$ and is equal to

$$\prod_p \frac{1}{E_p(\frac{1}{p})},$$

were $E_p(X)$ is a polynomial which is 1 and $(1-X)^2$ for the ramified primes $p = 3$ and $p = 14897$ respectively.

Table VI.

$d_1, d_2, \ldots$	$E_p(X)$
$1,1,1,1$	$(1-X)^3$
$1,1,2$	$(1-X^2)(1-X)$
$1,3$	$1-X^3$
$2,2$	$(1-X^2)(1+X)$
4	$1+X+X^2+X^3$

For the other primes, E_p is a degree 3 polynomial that depends on the degrees $d_1, d_2, \ldots$ of the irreducible factors of f modulo p as in Table VI.

The rate of convergence is very slow. Under assumption of the Riemann Hypothesis for the zeta function of the normal closure of F, it can be proved that a partial product involving the primes $\leq X$ approximates the limit with a relative error of the order of magnitude $O(1/\sqrt{X})$. This is also what happens in practice. A direct evaluation of an approximation to the Euler product using the primes $p < 1000000$ gives the value $2.31427982\ldots$. The relative error is about 0.0001, which is bit better than the square root of 1000000. Given this numerical result, it is extremely unlikely that the actual residue is k times smaller than the partial product for some integer $k \geq 2$. It is almost certain that $U = O_F^*$ and $h_F = 4$. A rigorous proof is given in the next sections.

4. Units modulo p-th powers.

In this section we consider the following situation. The field F is the field defined above, and we have $U \subset O_F^*$ where

$$U = \langle -1, \varepsilon_1, \varepsilon_2 \rangle.$$

We try to prove that $O_F^* = U$, in which case $[O_F^* : U] = 1$. In this section we show how to check something weaker, namely that a given prime number p does not divide $[O_F^* : U]$. This kind of information plays a role the determination of the class group as well as the unit group.

The following algebraic result is useful.

Lemma 4. *Let N be a subgroup of a finitely generated abelian group M and let p be a prime number. Let V be an $\mathbf{F}_p$-vector space. If there exists a group homomorphism $h : M \longrightarrow V$ with the property that $\dim h(N) = \dim M/pM$, then we have the following.*
(a) The natural map $N/pN \longrightarrow M/pM$ is bijective;
(b) the index $[M : N]$ is finite and not divisible by p.

Proof. The homomorphism h factors through M/pM. Consider the following commutative diagram

$$\begin{array}{ccccc} N/pN & \longrightarrow & M/pM & & \\ \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle h} & & \\ h(N) & \subset & h(M) & \subset & V \end{array}$$

The vertical arrows are surjective. Since $\dim h(N) \leq \dim h(M) \leq \dim M/pM$, the hypothesis $\dim h(N) = \dim M/pM$ means that we have equality everywhere. Therefore $h(N) = h(M)$ and the map $h : M/pM \to h(M)$ is an isomorphism. It follows that the map $N/pN \longrightarrow M/pM$ is surjective.

Since M is a finitely generated group, we have $\dim N/pN \leq \dim M/pM$, so that the map $N/pN \longrightarrow M/pM$ is a bijection. This proves (a). The surjectivity of the map $N/pN \longrightarrow M/pM$ also implies that the finitely generated group $Q = M/N$ satisfies $Q/pQ = 0$. This means that Q is finite of order prime to p, which implies (b).

We apply Lemma 4 with M and N equal to the multiplicative group O_F^* and its subgroup U respectively. The homomorphism h is provided by the reductions modulo

suitable prime ideals of O_F. Indeed, for any prime ideal $\mathfrak{p}$ of O_F there is a natural homomorphism $O_F^* \longrightarrow k_\mathfrak{p}^*$. Here $k_\mathfrak{p}$ denotes the residue field $O_F/\mathfrak{p}$. If p is a prime number dividing $\#k_\mathfrak{p}^* = N(\mathfrak{p}) - 1$, we get a homomorphism

$$\phi_\mathfrak{p} : O_F^* \longrightarrow k_\mathfrak{p}^*/k_\mathfrak{p}^{*p} \cong \mathbf{Z}/p\mathbf{Z} = V.$$

By combining these homomorphisms for various prime ideals $\mathfrak{p}$, we get homomorphisms from O_F^* to $\mathbf{F}_p$-vector spaces V of higher dimension. In applications, one usually tries to use prime ideals $\mathfrak{p}$ of small norm.

Recall the following elementary fact.

Lemma 5. *Let q be a prime power and let l be a prime. If l does not divide $q-1$, then every element of $\mathbf{F}_q^*$ is an l-th power. If l divides $q-1$, then $a \in \mathbf{F}_q^*$ is an l-th power if and only if $a^{(q-1)/l} \equiv 1 \pmod{p}$.*

Proof. If l does not divide $q-1$, raising to the l-th power is an isomorphism $\mathbf{F}_q^* \to \mathbf{F}_q^*$. This proves the first statement. When l divides $q-1$, the map $\mathbf{F}_q^* \longrightarrow \mathbf{F}_q^*$ given by $a \mapsto a^{(q-1)/l}$ is a group homomorphism, that induces an isomorphism between $\mathbf{F}_q^*/\mathbf{F}_q^{*l}$ and the subgroup μ_l of l-th roots of unity of $\mathbf{F}_q^*$. This follows from the fact that $\mathbf{F}_q^*$ is a cyclic group. This proves the lemma.

Since -1 is a p-th power when p is odd, the com putation of $[O_F^* : U] \pmod{p}$ is bit simpler when p is odd. In this section we only deal with odd primes p. For $p = 2$, see the next section. The following proposition is used in the proof of Proposition 12.

Proposition 6. *The index $[O_F^* : U]$ is not divisible by the primes $p = 3$, 5, 7 and 11.*

Proof. We explain the case $p = 3$ in some detail. We apply Lemma 4 with $M = O_F^*$ and N equal to the subgroup generated by $-1, \varepsilon_1$ and ε_2. Since -1 is a cube, the $\mathbf{F}_3$-dimension of $O_F^*/{O_F^*}^3$ is 2. The residue fields of the primes $\mathfrak{p}_7 = (7, \alpha - 2)$ and $\mathfrak{p}_{13} = (13, \alpha - 5)$ are equal to $\mathbf{F}_7$ and $\mathbf{F}_{13}$ respectively. The orders of their multiplicative groups are divisible by 3. Therefore $V = \mathbf{F}_7^*/{\mathbf{F}_7^*}^3 \times \mathbf{F}_{13}^*/{\mathbf{F}_{13}^*}^3$is an $\mathbf{F}_3$-vector space of dimension 2. The map $h : M \longrightarrow V$ of Lemma 4 is the map

$$O_F^* \longrightarrow \mathbf{F}_7^*/{\mathbf{F}_7^*}^3 \times \mathbf{F}_{13}^*/{\mathbf{F}_{13}^*}^3$$

given by reduction modulo $\mathfrak{p}_7$ in the first coordinate and by reduction modulo $\mathfrak{p}_{13}$ in the second. We check that the image of U has dimension 2.

First we deal with $\mathfrak{p}_7$. It turns out that both units $\varepsilon_1 = (1-\alpha)^2/(1+\alpha)$ and $\varepsilon_2 = 1 - \alpha^2 + \alpha^3$ are congruent to 5 (mod $\mathfrak{p}_7$) . We use the isomorphism of Lemma 5 to compute the bijection $\mathbf{F}_7^*/{\mathbf{F}_7^*}^3 \cong \mu_3$, where μ_3 indicates the subgroup third roots of unity in $\mathbf{F}_7^*$. This means that we raise everything to the power $(7-1)/3 = 2$. For both units we obtain $5^2 = 4 \in \mu_3 \subset \mathbf{F}_7^*$. Finally, we choose a generator of the cyclic group μ_3 and use it to identify μ_3 with $\mathbf{Z}_3$. Since $\mu_3 = \{1, 2, 4\}$, we may choose 2 as a generator. Then the map $\mathbf{Z}/3\mathbf{Z} \longrightarrow \mu_3$ given by $x \mapsto 2^x$ is a group isomorphism. The element $4 \in \mu_3$ corresponds to the element $2 \in \mathbf{Z}/3\mathbf{Z}$. It follows that

$$h(\varepsilon_1) = \begin{pmatrix} 2 \\ 2 \end{pmatrix}.$$

For $\mathfrak{p}_{13}$ the computation is similar. The units ε_1 and ε_2 are congruent to 9 and 10 modulo $\mathfrak{p}_{13}$ respectively. We use Lemma 5 and raise everything to the power $(13-1)/3 = 4$. We get 9 and 3 respectively. The subgroup μ_3 of $\mathbf{F}_{13}^*$ is $\{1, 3, 9\}$. The bijection $\mathbf{Z}/3\mathbf{Z} \longrightarrow \mu_3$ given by $x \mapsto 3^x$ identifies the elements 9 and 3 of μ_3 with the elements 2 and 1 of $\mathbf{Z}/3\mathbf{Z}$. It follows that

$$h(\varepsilon_2) = \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

Since the matrix

$$\begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$$

is invertible modulo 3, the dimension of the image of U is 2 and Lemma 4 applies. It follows that 3 does not divide the index $[O_F^* : U]$.

The computation could have been done in other ways, by using different primes. For instance the order of the multiplicative group of the prime $\mathfrak{p}_4$ is also divisible by 3. It is easy to check that both units ε_1 and ε_2 have images congruent to $\alpha + 1 \pmod{\mathfrak{p}_4}$. So, we could have used $\mathfrak{p}_4$ instead of $\mathfrak{p}_7$. Choosing different isomorphisms between the various groups of 3rd roots of unity and $\mathbf{Z}/3\mathbf{Z}$, replaces the columns of the matrix by scalar multiples. It does not affect the rank of the matrix.

The cases $p = 5$, 7 and 11. For each of these primes the $\mathbf{F}_p$-dimension of O_F^*/O_F^{*p} is 2. For the prime 5 we use the prime ideals $\mathfrak{p}_{31} = (31, \alpha + 9)$ and $\mathfrak{p}'_{31} = (31, \alpha - 6)$. Both have residue fields $\mathbf{F}_{31}$ We reduce ε_1 and ε_2 modulo $\mathfrak{p}_{31}$ and $\mathfrak{p}'_{31}$ and map them to the subgroup $\mu_5 = \{1, 2, 4, 8, 16\}$ of $\mathbf{F}_{31}$ by raising them to the power $(31-1)/5 = 6$ as in Lemma 5. One checks that ε_1 and ε_2 are mapped to $(16, 8)$ and $(16, 1)$ respectively in $\mu_5 \times \mu_5$. Next we compute discrete logarithms with respect to the generator 2 of μ_5. In other words, we apply the inverse of the isomorphism $\mathbf{Z}/5\mathbf{Z} \to \mu_5$ given by $x \mapsto 2^x$. We find that the images of ε_1 and ε_2 in $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$ are the columns of the matrix

$$\begin{pmatrix} 4 & 4 \\ 3 & 0 \end{pmatrix}.$$

Since this matrix is invertible modulo 5, Lemma 4 implies that 5 does not divide the index $[O_F^* : U]$.

For the prime 7 we use the prime ideals $\mathfrak{p}_{43}$ and $\mathfrak{p}'_{43}$. The residue fields are both equal to $\mathbf{F}_{43}$. For the prime 11 we use the primes $\mathfrak{p}_{23}$ and $\mathfrak{p}'_{23}$. In both cases we find an invertible 2×2-matrix and may conclude that 7 and 11 do not divide $[O_F^* : U]$. We leave the calculations to the reader.

This proves the proposition.

5. Units modulo squares.

In this section we discuss the analogue of Proposition 6 of the previous section for the prime $p = 2$. There are a few small differences. First of all, in this case -1 is not a p-th power. It follows that the the $\mathbf{F}_2$-dimension of $O_F^*/{O_F^*}^3$ is 3 rather than 2.

For the prime $p = 2$, there are extra homomorphisms from O_F^* to $\mathbf{Z}/2\mathbf{Z}$, provided by the embeddings $\phi_i : F \longrightarrow \mathbf{R}$. These give rise to homomorphisms

$$O_F^* \longrightarrow \mathbf{R}^*/{\mathbf{R}^*}^2 \cong \mathbf{Z}/2\mathbf{Z}.$$

given by $\varepsilon \mapsto \text{sign}(\phi_i(\varepsilon))$. They are easy to compute.

The mages of ε_1 and ε_2 under $(\phi_1, \phi_2, \phi_3, \phi_4)$ in $F_{\mathbf{R}}$ are given by

$$\varepsilon_1 = \begin{pmatrix} 12.5236 \\ 0.0086 \\ -2.76 - 1.25i \\ -2.76 + 1.25i \end{pmatrix} \qquad \text{and} \qquad \varepsilon_2 = \begin{pmatrix} 0.0019 \\ 1.1754 \\ 11.91 + 17.09i \\ 11.91 - 17.09i \end{pmatrix}.$$

Proposition 7. *Let U be the subgroup of O_F^* generated by -1, ε_1 and ε_2. Then the index $[O_F^* : U]$ is not divisible by 2.*

Proof. We apply Lemma 4 with $M = O_F^*$ and $N = U$. Then $M/2M \cong O_F^*/{O_F^*}^2$ is a 3-dimensional $\mathbf{F}_2$-vector space. We construct a homomorphism h from M to an $\mathbf{F}_2$-vector space V using the first embedding $\phi_1 : F \hookrightarrow \mathbf{R}$ and the primes $\mathfrak{p}_5$, $\mathfrak{p}_7$ and $\mathfrak{p}_{13}$. The residue fields are $\mathbf{F}_5$, $\mathbf{F}_7$ and $\mathbf{F}_{13}$ respectively. The vector space appearing in Lemma 5 is

$$V = \mathbf{R}^*/{\mathbf{R}^*}^2 \times \mathbf{F}_5^*/{\mathbf{F}_5^*}^2 \times \mathbf{F}_7^*/{\mathbf{F}_7^*}^2 \times \mathbf{F}_{13}^*/{\mathbf{F}_{13}^*}^2.$$

It is a 4-dimensional $\mathbf{F}_2$-vector space. A small computation shows that the images of -1, ε_1 and ε_2 are the columns of the matrix

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

As an example we explain in some detail how to compute the second column of the matrix A above. This is the image of ε_1 in V. The first coordinate is zero, because $\phi_1(\varepsilon_1) = 12.5236$ is positive and therefore trivial in the group $\mathbf{R}^*/{\mathbf{R}^*}^2 \cong \mathbf{Z}/2\mathbf{Z}$. The second coordinate is given by reducing ε_1 modulo $\mathfrak{p}_5 = (5, \alpha + 2)$. The residue field $O_F/\mathfrak{p}_5$ is $\mathbf{F}_5$. We get $\varepsilon_1 = (1 - \alpha)^2/(1 + \alpha) \equiv (1 + 2)^2/(1 - 2) \equiv 1 \pmod{\mathfrak{p}_5}$, which is the trivial element of $\mathbf{F}_5^*/{\mathbf{F}_5^*}^2 \cong \mathbf{Z}/2\mathbf{Z}$.

The third coordinate is given by reducing ε_1 modulo $\mathfrak{p}_7 = (7, \alpha - 2)$. The residue field is $\mathbf{F}_7$. We get $\varepsilon_1 \equiv (1 - 2)^2/(1 + 2) \equiv 5 \pmod{\mathfrak{p}_7}$. The subgroup of squares of $\mathbf{F}_7^*$ is $\{1, 2, 4\}$. So, this time ε_1 is mapped to the non-trivial element of $\mathbf{F}_7^*/{\mathbf{F}_7^*}^2 \cong \mathbf{Z}/2\mathbf{Z}$. Finally, the fourth coordinate is determined by reducing ε_1 modulo $\mathfrak{p}_{13} = (13, \alpha - 5)$. The residue field is $\mathbf{F}_{13}$. We get $\varepsilon_1 \equiv (1 - 5)^2/(1 + 5) \equiv 7 \pmod{\mathfrak{p}_{13}}$. To determine the image in $\mathbf{F}_{13}^*/{\mathbf{F}_{13}^*}^2$, we need to decide whether 7 is a square modulo 13 or not. This can be done by listing all squares in $\mathbf{F}_{13}^*$, or by applying Lemma 5. Indeed, from $7^6 \equiv (-3)^3 \equiv -1 \pmod{13}$ it follows that 7 is not a square modulo 13.

Since the rank of A is 3, the condition of Lemma 4 is satisfied and we conclude that U generates O_F^* modulo squares and that the index $[O_F^* : U]$ is not divisible by 2.

Theorem 8. *The class group Cl_F is cyclic of order* 4.

Proof. We saw at the end of section 2 that it suffices to show that 3 is not of the form $u\beta^2$ for some $u \in O_F^*$ and some $\beta \in O_F$. We apply Lemma 5 with M equal to the multiplicative group

$$O_3^* = \{x \in F^* : \mathrm{ord}_{\mathfrak{p}}(x) = 0 \text{ for all primes } \mathfrak{p} \neq \mathfrak{p}_3\}.$$

Then O_F^* is contained in O_3^*. It is the kernel of the non-zero homomorphism $v : O_3^* \longrightarrow \mathbf{Z}$ given by $v : x \mapsto v_{\mathfrak{p}_3}(x)$. In other words, we have an exact sequence

$$0 \longrightarrow O_F^* \longrightarrow O_3^* \xrightarrow{v} \mathbf{Z}$$

This implies that O_3^* is isomorphic to $O_F^* \times \mathbf{Z}$ so that O_3^*/O_3^{*2} is isomorphic to $\mathbf{Z}/2\mathbf{Z}^4$ Moreover, 3 is in O_3^* and β, if it exists, it is also in O_3^*.

Let U_3 denote the subgroup of O_3^* generated by U and 3. We apply Lemma 5 with $p = 2$, with $M = O_3^*$ and $N = U_3$. We extend the homomorphism h of part (a) to the group O_3^*. This makes sense, since elements of O_3^* are not zero modulo $\mathfrak{p}_5$, $\mathfrak{p}_7$ or $\mathfrak{p}_{13}$. A small computation shows that the image of 3 in V is the vector

$$\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix},$$

which is *independent* of the columns of the matrix A above. Therefore, $h(N)$ has dimension 4 in this case. Lemma 5 implies that the map $U_3/U_3^2 \longrightarrow O_3^*/O_3^{*2}$ is bijective. It follows that 3 is *not* contained in the 3-dimensional subspace generated by -1, ε_1 and ε_2. In other words, 3 is not of the form $u\beta^2$ for some $u \in U$ and some $\beta \in O_F$, as required.

Two final comments on the computations involved in these proofs. We did not make use of the embedding ϕ_2 and the prime $\mathfrak{p}_3$, because they happen not to add any information. The prime $\mathfrak{p}_5$ gives rise to a zero row of the matrix A and is of no help for the proof of Proposition 7, but its presence is important for the proof of Theorem 8.

Remark 9. From the relations given in Table III one finds that the ideals of norm ≤ 73 are distributed over the four ideal classes in the following way. Here c denotes the class of the ideal $\mathfrak{p}_2$.

Table V.

class	
1	$\mathfrak{p}_2'$, $\mathfrak{p}_{47}$
c	$\mathfrak{p}_2$, $\mathfrak{p}_{19}$, $\mathfrak{p}_{23}$, $\mathfrak{p}_{29}'$, $\mathfrak{p}_{43}'$
c^2	$\mathfrak{p}_7$, $\mathfrak{p}_{23}'$, $\mathfrak{p}_{29}$, $\mathfrak{p}_{43}$
c^3	$\mathfrak{p}_3$, $\mathfrak{p}_4$, $\mathfrak{p}_5$, $\mathfrak{p}_{13}$, $\mathfrak{p}_{31}'$, $\mathfrak{p}_{31}$, $\mathfrak{p}_{41}$

6. The unit group.

In this section we prove that the unit group O_F^* is equal to the group U generated by -1, ε_1 and ε_2. The images of ε_1 and ε_2 under the *logarithmic* map $L : O_F^* \longrightarrow (\prod_\phi \mathbf{R})^0$ are

$$L(\varepsilon_1) = \begin{pmatrix} 2.5276 \\ -4.7494 \\ 1.1109 \\ 1.1109 \end{pmatrix} \qquad \text{and} \qquad L(\varepsilon_2) = \begin{pmatrix} -6.2345 \\ 0.1616 \\ 3.0364 \\ 3.0364 \end{pmatrix}.$$

Their lengths are 5.6048 and 7.5720 respectively. The cosine of the angle θ between them is -0.2304. It follows that the covolume of the rank 2 lattice generated by the vectors of logarithms of ε_1 and ε_2 is

$$\|L(\varepsilon_1)\|\|(L(\varepsilon_2)\|\sin(\theta) = 41.2981.$$

The vectors $L(\varepsilon_1)$ and $L(\varepsilon_2)$ are linearly independent. This agrees with the fact that ε_1 and ε_2 generate a subgroup U of O_F^* of rank 2 and that U has finite index m in O_F^*.

We want to prove that $m = 1$. The following inequality is useful.

Lemma 10. *Let $n \in \mathbf{Z}_{>0}$, let $r \in \mathbf{R}_{>0}$ and suppose $x_1, \ldots, x_n \in \mathbf{R}$ satisfy $\sum_{i=1}^n x_i = 0$ and $\sum_{i=1}^n x_i^2 \leq r^2$. Then we have $\sum_{i=1}^n e^{2x_i} \leq e^{2r} + n - 1 - 2r$.*

Proof. For $i = 1, \ldots, n$ put $y_i = x_i/r$. Then we have $\sum_{i=1}^n y_i^2 \leq 1$ and hence $|y_i| \leq 1$ for $i = 1, \ldots, n$. It follows that $y_1^k + \ldots + y_n^k \leq y_1^2 + \ldots + y_n^2 \leq 1$ for $k \geq 2$. Let $f(x)$ denote the function $e^{2rx} - 2rx - 1$. Since the Taylor series expansion around 0 of $f(x)$ has no constant or linear term, while the higher degree terms have positive coefficients, we have $\sum_{i=1}^n f(y_i) \leq f(1)$. Therefore we have

$$\sum_{i=1}^n e^{2ry_i} \leq e^{2r} - 2r - 1 + 2r \sum_{i=1}^n y_i + n.$$

Since $\sum_{i=1}^n y_i$ vanishes, the result follows.

Proposition 11. *If $[O_F^* : U] \geq m$, then there exists $\eta \in O_F^*$ with $\eta \neq \pm 1$ and*

$$\|\eta\|^2 \leq \exp(14.502/\sqrt{m}) + 3 - 14.502/\sqrt{m}.$$

Proof. The covolume of the logarithmic unit lattice $L(O_F^*)$ is at most $41.2981/m$. By Minkowki's Theorem, a disk centered in the origin of $\mathbf{R}^2$ with radius r satisfying $\pi r^2 \geq 4 \cdot 41.2981/m$ contains a non-zero point of $L(O_F^*)$. This means that there exists a unit $\eta \neq \pm 1$ for which

$$\sum_{i=1}^4 (\log|\phi_i(\eta)|)^2 \leq 4 \cdot 41.2981/m\pi.$$

Since $\sum_{i=1}^4 \log|\phi_i(\eta)| = 0$, Lemma 10 applies with $r = \sqrt{4 \cdot 41.2981/m\pi} = 7.251/\sqrt{m}$ and the bound for $\|\eta\|^2$ follows.

On the other hand, we have that $\eta = \lambda_1 + \lambda_2\alpha + \lambda_3\alpha^2 + \lambda_4\alpha^3$ with $\lambda_i \in \mathbf{Z}$. In section 1 we saw that this means that $\|\eta\|^2 = Q(\lambda_1, \lambda_2\lambda_3, \lambda_4)$ where Q is the quadratic form given by

$$\begin{aligned} Q(X_1, X_2, X_3, X_4) \; =& 4(X_1 - 3X_3 + \tfrac{9}{4}X_4)^2 + 15.8644(X_2 - 0.1031\, X_3 - 5.9921\, X_4)^2 \\ &+ 63.8911(X_3 + 0.0019\, X_4)^2 + 99.2057\, X_4^2. \end{aligned}$$

In principle, it is possible to enumerate all $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) \in \mathbf{Z}^4$ for which $Q(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ is at most $\exp(14.502/\sqrt{m}) + 3 - 14.502/\sqrt{m}$. If it turns out that none of the corresponding elements in O_F has norm ± 1, then we know that $U = O_F^*$ and we are done.

But this is a cumbersome computation if the upper bound is large. The larger the lower bound m of Proposition 11 is, the better is the upper bound for $\|\eta\|^2 = Q(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$. Here is a table.

m	$\|\eta\|^2 \leq$
3	4322.076
5	652.075
7	237.663
11	77.8703
13	54.7978

Theorem 12. *The unit group O_F^* is generated by -1, ε_1 and ε_2.*

Proof. Suppose that $O_F^* \neq U$. Propositions 6 and 7 say that $[O_F^* : U]$ is not divisible by the primes $p \leq 11$. It follows that we can take $m = 13$ in Proposition 11. It follows that there exist $\lambda_1, \ldots, \lambda_4 \in \mathbf{Z}$ for which $\eta = \lambda_1 + \lambda_2\alpha + \lambda_3\alpha^2 + \lambda_4\alpha^3$ is a unit $\neq \pm 1$ and for which $\|\eta\|^2 = Q(\lambda_1, \lambda_2, \lambda_3, \lambda_4) \leq 54.7978$. Here Q is the quadratic form of section 1. Since

$$\begin{aligned} \|\eta\|^2 = Q(\lambda_1, \lambda_2, \lambda_3, \lambda_4) &= \\ = 4(\lambda_1 - 3\lambda_3 + \tfrac{9}{4}\lambda_4)^2 &+ 15.8644(\lambda_2 - 0.1031\, \lambda_3 - 5.9921\, \lambda_4)^2 \\ + 63.8911(\lambda_3 + 0.0019\, \lambda_4)^2 &+ 99.2057\, \lambda_4^2. \end{aligned}$$

we have $\lambda_3 = \lambda_4 = 0$. It follows that

$$\|\eta\|^2 = 4\lambda_1^2 + 15.864\lambda_2^2 < 54.810,$$

and hence $-1 \leq \lambda_2 \leq 1$. Since $\eta \notin \mathbf{Z}$ and since we may multiply η by -1, we may assume that $\lambda_2 = 1$. Then $\lambda_1^2 < (54.810 - 15.864)/4 = 9.74$ and hence $|\lambda_1| \leq 3$ However, it follows from the computations in section 1 that $\alpha - \lambda_1$ does not have norm ± 1 when $\lambda_1 \in \{-3, -2, -1, 0, 1, 2, 3\}$. Therefore η does not exist and we obtain a contradiction.

This means that $O_F^* = U$ as required.

The choice of m in the proof of Theorem 12 is somewhat arbitrary. If we decided to consider fewer primes in section 4, we would end up with a larger value for m. This means that the upper bound for $Q(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ in Proposition 11 is larger, so that we need to check more quadruples $(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$. If we deal with more primes in section 4, it is the other way around.