THE SPLITTING FIELD OF $X^3 - 2$ OVER $\mathbf{Q}$

KEITH CONRAD

In this note, we calculate all the basic invariants of the number field

$$K = \mathbf{Q}(\sqrt[3]{2}, \omega),$$

where $\omega = (-1 + \sqrt{-3})/2$ is a primitive cube root of unity. For example, the unit group has rank 2 by the Dirichlet Unit Theorem, and we'll find a basis.

Here is the notation for the fields and Galois groups to be used. Let

$$\begin{aligned} k &= \mathbf{Q}(\sqrt[3]{2}), \\ K &= \mathbf{Q}(\sqrt[3]{2}, \omega), \\ F &= \mathbf{Q}(\omega) = \mathbf{Q}(\sqrt{-3}), \\ G &= \mathrm{Gal}(K/\mathbf{Q}) \cong S_3, \\ N &= \mathrm{Gal}(K/F) \cong A_3, \\ H &= \mathrm{Gal}(K/k). \end{aligned}$$

First we work out the basic invariants for the fields F and k.

Theorem 1. *The field $F = \mathbf{Q}(\omega)$ has ring of integers $\mathbf{Z}[\omega]$, class number 1, discriminant -3, and unit group $\{\pm 1, \pm\omega, \pm\omega^2\}$. The ramified prime 3 factors as $3 = -(\sqrt{-3})^2$. For $p \neq 3$, the way p factors in $\mathbf{Z}[\omega] = \mathbf{Z}[X]/(X^2 + X + 1)$ is identical to the way $X^2 + X + 1$ factors mod p, so p splits if $p \equiv 1 \bmod 3$ and p stays prime if $p \equiv 2 \bmod 3$.*

We now turn to the field k, which will be discussed in more detail.

Though we will show below that $\mathcal{O}_k = \mathbf{Z}[\sqrt[3]{2}]$, the inclusion $\mathbf{Z}[\sqrt[3]{2}] \subset \mathcal{O}_k$ already is useful for computing the class number. It tells us that $|\operatorname{disc}(k)| \leq |\operatorname{disc}(1, \sqrt[3]{2}, \sqrt[3]{4})| = 108 = 2^2 3^3$, so the Minkowski bound for k is at most

$$\frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{|\operatorname{disc}(k)|} = \frac{16\sqrt{3}}{3\pi} \approx 2.94.$$

In $\mathcal{O}_k$, the rational prime 2 has the principal prime factorization $(2) = (\sqrt[3]{2})^3$, so k has class number 1: the ring $\mathcal{O}_k$ has unique factorization.

Next we show $\mathcal{O}_k = \mathbf{Z}[\sqrt[3]{2}]$.

Let $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ be an algebraic integer, with a, b, c all rational. Computing $\mathrm{Tr}_{k/\mathbf{Q}}$ of α, $\alpha\sqrt[3]{2}$, and $\alpha\sqrt[3]{4}$ we see $3a, 6b, 6c \in \mathbf{Z}$. So the denominators of a, b, and c involve at most 2 and 3. To show 2 and 3 do not appear in the denominator, we consider the situation p-adically for $p = 2$ and $p = 3$.

Lemma 1. *Let L/L' be an extension of local fields. If L/L' is unramified and a is any integer of L which generates the residue field extension, then $\mathcal{O}_L = \mathcal{O}_{L'}[a]$. If L/L' is totally ramified and λ is any prime of L, then $\mathcal{O}_L = \mathcal{O}_{L'}[\lambda]$.*

Proof. By [2, Prop. 3, p. 59], which can be applied since the residue field extension is separable, if λ is any prime of L and a is any integer of L which generates the residue field

of L over that of L', then powers of a or powers of $a+\lambda$ generate $\mathcal{O}_L$ as an $\mathcal{O}_{L'}$-algebra. When L/L' is unramified, let λ be a prime of L'. When L/L' is totally ramified, let $a = 1$ (or 0). □

We apply this with $L' = \mathbf{Q}_2$ or $\mathbf{Q}_3$ and $L = L'(\sqrt[3]{2})$. Since $X^3 - 2$ is Eisenstein in $\mathbf{Q}_2[X]$ and $(X-1)^3 - 2 = X^3 - 3X^2 + 3X - 3$ is Eisenstein in $\mathbf{Q}_3[X]$, by Lemma 1 the ring of integers of $\mathbf{Q}_2(\sqrt[3]{2})$ is $\mathbf{Z}_2[\sqrt[3]{2}]$ and the ring of integers of $\mathbf{Q}_3(\sqrt[3]{2}) = \mathbf{Q}_3(1+\sqrt[3]{2})$ is $\mathbf{Z}_3[1+\sqrt[3]{2}] = \mathbf{Z}_3[\sqrt[3]{2}]$.

Using this to calculate the ring of integers of $\mathbf{Q}(\sqrt[3]{2})$, we see that the coefficients of α have denominators prime to 2 and 3, hence $\mathcal{O}_k = \mathbf{Z}[\sqrt[3]{2}]$ and

$$\mathrm{disc}(k) = \mathrm{disc}(1, \sqrt[3]{2}, \sqrt[3]{4}) = -108$$

For a different approach (pun intended) to calculating the integers of k, see [2, Example, pp. 67-68].

We now turn to factorization of rational primes in $\mathcal{O}_k$. First let's treat the ramified primes, 2 and 3.

In $\mathbf{Q}_3(\sqrt[3]{2})$, 3 is totally ramified and $1+\sqrt[3]{2}$ is a prime element. This number also generates the global prime ideal factor of 3 in $\mathcal{O}_k$. Indeed, let $\pi \stackrel{\mathrm{def}}{=} 1+\sqrt[3]{2}$ be the root of $(X-1)^3 - 2$ in k. Expanding this polynomial and substituting $X = \pi$, we see

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

The number $u \stackrel{\mathrm{def}}{=} 1 + \sqrt[3]{2} + \sqrt[3]{4}$ has inverse $v \stackrel{\mathrm{def}}{=} \sqrt[3]{2} - 1$, so $u \in \mathcal{O}_k^\times$ and

$$3 = \pi^3 v. \tag{2}$$

Two calculations which we'll be using later are

$$\pi v = \sqrt[3]{4} - 1, \quad \pi^2 v = 1 - \sqrt[3]{2} + \sqrt[3]{4}. \tag{3}$$

The way p factors in $\mathbf{Z}[\sqrt[3]{2}]$ can be described by how $X^3 - 2$ factors mod p [2, Prop. 25, p. 27]. We need to know when 2 is a cube mod p and, if so (and $p \neq 2$), when there is a primitive cube root of unity mod p. The latter condition (for $p \neq 3$) is the same as determining when -3 is a square mod p, which by quadratic reciprocity occurs when $p \equiv 1 \bmod 3$. (Alternatively, that $\sqrt{-3} \in \mathbf{Z}/p\mathbf{Z} \Leftrightarrow (\mathbf{Z}/p\mathbf{Z})^\times$ contains an element of order 3, i.e. that $3|p-1$, proves a particular case of quadratic reciprocity: $(\frac{-3}{p}) = (\frac{p}{3})$.)

Now we factor primes $p \geq 5$ (so p is unramified).

If $p \equiv 2 \bmod 3$, then 2 is a cube mod p and there is no primitive cube root of unity in $\mathbf{Z}/p\mathbf{Z}$, so (since $h(k) = 1$)

$$(p) = (x_1)(x_2), \quad \mathrm{N}(x_1) = p, \ \mathrm{N}(x_2) = p^2.$$

Here, N denotes the norm of an ideal. Passing to norms of elements, since -1 is a norm from k we can choose suitable unit multiples so $p = x_1 x_2$ where $p = \mathrm{N}_{k/\mathbf{Q}}(x_1)$, $p^2 = \mathrm{N}_{k/\mathbf{Q}}(x_2)$. For example,

$$5 = (1+\sqrt[3]{4})(1 + 2\sqrt[3]{4} - \sqrt[3]{4}).$$

If $p \equiv 1 \bmod 3$ and $2^{(p-1)/3} \equiv 1 \bmod p$ (the smallest such p is 31) then $X^3 - 2$ splits completely mod p and

$$p = x_1 x_2 x_3, \quad \mathrm{N}_{k/\mathbf{Q}}(x_i) = p.$$

If $p \equiv 1 \bmod 3$ and $2^{(p-1)/3} \not\equiv 1 \bmod p$ then $X^3 - 2$ is irreducible mod p and p is prime in $\mathcal{O}_k$.

What is the unit group of $\mathbf{Z}[\sqrt[3]{2}]$? The only roots of unity are ± 1, and by Dirichlet the unit group has rank 1, so there is a single fundamental unit > 1. We already have found a unit greater than 1, namely u, and happily this turns out to be the fundamental unit. To

prove this, we'll show u is less than the square of the fundamental unit, so it must equal the fundamental unit.

(The unit u is not so hard to discover independently of any considerations of how 3 factors, which was the way we came across it. The norm form for k is

$$\mathrm{N}_{k/\mathbf{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc. \tag{4}$$

Glancing at the coefficients $1, 2, 4, -6$ on the right hand side, we see they add up to 1, so $1 + \sqrt[3]{2} + \sqrt[3]{4}$ is a unit of $\mathbf{Z}[\sqrt[3]{2}]$, with norm 1.)

Lemma 2. *Let $k/\mathbf{Q}$ be any cubic extension which is not Galois, with negative discriminant d, i.e. k has only one real embedding. View k as a subfield of $\mathbf{R}$ by its unique real embedding. Then for the fundamental unit $U > 1$ of $\mathcal{O}_k$, $|d|/4 < U^3 + 7$.*

Proof. Let $\sigma\colon k \to \mathbf{C}$ be one of the complex embeddings of k, so $\mathrm{N}_{k/\mathbf{Q}}(U) = U\sigma(U)\overline{\sigma}(U) = U|\sigma(U)|^2 > 0$, so $\mathrm{N}_{k/\mathbf{Q}}(U) = 1$.

Let $x = |\sigma(U)| = \frac{1}{\sqrt{U}} \in (0, 1)$. Write

$$\sigma(U) = xe^{iy}, \quad \overline{\sigma}(U) = xe^{-iy}, \quad U = \frac{1}{x^2}.$$

Since $\mathbf{Z}[U] \subset \mathcal{O}_k$, $|d| \leq |\operatorname{disc}(1, U, U^2)|$. We calculate the latter:

$$\begin{aligned}
\operatorname{disc}(1, U, U^2) &= \begin{vmatrix} 1 & U & U^2 \\ 1 & \sigma(U) & \sigma(U)^2 \\ 1 & \overline{\sigma}(U) & \overline{\sigma}(U)^2 \end{vmatrix}^2 \\
&= ((\overline{\sigma}(U) - \sigma(U))(\overline{\sigma}(U) - U)(\sigma(U) - U))^2 \\
&= -4\sin^2(y)(x^3 + 1/x^3 - 2\cos y)^2 \\
&< 0.
\end{aligned}$$

Taking absolute values,

$$\begin{aligned}
\frac{1}{4}|d| &\leq \sin^2(y)(x^3 + 1/x^3 - 2\cos y)^2 \\
&= (1 - c^2)(z - 2c)^2 \quad (c = \cos y,\ z = x^3 + 1/x^3 > 2) \\
&= (z^2 - 4cz + 4c^2)(1 - c^2) \\
&= z^2 - c^2z^2 - 4cz(1 - c^2) + 4c^2(1 - c^2) \\
&= z^2 - (cz + 2(1 - c^2))^2 + 4(1 - c^2)^2 + 4c^2(1 - c^2) \\
&= z^2 + 4 - (cz + 2(1 - c^2))^2 \\
&< z^2 + 4 \\
&= x^6 + 6 + \frac{1}{x^6} \\
&= U^3 + 6 + x^6 \\
&< U^3 + 7.
\end{aligned}$$

□

Applying this to $k = \mathbf{Q}(\sqrt[3]{2})$, the fundamental unit $U > 1$ of $\mathcal{O}_k$ satisfies $108/4 < U^3 + 7$, so $U > 2$, hence $U^2 > 4 > 1 + \sqrt[3]{2} + \sqrt[3]{4} = u$. Thus $U = u$.

By an explicit calculation, $\operatorname{disc}(1, u, u^2) = -108$ so $\mathbf{Z}[u] = \mathbf{Z}[\sqrt[3]{2}]$, which also follows from the transition matrix from $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ to $\{1, u, u^2\}$ having determinant -1; explicitly,

$\sqrt[3]{2} = u^2 - 3u + 2$. The minimal polynomial for u over $\mathbf{Q}$ can be found as follows:

$$u = \frac{1}{\sqrt[3]{2} - 1} \Rightarrow \left(\frac{1}{u} + 1\right)^3 = 2 \Rightarrow u^3 - 3u^2 - 3u - 1 = 0. \tag{5}$$

Theorem 2. *The field $\mathbf{Q}(\sqrt[3]{2})$ has ring of integers $\mathbf{Z}[\sqrt[3]{2}]$, class number 1, discriminant $-2^2 3^3$, unit group $\pm u^{\mathbf{Z}}$ where $u = 1 + \sqrt[3]{2} + \sqrt[3]{4}$. The ramified primes 2 and 3 factor as $2 = (\sqrt[3]{2})^3$, $3 = \pi^3 v$ where $\pi = 1 + \sqrt[3]{2}$ and $v = 1/u = \sqrt[3]{2} - 1$. Also*

$$\mathbf{Z}[\sqrt[3]{2}] = \mathbf{Z}[\pi] = \mathbf{Z}[u]$$

and the minimal polynomials of π and u are

$$T^3 - 3T^2 + 3T - 3, \quad T^3 - 3T^2 - 3T - 1.$$

Now we turn our attention to the field $K = \mathbf{Q}(\sqrt[3]{2}, \omega)$. It is the composite of F and k, so the only rational primes which ramify in K are 2 and 3. Let's determine how these primes factor in K.

Since 2 totally ramifies in k with ramification index 3 and its residue field degree in F is 2, we see $(2) = (\sqrt[3]{2})^3$ is the prime factorization of 2 in K: $(\sqrt[3]{2})$ stays prime when extended from k to K. (Locally, $\mathbf{Q}_2(\sqrt[3]{2}, \omega)$ is obtained from $\mathbf{Q}_2(\sqrt[3]{2})$ by adjoining a root of unity of order prime to 2, so it is unramified and $\sqrt[3]{2}$ stays prime in the splitting field.)

Since 3 totally ramifies in F and in k with respective ramification indices 2 and 3, it must totally ramify in K: $3\mathcal{O}_K = \mathfrak{P}^6$.

Is $\mathfrak{P}$ principal? Extending both (principal) factorizations of 3 in k and in F to K, we have

$$\mathfrak{P}^6 = (\sqrt{-3})^2 = (\pi)^3.$$

Therefore $\mathfrak{P}^3 = (\sqrt{-3})$ and $\mathfrak{P}^2 = (\pi)$. So $\mathfrak{P} = (\sqrt{-3}/\pi)$ is principal. We let $\eta \stackrel{\text{def}}{=} \sqrt{-3}/\pi$, so by (2) and (3)

$$\eta^2 = -\pi v = 1 - \sqrt[3]{4}.$$

Thus $(\eta^2 - 1)^3 = -4$, so η is a root of

$$T^6 - 3T^4 + 3T^2 + 3, \tag{6}$$

which is Eisenstein with respect to 3, as expected.

Explicitly,

$$\begin{aligned} \eta = \frac{\sqrt{-3}\pi^2 v}{3} &= \frac{(2\omega + 1)(1 - \sqrt[3]{2} + \sqrt[3]{4})}{3} \\ &= \frac{1 - \sqrt[3]{2} + \sqrt[3]{4}}{3} + \frac{2(1 - \sqrt[3]{2} + \sqrt[3]{4})}{3}\omega. \end{aligned}$$

The element η does not lie in $\mathbf{Z}[\sqrt[3]{2}, \omega]$, so this is not the full ring of integers. We'll see later that $\mathcal{O}_K \neq \mathbf{Z}[\eta]$ either.

To determine the class number of K, we want to compute the Minkowski bound. In lieu of knowing the discriminant of K, we can use the upper bound

$$|\operatorname{disc}(K)| \leq |\operatorname{disc}(1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{4})| = 2^4 3^9$$

to get

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\operatorname{disc}(K)|} \leq \frac{320\sqrt{3}}{\pi^3} \approx 17.87.$$

So we want to factor all (positive) rational primes ≤ 17 into prime factors in K.

We've already factored 2 and 3, so we now need to factor $p = 5$, 7, 11, 13, and 17. All prime ideal factors of p in K are Galois-conjugate, so p factors principally when there is at least one principal prime ideal factor.

Let's combine information about how $p \neq 2, 3$ factors (principally!) in F and k to make conclusions about factorization in K.

Recall that in F,

$$p \equiv 1 \bmod 3 \Rightarrow p = \alpha\overline{\alpha}, \quad p \equiv 2 \bmod 3 \Rightarrow p \text{ inert}$$

and in k

$$\begin{aligned} p \equiv 2 \bmod 3 &\Rightarrow (p) = (x_1)(x_2),\ \mathrm{N}(x_1) = p,\ \mathrm{N}(x_2) = p^2, \\ p \equiv 1 \bmod 3,\ 2^{(p-1)/3} \equiv 1 \bmod 3 &\Rightarrow (p) = (x_1)(x_2)(x_3),\ \mathrm{N}(x_i) = p, \\ p \equiv 1 \bmod 3,\ 2^{(p-1)/3} \not\equiv 1 \bmod 3 &\Rightarrow p \text{ inert}. \end{aligned}$$

For a prime $p \neq 2, 3$ in K we have $f_p g_p = 6$. If $p \equiv 2 \bmod 3$, then by looking in k we have $2|f_p$, $g_p \geq 2$. Therefore $g_p = 3$, so the ideal (x_1) over p of degree 1 stays prime in K, so p factors principally. If $p \equiv 1 \bmod 3$ and 2 mod p is not a cube, then looking in F shows $g_p \geq 2$ while looking in k shows $3|f_p$, so $f_p = 3$, $g_p = 2$ and $(\alpha), (\overline{\alpha})$ stay prime in K, so p factors principally in K.

Happily, for all primes $p \leq 17$ which are $\equiv 1 \bmod 3$, 2 mod p is not a cube. Thus all primes ≤ 17 factor principally in K and $h(K) = 1$.

Though we didn't need to factor any rational primes ≥ 5 explicitly to determine $h(K)$, it may be of interest to see some examples. Here is a list of explicit factorizations in K for $p \leq 17$. They were all found by hand, without using the computer. The trickiest one is factoring 11, which arose from solving the norm form equation $\mathrm{N}_{k/\mathbf{Q}}(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = 11$ by making guesses, using (4). All factorizations below are numerical, rather than into ideals.

$$\begin{aligned} 2 &= (\sqrt[3]{2})^3, \\ 3 &= -\eta^6 u^2, \\ 5 &= (1 + \sqrt[3]{4})(1 + \sqrt[3]{4}\omega)(1 + \sqrt[3]{4}\omega^2), \\ 7 &= (2 + \sqrt{-3})(2 - \sqrt{-3}) \\ 11 &= (3 + 2\sqrt[3]{2} + \sqrt[3]{4})(3 + 2\sqrt[3]{2}\omega + \sqrt[3]{4}\omega^2)(3 + 2\sqrt[3]{2}\omega^2 + \sqrt[3]{4}\omega), \\ 13 &= (4 + \omega)(4 + \omega^2) \\ 17 &= (1 + 2\sqrt[3]{2})(1 + 2\sqrt[3]{2}\omega)(1 + 2\sqrt[3]{2}\omega^2). \end{aligned}$$

Now we turn to a calculation of the discriminant of K. The only prime factors are 2 and 3. Let's compute each contribution locally. There is only one prime above 2 and 3 in k and K, so denote the completion at such a prime as K_p and k_p for $p = 2, 3$.

Using $\sim$ to denote equality up to multiplication by a unit in the integer ring of the local field,

$$\begin{aligned} \mathrm{disc}(K_2/\mathbf{Q}_2) &= \mathrm{N}_{K_2/k_2}(\mathrm{disc}(K_2/k_2))\,\mathrm{disc}(k_2/\mathbf{Q}_2)^2 \\ &\sim \mathrm{disc}(k_2/\mathbf{Q}_2)^2 \text{ since } K_2/k_2 \text{ is unramified} \\ &\sim \mathrm{N}_{k_2/\mathbf{Q}_2}(3(\sqrt[3]{2})^2)^2 \\ &\sim (\mathrm{N}_{k_2/\mathbf{Q}_2}(\sqrt[3]{2}))^4 \\ &= 2^4. \end{aligned}$$

The integers of $\mathbf{Q}_3(\sqrt[3]{2}, \omega)$ are $\mathbf{Z}_3[\eta]$, so by (6)

$$\begin{aligned} \mathrm{disc}(K_3/\mathbf{Q}_3) &\sim \mathrm{N}_{K_3/\mathbf{Q}_3}(6\eta^5 - 12\eta^3 + 6\eta) \\ &= 6^6 \,\mathrm{N}_{K_3/\mathbf{Q}_3}(\eta)\,\mathrm{N}_{K_3/\mathbf{Q}_3}(\eta^4 - 2\eta^2 + 1) \\ &\sim 3^6 \cdot 3 \cdot 1 \\ &\sim 3^7. \end{aligned}$$

Thus $\mathrm{disc}(K) = (-1)^{r_2}2^4 3^7 = -14992$. For instance, since $\mathrm{disc}(\mathbf{Z}[\eta]) = -2^{14}3^7$, $\mathcal{O}_K \neq \mathbf{Z}[\eta]$. (Rather than compute the entire discriminant of $\mathbf{Z}[\eta]$, we can note that the 3-adic computation applies globally also, and the 2^6 term which arises is too large a power of 2.) Also, the true Minkowski bound for K is

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\,\mathrm{disc}(K)|} = \frac{320\sqrt{3}}{3\pi^3} \approx 5.96,$$

so we only need to check how 2, 3, and 5 factor to get $h(K) = 1$, not all primes up to 17.

Now we calculate a $\mathbf{Z}$-basis for the ring of integers of K. Since we already know the discriminant, a putative basis can be checked by verifying it has the right discriminant. This is how the candidate power basis $\{1, \eta, \ldots, \eta^5\}$ was ruled out.

It turns out there *is* a power basis for $\mathcal{O}_K$, but rather than pull it out of nowhere, we first approach the problem similarly to the computation of the ring of integers in quadratic fields, viewing $K = k(\omega)$ as a quadratic extension of the real subfield k.

Let $x = a + b\omega \in \mathcal{O}_K$, where $a, b \in k$. As with quadratic extensions of $\mathbf{Q}$, we get information about a and b by taking traces. Since $\mathrm{Tr}_{K/k}(x) = 2a - b \in \mathbf{Z}[\sqrt[3]{2}]$ and $\mathrm{Tr}_{K/k}(x\omega) = -a - b \in \mathbf{Z}[\sqrt[3]{2}]$, we see

$$3a,\ 3b \in \mathbf{Z}[\sqrt[3]{2}].$$

Since

$$\begin{aligned} x \in \mathcal{O}_K &\Leftrightarrow \mathrm{Tr}_{K/k}(x), \mathrm{N}_{K/k}(x) \in \mathbf{Z}[\sqrt[3]{2}] \\ &\Leftrightarrow 2a - b, a^2 - ab + b^2 \in \mathbf{Z}[\sqrt[3]{2}] \end{aligned}$$

and $2a - b = 3a - (a + b)$, $a^2 - ab + b^2 = (a + b)^2 - 3ab$, we see

$$x \in \mathcal{O}_K \Leftrightarrow 3a,\ a + b,\ 3ab \in \mathbf{Z}[\sqrt[3]{2}].$$

Let $a = r/3, b = s/3$. Then $x \in \mathcal{O}_K$ precisely when $r, s \in \mathbf{Z}[\sqrt[3]{2}]$ and $r + s \equiv 0, rs \equiv 0$ in $\mathbf{Z}[\sqrt[3]{2}]/3$, which is the same as $r + s \equiv 0, s^2 \equiv 0 \bmod 3$.

In $\mathbf{Z}[\sqrt[3]{2}]$,

$$3|s^2 \Leftrightarrow \pi^3|s^2 \Leftrightarrow \pi^2|s,$$

so $r = -s + 3\alpha, s = \pi^2\beta$. Thus the algebraic integers of K are numbers of the form

$$\begin{aligned} \frac{-\pi^2\beta + 3\alpha}{3} + \frac{\pi^2\beta}{3}\omega &= \alpha + \pi^2\beta\frac{\omega - 1}{3} \\ &= \alpha + \beta u\frac{\omega - 1}{\pi}. \end{aligned}$$

In particular this implies $\theta \stackrel{\mathrm{def}}{=} (\omega - 1)/\pi$ is an algebraic integer, and

$$\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{2}] \oplus \mathbf{Z}[\sqrt[3]{2}]\theta = \mathbf{Z} \oplus \mathbf{Z}\sqrt[3]{2} \oplus \mathbf{Z}\sqrt[3]{4} \oplus \mathbf{Z}\theta \oplus \mathbf{Z}\sqrt[3]{2}\theta \oplus \mathbf{Z}\sqrt[3]{4}\theta. \tag{7}$$

Here is a more explicit formula for θ:

$$\begin{aligned}\theta &= \frac{(\omega-1)\pi^2 v}{3} \\ &= \frac{(\omega-1)(1-\sqrt[3]{2}+\sqrt[3]{4})}{3} \\ &= -\frac{1-\sqrt[3]{2}+\sqrt[3]{4}}{3} + \frac{1-\sqrt[3]{2}+\sqrt[3]{4}}{3}\omega.\end{aligned}$$

This looks similar to η, and in fact $\omega\theta = -\eta$.

We didn't actually use the fact that $\mathbf{Z}[\sqrt[3]{2}]$ is a PID in the construction of the $\mathbf{Z}$-basis for $\mathcal{O}_K$, only that the lone (totally ramified) prime ideal factor of (3) is principal.

To find the minimal polynomial for θ over $\mathbf{Q}$, note by (1) that $1/\pi$ is a root of $3T^3 - 3T^2 + 3T - 1$, so of $T^3 - T^2 + T - 1/3$. Replacing T by $T/(\omega-1)$ and clearing the denominators shows θ is a root of

$$g(T) = T^3 - (\omega-1)T^2 + (\omega-1)^2 T - \frac{(\omega-1)^3}{3} = T^3 + (1-\omega)T^2 - 3\omega T - \sqrt{-3}.$$

Therefore θ is a root of

$$g(T)\overline{g}(T) = T^6 + 3T^5 + 6T^4 + 9T^3 + 12T^2 + 9T + 3.$$

Computing the determinant of a transition matrix from the known $\mathbf{Z}$-basis in (7) to the powers of θ shows $[\mathcal{O}_K : \mathbf{Z}[\theta]] = 5$, so $\mathcal{O}_K \neq \mathbf{Z}[\theta]$. Alternatively, the discriminant of the minimal polynomial for θ can be calculated by PARI to be $-2^4 3^7 5^2 \neq \mathrm{disc}(\mathcal{O}_K)$. In $\mathbf{Z}/5\mathbf{Z}$, $g\overline{g}$ has a double root, 3.

As a further check on the calculation of the $\mathbf{Z}$-basis, let's calculate both sides of

$$|\operatorname{disc}(K)| = |\operatorname{N}_{k/\mathbf{Q}}(\operatorname{disc}(K/k))| \operatorname{disc}(k)^2.$$

We already checked the left hand side is $2^4 3^7$. Since $\operatorname{disc}(k)^2 = (2^2 3^3)^2$, we need to check $|\operatorname{N}_{k/\mathbf{Q}}(\operatorname{disc}(K/k))| = 3$, which is the same as $(\operatorname{disc}(K/k)) = (\pi)$. Well, $\mathcal{O}_K = \mathcal{O}_k[\theta]$, so

$$\operatorname{disc}(K/k) = \begin{vmatrix} \operatorname{Tr}_{K/k}(1) & \operatorname{Tr}_{K/k}(\theta) \\ \operatorname{Tr}_{K/k}(\theta) & \operatorname{Tr}_{K/k}(\theta^2) \end{vmatrix} = \begin{vmatrix} 2 & -\pi^2 v \\ -\pi^2 v & \pi v \end{vmatrix} = 2\pi v - \pi^4 v^2 = -\pi v,$$

so everything checks out (and this gives an alternate calculation of $\operatorname{disc}(K)$).

We now turn to computing the unit group of $\mathcal{O}_K$. The only roots of unity in K are $\{\pm 1, \pm\omega, \pm\omega^2\}$, since any root of unity other than ± 1 generates an even degree abelian extension of $\mathbf{Q}$, and the only such subfield of K is $F = \mathbf{Q}(\omega)$, so F contains all the roots of unity of K. The rank of the unit group is 2, and we will find a basis.

Where to begin? We have one obvious unit, namely $u = 1 + \sqrt[3]{2} + \sqrt[3]{4}$. We can take a $\mathbf{Q}$-conjugate, say $u' \stackrel{\text{def}}{=} 1 + \sqrt[3]{2}\omega + \sqrt[3]{4}\omega^2$, and hope that u and u' may be a basis. This turns out not to be the case, but let's see how much can be said.

As a set of 3 complex embeddings of K to use in the log map of $\mathcal{O}_K^\times$, we use $\mathrm{Gal}(K/F) = \{1, \sigma_2, \sigma_3 = \sigma_2^2\}$, where

$$\begin{aligned}\sigma_2(\sqrt[3]{2}) &= \sqrt[3]{2}\omega, \quad \sigma_2(\omega) = \omega, \\ \sigma_3(\sqrt[3]{2}) &= \sqrt[3]{2}\omega^2, \quad \sigma_3(\omega) = \omega.\end{aligned}$$

Note

$$u' = \sigma_2(u) = 1 - \sqrt[3]{4} + (\sqrt[3]{2} - \sqrt[3]{4})\omega = -\pi v - \sqrt[3]{2} v\omega$$

and

$$\sigma_2(u') = \sigma_3(u) = 1 - \sqrt[3]{2} + (\sqrt[3]{4} - \sqrt[3]{2})\omega = -v + \sqrt[3]{2} v\omega.$$

The log map $L\colon \mathcal{O}_K^\times \to \mathbf{R}^3$ has the effect

$$\begin{aligned} x &\mapsto (2\log|x|, 2\log|\sigma_2 x|, 2\log|\sigma_3 x|) \\ &= 2\log|x|(1,0,-1) + 2\log|\sigma_2 x|(0,1,-1). \end{aligned}$$

For all x in K, $\overline{\sigma}_2(x) = \sigma_3(\overline{x})$ and $\overline{\sigma}_3(x) = \sigma_2(\overline{x})$. Thus $|\sigma_3(u)| = |\sigma_2(u)|$ since u is real, so $|\sigma_2(u)| = 1/\sqrt{u}$. In particular,

$$u\sigma_2(u)\sigma_3(u) = u|\sigma_2(u)|^2 = 1. \tag{8}$$

(This is identical to a calculation in Lemma 2.)

The regulator of u and u' is the absolute value of

$$\begin{vmatrix} 2\log|u| & 2\log|\sigma_2(u)| \\ 2\log|u'| & 2\log|\sigma_2(u')| \end{vmatrix} = \begin{vmatrix} 2\log u & -\log u \\ -\log u & -\log u \end{vmatrix} = -3(\log u)^2. \tag{9}$$

This is nonzero, so the index of $L' \stackrel{\text{def}}{=} \mathbf{Z}L(u) + \mathbf{Z}L(u')$ in $L(\mathcal{O}_K^\times)$ is finite. But what is this index?

To compute it, we shall calculate the regulator of K. This will be done without knowing a basis for the units, by using special values of zeta functions, inspired by Stark's calculations in Sections 3.2, 3.3, and 3.4 of his article in [3].

The zeta function of a number field vanishes at $s = 0$ to order equal to the rank of its unit group, and its first nonzero Taylor coefficient is $-hR/w$. Using Artin L-functions we will express the zeta function of K in terms of the zeta functions of k and F (and $\mathbf{Q}$). All these fields have class number 1 and we know the regulators of $\mathbf{Q}$, F, and k. So we will be able to compute the regulator of K. In fact, before a plan was developed for computing a basis of the unit group, PARI was used to compute an approximate value of $R(K)$ as $-6\zeta_K(s)/s^2$ for s near 0, and it was noticed upon dividing $3(\log u)^2$ (taken from (9)) by the approximate regulator that the ratio was essentially 3, thus suggesting $[L(\mathcal{O}_K^\times) : L'] = 3$ and $R(K) = (\log u)^2$. To prove this, we use the following result.

Theorem 3. *Let $K/\mathbf{Q}$ be any Galois extension with Galois group $G \cong S_3$. Let F be the unique quadratic subfield, the fixed field of the unique subgroup $N \cong A_3$ of size 3. Let k be the fixed field of any cyclic 2 subgroup H of G. Then*

$$\zeta_K(s) = \zeta_F(s)\left(\frac{\zeta_k(s)}{\zeta_{\mathbf{Q}}(s)}\right)^2.$$

Proof. We express all zeta functions as Artin L-functions for representations of the common group G:

$$\begin{aligned} \zeta_K(s) &= L(s, \mathrm{Ind}_e^G(1_e)), \\ \zeta_k(s) &= L(s, \mathrm{Ind}_H^G(1_H)), \\ \zeta_F(s) &= L(s, \mathrm{Ind}_N^G(1_N)). \end{aligned}$$

Let χ_1 be the trivial character of G, χ_1' be the nontrivial 1-dimensional character, and χ_2 be the 2-dimensional irreducible character.

By Frobenius reciprocity,

$$\begin{aligned} \mathrm{Ind}_e^G(1_e) &= \chi_1 + \chi_1' + 2\chi_2, \\ \mathrm{Ind}_H^G(1_H) &= \chi_1 + \chi_2, \\ \mathrm{Ind}_N^G(1_N) &= \chi_1 + \chi_1', \end{aligned}$$

so

$$\begin{aligned}\zeta_K(s) &= L(s,\chi_1)L(s,\chi_1')L(s,\chi_2)^2,\\ \zeta_k(s) &= L(s,\chi_1)L(s,\chi_2),\\ \zeta_F(s) &= L(s,\chi_1)L(s,\chi_1').\end{aligned}$$

Thus

$$\zeta_K(s) = \zeta_F(s)L(s,\chi_2)^2 = \zeta_F(s)\left(\frac{\zeta_k(s)}{\zeta_{\mathbf{Q}}(s)}\right)^2.$$

□

Corollary 1. *With the same hypotheses as in Theorem 3,*

$$h(K)R(K) = h(F)R(F)(h(k)R(k))^2, \quad \operatorname{disc}(K) = \operatorname{disc}(F)\operatorname{disc}(k)^2.$$

Proof. Equating the first nonvanishing Taylor coefficients on both sides of the equation in Theorem 3 yields

$$-\frac{h(K)R(K)}{w(K)} = -\frac{h(F)R(F)}{w(F)}\left(\frac{-h(k)R(k)/2}{-1/2}\right)^2.$$

Since any nontrivial root of unity in K generates an even degree abelian extension of $\mathbf{Q}$, $w(K) = w(F)$. Thus we get the first desired equality. Now compute the residue at $s = 1$ of both sides in Theorem 3 to get the discriminant formula in absolute value (either take cases depending on if F is real or imaginary, or equate orders of vanishing at $s = -1$ and $s = -2$ to relate the number of real and complex embeddings for K, F, and k). The signs of the discriminants match up, so we get the second equality. □

In particular, for $K = \mathbf{Q}(\sqrt[3]{2}, \omega)$, $R(K) = R(\mathbf{Q}(\sqrt[3]{2}))^2 = (\log u)^2$ and $\operatorname{disc}(K) = -3 \cdot (2^2 3^3)^2 = -2^4 3^7$, giving a third computation of the discriminant of K.

That u and u' generate a subgroup of index 3 in $\mathcal{O}_K^\times$ mod torsion has an analogy in any S_3 extension K of $\mathbf{Q}$ which is not a real field i.e., K is the splitting field of a cubic field over $\mathbf{Q}$ with a negative discriminant. A fundamental unit for the unique real cubic subfield k of K, along with either of the $\mathbf{Q}$-conjugates of this unit has regulator $3(\log u)^2 = 3R(k)^2$. The calculation is identical to that for the field $\mathbf{Q}(\sqrt[3]{2}, \omega)$. Since $h(K)R(K) = h(F)(h(k)R(k))^2$ when F is imaginary quadratic, the index in $\mathcal{O}_K^\times/\mu_K$ of the group generated by the fundamental unit of k and a $\mathbf{Q}$-conjugate equals

$$\frac{3R(k)^2}{R(K)} = \frac{3h(K)}{h(F)h(k)^2}.$$

This fraction must be an integer. Is this clear from some other perspective?

The following result will allow us to refine $\{u, u'\}$ to a basis of units for $\mathcal{O}_{\mathbf{Q}(\sqrt[3]{2},\omega)}$.

Theorem 4. *Let $L' \subset L \cong \mathbf{Z}^2$ be free rank 2 lattices with $[L : L'] = p$ a prime. Write $L' = \mathbf{Z}e_1 \oplus \mathbf{Z}e_2$. Then one of e_1 or e_2 is not in pL. Choosing e_1 to not lie in pL, there is an integer a, uniquely determined modulo $p\mathbf{Z}$, such that $e_2 - ae_1 \in pL$. For any such a, write $e_2 - ae_1 = pw$, $w \in L$. Then e_1 and w is a basis of L, i.e.*

$$L = \mathbf{Z}e_1 \oplus \mathbf{Z}w.$$

Proof. Since $[L' : pL] = [L : pL]/[L : L'] = p$, not both e_1 and e_2 can lie in pL, say $e_1 \notin pL$. Then $e_1 \neq 0$ in $L'/pL \cong \mathbf{Z}/p\mathbf{Z}$, so we can solve the equation $ae_1 \equiv e_2 \bmod pL$ for some $a \in \mathbf{Z}$, uniquely determined mod p.

Let $e_2 - ae_1 = pw$. Then w is not a $\mathbf{Z}$-linear combination of e_1 and e_2, so $w \notin L'$. Thus L' is a proper subgroup of $\mathbf{Z}w \oplus \mathbf{Z}e_1$. Since $[L : L'] = p$, we must have $\mathbf{Z}w \oplus \mathbf{Z}e_1 = L$. □

For the intended application, consider the case $p = 3$. If neither e_1 nor e_2 is in pL, then a is prime to $p = 3$, so we may assume $a = \pm 1$. That is, either $e_2 - e_1$ or $e_2 + e_1$ is in $3L$ (but not both), and whichever one is will give rise to (thrice) a lattice element to pair together with e_1 to form a basis of L.

For $K = \mathbf{Q}(\sqrt[3]{2}, \omega)$, consider the lattice $L = L(\mathcal{O}_K^\times)$ under the log map, with $L' = \mathbf{Z}L(u) + \mathbf{Z}L(u')$. Since $[L : L'] = 3$, at least one of $L(u)$ and $L(u')$ is not in $3L$. However, since u and u' are Galois-conjugate, if one of $L(u)$, $L(u')$ is in $3L$ then so is the other. Thus neither one is, in particular $L(u)$ is not. So by Theorem 4 there must be a basis of $\mathcal{O}_K^\times$ containing u, the fundamental unit of $\mathcal{O}_k$. More precisely, by the previous paragraph either $uu' = \zeta\varepsilon^3$ or $u/u' = \zeta\varepsilon^3$, where ζ is a root of unity in K and $\varepsilon \in \mathcal{O}_K^\times$, and then u and ε form a basis. Since ζ actually only matters modulo cubes, we may assume $\zeta \in \{1, \omega, \omega^2\}$.

The equation $uu' = u\sigma_2(u) = \zeta\varepsilon^3$ implies (by (8)) $1/\sigma_3(u) = \zeta\varepsilon^3$. But then taking Galois conjugates implies u and $\sigma_2(u)$ are both cubes of units, up to multiplication by a root of unity. Then both have log images in $3L$, which is not the case. So we must have

$$\frac{u}{u'} = \frac{u}{\sigma_2(u)} = \zeta\varepsilon^3, \quad \varepsilon \in \mathcal{O}_K^\times.$$

Reduce this equation in the residue field $\mathcal{O}_K/\sqrt[3]{2} \cong \mathbf{F}_4$. Here $u, \sigma_2(u) \equiv 1$, and (how fortuitous!) $\varepsilon^3 \equiv 1$ since $\mathbf{F}_4^\times$ has size 3. So $\zeta \equiv 1$. Different cube roots of unity are distinct in $\mathbf{F}_4$, so $\zeta = 1$.

Therefore

$$\varepsilon^3 = \frac{u}{\sigma_2(u)} = u^2\sigma_3(u) = u^2(-v + \sqrt[3]{2}v\omega) = -u + (u+1)\omega \tag{10}$$

for some unit ε. To find ε using (10) we must extract a cube root in the sixth degree field K.

The ambiguity in the precise value of ε is not only up to multiplication by the cube root of unity inherent in determining ε from ε^3. The choice of looking at $u/\sigma_2(u)$ rather than $u/\sigma_3(u)$ also introduces a measure of variability; both σ_2 and σ_3 are generators of $\mathrm{Gal}(K/F)$. Since $u/\sigma_2(u)$ and $u/\sigma_3(u)$ are complex conjugates, considering cube roots of either shows there should be 6 possible values of ε satisfying an equation like (10), if we allow either σ_2 or σ_3 to be used.

If by black magic we discovered a cube root ε of $u/\sigma_2(u)$ then we don't need Theorem 4 to know u and ε are a basis, as that can be determined from (10) alone. Indeed, applying complex conjugation to the first equation in (10) and multiplying the resulting equation by (10) yields $u^3 = (\varepsilon\overline{\varepsilon})^3$ by (8), so

$$u = \varepsilon\overline{\varepsilon} \tag{11}$$

(both are positive numbers) and $2\log|\varepsilon| = \log u$. Applying σ_2 to (10) and then complex conjugation to the result yields

$$\sigma_2(\varepsilon)^3 = \frac{\sigma_2(u)}{\sigma_3(u)}, \quad \overline{\sigma}_2(\varepsilon)^3 = \frac{\sigma_3(u)}{\sigma_2(u)},$$

so $|\sigma_2(\varepsilon)| = 1$, hence

$$\log|\sigma_2(\varepsilon)| = 0, \quad 2\log|\sigma_3(\varepsilon)| = -2\log|\varepsilon| - 2\log|\sigma_2(\varepsilon)| = -\log u.$$

So the regulator of u and ε is the absolute value of

$$\begin{vmatrix} 2\log u & 2\log|\sigma_2(u)| \\ 2\log|\varepsilon| & 2\log|\sigma_2(\varepsilon)| \end{vmatrix} = \begin{vmatrix} 2\log u & -\log u \\ \log u & 0 \end{vmatrix} = (\log u)^2 = R(K),$$

so u and ε form a basis.

Also, the regulator of ε and $\overline{\varepsilon}$ is the absolute value of

$$\begin{vmatrix} 2\log|\varepsilon| & 2\log|\sigma_2(\varepsilon)| \\ 2\log|\overline{\varepsilon}| & 2\log|\sigma_2(\overline{\varepsilon})| \end{vmatrix} = \begin{vmatrix} \log u & 0 \\ \log u & -\log u \end{vmatrix} = -(\log u)^2,$$

so ε and $\overline{\varepsilon}$ are a basis for the units. The general unit has the form $\zeta\varepsilon^m\overline{\varepsilon}^n$, which along with its complex conjugate forms a basis of the units only when $(m,n) = (\pm 1, 0)$ or $(0, \pm 1)$.

Okay, let's get down to business and figure out what ε could be. We will determine the polynomial for ε in the quadratic extension K/k, and then use the quadratic formula to find the roots. We need to compute $\mathrm{Tr}_{K/k}(\varepsilon) = \varepsilon + \overline{\varepsilon}$ and $\mathrm{N}_{K/k}(\varepsilon) = \varepsilon\overline{\varepsilon}$. The latter was already computed in (11), it is u. From (10) we have

$$\mathrm{Tr}_{K/k}(\varepsilon^3) = -2u - (u+1) = -1 - 3u.$$

Since

$$\mathrm{Tr}_{K/k}(\varepsilon^3) = \varepsilon^3 + \overline{\varepsilon}^3 = (\varepsilon+\overline{\varepsilon})^3 - 3\varepsilon\overline{\varepsilon}(\varepsilon+\overline{\varepsilon}) = (\mathrm{Tr}_{K/k}\,\varepsilon)^3 - 3u\,\mathrm{Tr}_{K/k}(\varepsilon),$$

we see that $\mathrm{Tr}_{K/k}(\varepsilon)$ is a root (in k) of

$$T^3 - 3uT + (1+3u). \tag{12}$$

Should we use the cubic formula to find $\mathrm{Tr}_{K/k}(\varepsilon)$? No, we use PARI. Having computed approximate values for $\sqrt[3]{2}$ and u along the way towards asking PARI for the decimal approximations of the roots of this polynomial, it becomes apparent upon examining PARI's root calculation that two of the roots of (12) should be $-u$ and $\sqrt[3]{2}$. Then the third root is $u - \sqrt[3]{2} = 1 + \sqrt[3]{4}$. To prove these are the roots of $T^3 - 3uT + (1+3u)$ without using a computer, note by (5) that $-u$ is a root of (12). It is easily verified by hand that $\sqrt[3]{2}$ is a root.

So $\mathrm{Tr}_{K/k}(\varepsilon)$ is $-u$, $\sqrt[3]{2}$, or $1 + \sqrt[3]{4}$. That makes ε a root of one of the following three polynomials:

$$T^2 + uT + u, \quad T^2 - \sqrt[3]{2}T + u, \quad T^2 - (1+\sqrt[3]{4})T + u. \tag{13}$$

This gives 6 choices for the roots, all of which are different since these three monic polynomials are all irreducible over k (they have negative discriminants). A previous remark about ambiguities in specifying ε knowing only (10) more or less guarantees *any* of the roots of these is an adequate choice for ε (up to using σ_3 instead of σ_2), before doing any calculations.

Let's consider the first polynomial. For ε to be a root of it, the roots of this polynomial must lie in K. Since the field generated over k by the roots of T^2+uT+u is $k(\sqrt{u^2-4u}) = k(\sqrt{1-\sqrt[3]{4}})$, while $K = k(\omega) = k(\sqrt{-3})$, we must check if

$$\frac{1-\sqrt[3]{4}}{-3} = \frac{\sqrt[3]{4}-1}{3} = \frac{1}{9}\left(3\sqrt[3]{4} - 3\right)$$

is a square in $k = \mathbf{Q}(\sqrt[3]{2})$, which is the same as checking whether the algebraic integer $3\sqrt[3]{4} - 3$ is a square in $\mathcal{O}_k = \mathbf{Z}[\sqrt[3]{2}]$. Expanding the equation

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

there is an easy solution by inspection: $a = 1, b = -1, c = 1$. So

$$1 - \sqrt[3]{4} = -3\left(\frac{1 - \sqrt[3]{2} + \sqrt[3]{4}}{3}\right)^2.$$

This can also be seen from (3). So a candidate for ε as a root of $T^2 + uT + u$ is

$$\frac{-u + \sqrt{1 - \sqrt[3]{4}}}{2} = \frac{1}{2}\left(-u + \frac{1 - \sqrt[3]{2} + \sqrt[3]{4}}{3}\sqrt{-3}\right).$$

The other root of this polynomial is $\overline{\varepsilon}$. Writing $\sqrt{-3} = 2\omega + 1$, we have

$$\varepsilon \stackrel{\text{def}}{=} -\frac{1 + 2\sqrt[3]{2} + \sqrt[3]{4}}{3} + \frac{1 - \sqrt[3]{2} + \sqrt[3]{4}}{3}\omega = -\frac{\pi^2}{3} + \frac{\pi^2 v}{3}\omega = \frac{-u + \omega}{\pi}. \tag{14}$$

An explicit calculation shows the cube of this number is $u/\sigma_2(u)$, so we've found a choice for ε. For the other root $\overline{\varepsilon}$, $\overline{\varepsilon}^3 = u/\sigma_3(u)$.

The minimal polynomial of ε over $\mathbf{Q}$ is

$$(T^2 + uT + u)(T^2 + \sigma_2(u)T + \sigma_2(u))(T^2 + \sigma_3(u)T + \sigma_3(u)) = T^6 + 3T^5 - 5T^3 + 3T + 1.$$

What about the other roots of the three polynomials in (13)? The other root of $T^2 + uT + u$ is $\overline{\varepsilon}$. We expect the roots of the other two polynomials to be ε and $\overline{\varepsilon}$ multiplied by primitive cube roots of unity. Indeed,

$$\mathrm{Tr}_{K/k}(\varepsilon\omega) = \sqrt[3]{2}, \quad \mathrm{Tr}_{K/k}(\varepsilon\omega^2) = 1 + \sqrt[3]{4},$$

so the roots of $T^2 - \sqrt[3]{2}T + u$ are $\varepsilon\omega$ and $\overline{\varepsilon}\omega^2$ while the roots of $T^2 - (1 + \sqrt[3]{4})T + u$ are $\varepsilon\omega^2$ and $\overline{\varepsilon}\omega$.

Since θ and ε have the same ω coefficient, we compute $\theta - \varepsilon = \sqrt[3]{2}$, so by (7)

$$\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{2}] \oplus \mathbf{Z}[\sqrt[3]{2}]\varepsilon = \mathbf{Z}[u] \oplus \mathbf{Z}[u]\varepsilon.$$

But even better, $\mathrm{disc}(\mathbf{Z}[\varepsilon]) = -2^4 3^7$, the discriminant of $\mathcal{O}_K$. So we get a power basis: $\mathcal{O}_K = \mathbf{Z}[\varepsilon]$. The discriminant of $\mathbf{Z}[\varepsilon]$ was first computed using PARI, but by hand we can calculate the transition matrix between the powers of ε and a known basis of $\mathcal{O}_K$. A convenient basis is $\{1, u, u^2, \varepsilon, u\varepsilon, u^2\varepsilon\}$, since $\varepsilon^2 = -u\varepsilon - u$:

$$\begin{pmatrix} 1 \\ \varepsilon \\ \varepsilon^2 \\ \varepsilon^3 \\ \varepsilon^4 \\ \varepsilon^5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 \\ -1 & -3 & -2 & -1 & -3 & -1 \\ 1 & 4 & 6 & 0 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 \\ u \\ u^2 \\ \varepsilon \\ u\varepsilon \\ u^2\varepsilon \end{pmatrix}.$$

The determinant of the matrix is -1.

The $\mathbf{Q}$-conjugates of ε are units, so let's determine them explicitly in terms of the basis $\{\varepsilon, \overline{\varepsilon}\}$. Recall

$$2\log|\varepsilon| = \log u, \ 2\log|\sigma_2(\varepsilon)| = 0, \ 2\log|\sigma_3(\varepsilon)| = -\log u.$$

So

$$\begin{aligned} L(\varepsilon) &= (\log u)(1, 0, -1), \\ L(\overline{\varepsilon}) &= (\log u)(1, -1, 0), \\ L(\sigma_2(\varepsilon)) &= (\log u)(0, -1, 1) \\ &= L(\overline{\varepsilon}) - L(\varepsilon), \\ L(\sigma_3(\varepsilon)) &= (\log u)(-1, 1, 0) \\ &= -L(\overline{\varepsilon}). \end{aligned}$$

Thus $\sigma_2(\varepsilon) = \zeta\varepsilon^{-1}\overline{\varepsilon}$ and $\sigma_3(\varepsilon) = \zeta\overline{\varepsilon}^{-1}$, where ζ denotes some root of unity (not necessarily the same in both equations).

In $\mathcal{O}_K/\sqrt[3]{2} \cong \mathbf{F}_4$, σ_2 and σ_3 both induce the identity map and, by (14), $\varepsilon \equiv 1 + \omega \equiv \omega^2$, $\overline{\varepsilon} \equiv \omega$. So the equation $\sigma_2(\varepsilon) = \zeta\varepsilon^{-1}\overline{\varepsilon}$ reduces to

$$\omega^2 \equiv \zeta\omega^2,$$

so $\zeta = \pm 1$, i.e. $\sigma_2(\varepsilon) = \pm\varepsilon^{-1}\overline{\varepsilon} = \pm\overline{\varepsilon}^2/u$. To determine which sign holds we take traces down to $\mathbf{Q}$:

$$\mathrm{Tr}_{K/\mathbf{Q}}(\sigma_2(\varepsilon)) = \mathrm{Tr}_{K/\mathbf{Q}}(\varepsilon) = -3,$$

and

$$\mathrm{Tr}_{K/\mathbf{Q}}(\overline{\varepsilon}^2/u) = \mathrm{Tr}_{k/\mathbf{Q}}((1/u)\,\mathrm{Tr}_{K/k}(\overline{\varepsilon}^2)).$$

Since

$$\mathrm{Tr}_{K/k}(\overline{\varepsilon}^2) = \varepsilon^2 + \overline{\varepsilon}^2 = (\varepsilon + \overline{\varepsilon})^2 - 2\varepsilon\overline{\varepsilon} = u^2 - 2u,$$

we have

$$\mathrm{Tr}_{K/\mathbf{Q}}(\overline{\varepsilon}^2/u) = \mathrm{Tr}_{k/\mathbf{Q}}(u - 2) = 3 - 6 = -3.$$

So

$$\sigma_2(\varepsilon) = \frac{\overline{\varepsilon}^2}{u} = \varepsilon^{-1}\overline{\varepsilon}.$$

Similarly, $\sigma_3(\varepsilon) = \overline{\varepsilon}^{-1}$. Then

$$\overline{\sigma}_2(\varepsilon) = \varepsilon\overline{\varepsilon}^{-1},\ \overline{\sigma}_3(\varepsilon) = \varepsilon^{-1}.$$

Of course there is nothing canonical about complex conjugation as an element of $\mathrm{Gal}(K/\mathbf{Q})$.

Here is a faster method of discovering a unit to form a basis for $\mathcal{O}_K^\times$ when paired up with u. Since $(3) = (\eta)^6$, the ideal (η) is fixed by $G = \mathrm{Gal}(K/\mathbf{Q})$. In particular, for any $g \in G$ we have $g(\eta)/\eta \in \mathcal{O}_K^\times$. Perhaps for suitable g this ratio will be a unit that along with u gives us a basis! Since $\overline{\eta} = -\eta$, we get the following table (where $(\cdot)^*$ denotes complex conjugation) which shows that we really only need to try $g = \sigma_2$.

g	1	$(\cdot)^*$	σ_2	σ_3	$\overline{\sigma}_2$	$\overline{\sigma}_3$
$g(\eta)/\eta$	1	-1	$\sigma_2(\eta)/\eta$	$(\sigma_2(\eta)/\eta)^*$	$-(\sigma_2(\eta)/\eta)^*$	$-\sigma_2(\eta)/\eta$

Let's compute the image of $\sigma_2(\eta)/\eta$ under the log map. Since $\sigma_2(\eta)/\eta = \pi/\sigma_2(\pi) = (1 + \sqrt[3]{2})/(1 + \sqrt[3]{2}\omega)$,

$$\begin{aligned}\left|\frac{\sigma_2(\eta)}{\eta}\right|^2 &= \frac{(1+\sqrt[3]{2})^2}{\left|1+\sqrt[3]{2}\omega\right|^2} \\ &= \frac{(1+\sqrt[3]{2})^2}{1-\sqrt[3]{2}+\sqrt[3]{4}} \\ &= \frac{\pi^2}{\pi^2 v} \\ &= u\end{aligned}$$

and

$$\begin{aligned}\left|\sigma_2\left(\frac{\sigma_2(\eta)}{\eta}\right)\right|^2 &= \left|\frac{\sigma_3(\eta)}{\sigma_2(\eta)}\right|^2 \\ &= \left|\frac{1+\sqrt[3]{2}\omega}{1+\sqrt[3]{2}\omega^2}\right|^2 \\ &= 1.\end{aligned}$$

So the regulator of u and $\sigma_2(\eta)/\eta$ is

$$\begin{vmatrix} 2\log u & -\log u \\ \log u & 0 \end{vmatrix} = (\log u)^2 = R(K).$$

So u and $\sigma_2(\eta)/\eta$ forms a basis for the units. In fact, we see that $L(\sigma_2(\eta)/\eta) = L(\varepsilon)$, so $\sigma_2(\eta)/\eta = \zeta\varepsilon$ for some root of unity ζ. By an explicit calculation,

$$\begin{aligned}\frac{\sigma_2(\eta)}{\eta} &= \frac{\pi}{\sigma_2(\pi)} \\ &= \frac{\pi\overline{\sigma}_2(\pi)}{\sigma_2(\pi)\overline{\sigma_2(\pi)}} \\ &= \frac{\pi(1+\sqrt[3]{2}\omega^2)}{1-\sqrt[3]{2}+\sqrt[3]{4}} \\ &= \frac{\pi(1+\sqrt[3]{2}\omega^2)}{\pi^2 v} \\ &= \frac{\pi^2(1+\sqrt[3]{2}\omega^2)}{3} \\ &= -\frac{1}{3}(1-\sqrt[3]{2}+\sqrt[3]{4}) - \frac{1}{3}(2+\sqrt[3]{2}+2\sqrt[3]{4})\omega,\end{aligned}$$

we see that $\sigma_2(\eta)/\eta = \varepsilon\omega$. Therefore another basis for the units would be $\sigma_2(\eta)/\eta$ and its complex conjugate, so using reciprocals we get

$$\frac{1+\sqrt[3]{2}\omega}{1+\sqrt[3]{2}}, \quad \frac{1+\sqrt[3]{2}\omega^2}{1+\sqrt[3]{2}}$$

is a basis for the units of $\mathcal{O}_K$. Unlike ε, $\delta \stackrel{\text{def}}{=} \sigma_2(\eta)/\eta$ does not provide a power basis, as its minimal polynomial over $\mathbf{Q}$ is $f(T) = T^6 + 3T^4 + 4T^3 + 3T^2 + 1$, so the discriminant of $\mathbf{Z}[\delta]$ is

$$\begin{aligned}-\operatorname{N}_{K/\mathbf{Q}}(f'(\delta)) &= -\operatorname{N}_{K/\mathbf{Q}}(6\delta^5 + 12\delta^3 + 12\delta^2 + 6\delta) \\ &= -6^6 \operatorname{N}_{K/\mathbf{Q}}(\delta^4 + 2\delta^2 + 2\delta + 1),\end{aligned}$$

which is divisible by 2^6, which is too large a power of 2. (The complete value of the discriminant is $-2^{12}3^7$.)

This trick with the ideal (η) depended quite strongly on choosing η as the generator of interest. Let's see how it could have turned out differently. Recall we formed η as the quotient of generators for the prime ideal factors of 3 in F and k. The most general such ratio would be

$$\tilde{\eta} = \frac{\zeta\sqrt{-3}}{\pi u^n} = \zeta\eta u^{-n} = \zeta\eta\varepsilon^{-n}\overline{\varepsilon}^{-n},$$

so

$$\begin{aligned}\frac{\sigma_2(\tilde{\eta})}{\tilde{\eta}} &= \frac{\sigma_2(\eta)}{\eta}\frac{\sigma_2(\varepsilon)^{-n}}{\varepsilon^{-n}}\frac{\sigma_2(\overline{\varepsilon})^{-n}}{\overline{\varepsilon}^{-n}} \\ &= \omega\varepsilon\cdot\varepsilon^n\frac{\varepsilon^n}{\overline{\varepsilon}^n}\cdot\overline{\varepsilon}^n(\overline{\sigma}_3(\varepsilon)^{-n}) \\ &= \omega\varepsilon^{3n+1}.\end{aligned}$$

This forms a basis with $u = \varepsilon\overline{\varepsilon}$ precisely when $n = 0$, i.e. only for $\tilde{\eta} = \zeta\eta$!

We conclude by summarizing our findings about K, with particular emphasis on ε.

Theorem 5. *The field $K = \mathbf{Q}(\sqrt[3]{2}, \omega)$ has class number 1, discriminant $-2^4 3^7$, and regulator $(\log(1+\sqrt[3]{2}+\sqrt[3]{4}))^2$. The ramified primes 2 and 3 factor as*

$$(2) = (\sqrt[3]{2})^3, \quad (3) = (\eta)^6,$$

where $\eta = \sqrt{-3}/(1+\sqrt[3]{2})$.

The ring of integers of K is $\mathbf{Z}[\varepsilon]$, where

$$\varepsilon = -\frac{1 + 2\sqrt[3]{2} + \sqrt[3]{4}}{3} + \frac{1 - \sqrt[3]{2} + \sqrt[3]{4}}{3}\omega = \frac{\omega - u}{\pi},$$

with $\pi = 1 + \sqrt[3]{2}$, satisfies $\varepsilon^2 = -u\varepsilon - u$, where $u = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ is the fundamental unit of $\mathbf{Q}(\sqrt[3]{2})$. The minimal polynomial of ε over $\mathbf{Q}$ is $T^6 + 3T^5 - 5T^3 + 3T + 1$.

The unit group of $\mathcal{O}_K$ has six roots of unity, rank 2, and basis $\{\varepsilon, \overline{\varepsilon}\}$.

For a description of all power bases of $\mathcal{O}_K$, see [1].

References

[1] Chang, M-L., Non-monogeneity in a family of sextic fields, *J. Number Theory* **97** (2002), 252–268.
[2] Lang, S., "Algebraic Number Theory," 3rd ed., Springer-Verlag, New York, 1994.
[3] Waldschmidt, M. et al. (eds.), "From Number Theory to Physics," Springer-Verlag, New York, 1992.