THE SPLITTING FIELD OF $X^3 - 5$ OVER $\mathbb{Q}$

KEITH CONRAD

In this note, we calculate all the basic invariants of the number field
$$K = \mathbb{Q}(-\sqrt[3]{5}, \omega),$$
where $\omega = (-1 + \sqrt{-3})/2$ is a primitive cube root of unity.

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

\begin{align*}
k &= \mathbb{Q}(-\sqrt[3]{5}), \\
K &= \mathbb{Q}(-\sqrt[3]{5}, \omega), \\
F &= \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt[3]{-3}), \\
G &= \text{Gal}(K/\mathbb{Q}) \cong S_3, \\
N &= \text{Gal}(K/F) \cong A_3, \\
H &= \text{Gal}(K/k).
\end{align*}

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

**Theorem 1.** The field $F = \mathbb{Q}(\omega)$ has ring of integers $\mathbb{Z}[\omega]$, 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 $\mathbb{Z}[\omega] = \mathbb{Z}[X]/(X^2 + X + 1)$ is identical to the way $X^2 + X + 1$ factors mod $p$, so $p$ splits if $p \equiv 1 \mod 3$ and $p$ stays prime if $p \equiv 2 \mod 3$.

We now turn to the field $k$. Its norm form is
$$N_{k/\mathbb{Q}}(a + b\sqrt[3]{5} + c\sqrt[3]{25}) = a^3 + 5b^3 + 25c^3 - 15abc.$$

Since $\text{disc}(\mathbb{Z}[\sqrt[3]{5}]) = -N_{K/\mathbb{Q}}(3(\sqrt[3]{5})^2) = -3^35^2$, only 3 and 5 can ramify in $k$. Since $X^3 - 5$ is Eisenstein at 5 and
\begin{equation}
(X - 1)^3 - 5 = X^3 - 3X^2 + 3X - 6
\end{equation}
is Eisenstein at 3, both 3 and 5 are totally ramified. Therefore by the same local field argument as in [2], $\mathcal{O}_k = \mathbb{Z}[\sqrt[3]{5}]$, so $\text{disc}(\mathcal{O}_k) = -3^35^2$.

The factorization of 5 is $5\mathcal{O}_k = (\sqrt[3]{5})^3$. To factor 3, we use not (1) but a 3-Eisenstein polynomial whose constant term is $\pm 3$:
$$\begin{equation}
(X - 2)^3 + 5 = X^3 - 6X^2 + 12X - 3.
\end{equation}$$

Let $\pi \equiv 2 - \sqrt[3]{5}$ be a root of this. Then
\begin{align*}
\pi^3 &= 3 - 12\pi + 6\pi^2 \\
&= 3(1 - 4\pi + 2\pi^2) \\
&= 3(1 - 4\sqrt[3]{5} + 2\sqrt[3]{25}).
\end{align*}

Since $N_{k/\mathbb{Q}}(\pi) = 3$, $v \equiv 1 - 4\sqrt[3]{5} + 2\sqrt[3]{25}$ is a unit in $\mathcal{O}_k$ with norm 1 and $3 = \pi^3/v$.

Let
$$u \equiv \frac{1}{v} = 41 + 24\sqrt[3]{5} + 14\sqrt[3]{25},$$
so $3 = \pi^3 u$. We will show later that $u$ is the fundamental unit of $k$. (For comparison, in $\mathbb{Q}(\sqrt[3]{2}, \omega)$ we had $3 = \pi^3 v$ where $v < 1$ was the reciprocal of the fundamental unit.)

The minimal polynomial of $v$ over $\mathbb{Q}$ is

$$m(T) = T^3 - \text{Tr}_{k/\mathbb{Q}}(v)T^2 + \text{Tr}_{k/\mathbb{Q}}(u)T - 1 = T^3 - 3T^2 + 123T - 1,$$

and the minimal polynomial for $u$ over $\mathbb{Q}$ is

$$T^3 - 123T^2 + 3T - 1.$$

It is not a surprise that $m(T)$ has a large linear coefficient, since $m(0) = -N_{k/\mathbb{Q}}(v) = -1$ but $m$ has a zero $v \approx .008$ which is quite near 0, so $m'(0)$ ought to be large, in fact around $(m(v) - m(0))/v = 1/v \approx 1/.008 \approx 122.9$. Since the minimal polynomial for $u$ has a root mod 2, $2|\text{disc}(\mathbb{Z}[u])$ so $\mathbb{Z}[u] \not= \mathcal{O}_k$. (In full, $\text{disc}(\mathbb{Z}[u]) = -2^6 3^5 13^2$.)

To determine the class number of $k$, the Minkowski bound is

$$\frac{3!}{3^3} \left(\frac{4}{\pi}\right) 3 \cdot 5\sqrt{3} = \frac{40\sqrt{3}}{3\pi} < \frac{80}{3\pi} < \frac{27}{\pi} < 9.$$ 

So we must factor 2,3,5,7. We already saw 3 and 5 have principal prime factorizations. Since $X^3 - 5$ is irreducible mod 7, $(7)$ stays prime in $\mathcal{O}_k$. Mod 2,

$$X^3 - 5 \equiv X^3 + 1 \equiv (X + 1)(X^2 + X + 1).$$

So (2) = $pq$, where $N_p = 2$ and $N_q = 4$.

Seeking principal generators for $p$ and $q$, we look for norms of elements divisible by 2. From $N_{k/\mathbb{Q}}(1 + \sqrt[3]{5}) = 6$ we must have $(1 + \sqrt[3]{5}) = p(\pi)$, so we compute

$$\frac{1 + \sqrt[3]{5}}{\pi} = \frac{1 + \sqrt[3]{5}}{2 - \sqrt[3]{5}} = \frac{(1 + \sqrt[3]{5})(2 - \sqrt[3]{5}\omega)(2 - 3\sqrt[3]{5}\omega^2)}{3} = 3 + 2\sqrt[3]{5} + \sqrt[3]{25}.$$ 

This is a generator for $p$, from which we get a generator for $q$:

$$2 = (3 + 2\sqrt[3]{5} + \sqrt[3]{25})(-1 - \sqrt[3]{5} + \sqrt[3]{25}).$$

Thus $k$ has class number 1.

Let $U > 1$ be the fundamental unit of $k$. As in [2, Lemma 2], $|\text{disc}(\mathcal{O}_K)|/4 < U^3 + 7$, so

$$U^2 > \left(\frac{3\sqrt[3]{5}^2}{4} - 7\right)^{2/3} \approx 29.6.$$ 

Alas, this is not greater than $u \approx 122.9$, so we can’t conclude that $U^2 > u$, and hence that $U = u$. Yet $U = u$ is true. How can this be proven?

**Theorem 2.** The fundamental unit of $k = \mathbb{Q}(\sqrt[3]{5})$ is $u = 41 + 24\sqrt[3]{5} + 14\sqrt[3]{25}$.

**Proof.** We use a technique taken from the tome of Delone and Faddeev on cubic fields [3, pp. 88-92]. (For a table of cubic number field data, including fundamental units, see [3, pp. 141-146].) For a list of fundamental units of pure cubic fields $\mathbb{Q}(\sqrt[3]{m})$ with $m \leq 250$, see [4].

We will show $u$ is a fundamental unit by showing $u$ is not an $j$th power of an algebraic integer in $\mathcal{O}_k$ for any $j > 1$.

Suppose $u = \rho^j$, where $\rho^3 + a\rho^2 + b\rho + c = 0$ for integers $a, b, c$. Since $\rho$ must be some power of the fundamental unit, $c = -N_{k/\mathbb{Q}}(\rho) = -1$.

The key idea we’ll use is that symmetric functions in the $\mathbb{Q}$-conjugates of $u$ are symmetric functions in the $\mathbb{Q}$-conjugates of $\rho$, and hence are integral polynomials in $a$ and $b$ (since $c = -1$ is known already). Studying such integral polynomials will impose conditions on the coefficients $a, b$. 

We will denote the conjugates of $u$ and $\rho$ with prime notation, so
\[ u + u' + u'' = 123, \quad uu' + uu'' + u'u'' = 3, \quad uu'' = 1,\]
\[ \rho + \rho' + \rho'' = -a, \quad \rho \rho' + \rho \rho'' + \rho' \rho'' = b, \quad \rho \rho \rho'' = -c = 1.\]

So if $u = \rho'$ then $123 = \text{Tr}_k/\mathbf{Q}(\rho') = F_j(a, b)$ and $3 = G_j(a, b)$ for some $F_j, G_j \in \mathbf{Z}[X, Y]$. When $j = 2$ and $3$ we can work with $F_j$ and $G_j$ directly. But for larger $j$ that becomes too cumbersome.

Let’s suppose $u = \rho^2$. Then
\[ 123 = \rho^2 + (\rho')^2 + (\rho'')^2 = (\rho + \rho' + \rho'')^2 - 2(\rho \rho' + \rho \rho'' + \rho' \rho'') = a^2 - 2b \]
and
\[ 3 = (\rho \rho')^2 + (\rho \rho'')^2 + (\rho' \rho'')^2 = b^2 - 2ac = b^2 + 2a. \]

Solving for $a$ in terms of $b$ and feeding that into the first equation,
\[ 123 = \frac{(3 - b^2)^2}{4} - 2b \Rightarrow b^4 - 6b^2 - 8b - 483 = 0. \]
Therefore $b | 483 = 3 \cdot 7 \cdot 23$, but none of the divisors is a root of the quartic polynomial. So $u$ is not a square.

Now suppose $u = \rho^3$. In general,
\[ x^3 + y^3 + z^3 = (x + y + z)^3 - 3(x + y + z)(xy + xz + yz) + 3(xyz). \]
Thus
\[ 123 = \rho^3 + (\rho')^3 + (\rho'')^3 = -a^3 + 3ab + 3 \]
and
\[ 3 = (\rho \rho')^3 + (\rho \rho'')^3 + (\rho' \rho'')^3 = b^3 + 3ab + 3. \]
The second equation says $b = 0$ or $b^2 = -3a$. If $b = 0$, then $120 = -a^3$, which is impossible. So $b^2 = -3a$, hence
\[ 123 = b^6/27 - b^3 + 3 \Rightarrow b^6 - 27b^3 - 27 \cdot 120 = 0. \]
The roots of $T^2 - 27T - 27 \cdot 120$ are 72 and −45; neither is a cube. So $u$ is not a cube.

Now suppose $u = \rho^p$ for an odd prime $p$. Then $u \pm 1$ is divisible by $\rho \pm 1$ in $\mathbf{O}_k$, so in $\mathbf{Z}$
\begin{align*}
(3) \quad & N_{k/\mathbf{Q}}(\rho + 1) | N_{k/\mathbf{Q}}(u + 1) = 128, \quad N_{k/\mathbf{Q}}(\rho - 1) | N_{k/\mathbf{Q}}(u - 1) = 120. \\
(4) \quad & N_{k/\mathbf{Q}}(\rho + 1) = 1 + a + b - c = 2 + a + b, \quad N_{k/\mathbf{Q}}(\rho - 1) = -1 + a - b - c = -a - b.
\end{align*}

By the symmetric function theorem,
\[ 123 = \rho^p + (\rho')^p + (\rho'')^p = (\rho + \rho' + \rho'')^p + pA \equiv -a^p \mod p \equiv -a \mod p \]
for some integer $A$, and similarly
\[ 3 \equiv (\rho \rho' + \rho \rho'' + \rho' \rho'')^p \equiv b^p \equiv b \mod p. \]

By (4), the divisibility relations (3) concern not $a$ and $b$ but $2 - a + b$ and $-a - b$. For odd $p$, the congruences (5) and (6) are equivalent to
\begin{align*}
(7) \quad & 2 - a + b \equiv 128 \mod p, \quad -a - b \equiv 120 \mod p. \\
(8) \quad & 2 - a + b, \quad -a - b \in \mathbf{Z}^+, \quad 2 - a + b | 128, \quad -a - b | 120.
\end{align*}
we assemble a finite list of possibilities for $2 - a + b$ and for $-a - b$, along with the corresponding possibilities for $p$.
Larger primes appear less often (only 2, 3, 5, and 7 appear more than once), so we consider primes from largest to smallest.

First, we handle the “arbitrary” case, when $2 - a + b = 128$ and $-a - b = 120$. Then $a = -123, b = 3$, so $\rho$ is a root of $T^3 - 123T^3 + 3T - 1$, i.e. $\rho = u$. This is useless.

If $p = 127$ then $2 - a + b = 1$ and $-a - b = 120$. There is no solution; $2 - a + b$ and $-a - b$ have the same parity. Similarly, there is no solution when $p = 23, 17, 13$.

If $p = 59$ then $2 - a + b = 128$ and $-a - b = 2$, so $a = -64, b = 62$. We consider a root $\rho$ of the polynomial $T^3 - 64T^2 + 62T - 1$. If $\rho \in \mathcal{O}_k$ and $u = \rho^{1/3}$, then

$$u = \rho^{1/3} \Rightarrow \mathbb{Z}[\rho] \subset \mathbb{Z} \subset \mathcal{O}_k \Rightarrow 3^2 \cdot 5^2 \mid \text{disc}(\mathbb{Z}[\rho]) | 2^6 \cdot 3^3 \cdot 5^2 \cdot 13^2.$$  

Neither of these divisibility relations holds, since $T^3 - 64T^2 + 62T - 1$ has discriminant equal to the prime $13814533$.

We can similarly eliminate the possibility of other primes:

<table>
<thead>
<tr>
<th>$p$</th>
<th>polynomial</th>
<th>discriminant</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>$T^3 - 61T^2 - 59T - 1$</td>
<td>$2^4 \cdot 3 \cdot 7 \cdot 191$</td>
</tr>
<tr>
<td>29</td>
<td>$T^3 - 65T^2 + 61T - 1$</td>
<td>$2^5 \cdot 3 \cdot 33$</td>
</tr>
<tr>
<td>19</td>
<td>$T^3 - 66T^2 + 60T - 1$</td>
<td>$3^3 \cdot 508847$</td>
</tr>
<tr>
<td>11</td>
<td>$T^3 - 68T^2 + 58T - 1$</td>
<td>$2^2 \cdot 3^3 \cdot 41809$</td>
</tr>
</tbody>
</table>

Now we need to handle the primes $\leq 7$. The cases $p = 2, 3$ have already been treated, so 5 and 7 remain.

To eliminate 5 and 7 by constructing cubic polynomials from the tables above will require over 25 cases. Instead of pursuing this idea further, we show $u$ is not a fifth or seventh power in $\mathcal{O}_k$ by showing it is not such a power in some residue field $\mathcal{O}_k / p \cong \mathbb{F}_p$.

To show $u$ is not a fifth power in some $\mathbb{F}_p$, we want $5|p - 1$, so let’s try $p = 11$. Since $X^3 - 5$ has a (single) root mod 11, there is a prime ideal $p_{11}$ with norm 11. In $\mathcal{O}_k / p_{11}$,

$$u \equiv \rho^5 \equiv \pm 1 \Rightarrow 11|N_{k/Q}(u \pm 1).$$

Since $N_{k/Q}(u + 1) = 128$ and $N_{k/Q}(u - 1) = 120$, $u$ is not a fifth power.

For seventh powers, we want $7|p - 1$. Try $p = 29$. Since $X^3 - 5$ has a (single) root $-7$ mod 29, there is a prime ideal $p_{29}$ with norm 29, and in its residue field

$$u \equiv \rho^7 \Rightarrow u^2 \equiv \rho^{14} \equiv \pm 1.$$  

We already know $u^2 - 1 = (u - 1)(u + 1)$ has norm not divisible by 29. Since $N_{k/Q}(u^2 + 1) = 2^3 \cdot 1861$, $u$ is not a seventh power.

**Theorem 3.** The field $k = Q(\sqrt[3]{5})$ has ring of integers $\mathcal{O}_k = Z[\sqrt[3]{5}]$, class number 1, discriminant $-3^3 \cdot 5^2$, and unit group $\pm u^Z$ where $u = 41 + 24\sqrt[3]{5} + 14\sqrt[3]{25}$. Also $1/u = v = 1 - 4\sqrt[3]{5} + 2\sqrt[3]{25}$. The ramified primes 3 and 5 factor as $3 = \pi^3u$ and $5 = (\sqrt[3]{5})^2$, where $\pi = 2 - \sqrt[3]{5}$. The minimal polynomials of $\pi$ and $u$ are respectively

$$T^3 - 6T^2 + 12T - 3, \quad T^3 - 123T^2 + 3T - 1.$$
We now turn to $K$. The only ramified primes are 3 and 5. Just as in [2], $(3) = \langle \eta \rangle^6$ where $\eta = \sqrt[3]{2}/\sqrt[3]{3}$, so $(\mathfrak{p}^6$ overstays properties, $p$). To find the minimal polynomial of $\eta$ over $\mathbb{Q}$, we work out the one for $\eta^2 = -\pi u = -(12 + 7\sqrt{5} + 4\sqrt{25})$:

$$N_{K/\mathbb{Q}}(-\pi u) = - N_{K/\mathbb{Q}}(\pi) = -3, \quad \text{Tr}_{K/\mathbb{Q}}(-\pi u) = -36.$$  

The linear coefficient in the minimal polynomial for $-\pi u$ is

$$3 \text{Tr}_{K/\mathbb{Q}}(1/\pi u) = 3 \text{Tr}_{K/\mathbb{Q}}(\pi^2/3) = 12,$$

so the minimal polynomial for $-\pi u$ is $T^9 + 36T^7 + 12T + 1$, hence that for $\eta$ is

$$T^6 + 36T^4 + 12T^2 + 3,$$

so $\text{disc}(Z[\eta]) = -2^63^75^423^4$.

The discriminant of $K/\mathbb{Q}$ can be calculated locally using completions at $\eta$ and at $\sqrt{5}$ (which stays prime in $K$), but instead we can use [2, Corollary 1]:

$$\text{disc}(K) = \text{disc}(F) \text{disc}(k)^2 = -375^4.$$

The ring of integers of $K$ is computed by the same technique as in [2], with a similar result:

$$O_K = O_\mathbb{k} \oplus O_\mathbb{k} \theta,$$

where $\theta = (\omega - 1)/\pi$, so $\eta = -\omega \theta$. Since

$$\theta \bar{\theta} = \frac{3}{\pi^2} = \pi u = 12 + 7\sqrt{5} + 4\sqrt{25}, \quad \theta + \bar{\theta} = -\frac{3}{\pi} = -\pi^2 u = -(4 + 2\sqrt{5}) + \sqrt{25},$$

the minimal polynomial of $\theta$ over $k$ is

$$f(T) = T^2 + \pi u T + \pi u = T^2 + (4 + 2\sqrt{5} + \sqrt{25})T + (12 + 7\sqrt{5} + 3\sqrt{25}),$$

so the minimal polynomial of $\theta$ over $\mathbb{Q}$ is

$$f(\sigma f)(\sigma^2 f) = T^6 + 12T^5 + 54T^4 + 72T^3 + 48T^2 + 18T + 3,$$

where $\sigma \in N = \text{Gal}(K/F)$ is an element of order 3. This polynomial has discriminant $-2^83^75^4$, so $O_\mathbb{k} \neq \mathbb{Z}[\eta]$. Also $O_K \neq \mathbb{Z}[\eta]$.

Now we turn to class number computations. The Minkowski bound for $K$ is

$$\frac{6!}{6^6} \left( \frac{4}{\pi} \right)^3 5^2 2^3 \sqrt{3} = \frac{2^4 5^3 \sqrt{3}}{3\pi^3} \approx 37.2.$$  

The factorization statements in [2] for $\mathbb{Q}(\sqrt[3]{2}, \omega)$ apply similarly to $K = \mathbb{Q}(\sqrt[3]{5}, \omega)$, so the only possible rational primes which don’t factor principally in $K$ are those $p \equiv 1 \pmod{3}$ where 5 is a cube mod $p$, and such primes split completely in $K$. There is one prime $\leq 37$ with these properties, $p = 13$, so $\text{Cl}(K)$ is generated by the prime ideal factors of 13. Since $N_{K/\mathbb{Q}}(\theta - 1) = g(1) = 208 = 2^4 \cdot 13$, there is a principal prime ideal factor of 13, so $h(K) = 1$.

(For the interested reader, we compute an explicit generator of a prime ideal over 13 by factoring $(\theta - 1)$. 

The factorization of 2 is $2 O_K = p \mathfrak{p} \mathfrak{p} \mathfrak{p}^2$, where $p = (3 + 2\sqrt{5} + \sqrt{25})$, and $f_2(K/Q) = 2$. Which of $p$ and its conjugates divides $(\theta - 1)$? All three ideals have quotient $\mathbb{F}_4$, so the cube roots of unity are all distinct in the corresponding residue fields.

In $O_K/p$, $1 + \sqrt[3]{25} \equiv 0 \Rightarrow \sqrt[3]{5} \equiv 1 \Rightarrow \theta \equiv \omega - 1 \equiv \omega^2 \neq 1$. 

In $O_K/\mathfrak{p}^2$, $1 + \sqrt[3]{25} \omega^2 \equiv 0 \Rightarrow \sqrt[3]{5} \equiv \omega^2 \Rightarrow \theta \equiv (\omega - 1)/\omega^2 \equiv 1$. 

In $O_K/\mathfrak{p}^2$, $1 + \sqrt[3]{25} \omega \equiv 0 \Rightarrow \sqrt[3]{5} \equiv \omega \Rightarrow \theta \equiv (\omega - 1)/(\omega^2) \equiv 1$.

Therefore $(\theta - 1) = (\mathfrak{p} \mathfrak{p}^2 \mathfrak{p}_13$, where $\mathfrak{p}_13 | (13)$, so $\mathfrak{p}_13$ is a principal ideal with

$$\beta \overset{\text{def}}{=} \frac{\theta - 1}{(3 + 2\sqrt[3]{5} + \sqrt[3]{25} \omega)^2} = -(9 + 10\sqrt[3]{5} + 5\sqrt[3]{25} + (1 + 7\sqrt[3]{5} - \sqrt[3]{25})\theta)$$
as a generator.

Now we turn to the unit group of $\mathcal{O}_K$. Since the ideal $(\eta)$ is fixed by the Galois group of $K/\mathbb{Q}$, let’s consider the unit

$$\delta = \frac{\sigma(\eta)}{\eta} \in \mathcal{O}_K^\times,$$

where $\sigma \in \text{Gal}(K/F)$ sends $\sqrt[3]{5}$ to $\sqrt[3]{5}\omega$. We have

$$\pi = 2 - \sqrt[3]{5}, \quad \sigma(\pi) = 2 - \sqrt[3]{5}\omega, \quad \sigma^2(\pi) = 2 - \sqrt[3]{5}\omega^2 = \sigma(\pi).$$

Therefore

$$\delta = \frac{\pi}{\sigma(\pi)} = \frac{\pi}{\sigma\pi},$$

so

$$|\delta|^2 = \delta\overline{\delta} = \frac{\pi^2}{\sigma^2(\pi)} = \frac{\pi^2}{3} = \nu,$$

so

$$\nu = N_{K/k}(\delta), \quad u = N_{K/k}(1/\delta).$$

The log map on $\mathcal{O}_K^\times$ is given by

$$L(x) = (2 \log |x|, 2 \log |\sigma(x)|, 2 \log |\sigma^2(x)|).$$

We compute this for $x = u, \delta, \sigma(\delta)$, keeping only the first two coordinates.

Since $N_{K/\mathbb{Q}}(u) = u\sigma(u)\overline{\sigma}(u) = u|\sigma(u)|^2$, $2 \log |\sigma(u)| = 2 \log |\sigma^2(u)| = - \log u$.

Since

$$\sigma(\delta) = \frac{\sigma(\pi)}{\sigma^2(\pi)}, \quad \sigma^2(\delta) = \frac{\sigma^2(\pi)}{\pi},$$

we get

$$2 \log |\sigma(\delta)| = 0, \quad 2 \log |\sigma^2(\delta)| = -2 \log |\delta| = - \log \nu = \log u,$$

so

$$L(u) = (2 \log u, - \log u),$$

$$L(\sigma u) = (- \log u, - \log u),$$

$$L(\delta) = (- \log u, 0),$$

$$L(\overline{\delta}) = (- \log u, \log u),$$

$$L(\sigma(\delta)) = (0, \log u).$$

In particular, notice that $L(\sigma(\delta)) = L(\overline{\delta}) - L(\delta)$, which means $\sigma(\delta) = \zeta\overline{\delta}/\delta$, where $\zeta$ is a root of unity in $K$; in fact $\sigma(\delta) = \overline{\delta}/\delta$. The regulator computations are:

<table>
<thead>
<tr>
<th>unit pair</th>
<th>regulator</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u, \delta$</td>
<td>$(\log u)^2$</td>
</tr>
<tr>
<td>$\delta, \overline{\delta}$</td>
<td>$(\log u)^2$</td>
</tr>
<tr>
<td>$u, \sigma(u)$</td>
<td>$3(\log u)^2$</td>
</tr>
</tbody>
</table>

By [2, Cor. 1], $h(K)R(K) = h(F)R(F)/(h(k)R(k))^2 = (\log u)^2$, so

$$[\mathcal{O}_K^\times / \mu_K : \langle \delta, \overline{\delta} \rangle] = \frac{\text{Reg}(\delta, \overline{\delta})}{R(K)} = (\log u)^2 / R(K) = h(K).$$

We already checked $h(K) = 1$, so $\{\delta, \overline{\delta}\}$ is a pair of fundamental units for $K$.

To match the notation for fundamental units in [2], let

$$\epsilon \overset{\text{def}}{=} \omega^2 \delta = \omega^2 \frac{\pi}{\sigma(\pi)} = -7 + 4\sqrt[3]{5} + (7\sqrt[3]{5} - 12)\theta = 1 - 4\pi + (2 - 7\pi)\theta.$$

We know $\{\epsilon, \overline{\epsilon}\}$ is a pair of fundamental units. Might $\mathcal{O}_K = \mathbb{Z}[\epsilon]$? Let’s find the polynomial for $\epsilon$ over $k$, and then descend to $\mathbb{Q}$. 

We compute
\[ \text{Tr}_{K/k}(\varepsilon) = \omega^2 \frac{\pi}{\sigma(\pi)} + \omega \frac{\pi}{\sigma^2(\pi)} = \frac{\pi^2}{3} (\omega^2 \sigma^2(\pi) + \omega \sigma(\pi)) = \frac{\pi^2}{3} (-\pi) = -v. \]

So \( \varepsilon \) and \( \bar{\varepsilon} \) are both roots of \( f(T) = T^2 + vT + v \). (This is analogous to the role of the polynomial \( T^2 + uT + u \) in [2].) So the minimal polynomial of \( \varepsilon \) over \( \mathbb{Q} \) is
\[ f \sigma(f) \sigma^2(f) = T^6 + 3T^5 + 126T^4 + 247T^3 + 126T^2 + 3T + 1. \]

Alas, the discriminant of this is \(-2^{12}3^75^413^6\), so \( \mathcal{O}_K \neq \mathbb{Z} \{ \varepsilon \} \). (As an aside, the polynomial has symmetric coefficients, so \( \varepsilon^{-1} \) is a root, and in fact \( \varepsilon^{-1} = \sigma^2(\varepsilon) \).)

**Theorem 4.** The field \( K = \mathbb{Q}(\sqrt[3]{87} \omega) \) has class number 1, discriminant \(-3^75^4\), and regulator \((\log(41 + 24\sqrt[3]{5} + 14\sqrt[3]{25}))^2\). The ramified primes 3 and 5 factor as
\[ (3) = (\eta)^6, \quad (5) = (\sqrt[3]{5})^3, \]
where \( \eta = \sqrt{-3}/\pi, \pi = 2 - \sqrt[3]{5} \).

The ring of integers of \( K \) is \( \mathcal{O}_K \oplus \mathcal{O}_K \theta \), where \( \theta = (\omega - 1)/\pi \). The unit group of \( \mathcal{O}_K \) has six roots of unity, rank 2, and basis \( \{ \varepsilon, \sigma \} \), where
\[ \varepsilon = \omega^2 \pi / \sigma(\pi) \]
has minimal polynomial
\[ g(T) = T^6 + 3T^5 + 126T^4 + 247T^3 + 126T^2 + 3T + 1. \]

There is no power basis for \( \mathcal{O}_K \). For a more general result, see [1].

We now return to the computation of \( \text{Cl}(K) \). We noted that \( \text{Cl}(K) \) is generated by the prime ideal factors of 13, and then showed those factors are principal, using the special element \( \theta \). Here is an alternative computation of \( h(K) = 1 \) which does not depend on knowing about \( \theta \).

Let’s assume \( h(K) 
eq 1 \), i.e. none of the prime ideals over 13 in \( K \) is principal. Then the Galois group of \( K/\mathbb{Q} \) acts transitively on the nonidentity classes of \( \text{Cl}(K) \), and we show by this action that \( h(K) = 3 \) if \( h(K) > 1 \).

Let \( \mathfrak{P} \) be one prime ideal in \( K \) lying over 13. Let \( \tau \) denote complex conjugation, so \( \tau \sigma = \sigma^2 \tau \). Since \( k \) has class number 1, \( \mathfrak{P} \tau(\mathfrak{P}) \sim 1 \). Therefore
\[ \sigma(\mathfrak{P}) \tau(\sigma(\mathfrak{P})) \sim 1 \Rightarrow \sigma(\mathfrak{P}) \sigma^2(\tau(\mathfrak{P})) \sim 1 \Rightarrow \mathfrak{P} \sigma(\tau(\mathfrak{P})) \sim 1. \]
Therefore \( \tau \mathfrak{P} \sim \sigma(\tau \mathfrak{P}) \sim 1 \). So \( [\mathfrak{P}] \in \text{Cl}(K) \) is fixed by \( \tau \sigma \tau = \sigma^2 \), so its stabilizer subgroup is either \( \{ 1, \sigma, \sigma^2 \} \) or \( G \). Thus the number of nonidentity elements in \( \text{Cl}(K) \) is 1 or 2, so \( h(K) = 2 \) or 3. Since
\[ \mathfrak{P} \sigma(\mathfrak{P}) \sigma^2(\mathfrak{P}) = N_{K/E}(\mathfrak{P}) = (1 \pm 2\sqrt{-3}) \sim 1, \]
\( [\mathfrak{P}]^3 = 1 \), hence \( 3|h(K) \). So if \( h(K) > 1 \) then \( \text{Cl}(K) = \{ 1, [\mathfrak{P}], [\tau \mathfrak{P}] \} \) is cyclic of size 3.

We saw earlier that \( [\mathcal{O}_K^\times / \mu_K : \langle \delta, \overline{\delta} \rangle] = h(K) \). Assume \( h(K) = 3 \). We shall apply the results in [2, Thm. 4] about index 3 sublattices of \( \mathbb{Z}^3 \). In particular, neither \( L(\delta) \) nor \( L(\overline{\delta}) \) is in \( 3L \), so if the index is 3 then there is a basis \( \{ \delta, \xi \} \) of \( \mathcal{O}_K^x / \mu_K \), where
\[ \overline{\delta} = \zeta \xi^3 \quad \text{or} \quad \delta / \overline{\delta} = \zeta \xi^3 \]
for some root of unity \( \zeta \). Applying \( N_{K/k} \) to the first possibility yields \( v^2 = (N_{K/k}(\xi))^3 \) in \( \mathcal{O}_k^x \), which is absurd since \( v \) is a generator of \( \mathcal{O}_k^x \). Applying the log map to the second possibility yields
\[ L(\delta) - L(\overline{\delta}) = -L(\sigma(\delta)) \in 3L, \]
so by Galois action we have $L(\delta), L(\overline{\delta}) \in 3L$, a contradiction of $|L(\mathcal{O}_K^\times) : L(\delta)\mathbb{Z} + L(\overline{\delta})\mathbb{Z}| = 3$. Therefore $h(K) = 1$.

Here’s another point of view on the link between $h(K) = 1$ and principal factorization of $13 \mathcal{O}_K$. Since $N_{k/\mathbb{Q}}(2 + \sqrt[3]{5}) = 13$,

$$13 = (2 + \sqrt[3]{5})(2 + \sqrt[3]{5}\omega)(2 + \sqrt[3]{5}\omega^2) = (2 + \sqrt[3]{5})(4 - 2\sqrt[3]{5} + \sqrt[3]{25}).$$

We want to factor the second term on the right in $\mathcal{O}_k$. Since $N_{k/\mathbb{Q}}(1 + \sqrt[3]{25}) = 26$ and $h(k) = 1$, by (2) we must have a numerical factorization

$$1 + \sqrt[3]{25} = (3 + 2\sqrt[3]{5} + \sqrt[3]{25})(a + b\sqrt[3]{5} + c\sqrt[3]{25})$$

for some $a, b, c \in \mathbb{Z}$. Multiplying the two terms on the right we get a solution $a = -3, b = -2, c = 0$, i.e. $N_{k/\mathbb{Q}}(-3 + 2\sqrt[3]{5}) = 13$. Guided by (9), we divide $-3 + 2\sqrt[3]{5}$ into $4 - 2\sqrt[3]{5} + \sqrt[3]{25}$ to get the principal (in fact, numerical) factorization of 13 in $\mathbb{Z}[\sqrt[3]{5}]$:

$$13 = (2 + \sqrt[3]{5})(-3 + 2\sqrt[3]{5})(2 + 2\sqrt[3]{5} + \sqrt[3]{25}).$$

So 13 has principal prime factors in $\mathcal{O}_K$ if and only if the ideal $(2 + \sqrt[3]{5})$ of $k$ is the norm of a principal ideal in $K$, i.e. there is some $\alpha \in \mathcal{O}_K$ such that

$$N_{K/k}(\alpha) = \pm(2 + \sqrt[3]{5})u^m$$

for some $m \in \mathbb{Z}$. The norm must be positive, so the plus sign must hold. Since $u = N_{K/k}(1/\delta)$, $h(K) = 1$ if and only if $2 + \sqrt[3]{5}$ is a norm from $K$.

To explicitly exhibit $2 + \sqrt[3]{5}$ as a norm from $K$, we consider the generator $\beta$ of one of the prime factors of $13 \mathcal{O}_K$. Does $N_{K/k}(\beta) = 2 + \sqrt[3]{5}$? No, since $N_{K/k}(\beta) = 342 + 200\sqrt[3]{5} + 117\sqrt[3]{25}$, which is much larger than $2 + \sqrt[3]{5}$. By (10), $N_{K/k}(\beta)$ must equal $(2 + \sqrt[3]{5})u^m$, $(-3 + 2\sqrt[3]{5})u^m$, or $(2 + 2\sqrt[3]{5} + \sqrt[3]{25})u^m$ for some integer $m$. Taking logarithms to check in each case whether the unknown $m$ is an integer, we find that

$$N_{K/k}(\beta) = (2 + 2\sqrt[3]{5} + \sqrt[3]{25})u.$$  

The prime ideals in $\mathcal{O}_K$ lying over $(2 + \sqrt[3]{5})$ and $(2 + 2\sqrt[3]{5} + \sqrt[3]{25})$ are conjugate by $\sigma$ or $\sigma^2$, so let’s consider $N_{K/k}(\sigma\beta)$. Using PARI, $\sigma(\theta) = -4 + \sqrt[3]{25} - (6 - 2\sqrt[3]{25})\theta$, from which we compute

$$N_{K/k}(\sigma\beta) = \sigma(\beta)\sigma(\beta) = (2 + \sqrt[3]{5})u^{-2}.$$  

Thus

$$2 + \sqrt[3]{5} = N_{K/k}(\sigma\beta)u^2 = N_{K/k}(\sigma(\beta)/\delta^2).$$

**References**


