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

KEITH CONRAD

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

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

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

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

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.

As in [2], $\mathcal{O}_k = \mathbf{Z}[\sqrt[3]{3}]$, so $\mathrm{disc}(\mathcal{O}_k) = -\mathrm{N}_{k/\mathbf{Q}}(3(\sqrt[3]{3})^2) = -3^5$. The prime 3 is totally ramified: $3 = (\sqrt[3]{3})^3$.

The Minkowski bound for k is

$$\frac{3!}{3^3}\left(\frac{4}{\pi}\right)3^2\sqrt{3} = \frac{8\sqrt{3}}{\pi} < \frac{8(7/4)}{\pi} = \frac{14}{\pi} < 5.$$

We saw 3 factors principally in K. To factor 2, we note

$$X^3 - 3 \equiv X^3 + 1 \equiv (X+1)(X^2+X+1) \bmod 2,$$

so $2 = \mathfrak{p}\mathfrak{q}$ where $\mathrm{N}\,\mathfrak{p} = 2$, $\mathrm{N}\,\mathfrak{q} = 4$. The norm form for k is

$$\mathrm{N}_{k/\mathbf{Q}}(a + b\sqrt[3]{3} + c\sqrt[3]{9}) = a^3 + 3b^3 + 9c^3 - 9abc.$$

So $\mathrm{N}_{k/\mathbf{Q}}(-1+\sqrt[3]{3}) = 2$, from which we get principal generators for the prime factors of 2:

$$\mathfrak{p} = (-1+\sqrt[3]{3}), \mathfrak{q} = (1+\sqrt[3]{3}+\sqrt[3]{9})$$

Therefore $h(k) = 1$.

Also note $\mathrm{N}_{k/\mathbf{Q}}(2+\sqrt[3]{3} = \sqrt[3]{9}) = 2$, leading to

$$2+\sqrt[3]{3}+\sqrt[3]{9} = (-1+\sqrt[3]{3})(4+3\sqrt[3]{3}+2\sqrt[3]{9}).$$

Therefore $u \stackrel{\text{def}}{=} 4 + 3\sqrt[3]{3} + 2\sqrt[3]{9} \approx 12.4$ is a unit in $\mathcal{O}_k$, with $v \stackrel{\text{def}}{=} 1/u = -2 + \sqrt[3]{9}$. Therefore

$$\mathrm{Tr}_{k/\mathbf{Q}}(u) = 12, \quad \mathrm{Tr}_{k/\mathbf{Q}}(v) = -6, \quad \mathrm{N}_{k/\mathbf{Q}}(u) = \mathrm{N}_{k/\mathbf{Q}}(v) = 1.$$

So the minimal polynomial for u over $\mathbf{Q}$ is

$$T^3 - 12T^2 - 6T - 1.$$

Therefore

$$\begin{aligned}
\mathrm{disc}(\mathbf{Z}[u]) &= -\mathrm{N}_{k/\mathbf{Q}}(3u^2 - 24u - 6) \\
&= -3^3\,\mathrm{N}_{k/\mathbf{Q}}(u^2 - 8u - 2) \\
&= -3^3\,\mathrm{N}_{k/\mathbf{Q}}(18 + 12\sqrt[3]{3} + 9\sqrt[3]{9}) \\
&= -3^3\,\mathrm{N}_{k/\mathbf{Q}}(3\sqrt[3]{3})\,\mathrm{N}_{k/\mathbf{Q}}(4 + 3\sqrt[3]{3} + 2\sqrt[3]{3}) \\
&= -3^7.
\end{aligned}$$

So $\mathcal{O}_k \neq \mathbf{Z}[u]$. For U the fundamental unit of $\mathcal{O}_k$,

$$U^2 > \left(\frac{3^5}{4} - 7\right)^{2/3} \approx 14.242 > u,$$

so u is the fundamental unit of $\mathcal{O}_k$ by [2, Lemma 3].

We now turn to K. By [2, Corollay 7],

$$\mathrm{disc}(K) = \mathrm{disc}(F)\,\mathrm{disc}(k)^2 = -3^{11}.$$

The prime 3 totally ramifies as $(3) = (\eta)^6$ where $\eta = \sqrt{-3}/\sqrt[3]{3} = \sqrt[6]{-3}$. Since $\mathrm{disc}(\mathbf{Z}[\eta]) = \mathrm{N}_{K/\mathbf{Q}}(6\eta^5) = -2^6 3^{11}$, $\mathcal{O}_K \neq \mathbf{Z}[\eta]$. As in [2],

$$\mathcal{O}_K = \mathcal{O}_k \oplus \mathcal{O}_k\,\theta,$$

where $\theta = (\omega - 1)/\sqrt[3]{3}$. Note $\eta = -\omega\theta$; θ and η are both sixth roots of -3. For what it is worth, $\theta + \overline{\theta} = -\sqrt[3]{9}$ and $\theta\overline{\theta} = \sqrt[3]{3}$.

The Minkowski bound on K is

$$\frac{6!}{6^6}\left(\frac{4}{\pi}\right)^3 3^5\sqrt{3} = \frac{240\sqrt{3}}{\pi^3} \approx 13.4.$$

A rational prime p factors principally in K unless perhaps $p \equiv 1 \bmod 3$ and $3^{(p-1)/3} \equiv 1 \bmod p$. This is not the case for any prime up to 13, so $h(K) = 1$. Hence

$$R(K) = (\log u)^2.$$

So the units u and $\sigma(u)$ generate a subgroup of the units of K (mod torsion) with index $3h(K) = 3$. This implies that there exists $\varepsilon \in \mathcal{O}_K^\times$ and $\zeta \in \{1, \omega, \omega^2\}$ such that $u/\sigma(u) = \zeta\varepsilon^3$ or $u\sigma(u) = \zeta\varepsilon^3$, and then $\{u, \varepsilon\}$ is a basis for the units. We now find ε explicitly.

(The slick trick that works for $\mathbf{Q}(\sqrt[3]{2}, \omega)$ in [2] and $\mathbf{Q}(\sqrt[3]{5}, \omega)$ in [3] fails here: for σ a generator of $\mathrm{Gal}(K/F)$, $\sigma(\eta)/\eta = \omega^2$ is a root of unity, not a unit of infinite order. In fact, for $\tilde{\eta} = \zeta\sqrt{-3}/\sqrt[3]{3}u^m = \zeta\eta/u^m$ equal to the ratio of any two generators for the prime ideals in F and k lying over 3, $\sigma(\tilde{\eta})/\tilde{\eta} = \omega^2(u/\sigma u)^m$ can't be a basis for the units along with u, since they generate a subgroup of index at least 3.)

The equation $u\sigma(u) = \zeta\varepsilon^3$ is ruled out since it implies $L(\sigma^2 u) \in 3L$, so then $L(u), L(\sigma u) \in 3L$, contradicting index 3. So $u/\sigma(u) = \zeta\varepsilon^3$. The prime ideal $\mathfrak{p} = (-1 + \sqrt[3]{3})$ of k lying over 2 stays prime when extended to K, with residue field growing to $\mathbf{F}_4$. In $\mathcal{O}_K/(-1 + \sqrt[3]{3})$,

$$u \equiv 1, \quad \sigma(u) \equiv \omega \Rightarrow \frac{1}{\omega} \equiv \zeta.$$

So

$$u/\sigma(u) = \zeta\varepsilon^3.$$

From this we apply various elements of $\mathrm{Gal}(K/\mathbf{Q})$ to get

$$2\log|\varepsilon| = \log u, \quad 2\log|\sigma\varepsilon| = 0, \quad 2\log|\sigma^2(\varepsilon)| = -\log u.$$

Let's find the polynomial for ε over k. We have $\mathrm{N}_{K/k}(\varepsilon) = \varepsilon\overline{\varepsilon} = u$ and $\mathrm{Tr}_{K/k}(\varepsilon^3) = (\mathrm{Tr}_{K/k}(\varepsilon))^3 - 3u\,\mathrm{Tr}_{K/k}(\varepsilon)$, while more explicitly

$$\begin{aligned}
\mathrm{Tr}_{K/k}(\varepsilon^3) &= \omega\frac{u}{\sigma u} + \omega^2\frac{u}{\overline{\sigma}(u)} \\
&= \frac{\omega u\sigma^2 u + \omega^2 u\sigma u}{(\sigma u)(\sigma^2 u)}\cdot\frac{u}{u} \\
&= u^2(\omega\sigma^2 u + \omega^2\sigma u) \\
&= 26 + 18\sqrt[3]{3} + 12\sqrt[3]{9} \\
&= -2(1+3u).
\end{aligned}$$

So $\mathrm{Tr}_{K/k}(\varepsilon)$ is a root of $T^3 - 3uT - 2(1+3u)$. Using PARI, one root of this is $-1-\sqrt[3]{3}$. So the other two roots r_1 and r_2 satisfy $r_1 + r_2 = 1 + \sqrt[3]{3}$ and $r_1r_2 = -(11 + 7\sqrt[3]{3} + 5\sqrt[3]{9})$. So by the quadratic formula, r_1 and r_2 equal

$$\frac{1}{2}\left(1 + \sqrt[3]{3} \pm \sqrt{45 + 30\sqrt[3]{3} + 21\sqrt[3]{9}}\right).$$

Since the number under the square root should be a square in k and $45 + 30\sqrt[3]{3} + 21\sqrt[3]{9} = (\sqrt[3]{9})^2(10 + 7\sqrt[3]{3} + 5\sqrt[3]{9})$, with the norm of the second factor equal to 4, we expect the second factor is the square of an algebraic integer with norm 2:

$$10 + 7\sqrt[3]{3} + 5\sqrt[3]{9} = (-1+\sqrt[3]{3})^2 u^{2m}.$$

Some computer calculations show $m = 1$ works, leading to

$$\{r_1, r_2\} = \{2 + 2\sqrt[3]{3} + \sqrt[3]{9}, \quad -1 - \sqrt[3]{3} - \sqrt[3]{9}\}.$$

Thus

$$\mathrm{Tr}_{K/k}(\varepsilon) = \{-1-\sqrt[3]{3}, -1-\sqrt[3]{3}-\sqrt[3]{9}, 2+2\sqrt[3]{3}+\sqrt[3]{9}\}.$$

Let's try to find ε as a root of

$$T^2 + (1+\sqrt[3]{3})T + u.$$

A root should generate the same field over k as $K = k(\sqrt{-3})$, so

$$\frac{(1+\sqrt[3]{3})^2 - 4u}{-3} = \frac{45 + 30\sqrt[3]{3} + 21\sqrt[3]{3}}{9}$$

should be a square in k. Factoring out a $(\sqrt[3]{9})^2$ we have

$$45 + 30\sqrt[3]{3} + 21\sqrt[3]{3} = (\sqrt[3]{9})^2(10 + 7\sqrt[3]{3} + 5\sqrt[3]{9}) = (\sqrt[3]{9}(-1+\sqrt[3]{3})u)^2.$$

So the roots of $T^2 + (1+\sqrt[3]{3})T + u$ are

$$\frac{1}{2}\left(-(1+\sqrt[3]{3}) \pm \sqrt{-3}\cdot\frac{\sqrt[3]{9}}{3}\left(2+\sqrt[3]{3}+\sqrt[3]{9}\right)\right).$$

Writing $\sqrt{-3} = 2\omega + 1 = 3 + 2\sqrt[3]{3}\theta$, we get the roots are

$$1 + \sqrt[3]{3} + \sqrt[3]{9} + (2 + \sqrt[3]{3} + \sqrt[3]{9})\theta, \quad -2 - 2\sqrt[3]{3} - \sqrt[3]{9} - (2 + \sqrt[3]{3} + \sqrt[3]{9})\theta.$$

The cube of the first root is $u/\sigma u$ (the cube of the second is $u/\sigma^2 u$). So

$$\varepsilon \stackrel{\text{def}}{=} 1 + \sqrt[3]{3} + \sqrt[3]{9} + (2 + \sqrt[3]{3} + \sqrt[3]{9})\theta.$$

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

$$T^6 + 3T^5 + 15T^4 + 10T^3 + 15T^2 + 3T + 1,$$

which has discriminant $-2^{16}3^{11}$, so $\mathcal{O}_K \neq \mathbf{Z}[\varepsilon]$. Similarly, $\omega\varepsilon$ is a root of

$$T^6 + 3T^5 + 6T^4 - 17T^3 + 6T^2 + 3T + 1$$

with discriminant $-2^{12}3^{11}5^2$ and $\omega^2\varepsilon$ is a root of

$$T^6 - 6T^5 + 6T^4 + 10T^3 + 6T^2 - 6T + 1$$

with discriminant $-2^{10}3^{11}$.

So $\zeta\varepsilon$, for ζ any root of unity, never gives rise to a power basis for $\mathcal{O}_K$.

Theorem 2. *The field $K = \mathbf{Q}(\sqrt[3]{3}, \omega)$ has class number 1, discriminant -3^{11}, and regulator $(\log(4 + 3\sqrt[3]{3} + 2\sqrt[3]{9}))^2$. The ramified prime 3 factors as*

$$(3) = (\eta)^6,$$

where $\eta = \sqrt{-3}/\sqrt[3]{3} = \sqrt[6]{-3}$.

The ring of integers of K is $\mathcal{O}_k \oplus \mathcal{O}_k\,\theta$, where $\theta = (\omega - 1)/\sqrt[3]{3}$. The unit group of $\mathcal{O}_K$ has six roots of unity, rank 2, and basis $\{\varepsilon, \overline{\varepsilon}\}$, where

$$\varepsilon = 1 + \sqrt[3]{3} + \sqrt[3]{9} + (2 + \sqrt[3]{3} + \sqrt[3]{9})\theta$$

has minimal polynomial

$$T^6 + 3T^5 + 15T^4 + 10T^3 + 15T^2 + 3T + 1.$$

There is no power basis for $\mathcal{O}_K$. In fact, the only pure cubic field whose splitting field has a power basis for its ring of integers is $\mathbf{Q}(\sqrt[3]{2})$! See [1].

References

[1] M-L. Chang, Non-monogenity in a family of sextic fields, *J. Number Theory* **97** (2002), 252–268.

[2] K. Conrad, The Splitting Field of $X^3 - 2$ over $\mathbf{Q}$. Online at `https://kconrad.math.uconn.edu/blurbs/gradnumthy/Qw2.pdf`.

[3] K. Conrad, The Splitting Field of $X^3 - 5$ over $\mathbf{Q}$. Online at `https://kconrad.math.uconn.edu/blurbs/gradnumthy/Qw5.pdf`.