

THE SPLITTING FIELD OF $X^3 - 7$ OVER \mathbf{Q}

KEITH CONRAD

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

$$K = \mathbf{Q}(\sqrt[3]{7}, \omega),$$

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

$$\begin{aligned} k &= \mathbf{Q}(\sqrt[3]{7}), \\ K &= \mathbf{Q}(\sqrt[3]{7}, \omega), \\ F &= \mathbf{Q}(\omega) = \mathbf{Q}(\sqrt{-3}), \\ G &= \text{Gal}(K/\mathbf{Q}) \cong S_3, \\ N &= \text{Gal}(K/F) \cong A_3, \\ H &= \text{Gal}(K/k). \end{aligned}$$

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 $p \equiv 1 \pmod{3}$ and p stays prime if $p \equiv 2 \pmod{3}$.*

We now turn to the field k .

Since $\text{disc}(\mathbf{Z}[\sqrt[3]{7}]) = -N_{k/\mathbf{Q}}(3(\sqrt[3]{7})^2) = -3^3 7^2$, only 3 and 7 can ramify in k . Clearly 7 is totally ramified: $(7) = (\sqrt[3]{7})^3$. The prime 3 is also totally ramified, since

$$(X + 1)^3 - 7 = X^3 + 3X^2 + 3X - 6$$

is Eisenstein at 3. So by [2, Lemma 2], $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{7}]$ and $\text{disc}(\mathcal{O}_K) = -3^3 7^2$.

Let's find the fundamental unit of k . The norm form for k is

$$(1) \quad N_{k/\mathbf{Q}}(a + b\sqrt[3]{7} + \sqrt[3]{49}) = a^3 + 7b^3 + 49c^3 - 21abc,$$

so an obvious unit is $v \stackrel{\text{def}}{=} 2 - \sqrt[3]{7}$, which is between 0 and 1. Let $u \stackrel{\text{def}}{=} 1/v = 4 + 2\sqrt[3]{7} + \sqrt[3]{49} \approx 11.4$. Letting U be the fundamental unit for \mathcal{O}_k , we have

$$\frac{3^3 7^2}{4} < U^3 + 7 \Rightarrow U^2 > \left(\frac{3^3 7^2}{4} - 7 \right)^{2/3} \approx 47.1 > u,$$

so $U = u$.

(It turns out that $\mathbf{Z}[u] = \mathbf{Z}[\sqrt[3]{7}]$ – explicitly, $\sqrt[3]{7} = -4 + 12u - u^2$.)

The Minkowski bound for k is

$$\frac{3!}{3^3} \left(\frac{4}{\pi} \right) 21\sqrt{3} = \frac{56\sqrt{3}}{3\pi} \approx 10.3,$$

so we factor 2, 3, 5, 7. Since

$$X^3 - 7 \equiv (X + 1)(X^2 + X + 1) \pmod{2}, \quad X^3 - 7 = (X - 3)(X^2 + 3X - 1) \pmod{5},$$

so

$$(2) \quad (2) = \mathfrak{p}_2 \mathfrak{p}'_2, \quad (3) = \mathfrak{p}_3^3, \quad 5 = \mathfrak{p}_5 \mathfrak{p}'_5, \quad (7) = (\sqrt[3]{7})^3,$$

where $N \mathfrak{p}_2 = 2$, $N \mathfrak{p}'_2 = 4$, $N \mathfrak{p}_5 = 5$, $N \mathfrak{p}'_5 = 25$.

If \mathfrak{p}_2 is principal, say $\mathfrak{p}_2 = (\alpha)$, then $N_{k/\mathbf{Q}}(\alpha) = 2$. But by (1), the norm of an element of $\mathbf{Z}[\sqrt[3]{7}]$ is a cube mod 7, so there is no algebraic integer with norm 2, since the only nonzero cubes mod 7 are ± 1 . Thus \mathfrak{p}_2 is not principal, so $h(k) > 1$. Similarly \mathfrak{p}_3 is not principal. Since $\mathfrak{p}_3^3 = (3)$, $[\mathfrak{p}_3]$ has order 3 in $\text{Cl}(k)$, hence $3 \mid h(k)$. We now show that $[\mathfrak{p}_3]$ generates $\text{Cl}(k)$, so $h(k) = 3$.

By (2), $\text{Cl}(k)$ is generated by $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5$. Since $N_{k/\mathbf{Q}}(2 + \sqrt[3]{7}) = 15$, $\mathfrak{p}_3 \mathfrak{p}_5 \sim 1$, so $\mathfrak{p}_5 \sim \mathfrak{p}_3^2$. Since $N_{k/\mathbf{Q}}(-1 + \sqrt[3]{7}) = 6$, $\mathfrak{p}_2 \sim \mathfrak{p}_3^2$. Therefore $\text{Cl}(k)$ is generated by $[\mathfrak{p}_3]$.

Theorem 2. *The field $k = \mathbf{Q}(\sqrt[3]{7})$ has class number 3 and discriminant $-3^3 7^2$. The ramified primes 3 and 7 factor as*

$$(3) = (3, 1 - \sqrt[3]{7})^3, \quad (7) = (\sqrt[3]{7})^3,$$

with $\mathfrak{p}_3 = (3, 1 - \sqrt[3]{7})$ generating $\text{Cl}(k) \cong \mathbf{Z}/3\mathbf{Z}$. The ring of integers of k is $\mathbf{Z}[\sqrt[3]{7}]$. The unit group of \mathcal{O}_k has two roots of unity, rank 1, and generator $u = 4 + 2\sqrt[3]{7} + \sqrt[3]{49}$. The minimal polynomial of u is

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

and $\mathcal{O}_k = \mathbf{Z}[u]$.

We now turn to $K = \mathbf{Q}(\sqrt[3]{7}, \omega)$. By [2, Corollary 7], the discriminant is

$$\text{disc}(K) = \text{disc}(F) \text{disc}(k)^2 = -3^7 7^4.$$

Let's factor the ramified primes 3 and 7. In \mathcal{O}_F , $(7) = (2 + \sqrt{-3})(2 - \sqrt{-3})$. In \mathcal{O}_k , $(7) = (\sqrt[3]{7})^3$. So in \mathcal{O}_K , $3 \mid e_7$ and $g_7 \geq 2$, hence $e_7 = 3$ and $g_7 = 2$. Thus 7 factors principally, with ramification index 3:

$$(3) \quad 7 \mathcal{O}_K = (2 + \sqrt{-3})^3 (2 - \sqrt{-3})^3.$$

Since

$$3 \mathcal{O}_F = (\sqrt{-3})^2, \quad 3 \mathcal{O}_k = \mathfrak{p}_3^3,$$

we get $3 \mathcal{O}_K = \mathfrak{P}_3^6$. Therefore $g\mathfrak{P}_3 = \mathfrak{P}_3$ for all $g \in G$ and

$$(4) \quad \mathfrak{P}_3^3 = \sqrt{-3} \mathcal{O}_K, \quad \mathfrak{P}_3^2 = \mathfrak{p}_3 \mathcal{O}_K.$$

The ideal \mathfrak{P}_3 is not principal, since if $\mathfrak{P}_3 = (x)$ then $N_{K/k} \mathfrak{P}_3 = \mathfrak{p}_3 = (N_{K/k}(x))$ is principal, which is not so. By (4), $[\mathfrak{P}_3] \in \text{Cl}(K)$ has order 3.

To compute $\text{Cl}(K)$, we compute the Minkowski bound:

$$\frac{6!}{6^6} \left(\frac{4}{\pi}\right)^3 7^2 3^3 \sqrt{3} = \frac{3920\sqrt{3}}{3\pi^3} \approx 72.992,$$

so $\text{Cl}(K)$ is generated by the prime ideal factors of all rational primes ≤ 71 :

$$(5) \quad 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71.$$

We will determine relations in $\text{Cl}(K)$ that allow us to avoid working directly with most of the primes.

By (3), we can ignore $p = 7$.

If $p \equiv 1 \pmod{3}$ and $7 \pmod{p}$ is not a cube (with $p \neq 7$), then $p = \alpha \bar{\alpha}$ in \mathcal{O}_F and p stays prime in \mathcal{O}_k . Thus $f_p(K/\mathbf{Q}) = 3$, $g_p(K/\mathbf{Q}) = 2$, so $\alpha \mathcal{O}_K$ and $\bar{\alpha} \mathcal{O}_K$ are prime, hence p

factors principally in \mathcal{O}_K . This applies to the primes 13, 31, 37, 43, 61, 67. The only $p \equiv 1 \pmod{3}$, $p \leq 71$, $p \neq 7$, which it does not apply to is $p = 19$. We'll consider the prime factors of 19 in \mathcal{O}_K later.

Turning to the case of $p \equiv 2 \pmod{3}$, we have $p\mathcal{O}_k = \mathfrak{p}\mathfrak{p}'$ where $N\mathfrak{p} = p$, $N\mathfrak{p}' = p^2$. From this we get that in \mathcal{O}_K , $\mathfrak{P} \stackrel{\text{def}}{=} \mathfrak{p}\mathcal{O}_K$ is prime, $\overline{\mathfrak{P}} = \mathfrak{P}$, and $\mathfrak{p}'\mathcal{O}_K = \sigma\mathfrak{P}\sigma^2\mathfrak{P} = \sigma\mathfrak{P}\sigma\mathfrak{P}$, where σ is a generator of $N = \text{Gal}(K/F)$, i.e. σ has order 3 in $G = \text{Gal}(K/\mathbf{Q})$. If p is a norm from $\mathbf{Z}[\sqrt[3]{7}]$, then $p \equiv \pm 1 \pmod{7}$, \mathfrak{p} is principal in \mathcal{O}_k , and \mathfrak{P} (and hence each of its Galois conjugates) is principal in \mathcal{O}_K . The $p \equiv 2 \pmod{3}$ in (5) that are $\equiv \pm 1 \pmod{7}$ are $p = 29, 41, 71$, and happily they are all norms from $\mathbf{Z}[\sqrt[3]{7}]$:

$$29 = N_{k/\mathbf{Q}}(-3 + 2\sqrt[3]{7}), \quad 41 = N_{k/\mathbf{Q}}(-2 + \sqrt[3]{49}), \quad 71 = N_{k/\mathbf{Q}}(4 + \sqrt[3]{7}).$$

So 29, 41, 71 factor principally in \mathcal{O}_K . For the other $p \equiv 2 \pmod{3}$, which are not norms from $\mathbf{Z}[\sqrt[3]{7}]$, Theorem 2 says $\mathfrak{p} \sim \mathfrak{p}_3$ or $\mathfrak{p} \sim \mathfrak{p}_3^2$ in $\text{Cl}(k)$. Extending these relations from $\text{Cl}(k)$ to $\text{Cl}(K)$ implies $\mathfrak{P} \sim \mathfrak{P}_3^2$ or $\mathfrak{P} \sim \mathfrak{P}_3^4 \sim \mathfrak{P}_3$ in $\text{Cl}(K)$. Since \mathfrak{P}_3 is fixed by $\text{Gal}(K/\mathbf{Q})$, applying G to \mathfrak{P} shows all prime ideal factors of p in \mathcal{O}_K are equivalent to \mathfrak{P}_3 or \mathfrak{P}_3^2 in $\text{Cl}(K)$.

To summarize, $\text{Cl}(K)$ is generated by $[\mathfrak{P}_3]$ (with order 3) and the prime ideal factors of 19. It turns out that the factors of 19 are related to \mathfrak{P}_3 in $\text{Cl}(K)$, so $h(K) = 3$. To show this, we'll need to factor some principal ideals of \mathcal{O}_K , which requires using some explicit algebraic integers in \mathcal{O}_K . So let's defer calculation of $\text{Cl}(K)$ and turn to computing a basis for \mathcal{O}_K .

Since $\mathcal{O}_F = \mathbf{Z}[\omega]$ is a PID, \mathcal{O}_K is a free \mathcal{O}_F -module of rank 3. To find a basis we will use $\text{disc}(K/F)$:

$$\text{disc}(K/\mathbf{Q}) = N_{F/\mathbf{Q}}(\text{disc}(K/F)) \text{disc}(F/\mathbf{Q})^3 \Rightarrow N_{F/\mathbf{Q}}(\text{disc}(K/F)) = 3^4 7^4.$$

Since $2 + \sqrt{-3}$ and $2 - \sqrt{-3}$ both ramify in K with ramification index 3, we conclude that

$$(6) \quad \text{disc}(K/F) = (\sqrt{-3})^4 (2 + \sqrt{-3})^2 (2 + \sqrt{-3})^2 = 9 \cdot 49.$$

The natural first thing to check is if $\mathcal{O}_K = \mathbf{Z}[\omega][\sqrt[3]{7}] = \mathbf{Z}[\sqrt[3]{7}, \omega]$. Alas,

$$\text{disc}_{K/F}(1, \sqrt[3]{7}, \sqrt[3]{49}) = 3^3 7^2$$

is off from $\text{disc}_{K/F}(\mathcal{O}_F)$ by a factor of 3. So we want to find an element of $\mathbf{Z}[\sqrt[3]{7}, \omega]$ that upon division by $\sqrt{-3}$ is nonobviously still in \mathcal{O}_K . Since

$$(1 - \sqrt[3]{7})\mathcal{O}_k = \mathfrak{p}_2\mathfrak{p}_3 \Rightarrow (1 - \sqrt[3]{7})\mathcal{O}_K = \mathfrak{p}_2\mathfrak{P}_3^2, \quad \text{and } (\sqrt{-3})\mathcal{O}_K = \mathfrak{P}_3^3,$$

we have

$$\frac{(1 - \sqrt[3]{7})^2}{(\sqrt{-3})} = \mathfrak{p}_2^2\mathfrak{P}_3$$

is an integral ideal, so

$$\eta \stackrel{\text{def}}{=} \frac{(1 - \sqrt[3]{7})^2}{-\sqrt{-3}} = (2\omega + 1) \cdot \frac{1 - 2\sqrt[3]{7} + \sqrt[3]{49}}{3}$$

is an algebraic integer that is not in $\mathbf{Z}[\sqrt[3]{7}, \omega]$. Since $\text{disc}_{K/F}(1, \sqrt[3]{7}, \eta) = 9 \cdot 49$, $\{1, \sqrt[3]{7}, \eta\}$ is a $\mathbf{Z}[\omega]$ -basis of \mathcal{O}_K , by (6). (But $\text{disc}_{K/F}(1, \eta, \eta^2) = 9 \cdot 25 \cdot 49$, so $\mathcal{O}_K \neq \mathcal{O}_F[\eta]$.)

Writing $2\omega + 1 = 3\omega + (1 - \omega)$, we're led from η to the algebraic integer

$$(7) \quad \theta \stackrel{\text{def}}{=} \frac{(\omega - 1)(1 - \sqrt[3]{7})^2}{3} = -\omega^2\eta,$$

so $\{1, \sqrt[3]{7}, \theta\}$ is a second basis for $\mathcal{O}_K/\mathcal{O}_F$ (and $\text{disc}_{K/F}(1, \sqrt[3]{7}, \theta) = 9 \cdot 49\omega$).

Having expressed \mathcal{O}_K as a free module over \mathcal{O}_F , can we do likewise over \mathcal{O}_k ? Since \mathcal{O}_k is not a PID, we have no reason to suppose that \mathcal{O}_K is a free \mathcal{O}_k -module, and in fact it is *not*. To show this, we mimic the argument in [3].

Assume \mathcal{O}_K is a free \mathcal{O}_k -module, so it must have rank 2:

$$\mathcal{O}_K = \mathcal{O}_k e_1 \oplus \mathcal{O}_k e_2.$$

Thus

$$1 = \alpha_1 e_1 + \alpha_2 e_2, \quad \omega = \beta_1 e_1 + \beta_2 e_2,$$

where $\alpha_i, \beta_i \in \mathcal{O}_k = \mathbf{Z}[\sqrt[3]{7}]$. Applying complex conjugation (the nontrivial element of $\text{Gal}(K/k)$),

$$1 = \alpha_1 \bar{e}_1 + \alpha_2 \bar{e}_2, \quad \omega^2 = \beta_1 \bar{e}_1 + \beta_2 \bar{e}_2.$$

These can be combined into the matrix equation

$$\begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} \begin{pmatrix} e_1 & \bar{e}_1 \\ e_2 & \bar{e}_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \omega & \omega^2 \end{pmatrix}.$$

The determinant $\Delta \stackrel{\text{def}}{=} \alpha_1 \beta_2 - \alpha_2 \beta_1$ of the first matrix is in \mathcal{O}_k . The determinant of the second matrix is negated under complex conjugation, so its *square* is in \mathcal{O}_k . And the determinant of the matrix on the right is $\omega^2 - \omega = -1 - 2\omega = -\sqrt{-3}$. So equating the squares of the determinants of both sides yields

$$\Delta^2 \delta = -3,$$

where $\delta = (e_1 \bar{e}_2 - \bar{e}_1 e_2)^2$. As an equation in ideals of \mathcal{O}_k , we get

$$(\Delta)^2 (\delta) = 3 \mathcal{O}_k = \mathfrak{p}_3^3.$$

Since \mathfrak{p}_3 and \mathfrak{p}_3^2 are not principal ideals, and \mathfrak{p}_3^3 is not the square of an integral ideal, the only way for this equation to hold is if $(\Delta)^2 = (1)$, $(\delta) = (3)$. Thus $(\Delta) = (1)$, so $\Delta \in \mathcal{O}_k^\times$. That means $\{1, \omega\}$ is an \mathcal{O}_k -basis for \mathcal{O}_K . So

$$\mathcal{O}_K = \mathcal{O}_k \oplus \mathcal{O}_k \omega = \mathbf{Z}[\sqrt[3]{7}, \omega],$$

which we already saw is false. So \mathcal{O}_K is not a free \mathcal{O}_k -module.

We now return to the computation of $\text{Cl}(K)$. Recall θ , defined in (7). Since $\theta + \bar{\theta} = -(1 - \sqrt[3]{7})^2$ and $\theta \bar{\theta} = -9 + \sqrt[3]{7} + 2\sqrt[3]{49}$, the minimal polynomial of θ over k is

$$f(T) = T^2 + (1 - \sqrt[3]{7})^2 T + (-9 + \sqrt[3]{7} + 2\sqrt[3]{49}),$$

so the minimal polynomial of θ over \mathbf{Q} is

$$g(T) = f\sigma(f)\sigma^2(f) = T^6 + 3T^5 + 18T^4 + 45T^3 + 237T^2 + 180T + 48.$$

Thus $N_{K/\mathbf{Q}}(\theta - 1) = g(1) = 532 = 2^2 \cdot 7 \cdot 19$, so $(\theta - 1) = \mathfrak{P}_2(2 \pm \sqrt{-3})\mathfrak{P}_{19}$, where $\mathfrak{P}_2 \mid (2)$, $\mathfrak{P}_{19} \mid (19)$. Therefore $\mathfrak{P}_{19} \sim \mathfrak{P}_2^{-1}$. From the discussion of factoring primes $p \equiv 2 \pmod{3}$, the ideal class of a factor of 2 is $[\mathfrak{P}_3]$ or $[\mathfrak{P}_3^2]$. Therefore $[\mathfrak{P}_{19}] = [\mathfrak{P}_2]^{-1} = [\mathfrak{P}_3]$ or $[\mathfrak{P}_3^2]$. So $\text{Cl}(K)$ is generated by $[\mathfrak{P}_3]$.

(In fact, $[\mathfrak{P}_{19}] = [\mathfrak{P}_3^2]$. We saw already that in $\text{Cl}(k)$, $\mathfrak{p}_2 \sim \mathfrak{p}_3^{-1} \sim \mathfrak{p}_3^2$. Therefore in $\text{Cl}(K)$, $\mathfrak{p}_2 \mathcal{O}_K \sim \mathfrak{P}_3^4 \sim \mathfrak{P}_3$. Since \mathfrak{P}_3 is fixed by G , all prime factors of 2 in \mathcal{O}_K are equivalent to \mathfrak{P}_3 . So by the previous paragraph, $\mathfrak{P}_{19} \sim \mathfrak{P}_3^2$.)

We now can find a pair of fundamental units for \mathcal{O}_K^\times . By [2, Corollary 7] and the discussion following it,

$$h(K)R(K) = h(F)R(F)(h(k)R(k))^2 = (3 \log u)^2 = 9(\log u)^2$$

and

$$[\mathcal{O}_K^\times / \mu_K : \langle u, \sigma u \rangle] = 3h(K)/h(F)h(k)^2 = h(K)/3.$$

Since $h(K) = 3$, $\{u, \sigma u\}$ is a pair of fundamental units for K and $R(K) = 3(\log u)^2 \approx 17.876$.

Theorem 3. *The field $K = \mathbf{Q}(\sqrt[3]{7}, \omega)$ has class number 3, discriminant $-3^7 7^4$, and regulator $3(\log u)^2$, where $u = 4 + 2\sqrt[3]{7} + \sqrt[3]{49}$. The ramified primes 3 and 7 factor as*

$$3 = \mathfrak{P}_3^6, \quad (7) = (2 + \sqrt{-3})^3(2 - \sqrt{-3})^3.$$

The ring of integers of K is

$$\mathcal{O}_K = \mathcal{O}_F \oplus \mathcal{O}_F \sqrt[3]{7} \oplus \mathcal{O}_F \theta,$$

where $\theta = (\omega - 1)(1 - \sqrt[3]{7})^2/3$. The ideal class group of \mathcal{O}_K is generated by $[\mathfrak{P}_3]$. The unit group of \mathcal{O}_K has six roots of unity, rank 2, and basis $\{u, \sigma u\}$.

There is no power basis for \mathcal{O}_K . See [1].

REFERENCES

- [1] M-L. Chang, Non-monogeneity 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] R. MacKenzie and J. Schuneman, A Number Field Without a Relative Integral Basis, *Amer. Math. Monthly*, **78** (1971), 882-883.