THE SPLITTING FIELD OF $X^3 - 6$ OVER Q

KEITH CONRAD

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

$$K = \mathbf{Q}(\sqrt[3]{6}, \omega),$$

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

$$\begin{aligned}
k &= \mathbf{Q}(\sqrt[3]{6}),\\
K &= \mathbf{Q}(\sqrt[3]{6}, \omega),\\
F &= \mathbf{Q}(\omega) = \mathbf{Q}(\sqrt{-3}),\\
G &= \mathrm{Gal}(K/\mathbf{Q}) \cong S_3,\\
N &= \mathrm{Gal}(K/F) \cong A_3,\\
H &= \mathrm{Gal}(K/k).
\end{aligned}$$

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.

Since $\mathrm{disc}(\mathbf{Z}[\sqrt[3]{6}]) = -\,\mathrm{N}_{k/\mathbf{Q}}(3(\sqrt[3]{6})^2) = -3^3 6^2$, only 2 and 3 can ramify in k. Since $X^3 - 6$ is Eisenstein at 2 and 3, both 2 and 3 are totally ramified: $(2) = \mathfrak{p}_2^3$, $(3) = \mathfrak{p}_3^3$. So $\mathcal{O}_k = \mathbf{Z}[\sqrt[3]{6}]$ and $\mathrm{disc}(\mathcal{O}_k) = -2^2 3^5$.

The Minkowski bound on k is

$$\frac{3!}{3^3}\left(\frac{4}{\pi}\right) 2 \cdot 3^2 \sqrt{3} \approx 8.82.$$

So we want to factor the primes $2, 3, 5, 7$. We already know 2 and 3 are totally ramified. Mod 5, $X^3 - 6 \equiv (X-1)(X^2 + X + 1)$, so $(5) = \mathfrak{p}_5 \mathfrak{p}_5'$, where $\mathrm{N}\,\mathfrak{p}_5 = 5$, $\mathrm{N}\,\mathfrak{p}_5' = 25$. Since $X^3 - 6 \equiv (X+1)(X+2)(X-3) \bmod 7$, 7 splits completely.

The norm form for k is

$$\mathrm{N}_{k/\mathbf{Q}}(a + b\sqrt[3]{6} + \sqrt[3]{36}) = a^3 + 6b^3 + 36c^3 - 18abc, \tag{1}$$

so

$$(1 + \sqrt[3]{6}) = \mathfrak{p}_7, \quad (-1 + \sqrt[3]{6}) = \mathfrak{p}_5, \quad (2 + \sqrt[3]{6}) = \mathfrak{p}_2\mathfrak{p}_7', \quad (2 - \sqrt[3]{6}) = \mathfrak{p}_2,$$
$$(1 + 2\sqrt[3]{6}) = (\mathfrak{p}_7'')^2, \quad (3 - \sqrt[3]{6}) = \mathfrak{p}_3\mathfrak{p}_7'', \quad (4 + \sqrt[3]{6}) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_7'', \quad (-3 + \sqrt[3]{36}) = \mathfrak{p}_3^2.$$

Therefore all prime factors of 2, 3, 5, 7 are principal, so $h(k) = 1$. The ratio

$$\frac{(2 - \sqrt[3]{6})^3}{2} = 1 - 6\sqrt[3]{6} + 3\sqrt[3]{36} \approx .003$$

is a unit, and its reciprocal is

$$u \overset{\text{def}}{=} 109 + 60\sqrt[3]{6} + 33\sqrt[3]{36} \approx 326.99.$$

The minimal polynomial of $2 - \sqrt[3]{6}$ is $T^3 + 6T^2 + 12T - 2$, while the minimal polynomial of u is $T^3 - 327T^2 + 3T - 1$.

Other explicit principal ideals also give rise to u. For instance, $\mathfrak{p}_3$ is generated by

$$\frac{3}{-3 + \sqrt[3]{36}} = 3 + 2\sqrt[3]{6} + \sqrt[3]{36} \approx 9.9,$$

which has norm 3, and we get a unit > 1 from

$$\frac{(3 + 2\sqrt[3]{6} + \sqrt[3]{36})^3}{3} = 109 + 60\sqrt[3]{6} + 33\sqrt[3]{36}.$$

The ideal $\mathfrak{p}_7''$ is generated by

$$\frac{3 - \sqrt[3]{6}}{3 + 2\sqrt[3]{6} + \sqrt[3]{36}} = -5 + \sqrt[3]{6} + \sqrt[3]{36} \approx .119.$$

and also by

$$\frac{4 + \sqrt[3]{6}}{(2 - \sqrt[3]{6})(-1 + \sqrt[3]{6})} = 13 + 7\sqrt[3]{6} + 4\sqrt[3]{36} \approx 38.9$$

So the ratio is a unit of $\mathcal{O}_k$. To get a unit > 1, we compute

$$\frac{13 + 7\sqrt[3]{6} + 4\sqrt[3]{36}}{-5 + \sqrt[3]{6} + \sqrt[3]{36}} = 109 + 60\sqrt[3]{6} + 33\sqrt[3]{36}$$

It turns out that u is a fundamental unit of $\mathcal{O}_k$, but [2, Lemma 2] does not apply, since for the fundamental unit U, $U^2 > (3^5 - 7)^{2/3} \approx 38.189$, a lower bound which is too small to conclude $U^2 > u$.

Theorem 2. *The fundamental unit of* $\mathbf{Z}[\sqrt[3]{6}]$ *is* $u = 109 + 60\sqrt[3]{6} + 33\sqrt[3]{36}$.

Proof. We follow the same approach as [3, Thm. 2], essentially just replacing 123 in [3] by 327. Write $u = \rho^j$ with $\rho^3 + a\rho^2 + b\rho + c$, $c = -1$.

If $u = \rho^2$ then $327 = a^2 - 2b$, $3 = b^2 + 2a$. Solving for a in the second equation turns the first one into

$$b^4 - 6b^2 - 8b - 1299 = 0,$$

so $b | 1299 = 3 \cdot 433$. No divisor works.

If $u = \rho^3$ then $327 = -a^3 + 3ab + 3$ and $3 = b^3 + 3ab + 3$, and there is no solution by the same method as in [3].

If $u = \rho^p$ for p an odd prime, then $\mathrm{N}_{k/\mathbf{Q}}(\rho + 1) = 2 - a + b$ is a positive integer which divides $\mathrm{N}_{k/\mathbf{Q}}(u + 1) = 332 = 2^2 83$, $\mathrm{N}_{k/\mathbf{Q}}(\rho - 1) = -a - b$ is a positive integer which divides $\mathrm{N}_{k/\mathbf{Q}}(u - 1) = 324 = 2^2 3^4$, and

$$327 \equiv -a \bmod p, \quad 3 \equiv b \bmod p.$$

This is the same as

$$2 - a + b \equiv 332 \bmod p, \quad -a - b \equiv 324 \bmod p.$$

Here is the table of values of $2 - a + b$ and $-a - b$ along with the corresponding primes p:

$2 - a + b$	1	2	4	83	166	332
p	331	2,3,5,11	2, 41	3,83	2, 83	arb.

$-a-b$	1	2	3	4	6	9	12	18	27	36	54	81	108	162	324
p	17, 19	2, 7, 23	3, 107	2, 5	2,3, 53	3, 5, 7	2, 3, 13	2, 3, 17	3, 11	2, 3	2, 3, 5	3	2, 3	2, 3	arb.

Following the same procedure as in [3], we eliminate primes $p \geq 7$ by checking the resulting cubic polynomial for a putative ρ has discriminant not divisible by $\operatorname{disc}(\mathcal{O}_k) = 2^2 3^5$ (it also must be a divisor of $\operatorname{disc}(\mathbf{Z}[u]) = -2^4 3^{11} 7^2$, but this won't be needed). We already eliminated $p = 2, 3$. The prime 5 appears often in the above tables, so we handle it instead by finding a residue field $\mathcal{O}_k/\mathfrak{p} \cong \mathbf{F}_p$ where u is not a fifth power. Choose $p \equiv 1 \bmod 5$, say $p = 11$. Since $X^3 - 6 \equiv (X+3)(X^2+8X+9) \bmod 11$, there is $\mathfrak{p}$ with norm 11. Then

$$u = \rho^5 \Rightarrow u \equiv \rho^5 \bmod \mathfrak{p} \equiv \pm 1.$$

However, neither $\mathrm{N}_{k/\mathbf{Q}}(u+1)$ nor $\mathrm{N}_{k/\mathbf{Q}}(u-1)$ is divisible by 11, so $u \neq \rho^5$. □

Theorem 3. *The field $k = \mathbf{Q}(\sqrt[3]{6})$ has ring of integers $\mathbf{Z}[\sqrt[3]{6}]$, class number 1, discriminant $-2^2 3^5$, and fundamental unit $u = 109 + 60\sqrt[3]{6} + 33\sqrt[3]{36}$. The ramified primes 2 and 3 factor as*

$$2 = (2 - \sqrt[3]{6})^3 u, \quad 3 = \pi^3 v,$$

where $\pi = 3 + 2\sqrt[3]{6} + \sqrt[3]{36}$ and $v = 1/u$. The minimal polynomial of u over $\mathbf{Q}$ is $T^3 - 327T^2 + 3T - 1$ and of π is $T^3 - 9T^2 - 9T - 3$.

We now turn to K. Following [2],

$$\operatorname{disc}(K) = \operatorname{disc}(F)\operatorname{disc}(k)^2 = -2^4 3^{11}, \quad h(K)R(K) = (h(k)R(k))^2 = (\log u)^2. \tag{2}$$

The prime 3 is totally ramified: $3\,\mathcal{O}_K = (\eta)^6$, where $\eta \overset{\text{def}}{=} \sqrt{-3}/\pi$. The (principal) prime factor of 2 in $\mathcal{O}_k$ remains prime in $\mathcal{O}_K$: $2\,\mathcal{O}_K = (2 - \sqrt[3]{6})^3$.

As in [2], $\mathcal{O}_K = \mathcal{O}_k \oplus \mathcal{O}_k\,\theta$, where $\theta \overset{\text{def}}{=} (\omega - 1)/\pi$. Since

$$\theta\overline{\theta} = \frac{3}{\pi^2} = \pi v = 3 + 2\sqrt[3]{6} - 2\sqrt[3]{36}, \quad \theta + \overline{\theta} = -\frac{3}{\pi} = -\pi^2 v = 3 - \sqrt[3]{36},$$

the minimal polynomial of θ over k is $f(T) = T^2 - (3 - \sqrt[3]{36})T + (3 + 2\sqrt[3]{6} - 2\sqrt[3]{36})$, so the minimal polynomial of θ over $\mathbf{Q}$ is

$$g(T) = f\sigma(f)\sigma^2(f) = T^6 - 9T^5 + 36T^4 - 81T^3 + 72T^2 + 27T + 3.$$

Since $\operatorname{disc}(g(T)) = -2^8 3^{11} 5^2 7^2$, $\mathcal{O}_K \neq \mathbf{Z}[\theta]$.

The Minkowski bound for K is

$$\frac{6!}{6^6}\left(\frac{4}{\pi}\right)^3 2^2 3^5 \sqrt{3} = \frac{960\sqrt{3}}{\pi^3} \approx 53.626.$$

So we want to factor all primes ≤ 53, hopefully many will have principal ideal factors.

We already checked the ramified primes 2 and 3 have principal prime factors in $\mathcal{O}_K$, so we turn to unramified primes p. The only time p might not have a principal prime factor in $\mathcal{O}_K$ is if $p \equiv 1 \bmod 3$ and $X^3 - 6 \bmod p$ has a root (hence 3 roots). For $p \leq 53$, this happens only for $p = 7, 37$:

$$X^3 - 6 \equiv (X+1)(X+2)(X+4) \bmod 7, \quad X^3 - 6 \equiv (X+6)(X+8)(X+23) \bmod 37.$$

Thus 7 and 37 split completely in $\mathcal{O}_K$. To determine if they have principal prime factors, we compute $\mathrm{N}_{K/k}(\theta - m) = g(m)$ for various integers m, hoping to see a 7 or 37 arise. This would correspond to $m \bmod 7$ or $m \bmod 37$ being a root of $g(T)$. Since $g(-1) \equiv 0 \bmod 7$, we compute $\mathrm{N}_{K/\mathbf{Q}}(\theta + 1) = g(-1) = 5^2 7$. Therefore 7 factors principally. Since $g(-2) \equiv 0 \bmod 37$, we compute $\mathrm{N}_{K/\mathbf{Q}}(\theta + 2) = 7^2 37$. Thus 37 factors principally, so $h(K) = 1$.

By (2), $R(K) = (\log u)^2$, so u and σu generate a subgroup of index 3 in the units of $\mathcal{O}_K$ (mod torsion). To find a unit which together with u forms a pair of fundamental units, consider

$$\delta \overset{\text{def}}{=} \frac{\sigma\eta}{\eta} = \frac{\pi}{\sigma\pi}.$$

By exactly the same calculations as in [3], $\{u, \delta\}$ and $\{\delta, \overline{\delta}\}$ are both pairs of fundamental units.

Theorem 4. *The field $K = \mathbf{Q}(\sqrt[3]{6}, \omega)$ has class number 1, discriminant $-2^4 3^{11}$, and regulator $(\log u)^2$, where $u = 109 + 60\sqrt[3]{6} + 33\sqrt[3]{36}$. The ramified primes 2 and 3 factor as*

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

where $\eta = \sqrt{-3}/\pi$, $\pi = 3 + 2\sqrt[3]{6} + \sqrt[3]{36}$. The ring of integers of K is

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

where $\theta = (\omega - 1)/\pi$. The unit group of $\mathcal{O}_K$ has six roots of unity, rank 2, and bases $\{u, \delta\}$ and $\{\delta, \overline{\delta}\}$, where $\delta = \pi/\sigma(\pi)$.

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

References

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

[2] Conrad, K. The Splitting Field of $X^3 - 2$ over $\mathbf{Q}$.

[3] Conrad, K. The Splitting Field of $X^3 - 5$ over $\mathbf{Q}$.