Ramification in a family of
$\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$-extensions of the rationals

Bill Allombert & Stéphane Vinatier

January 2010

Abstract

We construct for each prime number $p \equiv 1 \pmod{3}$, a $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$-extension of the rationals that is ramified exactly at 3 and $p$, and we explicit the discriminant and the ramification groups as functions of $p$.

1 Introduction

In this paper we present a very simple, explicit and pleasant way to construct an infinite family of Galois extensions of the rationals, of Galois group isomorphic to the non abelian group of order 27 and exponent 9, namely the semi-direct product $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$. These extensions are parametrized by the prime numbers $p$ congruent to 1 modulo 3. They are only ramified at two places, 3 and the parametrizing prime $p$. It follows from [P3, Proposition 2.5] that this is the minimal number of ramified places for Galois extensions with this Galois group. Our extensions can be described as the splitting field of a surprisingly simple degree 9 polynomial depending on $p$ only in its constant coefficient.

The simplicity of our construction enables us to achieve the complete study of the ramification above 3. Its decomposition as a product of prime ideals takes five different patterns, depending on the integers $a$ and $b$ such that $p = a^2 + 3b^2$. We explicit a uniformizing parameter and the sequence of ramification groups in every case. In particular we find that the extension is weakly ramified (i.e. with trivial second ramification groups) in some of the cases, which yields a family of weakly ramified extensions with Galois group isomorphic to $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ that is different from that studied in [V].

We performed computations using PARI/GP[P1] for a number of elements of this family using specially devised algorithms and checked that the results were in agreement with the theory.

Such extensions have already been constructed by several authors, by several means, and in several contexts. In particular a construction for any prime number $p$ of generic Galois extensions of $\mathbb{Q}$ of Galois group $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ can be found in
[L1], with an application to the $p = 3$ case. Our construction is far less general, but has revealed extremely easy to handle for the study of the ramification, which was our main goal.

2 Construction of $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$-extensions

We let $\zeta_9$ denote a primitive 9-th root of unity in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and we set $\zeta_3 = \zeta_9^3$ and $\sqrt{-3} = 2\zeta_3 + 1$.

If $L/K$ is an extension of number fields, we denote by $N_{L/K}$ the norm, by $D_{L/K}$ the different ideal and by $d_{L/K}$ the relative discriminant ideal. We also denote by $O_K$ the ring of integers of $K$ and by $d_K$ its absolute discriminant. If $p$ is a prime ideal of $O_K$ of uniformizing parameter $\pi$, we denote by $K_p$ or $K_\pi$ the completion of $K$ for the $p$–adic topology, and by $v_\pi$ the $p$–adic valuation in $K_p$.

Let $p$ be a prime number so that $p \equiv 1 \pmod{3}$, then by a theorem of Fermat there exist two integers $a$ and $b$, unique up to sign, such that

$$p = a^2 + 3b^2.$$ 

We chose the sign of $a$ so that $a \equiv 1 \pmod{3}$ and we denote by $a'$ the integer such that $a = 1 + 3a'$. If $b \not\equiv 0 \pmod{3}$, we chose the sign of $b$ so that $b \equiv 1 \pmod{3}$ and we denote by $b'$ the integer such that $b = 1 + 3b'$; otherwise, we set $b = 3b'$ and if $b' \not\equiv 0 \pmod{3}$ we chose the sign of $b$ so that $b' \equiv -1 \pmod{3}$. We set $\alpha = a + b\sqrt{-3}$ and

$$\beta = \frac{a + b\sqrt{-3}}{a - b\sqrt{-3}}$$

which belong to the field $\mathbb{Q}(\zeta_3)$.

We construct the fields

$$M = \mathbb{Q}(\sqrt[9]{\beta}) \quad \text{and} \quad L = \mathbb{Q}(\zeta_9, \sqrt[9]{\beta})$$

where $\sqrt[9]{\beta}$ denotes a fixed 9-th root of $\beta$ in $\overline{\mathbb{Q}}$. Note that $\beta = \frac{a^2 - 3b^2 + 2ab\sqrt{-3}}{p}$, so $\sqrt{-3}$ and $\zeta_3$ lie in $M$.

**Proposition 1** The extension of number fields $L/\mathbb{Q}$ is Galois, with Galois group generated by $\sigma$ and $\tau$ defined by:

$$\sigma(\zeta_9) = \zeta_9^3 \quad \text{and} \quad \sigma(\sqrt[9]{\beta}) = \frac{1}{\sqrt[9]{\beta}},$$

$$\tau(\zeta_9) = \zeta_9 \quad \text{and} \quad \tau(\sqrt[9]{\beta}) = \zeta_9 \sqrt[9]{\beta}.$$ 

The following relations hold:

$$\sigma^6 = 1, \quad \tau^9 = 1 \quad \text{and} \quad \sigma \tau \sigma^{-1} = \tau^{-2}.$$
Proof. The extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ is cyclic, let us call $s$ the generator of its Galois group such that $s(\zeta_9) = \zeta_9^2$. The extension $L/\mathbb{Q}(\zeta_9)$ is cyclic by Kummer theory, with Galois group generated by an element $\tau$ satisfying $\tau(\zeta_9) = \zeta_9$ and $\tau(\sqrt[9]{\beta}) = \zeta_9\sqrt[9]{\beta}$. By Kummer theory, $L/\mathbb{Q}$ is Galois if and only if $s(\beta) = \beta^n\gamma^9$ for some integer $u$ prime to 9 and some $\gamma \in \mathbb{Q}(\zeta_9)$. Since $s(\zeta_3) = \zeta_3^{-1}$, we get $s(\sqrt{-3}) = -\sqrt{-3}$ and $s(\beta) = \beta^{-1}$, so the condition holds and $L/\mathbb{Q}$ is Galois and $s$ can be extended to an automorphism $\sigma$ of $L/\mathbb{Q}$. We have

$$
\sigma\tau\sigma^{-1}(\zeta_9) = \zeta_9 = \tau^{-2}(\zeta_9) \\
\sigma\tau\sigma^{-1}(\sqrt[9]{\beta}) = \zeta_9^{-2}\sqrt[9]{\beta} = \tau^{-2}(\sqrt[9]{\beta})
$$

so $\sigma\tau\sigma^{-1} = \tau^{-2}$ holds. □

We then construct the field

$$
K = L^{(\sigma^3)} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1}, \sqrt[9]{\beta} + \sqrt[9]{\beta^{-1}}).
$$

We sum up the construction in the diagram of Figure 1.

![Figure 1: Extensions diagram](image)

**Theorem 1** The extension $K/\mathbb{Q}$ is Galois with Galois group isomorphic to the non abelian semi-direct product $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ of order 27 and exponent 9.
Proof. We have $\sigma^3 \tau \sigma^{-3} = \tau$, so $\tau \sigma^3 \tau^{-1} = \sigma^3$ and the subgroup $\langle \sigma^3 \rangle$ is normal in $\langle \sigma, \tau \rangle$. Hence $K/\mathbb{Q}$ is Galois with group $\langle \sigma, \tau \rangle/\langle \sigma^3 \rangle$ and relations

$$\sigma^3 = 1, \quad \tau^9 = 1, \quad \text{and} \quad \sigma \tau \sigma^{-1} = \tau^{-2}$$

which is isomorphic to $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. ■

For effective computation in the field $L$, the following is useful:

Proposition 2 The minimal polynomial of the element $\sqrt[3]{b} + \sqrt[3]{b}^{-1}$ is given by

$$X^9 - 9X^7 + 27X^5 - 30X^3 + 9X + 2 - 4a^2/p$$

(1)

Proof. This is a straightforward computation best performed using a computer algebra system, for example PARI/GP [P1]. ■

3 Ramification

In this section, we make a complete and explicit study of the ramification in the extension $K/\mathbb{Q}$. We begin by stating the main results.

Theorem 2 The extension $K/\mathbb{Q}$ is unramified outside 3 and $p$ with discriminant:

$$d_K = \begin{cases} 
3^{66}p^{24} & \text{if } v_3(b) = 0, \\
3^{48}p^{24} & \text{if } v_3(b) = 1, \\
3^{36}p^{24} & \text{if } v_3(b) \geq 2. 
\end{cases}$$

The ramification index above $p$ in $K/\mathbb{Q}$ equals 9. The ideal generated by 3 in the ring of integers of $K$ is the product of $g$ prime ideals, each of residual degree $f$ and ramification index $e$, as given in the following table:

<table>
<thead>
<tr>
<th>$v_3(b)$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>$\geq 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>9</td>
<td>9</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>$f$</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>$g$</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>9</td>
</tr>
</tbody>
</table>

in which the indicated congruences are modulo 3.

The proof of Theorem 2 occupies the rest of this section; we divide its presentation into several subsections for clarity.
3.1 Classical results

Let us recall some classical results without proof for further reference. We begin with results concerning extensions of local fields with finite residue field (so that a polynomial that is irreducible on the residue field is separable).

**Lemma 1** Let $E/F$ be an unramified extension of local fields and $D$ a local field, then the extension $ED/FD$ is unramified.

**Lemma 2** Let $E$ be a local field with uniformizing parameter $\pi$, $f$ be a monic polynomial with integral coefficients in $E$ and $\alpha$ a root of $f$ in an algebraic closure of $E$. Denote by $\bar{f}$ the reduction of $f$ modulo $\pi$, then:

(i) if $\bar{f}$ is irreducible, the extension $E(\alpha)/E$ is unramified;

(ii) if $\bar{f}$ is a square-free totally split polynomial, then $E(\alpha) = E$;

(iii) if $f$ is an Eisenstein polynomial, the extension $E(\alpha)/E$ is totally ramified, $\alpha$ is a uniformizing parameter of $E(\alpha)$, and $v_\pi(d_{E(\alpha)/E})$ equals the valuation of the discriminant of the polynomial $f$.

The second case (ii) is a consequence of Hensel’s Lemma; for cases (i) and (iii), see [S, I.6]. Recall that an extension $E/F$ of local fields is said to be tamely ramified if the ramification index is prime to the characteristic of the residue field of $F$. We know by Proposition 13 of [S, III.7]:

**Lemma 3** Let $E/F$ be a tamely ramified extension of local fields, of ramification index $e$, then the valuation in $E$ of the different of $E/F$ equals $e - 1$.

The next result is valid for local and global fields as well [S, III.4 Prop. 8].

**Lemma 4** Let $D/E/F$ be a tower of extensions of number fields, then $D_{D/E/F} = D_{D/E}D_{E/F}$ and $d_{D/F} = N_{E/F}(d_{D/E})d_{E/F}^{[D:E]}$.

3.2 Ramification outside 3

First note that the cyclotomic extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ is unramified outside 3. Remind that $p = a^2 + 3b^2$ and $\alpha = a + b\sqrt{-3}$, so $\beta = \alpha/\sigma(\alpha)$. The extension $L/\mathbb{Q}(\zeta_9)$ is the splitting field of the polynomial $X^9 - \alpha \sigma(\alpha)^8$, whose discriminant is $3^{18} \times \alpha^8 \sigma(\alpha)^{64}$, of norm $3^{108}p^{216}$, so this extension is unramified outside 3 and $p$. It follows that $L/\mathbb{Q}$ and a fortiori its subextension $K/\mathbb{Q}$ are unramified outside 3 and $p$.

Now we compute the ramification of $p$. The prime $p$ splits in $\mathbb{Q}(\zeta_3)$ as $(p) = (\alpha)(\sigma(\alpha))$. Remind that $\zeta_3 \in M = \mathbb{Q}(\sqrt[3]{3})$, so the extension $M/\mathbb{Q}(\zeta_3)$ is the splitting field of the polynomial $X^3 - \alpha/\sigma(\alpha)$, which is an Eisenstein polynomial for the prime $(\alpha)$. It follows from Lemma 2 that $(\alpha)$ is totally (and tamely)
ramified, and that the \((\alpha)\)-adic valuation of \(d_{M/Q(\zeta_3)}\) is 8. Since \(M = Q(\sqrt{3}^{-1})\), the same result holds for the \((\sigma(\alpha))\)-adic valuation, and so by Lemma 4 the \(p\)-adic valuation of the absolute discriminant is 16. Since the extension \(Q(\zeta_3)/Q(\zeta_3)\) is unramified above \(p\), it follows from Lemma 1 that the extension \(L/M\) is unramified above \(p\). By Lemma 4, the \(p\)-adic valuation of the absolute discriminant of \(L\) is 48. Similarly the extension \(Q(\zeta_3)/Q\) is unramified above \(p\), so by Lemma 1 the same is true for the extension \(L/K\). Eventually by Lemma 4, the \(p\)-adic valuation of the discriminant of \(K\) is half the \(p\)-adic valuation of the discriminant of \(L\), hence is 24.

### 3.3 Ramification above 3

From now on we consider the ramification above 3. As in the preceding subsection, we shall make computations in the very explicit extension \(L/Q\), then infer the result we are interested in about the valuation of the absolute discriminant of \(K\) thanks to the equality:

**Lemma 5** \(2v_3(d_K) = v_3(d_L) - \frac{54}{e(3, L/Q)}\).

**Proof.** From Lemma 4 one gets \(v_3(d_L) = v_3\left(N_{K/Q}(d_{L/K})\right) + 2v_3(d_K)\). The extension \(Q(\zeta_3)/Q\) is totally ramified at 3 and \((3) = (\sqrt{-3})^2\) as ideals of \(\mathbb{Z}[\zeta_3]\). Since \(Q(\zeta_3) \subseteq L\), the ramification index \(e(3, L/Q)\) of 3 in \(L/Q\) is even. Further, \([L : K] = 2\) whereas \([K : Q]\) is odd, so \(L/K\) is totally and tamely ramified above 3, and by Lemma 3 the exponent in \(D_{L/K}\) of the prime ideals of \(L\) lying above 3 is 1. The same is true for the exponent in \(d_{L/K}\) of the prime ideals of \(K\) lying above 3, so taking the norm to \(Q\) yields \(v_3\left(N_{K/Q}(d_{L/K})\right) = fg\), where \(fg = \frac{[K : Q]}{e(3, K/Q)}\) happens to equal \(\frac{[L : Q]}{e(3, L/Q)}\).

The extension \(M/Q(\zeta_3)\) is the splitting field of the polynomial \(X^9 - \beta\). Setting \(X = Y + 1\) yields:

\[
S(Y) = Y^9 + 3s(Y)Y + 1 - \beta
\]

where \(s(Y)\) is a polynomial with integral coefficients. \(S\) is an Eisenstein polynomial for the prime \((\sqrt{-3})\) if and only if the \((\sqrt{-3})\)-adic valuation of \(1 - \beta\) is 1. The ideal \((\sigma(\alpha))\) being coprime to \((\sqrt{-3})\), we have

\[
v_{\sqrt{-3}}(1 - \beta) = v_{\sqrt{-3}}(\sigma(\alpha) - \alpha) = v_{\sqrt{-3}}(-2b\sqrt{-3}) = 1 + 2v_3(b). \tag{2}
\]

#### 3.3.1 The case \(v_3(b) = 0\)

Here we suppose \(v_3(b) = 0\). \(S\) is an Eisenstein polynomial for the prime \((\sqrt{-3})\), hence by Lemma 2, the prime \((\sqrt{-3})\) is totally ramified in \(M/Q(\zeta_3)\), \(\pi = \sqrt{3} - 1\) is a uniformizing parameter for the completion of \(M\) at the only prime above
In both cases, the extension is unramified, and so by Lemma 4, the \( \beta \)-adic valuation of the discriminant of \( M \) is 45.

The extension \( L/M \) is a Kummer extension of prime degree generated by \( \zeta_9 = \sqrt[3]{3} \), hence we could apply Hecke’s theorem (see for example [C2, 10.2.3]), but we prefer to stick with elementary arguments, since we are looking for an explicit result. Since we suppose \( v_3(b) = 0 \), we may write \( a = 1 + 3a' \) and \( b = 1 + 3b' \) with \( a', b' \in \mathbb{Z} \). We also write \( p = 1 + 3p' \) with \( p' \in \mathbb{Z} \). Note that \( p' \equiv 2a' + 1 \) (mod 3). We consider the element of \( L \) defined by

\[
\theta = \frac{\zeta_9 - \sqrt[3]{3}}{\sqrt[3]{3}}.
\]

It generates \( L \) over \( M \) and is a root of the polynomial \( (\sqrt[3]{-3}X + \sqrt[3]{3})^3 - \zeta_3 \), whose coefficients are in \( M \). We have the identity

\[
(\sqrt[3]{-3}X + \sqrt[3]{3})^3 - \zeta_3 = -3\sqrt[3]{-3}X^3 - 9\sqrt[3]{3}X^2 + 3\sqrt[3]{3}\beta X + \beta - \zeta_3.
\]

Now \( \zeta_3 = \frac{-1 + \sqrt[3]{-3}}{2} = \frac{1 - \sqrt[3]{-3}}{4} \), so \( \zeta_3 = (1 - \sqrt[3]{-3}) \sum_{i \geq 0} 3^i \) in \( \mathbb{Q}_3(\zeta_3) \) and

\[
\zeta_3 \equiv 1 - \sqrt[3]{-3} + 3 - 3\sqrt[3]{-3} \pmod{9} \tag{3}
\]

Further, \( \beta = 1 + 2a\sqrt[3]{3} - 3b \), which yields:

\[
\beta \equiv 1 - \sqrt[3]{-3} + 3 + (-1 + a' - b')3\sqrt[3]{-3} \pmod{9} \tag{4}
\]

with the notations introduced above. We get from this computation that \( \beta \equiv \zeta_3 \pmod{3\sqrt[3]{-3}} \), so \( \eta = \frac{\beta - \zeta_3}{3\sqrt[3]{-3}} \) is integral in \( \mathbb{Q}_3(\zeta_3) \). More precisely, \( \eta \equiv a' - b' \pmod{\sqrt[3]{-3}} \). It follows that \( \theta \) is a root of the polynomial:

\[
T(X) = X^3 - \sqrt[3]{-3}\sqrt[3]{3}X^2 - \sqrt[3]{3}\beta X - \eta
\]

with integral coefficients in \( M \). Note that \( \sqrt[3]{3} - 1 = (\sqrt[3]{3} - 1)(\sqrt[3]{3} + 1)(\zeta_3\sqrt[3]{3} - 1)(\zeta_3^2\sqrt[3]{3} - 1) \), so \( T \) reduces modulo \( \pi = \sqrt[3]{3} - 1 \) to the polynomial \( T(X) = X^3 - X + b' - a' \). We have to consider two possibilities:

- if \( a' \not\equiv b' \pmod{3} \), \( T \) is an Artin-Schreier polynomial, hence is irreducible over \( \mathbb{F}_3 \), so by Lemma 2 the primitive element \( \theta \) generates an unramified extension in which the prime above 3 is inert;

- if \( a' \equiv b' \pmod{3} \), \( T(X) = X^3 - X \) is a square-free totally split polynomial so, by Hensel’s Lemma, \( T \) is totally split over \( M_\pi \), \( \theta \) belongs to this field, and the prime above 3 splits in \( L/M \).

In both cases, the extension is unramified, and so by Lemma 4, the \( \beta \)-adic valuation of the discriminant of \( L \) is 135. The ramification index of \( L/Q \) is 18 so, by Lemma 5, the \( \beta \)-adic valuation of the discriminant of \( K \) is 66.
3.3.2 Ramification above 3 when \( v_3(b) \geq 1 \)

Now we suppose \( v_3(b) \geq 1 \). We first study the extension \( \mathbb{Q}(\sqrt[3]{\beta})/\mathbb{Q}(\zeta_3) \). It is a Kummer extension and we will use the same technique as above. Let us consider the element \( \frac{\sqrt[3]{\beta}-1}{\sqrt[3]{-3}} \). It generates the extension and is a root of the polynomial

\[
(\sqrt[3]{-3}X + 1)^3 - \beta = -3\sqrt[3]{-3}X^3 - 9X^2 + 3\sqrt[3]{-3}X + 1 - \beta .
\]

It is also a root of

\[
U(X) = X^3 - \sqrt[3]{-3}X^2 - X + \frac{\beta - 1}{3\sqrt[3]{-3}}
\]

which, by equation (2), has integral coefficients in \( \mathbb{Q}(\zeta_3) \) under our assumption. We deduce from \( \frac{\beta - 1}{3\sqrt[3]{-3}} = \frac{2(a + b\sqrt[3]{-3})}{p} \) and \( b = 3b' \) that

\[
\frac{\beta - 1}{3\sqrt[3]{-3}} \equiv -b' \pmod{3} .
\]

This leads to two possibilities:

- \( v_3(b) = 1 \), then the reduction of \( U(X) \) modulo \( \sqrt[3]{-3} \) is \( X^3 - X - b' \) which is irreducible, hence \( \sqrt[3]{-3} \) is inert in the extension;
- \( v_3(b) \geq 2 \), then the reduction of \( U(X) \) modulo \( \sqrt[3]{-3} \) is \( X^3 - X \) which is square-free and totally split, hence \( \sqrt[3]{-3} \) is totally split in the extension.

Note that in both cases the extension is unramified above 3.

3.3.3 The case \( v_3(b) \geq 2 \)

We begin with the second case \( v_3(b) \geq 2 \). Denote by \( N \) the field \( \mathbb{Q}(\sqrt[3]{\beta}) \), and by \( \wp_1, \wp_2, \wp_3 \) the prime ideals of \( \mathcal{O}_N \) above \( \sqrt[3]{-3} \), since \( N/\mathbb{Q}(\zeta_3) \) is totally split above \( \sqrt[3]{-3} \) by the preceding result. The reduction of \( U(X) \) modulo \( \wp = \wp_1 \) equals \( X(X - 1)(X + 1) \), so one of the roots of \( U \) belongs to \( \wp \) and we set \( \gamma \) to be the cubic root of \( \beta \) such that \( \gamma - 1 \equiv 0 \pmod{\wp} \). Using congruence (3), we get that the other roots of \( U \) satisfy:

\[
\frac{\zeta_3\gamma - 1}{\sqrt[3]{-3}} \equiv -1 \pmod{\wp} ; \quad \frac{\zeta_3^2\gamma - 1}{\sqrt[3]{-3}} \equiv 1 \pmod{\wp} ,
\]

so \( v_\wp(\zeta_3\gamma - 1) = v_\wp(\zeta_3^2\gamma - 1) = v_\wp(\sqrt[3]{-3}) = 1 \). The identity \( 1 - \beta = (1 - \gamma)(1 - \zeta_3\gamma)(1 - \zeta_3^2\gamma) \) yields

\[
v_\wp(1 - \gamma) = v_\wp(1 - \beta) - 2 = 2v_3(b) - 1 \geq 3 ,
\]

so that \( \frac{\gamma - 1}{3\sqrt[3]{-3}} \) is integral in \( N_\wp \).
The element \( 1 - \frac{\sqrt[3]{7}}{\sqrt{3}} \) is a generator of the extension \( M/N \) and a root of the polynomial
\[
X^3 + \sqrt{-3}X^2 - X + \frac{1 - \gamma}{3\sqrt{-3}}
\]
with integral coefficients in \( N_p \), so as above either \( v_3(b) = 2 \) and \( \wp \) is inert in \( M/N \), either \( v_3(b) \geq 3 \) and \( \wp \) is totally split. Let \( \mathfrak{p} \) denote a prime ideal of \( \mathcal{O}_L \) above \( \wp \) and set \( \wp' = \mathfrak{p} \cap \mathcal{O}_M \), then in both cases the extension \( M/Q(\zeta_3) \) is unramified at \( \wp' \). By Lemma 1, we deduce that the extension \( L/Q(\zeta_3) \) is unramified at \( \wp \). The discriminant of the cyclotomic field \( Q(\zeta_3) \) is \(-3^9\), so \( v_\wp(D_{L/Q}) = 9 \); further \( v_{\wp'}(D_{L/Q}) = 9 \) for any prime \( \wp' \) above 3 in \( \mathcal{O}_L \) since the different is an ambiguous ideal. This yields that the 3–adic valuation of the discriminant of \( L \) is 81. The ramification index in \( L/Q \) is 6, so by Lemma 5 we conclude that the 3–adic valuation of the discriminant of \( K \) is 36.

**Remark.** Contrary to \( \wp_1 \), the ideals \( \wp_2 \) and \( \wp_3 \) of \( \mathcal{O}_N \) are ramified in \( M/N \). As we shall see more precisely in subsection 4.2 for the extension \( K/Q \), of Galois group isomorphic to that of \( L/Q(\zeta_3) \), the three conjugated subgroups of order 3 of \( \text{Gal}(L/Q(\zeta_3)) \) appear as ramification groups of prime ideals above 3 in \( \mathcal{O}_L \), hence some of these ideals are not ramified in \( L/M = L^{(\sigma^2)} \) and have to be above ideals that ramify in \( M/N \).

### 3.3.4 The case \( v_3(b) = 1 \)

Finally we consider the case \( v_3(b) = 1 \). Let us denote by \( \gamma \) a cubic root of \( \beta \). The identity
\[
1 - \beta = (1 - \gamma)(1 - \zeta_3 \gamma)(1 - \zeta_3^2 \gamma)
\]
and the fact that \( 1 - \gamma, 1 - \zeta_3 \gamma \) and \( 1 - \zeta_3^2 \gamma \) are conjugated give us that
\[
v_{\sqrt{-3}}(1 - \gamma) = 1,
\]
so the minimal polynomial of \( \sqrt[3]{7} - 1 \), namely \( X^3 + 3X^2 + 3X + 1 - \gamma \), is an Eisenstein polynomial. By Lemma 2 the extension \( M/Q(\sqrt[3]{7}) \) is totally ramified and the \((\sqrt{-3})\)–adic valuation of the relative discriminant ideal is equal to the \((\sqrt{-3})\)–adic valuation of the polynomial \( X^3 - \gamma \). The discriminant of this polynomial is \( 3^3 \gamma^2 \) and its \((\sqrt{-3})\)–adic valuation is 6, so by Lemma 4, the \((\sqrt{-3})\)–adic valuation of the discriminant of \( M/Q(\zeta_3) \) is 18 and the 3–adic valuation of the absolute discriminant of \( M \) is 27.

We now deal with the extension \( L/M \). We set \( \pi = \sqrt[3]{7} - 1 \); it is a uniformizing parameter for the only prime above 3 in \( \mathcal{O}_M \). Since the residual degree of \( M_\pi/Q_3 \) equals 3, we know that the group of local units \( \mathcal{O}_{M_\pi}^\times \) contains a cyclic subgroup of order 26 = \( 3^3 - 1 \), which we denote by \( \mu_{26} \). Recall that any integral element \( x \) of \( M_\pi \) may be written uniquely as \( x = \sum_{i \geq 0} x_i \pi^i \) with \( x_i \in \mu_{26} \cup \{0\} \) for all \( i \). We first show that \( \sqrt{-3} \) is —almost— a cube in \( M_\pi \) modulo \( \pi^8 \).
Lemma 6 There exists \( \delta \in \mu_{26} \setminus \{\pm 1\} \) such that \( \sqrt{-3} \equiv (\delta \pi (1 + \pi))^3 - \delta^9 \pi^7 \) (mod \( \pi^8 \)).

Proof. Recall from section 2 that \( b = 3b' \) with \( b' \equiv -1 \) (mod 3). From congruence (5) we get
\[
\sqrt{-3} \equiv \frac{\beta - 1}{3} \quad \text{(mod } 3\sqrt{-3}) \, .
\]
On the other hand, developing \( \pi^3 = (\sqrt{3} - 1)^3 \) yields \( \gamma - 1 = \pi^3 + 3\pi \sqrt{3} \); developing \( (\gamma - 1)^3 \) yields \( \beta - 1 \equiv \pi^9 + 3\pi^3 + 3\pi^6 + 9\pi^3 \sqrt{3} \) (mod \( \pi^{16} \)), hence
\[
\sqrt{-3} \equiv \frac{\pi^9}{3} + \pi^3 + \pi^6 + 3\pi \quad \text{(mod } \pi^8) \quad (6)
\]
since \( \sqrt{3} \equiv 1 \) (mod \( \pi \)). Let \( a_0 \in \mu_{26}, a_1, a_2, \ldots \in \mu_{26} \cup \{0\} \) be such that
\[
\sqrt{-3} = \sum_{i \geq 0} a_i \pi^{3i} = a_0 \pi^3 \left( 1 + \sum_{i \geq 1} b_i \pi^i \right),
\]
where \( b_i = \frac{a_i}{a_0} \) for \( i \geq 1 \), then we have the congruence modulo \( \pi^{11} \):
\[
3 \equiv -a_0^2 \pi^6 \left( 1 - b_1 \pi + (b_1^2 - b_2) \pi^2 - (b_1 b_2 + b_3) \pi^3 + (b_2^2 - b_1 b_3 - b_4) \pi^4 \right) \, . \quad (7)
\]
Consequently \( 3\pi \equiv -a_0^2 \pi^7 \) (mod \( \pi^8 \)) and
\[
\frac{\pi^9}{3} \equiv -\frac{\pi^3}{a_0^2} \left( 1 + b_1 \pi + b_2 \pi^2 + (b_3 - b_1^2) \pi^3 + (b_4 - b_1^4) \pi^4 \right) \quad \text{(mod } \pi^8) \, .
\]
Congruence (6) yields the system of equations:
\[
\begin{aligned}
a_0^3 &= -1 + a_0^2 \quad \text{(i)} \\
a_0^3 b_1 &= -b_1 \quad \text{(ii)} \\
a_0^3 b_2 &= -b_2 \quad \text{(iii)} \\
a_0^3 b_3 &= a_0^2 + b_1^2 - b_3 \quad \text{(iv)} \\
a_0^3 b_4 &= -a_0^4 + b_1^4 - b_4 \quad \text{(v)}
\end{aligned}
\]
From equation (i), \( a_0 \) is a root of \( t^3 - t^2 + 1 \) (which is irreducible over \( \mathbb{F}_3 \)), hence \( a_0^3 \neq -1 \), so (ii) and (iii) imply \( b_1 = b_2 = 0 \). Then the system easily yields \( b_3 = 1 \) and \( b_4 = -a_0^2 \), so \( \sqrt{-3} \equiv a_0 \pi^3 + a_0 \pi^6 - a_0^3 \pi^7 \) (mod \( \pi^8 \)). Let \( \delta \in \mu_{26} \) be such that \( \delta^3 = a_0 \) to get the result. 

Consider the polynomial
\[
V(X) = X^3 + \frac{3(1 + \pi)^2}{\pi^4} \zeta_3 X - \frac{(1 + \pi)^3}{\pi^6} \sqrt{-3}
\]
and let \( x = \frac{\delta (1 + \pi)^2}{\pi} \). We claim that \( V(X + x) \), which equals:

\[
X^3 + 3xX^2 + \left(3x^2 + \frac{3(1 + \pi)^2}{\pi^4}\zeta_3\right)X + \frac{3(1 + \pi)^2}{\pi^4}\zeta_3x + x^3 - \frac{(1 + \pi)^3}{\pi^6}\sqrt{-3}
\]

is an Eisenstein polynomial for the prime \((\pi)\): it is clear that the coefficients of \(X\) and \(X^2\) have valuation greater than 1; further, congruence (7) yields:

\[
\frac{3(1 + \pi)^2}{\pi^4}\zeta_3x \equiv \frac{3}{\pi^5}\delta \equiv -\delta^7\pi \pmod{\pi^2}
\]

and we deduce from Lemma 6 that

\[
x^3 - \frac{(1 + \pi)^3}{\pi^6}\sqrt{-3} = \frac{(1 + \pi)^3}{\pi^6}\left(\delta^3\pi^3(1 + \pi)^3 - \sqrt{-3}\right) \equiv \delta^6\pi \pmod{\pi^2},
\]

so that

\[
\frac{3(1 + \pi)^2}{\pi^4}\zeta_3x + x^3 - \frac{(1 + \pi)^3}{\pi^6}\sqrt{-3} \equiv \delta^7(\delta^2 - 1)\pi \not\equiv 0 \pmod{\pi^2},
\]

namely the constant coefficient of \(V(X + x)\) is of \(\pi\)-adic valuation 1.

By Lemma 2, the extension \(L/M\) is totally ramified above \(\pi\), and the \(\pi\)-adic valuation of its discriminant equals that of the discriminant of \(V\), which is easily computed:

\[
\text{disc}(V) = -\frac{27(1 + \pi)^6}{\pi^{12}},
\]

hence \(v_3(\text{d}_{L/M}) = 6\). Lemma 4 then shows \(v_3(\text{d}_{L/Q}) = 99\) and we conclude using Lemma 5 that \(v_3(\text{d}_{K/Q}) = 48\).

This ends the proof of Theorem 2.

4 Some consequences

4.1 Uniformizing parameters

In the proof of Theorem 2, we managed to find a uniformizing parameter of \(L\) at any prime ideal above 3 when \(v_3(b) = 0\) or \(v_3(b) \geq 2\), and to construct an Eisenstein polynomial \(V(X + x)\) for \(L/M\) when \(v_3(b) = 1\). Since Cardano’s formulas \([C1]\) enable computing the roots of \(V\), we get an explicit uniformizing parameter in every case:

Corollary 1 With the notations introduced above, a uniformizing parameter of \(L\) at any prime ideal above 3 is \(\pi = \sqrt[3]{3} - 1\) when \(v_3(b) = 0\); \(\zeta_9 - 1\) when \(v_3(b) \geq 2\); when \(v_3(b) = 1\), let \(p\) denote the only prime ideal of \(\mathcal{O}_L\) above 3, we get a local uniformizing parameter:

\[
\frac{1 + \pi}{\pi^2}\zeta_9(1 - \zeta_9) - \frac{\delta (1 + \pi)^2}{\pi} \in L_p,
\]

where \(\delta\) is defined as in Lemma 6.
Taking the norm from \( L \) to \( K \), or from \( L_p \) to \( K_p \) where \( \mathfrak{p} = \mathcal{O}_K \cap p \), one easily deduces formulas for a uniformizing parameter of \( K \) or of \( K_p \) at any prime ideal above 3: \( 2 - \sqrt[3]{3} - \sqrt[3]{3}^{-1} \) when \( v_3(b) = 0 \), \( 2 - \zeta_9 - \zeta_9^{-1} \) when \( v_3(b) \geq 2 \); when \( v_3(b) = 1 \), we would prefer not to write the formula unless we really need to.

### 4.2 Ramification subgroups

Let \( E/F \) denote a Galois extension of number fields, of Galois group \( G \), and let \( \mathfrak{p} \) denote a prime ideal of \( \mathcal{O}_E \), of decomposition group \( G_{-1}(\mathfrak{p}) \subseteq G \). Recall that \( G_{-1}(\mathfrak{p}) \) is isomorphic to the Galois group of the extension of local fields \( E_p/F_\nu \), where \( \mathfrak{p} = \mathfrak{p} \cap \mathcal{O}_F \), and that there exists a filtration

\[
G_{-1}(\mathfrak{p}) \supseteq G_0(\mathfrak{p}) \supseteq G_1(\mathfrak{p}) \supseteq G_2(\mathfrak{p}) \cdots
\]

of (finitely many non trivial) normal subgroups \( G_i(\mathfrak{p}) \) of \( G_{-1}(\mathfrak{p}) \), such that \( G_0(\mathfrak{p}) \) is the ramification group of \( E/F \) above \( \mathfrak{p} \) (hence its order \( |G_0(\mathfrak{p})| \) equals the ramification index of \( E/F \) above \( \mathfrak{p} \)) and \( G_1(\mathfrak{p}) \) is the \( p \)-Sylow subgroup of \( G_0(\mathfrak{p}) \), where \( p \) stands for the characteristic of the residual field \( \mathcal{O}_E/\mathfrak{p} \).

We shall say that an integer \( n \geq -1 \) is a *jump* for the ramification filtration \( (G_i(\mathfrak{p}))_{i \geq -1} \) if \( G_{n+1}(\mathfrak{p}) \neq G_n(\mathfrak{p}) \). The valuation at the prime ideal \( \mathfrak{p} \) of the different of \( E/F \) is given by Hilbert’s formula [S, IV.1 Prop.4]:

\[
v_p(D_{E/F}) = \sum_{i \geq 0} (|G_i(\mathfrak{p})| - 1) .
\]

The extension \( E/F \) is *weakly ramified* if \( G_2(\mathfrak{p}) \) is trivial for every prime ideal \( \mathfrak{p} \) of \( \mathcal{O}_E \), in other words if no prime ideal of \( \mathcal{O}_E \) has a jump larger than 1 in its ramification filtration. See for instance [E, §2] for the interest of this definition in terms of Galois module structure.

We can now state the following easy consequence of Theorem 2 about the jumps of the ramification filtration above 3 in \( K/Q \).

**Corollary 2** The set of jumps in the ramification filtration of any prime ideal of \( \mathcal{O}_K \) above 3 is: \( \{1, 4\} \) if \( v_3(b) = 0 \) and \( a' \equiv b' \pmod{3} \); \( \{-1, 1, 4\} \) if \( v_3(b) = 0 \) and \( a' \not\equiv b' \pmod{3} \); \( \{-1, 1\} \) if \( v_3(b) = 1 \) or \( 2 \); \( \{1\} \) if \( v_3(b) \geq 3 \).

Consequently, the extension \( K/Q \) is weaklyramified if and only if \( v_3(b) \geq 1 \).

**Proof.** Denote by \( (G_i)_{i \geq -1} \), the ramification filtration for a prime \( \mathfrak{p} \) above 3 in \( \mathcal{O}_K \). Using the notations of Theorem 2, one has \( |G_{-1}| = ef \); further since \( K/Q \) is a 3-extension, one also has \( |G_0| = |G_1| = e \), and Hilbert’s formula (8) yields:

\[
v_p(D_{K/Q}) = 2(e - 1) + \sum_{i \geq 2} (|G_i| - 1) .
\]

Since \( d_{K/Q} = N_{K/Q}(D_{K/Q}) \), one has \( v_3(d_{K/Q}) = fgv_p(D_{K/Q}) = \frac{27}{e} v_p(D_{K/Q}) \). The computation of the jumps follows in each case using Theorem 2 and recalling
that $G_{i+1} \subseteq G_i$ for all $i$. Further, $K/Q$ is unramified outside 3 and $p$ and tamely ramified at $p$, which implies $G_1(\varphi) = \{1\}$ for any prime ideal $\varphi$ of $\mathcal{O}_K$ above $p$.

Note that cases $v_3(b) = 1$ and $v_3(b) = 2$ are quite different, even though they share the same set of jumps above 3, since the decomposition group above 3 is $G$ in the first case and a subgroup of $G$ of order 9 in the second. In particular, the local extension $K_p/Q_3$, where $p$ stands for a prime ideal of $\mathcal{O}_K$ above 3, is non abelian in the first case, abelian in the second. In fact, we are able to state the following more precise result about the ramification subgroups above 3 in $K/Q$. Before doing so, recall that $G = \text{Gal}(K/Q)$ has the following presentation:

$$G = \langle \sigma, \tau \mid \sigma^3 = 1, \tau^9 = 1, \sigma \tau \sigma^{-1} = \tau^{-2} \rangle,$$

from which one easily checks that $G$ has the subgroups diagram of Figure 2, in which all subgroups of index 3 (second line) are normal, whereas only one subgroup of index 9 (third line) is normal: $\langle \tau^3 \rangle$, the three other ones being conjugated.

**Figure 2: Subgroups diagram of $G$**

**Proposition 3** Let $p$ be a prime ideal of $\mathcal{O}_K$ above $p$, then $G_0(p) = \langle \tau \rangle$. Let $p_1, \ldots, p_g$ denote the prime ideals of $\mathcal{O}_K$ above 3, then:

- $v_3(b) = 0$: for $1 \leq k \leq g$, $G_{-1}(p_k) = G$ if $a \neq b$ (mod 3), the ramification group otherwise; in both cases, $G_0(p_k) = G_1(p_k) = \langle \sigma^2 \tau \rangle$ and $G_2(p_k) = G_3(p_k) = G_4(p_k) = \langle \tau^3 \rangle$, the only subgroup of order 3 of $G_0(p_k)$;

- $v_3(b) = 1$: $G_{-1}(p_1) = G$ and $G_0(p_1) = G_1(p_1)$ is the only normal subgroup of $G$ of order 9 and exponent 3, namely $\langle \tau^3, \sigma \rangle$;

- $v_3(b) = 2$: $G_{-1}(p_k) = \langle \tau^3, \sigma \rangle$ for every $1 \leq k \leq 3$ and the groups $G_0(p_k) = G_1(p_k)$, $1 \leq k \leq 3$, are the three conjugated subgroups of order 3 of $G$, namely $\langle \sigma \rangle$, $\langle \tau \tau^3 \rangle$ and $\langle \tau \tau^6 \rangle$;
• \(v_3(b) \geq 3\): each of the three conjugated subgroups of order 3 of \(G\) equals 
\(G_{-1}(p_k) = G_0(p_k) = G_1(p_k)\) for exactly three values of \(1 \leq k \leq 9\).

**Proof.** The assertion about \(p\) is easy since we have seen in Subsection 3.2 that \(p\) is unramified in \(\mathbb{Q}(\zeta_9)/\mathbb{Q}\) and that any prime ideal of \(\mathcal{O}_L\) above \(p\) is totally ramified in \(L/\mathbb{Q}(\zeta_9) = L^{(\tau)}\). So the ramification group in \(L/\mathbb{Q}\) of such a prime ideal is \(\langle \tau \rangle\) and we get the result using Herbrand’s theorem [S, IV.3 Lemme 5].

A study of the group 
\[
\mathcal{G} = \text{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^6 = 1, \tau^9 = 1, \sigma \tau \sigma^{-1} = \tau^{-2} \rangle
\]
shows that \(\mathcal{G}\) has four subgroups of order 9, three of which are cyclic: \(\langle \tau \rangle, \langle \sigma^2 \tau \rangle, \langle \sigma^4 \tau \rangle\), and one is of exponent 3: \(\langle \sigma^2, \tau^3 \rangle\). We already know by Theorem 2 that \(L/L^{(\tau)} = \mathbb{Q}(\zeta_9)\) is never totally ramified above the prime ideal \((1 - \zeta_3)\), hence \(\tau\) never belongs to the ramification group of a prime ideal of \(\mathcal{O}_L\) above \(3\). Let us show that the same is true for \(\sigma^4 \tau\), and for \(\sigma^2 \tau\) when \(v_3(b) \geq 1\); we shall see below that the assertion about \(\sigma^2 \tau\) does not extend to the case \(v_3(b) = 0\).

**Lemma 7** Set \(\gamma = (\sqrt{-3})^3\), then \(L^{(\sigma^2 \tau)} = \mathbb{Q}(\zeta_9^2 \gamma)\) is ramified over \(\mathbb{Q}(\zeta_3)\) above \(\sqrt{-3}\) when \(v_3(b) \geq 1\), and \(L^{(\sigma^4 \tau)} = \mathbb{Q}(\zeta_9 \gamma)\) is always ramified over \(\mathbb{Q}(\zeta_3)\) above \(\sqrt{-3}\).

We illustrate the result in Figure 3.

![Figure 3: Ramification above \(\sqrt{-3}\) in the subextensions of \(L\) of index 9](image-url)

**Proof.** One easily checks that \(\sigma^2 \tau(\zeta_9^2 \gamma) = \zeta_9^2 \gamma\) and \(\sigma^4 \tau(\zeta_9 \gamma) = \zeta_9 \gamma\), then comparing degrees yields \(L^{(\sigma^2 \tau)} = \mathbb{Q}(\zeta_9^2 \gamma)\) and \(L^{(\sigma^4 \tau)} = \mathbb{Q}(\zeta_9 \gamma)\). Further, \(\zeta_9 \gamma\) is a root of \(R(X) = X^3 - \zeta_9^2 \beta \in \mathbb{Z}_3[\zeta_3][X]\) and 
\[
R(X + 1) = X^3 + 3X^2 + 3X + 1 - \zeta_9^2 \beta ,
\]
which is an Eisenstein polynomial for the prime ideal \((\sqrt{-3}) = (1 - \zeta_9^2)\) when \(v_3(b) \geq 1\), since \(1 - \zeta_9^2 \beta = \zeta_9^3 (1 - \beta) + (1 - \zeta_9^2)\) and \(v_{\sqrt{-3}}(1 - \beta) \geq 3\) in this case;
the case \( v_3(b) = 0 \) is different: congruences (3) and (4) shown in subsection 3.3.1 yield
\[
\zeta_3^2 \beta \equiv 1 \pmod{3},
\]
hence \( R(X + 1) \) is no longer Eisenstein for the prime ideal \( (\sqrt{-3}) \). Analogously, the minimal polynomial of \( \zeta_9 \gamma - 1 \) is \( X^3 + 3X^2 + 3X + 1 - \zeta_3 \beta \), which is always an Eisenstein polynomial for the prime ideal \( (\sqrt{-3}) = (1 - \zeta_3) \), since \( \zeta_3 \beta \neq 1 \pmod{3} \) when \( v_3(b) = 0 \), hence the extension \( \mathbb{Q}(\zeta_3^2 \gamma)/\mathbb{Q}(\zeta_3) \) is always totally ramified above this prime.

Let us deduce the first two statements of Proposition 3 from Lemma 7. Suppose \( v_3(b) = 0 \): \( L^{(\sigma^4 \tau)} = \mathbb{Q}(\zeta_9 \gamma) \) and \( \mathbb{Q}(\gamma) = L^{(\sigma^2, \tau^3)} \) are ramified over \( \mathbb{Q}(\zeta_3) \) above \( \sqrt{-3} \), just as \( L^{(\tau)} = \mathbb{Q}(\zeta_9) \), hence neither \( \langle \sigma^4 \tau \rangle \), nor \( \langle \sigma^2, \tau^3 \rangle \), nor \( \langle \tau \rangle \), may be contained in the ramification group of a prime ideal \( \wp \) of \( \mathcal{O}_L \) above 3; by Theorem 2, such a group is of order 18, its 3-Sylow subgroup \( \mathcal{G}_1(\wp) \) of order 9 thus has to be \( \langle \sigma^2 \tau \rangle \) (which implies that \( \mathbb{Q}(\zeta_3^2 \gamma)/\mathbb{Q}(\zeta_3) \) is unramified above \( \sqrt{-3} \) as announced). Set \( \wp = \wp \cap \mathcal{O}_K \), one knows (using Herbrand’s theorem, substitute \( u \) for 1 in [S, IV.3 Lemme 5]) that:
\[
G_1(\wp) = \left( \mathcal{G}_1(\wp) \langle \sigma^3 \rangle \right)/\langle \sigma^3 \rangle,
\]
so \( G_0(\wp) = G_1(\wp) = \langle \sigma^2 \tau \rangle \). The result concerning the ramification subgroups of higher index is straightforward in view of Corollary 2 and of the subgroups diagram of \( G \) (Figure 2).

In the case \( v_3(b) = 1 \), the result of Lemma 7 implies that \( L/L^{(\sigma^2 \tau)} \) and \( L/L^{(\sigma^4 \tau)} \) are not totally ramified above 3, hence neither \( \sigma^2 \tau \) nor \( \sigma^4 \tau \) may belong to the first ramification group \( \mathcal{G}_1(\wp) \) of a prime ideal \( \wp \) of \( \mathcal{O}_L \) above 3. This was already known for \( \tau \), consequently \( \mathcal{G}_1(\wp) \) contains no element of order 9 of \( \mathcal{G} \), hence can only equal \( \langle \sigma^2, \tau^3 \rangle \) since its order is 9. This proves the assertion of the Proposition for the case \( v_3(b) = 1 \) using (9).

Before dealing with the case \( v_3(b) \geq 2 \), let us state an auxiliary result that is valid in all cases. Consider the abelian subgroup \( \langle \tau, \sigma^3 \rangle \) of \( \mathcal{G} \) of order 18, the corresponding subextension \( W \) of \( L \) satisfies
\[
W = L^{(\tau, \sigma^3)} = \mathbb{Q}(\zeta_9)^{\langle \sigma^3 \rangle} = K^{(\tau)},
\]
in other words:

**Lemma 8** The only subextension \( W \) of \( \mathbb{Q}(\zeta_9) \) of degree 3 over \( \mathbb{Q} \) is the fixed field of \( K \) under \( \langle \tau \rangle \).

Suppose \( v_3(b) \geq 2 \). The extension \( W/\mathbb{Q} \) is ramified (weakly ramified indeed) above 3, hence by Theorem 2 the extension \( K/W \) can not be ramified at a prime ideal \( \wp \) above 3. The ramification group \( G_0(\wp) \) then has to be one of the three conjugated subgroups of order 3 of \( G \) (see Figure 3): \( \langle \tau \rangle, \langle \tau \tau^3 \rangle \) or \( \langle \tau \tau^6 \rangle \).
Since 3 splits in $K/\mathbb{Q}$, these three subgroups occur as ramification groups, of one prime ideal above 3 each in case $v_3(b) = 2$, of three of these each in case $v_3(b) \geq 3$.

The three cyclic subgroups of order 9 of $G$ only contain one subgroup of order 3: $\langle \tau^3 \rangle$, hence the decomposition group of a prime ideal of $O_K$ above 3 can only be $\langle \sigma, \tau^3 \rangle$ in the case $v_3(b) = 2$. ■

The proof of Proposition 3 given above involves arguments already used in [V, §4.2], which we present here in a more complete and systematic manner.

5 Class groups

We are interested in the 3-part of the class group of the field $K$. We begin by considering the bicyclic bicubic subextension $B$ of $K$ fixed by $\langle \tau^3 \rangle$, the (only) normal subgroup of order 3. Recall our conventions for $a$ and $b$ such that $p = a^2 + 3b^2$ at the beginning of Section 2.

**Proposition 4** The class number $h_B$ of $B$ is divisible by 3 if and only if

$$p \equiv 1 \mod 9 \text{ and } (a \equiv b \text{ or } b \equiv 0 \mod 9).$$

**Proof.** We know that 3 and $p$ are the only ramified primes in $K/\mathbb{Q}$, as well as in $B/\mathbb{Q}$. By [P2, Theorem 9], we deduce that 3 divides $h_B$ if and only if $p$ is a cubic residue modulo 9 and 3 is a cubic residue modulo $p$. Since $p \equiv 1 \mod 3$, $p$ is a cubic residue modulo 9 if and only if $p \equiv 1 \mod 9$.

Further $p$ can be uniquely written as $p = \frac{1}{3}(L^2 + 3M^2)$ up to the signs of $L$ and $M$ (see [IR, Proposition 8.3.2]). To do that, note that exactly one out of $s = a+b$, $d = a-b$, $b$ is divisible by 3, and that $4p = (2a)^2 + 3(2b)^2 = (2s-d)^2 + 3d^2 = (2d-s)^2 + 3s^2$. By [L2, Proposition 7.2], 3 is a cube modulo $p$ if and only if 3 divides $M$, namely if and only if one of $a+b$, $a-b$, $b$ is divisible by 9. This yields the result since $a \equiv -b \mod 9$ is not possible with our conventions. ■

The preceding result can be expressed in the following condensed way.

**Corollary 3** One has: $3 \mid h_B \iff a' \equiv b' \equiv b \mod 3$. Therefore $3 \mid h_B$ can only occur when $v_3(b) = 0$ with $a' \equiv b' \mod 3$, and when $v_3(b) \geq 2$.

Not every $p$ with $v_3(b) = 0$ and $a' \equiv b' \mod 3$ has $h_B$ divisible by 3, see $p = 61$ in the Table given in Subsection 6.2 below.

**Proof.** Since $p \equiv 1 + 3(2a' + b) \mod 9$ (note that $b^2 \equiv b \mod 3$ with our conventions),

$$p \equiv 1 \mod 9 \iff a' \equiv b \mod 3.$$  

Assume $p \equiv 1 \mod 9$. If $b \equiv 0 \mod 9$ then $b = 3b'$ with $b' \equiv 0 \mod 3$, thus $a' \equiv b' \equiv b(\equiv 0) \mod 3$. If $a \equiv b \mod 9$ then $a \equiv a' \equiv b \equiv 1 \mod 3$, so
b = 1 + 3b′ ≡ 1 + 3a′ mod 9, hence b′ ≡ a′ mod 3. We get by Proposition 4 that
3 ∣ h_B implies a′ ≡ b′ ≡ b mod 3.

Assume a′ ≡ b′ ≡ b mod 3 (so p ≡ 1 mod 9). If b ≡ 0 mod 3 then the same
holds for b′ thus b = 3b′ ≡ 0 mod 9; otherwise b ≡ 1 mod 3 and the same holds
for a′ and b′, which yields a ≡ b(≡ 4) mod 9. In both cases we get 3 ∣ h_B by
Proposition 4.

The second assertion is clear. ■

One easily extends the former proof to show the extra characterization:

3 ∣ h_B ⇐⇒ (a ≡ 1, b ≡ 0 mod 9) or (a ≡ b ≡ 4 mod 9).

We now deduce a result for the class group of the field K.

**Corollary 4** Suppose (p ≡ 1 and a ≡ b mod 9) or (p ≡ 1 and b ≡ 0 mod 9),
then 3 divides the class number h_K of K.

**Proof.** The Hilbert class field H_B of B is unramified over B of degree h_B. Since
K/B is totally ramified above p by Proposition 3, it is linearly disjoint with
H_B/B, hence the compositum KH_B is unramified of degree h_B above K. We get
that h_B ∣ h_K, so Proposition 4 yields the result. ■

Reversing the argument, we can show the following result about the subfield
\( \mathbb{Q}(\sqrt[3]{\beta} + \sqrt[3]{\beta^{-1}}) \) of K of minimal polynomial \( f_p \) defined in Proposition 2.

**Proposition 5** Suppose \( v_3(b) = 0 \) then the class group of \( K^{(\sigma)} = \mathbb{Q}(\sqrt[3]{\beta} + \sqrt[3]{\beta^{-1}}) \)
contains a subgroup of order 3.

**Proof.** By Proposition 3, the ramification group of the ideals above 3 in K
is \( \langle \sigma^2 \tau \rangle \), so \( K/K^{(\sigma)} \) is unramified above 3. Since \( L/\mathbb{Q}(\zeta_9) \) (resp. \( \mathbb{Q}(\zeta_9)/\mathbb{Q} \))
is totally ramified (resp. unramified) above p, we deduce that the ramification
group of the prime ideals above p in K is \( \langle \tau \rangle \). Hence \( K/K^{(\sigma)} \) is unramified,
and its Galois group, which is cyclic of order 3, is isomorphic to a subgroup of
the class group of \( K^{(\sigma)} \). ■

### 6 Numerical instances

#### 6.1 Ramification

The next table presents examples of prime numbers p congruent to 1 modulo 3,
which are the smallest ones corresponding to each entry in the table of Theorem 2
(the congruences appearing in the table are modulo 3). We give the ramification
groups for the prime ideals above 3. All unspecified ramification groups are
trivial.
The computations performed under PARI/GP\[P1\] are in agreement with the results of the previous sections. We used an algorithm described in \[A\] for the computation of the Galois group and an experimental facility for the computation of ramification groups that was developed specially for this project.

### 6.2 Class groups

Here is a table presenting the structure of the class group of $K$ and of its bicubic bicyclic subextension $B = K(\tau^3)$, for the values of the parameter $p$ congruent to 1 mod 3 in the range $[7, 307]$. The computations have been achieved using PARI/GP\[P1\]; the validity of the results relies on the General Riemann Hypothesis. All unspecified class groups are trivial.

<table>
<thead>
<tr>
<th>$p$</th>
<th>61</th>
<th>7</th>
<th>31</th>
<th>307</th>
<th>2203</th>
</tr>
</thead>
<tbody>
<tr>
<td>$v_3(b)$</td>
<td>$0$</td>
<td>$0$</td>
<td>$1$</td>
<td>$2$</td>
<td>$3$</td>
</tr>
<tr>
<td>$e$</td>
<td>$9$</td>
<td>$9$</td>
<td>$9$</td>
<td>$3$</td>
<td>$3$</td>
</tr>
<tr>
<td>$f$</td>
<td>$1$</td>
<td>$3$</td>
<td>$3$</td>
<td>$1$</td>
<td>$9$</td>
</tr>
<tr>
<td>$g$</td>
<td>$3$</td>
<td>$1$</td>
<td>$1$</td>
<td>$3$</td>
<td>$9$</td>
</tr>
<tr>
<td>$3\mathcal{O}_K$</td>
<td>$p_1^9p_2^3p_3^9$</td>
<td>$p_1^9$</td>
<td>$p_2^9$</td>
<td>$p_1^9p_2^3p_3^9$</td>
<td>$\prod_{i=1}^9 p_i^3$</td>
</tr>
<tr>
<td>$G_{-1}(p_i)$</td>
<td>$\langle \sigma^2, \tau \rangle$</td>
<td>$G$</td>
<td>$\langle \sigma, \tau \rangle$</td>
<td>$\langle \sigma, \tau \rangle$</td>
<td>$\langle \sigma, \tau \rangle$</td>
</tr>
<tr>
<td>$G_0(p_i)$</td>
<td>$\langle \sigma^2, \tau \rangle$</td>
<td>$\langle \sigma, \tau \rangle$</td>
<td>$\langle \sigma, \tau \rangle$</td>
<td>$\langle \sigma, \tau \rangle$</td>
<td>$\langle \sigma, \tau \rangle$</td>
</tr>
<tr>
<td>$G_1(p_i)$</td>
<td>$\langle \sigma^2, \tau \rangle$</td>
<td>$\langle \sigma, \tau \rangle$</td>
<td>$\langle \sigma, \tau \rangle$</td>
<td>$\langle \sigma, \tau \rangle$</td>
<td>$\langle \sigma, \tau \rangle$</td>
</tr>
<tr>
<td>$G_2(p_i)$</td>
<td>$\langle \tau^3 \rangle$</td>
<td>$\langle \tau^3 \rangle$</td>
<td>$\langle \tau^3 \rangle$</td>
<td>$\langle \tau^3 \rangle$</td>
<td>$\langle \tau^3 \rangle$</td>
</tr>
<tr>
<td>$G_3(p_i)$</td>
<td>$\langle \tau^3 \rangle$</td>
<td>$\langle \tau^3 \rangle$</td>
<td>$\langle \tau^3 \rangle$</td>
<td>$\langle \tau^3 \rangle$</td>
<td>$\langle \tau^3 \rangle$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p$</th>
<th>$a$</th>
<th>$b$</th>
<th>$a'$</th>
<th>$b'$</th>
<th>$\text{Cl}(B)$</th>
<th>$\text{Cl}(K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>$-2$</td>
<td>$1$</td>
<td>$-1$</td>
<td>$0$</td>
<td>$\langle 3 \rangle$</td>
<td>$\langle 3 \rangle$</td>
</tr>
<tr>
<td>13</td>
<td>$1$</td>
<td>$-2$</td>
<td>$0$</td>
<td>$-1$</td>
<td>$\langle 3 \rangle$</td>
<td>$\langle 3 \rangle$</td>
</tr>
<tr>
<td>19</td>
<td>$4$</td>
<td>$1$</td>
<td>$1$</td>
<td>$0$</td>
<td>$\langle 3 \rangle$</td>
<td>$\langle 3 \rangle$</td>
</tr>
<tr>
<td>31</td>
<td>$-2$</td>
<td>$-3$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$\langle 3 \rangle$</td>
<td>$\langle 3 \rangle$</td>
</tr>
<tr>
<td>37</td>
<td>$-5$</td>
<td>$-2$</td>
<td>$-2$</td>
<td>$-1$</td>
<td>$\langle 3 \rangle$</td>
<td>$\langle 3 \rangle$</td>
</tr>
<tr>
<td>43</td>
<td>$4$</td>
<td>$-3$</td>
<td>$1$</td>
<td>$-1$</td>
<td>$\langle 3 \rangle$</td>
<td>$\langle 3 \rangle$</td>
</tr>
<tr>
<td>61</td>
<td>$7$</td>
<td>$-2$</td>
<td>$2$</td>
<td>$-1$</td>
<td>$\langle 3 \rangle$</td>
<td>$\langle 3 \rangle$</td>
</tr>
<tr>
<td>67</td>
<td>$-8$</td>
<td>$1$</td>
<td>$-3$</td>
<td>$0$</td>
<td>$\langle 3 \rangle$</td>
<td>$\langle 3 \rangle$</td>
</tr>
<tr>
<td>73</td>
<td>$-5$</td>
<td>$4$</td>
<td>$-2$</td>
<td>$1$</td>
<td>$3$</td>
<td>$9 \times 3$</td>
</tr>
<tr>
<td>79</td>
<td>$-2$</td>
<td>$-5$</td>
<td>$-1$</td>
<td>$-2$</td>
<td>$2 \times 2$</td>
<td>$2 \times 2$</td>
</tr>
<tr>
<td>97</td>
<td>$7$</td>
<td>$4$</td>
<td>$2$</td>
<td>$1$</td>
<td>$\langle 3 \rangle$</td>
<td>$\langle 3 \rangle$</td>
</tr>
<tr>
<td>103</td>
<td>$10$</td>
<td>$1$</td>
<td>$3$</td>
<td>$0$</td>
<td>$\langle 3 \rangle$</td>
<td>$\langle 3 \rangle$</td>
</tr>
<tr>
<td>109</td>
<td>$1$</td>
<td>$6$</td>
<td>$0$</td>
<td>$2$</td>
<td>$\langle 3 \rangle$</td>
<td>$\langle 3 \rangle$</td>
</tr>
<tr>
<td>127</td>
<td>$10$</td>
<td>$-3$</td>
<td>$3$</td>
<td>$-1$</td>
<td>$2 \times 2$</td>
<td>$6 \times 2$</td>
</tr>
</tbody>
</table>
In the table we have bold faced the value of $a$ when it is congruent to that of $b$ modulo 9, the value of $a'$ when it is congruent to that of $b$ modulo 3; we have bold faced the value of $b$ in any of these two cases, and that of $b'$ when $b \equiv a' \equiv b' \mod 3$, which is equivalent to $3 \mid h_B$ by Proposition 4. We then see that $3 \mid h_K$ exactly when some of $a, b, a', b'$ are bold faced. Consequently we are in a position to make the following conjecture. (Recall that $p \equiv 1 \mod 9$ is equivalent to $a' \equiv b \mod 3$.)

**Conjecture 1** Each of the following conditions implies $v_3(h_K) \geq 1$:

(i) $p \equiv 1 \mod 9$ ;  
(ii) $a \equiv b \mod 9$.

This statement amounts to saying that the logical connective “and” in the first case of the statement of Corollary 4 can be replaced by “or”. One may check in the preceding table that $v_3(h_K) \geq 1$ is in fact equivalent to $(p \equiv 1$ or $a \equiv b \mod 9)$ for the values of the parameter in the range $[7, 307]$.

On the other hand, the other condition that appears in the statement of Corollary 4, namely $b \equiv 0 \mod 9$, is not sufficient to get $v_3(h_K) \geq 1$, as is readily shown by the computation of the class group of $K$ associated to the next value of $p$ with $9 \mid b$, 439, which yields a principal extension. We take advantage of the fact that the 3-power of the discriminant is the smallest possible in the case $9 \mid b$ to present a few more computations that confirm our conjecture [hopefully!] (even the equivalence is satisfied for the values of $p$ with $9 \mid b$ in the range $[397, 499]$).
\begin{table}[h]
\centering
\begin{tabular}{|c|cccc|cc|}
\hline
$p$ & $a$ & $b$ & $a'$ & $b'$ & $Cl(B)$ & $Cl(K)$ \\
\hline
499 & 16 & 9 & 5 & 3 & $2 \times 2$ & $2 \times 2$ \\
643 & -20 & 9 & -7 & 3 & & \\
727 & 22 & 9 & 7 & 3 & $2 \times 2$ & \\
919 & -26 & 9 & -9 & 3 & $39 \times 3$ & \\
997 & -5 & 18 & -2 & 6 & & \\
1021 & 7 & 18 & 2 & 6 & & \\
1093 & -11 & 18 & -4 & 6 & & \\
\hline
\end{tabular}
\end{table}

References


