On the ideal class group of the normal closure of $\mathbb{Q}(\sqrt[3]{n})$

René Schoof

Dipartimento di Matematica, Università di Roma “Tor Vergata”, I-00133 Roma ITALY

Abstract

For a prime number $p$ and an integer $n$ we determine the Galois cohomology groups of the class group of the normal closure of $\mathbb{Q}(\sqrt[3]{n})$ to a certain extent and use this information to prove a result about the group structure of the class group.

1. Introduction.

For an integer $m \geq 1$, we let $\zeta_m$ denote a primitive $m$-th root of unity. In 1971, Taira Honda [Ho] proved that the class number of $\mathbb{Q}(\zeta_3, \sqrt[3]{n})$ is equal to $h^2$ or $3h^2$, where $h$ is the class number of $\mathbb{Q}(\sqrt[3]{n})$. Around 2016, L.C. Washington proposed a refinement of this statement for certain values of $n$, which was then proved by the author. The result can be phrased as follows.

Proposition 1.1. Let $n \in \mathbb{Z}$ not be a cube. If $n$ is not divisible by any prime number congruent to 1 (mod 3), then the class group of $\mathbb{Q}(\zeta_3, \sqrt[3]{n})$ is isomorphic to $H \times H$ for some finite abelian group $H$.

In this note we put the statement of Prop.1.1 in a more general context and replace our earlier ad hoc proof of it by more conceptual arguments. This leads to a study of the Galois module structure of the class groups of the fields $\mathbb{Q}(\zeta_p, \sqrt[3]{n})$ for primes $p \geq 3$. In a recent paper Hubbard and Washington write that their proof of [6, Thm. 7] was inspired by the original proof of Proposition 1.1 for $p = 3$. That’s why we present it in an appendix.

The problem naturally splits into two parts. For the non-$p$-part of the class group, Proposition 1.1 can easily be generalized without any condition on $p$ or on the prime divisors $l$ of $n$. This is done in section 2 using Morita theory. For the $p$-part the problem is more subtle. We need to make the

Preprint submitted to Journal of Number Theory April 8, 2020
assumption that \( p \) is a regular prime, i.e. that \( p \) does not divide the class number of \( \mathbb{Q}(\zeta_p) \). The following proposition follows from our main results, which are Proposition 3.2 and Theorem 4.4. For \( p = 3 \) we recover Proposition 1.1.

**Proposition 1.2.** Let \( p > 2 \) be a regular prime and let \( n \in \mathbb{Z} \) not be a \( p \)-th power. Suppose that all prime divisors \( l \neq p \) of \( n \) are primitive roots modulo \( p \). Then the kernel \( Cl^0 \) of the norm map from the class group of \( \mathbb{Q}(\zeta_p, \sqrt[p]{n}) \) to the class group of \( \mathbb{Q}(\zeta_p) \) sits in an exact sequence

\[
0 \rightarrow V \rightarrow Cl^0 \rightarrow H \times H \times \ldots \times H \rightarrow 0,
\]

where \( H \) is a finite abelian group \( H \) and \( V \) an \( \mathbb{F}_p \)-vector space of dimension at most \( \left( \frac{p-3}{2} \right)^2 \).

Throughout this note we fix a prime \( p > 2 \) and a primitive \( p \)-th root of unity \( \zeta_p \). We study the ideal class groups of the fields

\[
K = \mathbb{Q}(\zeta_p, \sqrt[n]{\mathbb{Q}}),
\]

where \( n \in \mathbb{Z} \) is not a \( p \)-th power. We have inclusions

\[
\mathbb{Q} \subset \mathbb{Q}(\zeta_p) \subset K.
\]

Put \( \Omega = \text{Gal}(K/\mathbb{Q}) \), \( G = \text{Gal}(K/\mathbb{Q}(\zeta_p)) \) and \( \Delta = \text{Gal}(K/\mathbb{Q}(\sqrt[p]{n})) \). Restriction to \( \mathbb{Q}(\zeta_p) \) identifies \( \Delta \) with \( \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \). The group \( \Omega \) is the semidirect product of \( \Delta \) by \( G \). There is a natural exact sequence

\[
1 \rightarrow G \rightarrow \Omega \rightarrow \Delta \rightarrow 1.
\]

The group \( G \) is isomorphic to \( \mathbb{Z}/p\mathbb{Z} \) and \( \Delta \) is somorphic to \( (\mathbb{Z}/p\mathbb{Z})^* \). If \( t \) denotes a generator of \( G \) and \( s \in \Delta \subset G \) is a generator of \( \Delta \), then a presentation of the group \( \Omega \) is given by

\[
\Omega = \langle t, s : s^{p-1} = 1, t^p = 1, sts^{-1} = t^{\omega(s)} \rangle.
\]

Here \( \omega : \Delta \rightarrow (\mathbb{Z}/p\mathbb{Z})^* \) denotes the cyclotomic character. In other words, we have \( \sigma(\zeta_p) = \zeta_p^{\omega(\sigma)} \) for all \( \sigma \in \Delta \).
The class group $Cl_K$ is a $\mathbb{Z}[\Omega]$-module. The $G$-norm map $N_G : Cl_K \to Cl_K$ factors through the class group of $\mathbb{Q}(\zeta_p)$:

$$
\begin{array}{c}
0 \\
\downarrow \\
\downarrow
\end{array} 
\begin{array}{c}
ker N_G \\
\rightarrow \\
\rightarrow
\end{array} 
\begin{array}{c}
Cl_K \\
\rightarrow \\
\rightarrow
\end{array} 
\begin{array}{c}
Cl_{\mathbb{Q}(\zeta_p)} \\
\rightarrow \\
\rightarrow
\end{array}
$$

The map from $Cl_{\mathbb{Q}(\zeta_p)}$ to the image of $N_G$ is an isomorphism on the prime to $p$-parts. So, the sequence

$$0 \to ker N_G \to Cl_K \to Cl_{\mathbb{Q}(\zeta_p)} \to 0.$$

is exact on the non-$p$-parts. We study the $p$-part of $Cl_K$ under the assumption that $p$ is a regular prime. In this case the $p$-parts of $Cl_K$ and $ker N_G$ are obviously equal.

Since we fix $p$, we concentrate on $ker N_G$ as $K$ varies. This is a left module over the non-commutative ring $R = \mathbb{Z}[\Omega]/(Tr_G)$, where $Tr_G$ denotes the central element $\sum_{g \in G}[g]$ of $\mathbb{Z}[\Omega]$. Since we have $\mathbb{Z}[G]/(Tr_G) \cong \mathbb{Z}[\zeta_p]$, the ring $R$ is isomorphic to the twisted group ring $\mathbb{Z}[\zeta_p][\Delta]'$. Multiplication in this ring satisfies $[\sigma]\lambda = \sigma(\lambda)[\sigma]$ for $\lambda \in \mathbb{Z}[\zeta_p]$ and $\sigma \in \Delta$. A module over $\mathbb{Z}[\zeta_p][\Delta]'$ can alternatively be viewed as a module over $\mathbb{Z}[\zeta_p]$, equipped with a semilinear action of $\Delta$.

2. The non-$p$-part.

Using the notations of the introduction, the non-$p$-part of the class group of $K$ is a left module over the twisted group ring $\mathbb{Z}[\zeta_p, \frac{1}{p}][\Delta]'$. Alternatively, it is a $\mathbb{Z}[\zeta_p, \frac{1}{p}]$-module equipped with semilinear left $\Delta$-action. The category of such modules is Morita equivalent to the category of modules over $\mathbb{Z}[\zeta_p, \frac{1}{p}]$. This follows from the following general result.

**Theorem 2.1.** Let $R \subset S$ be a finite Galois extension of commutative rings with Galois group $\Delta$. Then the ring $R$ and the twisted group ring $S[\Delta]'$ are Morita equivalent. In other words, the functors $R\text{-Mod} \to S[\Delta]'\text{-Mod}$ given by $M \mapsto M \otimes_R S$ and $S[\Delta]'\text{-Mod} \to R\text{-Mod}$ given by $N \mapsto N^{\Delta}$, induce an equivalence of categories.

**Proof.** Since $S$ is Galois over $R$, it is a faithful projective $R$-module and hence an $R$-progenerator. Since the natural map $S[\Delta]' \to \text{End}_R(S)$ is
an isomorphism [1, appendix], the result follows from Morita’s Theorem as presented in [4, Prop.3.3]. To see this, note that for a left $S$-module $N$ we have isomorphisms

$$N^\Delta \cong \text{Hom}_S(A, N) \cong \text{Hom}_R(R^\vee \otimes_S N) \cong R^\vee \otimes_S N.$$ 

Here $R^\vee$ denotes the right $S$-module $\text{Hom}_R(A, R)$ that appears in [4, Prop.3.3].

Let $p$ be a prime. An application of Theorem 2.1 to the Galois extension $\mathbb{Z}_{[\frac{1}{p}]} \subset \mathbb{Z}_{[\zeta_p, \frac{1}{p}]}$ with Galois group $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^\ast$ implies the following result.

**Corollary 2.2.** Let $p$ be prime, let $n \in \mathbb{Z}$ not be a $p$-th power, and let $K = \mathbb{Q}(\zeta_p, \sqrt[n]{p})$. Let $M$ denote the non-$p$-part of the kernel of the $G$-norm map $\text{Cl}_K \to \text{Cl}_K$. Then $M$ is isomorphic to $M^\Delta \otimes_{\mathbb{Z}} \mathbb{Z}_{[\zeta_p]}$. In particular, as an abelian group, $M$ is isomorphic to a product of $p - 1$ copies of $M^\Delta$.

The following proposition also implies Corollary 2.2. Its proof avoids general Morita theory and is based on an explicit computation.

**Proposition 2.3.** Let $Q \subset F$ be a Galois extension with $\Delta = \text{Gal}(F/Q)$. Let $M$ be a module over the ring of integers $O_F$ that is equipped with a semilinear action by $\Delta$. Let $M^\Delta$ denote its subgroup of $\Delta$-invariant elements and let $\phi$ denote the natural $O_F$-linear map

$$\phi : M^\Delta \otimes_{\mathbb{Z}} O_F \to M,$$

given by $\phi(m \otimes \lambda) = \lambda m$ for $m \in M^\Delta$ and $\lambda$ in $O_F$. Then the kernel and the cokernel of $\phi$ are $O_F$-modules that are killed by the different $\delta_F$ of $F$.

**Proof.** Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis for $O_F$. Then any element in $M^\Delta \otimes_{\mathbb{Z}} O_F$ can be written as $\sum_i m_i \otimes \omega_i$, where $m_i \in M^\Delta$. Suppose that $x = \sum_i m_i \otimes \omega_i$ is in the kernel of $\phi$. This means that $\sum_i \sigma(\omega_i)m_i = 0$ in $M$. Applying $\sigma \in \Delta$, we see that $\sum_i \sigma(\omega_i)m_i = 0$ for every $\sigma \in \Delta$.

Now let $z \in \delta_F$. Let $\omega_1^*, \ldots, \omega_n^* \in F$ be the dual base of $\omega_1, \ldots, \omega_n$. This means that

$$\sum_{\sigma \in \Delta} \sigma(\omega_i \omega_j^*) = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j. \end{cases}$$

By definition of the different, $z\sigma(\omega_i^*)$ is in $O_F$ for every $j$ and for every $\sigma \in \Delta$. We have

$$\sum_{\sigma \in \Delta} z\sigma(\omega_j^*) \sum_i \sigma(\omega_i)m_i = 0, \quad \text{for all } j.$$
Therefore
\[ \sum_i z(\sum_{\sigma \in \Delta} \sigma(\omega^*_i)\sigma(\omega_i))m_i = 0, \quad \text{for all } j. \]

It follows that \( zm_i = 0 \) for every \( i \) and hence \( zx = 0 \). This implies that \( \delta_F \) annihilates \( x \), as required.

To prove that the cokernel of \( \phi \) is also killed by \( \delta_F \), let \( m \in M \). Then \( \sum_{\sigma \in \Delta} \sigma(\omega_i m) \) is \( \Delta \)-invariant for every \( i \) and hence is in \( \text{im} \phi = M^\Delta O_F \). For all \( z \in \delta_F \) and every \( \tau \in \Delta \) the elements
\[ \sum_{\sigma \in \Delta} \sum_i z\tau(\omega^*_i)\sigma(\omega_i)\sigma(m), \quad (**) \]
are in \( M^\Delta O_F \). Since the matrices \( \sigma(\omega_i) \) and \( \sigma(\omega^*_i) \) are inverse to one another, we have that \( \sum_i \tau(\omega^*_i)\sigma(\omega_i) = 1 \) when \( \sigma = \tau \) and zero otherwise. Therefore the expression \( (**) \) is equal to \( z\tau(m) \) for each \( \tau \). In particular \( zm \) is in the image of \( \phi \). It follows that \( \delta_F \) kills the cokernel of \( \phi \), as required.

For a prime \( p \) the different \( \delta_F \) of \( F = \mathbb{Q}(\zeta_p) \) is equal to \( (\zeta_p - 1)^{p-2} \). Therefore \( \delta_F \) is a divisor of \( p \). It follows that for a finite \( O_F \)-module of order prime to \( p \), multiplication by \( \delta_F \) is an isomorphism and hence the map \( M^\Delta \otimes_{\mathbb{Z}O_F} \rightarrow M \) is an isomorphism. This easily implies Corollary 2.2.

Proposition 2.3 is in some sense best possible. Indeed, consider \( F = \mathbb{Q}(\zeta_p) \) and \( A = \mathbb{Z}[\zeta_p] = O_F \) and \( M = \mathbb{Z}[\zeta_p]/(\zeta_p - 1) = \mathbb{Z}/(p) \) with trivial \( \Delta \)-action. Then \( M^\Delta = M \) and \( M \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_p] = \mathbb{Z}[\zeta_p]/(p) \). In this case the kernel of \( \phi \) is isomorphic to \( (\zeta_p - 1)/(p) \) \( \cong \mathbb{Z}[\zeta_p]/\delta_F \). On the other hand, let \( M = (\zeta_p - 1)/(p) \). In this case there are no \( \Delta \)-invariant elements, so that the cokernel of \( \phi \) is \( M = (\zeta_p - 1)/(p) \).

3. The \( p \)-part.

For any prime \( p \geq 3 \) let \( \mathbb{Z}_p \) denote the ring of \( p \)-adic integers and put \( A = \mathbb{Z}_p[\zeta_p] \). In the notation of section 1, the \( p \)-part of the kernel of the norm map \( Cl_K \rightarrow Cl_K \) is a module over the twisted group ring \( A[\Delta]' \) as defined in section 1. In other words, it is a module over the discrete valuation ring \( A \) and it comes equipped with a semilinear \( \Delta \)-action.

In this section we study this type of modules. They form an abelian category. Since the natural action of \( \Delta \) on \( A \) is semilinear, the ring \( A \) is itself an example. So are its ideals and quotients. The ideals are of the form \( \pi^iA \)
for \( i \geq 0 \). Here \( \pi \) denotes a \( p-1 \)-th root of \(-p\) in \( A \). It is easy to see that \( \pi \) is equal to \( \zeta_{p} - 1 \) times a unit, so that \( \pi \) generates the maximal ideal of \( A \). For any \( \sigma \in \Delta \) we have \( \sigma(\pi) = \omega(\sigma)\pi \). The residue field \( A/\pi A \) is isomorphic to \( \mathbb{F}_{p} \) with trivial \( \Delta \)-action.

For every character \( \chi : \Delta \rightarrow \mathbb{Z}_{p}^{*} \) and every \( A[\Delta]' \)-module \( M \), we write \( M(\chi) \) for the \( \chi \)-twist of \( M \). This is also an \( A[\Delta]' \)-module. As an \( A \)-module it is just \( M \), but the \( \Delta \)-action is twisted by \( \chi \) on \( M(\chi) \) multiplying \( m \in M(\chi) \) by \( \sigma \in \Delta \) gives \( \chi(\sigma)\sigma m \), where \( \sigma m \) denotes the product of \( m \) by \( \sigma \) in the untwisted module \( M \). The map \( A(\omega^{i}) \rightarrow \pi^{i}A \) given by \( \lambda \mapsto \lambda\pi^{i} \) is an \( A[\Delta]' \)-linear isomorphism.

For every character \( \chi : \Delta \rightarrow \mathbb{Z}_{p}^{*} \) and every \( A[\Delta]' \)-module \( M \), we define its \( \chi \)-eigenspace by

\[
M_{\chi} = \{ x \in M : \sigma(x) = \chi(\sigma)x \text{ for all } \sigma \in \Delta \}.
\]

This is a \( \mathbb{Z}_{p} \)-submodule of \( M \). It is, in general, not an \( A \)-module. The natural map

\[
\bigoplus_{\chi} M_{\chi} \rightarrow M,
\]

is an isomorphism. For \( \chi = 1 \) we recover the subgroup of \( \Delta \)-invariants \( M_{1} = M^{\Delta} \). We have that \( M(\chi)^{\Delta} = M_{\chi^{-1}} \).

If \( M \) is killed by \( \pi \), then \( M \) is a module over the ring \( A[\Delta]'/\pi A[\Delta]' \cong \mathbb{F}_{p}[\Delta] \). So, the semilinear \( \Delta \)-action on \( M \) is actually linear. As an \( A[\Delta]' \)-module, \( \mathbb{F}_{p}[\Delta] \) is a product of modules of the form \( \mathbb{F}_{p}(\chi) \), one for each character \( \chi \) of \( \Delta \). Every module \( M \) that is killed by \( \pi \) is therefore a product of various copies of \( \mathbb{F}_{p}(\chi) \).

Every \( A[\Delta]' \)-module admits a filtration with submodules

\[
M \supset \pi M \supset \pi^{2}M \supset \pi^{3}M \supset \ldots
\]

The successive subquotients are killed by \( \pi \) and hence are isomorphic to products of copies of \( \mathbb{F}_{p}(\chi) \) for certain characters \( \chi \) of \( \Delta \). For the ring \( A \) itself we have

\[
A \supset \pi A \supset \pi^{2}A \supset \pi^{3}A \supset \ldots
\]

with successive subquotients (from left to right) isomorphic to \( \mathbb{F}_{p} \), \( \mathbb{F}_{p}(\omega) \), \( \mathbb{F}_{p}(\omega^{2}) \), \ldots. When \( i < j \) we have for \( \pi^{i}A/\pi^{j}A \) the filtration

\[
\pi^{i}A/\pi^{j}A \supset \pi^{i+1}A/\pi^{j}A \supset \pi^{i+2}A/\pi^{j}A \supset \ldots \supset \pi^{j-1}A/\pi^{j}A \supset 0
\]
with successive subquotients isomorphic to $F_p(\omega^i), F_p(\omega^{i+1}), \ldots, F_p(\omega^{j-1})$.

The next result describes the structure of finite $A[\Delta]'$-modules that are generated by $\Delta$-invariant elements.

**Proposition 3.1.** Let $M$ be a finite $A[\Delta]'$-module. Then $\Delta$ acts trivially on the quotient $M/\pi M$ if and only if there is an $A[\Delta]'$-isomorphism

$$M \cong \bigoplus_{i=1}^t A/\pi^{n_i} A, \quad \text{for certain integers } n_i \geq 1.$$  

**Proof.** For any module $M$ of this type, the quotient $M/\pi M$ is isomorphic to a product of copies of $A/\pi A = F_p$ with trivial $\Delta$-action. Conversely, suppose that $M/\pi M$ has trivial $\Delta$-action. Since the order of $\Delta$ is prime to $p$, the map $M^\Delta \rightarrow (M/\pi M)^\Delta = M/\pi M$ is surjective. This implies that $M$ can be generated over $A$ by $\Delta$-invariant elements $v_1, \ldots, v_t$ say. In other words, the $A$-homomorphism $A^t \rightarrow M$ that maps the $i$-th basis vector to $v_i$ is a well defined surjective $A[\Delta]'$-homomorphism. Since $M$ is finite, it induces a surjective $A[\Delta]'$-homomorphism of the form

$$\phi : \bigoplus_{i=1}^t A/\pi^{n_i} A \rightarrow M,$$

for certain $n_i \geq 1$. If $\phi$ is also injective, we are done. If not, $\ker \phi$ contains a non-zero element $x$ that is killed by $\pi$ on which $\Delta$ acts via some character $\chi = \omega^m$. So $x$ generates an $A[\Delta]'$-module isomorphic to $F_p(\chi)$. We have $x = (\lambda_1 (\mod \pi^{n_1}), \ldots, \lambda_t (\mod \pi^{n_t}))$ for certain $\lambda_i \in A$ for which $\lambda_i \equiv 0 (\mod \pi^{n_i-1})$ for each $i$ and for which $\sum_{i=1}^t \lambda_i v_i = 0$ in $M$.

Since $\pi^{n_i-1}/\pi^{n_i} A \cong F_p(\omega^{n_i-1})$, the coordinates $\lambda_i$ must be congruent to 0 (mod $\pi^{n_i}$) for the indices $i$ for which $n_i - 1 \not\equiv m (\mod p-1)$. Let $I$ denote the set of indices for which $n_i - 1 \equiv m (\mod p-1)$. For $i \in I$ we define $k_i$ by $n_i - 1 = m + k_i (p-1)$. For at least one index $i \in I$ we have $\lambda_i \not\equiv 0 (\mod \pi^{n_i})$. Without loss of generality we may assume that this happens for $i = 1$ and that moreover $n_1$ and hence $k_1$ is minimal. For $i \in I$ we define $\mu_i \in A$ by

$$\lambda_i = \pi^m p^{k_i} \mu_i.$$  

We let $m_i \in \mathbb{Z}$ such that $\mu_i \equiv m_i (\mod \pi)$. Note that $\mu_i$ and hence $m_i$ are invertible in $A$.

From $\phi$ we construct now a second $R$-homomorphism $\phi'$

$$\phi' : (A/\pi^{n_1-1} A) \oplus \bigoplus_{i=2}^t A/\pi^{n_i} A \rightarrow M,$$  

(*)
by mapping the first basis vector $e_1 = (1, 0, 0, \ldots)$ to $\sum_{i=1}^t m_i p^{k_i-1} v_i$, mapping the basis vectors $e_i$ to $\phi(e_i)$ when $i \geq 2$ and extend $A$-linearly. In this way $\phi'(e_i) \in M^A$ for every $i$. Since $\phi$ is surjective and $m_1$ is invertible in $\mathbb{Z}_p$, the morphism $\phi'$ is also surjective. We only need to check that it is well defined. This means that $\phi'$ should map $p^{k_1} \pi^m e_1$ to zero. We have
\[
\phi'(p^{k_1} \pi^m e_1) = \sum_i m_i p^{k_i} \pi^m v_i = \sum_i \mu_i p^{k_i} \pi^m v_i = \sum_i \lambda_i v_i = 0.
\]
Note that the left hand side module in (*) is strictly smaller than the one we started with. Therefore, by repeating this process, we eventually end up with an isomorphism.

This proves the proposition.

**Proposition 3.2.** Let $M$ be a finite $A[\Delta]'$-module that is generated by $\Delta$-invariant elements. Let $d_i = \dim M[\pi]_{\omega^{i-1}}$ for $1 \leq i \leq p-2$. Then there is a finite abelian $p$-group $H$ and an exact sequence of $A[\Delta]'$-modules
\[
0 \longrightarrow \bigoplus_{i=1}^{p-2} (A/\pi^i A)^{d_i} \longrightarrow M \longrightarrow H \otimes_{\mathbb{Z}_p} A \longrightarrow 0.
\]

**Proof.** Suppose that $M$ is of the form $A/\pi^n A$ for some $n \geq 0$ Then there are integers $m \geq 0$ and $i \in \{0, 1, \ldots, p-2\}$ for which $n = (p-1)m+i$. Since $p = \pi^{p-1}$ times a unit, we get an exact sequence
\[
0 \longrightarrow A/\pi^i A \longrightarrow M \longrightarrow A/p^m A \longrightarrow 0.
\]
Putting $H = \mathbb{Z}/p^m\mathbb{Z}$, we have $A/p^m A = H \otimes_{\mathbb{Z}_p} A$. We put $V = A/\pi^i A$. Then $V = 0$ for $i = 0$. For $1 \leq i \leq p-2$, the submodule $M[\pi]$ is the same as the $\pi$-torsion submodule of $V$, which is isomorphic to $\mathbb{F}_p(\omega^{j-1})$. So $d_i = 1$, while $d_j = 0$ for $j \in \{1, \ldots, p-2\}$ different from $i$.

This takes care of $M = A/\pi^n A$. By Proposition 3.1, an arbitrary module $M$ generated by $\Delta$-invariant elements is a direct sum of modules of the form $A/\pi^n A$. Since the statement of the proposition is additive in $M$, the proposition is also proved for general modules $M$.

The $A[\Delta]'$-module $\bigoplus_{i=1}^{p-2} (A/\pi^i A)^{d_i}$ of Proposition 3.2 is killed by $\pi^{p-2}$ and hence by $p$. Its $\mathbb{F}_p$-dimension is $\sum_{i=1}^{p-2} id_i$. 

4. Class field theory.

As in the introduction, \( p > 2 \) is a prime and \( \zeta_p \) is a primitive \( p \)-th root of unity. Let \( n \in \mathbb{Z} \) not be a \( p \)-th power and let \( K = \mathbb{Q}(\zeta_p, \sqrt[p]{n}) \). Let \( G \) denote the Galois group of \( K \) over \( \mathbb{Q}(\zeta_p) \), let \( \Omega = \text{Gal}(K/\mathbb{Q}) \) and let \( \Delta = \text{Gal}(K/\mathbb{Q}(\sqrt[p]{n})) \approx \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \).

In this section we study the Tate \( G \)-cohomology groups of the class group of \( K \). The class group of \( K \) is a \( \mathbb{Z}[\Omega] \)-module, and Tate \( G \)-cohomology groups of \( \mathbb{Z}[\Omega] \)-modules are \( \mathbb{F}_p[\Delta] \)-modules. This follows from the fact that Tate \( G \)-cohomology groups are killed by \( p \) and are \( G \)-invariant. Since \( G \) is cyclic, its Tate cohomology groups are periodic with period 2. The isomorphism, given by cupping with a generator of \( H^2(G, \mathbb{Z}) \), is not \( \Delta \)-equivariant. Indeed, \( \hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \) has trivial \( \Delta \)-action, while \( H^2(G, \mathbb{Z}) = G^{\text{dual}} \) has \( \Delta \)-action via \( \omega^{-1} \). For \( q \in \mathbb{Z} \) and an arbitrary \( \Omega \)-module \( M \) the maps

\[
\hat{H}^q(G, M) \longrightarrow \hat{H}^{q+2}(G, M)(\omega),
\]
given by cupping with a generator of \( H^2(G, \mathbb{Z}) \), are \( \mathbb{F}_p[\Delta] \)-isomorphisms.

For future reference we recall a property of the cohomology groups of \( \mathbb{Z}[\Omega] \)-modules \( M \).

**Lemma 4.1.** Let \( M \) be a \( \mathbb{Z}[\Omega] \)-module and let \( q \geq 1 \). Then the inflation-restriction sequences

\[
0 \longrightarrow H^q(\Delta, M^G) \longrightarrow H^q(\Omega, M) \longrightarrow H^q(G, M)^\Delta \longrightarrow 0
\]

are exact.

**Proof.** Since the orders of \( \Delta \) and \( G \) are coprime, the \( E_2 \)-terms of the Hochschild-Serre spectral sequence [2, Ch.XVI] off the axes are zero. This implies the lemma.

By \( O_K \) we denote the ring of integers of \( K \) and by \( O_K^* \) its group of units. By \( U_K \) we denote the idele unit group and by \( C_K \) the idele class group of \( K \). See [3] for the basic properties of the Galois cohomology groups of these \( \mathbb{Z}[\Omega] \)-modules. There is a natural exact sequence

\[
0 \longrightarrow O_K^* \longrightarrow U_K \longrightarrow C_K \longrightarrow Cl_K \longrightarrow 0.
\]

We use the same notation with \( K \) replaced by \( \mathbb{Q}(\zeta_p) \). In order to get information on the \( \mathbb{F}_p[\Delta] \)-structure of the \( G \)-cohomology groups of \( Cl_K \), we determine the \( \Delta \)-action on the \( G \)-cohomology groups of \( U_K \) and, for completeness, also of \( C_K \).
Lemma 4.2. The cohomology groups \( \hat{H}^q(G, C_K) \) are trivial when \( q \) is odd and isomorphic to \( F_p \) if \( q \) is even. In the latter case, \( \Delta \) acts on \( \hat{H}^q(G, C_K) \) through the character \( \omega^{1-q/2} \).

Proof. The first statement follows from global class field theory. See [3, VII, Thms 8.3 and 9.1] To prove the second, it suffices to show that \( \Delta \) acts trivially on \( H^2(G, C_K) \). By global class field theory the groups \( H^2(\Omega, C_K) \), \( H^2(G, C_K) \) and \( H^2(\Delta, C_{Q(\zeta_p)}) \) are isomorphic to the groups \( \hat{H}^0(\Omega, Z) \), \( \hat{H}^0(G, Z) \) and \( \hat{H}^0(\Delta, Z) \), and hence are cyclic of orders \( p(p-1) \), \( p \) and \( p-1 \) respectively.

By Lemma 4.1 with \( M = C_K \), the sequence

\[
0 \longrightarrow H^2(\Delta, C_{Q(\zeta_p)}) \longrightarrow H^2(\Omega, C_K) \longrightarrow H^2(G, C_K)^\Delta \longrightarrow 0
\]

is exact. It follows that \( H^2(G, C_K) = H^2(G, C_K)^\Delta \) as required.

Lemma 4.3. The cohomology groups \( \hat{H}^q(G, U_K) \) are isomorphic to twists of the \( \Delta \)-module

\[
\bigoplus_{l \text{ ram in } K} Z/pZ[\Delta/\Delta_l].
\]

Here the sum runs over primes \( l \) for which the primes \( v \) lying over \( l \) in \( Q(\zeta_p) \) are ramified in \( K \) and \( \Delta_l \subset \Delta \) denotes the decomposition subgroup of \( v \). The \( \Delta \)-action on \( H^1(G, U_K) \) and \( H^2(G, U_K) \) is the natural action on the various summands \( Z/pZ[\Delta/\Delta_l] \). The \( \Delta \)-action on \( \hat{H}^q(G, U_K) \) is twisted by \( \omega^{1-q/2} \) if \( q \) is even and by \( \omega^{(1-q)/2} \) if \( q \) is odd.

Proof. For a prime number \( l \), let \( v \) denote a prime of \( Q(\zeta_p) \) lying over \( l \) and let \( w \) be a prime of \( K \) lying over \( v \). Let \( \Omega_w \subset \Omega \) denote the decomposition group of \( w \). Let \( \Delta_l \subset \Delta \) denote the decomposition group of \( v \). It only depends on \( l \). Let \( G_v \subset G \) denote the decomposition group of \( w \). It only depends on \( v \). There is an exact sequence

\[
1 \longrightarrow G_v \longrightarrow \Omega_w \longrightarrow \Delta_l \longrightarrow 1.
\]

By Shapiro’s Lemma, for every \( q \in Z \), the cohomology group \( \hat{H}^q(G, U_K) \) is isomorphic to

\[
\bigoplus_{l \text{ ram in } K} \bigoplus_{v|l} \hat{H}^q(\Omega_w, O_w^*).
\]

Each summand \( \hat{H}^q(\Omega_w, O_w^*) \) is naturally an \( F_p[\Delta_l] \)-module and we have isomorphisms

\[
\bigoplus_{v|l} \hat{H}^q(\Omega_w, O_w^*) \cong \text{Ind}^{\Delta_l}_{\Delta_v} \hat{H}^q(\Omega_w, O_w^*).
\]
of $F_p[\Delta]$-modules. By periodicity of the cohomology of $G$, it suffices to compute $H^1(G, U_K)$ and $H^2(G, U_K)$ and determine the $\Delta$-action.

First we show for $q = 1$ and 2, that the action of $\Delta$ on $\hat{H}^q(G_v, O^*_v)$ is trivial. By Hilbert 90, the orders of the cohomology groups $H^1(\Delta_l, O^*_v)$, $H^1(\Omega_v, O^*_w)$ and $H^1(G_v, O^*_w)$ are equal to the ramification indices of $v$ over $l$, of $w$ over $l$ and of $w$ over $v$ respectively. It follows that $\#H^1(\Omega_v, O^*_w)$ is equal to the product of the cardinalities of the groups $H^1(\Delta_l, O^*_v)$ and $H^1(G_v, O^*_w)$.

The exactness of the sequence of Lemma 4.2

$$0 \rightarrow H^1(\Delta_l, O^*_v) \rightarrow H^1(\Omega_v, O^*_w) \rightarrow H^1(G_v, O^*_w) \Delta_l \rightarrow 0,$$

shows then that $H^1(G_v, O^*_w)$ is $\Delta_l$-invariant. So $\Delta$ permutes the summands of $H^1(G, U_K)$. Since $H^1(G_v, O^*_w) = \mathbb{Z}/p\mathbb{Z}$ for each prime $v$ of $Q(\zeta_p)$ that is ramified in $K$, we find that

$$H^1(G, U_K) = \bigoplus_{l \text{ ram in } K} \mathbb{Z}/p\mathbb{Z}[\Delta/\Delta_l],$$

as required.

For $q = 2$ we consider the exact sequence of Lemma 4.2 for $M = K^*_w$:

$$0 \rightarrow H^2(\Delta_l, O^*_v) \rightarrow H^2(\Omega_v, K^*_w) \rightarrow H^2(G_v, K^*_w) \Delta_l \rightarrow 0.$$  

By local class field theory, the cohomology groups $H^2(\Delta_l, Q(\zeta_p)_v^*)$, $H^2(\Omega_v, K^*_w)$ and $H^2(G_v, K^*_w)$ have orders equal to the cardinality of $\Delta_l$, $\Omega_v$ and $G_v$ respectively. The exactness of the sequence then shows that $H^2(G_v, K^*_w)$ is $\Delta_l$-invariant. Since the natural map $H^2(G_v, O^*_w) \rightarrow H^2(G_v, K^*_w)$ is injective, the same is true for $H^2(G_v, O^*_w)$.

Since $H^2(G_v, O^*_w)$ is isomorphic to the order $p$ group $\hat{H}^0(G_v, O^*_w)$, we find as in the previous case an isomorphism of $\Delta$-modules

$$H^2(G, U_K) = \bigoplus_{l \text{ ram in } K} \mathbb{Z}/p\mathbb{Z}[\Delta/\Delta_l],$$

with the required $\Delta$-action. This proves the lemma.

We now turn to the class group $Cl_K$. It is convenient to put $Q_K = U_K/O^*_K$, so that we have short exact sequences

$$0 \rightarrow O^*_K \rightarrow U_K \rightarrow Q_K \rightarrow 0,$$

$$0 \rightarrow Q_K \rightarrow C_K \rightarrow Cl_K \rightarrow 0,$$

11
and the long exact sequences of $G$-cohomology groups associated to them. We make the assumption that $p$ is regular, i.e. that $p$ does not divide the class number of $\mathbb{Q}(\zeta_p)$. This implies that the cokernel of the natural map $U_{\mathbb{Q}(\zeta_p)} \to C_{\mathbb{Q}(\zeta_p)}$ has order prime to $p$, so that $\hat{H}^0(G, U_K) \to \hat{H}^0(G, C_K)$ is surjective. It follows that the map $\hat{H}^0(G, Q_K) \to \hat{H}^0(G, C_K)$ is also surjective. An application of the snake lemma to the commutative diagram

\[
\begin{array}{cccccc}
0 & \to & Q_{\mathbb{Q}(\zeta_p)} & \to & C_{\mathbb{Q}(\zeta_p)} & \to & C^l_{\mathbb{Q}(\zeta_p)} & \to & 0 \\
& & \downarrow & \approx & \downarrow & & \end{array}
\]

shows that the natural map $Q_{\mathbb{Q}(\zeta_p)} \to Q^G_K$ is an isomorphism. This implies that the map $U_{\mathbb{Q}(\zeta_p)} \to Q^G_K$ is surjective, so that $\hat{H}^0(G, U_K) \to \hat{H}^0(G, Q_K)$ is also surjective. Finally, by class field theory we have $H^1(G, C_K) = 0$. This leads to the following diagram with exact rows and columns.

\[
\begin{array}{cccccc}
\hat{H}^0(G, O_K^*) & \to & \hat{H}^0(G, U_K) & \to & H^1(G, O_K^*) & \to & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
\hat{H}^0(G, U_K) & \to & H^1(G, U_K) & \to & H^1(G, Q_K) & \to & 0 \\
\downarrow & & \downarrow & \approx & \downarrow & & \\
\hat{H}^0(G, O_K^*) & \to & \hat{H}^0(G, Cl_K) & \to & \hat{H}^0(G, Q_K) & \to & \hat{H}^0(G, C_K) & \to & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
H^1(G, O_K^*) & \to & H^1(G, U_K) & \to & H^1(G, Q_K) & \to & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
H^2(G, O_K^*) & \to & H^2(G, U_K) & \to & H^2(G, Q_K) & \to & \\
\downarrow & & \downarrow & & \\
H^2(G, O_K^*) & \to & H^2(G, U_K) & \to & \\
\end{array}
\]

The $G$-cohomology groups are $\mathbf{F}_p[\Delta]$-modules and all maps, including the
connecting homomorphisms, are $\Delta$-linear. Since this last fact plays an important role, we explain why this is so. A complete $\Omega$-resolution $P_\bullet = \{P_i\}_{i \in \mathbb{Z}}$ as in [3, IV.6] is also a complete $G$-resolution. For any $\Omega$-module $M$ and any $i \in \mathbb{Z}$, the groups $\text{Hom}_G(P_i, M)$ are naturally objects of the abelian category of $\Delta$-modules. The cohomology groups of the complex $X^\bullet(M) = \text{Hom}_G(P_\bullet, M)$ are the usual Tate $G$-cohomology groups. The long exact sequence of cohomology groups associated to the exact sequence of complexes $0 \to X^\bullet(A) \to X^\bullet(B) \to X^\bullet(C) \to 0$ is a sequence of morphisms in the category of $\Delta$-modules.

**Theorem 4.4.** Let $M$ denote the $p$-part of the class group of $K$. Suppose that $p$ is a regular prime and that all primes $l \neq p$ that ramify in $K$ are primitive roots modulo $p$. Then

(i) the group $\Delta$ acts via $\omega$ on $M/\pi M$;

(ii) for every non-trivial character $\chi$ of $\Delta$ the $F_p$-dimension of $M[\pi]_\chi$ is at most 1. Moreover, if $\chi$ is a non-trivial even character or $\chi = \omega^{-1}$, then $M[\pi]_\chi$ vanishes.

**Proof.** For $l = p$ we always have that $\Delta_p = \Delta$. The assumption on the primes $l$ means that $\Delta_l = \Delta$ for the ramified primes $l \neq p$ as well. Lemma 4.3 implies therefore that both $H^1(G, U_K)$ and $H^2(G, U_K)$ are isomorphic to

$$\bigoplus_{l \text{ ram in } K} \mathbb{Z}/p \mathbb{Z},$$

equipped with trivial $\Delta$-action. Therefore $\Delta$ acts via $\omega$ on $\hat{H}^0(G, U_K)$. It follows from the diagram that the $\Delta$-module $\hat{H}^{-1}(G, Cl_K)$ is a subquotient of $\hat{H}^0(G, U_K)$, so that $\Delta$ acts also via $\omega$ on $\hat{H}^{-1}(G, Cl_K)$.

On the other hand, the diagram shows that the $\Delta$-module $\hat{H}^0(G, Cl_K)$ sits in an exact sequence

$$H^1(G, U_K) \to \hat{H}^0(G, Cl_K) \to H^2(G, O_K^*).$$

The group $\Delta$ acts trivially on $H^1(G, U_K)$. Therefore the $\chi$-eigenspace of $\hat{H}^0(G, Cl_K)$ is contained in the one of $H^2(G, O_K^*)$ when $\chi$ is non-trivial. The $\Delta$-module $H^2(G, O_K^*)$ is isomorphic to $\hat{H}^0(G, O_K^*)(\omega^{-1})$ and is hence a quotient of $(\mathbb{Z}[\zeta_p]^*/\mathbb{Z}[\zeta_p]^*\mathbb{F}_p)(\omega^{-1})$. By an equivariant version [7, Prop.13.7] of Dirichlet’s Unit Theorem, $\mathbb{Z}[\zeta_p]^*/\mathbb{Z}[\zeta_p]^*\mathbb{F}_p$ is a product of copies of $\mathbb{F}_p(\chi)$, one for each non-trivial even character $\chi$ and one copy of $\mathbb{F}_p(\omega)$.
Since $p$ is regular, $M$ is killed by the $G$-norm $N_G$, so that it is a $\mathbb{Z}_p[\Delta]'$-module. Recalling the fact that a $G$-module that is killed by $N_G$ is invariant, if and only if it is killed by a generator of the maximal ideal of $\mathbb{Z}_p[\zeta_p] = \mathbb{Z}_p[G]/(\text{Tr}_G)$, we find that $M/\pi M = \hat{H}^{-1}(G, Cl_K)$ and $M[\pi] = \hat{H}^0(G, Cl_K)$.

This implies the theorem.

**Proof of Proposition 1.2.** Corollary 2.2 takes care of the prime to $p$-part of $Cl_K$. We now consider the $p$-part. Since the statement does not regard the $\Delta$-structure, we may twist the $p$-part $M$ of the class group of $K$ by the character $\omega^{-1}$. We denote the result by $M'$. By Theorem 4.4, the group $\Delta$ acts trivially on $M'/\pi M'$, so that the $A$-module $M'$ is generated by $\Delta$-invariant elements. By Proposition 3.2 there is an exact sequence

$$0 \longrightarrow \bigoplus_{i=1}^{p-2} (A/\pi^i A)^{d_i} \longrightarrow M' \longrightarrow H \otimes_{\mathbb{Z}_p} A \longrightarrow 0$$

where $d_i = \dim M'[\pi](\omega^{i-1}) = \dim M[\pi](\omega^i)$ for $1 \leq i \leq p - 2$. Theorem 4.4 implies that $d_i = 0$ when $i$ is even, while $d_i \leq 1$ when $i$ is odd but not $p - 2$.

It follows that

$$\dim \bigoplus_{i=1}^{p-2} (A/\pi^i A)^{d_i} = \sum_{i=1}^{p-2} id_i \leq \sum_{i=1, \text{odd}}^{p-4} i = \left(\frac{p-3}{2}\right)^2,$$

as required.

5. **Appendix**

In this appendix we present our original proof of Proposition 1.1. Let $S_3$ denote the symmetric group on three letters. Let $\sigma \in S_3$ of order 2 and let $\rho \in S_3$ of order 3. For any $\mathbb{Z}[S_3]$-module, let $M^- = \{x \in M : \sigma x = -x\}$ and write $M[\rho - 1]$ for $\{x \in M : \rho x = x\}$.

**Lemma 5.1.** Let $M$ be a finite $\mathbb{Z}[S_3]$-module of odd order. Suppose that one of the following holds:

(a) $3$ does not divide $\# M$ and $\rho^2 + \rho + 1$ kills $M$.

(b) $\# M$ is odd and $\sigma$ acts trivially on $M[\rho - 1]$ and as $-1$ on $M/(\rho - 1)M$.

Then the homomorphism

$$f : M^- \times M^- \longrightarrow M$$

given by $f(x, y) = x - \rho y$ is bijective.
Proof. Suppose that \( x, y \in M^- \) and \( (x, y) \in \ker f \). Then we have \( x = \rho y \) and hence \( y = -\sigma y = -\rho \sigma \rho y = -\rho \sigma x = \rho x = \rho^2 y \). Since \( \rho \) has order 3, it follows that \( \rho - 1 \) kills \( y \) and hence \( x \). It follows that \( \ker f \subset M[\rho - 1] \).

Similarly, let \( m \in M \). Then \( (\sigma - 1)m \) and \( (\sigma - 1)\rho m \) are in \( M^- \). We have

\[
f((\sigma - 1)m, (\sigma - 1)\rho m) = (\sigma - 1 - \rho(\sigma - 1)\rho)m = (-1 + \rho^2)m.
\]

This means that \( (\rho - 1)M \) is contained in the image of \( f \). So there is a natural surjective homomorphism \( M/(\rho - 1)M \to \cok f \).

In case (a) we observe that since \( \rho^2 + \rho + 1 = 0 \), both \( M[\rho - 1] \) and \( M/(\rho - 1)M \) are killed by 3. Since 3 does not divide \#\( M \), both groups are trivial and hence so are \( \ker f \) and \( \cok f \).

For (b) we note that by assumption \( \sigma \) acts trivially on \( M[\rho - 1] \) and hence on \( \ker f \). Since \( \sigma \) acts as \(-1\) on \( M^- \) and since \#\( M \) is odd, it follows that \( \ker f = 0 \). For the surjectivity, we note that by assumption \( \sigma \) acts as \(-1\) on \( M/(\rho - 1)M \) and hence on \( \cok f \). On the other hand, \( M^- \) is in the image of \( f \), so that \( \sigma \) acts trivially on \( \cok f \). We conclude that \( \cok f \) is trivial.

This proves the lemma.

If \( n \in \mathbb{Z} \) is not a cube, the Galois group of \( \mathbb{Q}(\zeta_3, \sqrt[3]{n}) \) is isomorphic to \( S_3 \).

An application of part (a) of the lemma to \( M = \Cl_K \) proves Corollary 2.2 for the non-3-part of \( \Cl_K \). Part (b) takes care of the 3-part. To see this, we must check the conditions that \( \sigma \) acts trivially on \( \check{H}^0(G, \Cl_K) = M[\rho] \) and acts as \(-1\) on \( M/(\rho - 1)M = \check{H}^{-1}(G, \Cl_K) \). Since \( n \) is not divisible by any primes congruent to 1 (mod 3), this follows from Theorem 4.4.

Bibliography.


