Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

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

René Schoof

Dipartimento di Matematica, Università di Roma "Tor Vergata", I-00133 Roma, Italy

A R T I C L E I N F O

Article history:
Received 29 November 2019
Received in revised form 9 April 2020
Accepted 10 April 2020
Available online xxxx
Communicated by A. Pal

Keywords:
Algebraic number fields
Class groups
Galois cohomology
Class field theory

A B S T R A C T

For a prime number p and an integer n we determine the Galois cohomology groups of the class group of the normal closure of $\mathbf{Q}(\sqrt[p]{n})$ 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 ζ_m denote a primitive m-th root of unity. In 1971, Taira Honda [5] proved that the class number of $\mathbf{Q}(\zeta_3, \sqrt[3]{n})$ is equal to h^2 or $3h^2$, where h is the class number of $\mathbf{Q}(\sqrt[3]{n})$. 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.

E-mail address: schoof.rene@gmail.com.

https://doi.org/10.1016/j.jnt.2020.04.004

Please cite this article in press as: R. Schoof, On the ideal class group of the normal closure of $\mathbf{Q}(\sqrt[p]{n})$, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2020.04.004

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

In this note we put the statement of Proposition 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 $\mathbf{Q}(\zeta_p, \sqrt[p]{n})$ 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 assumption that p is a *regular* prime, i.e. that p does not divide the class number of $\mathbf{Q}(\zeta_p)$. 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 $n \in \mathbf{Z}$ 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 $\mathbf{Q}(\zeta_p, \sqrt[p]{n})$ to the class group of $\mathbf{Q}(\zeta_p)$ sits in an exact sequence*

$$0 \longrightarrow V \longrightarrow Cl^0 \longrightarrow \underbrace{H \times H \times \ldots \times H}_{p-1 \text{ times}} \longrightarrow 0,$$

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

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

$$K = \mathbf{Q}(\zeta_p, \sqrt[p]{n}),$$

where $n \in \mathbf{Z}$ is not a p-th power. We have inclusions

$$\mathbf{Q} \subset \mathbf{Q}(\zeta_p) \subset K.$$

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

$$1 \longrightarrow G \longrightarrow \Omega \longrightarrow \Delta \longrightarrow 1.$$

Please cite this article in press as: R. Schoof, On the ideal class group of the normal closure of $\mathbf{Q}(\sqrt[p]{n})$, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2020.04.004

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

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

Here $\omega : \Delta \longrightarrow (\mathbf{Z}/p\mathbf{Z})^*$ 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 $\mathbf{Z}[\Omega]$-module. The G-norm map $N_G : Cl_K \longrightarrow Cl_K$ factors through the class group of $\mathbf{Q}(\zeta_p)$:

$$\begin{array}{ccccc} Cl_K & & \xrightarrow{N_G} & & Cl_K \\ & \searrow & & \nearrow & \\ & & Cl_{\mathbf{Q}(\zeta_p)} & & \end{array}$$

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

$$0 \longrightarrow \ker N_G \longrightarrow Cl_K \longrightarrow Cl_{\mathbf{Q}(\zeta_p)} \longrightarrow 0$$

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 $R = \mathbf{Z}[\Omega]/(\mathrm{Tr}_G)$, where Tr_G denotes the central element $\sum_{g\in G}[g]$ of $\mathbf{Z}[\Omega]$. Since we have $\mathbf{Z}[G]/(\mathrm{Tr}_G) \cong \mathbf{Z}[\zeta_p]$, the ring R is isomorphic to the *twisted group ring* $\mathbf{Z}[\zeta_p][\Delta]'$. Multiplication in this ring satisfies $[\sigma]\lambda = \sigma(\lambda)[\sigma]$ for $\lambda \in \mathbf{Z}[\zeta_p]$ and $\sigma \in \Delta$. A module over $\mathbf{Z}[\zeta_p][\Delta]'$ can alternatively be viewed as a module over $\mathbf{Z}[\zeta_p]$, equipped with a *semilinear* action of Δ.

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 $\mathbf{Z}[\zeta_p, \frac{1}{p}][\Delta]'$. Alternatively, it is a $\mathbf{Z}[\zeta_p, \frac{1}{p}]$-module equipped with semilinear left Δ-action. The category of such modules is *Morita equivalent* to the category of modules over $\mathbf{Z}[\zeta_p, \frac{1}{p}]$. 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 Δ. Then the ring R and the twisted group ring $S[\Delta]'$ are Morita equivalent. In other words, the functors R-$\underline{\mathrm{Mod}} \longrightarrow S[\Delta]'$-$\underline{\mathrm{Mod}}$ given by $M \mapsto M \otimes_R S$ and $S[\Delta]'$-$\underline{\mathrm{Mod}} \longrightarrow R$-$\underline{\mathrm{Mod}}$ given by $N \mapsto N^\Delta$, induce an equivalence of categories.*

Please cite this article in press as: R. Schoof, On the ideal class group of the normal closure of $\mathbf{Q}(\sqrt[p]{n})$, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2020.04.004

Proof. Since S is Galois over R, it is a faithful projective R-module and hence an R-progenerator. Since the natural map $S[\Delta]' \longrightarrow \mathrm{End}_R(S)$ 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

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

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

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

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

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

$$\phi : M^\Delta \otimes_{\mathbf{Z}} O_F \longrightarrow M,$$

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

Proof. Let $\omega_1, \ldots, \omega_n$ be a $\mathbf{Z}$-basis for O_F. Then any element in $M^\Delta \otimes_{\mathbf{Z}} O_F$ 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 ϕ. This means that $\sum_i \omega_i m_i = 0$ 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, $z\sigma(\omega_j^*)$ is in O_F for every j and for every $\sigma \in \Delta$. We have

$$\sum_{\sigma \in \Delta} z\sigma(\omega_j^*) \sum_i \sigma(\omega_i) m_i = 0, \qquad \text{for all } j.$$

Therefore

$$\sum_i z(\sum_{\sigma\in\Delta}\sigma(\omega_j^*)\sigma(\omega_i))m_i = 0, \qquad \text{for all } j.$$

It follows that $zm_i = 0$ for every i and hence $zx = 0$. This implies that δ_F annihilates x, as required.

To prove that the cokernel of ϕ is also killed by δ_F, let $m \in M$. Then $\sum_{\sigma\in\Delta}\sigma(\omega_i m)$ is Δ-invariant for every i and hence is in $\operatorname{im}\phi = M^\Delta O_F$. For all $z \in \delta_F$ and every $\tau \in \Delta$ the elements

$$\sum_{\sigma\in\Delta}\sum_i z\tau(\omega_i^*)\sigma(\omega_i)\sigma(m), \tag{$*$}$$

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 τ. In particular zm is in the image of ϕ. It follows that δ_F kills the cokernel of ϕ, as required.

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

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

3. The p-part

For any prime $p \geq 3$ let $\mathbf{Z}_p$ denote the ring of p-adic integers and put $A = \mathbf{Z}_p[\zeta_p]$. In the notation of section 1, the p-part of the kernel of the norm map $Cl_K \longrightarrow Cl_K$ 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 Δ-action.

In this section we study this type of modules. They form an abelian category. Since the natural action of Δ on A is semilinear, the ring A is itself an example. So are its ideals and quotients. The ideals are of the form $\pi^i A$ for $i \geq 0$. Here π denotes a $p-1$-th root of $-p$ in A. It is easy to see that π is equal to $\zeta_p - 1$ times a unit, so that π 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 $\mathbf{F}_p$ with trivial Δ-action.

Please cite this article in press as: R. Schoof, On the ideal class group of the normal closure of $\mathbf{Q}(\sqrt[p]{n})$, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2020.04.004

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

For every character $\chi : \Delta \longrightarrow \mathbf{Z}_p^*$ and an $A[\Delta]'$-module M, we define its χ-*eigenspace* by

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

This is a $\mathbf{Z}_p$-submodule of M. It is, in general, not an A-module. The natural map

$$\bigoplus_\chi M_\chi \longrightarrow M,$$

is an isomorphism. For $\chi = 1$ we recover the subgroup of Δ-invariants $M_1 = M^\Delta$. We have that $M(\chi)^\Delta = M_{\chi^{-1}}$.

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

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 π and hence are isomorphic to products of copies of $\mathbf{F}_p(\chi)$ for certain characters χ of Δ. 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 $\mathbf{F}_p$, $\mathbf{F}_p(\omega)$, $\mathbf{F}_p(\omega^2)$, ... 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 $\mathbf{F}_p(\omega^i)$, $\mathbf{F}_p(\omega^{i+1})$, ..., $\mathbf{F}_p(\omega^{j-1})$.

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

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

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

Proof. For any module M of this type, the quotient $M/\pi M$ is isomorphic to a product of copies of $A/\pi A = \mathbf{F}_p$ with trivial Δ-action. Conversely, suppose that $M/\pi M$ has trivial Δ-action. Since the order of Δ is prime to p, the map $M^\Delta \longrightarrow (M/\pi M)^\Delta = M/\pi M$ is surjective. This implies that M can be generated over A by Δ-invariant elements $v_1, \ldots, v_t$ say. In other words, the A-homomorphism $A^t \longrightarrow M$ 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

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

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

Since $\pi^{n_i-1}/\pi^{n_i}A \cong \mathbf{F}_p(\omega^{n_i-1})$, the coordinates λ_i must be congruent to $0 \pmod{\pi^{n_i}}$ for the indices i for which $n_i - 1 \not\equiv m \pmod{p-1}$. Let I denote the set of indices for which $n_i - 1 \equiv m \pmod{p-1}$. 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 $\lambda_i \not\equiv 0 \pmod{\pi^{n_i}}$. 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 $m_i \in \mathbf{Z}$ such that $\mu_i \equiv m_i \pmod{\pi}$. Note that μ_i and hence m_i are invertible in A.

From ϕ we construct now a second R-homomorphism ϕ'

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

by mapping the first basis vector $e_1 = (1, 0, 0, \ldots)$ to $\sum_{i=1}^t m_i p^{k_i - k_1} v_i$, mapping the basis vectors e_i to $\phi(e_i)$ when $i \geq 2$ and extend A-linearly. In this way $\phi'(e_i) \in M^\Delta$ for every i. Since ϕ is surjective and m_1 is invertible in $\mathbf{Z}_p$, the morphism ϕ' is also surjective. We only need to check that it is well defined. This means that ϕ' 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.

Please cite this article in press as: R. Schoof, On the ideal class group of the normal closure of $\mathbf{Q}(\sqrt[p]{n})$, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2020.04.004

Proposition 3.2. *Let M be a finite $A[\Delta]'$-module that is generated by Δ-invariant elements. Let $d_i = \dim M[\pi]_{\omega^{i-1}}$ for $1 \le i \le p-2$. Then there is a finite abelian p-group H and an exact sequence of $A[\Delta]'$-modules*

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

Proof. Suppose that M is of the form $A/\pi^n A$ for some $n \ge 0$ Then there are integers $m \ge 0$ 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 $H = \mathbf{Z}/p^m\mathbf{Z}$, we have $A/p^m A = H \otimes_{\mathbf{Z}_p} A$. We put $V = A/\pi^i A$. Then $V = 0$ for $i = 0$. For $1 \le i \le p-2$, the submodule $M[\pi]$ is the same as the π-torsion submodule of V, which is isomorphic to $\mathbf{F}_p(\omega^{i-1})$. 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 Δ-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 $\oplus_{i=1}^{p-2} (A/\pi^i A)^{d_i}$ of Proposition 3.2 is killed by π^{p-2} and hence by p. Its $\mathbf{F}_p$-dimension is $\sum_{i=1}^{p-2} i d_i$.

4. Class field theory

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

In this section we study the Tate G-cohomology groups of the class group of K. The class group of K is a $\mathbf{Z}[\Omega]$-module, and Tate G-cohomology groups of $\mathbf{Z}[\Omega]$-modules are $\mathbf{F}_p[\Delta]$-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 $H^2(G, \mathbf{Z})$, is *not* Δ-equivariant. Indeed, $\widehat{H}^0(G, \mathbf{Z}) = \mathbf{Z}/p\mathbf{Z}$ has trivial Δ-action, while $H^2(G, \mathbf{Z}) = G^{\mathrm{dual}}$ has Δ-action via ω^{-1}. For $q \in \mathbf{Z}$ and an arbitrary Ω-module M the maps

$$\widehat{H}^q(G, M) \xrightarrow{\cong} \widehat{H}^{q+2}(G, M)(\omega),$$

given by cupping with a generator of $H^2(G, \mathbf{Z})$, are $\mathbf{F}_p[\Delta]$-isomorphisms.

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

Lemma 4.1. *Let M be a $\mathbf{Z}[\Omega]$-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 Δ 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 $\mathbf{Z}[\Omega]$-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 $\mathbf{Q}(\zeta_p)$. In order to get information on the $\mathbf{F}_p[\Delta]$-structure of the G-cohomology groups of Cl_K, we determine the Δ-action on the G-cohomology groups of U_K and, for completeness, also of C_K.

Lemma 4.2. *The cohomology groups $\widehat{H}^q(G, C_K)$ are trivial when q is odd and isomorphic to $\mathbf{F}_p$ if q is even. In the latter case, Δ acts on $\widehat{H}^q(G, C_K)$ 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 Δ 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 $H^2(\Delta, C_{\mathbf{Q}(\zeta_p)})$ are isomorphic to the groups $\widehat{H}^0(\Omega, \mathbf{Z})$, $\widehat{H}^0(G, \mathbf{Z})$ and $\widehat{H}^0(\Delta, \mathbf{Z})$, and hence are cyclic of orders $p(p-1)$, p and $p-1$ respectively. By Lemma 4.1 with $M = C_K$, the sequence

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

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

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

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

Here the sum runs over primes l for which the primes v lying over l in $\mathbf{Q}(\zeta_p)$ are ramified in K and $\Delta_l \subset \Delta$ denotes the decomposition subgroup of v. The Δ-action on $H^1(G, U_K)$ and $H^2(G, U_K)$ is the natural action on the various summands $\mathbf{Z}/p\mathbf{Z}[\Delta/\Delta_l]$. The Δ-action on $\widehat{H}^q(G, U_K)$ 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 $\mathbf{Q}(\zeta_p)$ 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 $q \in \mathbf{Z}$, the cohomology group $\widehat{H}^q(G, U_K)$ is isomorphic to

$$\bigoplus_{l \text{ ram in } K} \bigoplus_{v|l} \widehat{H}^q(G_v, O_w^*).$$

Each summand $\widehat{H}^q(G_v, O_w^*)$ is naturally an $\mathbf{F}_p[\Delta_l]$-module and we have isomorphisms

$$\bigoplus_{v|l} \widehat{H}^q(G_v, O_w^*) \cong \mathrm{Ind}_{\Delta_v}^{\Delta} \widehat{H}^q(G_v, O_w^*)$$

of $\mathbf{F}_p[\Delta]$-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 Δ-action.

First we show for $q = 1$ and 2, that the action of Δ_v on $\widehat{H}^q(G_v, O_w^*)$ 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

$$0 \longrightarrow H^1(\Delta_l, O_v^*) \longrightarrow H^1(\Omega_v, O_w^*) \longrightarrow H^1(G_v, O_w^*)^{\Delta_l} \longrightarrow 0,$$

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

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

as required.

Please cite this article in press as: R. Schoof, On the ideal class group of the normal closure of $\mathbf{Q}(\sqrt[p]{n})$, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2020.04.004

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

$$0 \longrightarrow H^2(\Delta_l, \mathbf{Q}(\zeta_p)_v^*) \longrightarrow H^2(\Omega_v, K_w^*) \longrightarrow H^2(G_v, K_w^*)^{\Delta_v} \longrightarrow 0.$$

By *local* class field theory, the cohomology groups $H^2(\Delta_l, \mathbf{Q}(\zeta_p)_v^*)$, $H^2(\Omega_v, K_w^*)$ and $H^2(G_v, K_w^*)$ have orders equal to the cardinality of Δ_l, Ω_v and G_v respectively. The exactness of the sequence then shows that $H^2(G_v, K_w^*)$ is Δ_l-invariant. Since the natural map $H^2(G_v, O_w^*) \longrightarrow H^2(G_v, K_w^*)$ 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 $\widehat{H}^0(G_v, O_w^*)$, we find as in the previous case an isomorphism of Δ-modules

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

with the required Δ-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

$$0 \longrightarrow O_K^* \longrightarrow U_K \longrightarrow Q_K \longrightarrow 0,$$

$$0 \longrightarrow Q_K \longrightarrow C_K \longrightarrow Cl_K \longrightarrow 0,$$

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 $\mathbf{Q}(\zeta_p)$. This implies that the cokernel of the natural map $U_{\mathbf{Q}(\zeta_p)} \to C_{\mathbf{Q}(\zeta_p)}$ has order prime to p, so that $\widehat{H}^0(G, U_K) \longrightarrow \widehat{H}^0(G, C_K)$ is surjective. It follows that the map $\widehat{H}^0(G, Q_K) \longrightarrow \widehat{H}^0(G, C_K)$ is also surjective. An application of the snake lemma to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q_{\mathbf{Q}(\zeta_p)} & \longrightarrow & C_{\mathbf{Q}(\zeta_p)} & \longrightarrow & Cl_{\mathbf{Q}(\zeta_p)} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \cong & & \downarrow & & \\ 0 & \longrightarrow & Q_K^G & \longrightarrow & C_K^G & \longrightarrow & Cl_K^G & & \end{array}$$

shows that the natural map $Q_{\mathbf{Q}(\zeta_p)} \longrightarrow Q_K^G$ is an isomorphism. This implies that the map $U_{\mathbf{Q}(\zeta_p)} \longrightarrow Q_K^G$ is surjective, so that $\widehat{H}^0(G, U_K) \longrightarrow \widehat{H}^0(G, Q_K)$ 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.

$$
\begin{tikzcd}
 & & \widehat{H}^0(G, O_K^*) \arrow[d] & & \\
 & & \widehat{H}^0(G, U_K) \arrow[d] \arrow[dr] & & \\
0 \arrow[r] & \widehat{H}^{-1}(G, Cl_K) \arrow[r] & \widehat{H}^0(G, Q_K) \arrow[r] \arrow[d, "=0"] & \widehat{H}^0(G, C_K) \arrow[r] & 0 \\
 & & H^1(G, O_K^*) \arrow[d] & & \\
 & & H^1(G, U_K) \arrow[d] & & \\
0 \arrow[r] & \widehat{H}^0(G, Cl_K) \arrow[r] & H^1(G, Q_K) \arrow[r] \arrow[d] & 0 & \\
 & & H^2(G, O_K^*) \arrow[d] & & \\
 & & H^2(G, U_K) & &
\end{tikzcd}
$$

The G-cohomology groups are $\mathbf{F}_p[\Delta]$-modules and all maps, including the connecting homomorphisms, are Δ-linear. Since this last fact plays an important role, we explain why this is so. A complete Ω-resolution $P_\bullet = \{P_i\}_{i\in\mathbf{Z}}$ as in [3, IV.6] is also a complete G-resolution. For any Ω-module M and any $i \in \mathbf{Z}$, the groups $\mathrm{Hom}_G(P_i, M)$ are naturally objects of the abelian category of Δ-modules. The cohomology groups of the complex $X^\bullet(M) = \mathrm{Hom}_G(P_\bullet, M)$ 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 Δ-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 Δ acts via ω on $M/\pi M$;
(ii) for every non-trivial character χ of Δ the $\mathbf{F}_p$-dimension of $M[\pi]_\chi$ is at most 1. Moreover, if χ 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

$$\bigoplus_{l\,\mathrm{ram\,in\,K}} \mathbf{Z}/p\mathbf{Z},$$

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

Please cite this article in press as: R. Schoof, On the ideal class group of the normal closure of $\mathbf{Q}(\sqrt[p]{n})$, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2020.04.004

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

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

The group Δ acts trivially on $H^1(G, U_K)$. Therefore the χ-eigenspace of $\widehat{H}^0(G, Cl_K)$ is contained in the one of $H^2(G, O_K^*)$ when χ is non-trivial. The Δ-module $H^2(G, O_K^*)$ is isomorphic to $\widehat{H}^0(G, O_K^*)(\omega^{-1})$ and is hence a quotient of $(\mathbf{Z}[\zeta_p]^*/\mathbf{Z}[\zeta_p]^{*p})(\omega^{-1})$. By an equivariant version [7, Prop.13.7] of Dirichlet's Unit Theorem, $\mathbf{Z}[\zeta_p]^*/\mathbf{Z}[\zeta_p]^{*p}$ is a product of copies of $\mathbf{F}_p(\chi)$, one for each non-trivial even character χ and one copy of $\mathbf{F}_p(\omega)$.

Since p is regular, M is killed by the G-norm N_G, so that it is a $\mathbf{Z}_p[\Delta]'$-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 $\mathbf{Z}_p[\zeta_p] = \mathbf{Z}_p[G]/(\mathrm{Tr}_G)$, we find that $M/\pi M = \widehat{H}^{-1}(G, Cl_K)$ and $M[\pi] = \widehat{H}^0(G, Cl_K)$.

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 Δ-structure, we may twist the p-part M of the class group of K by the character ω^{-1}. We denote the result by M'. By Theorem 4.4, the group Δ acts trivially on $M'/\pi M'$, so that the A-module M' is generated by Δ-invariant elements. By Proposition 3.2 there is an exact sequence

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

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

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

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 $\mathbf{Z}[S_3]$-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 $\mathbf{Z}[S_3]$-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 σ 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 ρ 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 $M/(\rho-1)M \to \operatorname{cok} f$.

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 $\operatorname{cok} f$.

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

This proves the lemma.

If $n \in \mathbf{Z}$ is not a cube, the Galois group of $\mathbf{Q}(\zeta_3, \sqrt[3]{n})$ 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 σ acts trivially on $\widehat{H}^0(G, Cl_K) = M[\rho]$ and acts as -1 on $M/(\rho-1)M = \widehat{H}^{-1}(G, Cl_K)$. Since n is not divisible by any primes congruent to 1 (mod 3), this follows from Theorem 4.4.

References

[1] M. Auslander, O. Goldman, The Brauer group of a commutative ring, Trans. Am. Math. Soc. 97 (1960) 367–409.
[2] H. Cartan, S. Eilenberg, Homological Algebra, Princeton University Press, Princeton, 1956.
[3] J. Cassels, A. Fröhlich (Eds.), Algebraic Number Theory, Proceedings of an Instructional Conference, Academic Press, London, 1967.
[4] F. DeMeyer, E. Ingraham, Separable Algebras over Commutative Rings, Lecture Notes in Mathematics, vol. 181, Springer-Verlag, Berlin, 1971.
[5] T. Honda, Pure cubic fields whose class numbers are multiples of three, J. Number Theory 3 (1971) 7–12.
[6] D. Hubbard, L. Washington, Iwasawa invariants of some non-cyclotomic $\mathbf{Z}_p$-extensions, J. Number Theory 188 (2018) 18–47.
[7] R. Schoof, Catalan's Conjecture, Universitext, Springer-Verlag, London, ISBN 978-1-84800-184-8, 2008.

Please cite this article in press as: R. Schoof, On the ideal class group of the normal closure of $\mathbf{Q}(\sqrt[p]{n})$, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2020.04.004