

Distribution of prime ideals across ideal classes in the class groups

Prem Prakash Pandey

Department of Mathematics, IISER Berhampur, Engineering School Road, Khodasingi, Brahmapur 760 010, India
 e-mail: premshivaganga@gmail.com

Communicated by: Dr. Anupam Saikia

Received: September 26, 2017

Abstract. In this article we investigate the distribution of prime ideals of residue degree bigger than one across the ideal classes in the class group of a number field L . A criterion for the class group of L being generated by the classes of prime ideals of residue degree $f > 1$ is provided. Further, some consequences of this study on the solvability of norm equations for L/\mathbb{Q} and on the problem of finding annihilators for relative extensions are discussed.

2010 Mathematics Subject Classification: 11R44, 11R40.

1. Introduction

In this article, L and K denote number fields such that K is a subfield of L . We assume that L/K is Galois and write $G := Gal(L/K)$. Let \mathfrak{p} be a prime ideal of L , \mathfrak{p} denote the prime ideal of K below \mathfrak{p} . The residue degree $[\mathbb{O}_L/\mathfrak{p} : \mathbb{O}_K/\mathfrak{p}]$ will be denoted by $res_K^L(\mathfrak{p})$, and when $K = \mathbb{Q}$ we should simply write $res(\mathfrak{p})$. Also we let ℓ be an odd prime number and fix a primitive ℓ^{th} root of unity ζ_ℓ . Let $\mathbb{Q}(\zeta_\ell)$ denote the subfield of \mathbb{C} obtained by adjoining ζ_ℓ to \mathbb{Q} . An important result in algebraic number theory is the following theorem, which is one of many density theorems.

Theorem 1.1. *Every ideal class in the class group of L contains infinitely many prime ideals \mathfrak{p} of residue degree one, that is, $res(\mathfrak{p}) = 1$.*

Let c be an ideal class in the class group of L and \mathfrak{p} be a prime ideal in c . If p denotes the rational prime lying below \mathfrak{p} then, by Theorem 1.1, one may assume that p is unramified in L/\mathbb{Q} and the following factorization holds

$$p\mathbb{O}_L = \prod_{\sigma \in Gal(L/\mathbb{Q})} \sigma(\mathfrak{p}).$$

Thus, for $N = \sum_{\sigma \in Gal(L/\mathbb{Q})} \sigma$ we have

$$c^N = [\mathfrak{p}]^N = [(p)],$$

which is trivial. This shows that N annihilates the class group $Cl(L)$. But N is not very useful as annihilator, as in applications of annihilators, mostly one uses $(1 - \sigma)\theta$ for annihilation, where $\theta \in \mathbb{Z}[Gal(L/\mathbb{Q})]$ is any annihilator of the class group of L and $\sigma \in Gal(L/\mathbb{Q})$ is the complex conjugation (e.g. see the works of Mihailescu on Catalan's conjecture, in [15] or [2]).

There are various accounts of finding elements in the group ring $\mathbb{Z}[G]$ which annihilate the class group $Cl(L)$ of L . When $K = \mathbb{Q}$, the Stickelberger theorem is a celebrated result in this direction (see [9] or [17]). In full generality (that is when K is arbitrary) there is no description of elements in $\mathbb{Z}[G]$ which annihilate the class group $Cl(L)$ (though there are some results in special cases, see [4] or [14,16]). On the other hand, if K has class number one, then it is easy to see (for example, as illustrated after Theorem 1.1), that the G -trace $N = \sum_{\sigma \in G} \sigma$ annihilates the

class group $C\ell(L)$. The perspective taken in this article is to explore an analogue of Theorem 1.1 for higher residue degrees and possible consequences. For extension L/K , we define the set

$$\mathcal{R}_K^L := \{f \in \mathbb{N} : C\ell(L) \text{ is generated by classes of unramified prime ideals } \mathfrak{p} \text{ with } \text{res}_K^L(\mathfrak{p}) = f\}.$$

From Theorem 1.1 it follows that $1 \in \mathcal{R}_K^L$ for any extension L/K . For $L = \mathbb{Q}(\zeta_\ell)$ and $K = \mathbb{Q}$, Kummer had proved this using only algebraic tools (see [8] or chapter 9 in [15]). This algebraic proof has been further extended by Lenstra and Stevenhagen in more general set-up (see [11]). To the best of our knowledge, the following question (which can be seen as a generalization of Theorem 1.1) has not been addressed in the literature.

Question 1. When does the set \mathcal{R}_K^L has more than one element?

The question is interesting only when the class number of L is bigger than 1. When G is cyclic and K has class number 1, then each element of \mathcal{R}_K^L gives rise to an annihilator of the class group $C\ell(L)$. Let $f \in \mathcal{R}_K^L$ and let G' be the unique subgroup of G of order f . If $\{\sigma_1, \dots, \sigma_g\}$ is a complete set of representatives of the elements of G/G' , then we put $\theta_f = \sum_{i=1}^g \sigma_i$ and prove the following theorem.

Theorem 1.2. Consider a cyclic extension L/K of number fields. Then at least one of the following holds:

- (1) the class number of K is bigger than one,
- (2) the element θ_f annihilates $C\ell(L)$ for each $f \in \mathcal{R}_K^L$.

For $f = 1$ we have $\theta_1 = N$, the G -trace. Using Theorem 1.2, in section 3, we shall show that for the fields $L = \mathbb{Q}(\zeta_{23})$ and $K = \mathbb{Q}$ we have $\mathcal{R}_K^L = \{1\}$. Next, we give a criterion to determine if a positive integer f is in \mathcal{R}_K^L or not. For this, let $H := H(L)$ be the Hilbert class field of L (maximal unramified abelian extension of L). Then H/K is Galois (see Lemma 1) and we have a short exact sequence

$$0 \longrightarrow \text{Gal}(H/L) \longrightarrow \text{Gal}(H/K) \longrightarrow \text{Gal}(L/K) \longrightarrow 0. \quad (1)$$

For any $\sigma \in \text{Gal}(L/K)$ we use $\bar{\sigma}$ for any lift of σ to H , that is, $\bar{\sigma} \in \text{Gal}(H/K)$ and $\bar{\sigma}|_L = \sigma$. Now we are in a position to state the criterion.

Theorem 1.3. For an integer $f > 1$, the ideal class group $C\ell(L)$ is generated by the classes of prime ideals \mathfrak{p} with $\text{res}_K^L(\mathfrak{p}) = f$ if and only if the set

$$\{(\bar{\sigma})^f : \sigma \in \text{Gal}(L/K) \text{ and the order of } \sigma \text{ is } f\}$$

generates the group $\text{Gal}(H/L)$.

We give a proof of Theorem 1.3 in the next section. The proof also demonstrates that the size of the subgroup generated by the set $\{(\bar{\sigma})^f : \sigma \in \text{Gal}(L/K)\}$ is of order f measures the size of the subgroup of the class group which is generated by the classes of prime ideals \mathfrak{p} with $\text{res}_K^L(\mathfrak{p}) = f$. This can be exploited to study the (absolute) norm equations. The study of solvability of norm equations for number fields and algorithms to determine solutions to norm equations are well pursued (see [6,1,5,3] and references in there). The special case $\mathcal{R}_K^L = \{1\}$ has an immediate bearing on the solvability of the norm equations. In this direction we give the following sufficient condition for the solvability of norm equations.

Theorem 1.4. Let L be a number field whose class number is a prime number. If $\mathcal{R}_\mathbb{Q}^L = \{1\}$ then the norm equation

$$|N_{L/\mathbb{Q}}(x)| = a, a \geq 0 \quad (2)$$

is solvable whenever the prime divisors p of a are unramified, of residue degree bigger than 1 and $v_p(a)$ is a multiple of the residue degree of p . Here $v_p(a)$ is the p -adic valuation of a , that is, the highest power of p which divides a .

The only reason for considering the absolute norm equation in Theorem 1.4 is that we can not say, in general, whether -1 is a norm or not. Thus, if the extension L/\mathbb{Q} is not totally real then in Theorem 1.4 we can replace equation (2) by

$$N_{L/\mathbb{Q}}(x) = a.$$

In section 3, Theorem 1.4 is used to give a very concrete description of the solvability of the norm equations for the extension $\mathbb{Q}(\zeta_{23})/\mathbb{Q}$ in a very elementary way (see Theorem 3.3).

2. Proofs

We begin this section with a proof of Theorem 1.2.

Proof of Theorem 1.2 If the class number of K is bigger than one then nothing to prove. So we assume that the class number of K is one. Let c be an ideal class in $C\ell(L)$. Then

$$c = [p_1][p_2] \dots [p_r]$$

for unramified prime ideals p_1, \dots, p_r of residue degree f . Thus it is enough to prove that θ_f annihilates all the unramified prime ideals of residue degree f .

Let \mathfrak{p} be an unramified prime ideal of the residue degree f in L and let \mathfrak{p} be the prime ideal of K lying below \mathfrak{p} . Let $D_{\mathfrak{p}}$ denote the decomposition group at \mathfrak{p} . Then $D_{\mathfrak{p}}$ is the unique subgroup of G of order f and it does not depend on \mathfrak{p} . If $\{\sigma_1, \dots, \sigma_g\}$ is a complete set of representatives of $G/D_{\mathfrak{p}}$, then $\{\sigma_i(\mathfrak{p}) : 1 \leq i \leq g\}$ is the set of all conjugates of \mathfrak{p} . Thus the factorization of $\mathfrak{p}\mathbb{O}_L$ is given by

$$\mathfrak{p}\mathbb{O}_L = \prod_{i=1}^g \sigma_i(\mathfrak{p}).$$

Since θ_f is a multiple of $\sum_{i=1}^g \sigma_i$ by some $\tau \in D_{\mathfrak{p}}$, it follows that

$$\mathfrak{p}^{\theta_f} = \tau(\mathfrak{p}\mathbb{O}_L)$$

is principal. Thus θ_f annihilates the class group $C\ell(L)$. □

To prove Theorem 1.3 we need some preliminaries. We begin with the following elementary lemma (as was indicated in section 1).

Lemma 1. *If L/K is a Galois extension of number fields and H is the Hilbert class field of L , then H/K is Galois.*

Proof. We fix an algebraic closure $\bar{\mathbb{Q}}$ of \mathbb{Q} . Let $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/K)$, then $\sigma(L) = L$, as L/K is Galois. We observe that the extension $\sigma(H)/\sigma(L)$ is abelian and unramified. That is, the extension $\sigma(H)/L$ is abelian and unramified. From the maximality of H it follows that $\sigma(H) \subset H$, proving that H/K is Galois. □

For an unramified prime ideal \mathfrak{p} in L , let $\left(\frac{\mathfrak{p}}{L/K}\right)$ denote the Frobenius of \mathfrak{p} with respect to the extension L/K . If L/K is abelian then we also write $\left(\frac{\mathfrak{p}}{L/K}\right)$ for $\left(\frac{\mathfrak{p}}{L/K}\right)$, where $\mathfrak{p} = \mathfrak{p} \cap \mathbb{O}_K$. From the definition of the Frobenius, we have the following lemma (see page 127 in [7]).

Lemma 2. *Let L/K be a Galois extension of number fields and let F be an intermediate field such that F/K is Galois. Then for any unramified prime ideal \mathfrak{p} of L one has $\left(\frac{\mathfrak{p}}{L/K}\right)_F = \left(\frac{\mathfrak{p} \cap \mathbb{O}_F}{F/K}\right)$.*

Next we recall the Chebotarëv density Theorem (see [10]). For any $\sigma \in \text{Gal}(L/K)$, let $P_{L/K}(\sigma)$ denote the set of prime ideals \mathfrak{p} in K such that there is a prime ideal \mathfrak{p} of L above \mathfrak{p} such that $\left(\frac{\mathfrak{p}}{L/K}\right) = \sigma$.

Theorem 2.1 (Chebotarëv Density Theorem). *Let $\sigma \in \text{Gal}(L/K)$ and C_{σ} stand for the conjugacy class of σ then the density of $P_{L/K}(\sigma)$ is $|C_{\sigma}|/[L : K]$.*

Proof of Theorem 1.3 For any $\sigma \in \text{Gal}(L/K)$ of order f , it is immediate to see that

$$(\tilde{\sigma})^f \mid L = id,$$

and thus $(\tilde{\sigma})^f \in \text{Gal}(H/L)$.

Assume that the set $\{(\tilde{\sigma})^f : \sigma \in \text{Gal}(L/K) \text{ and the order of } \sigma \text{ is } f\}$ generates the group $\text{Gal}(H/L)$. Let c be an ideal class in $C\ell(L)$ and τ be the corresponding element in $\text{Gal}(H/L)$ under the Artin isomorphism between $C\ell(L)$ and the Galois group $\text{Gal}(H/L)$. Then there is a prime ideal \mathfrak{p} in c such that

$$\left(\frac{\mathfrak{p}}{H/L}\right) = \tau.$$

From our assumption, there are elements $\sigma_1, \dots, \sigma_r$ in $\text{Gal}(L/K)$ of order f such that

$$\tau = (\tilde{\sigma}_1)^f \dots (\tilde{\sigma}_r)^f.$$

By Chebotarev density theorem, for each $i, 1 \leq i \leq r$ there exists prime ideal \wp_i of H such that

$$\left(\frac{\wp_i}{H/K} \right) = \tilde{\sigma}_i.$$

Let $\mathfrak{p}_i = \wp_i \cap \mathbb{O}_L$ for $i = 1, \dots, r$. Then from Lemma 2 it follows that $\left(\frac{\mathfrak{p}_i}{L/K} \right) = \sigma_i$, for $i = 1, \dots, r$. Since the order of σ_i is f , we conclude that the residue degree of \mathfrak{p}_i is f . Next we note that

$$\left(\frac{\wp_i}{H/L} \right) = (\tilde{\sigma}_i)^f.$$

Since H/L is abelian, we get

$$\left(\frac{\mathfrak{p}_i}{H/L} \right) = (\tilde{\sigma}_i)^f.$$

This leads to

$$\left(\frac{\mathfrak{p}}{H/L} \right) = \left(\frac{\mathfrak{p}_1}{H/L} \right) \dots \left(\frac{\mathfrak{p}_r}{H/L} \right).$$

From the above equality, it follows that $\mathfrak{c} = [\mathfrak{p}_1] \dots [\mathfrak{p}_r]$, as desired.

Conversely assume that the ideal class group $\mathcal{C}\ell(L)$ is generated by the classes of prime ideals of residue degree f .

Let $\tau \in \text{Gal}(H/L)$ and let \mathfrak{c} be the ideal class corresponding to τ under the Artin isomorphism. By our assumption, there are prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of residue degree f such that $\mathfrak{c} = [\mathfrak{p}_1] \dots [\mathfrak{p}_r]$. Put $\sigma_i = \left(\frac{\mathfrak{p}_i}{L/K} \right)$, for $i = 1, \dots, r$. Then it follows immediately that σ_i is of order f and $\tau = (\tilde{\sigma}_1)^f \dots (\tilde{\sigma}_r)^f$. This proves the Theorem. \square

Remark 1. From the proof of the Theorem 1.3, it is immediate that the size of the subgroup generated by the set $\{(\tilde{\sigma})^f : \sigma \in \text{Gal}(L/K) \text{ is of order } f\}$ measures the size of the subgroup of the class group $\mathcal{C}\ell(L)$ which is generated by the classes of prime ideals of residue degree f . In particular, if the class number of L is prime and $f \notin \mathcal{R}_K^L$ then all the prime ideals of residue degree f are principal in L .

Proof of Theorem 1.4 Let p be a prime of residue degree $f > 1$ which is unramified in L . We shall show that there is an element $\alpha \in L$ such that $|N_{L/K}(\alpha)| = p^f$. Since the class number of L is a prime number and $\mathcal{R}_K^L = \{1\}$, the subgroup generated by the set

$$\{(\tilde{\sigma})^f : \sigma \in \text{Gal}(L/K) \text{ and the order of } \sigma \text{ is } f\}$$

is trivial. Consequently, from the Remark 1, all the prime ideals \mathfrak{p} of L above p are principal. Let \mathfrak{p} be a prime ideal of L dividing p and α be a generator of \mathfrak{p} . Then we have

$$|N_{L/\mathbb{Q}}(\alpha)| = p^f.$$

The theorem follows at once from the multiplicative property of the norm map. \square

3. An example

In this section, we consider the fields $L = \mathbb{Q}(\zeta_{23})$ and $K = \mathbb{Q}$ and show that $\mathcal{R}_K^L = \{1\}$. Note that, the condition 'unramified' in the definition of \mathcal{R}_K^L is redundant in this case. If \mathfrak{p} is a prime ideal in $\mathbb{Q}(\zeta_{23})$ of residue degree f then $f|22$, and thus $f \in \{1, 2, 11, 22\}$. We shall show that for no $f \in \{2, 11, 22\}$ each ideal class of L can contain a prime

ideal of residue degree f . Since the class number of $\mathbb{Q}(\zeta_{23})$ is bigger than 1, it follows that $f = 22$ is not possible. So it remains to show that $f = 2$ or $f = 11$ is not possible.

Before proceeding further, we recall some results on cyclotomic fields which will be needed. Let h_ℓ^+ and h_ℓ denote the class numbers of $\mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$ and $\mathbb{Q}(\zeta_\ell)$ respectively and put $h_\ell^- = h_\ell/h_\ell^+$. Let G be the Galois group $\text{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ and S denote the Stickelberger ideal in $\mathbb{Z}[G]$. It is well known that $[\mathbb{Z}[G] : S] = h_\ell^-$. We now describe a basis of S (see chapter 9 in [15]).

For each $a \geq 1$ with $(a, \ell) = 1$ we define

$$\theta_a = \sum_{i=1}^{\ell-1} \left\lfloor \frac{ai}{\ell} \right\rfloor \sigma_i^{-1},$$

where $\sigma_i : \zeta_\ell \mapsto \zeta_\ell^i$ and $\lfloor x \rfloor$ denotes the largest integer not bigger than x . Further we put $f_i = \theta_{i+1} - \theta_i$. Then we have following Theorem due to Kummer.

Theorem 3.1 (Theorem 9.3, [15]). *The elements $f_1, \dots, f_{(p-1)/2}$ together with the G -trace $N = \sum_{\sigma \in G} \sigma$ forms a \mathbb{Z} -basis of S .*

We recall following fact (see Theorem 1.1 in [12]).

Theorem 3.2. *We have $h_\ell^+ = 1$ for $\ell < 100$.*

Now we fix $\ell = 23$, we have $h_{23} = h_{23}^-$. Thus, if $\theta \in \mathbb{Z}[G]$ annihilates the class group of $\mathbb{Q}(\zeta_{23})$ then θ must lie in S . In the case of $\mathbb{Q}(\zeta_{23})$, we have

$$f_1 = \sum_{i \in I_1} \sigma_i, \quad \text{where } I_1 = \{2, 16, 5, 20, 13, 19, 9, 17, 15, 11, 22\},$$

$$f_2 = \sum_{i \in I_2} \sigma_i, \quad \text{where } I_2 = \{3, 18, 7, 21, 13, 19, 9, 17, 15, 11, 22\},$$

$$f_3 = \sum_{i \in I_3} \sigma_i, \quad \text{where } I_3 = \{4, 10, 2, 16, 5, 20, 9, 17, 15, 11, 22\},$$

$$f_4 = \sum_{i \in I_4} \sigma_i, \quad \text{where } I_4 = \{2, 16, 5, 20, 13, 19, 9, 17, 15, 11, 22\},$$

$$f_5 = \sum_{i \in I_5} \sigma_i, \quad \text{where } I_5 = \{6, 3, 18, 2, 16, 13, 19, 9, 15, 11, 22\},$$

$$f_6 = \sum_{i \in I_6} \sigma_i, \quad \text{where } I_6 = \{10, 7, 21, 5, 20, 19, 9, 17, 15, 11, 22\},$$

$$f_7 = \sum_{i \in I_7} \sigma_i, \quad \text{where } I_7 = \{8, 4, 18, 2, 16, 20, 13, 9, 17, 11, 22\},$$

$$f_8 = \sum_{i \in I_8} \sigma_i, \quad \text{where } I_8 = \{3, 21, 16, 5, 13, 19, 9, 17, 15, 11, 22\},$$

$$f_9 = \sum_{i \in I_9} \sigma_i, \quad \text{where } I_9 = \{14, 10, 7, 2, 5, 20, 19, 17, 15, 11, 22\},$$

$$f_{10} = \sum_{i \in I_{10}} \sigma_i, \quad \text{where } I_{10} = \{18, 21, 16, 20, 13, 19, 9, 17, 15, 11, 22\},$$

$$f_{11} = \sum_{i \in I_{11}} \sigma_i, \quad \text{where } I_{11} = \{12, 6, 4, 3, 7, 2, 5, 13, 9, 15, 22\}.$$

If the class group of $\mathbb{Q}(\zeta_{23})$ is generated by prime ideals of residue degree 11 then by Theorem 1.2 the element θ_{11} is an annihilator of the class group of $\mathbb{Q}(\zeta_{23})$. Thus we have $\theta_{11} \in S$. Hence, from Theorem 3.1, there are integers a_0, \dots, a_{11} such that

$$\theta_{11} = a_0N + a_1f_1 + \dots + a_{11}f_{11}. \quad (3)$$

For any prime ideal \mathfrak{p} of $\mathbb{Q}(\zeta_{23})$ of residue degree 11 the decomposition group is

$$D_{\mathfrak{p}} = \{\sigma_2, \sigma_4, \sigma_8, \sigma_{16}, \sigma_9, \sigma_{18}, \sigma_{13}, \sigma_3, \sigma_6, \sigma_{12}, \sigma_1\}.$$

Thus $\{\sigma_1, \sigma_5\}$ is a complete set of coset representatives of $G/D_{\mathfrak{p}}$. Note that any other set of coset representatives of $G/D_{\mathfrak{p}}$ is a multiple by an element of $D_{\mathfrak{p}}$. Hence, without loss of generality we take

$$\theta_{11} = \sigma_1 + \sigma_5. \quad (4)$$

Comparing the coefficients of σ_i in equations (3) and (4) we obtain a contradiction as explained below.

Comparing the coefficient of σ_1 leads to $a_0 = 1$ and comparing the coefficient of σ_{12} leads to $a_{11} = -1$. On the other hand comparing the coefficients of σ_{11} gives

$$1 + a_1 + a_2 + \dots + a_{10} = 0 \quad (5)$$

and from the coefficients of σ_{22} we obtain

$$1 + a_1 + a_2 + \dots + a_{11} = 0. \quad (6)$$

Equations (5) and (6) together give $a_{11} = 0$ which contradicts to $a_{11} = -1$. Thus $\theta_{11} \notin S$ and it follows that the class group of $\mathbb{Q}(\zeta_{23})$ is not generated by the classes of prime ideals of residue degree 11.

Next, we show that the class group of $\mathbb{Q}(\zeta_{23})$ is not generated by the classes of prime ideals of residue degree 2. If \mathfrak{p} is a prime ideal of residue degree 2, then the decomposition group at \mathfrak{p} is

$$D_{\mathfrak{p}} = \{\sigma_1, \sigma_{22}\}.$$

As done earlier, we may assume that

$$\theta_2 = \sigma_1 + \dots + \sigma_{11}. \quad (7)$$

From Theorem 1.2 θ_2 annihilates the class group of $\mathbb{Q}(\zeta_{23})$ and thus $\theta_2 \in S$. From Theorem 3.1, there are integers a_0, \dots, a_{11} such that

$$\theta_2 = a_0N + a_1f_1 + \dots + a_{11}f_{11}. \quad (8)$$

The equations (7) and (8) leads to an inconsistent system of equation in σ_i , $1 \leq i \leq 22$ and this is summarized below.

Coefficients of σ_1 gives $a_0 = 1$, coefficients of σ_8 gives $a_7 = 0$ and coefficients of σ_{12} gives $a_{11} = -1$. Using these, the coefficients of σ_4 gives $a_3 = 1$ and coefficients of σ_6 gives $a_5 = 1$. Using these values in the relations obtained from coefficients of σ_{11} and σ_{22} further leads to $a_9 = 0$. Now coefficients of σ_{14} leads to $a_4 = -1$. In same way, coefficients of σ_2 leads to $a_1 = -1$, coefficients of σ_{10} leads to $a_6 = -1$. Further the coefficients of σ_{20} gives $a_{10} = 0$. Now we see that the coefficients of σ_3 and that of σ_{21} lead to the inconsistent system

$$a_2 + a_8 = -1 \quad \text{and} \quad a_2 + a_8 = 0.$$

Thus we have proved that

$$\mathcal{R}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{23})} = \{1\}.$$

Remark 2. Proceeding along the same line, we have made computations for $L = \mathbb{Q}(\zeta_{29})$ and $K = \mathbb{Q}$ and found that $\mathcal{R}_K^L = \{1\}$.

Now we give a complete description of solvability of norm equations for $\mathbb{Q}(\zeta_{23})/\mathbb{Q}$. Since the splitting type of any rational prime q in $\mathbb{Q}(\zeta_{23})$ is well understood (see chapter 3 in [17]), the description in Theorem 3.3 is the best one can expect. If we let $N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{23})}$ to also denote the norm map from the group $J_{\mathbb{Q}(\zeta_{23})}$ of ideles of $\mathbb{Q}(\zeta_{23})$ to the group $J_{\mathbb{Q}}$ of ideles of \mathbb{Q} , then the quotient group

$$\mathbb{Q}^* \cap N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{23})}(J_{\mathbb{Q}(\zeta_{23})})/N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{23})}(\mathbb{Q}(\zeta_{23})^*)$$

is finite and its cardinality is the knot number of $\mathbb{Q}(\zeta_{23})$ (see [3]). The next theorem asserts that the knot number of $\mathbb{Q}(\zeta_{23})$ is 1.

Theorem 3.3. For any $a \in \mathbb{Q}$ the norm equation

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{23})}(x) = a$$

is solvable if and only if $v_p(a)$ is a multiple of the residue degree of p for all primes p and $a \geq 0$.

Proof. Since $\mathbb{Q}(\zeta_{23})$ is totally complex, the values of norm map are non-negative. It suffices to show that for each prime q there is an $\alpha \in \mathbb{Q}(\zeta_{23})$ such that

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{23})}(\alpha) = p^f, \quad \text{where } f \text{ is the residue degree of } p. \tag{9}$$

For $p = 23$, equation (9) holds for $\alpha = 1 - \zeta_{23}$. When p is a prime of residue degree $f > 1$, then p is unramified and existence of an α satisfying equation (9) is guaranteed from the Theorem 1.4.

Now assume that p splits completely in $\mathbb{Q}(\zeta_{23})$, and let \mathfrak{p} be a prime ideal of $\mathbb{Q}(\zeta_{23})$. If \mathfrak{p} is principal then we are done. The class number of $\mathbb{Q}(\zeta_{23})$ is 3 (see [17,12]). Consequently there is a $\beta \in \mathbb{Q}(\zeta_{23})$ such that

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{23})}(\beta) = p^3.$$

On the other hand

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{23})}(p) = p^{22}.$$

Let $s, t \in \mathbb{Z}$ be such that $3s + 22t = 1$ then equation (9) holds for $\alpha = \beta^s p^t$. □

From the proof of Theorem 3.3 it also follows that if the class number h_L of L and the degree $[L : \mathbb{Q}]$ are coprime then the norm equation

$$|N_{\mathbb{Q}}^L(\alpha)| = p^f, \quad \text{where } f \text{ is the residue degree of } p$$

is solvable for each prime p .

4. Concluding remarks

The purpose of this article is to convince the reader that the problem “whether prime ideals of residue degree bigger than one are well distributed across the ideal class group or not” is a useful problem. In general, we are not aware of any method to tackle this problem; the analytic methods which successfully tackle the distribution of prime ideals of residue degree one are limited to prime ideals of residue degree one.

From the two examples we made computations for, it is tempting to look for some relation between ‘ $\mathcal{R}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_t)} = \{1\}$ ’ and ‘ $h_{\mathbb{Q}}^+ = 1$ ’.

The study carried out here is in the spirit that ‘look at subfields of L to get information on L ’. Such studies has been carried out earlier too, for example see [13].

Acknowledgements

The author would like to express his gratitude to Prof. Dipendra Prasad for some very fruitful discussions, and making some corrections in earlier versions. We thank the referee for careful reading of the article.

References

- [1] V. Acciari, Solvability of norm equations over cyclic number fields of prime degree, *Mathematics of Computation*, **65** no. 216, (1996) 1663–1674.
- [2] Y. Bilu, Catalan’s conjecture (after Mihailescu), *Seminare Bourbaki* (2002–2003).
- [3] T. D. Browning and R. Newton, The proportion of failures of the Hasse norm principle, *Mathematika*, **62** no. 2, (2016) 337–347.
- [4] S. Dasgupta, Stark’s conjectures, B. A. (with Honors) thesis, Harvard university (1999).
- [5] C. Fieker, A. Jurk and M. Pohst, On solving relative norm equations in algebraic number fields, *Mathematics of Computation*, **66** no. 217, (1997) 399–410.
- [6] D. A. Garbanati, An algorithm for finding an algebraic number whose norm is a given rational number, *J. Reine Angew. Math.*, **316** (1980) 1–13.
- [7] G. J. Janusz, Algebraic number fields, second edition, Graduate Studies in Mathematics, American Mathematical Society, Vol. 7 (1996),
- [8] E. E. Kummer, Collected papers, Vol. I. Springer Verlag, Berlin 1975.
- [9] S. Lang, Cyclotomic fields 1 and 2, 2nd ed., *Grad. Texts in Math.*, Springer, New York, **123** (1990).
- [10] S. Lang, Algebraic number theory, 2nd ed., *Grad. Texts in Math.*, Springer, New York, **110** (1994).
- [11] H. W. Lenstra Jr. and P. Stevenhagen, Primes of degree one and algebraic cases of Chebotarev’s Theorem, *L’Enseignement Mathématique, t.*, **37** (1991) 17–30.
- [12] J. C. Miller, Class numbers of real cyclotomic fields of composite conductor, *LMS J. Comput. Math.*, suppl. A, **17** (2014) 404–417.
- [13] M. Rosen, Class groups in cyclic ℓ -extensions: comments on a paper by G. Cornell, *Proc. Amer. Math. Soc.*, **142** no. 1, (2014) 21–18.
- [14] J. W. Sands, Galois groups of exponent two and the Brumer-Stark conjecture, *J. Reine Angew. Math.*, **349** (1984) 129–135.
- [15] R. Schoof, Catalan’s conjecture, Universitext, Springer (2008).
- [16] John Tate, Brumer-Stark-Stickelberger, *Seminaire de Theorie des Nombres de Bordeaux*, **10** (1980–1981) 1–16.
- [17] L. C. Washington, Introduction to Cyclotomic fields, Second Edition, Springer (1991).