Kalyan Chakraborty
Azizul Hoque
Prem Prakash Pandey *Editors*

Class Groups of Number Fields and Related Topics

Springer

Class Groups of Number Fields and Related Topics

Kalyan Chakraborty · Azizul Hoque ·
Prem Prakash Pandey
Editors

Class Groups of Number Fields and Related Topics

Springer

Editors
Kalyan Chakraborty
School of Mathematics
Harish-Chandra Research Institute
Allahabad, Uttar Pradesh, India

Azizul Hoque
School of Mathematics
Harish-Chandra Research Institute
Allahabad, Uttar Pradesh, India

Prem Prakash Pandey
Department of Mathematics
IISER Berhampur
Berhampur, Odisha, India

ISBN 978-981-15-1513-2 ISBN 978-981-15-1514-9 (eBook)
https://doi.org/10.1007/978-981-15-1514-9

Mathematics Subject Classification (2010): 11Rxx, 11Sxx, 13C20

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

*To all concerned, who were responsible for
the successful completion of
ICCGNFRT-2017*

Preface

The number theory seminar has been organized, from January 20, 2017, by Algebraic/Algorithmic/Analytic Number Theory Seminar (ANTS) at Harish-Chandra Research Institute, Allahabad, India. This lecture series was started by Kalyan Chakraborty, Azizul Hoque and other members of the group. Prior to the existence of this group, we had decided to hold a series of three conferences on the theme ‘Class Groups of Number Fields and Related Topics.’ By October 2019, we had organized these three conferences. However, seeing its success and also on the request of all concerned, we have decided to continue this yearly conference.

The first ‘International Conference on Class Groups of Number Fields and Related Topics (ICCGNFRT)’ was held during September 4–7, 2017, at Harish-Chandra Research Institute, Allahabad, India.

This collection comprises original research papers and survey articles presented at ICCGNFRT-2017. There are 16 chapters on important topics in algebraic number theory and related parts of analytic number theory. These topics include class groups and class numbers of number fields, units, the Kummer–Vandiver conjecture, class number one problem, Diophantine equations, Thue equations, continued fractions, Euclidean number fields, heights, rational torsion points on elliptic curves, cyclotomic numbers, Jacobi sums and Dedekind zeta values.

We are grateful to Springer and its mathematics editor(s), especially Mr. Shamim Ahmad, for publishing this volume.

Allahabad, India
October 2019

Kalyan Chakraborty
Azizul Hoque
Prem Prakash Pandey

Contents

About the Editors

Kalyan Chakraborty is Professor at Harish-Chandra Research Institute (HRI), Allahabad, India, where he also obtained his Ph.D. in Mathematics. Professor Chakraborty was a postdoctoral fellow at IMSc, Chennai, and at Queen's University, Canada, and a visiting scholar at the University of Paris VI, VII, France; Tokyo Metropolitan University, Japan; Universitá Roma Tre, Italy; The University of Hong Kong, Hong Kong; Northwest University and Shandong University, China; Mahidol University, Thailand; Mandalay University, Myanmar; and many more. His broad area of research is number theory, particularly class groups, Diophantine equations, automorphic forms, arithmetic functions, elliptic curves, and special functions. He has published more than 60 research articles in respected journals and two books on number theory, and has been on the editorial boards of various leading journals. Professor Chakraborty is Vice-President of the Society for Special Functions and their Applications.

Azizul Hoque is a national postdoctoral fellow at Harish-Chandra Research Institute (HRI), Allahabad. He earned his Ph.D. in Pure Mathematics from Gauhati University, Guwahati, in 2015. Before joining HRI, Dr. Hoque was Assistant Professor at the Regional Institute of Science and Technology, Meghalaya, and at the University of Science and Technology, Meghalaya. He has visited Hong Kong University, Hong Kong; Northwest University, China; Shandong University, China; Mahidol University, Thailand; and many more. His research has mostly revolved around class groups, Diophantine equations, elliptic curves, zeta values, and related topics, and he has published a considerable number of papers in respected journals. He has been involved in a number of conferences and received numerous national and international grants.

Prem Prakash Pandey is Assistant Professor at the Indian Institute of Science Education and Research (IISER) Berhampur, Odisha. Before that, he was a postdoctoral fellow at HRI, Allahabad, and NISER Bhubaneswar, Odisha. After completing his Ph.D. at the Institute of Mathematical Sciences (IMSc), Chennai, he spent a couple of years at Chennai Mathematical Institute (CMI), Chennai, as a visiting scholar. Dr. Pandey's interests include class groups of number fields, annihilators of class groups, Diophantine equations, and related topics. During his time at HRI, he worked on divisibility problems for class numbers of quadratic fields with Dr. Hoque and Prof. Chakraborty.

Heights and Principal Ideals of Certain Cyclotomic Fields

René Schoof

1 Introduction

Any prime number l splits completely in the cyclotomic field $\mathbf{Q}(\zeta_{l-1})$. The primes lying over l all have norm l and are Galois conjugate. Consider the following set of prime numbers:

$$S = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 61, 67, 71\}.$$

In this expository note we give a self-contained proof of the following theorem

Theorem 1.1 *For a prime number l the following are equivalent.*

(i) $l \in S$;
(ii) *the class number of* $\mathbf{Q}(\zeta_{l-1})$ *is* 1;
(iii) *The prime ideals lying over* l *in* $\mathbf{Q}(\zeta_{l-1})$ *are principal.*

It is trivial that (ii) implies (iii). The fact that (i) implies (ii) is not trivial, but it is standard. In fact, using Odlyzko's [5] discriminant bounds, Masley and Montgomery [4] determined in the 1970's all cyclotomic fields with class number 1. See [7]. For proving that (i) implies (ii) one needs much less. We work this out in Sect. 3.

A proof of the fact that (iii) implies (i) was recently published by Bernat Plans [6]. It is an application of a theorem, proved in 2000 by Amoroso and Dvornicich [1], supplemented by computations by Hoshi [2]. In their paper, Amoroso and Dvornicich themselves already had used their theorem in a similar way proving that certain cyclcotomic fields have nontrivial class numbers. We prove a weak version of their theorem in Sect. 2.

Condition (iii) of Theorem 1.1 first came up in a 1974 paper by Lenstra [3] on a problem related to Noether's problem and the inverse problem of Galois theory.

R. Schoof (✉)
Dipartimento di Matematica, Università di Roma Tor Vergata, I-00133 Roma, Italy
e-mail: schoof.rene@gmail.com

K. Chakraborty et al. (eds.), *Class Groups of Number Fields and Related Topics*,
https://doi.org/10.1007/978-981-15-1514-9_8

Lenstra showed that the set of prime numbers satisfying the condition has Dirichlet density zero [3, , Cor.6.7].

We deduce Theorem 1.1 in Sect. 4 from the results in Sects. 2 and 3.

This note is based on an expository lecture given at the ICCGNFRT meeting at the HRI, Allahabad, September 2017.

2 Heights

We recall some basic properties of heights. For every finite or infinite prime v of a number field F, let $|x|_v$ denote the corresponding normalized valuation of $x \in F^*$. This means that for finite primes v we put $|x|_v = q^{-v(x)}$, where q is the cardinality of the residue field. For infinite real primes we use the usual absolute value and for complex primes its square.

Then the *product formula* holds: for every $x \in F^*$ we have

$$\prod_v |x|_v \;=\; 1.$$

For any positive real t we put $\log^+ t = \max(\log t, 0)$. The *height* $h(x)$ of $x \in F^*$ is defined as

$$h(x) \;=\; \sum_v \log^+ |x|_v.$$

Note that the value of $h(x)$ depends not only on x but also on the number field F. The *absolute height*

$$\frac{h(x)}{[F:\mathbf{Q}]}$$

is independent of F and depends only on x.

It is easy to see that for all $x, y \in F^*$ and every prime v we have

$$|x-y|_v \;\leq\; 2^{u_v} \max(1, |x|_v)\cdot \max(1, |y|_v),$$

where $u_v = 0$, 1 or 2, depending on whether v is finite, real or complex, respectively. Indeed, by symmetry we may assume that $|x|_v \geq |y|_v$. Then the triangle inequality implies that $|1-y/x|_v$ is at most 2^{u_v}. It follows that $|x-y|_v \;\leq\; 2^{u_v}|x|_v$ and the inequality follows.

Sharper upper bounds for $|x-y|_v$ give rise to lower bounds for the heights of either x or y.

Proposition 2.1 *Let F be a number field and let x and y be distinct elements of F^*. For every prime v, let $0 < c_v \leq 1$. If*

$$|x-y|_v \;\leq\; 2^{u_v} c_v \cdot \max(1, |x|_v)\cdot \max(1, |y|_v), \qquad \textit{for all primes } v.$$

Then

$$h(x) + h(y) \geq -[F : \mathbf{Q}] \log 2 - \sum_v \log c_v.$$

Proof By the product formula and the inequalities of the hypothesis we have

$$0 = \sum_v \log |x - y|_v \leq \sum_v \log(2^{u_v} c_v) + h(x) + h(y).$$

The result then follows from the fact that $\sum_v u_v = \sum_{v \text{ infinite}} u_v = [F : \mathbf{Q}]$.

The following lemma is used in the proof of the result by Amoroso and Dvornicich.

Lemma 2.2 *Let F be a number field, let v be a finite prime of F and let $\chi, \chi' : F^* \longrightarrow F^*$ be two homomorphisms that preserve v-integrality. Let $c \in \mathbf{R}_{>0}$. If we have*

$$|\chi(\alpha) - \chi'(\alpha)|_v \;\leq\; c, \qquad \textit{for all non-zero}\; \alpha \in O_F,$$

then

$$|\chi(\alpha) - \chi'(\alpha)|_v \;\leq\; c \cdot \max(1, |\chi(\alpha)_v) \cdot \max(1, |\chi'(\alpha)|_v), \qquad \textit{for all}\; \alpha \in F^*.$$

Proof Let $\alpha \in F^*$. By the Chinese remainder theorem, we can find an element $\beta \in O_F$ for which $\alpha\beta \in O_F$ and $|\beta|_v = \max(1, |\alpha|_v)^{-1}$. Since χ preserves v-integrality, this implies that $|\chi(\beta)|_v = \max(1, |\chi(\alpha)|_v)^{-1}$. From the identity

$$\chi(\alpha) - \chi'(\alpha) \;=\; \frac{1}{\chi(\beta)} \left(\chi(\alpha\beta) - \chi'(\alpha\beta) + \chi'(\alpha)\chi'(\beta) - \chi'(\alpha)\chi(\beta)\right),$$

we deduce the inequality

$$|\chi(\alpha) - \chi'(\alpha)|_v \;\leq\; \frac{c}{|\chi(\beta)|_v} \max(1, |\chi'(\alpha)|_v) \;=\; c \max(1, |\chi(\alpha)|_v) \max(1, |\chi'(\alpha)|_v),$$

as required.

Proposition 2.3 *(Amoroso and Dvornicich [1]) Let m be a positive integer and let ζ_m denote a primitive m-th root of unity. Suppose that $\alpha \in \mathbf{Q}(\zeta_m)^*$ is not a root of unity. Then for every prime number p we have*

$$\frac{h(\alpha)}{[F : \mathbf{Q}]} \geq \frac{\log(p/2)}{2p}.$$

If p does not divide m, we have the sharper estimate

$$\frac{h(\alpha)}{[F : \mathbf{Q}]} \geq \frac{\log(p/2)}{p + 1}.$$

Proof Put $F = \mathbf{Q}(\zeta_m)$. If p does not divide m, we apply Proposition 2.1 to $x = \alpha^p$, $y = \sigma(\alpha)$ and $c_v = |p|_v$ when v lies over p, while $c_v = 1$ for the other primes v. Here σ is the Frobenius automorphism in $\mathrm{Gal}(F/\mathbf{Q})$ of the primes lying over p. It fixes every v lying over p. Since $h(\alpha^p) = ph(\alpha)$ and $h(\sigma(\alpha)) = h(\alpha)$, the second estimate then follows.

It remains to check that $x = \alpha^p$, $y = \sigma(\alpha)$ satisfy the hypotheses of Proposition 2.1. Since α is not a root of unity, the elements x and y are distinct. In order to check the inequality in the condition of Proposition 2.1, we recall that the ring of integers of F is $\mathbf{Z}[\zeta_m]$. The fact that $\sigma(\zeta_m) = \zeta_m^p$, implies therefore that $\sigma(\alpha) \equiv \alpha^p \pmod{p}$ for all integral α. This implies that the inequality holds for integral $x = \sigma(\alpha)$ and $y = \alpha^p$. An application of Lemma 2.2 to the homomorphisms $\chi(\alpha) = \sigma(\alpha)$ and $\chi\prime(\alpha) = \alpha^p$ shows that it also holds for all $\alpha \in F^*$ and we are done.

If p divides m, we we apply Proposition 2.1 to $x = \alpha^p$, $y = \sigma(\alpha)^p$ and and $c_v = |p|_v$ when v lies over p, while $c_v = 1$ for the other primes v. Here σ generates the Galois group of F over its subfield $\mathbf{Q}(\zeta_{m/p})$. The first inequality follows readily.

It remains to check the hypotheses of Proposition 2.1. Since σ fixes $\mathbf{Q}(\zeta_{m/p})$, we have $\sigma(\zeta_m) = \zeta_m^t$ for some $t \equiv 1 \pmod{m/p}$. It follows that $\sigma(\zeta_m)^p = \zeta_m^p$ and hence $\sigma(\alpha)^p \equiv \alpha^p \pmod{p}$ for all $\alpha \in \mathbf{Z}[\zeta_m]$. In other words, the inequality in the hypothesis of Proposition 2.1 holds for $x = \sigma(\alpha)^p$ and $y = \alpha^p$ for every integral $\alpha \in F$. An application of Lemma 2.2 to the homomorphisms $\chi(\alpha) = \sigma(\alpha)^p$ and $\chi\prime(\alpha) = \alpha^p$ shows that the inequality holds for all $\alpha \in F^*$.

Finally, if x and y were equal, then $\alpha = \sigma(\alpha)\zeta'$ for some $\zeta' \in \mu_p$. The kernel of the homomorphism $\mu_m \longrightarrow \mu_m$ given by $\xi \mapsto \sigma(\xi)/\xi = \xi^{t-1}$, is $\mu_{m/p}$. Therefore the image is μ_p. It follows that $\zeta' = \sigma(\xi)/\xi$ for some $\xi \in \mu_m$. This means that $\xi\alpha$ is fixed by σ and is hence contained in the subfield $\mathbf{Q}(\zeta_{m/p})$. Since α and $\xi\alpha$ have the same height, we may replace α by $\xi\alpha$ and $F = \mathbf{Q}(\zeta_m)$ by $\mathbf{Q}(\zeta_{m/p})$. We repeat this until either $x \neq y$, in which case all conditions of Proposition 1 are satisfied, or until p does not divide m, in which case we have the sharper estimate that we already proved.

Corollary 2.4 *Let l be a prime number and suppose that the prime ideals of $\mathbf{Q}(\zeta_{l-1})$ lying over l are principal. Then we have*

$$\frac{\log l}{\phi(\ell - 1)} \geq \frac{\log(5/2)}{10},$$

where ϕ is Euler's function. Moreover, for any prime p for which $l \not\equiv 1 \pmod{p}$, we have

$$\frac{\log l}{\phi(\ell - 1)} \geq \frac{\log(p/2)}{p+1}.$$

Proof We put $F = \mathbf{Q}(\zeta_{l-1})$ and, as in [1, Cor.1], we put $\alpha = \overline{\pi}/\pi$, where π is a generator of a prime of F lying over l. Since l splits completely in F, the quotient $\overline{\pi}/\pi = \alpha$ is not a root of unity. Since $h(\alpha) = \log l$, an application of Proposition 2.3 implies the result.

Remark 2.5 For $p = 2$, the bounds of Proposition 2.3 are trivial. However, one can obtain nontrivial bounds by observing that for $\alpha \in \mathbf{Z}[\zeta_m]$ one has $\sigma(\alpha)^2 \equiv \alpha^4 \pmod 4$ when $m \not\equiv 0 \pmod 4$ and σ is the Frobenius automorphism of the primes lying over 2. When $m \equiv 0 \pmod 4$ and σ is the automorphism of $\mathbf{Q}(\zeta_m)$ for which $\sigma(\zeta_m) = \zeta_m^{1+m/2} = -\zeta_m$, one has $\sigma(\alpha)^2 \equiv \alpha^2 \pmod 4$. This leads to the inequality

$$\frac{h(\alpha)}{[F:\mathbf{Q}]} \geq \frac{\log(2)}{6},$$

for all m and all $\alpha \in \mathbf{Q}(\zeta_m)^*$ that are not a root of unity.

Remark 2.6 In the proof of Proposition 2.3 of the case where p divides m, one may actually take $c_v = |p|_v^{p/(p-1)}$ for the primes v lying over p. This is slightly smaller and gives a better estimate in Corollary 2.4. It makes little difference for the proof of Theorem 1.1.

3 Discriminant Bounds

In this section, we explain how to prove the implication (i) ⇒ (ii) of the main theorem. We use Odlyzko's discriminant bounds [5].

In general, the class number of a cyclotomic field $\mathbf{Q}(\zeta_m)$ is the product of the class number of the maximal real subfield $\mathbf{Q}(\zeta_m)^+$ of $\mathbf{Q}(\zeta_m)$ and the so-called *relative class number*. The latter is a product of generalized Bernoulli numers and is easy to compute [7, Theorem 4.17]. It is an easy matter to check that for the primes in the set S of Theorem 1.1, the relative class numbers of $\mathbf{Q}(\zeta_{l-1})$ are all equal to 1. This is left to the reader, who may prefer to consult the table in [7, p.412]. To show that the class numbers themselves are also 1, it suffices to show that the class numbers of the subfields $\mathbf{Q}(\zeta_m)^+$ are 1.

The absolute degree of $\mathbf{Q}(\zeta_m)$ over $\mathbf{Q}$ is $\phi(m)$. The root discriminant δ_m of $\mathbf{Q}(\zeta_m)$ is the $\phi(m)$-th root of the absolute value of its discriminant. Explicitly, δ_m is equal to $m \prod_p p^{-1/(p-1)}$, where the product runs over the prime divisors of m. See [7, Proposition 2.7]. For $m > 2$, the subfield $\mathbf{Q}(\zeta_m)^+$ has absolute degree $\frac{1}{2}\phi(m)$, while its root discriminant is at most δ_m.

Consider the set S of primes of Theorem 1.1. For the primes $l = 2, 3, 5, 7, 11$ and 13, the field $\mathbf{Q}(\zeta_{l-1})^+$ is either $\mathbf{Q}$ or one of the quadratic fields $\mathbf{Q}(\sqrt{3})$ or $\mathbf{Q}(\sqrt{5})$. It is well known and easy to verify that the class numbers of these fields are equal to 1. This leaves us with the primes $l = 17, 19, 23, 29, 31, 37, 41, 43, 61, 67$ and 71.

In Table 1 we list the degrees and root discriminants of these fields.

The root discriminant of any totally real number of degree d is bounded below by Odlyzko's discriminant bound Odl(d). See [7, , 11.4]. The function Odl$((d)$ is monotonically increasing. For degree $d \leq 14$, we list its values, or rather approximations to them, in Table 2. See also [5].

Table 1 Degrees and root discriminants of $\mathbf{Q}(\zeta_{l-1})$

l	$\phi(l-1)$	δ_{l-1}		l	$\phi(l-1)$	δ_{l-1}
17	8	8.000		41	16	13.375
19	6	5.197		43	12	8.767
23	10	8.655		61	16	11.583
29	12	10.123		67	20	14.991
31	8	5.792		71	24	16.923
37	12	10.393				

Table 2 Odlyzko's bounds

d	Odl(d)		d	Odl(d)		d	Odl(d)		d	Odl(d)
1	0.996		5	6.514		9	11.787		13	16.044
2	2.222		6	7.926		10	12.941		14	16.971
3	3.609		7	9.279		11	14.034			
4	5.062		8	10.568		12	15.068			

The Hilbert class field of $\mathbf{Q}(\zeta_{l-1})^+$ is totally real. Its degree over $\mathbf{Q}(\zeta_{l-1})^+$ is equal to the class number of $\mathbf{Q}(\zeta_{l-1})^+$. Since it is an everywhere unramified extension of $\mathbf{Q}(\zeta_{l-1})^+$, its root discriminant is equal to the root discriminant of $\mathbf{Q}(\zeta_{l-1})^+$, which is at most δ_{l-1}. Therefore, we can use Odlyzko's bounds to bound the class number h of $\mathbf{Q}(\zeta_{l-1})^+$. To be precise, we have

$$h\phi(l-1)/2 < d,$$

for any d for which Odl(d) exceeds δ_{l-1}. It follows easily from the entries in the two tables that $h < 2$ in each case. For instance, for $l = 71$, we have $\delta_{l-1} = 16.923\ldots$. Since Odl$(14) = 16.971$, we may take $d = 14$ and we find that $h \cdot \frac{1}{2} \cdot 24 < 14$.

This implies that for the primes in the set S of Theorem 1.1, the class numbers of $\mathbf{Q}(\zeta_{l-1})^+$ are equal to 1, as required.

4 Plans' Theorem

In this section, we prove the implication (iii) ⇒ (i) of Theorem 1.1.

The degree $[\mathbf{Q}(\zeta_{l-1} : \mathbf{Q}] = \phi(l-1)$ grows faster than $\log l$. In fact, it is easy to prove that $\phi(l-1) \geq \sqrt{(l-1)/2}$. Therefore the first inequality of Corollary 2.4 can only hold for finitely many primes. It is not difficult to check that the prime numbers l that satisfy the first inequality of Corollary 2.4 are necessarily ≤ 211. An application of the second inequality of Corollary 2.4 with the primes $p \leq 11$ reduces this bound to 79 and excludes $l = 59$. The only primes not in S are $l = 47, 53, 73$ and 79. The relevant cyclotomic fields are $\mathbf{Q}(\zeta_m)$ with $m = 23, 52, 72$ and 39, respectively. We deal with them one by one.

The equation $x^2 + 23y^2 = 4 \cdot 47$ has no solutions in integers. This implies that there is no element of norm 47 in the ring of integers of the quadratic subfield $\mathbf{Q}(\sqrt{-23})$ of $\mathbf{Q}(\zeta_{23})$. This means that the prime ideals over 47 of $\mathbf{Q}(\sqrt{-23})$ are not principal. It follows that the prime ideals over 47 of $\mathbf{Q}(\zeta_{23})$ are not principal either. Similarly, the equation $x^2 + 39y^2 = 4 \cdot 79$ has no solutions in integers. It follows that the prime ideals over 79 of $\mathbf{Q}(\zeta_{39})$ are not principal.

Since the image of the local norm map $\mathbf{Z}_{13}[\zeta_{13}]^* \longrightarrow \mathbf{Z}_{13}^*$ is the group $1 + 13\mathbf{Z}_{13}$, the norm map from $\mathbf{Q}(\zeta_{52})$ to $\mathbf{Q}(i)$ maps numbers that are units at the primes lying over 13 to elements of $\mathbf{Q}(i)^*$ that are congruent to $1 \pmod{13}$. Therefore, the norm map from the class group Cl_{52} of $\mathbf{Q}(\zeta_{52})$ to the (trivial) class group of $\mathbf{Q}(i)$ 'factors' through the ray class group of conductor 13 of $\mathbf{Q}(i)$. In other words, the norm induces a homomorphism

$$N : Cl_{52} \longrightarrow (\mathbf{Z}[i]/(13))^*/\langle i \rangle.$$

It maps the class of an ideal I of $\mathbf{Z}[\zeta_{52}]$ that is prime to 13, to a generator of the ideal $N(I)$ of $\mathbf{Z}[i]$. In particular, any prime of $\mathbf{Z}[\zeta_{52}]$ lying over 53 is mapped to the image of $7 \pm 2i$ in the ray class group. Since $7 \pm 2i$ has order 3 in the group $(\mathbf{Z}[i]/(13))^*/\langle i \rangle$, this image is nontrivial. Therefore the class in Cl_{52} of a prime lying over 53 is not trivial either. It follows that the primes over 53 in $\mathbf{Q}(\zeta_{52})$ are not principal.

Similarly, the image of the local norm map $\mathbf{Z}_3[\zeta_9]^* \longrightarrow \mathbf{Z}_3^*$ is the group $1 + 9\mathbf{Z}_3$. Therefore, the norm map from $\mathbf{Q}(\zeta_{72})$ to $\mathbf{Q}(\sqrt{-2})$ maps numbers that are units at the primes lying over 3 to elements of $\mathbf{Q}(\sqrt{-2})^*$ that are congruent to $1 \pmod{9}$. It follows that the norm maps the class group Cl_{72} of $\mathbf{Q}(\zeta_{72})$ to the ray class group of conductor 9 of $\mathbf{Q}(\sqrt{-2})$. In other words, the norm induces a homomorphism

$$N : Cl_{72} \longrightarrow (\mathbf{Z}[\sqrt{-2}]/(9))^*/\{\pm 1\}.$$

It maps the class of any prime over 73 to the image of $1 \pm 6\sqrt{-2}$ in the ray class group. Since $1 \pm 6\sqrt{-2}$ has order 3 in the group $(\mathbf{Z}[\sqrt{-2}]/(9))^*/\{\pm 1\}$, this image is nontrivial. Therefore the class in Cl_{72} of a prime lying over 73 is not trivial either.

This proves Theorem 1.1.

References

1. F. Amoroso, R. Dvornicich, A lower bound for the height in abelian extensions. J. Number Theory **80**, 260–272 (2000)
2. A. Hoshi, On Noether's problem for cyclic groups of prime order. Proc. Japan Acad. Ser. A **91**, 39–44 (2015)
3. H.W. Lenstra, Rational functions invariant under an abelian group. Invent. Math. **25**, 299–325 (1974)

4. J. Masley, H. Montgomery, Cyclotomic fields with unique factorization. J. Reine Angew. Math. **286**(287), 248–256 (1976)
5. A. Odlyzko, Table 2. Unconditional bounds for discriminants, 29 Nov 1976. http://www.dtc.umn.edu/~odlyzko/unpublished/discr.bound.table2
6. B. Plans, On Noether's rationality problem for cyclic groups over Q. Proc. AMS **145**, 2407–2409 (2016)
7. L.C. Washington, *Introduction to Cyclotomic Fields, Graduate Texts in Math*, vol. 83, 2nd edn. (Springer-Verlag 1997)