THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

Imaginary quadratic fields with isomorphic abelian Galois groups

Athanasios Angelakis and Peter Stevenhagen

msp

THE OPEN BOOK SERIES **1** (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.21

msp

Imaginary quadratic fields with isomorphic abelian Galois groups

Athanasios Angelakis and Peter Stevenhagen

In 1976, Onabe discovered that, in contrast to the Neukirch-Uchida results that were proved around the same time, a number field K is not completely characterized by its absolute abelian Galois group A_K. The first examples of nonisomorphic K having isomorphic A_K were obtained on the basis of a classification by Kubota of idele class character groups in terms of their infinite families of Ulm invariants, and did not yield a description of A_K. In this paper, we provide a direct "computation" of the profinite group A_K for imaginary quadratic K, and use it to obtain *many* different K that all have the *same minimal* absolute abelian Galois group.

1. Introduction

The absolute Galois group G_K of a number field K is a large profinite group that we cannot currently describe in very precise terms. This makes it impossible to answer fundamental questions on G_K, such as the inverse Galois problem over K. Still, Neukirch [7] proved that normal number fields are completely characterized by their absolute Galois groups: If G_{K_1} and G_{K_2} are isomorphic as topological groups, then K_1 and K_2 are isomorphic number fields. The result was refined by Ikeda, Iwasawa, and Uchida ([8], [9, Chapter XII, §2]), who disposed of the restriction to normal number fields, and showed that every topological isomorphism $G_{K_1} \xrightarrow{\sim} G_{K_2}$ is actually induced by an inner automorphism of $G_{\mathbb{Q}}$. The same statements hold if all absolute Galois groups are replaced by their maximal *prosolvable* quotients.

It was discovered by Onabe [10] that the situation changes if one moves a further step down from G_K, to its maximal *abelian* quotient $A_K = G_K/\overline{[G_K, G_K]}$, which is the Galois group $A_K = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ of the maximal abelian extension K^{ab} of K.

MSC2010: primary 11R37; secondary 20K35.
Keywords: absolute Galois group, class field theory, group extensions.

Even though the Hilbert problem of explicitly generating K^{ab} for general number fields K is still open after more than a century, the group A_K can be described by class field theory, as a quotient of the idele class group of K.

Kubota [5] studied the group X_K of continuous characters on A_K, and expressed the structure of the p-primary parts of this countable abelian torsion group in terms of an infinite number of so-called *Ulm invariants*. It had been shown by Kaplansky [4, Theorem 14] that such invariants determine the isomorphism type of a countable reduced abelian torsion group. Onabe computed the Ulm invariants of X_K explicitly for a number of small imaginary quadratic fields K, and concluded from this that there exist nonisomorphic imaginary quadratic fields K and K' for which the absolute abelian Galois groups A_K and $A_{K'}$ are isomorphic as profinite groups. This may even happen in cases where K and K' have different class numbers, but the explicit example $K = \mathbb{Q}(\sqrt{-2})$, $K' = \mathbb{Q}(\sqrt{-5})$ of this that occurs in Onabe's main theorem [10, Theorem 2] is incorrect. This is because the value of the finite Ulm invariants in [5, Theorem 4] is incorrect for the prime 2 in case the ground field is a special number field in the sense of our Lemma 3.2. As it happens, $\mathbb{Q}(\sqrt{-5})$ and the exceptional field $\mathbb{Q}(\sqrt{-2})$ do have different Ulm invariants at 2. The nature of Kubota's error is similar to an error in Grunwald's theorem that was corrected by a theorem of Wang occurring in Kubota's paper [5, Theorem 1]. It is related to the noncyclic nature of the 2-power cyclotomic extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_{2^\infty})$.

In this paper, we obtain Onabe's corrected results by a direct class field theoretic approach that completely avoids Kubota's dualization and the machinery of Ulm invariants. We show that the imaginary quadratic fields $K \neq \mathbb{Q}(\sqrt{-2})$ that are said to be of 'type A' in [10] share a *minimal* absolute abelian Galois group that can be described completely explicitly as

$$A_K = \widehat{\mathbb{Z}}^2 \times \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}.$$

The numerical data that we present suggest that these fields are in fact very common among imaginary quadratic fields: More than 97% of the 2356 fields of odd prime class number $h_K = p < 100$ are of this nature. We believe (Conjecture 7.1) that there are actually *infinitely many* K for which A_K is the minimal group above. Our belief is supported by certain reasonable assumptions on the average splitting behavior of exact sequences of abelian groups, and these assumptions are tested numerically in the final section of the paper.

2. Galois groups as $\widehat{\mathbb{Z}}$-modules

The profinite abelian Galois groups that we study in this paper naturally come with a topology for which the identity has a basis of open neighborhoods that are open subgroups of finite index. This implies that they are not simply $\mathbb{Z}$-modules, but that

the exponentiation in these groups with ordinary integers extends to exponentiation with elements of the profinite completion $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Z}$. By the Chinese remainder theorem, we have a decomposition of the profinite ring $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ into a product of rings of p-adic integers, with the index p ranging over all primes. As $\widehat{\mathbb{Z}}$-modules, our Galois groups decompose correspondingly as a product of pro-p-groups.

It is instructive to look first at the $\widehat{\mathbb{Z}}$-module structure of the absolute abelian Galois group $A_{\mathbb{Q}}$ of $\mathbb{Q}$, which we know very explicitly by the Kronecker-Weber theorem. This theorem states that $\mathbb{Q}^{\mathrm{ab}}$ is the maximal cyclotomic extension of $\mathbb{Q}$, and that an element $\sigma \in A_{\mathbb{Q}}$ acts on the roots of unity that generate $\mathbb{Q}^{\mathrm{ab}}$ by exponentiation. More precisely, we have $\sigma(\zeta) = \zeta^u$ for all roots of unity, with u a uniquely defined element in the unit group $\widehat{\mathbb{Z}}^*$ of the ring $\widehat{\mathbb{Z}}$. This yields the well-known isomorphism $A_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^* = \prod_p \mathbb{Z}_p^*$.

For odd p, the group $\mathbb{Z}_p^*$ consists of a finite torsion subgroup T_p of $(p-1)$-st roots of unity, and we have an isomorphism

$$\mathbb{Z}_p^* = T_p \times (1 + p\mathbb{Z}_p) \cong T_p \times \mathbb{Z}_p$$

because $1 + p\mathbb{Z}_p$ is a free $\mathbb{Z}_p$-module generated by $1 + p$. For $p = 2$ the same is true with $T_2 = \{\pm 1\}$ and $1 + 4\mathbb{Z}_2$ the free $\mathbb{Z}_2$-module generated by $1 + 4 = 5$. Taking the product over all p, we obtain

$$A_{\mathbb{Q}} \cong T_{\mathbb{Q}} \times \widehat{\mathbb{Z}}, \tag{1}$$

with $T_{\mathbb{Q}} = \prod_p T_p$ the product of the torsion subgroups $T_p \subset \mathbb{Q}_p^*$ of the multiplicative groups of the completions $\mathbb{Q}_p$ of $\mathbb{Q}$. More canonically, $T_{\mathbb{Q}}$ is the *closure* of the torsion subgroup of $A_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$, and $A_{\mathbb{Q}}/T_{\mathbb{Q}}$ is a free $\widehat{\mathbb{Z}}$-module of rank 1. The invariant field of $T_{\mathbb{Q}}$ inside $\mathbb{Q}^{\mathrm{ab}}$ is the unique $\widehat{\mathbb{Z}}$-extension of $\mathbb{Q}$.

Even though it looks at first sight as if the isomorphism type of $T_{\mathbb{Q}}$ depends on the properties of prime numbers, one should realize that in an infinite product of finite cyclic groups, the Chinese remainder theorem allows us to rearrange factors in many different ways. One has for instance a noncanonical isomorphism

$$T_{\mathbb{Q}} = \prod_p T_p \cong \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}, \tag{2}$$

as both of these products, when written as a countable product of cyclic groups of prime power order, have an infinite number of factors $\mathbb{Z}/\ell^k\mathbb{Z}$ for each prime power ℓ^k. Note that, for the product $\prod_p T_p$ of cyclic groups of order $p-1$ (for $p \neq 2$), this statement is not completely trivial: It follows from the existence, by the well-known theorem of Dirichlet, of infinitely many primes p that are congruent to 1 mod ℓ^k, but not to 1 mod ℓ^{k+1}.

Now suppose that K is an arbitrary number field, with ring of integers $\mathbb{O}$. By class field theory, A_K is the quotient of the idele class group $C_K = \left(\prod'_{\mathfrak{p}\leq\infty} K_{\mathfrak{p}}^*\right)/K^*$ of K by the connected component of the identity. In the case of imaginary quadratic fields K, this connected component is the subgroup $K_\infty^* = \mathbb{C}^* \subset C_K$ coming from the unique infinite prime of K, and in this case the Artin isomorphism for the absolute abelian Galois group A_K of K reads

$$A_K = \widehat{K}^*/K^* = \Big(\prod_{\mathfrak{p}}{}' K_{\mathfrak{p}}^*\Big)/K^*. \tag{3}$$

Here $\widehat{K}^* = \prod'_{\mathfrak{p}} K_{\mathfrak{p}}^*$ is the group of *finite* ideles of K, that is, the restricted direct product of the groups $K_{\mathfrak{p}}^*$ at the finite primes $\mathfrak{p}$ of K, taken with respect to the unit groups $\mathbb{O}_{\mathfrak{p}}^*$ of the local rings of integers. For the purposes of this paper, which tries to describe A_K as a profinite abelian group, it is convenient to treat the isomorphism for A_K in (3) as an identity — as we have written it down.

The expression (3) is somewhat more involved than the corresponding identity $A_{\mathbb{Q}} = \widehat{\mathbb{Z}}^*$ for the rational number field, but we will show in Lemma 3.2 that the *inertial part* of A_K, that is, the subgroup $U_K \subset A_K$ generated by all inertia groups $\mathbb{O}_{\mathfrak{p}}^* \subset C_K$, admits a description very similar to (1).

Denote by $\widehat{\mathbb{O}} = \prod_{\mathfrak{p}} \mathbb{O}_{\mathfrak{p}}$ the profinite completion of the ring of integers $\mathbb{O}$ of K. In the case that K is imaginary quadratic, the inertial part of A_K takes the form

$$U_K = \Big(\prod_{\mathfrak{p}} \mathbb{O}_{\mathfrak{p}}^*\Big)/\mathbb{O}^* = \widehat{\mathbb{O}}^*/\mu_K, \tag{4}$$

since the unit group $\mathbb{O}^*$ of $\mathbb{O}$ is then equal to the group μ_K of roots of unity in K. Apart from the quadratic fields of discriminant -3 and -4, which have 6 and 4 roots of unity, respectively, we always have $\mu_K = \{\pm 1\}$, and (4) can be viewed as the analogue for K of the group $\widehat{\mathbb{Z}}^* = A_{\mathbb{Q}}$.

In the next section, we determine the structure of the group $\widehat{\mathbb{O}}^*/\mu_K$. As the approach works for any number field, we will not assume that K is imaginary quadratic until the very end of that section.

3. Structure of the inertial part

Let K be any number field, and $\widehat{\mathbb{O}} = \prod_{\mathfrak{p}} \mathbb{O}_{\mathfrak{p}}$ the profinite completion of its ring of integers. Denote by $T_{\mathfrak{p}} \subset \mathbb{O}_{\mathfrak{p}}^*$ the subgroup of local roots of unity in $K_{\mathfrak{p}}^*$, and put

$$T_K = \prod_{\mathfrak{p}} T_{\mathfrak{p}} \subset \prod_{\mathfrak{p}} \mathbb{O}_{\mathfrak{p}}^* = \widehat{\mathbb{O}}^*. \tag{5}$$

The analogue of (1) for K is the following.

Lemma 3.1. *The closure of the torsion subgroup of* $\widehat{\mathbb{O}}^*$ *is equal to* T_K, *and* $\widehat{\mathbb{O}}^*/T_K$ *is a free* $\widehat{\mathbb{Z}}$*-module of rank* $[K:\mathbb{Q}]$. *Less canonically, we have an isomorphism*

$$\widehat{\mathbb{O}}^* \cong T_K \times \widehat{\mathbb{Z}}^{[K:\mathbb{Q}]}.$$

Proof. As the finite torsion subgroup $T_\mathfrak{p} \subset \mathbb{O}_\mathfrak{p}^*$ is closed in $\mathbb{O}_\mathfrak{p}^*$, the first statement follows from the definition of the product topology on $\widehat{\mathbb{O}}^* = \prod_\mathfrak{p} \mathbb{O}_\mathfrak{p}^*$.

Reduction modulo $\mathfrak{p}$ in the local unit group $\mathbb{O}_\mathfrak{p}^*$ gives rise to an exact sequence

$$1 \longrightarrow 1+\mathfrak{p} \longrightarrow \mathbb{O}_\mathfrak{p}^* \longrightarrow k_\mathfrak{p}^* \longrightarrow 1$$

that can be split by mapping the elements of the unit group $k_\mathfrak{p}^*$ of the residue class field to their Teichmüller representatives in $\mathbb{O}_\mathfrak{p}^*$. These form the cyclic group of order $\#k_\mathfrak{p}^* = N\mathfrak{p} - 1$ in $T_\mathfrak{p}$ consisting of the elements of order coprime to $p = \mathrm{char}(k_\mathfrak{p})$. The kernel of reduction $1+\mathfrak{p}$ is by [3, one-unit theorem, p. 231] a finitely generated $\mathbb{Z}_p$-module of free rank $[K_\mathfrak{p}:\mathbb{Q}_p]$ having a finite torsion group consisting of roots of unity in $T_\mathfrak{p}$ of p-power order. Combining these facts, we find that $\mathbb{O}_\mathfrak{p}^*/T_\mathfrak{p}$ is free over $\mathbb{Z}_p$ of rank $[K_\mathfrak{p}:\mathbb{Q}_p]$ or, less canonically, that we have a local isomorphism

$$\mathbb{O}_\mathfrak{p}^* \cong T_\mathfrak{p} \times \mathbb{Z}_p^{[K_\mathfrak{p}:\mathbb{Q}_p]}$$

for each prime $\mathfrak{p}$. Taking the product over all $\mathfrak{p}$, and using the fact that the sum of the local degrees at p equals the global degree $[K:\mathbb{Q}]$, we obtain the desired global conclusion. □

In order to derive a characterization of $T_K = \prod_\mathfrak{p} T_\mathfrak{p}$ for arbitrary number fields K similar to (2), we observe that we have an exact divisibility $\ell^k \parallel \#T_\mathfrak{p}$ of the order of $T_\mathfrak{p}$ by a prime power ℓ^k if and only if the local field $K_\mathfrak{p}$ at $\mathfrak{p}$ contains a primitive ℓ^k-th root of unity, but *not* a primitive ℓ^{k+1}-th root of unity. We may reword this as: The prime $\mathfrak{p}$ splits completely in the cyclotomic extension $K \subset K(\zeta_{\ell^k})$, but *not* in the cyclotomic extension $K \subset K(\zeta_{\ell^{k+1}})$. If such $\mathfrak{p}$ exist at all for ℓ^k, then there are infinitely many of them, by the Chebotarev density theorem.

Thus, T_K can be written as a product of groups $(\mathbb{Z}/\ell^k\mathbb{Z})^\mathbb{Z} = \mathrm{Map}(\mathbb{Z}, \mathbb{Z}/\ell^k\mathbb{Z})$ that are themselves countable products of cyclic groups of order ℓ^k. The prime powers $\ell^k > 1$ that occur for K are *all* but those for which we have an equality

$$K(\zeta_{\ell^k}) = K(\zeta_{\ell^{k+1}}).$$

For $K = \mathbb{Q}$ all prime powers ℓ^k occur, but for general K, there are finitely many prime powers that may disappear. This is due to the fact that the infinite cyclotomic extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_{\ell^\infty})$ with group $\mathbb{Z}_\ell^*$ can partially "collapse" over K.

To describe the exceptional prime powers ℓ^k that disappear for K, we consider, for ℓ an *odd* prime, the number

$$w(\ell) = w_K(\ell) = \#\mu_{\ell^\infty}(K(\zeta_\ell))$$

of ℓ-power roots of unity in the field $K(\zeta_\ell)$. For almost all ℓ, this number equals ℓ, and we call ℓ *exceptional* for K if it is divisible by ℓ^2. Note that no odd exceptional prime numbers exist for imaginary quadratic fields K.

For the prime $\ell = 2$, we consider instead the number

$$w(2) = w_K(2) = \#\mu_{2^\infty}(K(\zeta_4))$$

of 2-power roots in $K(\zeta_4) = K(i)$. If K contains $i = \zeta_4$, or if $w(2)$ is divisible by 8, we call 2 *exceptional* for K. Note that the only imaginary quadratic fields K for which 2 is exceptional are $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-2})$.

The number $w(K)$ of *exceptional roots of unity* for K is now defined as

$$w(K) = \prod_{\ell \text{ exceptional}} w(\ell).$$

Note that $w(K)$ refers to roots of unity that may or may not be contained in K itself, and that every prime ℓ dividing $w(K)$ occurs with exponent at least 2. The prime powers $\ell^k > 1$ that do *not* occur when T_K is written as a direct product of groups $(\mathbb{Z}/\ell^k\mathbb{Z})^{\mathbb{Z}}$ are the *strict* divisors of $w(\ell)$ at exceptional primes ℓ, with the exceptional prime $\ell = 2$ giving rise to a special case.

Lemma 3.2. *Let K be a number field, and $w = w(K)$ its number of exceptional roots of unity. Then we have a noncanonical isomorphism of profinite groups*

$$T_K = \prod_{\mathfrak{p}} T_{\mathfrak{p}} \cong \prod_{n \geq 1} \mathbb{Z}/nw\mathbb{Z},$$

except when 2 is exceptional for K and $i = \zeta_4$ is not contained in K. In this special case, we have

$$T_K = \prod_{\mathfrak{p}} T_{\mathfrak{p}} \cong \prod_{n \geq 1} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/nw\mathbb{Z}).$$

The group T_K is isomorphic to the group $T_{\mathbb{Q}}$ in (2) *if and only if we have $w = 1$.*

Proof. If ℓ is odd, the tower of field extensions

$$K(\zeta_\ell) \subset K(\zeta_{\ell^2}) \subset \cdots \subset K(\zeta_{\ell^k}) \subset K(\zeta_{\ell^{k+1}}) \subset \cdots$$

is a $\mathbb{Z}_\ell$-extension, and the steps $K(\zeta_{\ell^k}) \subset K(\zeta_{\ell^{k+1}})$ with $k \geq 1$ in this tower that are equalities are exactly those for which ℓ^{k+1} divides $w(\ell)$.

Similarly, the tower of field extensions

$$K(\zeta_4) \subset K(\zeta_8) \subset \cdots \subset K(\zeta_{2^k}) \subset K(\zeta_{2^{k+1}}) \subset \cdots$$

is a $\mathbb{Z}_2$-extension in which the steps $K(\zeta_{2^k}) \subset K(\zeta_{2^{k+1}})$ with $k \geq 2$ that are equalities are exactly those for which 2^{k+1} divides $w(2)$. The extension $K = K(\zeta_2) \subset K(\zeta_4)$ that we have in the remaining case $k = 1$ is an equality if and only if K contains $i = \zeta_4$.

Thus, a prime power $\ell^k > 2$ that does not occur when T_K is written as a product of groups $(\mathbb{Z}/\ell^k\mathbb{Z})^{\mathbb{Z}}$ is the same as a *strict* divisor $\ell^k > 2$ of $w(\ell)$ at an exceptional prime ℓ. The special prime power $\ell^k = 2$ does not occur if and only if $i = \zeta_4$ is in K. Note that in this case, 2 is by definition exceptional for K.

It is clear that replacing the group $\prod_{n\geq 1} \mathbb{Z}/n\mathbb{Z}$ from (2) by $\prod_{n\geq 1} \mathbb{Z}/nw\mathbb{Z}$ has the effect of removing cyclic summands of order ℓ^k with $\ell^{k+1} \mid w$, and this shows that the groups given in the Lemma are indeed isomorphic to T_K. Only for $w = 1$ we obtain the group $T_{\mathbb{Q}}$ in which all prime powers ℓ^k arise. □

Lemmas 3.1 and 3.2 tell us what $\widehat{\mathbb{O}}^*$ looks like as a $\widehat{\mathbb{Z}}$-module. In particular, it shows that the dependence on K is limited to the degree $[K : \mathbb{Q}]$, which is reflected in the rank of the free $\widehat{\mathbb{Z}}$-part of $\widehat{\mathbb{O}}^*$, and the nature of the exceptional roots of unity for K. For the group $\widehat{\mathbb{O}}^*/\mu_K$, the same is true, but the proof requires an extra argument, and the following lemma.

Lemma 3.3. *There are infinitely many primes* $\mathfrak{p}$ *of* K *for which we have*

$$\gcd(\#\mu_K, \#T_{\mathfrak{p}}/\#\mu_K) = 1.$$

Proof. For every prime power $\ell^k > 1$ that exactly divides $\#\mu_K$, the extension $K = K(\zeta_{\ell^k}) \subset K(\zeta_{\ell^{k+1}})$ is a cyclic extension of prime degree ℓ. For different prime powers $\ell^k \parallel \#\mu_K$, we get different extensions, so infinitely many primes $\mathfrak{p}$ of K are inert in all of them. For such $\mathfrak{p}$, we have $\gcd(\#\mu_K, \#T_{\mathfrak{p}}/\#\mu_K) = 1$. □

Lemma 3.4. *We have a noncanonical isomorphism* $T_K/\mu_K \cong T_K$.

Proof. Pick a prime $\mathfrak{p}_0$ of K that satisfies the conditions of Lemma 3.3. Then μ_K embeds as a direct summand in $T_{\mathfrak{p}_0}$, and we can write $T_{\mathfrak{p}_0} \cong \mu_K \times T_{\mathfrak{p}_0}/\mu_K$ as a product of two cyclic groups of coprime order. It follows that the natural exact sequence

$$1 \longrightarrow \prod_{\mathfrak{p}\neq\mathfrak{p}_0} T_{\mathfrak{p}} \longrightarrow T_K/\mu_K \longrightarrow T_{\mathfrak{p}_0}/\mu_K \longrightarrow 1$$

can be split using the composed map $T_{\mathfrak{p}_0}/\mu_K \to T_{\mathfrak{p}_0} \to T_K \to T_K/\mu_K$. This makes T_K/μ_K isomorphic to the product of $\prod_{\mathfrak{p}\neq\mathfrak{p}_0} T_{\mathfrak{p}}$ and a cyclic group for which the order is a product of prime powers that already "occur" infinitely often in T_K. Thus T_K/μ_K is isomorphic to a product of exactly the same groups $(\mathbb{Z}/\ell^k\mathbb{Z})^{\mathbb{Z}}$ that occur in T_K, and therefore isomorphic to T_K itself. □

For imaginary quadratic K, where $\widehat{\mathbb{O}}^*/\mu_K$ constitutes the inertial part U_K of A_K from (4), we summarize the results of this section in the following way.

Theorem 3.5. *Let K be an imaginary quadratic field. Then the subgroup T_K/μ_K of U_K is a direct summand of U_K. For $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$, we have isomorphisms*

$$U_K = \widehat{\mathbb{O}}^*/\mu_K \cong \widehat{\mathbb{Z}}^2 \times (T_K/\mu_K) \cong \widehat{\mathbb{Z}}^2 \times \prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z}$$

of profinite groups.

For K equal to $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$, the prime 2 is exceptional for K, and the groups $T_K/\mu_K \cong T_K$ are different as they do not have cyclic summands of order 2 and 4, respectively.

4. Extensions of Galois groups

In the previous section, all results could easily be stated and proved for arbitrary number fields. From now on, K will denote an imaginary quadratic field. In order to describe the full group A_K from (3), we consider the exact sequence

$$1 \longrightarrow U_K = \widehat{\mathbb{O}}^*/\mu_K \longrightarrow A_K = \widehat{K}^*/K^* \xrightarrow{\psi} \mathrm{Cl}_K \longrightarrow 1 \tag{6}$$

that describes the class group Cl_K of K in idelic terms. Here ψ maps the class of the finite idele $(x_{\mathfrak{p}})_{\mathfrak{p}} \in \widehat{K}^*$ to the class of its associated ideal $\prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$, with $e_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}\, x_{\mathfrak{p}}$.

The sequence (6) shows that U_K is an open subgroup of A_K of index equal to the class number h_K of K. In view of Theorem 3.5, this immediately yields Onabe's discovery that different K can have the same absolute abelian Galois group.

Theorem 4.1. *An imaginary quadratic number field $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$ of class number 1 has absolute abelian Galois group isomorphic to*

$$G = \widehat{\mathbb{Z}}^2 \times \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}.$$

In Onabe's paper [10, §5], the group G, which is not explicitly given but characterized by its infinitely many Ulm invariants, is referred to as 'of type A'. We will refer to G as the *minimal* Galois group, as every absolute abelian Galois group of an imaginary quadratic field $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$ contains a subgroup isomorphic to G. We will show that there are actually *many* more K having this absolute abelian Galois group than the seven fields K of class number 1 to which the preceding theorem applies.

Now take for K any imaginary quadratic field of class number $h_K > 1$. Then Theorem 3.5 and the sequence (6) show that A_K is an abelian group extension of Cl_K by the minimal Galois group G from Theorem 4.1. If the extension (6) were split, we would find that A_K is isomorphic to $G \times \mathrm{Cl}_K \cong G$; but it turns out that splitting at this level *never* occurs for nontrivial Cl_K, in the following strong sense.

Theorem 4.2. *For every imaginary quadratic field K of class number $h_K > 1$, the sequence* (6) *is totally nonsplit*; *that is*, *there is no nontrivial subgroup $C \subset \mathrm{Cl}_K$ for which the associated subextension $1 \to U_K \to \psi^{-1}[C] \to C \to 1$ is split.*

Proof. Suppose there is a non-trivial subgroup $C \subset \mathrm{Cl}_K$ over which the extension (6) splits, and pick $[\mathfrak{a}] \in C$ of prime order p. Then there exists an element

$$\big((x_\mathfrak{p})_\mathfrak{p} \bmod K^*\big) \in \psi^{-1}([\mathfrak{a}]) \subset A_K = \widehat{K}^*/K^*$$

of order p. In other words, there exists $\alpha \in K^*$ such that we have $x_\mathfrak{p}^p = \alpha \in K_\mathfrak{p}^*$ for all $\mathfrak{p}$, and such that α generates the ideal $\mathfrak{a}^p$. But this implies by [1, Chapter IX, Theorem 1] that α is a p-th power in K^*, and hence that $\mathfrak{a}$ is a principal ideal. Contradiction. □

At first sight, Theorem 4.2 seems to indicate that in the case $h_K > 1$, the group A_K will *not* be isomorphic to the minimal Galois group $G \cong U_K$. However, finite abelian groups requiring no more than k generators do allow extensions by free $\widehat{\mathbb{Z}}$-modules of finite rank k that are again free of rank k, just like they do with free $\mathbb{Z}$-modules in the classical setting of finitely generated abelian groups. The standard example for $k = 1$ is the extension

$$1 \longrightarrow \widehat{\mathbb{Z}} \xrightarrow{\times p} \widehat{\mathbb{Z}} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 1$$

for an integer $p \neq 0$, prime or not. Applying to this the functor $\mathrm{Hom}(-, M)$ for a multiplicatively written $\widehat{\mathbb{Z}}$-module M, we obtain an isomorphism

$$M/M^p \xrightarrow{\sim} \mathrm{Ext}(\mathbb{Z}/p\mathbb{Z}, M) \tag{7}$$

by the Hom-Ext-sequence from homological algebra [6]. We will use it in Section 5.

Lemma 4.3. *Let B be a finite abelian group, F a free $\widehat{\mathbb{Z}}$-module of finite rank k, and*

$$1 \longrightarrow F \longrightarrow E \longrightarrow B \longrightarrow 1$$

an exact sequence of $\widehat{\mathbb{Z}}$-modules. Then E is free of rank k if and only if this sequence is totally nonsplit.

Proof. One may reduce the statement to the familiar case of modules over principal ideal domains by writing $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, and consider the individual p-parts of the sequence. As a matter of convention, note that in the degenerate case where B is the trivial group, there are no nontrivial subgroups $C \subset B$ over which the sequence splits, making the sequence by definition totally nonsplit. □

In order to apply the preceding lemma, we replace the extension (6) by the pushout under the quotient map $U_K = \widehat{\mathbb{O}}^*/\mu_K \to U_K/T_K = \widehat{\mathbb{O}}^*/T_K$ from U_K to

its maximal $\widehat{\mathbb{Z}}$-free quotient. This yields the exact sequence of $\widehat{\mathbb{Z}}$-modules

$$1 \longrightarrow \widehat{\mathbb{O}}^*/T_K \longrightarrow \widehat{K}^*/(K^* \cdot T_K) \longrightarrow \mathrm{Cl}_K \longrightarrow 1 \tag{8}$$

in which Cl_K is finite and $\widehat{\mathbb{O}}^*/T_K$ is free of rank 2 over $\widehat{\mathbb{Z}}$ by Lemma 3.1.

Theorem 4.4. *Let K be an imaginary quadratic field of class number $h_K > 1$, and suppose the sequence* (8) *is totally nonsplit. Then the absolute abelian Galois group of K is the minimal group G occurring in Theorem 4.1.*

Proof. If the extension (8) is totally nonsplit, then $\widehat{K}^*/(K^* \cdot T_K)$ is free of rank 2 over $\widehat{\mathbb{Z}}$ by Lemma 4.3. In this case the exact sequence of $\widehat{\mathbb{Z}}$-modules

$$1 \longrightarrow T_K/\mu_K \longrightarrow A_K = \widehat{K}^*/K^* \longrightarrow \widehat{K}^*/(K^* \cdot T_K) \longrightarrow 1$$

is split, and A_K is isomorphic to $U_K = G = \widehat{\mathbb{Z}}^2 \times (T_K/\mu_K)$. □

Remark. We will use Theorem 4.4 in this paper to find many imaginary quadratic fields K having the same minimal absolute abelian Galois group G. It is however interesting to note that this is the only way in which this can be done, as Theorem 4.4 actually admits a converse: If the absolute abelian Galois group of an imaginary quadratic field K of class number $h_K > 1$ is the minimal group G, then the sequence (8) is totally nonsplit. The proof, which we do not include in this paper, will be given in the forthcoming doctoral thesis of the first author.

It is instructive to see what all the preceding extensions of Galois groups amount to in terms of field extensions. The diagram of fields in Figure 1 lists all subfields of the extension $K \subset K^{\mathrm{ab}}$ corresponding to the various subgroups we considered in analyzing the structure of $A_K = \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

We denote by H the Hilbert class field of K. This is the maximal totally unramified abelian extension of K, and it is finite over K with group Cl_K. The inertial part of A_K is the Galois group $U_K = \mathrm{Gal}(K^{\mathrm{ab}}/H)$, which is isomorphic to G for all imaginary quadratic fields $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$. The fundamental sequence (6) corresponds to the tower of fields

$$K \subset H \subset K^{\mathrm{ab}}.$$

By Theorem 3.5, the invariant field L of the closure T_K/μ_K of the torsion subgroup of U_K is an extension of H with group $\widehat{\mathbb{Z}}^2$. The tower of field extensions

$$K \subset H \subset L$$

corresponds to the exact sequence of Galois groups (8).

We define L_0 as the "maximal $\widehat{\mathbb{Z}}$-extension" of K, that is, as the compositum of the $\mathbb{Z}_p$-extensions of K for *all* primes p. As is well-known, an imaginary quadratic field admits two independent $\mathbb{Z}_p$-extensions for each prime p, so $F = \mathrm{Gal}(L_0/K)$

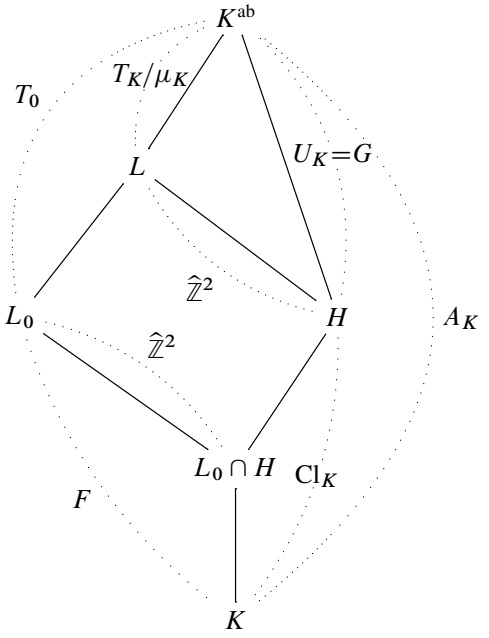

Figure 1. The structure of $A_K = \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

is a free $\widehat{\mathbb{Z}}$-module of rank 2, and L_0 is the invariant field under the closure T_0 of the torsion subgroup of A_K. The image of the restriction map $T_0 \to \mathrm{Cl}_K$ is the maximal subgroup of Cl_K over which (8) splits. The invariant subfield of H corresponding to it is the intersection $L_0 \cap H$. The totally nonsplit case occurs when H is contained in L_0, leading to $L_0 \cap H = H$ and $L_0 = L$. In this case $\mathrm{Gal}(L/K) = \mathrm{Gal}(L_0/K)$ is itself a free $\widehat{\mathbb{Z}}$-module of rank 2, and A_K is an extension of $\widehat{\mathbb{Z}}^2$ by T_K/μ_K that is isomorphic to G.

5. Finding minimal Galois groups

In order to use Theorem 4.4 and find imaginary quadratic K for which the absolute abelian Galois group A_K is the minimal group G from Theorem 4.1, we need an algorithm that can effectively determine, on input K, whether the sequence of $\widehat{\mathbb{Z}}$-modules

$$1 \longrightarrow \widehat{\mathbb{O}}^*/T_K \longrightarrow \widehat{K}^*/(K^* \cdot T_K) \longrightarrow \mathrm{Cl}_K \longrightarrow 1 \tag{8}$$

from Section 4 is totally nonsplit. This means that for every ideal class $[\mathfrak{a}] \in \mathrm{Cl}_K$ of prime order, the subextension $E[\mathfrak{a}]$ of (8) lying over the subgroup $\langle [\mathfrak{a}] \rangle \subset \mathrm{Cl}_K$ is nonsplit.

Any profinite abelian group M is a module over $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, and can be written accordingly as a product $M = \prod_p M_p$ of p-primary parts, where $M_p = M \otimes_{\widehat{\mathbb{Z}}} \mathbb{Z}_p$ is a pro-p-group and $\mathbb{Z}_p$-module. In the same way, an exact sequence of $\widehat{\mathbb{Z}}$-modules is a "product" of exact sequences for their p-primary parts, and splitting over a group of prime order p only involves p-primary parts for that p.

For the free $\widehat{\mathbb{Z}}$-module $M = \widehat{\mathbb{O}}^*/T_K$ in (8), we write T_p for the torsion subgroup of $\mathbb{O}_p^* = (\mathbb{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^* = \prod_{\mathfrak{p}|p} \mathbb{O}_{\mathfrak{p}}^*$. Then the p-primary part of M is the pro-p-group

$$M_p = \mathbb{O}_p^*/T_p = \prod_{\mathfrak{p}|p} (\mathbb{O}_{\mathfrak{p}}^*/T_{\mathfrak{p}}) \cong \mathbb{Z}_p^2. \tag{9}$$

In order to verify the hypothesis of Theorem 4.4, we need to check that the extension $E[\mathfrak{a}]$ has nontrivial class in $\mathrm{Ext}(\langle[\mathfrak{a}]\rangle, M)$ for all $[\mathfrak{a}] \in \mathrm{Cl}_K$ of prime order p. We can do this by verifying in each case that the element of $M/M^p = M_p/M_p^p$ corresponding to it under the isomorphism (7) is nontrivial. This yields the following theorem.

Theorem 5.1. *Let K be an imaginary quadratic field, and define for each prime number p dividing h_K the homomorphism*

$$\phi_p : \mathrm{Cl}_K[p] \longrightarrow \mathbb{O}_p^*/T_p(\mathbb{O}_p^*)^p$$

that sends the class of a p-torsion ideal $\mathfrak{a}$ coprime to p to the class of a generator of the ideal $\mathfrak{a}^p$. Then (8) *is totally nonsplit if and only if all maps ϕ_p are injective.*

Proof. Under the isomorphism (7), the class of the extension

$$1 \longrightarrow M \longrightarrow E \xrightarrow{f} \mathbb{Z}/p\mathbb{Z} \longrightarrow 1$$

in $\mathrm{Ext}(\mathbb{Z}/p\mathbb{Z}, M)$ corresponds by [6, Chapter III, Proposition 1.1] to the residue class of the element

$$(f^{-1}(1 \bmod p\mathbb{Z}))^p \in M/M^p.$$

In the case of $E[\mathfrak{a}]$, we apply this to $M = \widehat{\mathbb{O}}^*/T_K$, and choose the identification $\mathbb{Z}/p\mathbb{Z} = \langle[\mathfrak{a}]\rangle$ under which $1 \bmod p\mathbb{Z}$ is the *inverse* of $[\mathfrak{a}]$. Then $f^{-1}(1 \bmod p\mathbb{Z})$ is the residue class in $\widehat{K}^*/(K^* \cdot T_K)$ of any finite idele $x \in \widehat{K}^*$ that is mapped to ideal class of $\mathfrak{a}^{-1}$ under the map ψ from (6).

We pick $\mathfrak{a}$ in its ideal class coprime to p, and take for $x = (x_{\mathfrak{p}})_{\mathfrak{p}}$ an idele that locally generates $\mathfrak{a}^{-1}$ at all p. If $\alpha \in K^*$ generates $\mathfrak{a}^p$, then $x^p\alpha$ is an idele in $\widehat{\mathbb{O}}^*$ that lies in the same class modulo K^* as x^p, and its image

$$(f^{-1}(1 \bmod p\mathbb{Z}))^p = x^p = x^p\alpha \in M/M^p = M_p/M_p^p = \mathbb{O}_p^*/T_p(\mathbb{O}_p^*)^p$$

corresponds to the class of $E[\mathfrak{a}]$ in $\mathrm{Ext}(\langle[\mathfrak{a}]\rangle, \mathbb{O}^*/T_K)$. As the idele $x = (x_{\mathfrak{p}})_{\mathfrak{p}}$ has components $x_{\mathfrak{p}} \in \mathbb{O}_{\mathfrak{p}}^*$ at $\mathfrak{p} \mid p$ by the choice of $\mathfrak{a}$, we see that this image in

$M_p/M_p^p = \mathbb{O}_p^*/T_p(\mathbb{O}_p^*)^p$ is the element $\phi_p([\mathfrak{a}])$ we defined. The map ϕ_p is clearly a homomorphism, and we want it to assume nontrivial values on the elements of order p in $\mathrm{Cl}_K[p]$, for each prime p dividing h_K. The result follows. □

Remark. In Theorem 5.1, it is not really necessary to restrict to representing ideals $\mathfrak{a}$ that are coprime to p. One may take $K_p^*/T_p(K_p^*)^p$ as the target space of ϕ_p to accommodate all $\mathfrak{a}$, with $K_p = K \otimes_{\mathbb{Z}} \mathbb{Z}_p$, and observe that the image of ϕ_p is in the subgroup $\mathbb{O}_p^*/T_p(\mathbb{O}_p^*)^p$, as the valuations of $\mathfrak{a}^p$ at the primes over p are divisible by p.

Remark. It is possible to prove Theorem 5.1 without explicit reference to homological algebra. What the proof shows is that, in order to lift an ideal class of arbitrary order n under (8), it is necessary and sufficient that its n-th power is generated by an element α that is locally everywhere a n-th power *up to multiplication by local roots of unity.* This extra leeway in comparison with the situation in Theorem 4.2 makes it into an interesting splitting problem for the group extensions involved, as this condition on α may or may not be satisfied. Note that at primes outside n, the divisibility of the valuation of α by n automatically implies the local condition.

In Onabe's paper, which assumes throughout that Cl_K itself is a cyclic group of prime order, the same criterion is obtained from an analysis of the Ulm invariants occurring in Kubota's setup [5].

Our Theorem 5.1 itself does not assume any restriction on Cl_K, but its use in finding K with minimal absolute Galois group G does imply certain restrictions on the structure of Cl_K. The most obvious implication of the injectivity of the map ϕ_p in the theorem is a bound on the p-rank of Cl_K, which is defined as the dimension of the group $\mathrm{Cl}_K\,/\,\mathrm{Cl}_K^p$ as an $\mathbb{F}_p$-vector space.

Corollary 5.2. *If* Cl_K *has* p*-rank at least* 3 *for some* p*, then the sequence* (8) *splits over a subgroup of* Cl_K *of order* p*.*

Proof. It follows from the isomorphism in (9) that the image of ϕ_p lies in a group that is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$. If Cl_K has p-rank at least 3, then ϕ_p will not be injective. Now apply Theorem 5.1. □

As numerical computations in uncountable $\widehat{\mathbb{Z}}$-modules such as $\widehat{K}^*/(K^* \cdot T_K)$ can only be performed with finite precision, it is not immediately obvious that the splitting type of an idelic extension as (8) can be found by a finite computation. The maps ϕ_p in Theorem 5.1 however are linear maps between finite-dimensional $\mathbb{F}_p$-vector spaces that lend themselves very well to explicit computations. One just needs some standard algebraic number theory to compute these spaces explicitly. A high-level description of an algorithm that determines whether the extension (8) is totally nonsplit is then easily written down.

Algorithm 5.3.

Input: An imaginary quadratic number field K.

Output: *No* if the extension (8) for K is not totally nonsplit, *yes* otherwise.

1. Compute the class group Cl_K of K. If Cl_K has p-rank at least 3 for some p, output *no* and stop.
2. For each prime p dividing h_K, compute $n \in \{1, 2\}$ $\mathbb{O}$-ideals coprime to p such that their classes in Cl_K generate $\mathrm{Cl}_K[p]$, and generators x_1 up to x_n for their p-th powers. Check whether x_1 is trivial in $\mathbb{O}_p^*/T_p(\mathbb{O}_p^*)^p$. If it is, output *no* and stop. If $n = 2$, check whether x_2 is trivial in $\mathbb{O}_p^*/T_p \cdot \langle x_1 \rangle \cdot (\mathbb{O}_p^*)^p$. If it is, output *no* and stop.
3. If all primes $p \mid h_K$ are dealt with without stopping, output *yes* and stop.

Step 1 is a standard task in computational algebraic number theory. For imaginary quadratic fields, it is often implemented in terms of binary quadratic forms, and particularly easy. From an explicit presentation of the group, it is also standard to find the global elements x_1 and, if needed, x_2. The rest of Step 2 takes place in a *finite* group, and this means that we only compute in the rings $\mathbb{O}_p$ up to small precision. For instance, computations in $\mathbb{Z}_p^*/T_p(\mathbb{Z}_p^*)^p$ amount to computations modulo p^2 for odd p, and modulo p^3 for $p = 2$.

6. Splitting behavior at 2

The splitting behavior of the sequence (8) depends strongly on the structure of the p-primary parts of Cl_K at the primes $p \mid h_K$. In view of Theorem 5.1 and Corollary 5.2, fields with cyclic class groups and few small primes dividing h_K appear to be more likely to have minimal Galois group G. In Section 7, we will provide numerical data to examine the average splitting behavior.

For odd primes p, class groups of p-rank at least 3 arising in Corollary 5.2 are very rare, at least numerically and according to the Cohen-Lenstra heuristics. At the prime 2, the situation is a bit different, as the 2-torsion subgroup of Cl_K admits a classical explicit description going back to Gauss. Roughly speaking, his theorem on ambiguous ideal classes states that $\mathrm{Cl}_K[2]$ is an $\mathbb{F}_2$-vector space generated by the classes of the primes $\mathfrak{p}$ of K lying over the rational primes that ramify in $\mathbb{Q} \subset K$, subject to a single relation coming from the principal ideal $(\sqrt{D_K})$. Thus, the 2-rank of Cl_K for a discriminant with t distinct prime divisors equals $t - 1$. In view of Corollary 5.2, our method to construct K with absolute abelian Galois group G does not apply if the discriminant D_K of K has more than 3 distinct prime divisors.

If $-D_K$ is a prime number, then h_K is odd, and there is nothing to check at the prime 2.

For D_K with two distinct prime divisors, the 2-rank of Cl_K equals 1, and we can replace the computation at $p = 2$ in Algorithm 5.3 by something that is much simpler.

Theorem 6.1. *Let K be an imaginary quadratic field with even class number, and suppose that its 2-class group is cyclic. Then the sequence* (8) *is nonsplit over $\mathrm{Cl}_K[2]$ if and only if the discriminant D_K of K is of one of the following types*:

(1) $D_K = -pq$ *for primes* $p \equiv -q \equiv 5 \bmod 8$;

(2) $D_K = -4p$ *for a prime* $p \equiv 5 \bmod 8$;

(3) $D_K = -8p$ *for a prime* $p \equiv \pm 3 \bmod 8$.

Proof. If K has a nontrivial cyclic 2-class group, then $D_K \equiv 0, 1 \bmod 4$ is divisible by exactly two different primes.

If D_K is odd, we have $D_K = -pq$ for primes $p \equiv 1 \bmod 4$ and $q \equiv 3 \bmod 4$, and the ramified primes $\mathfrak{p}$ and $\mathfrak{q}$ of K are in the unique ideal class of order 2 in Cl_K. Their squares are ideals generated by the integers p and $-q$ that become squares in the genus field $F = \mathbb{Q}(\sqrt{p}, \sqrt{-q})$ of K, which is a quadratic extension of K with group $C_2 \times C_2$ over $\mathbb{Q}$ that is locally unramified at 2.

If we have $D_K \equiv 5 \bmod 8$, then 2 is inert in $\mathbb{Q} \subset K$, and 2 splits in $K \subset F$. This means that K and F have isomorphic completions at their primes over 2, and that p and $-q$ are local squares at 2. In this case ϕ_2 is the trivial map in Theorem 5.1, and is not injective.

If we have $D \equiv 1 \bmod 8$ then 2 splits in $\mathbb{Q} \subset K$. In the case $p \equiv -q \equiv 1 \bmod 8$ the integers p and $-q$ are squares in $\mathbb{Z}_2^*$, and ϕ_2 is again the trivial map. In the other case $p \equiv -q \equiv 5 \bmod 8$, the generators p and $-q$ are nonsquares in $\mathbb{Z}_2^*$, also up to multiplication by elements in $T_2 = \{\pm 1\}$. In this case ϕ_2 is injective.

If D_K is even, we either have $D_K = -4p$ for a prime $p \equiv 1 \bmod 4$ or $D_K = -8p$ for an odd prime p. In the case $D_K = -4p$ the ramified prime over 2 is in the ideal class of order 2. For $p \equiv 1 \bmod 8$, the local field $\mathbb{Q}_2(\sqrt{-p}) = \mathbb{Q}_2(i)$ contains a square root of $2i$, and ϕ_2 is not injective. For $p \equiv 5 \bmod 8$, the local field $\mathbb{Q}_2(\sqrt{-p}) = \mathbb{Q}_2(\sqrt{3})$ does not contain a square root of ± 2, and ϕ_2 is injective. In the case $D_K = -8p$ the ramified primes over both 2 and p are in the ideal class of order 2. For $p \equiv \pm 1 \bmod 8$ the generator $\pm p$ is a local square at 2. For $p \equiv \pm 3 \bmod 8$ it is not. □

In the case where the 2-rank of Cl_K exceeds 1, the situation is even simpler.

Theorem 6.2. *Let K be an imaginary quadratic field for which the 2-class group is noncyclic. Then the map ϕ_2 in Theorem 5.1 is not injective.*

Proof. As every 2-torsion element in Cl_K is the class of a ramified prime $\mathfrak{p}$, its square can be generated by a rational prime number. This implies that the image

of ϕ_2 is contained in the cyclic subgroup

$$\mathbb{Z}_2^*/\{\pm 1\}(\mathbb{Z}_2^*)^2 \subset \widehat{\mathbb{O}}^*/T_2(\widehat{\mathbb{O}}^*)^2$$

of order 2. Thus ϕ_2 is not injective if Cl_K has noncyclic 2-part. □

In view of Theorem 4.4 and the remark following it, imaginary quadratic fields K for which A_K is the minimal Galois group from Theorem 4.1 can only be found among those K for which $-D_K$ is prime, or in the infinite families from Theorem 6.1. In the next section, we will find many of such K.

7. Computational results

In Onabe's paper [10], only cyclic class groups Cl_K of prime order $p \leq 7$ are considered. In this case there are just 2 types of splitting behavior for the extension (8), and Onabe provides a list of the first few K with $h_K = p \leq 7$, together with the type of splitting they represent. For $h_K = 2$ the list is in accordance with Theorem 6.1. In the cases $h_k = 3$ and $h_K = 5$ there are only 2 split examples against 10 and 7 nonsplit examples, and for $h_K = 7$ no nonsplit examples are found. This suggests that ϕ_p is rather likely to be injective for increasing values of $h_K = p$.

This belief is confirmed if we extend Onabe's list by including *all* imaginary quadratic K of odd prime class number $h_K = p < 100$. By the work of Watkins [11], we now know, much more precisely than Onabe did, what the exact list of fields with given small class number looks like. The extended list, with the 65 out of 2356 cases in which the extension (8) splits mentioned explicitly, is given in Table 1.

As the nonsplit types give rise to fields K having the minimal group G as its absolute Galois group, one is inevitably led to the following conjecture.

Conjecture 7.1. *There are infinitely many imaginary quadratic fields K for which the absolute abelian Galois group is isomorphic to*

$$G = \widehat{\mathbb{Z}}^2 \times \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}.$$

The numerical evidence may be strong, but we do not even have a theorem that there are infinitely many prime numbers that occur as the class number of an imaginary quadratic field. And even if we had, we have no theorem telling us what the distribution between split and nonsplit will be.

From Table 1, one easily gets the impression that among all K with $h_K = p$, the fraction for which the sequence (8) splits is about $1/p$. In particular, assuming infinitely many imaginary quadratic fields to have prime class number, we would expect 100% of these fields to have the minimal absolute abelian Galois group G.

If we fix the class number $h_K = p$, the list of K will be finite, making it impossible to study the average distribution of the splitting behavior over $\mathrm{Cl}_K[p]$. For

p	$\#\{K : h_K = p\}$	#Nonsplit	$-D_K$ for split K
2	18	8	35, 51, 91, 115, 123, 187, 235, 267, 403, 427
3	16	13	107, 331, 643
5	25	19	347, 443, 739, 1051, 1123, 1723
7	31	27	859, 1163, 2707, 5107
11	41	36	9403, 5179, 2027, 10987, 13267
13	37	34	1667, 2963, 11923
17	45	41	383, 8539, 16699, 25243
19	47	43	4327, 17299, 17539, 17683
23	68	65	2411, 9587, 21163
29	83	80	47563, 74827, 110947
31	73	70	9203, 12923, 46867
37	85	83	20011, 28283
41	109	106	14887, 21487, 96763
43	106	105	42683
47	107	107	—
53	114	114	—
59	128	126	125731, 166363
61	132	131	101483
67	120	119	652723
71	150	150	—
73	119	117	358747, 597403
79	175	174	64303
83	150	150	—
89	192	189	48779, 165587, 348883
97	185	184	130051

Table 1. Splitting types for fields K with $h_K = p < 100$. The second column gives the number of imaginary quadratic fields with class number p; the third column gives the number of such fields for which the sequence (8) does not split; and the fourth column gives $-D_K$ for the fields K for which (8) splits.

this reason, we computed the average splitting behavior over $\mathrm{Cl}_K[p]$ for the set S_p of imaginary quadratic fields K for which the class number has a *single* factor p.

More precisely, Table 2 lists, for the first N_p imaginary quadratic fields $K \in S_p$ of absolute discriminant $|D_K| > B_p$, the fraction f_p of K for which the sequence (8) is split over $\mathrm{Cl}_K[p]$. We started counting for absolute discriminants exceeding B_p to avoid the influence that using many very small discriminants may have on observing the asymptotic behavior. Numerically, the values for $p \cdot f_p \approx 1$ in the table show that the fraction f_p is indeed close to $1/p$.

For the first three odd primes, we also looked at the distribution of the splitting over the three kinds of local behavior in K of the prime p (split, inert or ramified)

p	N_p	B_p	$p \cdot f_p$	p	N_p	B_p	$p \cdot f_p$
3	300	10^7	0.960	43	2150	10^6	1.080
5	500	10^7	0.930	47	470	10^7	0.900
7	700	10^7	0.960	53	530	10^5	1.000
11	1100	10^7	0.990	59	590	10^6	0.900
13	1300	10^7	1.070	61	1830	10^5	0.933
17	1700	10^7	0.920	67	670	10^6	0.900
19	1900	10^7	1.000	71	1000	10^5	1.136
23	2300	10^7	1.030	73	3650	10^5	0.900
29	2900	10^6	1.000	79	1399	10^7	1.130
31	3100	10^6	0.970	83	1660	10^6	1.000
37	3700	10^6	0.930	89	890	10^5	1.100
41	4100	10^6	1.060	97	970	10^8	1.100

Table 2. Splitting fractions at p for h_K divisible by $p < 100$. For the given values of p, N_p, and B_p, we consider the first N_p imaginary quadratic fields K with $|D_K| > B_p$ and whose class numbers are divisible by a single factor of p. The fourth column gives the value of $p \cdot f_p$, where f_p is the fraction of these fields for which the sequence (8) is split over $\mathrm{Cl}_K[p]$.

and concluded that, at least numerically, there is no clearly visible influence; see Table 3.

p	N_p	B_p	$p \cdot f_p$	Split	Inert	Ramified
3	300	10^7	0.960	0.925	0.947	1.025
5	500	10^7	0.930	0.833	0.990	1.022
7	700	10^7	0.960	0.972	0.963	0.897

Table 3. Splitting fractions at p according to local behavior at p. The first four columns are as in Table 2. The remaining columns give the values of p times the quantity analogous to f_p, where we further limit our attention to fields in which p has the prescribed splitting behavior.

We further did a few computations that confirmed the natural hypothesis that the splitting behaviors at different primes p and q that both divide the class number once are independent of each other.

Acknowledgement

We thank Georges Gras for spotting an inaccuracy in part (2) of Theorem 6.1, and for pointing out related results in his textbook on class field theory [2].

References

[1] Emil Artin and John Tate, *Class field theory*, AMS Chelsea, Providence, RI, 2009, reprinted with corrections from the 1967 original. MR 2009k:11001

[2] Georges Gras, *Class field theory*: *from theory to practice*, Springer, Berlin, 2003. MR 2003j: 11138

[3] Helmut Hasse, *Number theory*, Grundlehren der mathematischen Wissenschaften, no. 229, Springer, Berlin, 1980, reprint of the 1980 edition. MR 81c:12001b

[4] Irving Kaplansky, *Infinite abelian groups*, University of Michigan Press, Ann Arbor, 1954. MR 16,444g

[5] Tomio Kubota, *Galois group of the maximal abelian extension over an algebraic number field*, Nagoya Math. J. **12** (1957), 177–189. MR 20 #4539

[6] Saunders Mac Lane, *Homology*, Grundlehren der mathematischen Wissenschaften, no. 114, Springer, Berlin, 1975. MR 96d:18001

[7] Jürgen Neukirch, *Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper*, Invent. Math. **6** (1969), 296–314. MR 39 #5528

[8] ———, *Über die absoluten Galoisgruppen algebraischer Zahlkörper*, Journées Arithmétiques de Caen (Caen, 1976), Astérisque, no. 41-42, Soc. math. de France, Paris, 1977, pp. 67–79. MR 57 #5954

[9] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der mathematischen Wissenschaften, no. 323, Springer, Berlin, 2008. MR 2008m:11223

[10] Midori Onabe, *On the isomorphisms of the Galois groups of the maximal abelian extensions of imaginary quadratic fields*, Natur. Sci. Rep. Ochanomizu Univ. **27** (1976), no. 2, 155–161. MR 55 #7999

[11] Mark Watkins, *Class numbers of imaginary quadratic fields*, Math. Comp. **73** (2004), no. 246, 907–938. MR 2005a:11175

ATHANASIOS ANGELAKIS: aangelakis@math.leidenuniv.nl
Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands

PETER STEVENHAGEN: psh@math.leidenuniv.nl
Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS