Universal Adelic Groups for Imaginary Quadratic Number Fields and Elliptic Curves

Athanasios Angelakis

▶ **To cite this version:**

Athanasios Angelakis. Universal Adelic Groups for Imaginary Quadratic Number Fields and Elliptic Curves. Group Theory [math.GR]. Université de Bordeaux; Universiteit Leiden (Leyde, Pays-Bas), 2015. English. NNT : 2015BORD0180 . tel-01359692

HAL Id: tel-01359692

https://theses.hal.science/tel-01359692

Submitted on 23 Sep 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Universal Adelic Groups for Imaginary Quadratic Number Fields and Elliptic Curves

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 2 september 2015
klokke 15:00 uur

door

Athanasios Angelakis
geboren te Athene
in 1979

Samenstelling van de promotiecommissie:

Promotor: Prof. dr. Peter Stevenhagen (Universiteit Leiden)

Promotor: Prof. dr. Karim Belabas (Université Bordeaux I)

Overige leden:

Prof. dr. G. Gras (Université de Franche-Comté)

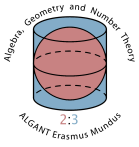
Prof. dr. G. Cornelissen (Universiteit Utrecht)

Prof. dr. H. W. Lenstra (Universiteit Leiden)

Dr. B. de Smit (Universiteit Leiden)

Dr. R. van Luijk (Universiteit Leiden)

This PhD project was funded by the Erasmus Mundus program Algant-DOC, and was carried out at the Universiteit Leiden and the Université Bordeaux 1



université de BORDEAUX

THÈSE

présentée à

L'UNIVERSITÉ DE BORDEAUX

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par Athanasios ANGELAKIS

POUR OBTENIR LE GRADE DE

DOCTEUR

SPECIALITÉ : Mathématiques Pures

Universal Adelic Groups for Imaginary Quadratic Number Fields and Elliptic Curves

Directeurs de recherche : Peter STEVENHAGEN, Karim BELABAS

Soutenue le 2 Septembre 2015 à Leiden

Devant la commission d'examen formée de :

M STEVENHAGEN, Peter	Professeur	Universiteit Leiden	Directeur
M BELABAS, Karim	Professeur	Université Bordeaux I	Directeur
M GRAS, Georges	Professeur	Université de Franche-Comté	Rapporteur
M CORNELISSEN, Gunther	Professeur	Universiteit Utrecht	Rapporteur
M LENSTRA, Hendrik	Professeur	Universiteit Leiden	Examinateur
M DE SMIT, Bart	Docteur	Universiteit Leiden	Examinateur
M VAN LUIJK, Ronald	Docteur	Universiteit Leiden	Examinateur

στους γονείς μου
Γεώργιο και Παναγιώτα Αγγελάκη

to my parents
Georgios and Panagiota Angelakis

Contents

Preface

This thesis consists of 4 chapters.

The first chapter is of an introductory nature. In more or less historical order, it discusses the basic invariants associated to algebraic number fields, and brings up the fundamental question whether or to which extent such invariants characterize the number field. It surveys some of the older results in the area before focusing on the case of absolute abelian Galois groups that occurs center stage in the next two chapters, and on a question for elliptic curves that can be attacked with the techniques from those two chapters.

Chapters 2 and 3 are based on our 2013 paper [**?**]. In these chapters, which are not subject to the size restrictions that papers for the Algorithmic Number Theory Symposium ANTS have to satisfy, there is more background material than in [**?**]. More importantly, the results in these Chapters go beyond the results in the paper, and they include the non-trivial proof of the fact that the key criterion to find imaginary quadratic fields with 'minimal' absolute abelian Galois groups (Theorem 3.2.2) can also be used to find Galois groups that are *provably* non-minimal.

Chapter 4 moves in a different direction. It explicitly computes adelic point groups of elliptic curves over the field of rational numbers, and shows that the outcome can be made as explicit as in the case of the minimal absolute abelian Galois groups, and, in an even stronger sense than in that case, barely depends on the particular elliptic curve. The results obtained do generalize to arbitrary number fields, and it is this generalization that we plan to deal with in a forthcoming paper.

CHAPTER 1

Invariants of Number Fields

ABSTRACT. In this introductory chapter, we investigate to which extent the various invariants associated to a number field characterize the number field up to isomorphism. Special attention will be given to the absolute abelian Galois group of the number field, which occurs center stage in Chapters 2 and 3. In the final section, we discuss a question on elliptic curves that can be studied using the techniques from those Chapters.

"Reason is immortal,
all else is mortal."

Pythagoras, 570 – 495 BC

1.1. Classical Invariants

Algebraic number fields, which are finite field extensions of $\mathbf{Q}$, are the key objects in algebraic number theory. They can be given explicitly in the form $K = \mathbf{Q}(\alpha) = \mathbf{Q}[X]/(f)$, where $\alpha = X \bmod f$ is the root of some monic irreducible polynomial $f \in \mathbf{Z}[X]$. Given in this way, they come with a subring $\mathbf{Z}[\alpha] = \mathbf{Z}[X]/(f)$ of K that can often play the role that $\mathbf{Z}$ plays for the arithmetic in $\mathbf{Q}$.

Many classical problems in number theory naturally lead to number rings $\mathbf{Z}[\alpha]$. The Pell equation $x^2 = dy^2 + 1$, which was popularized by Fermat's 1657 challenge to the British mathematicians, can be written [**?**] as

$$(x + y\sqrt{d}) \cdot (x - y\sqrt{d}) = 1$$

inside the quadratic number ring $\mathbf{Z}[\sqrt{d}]$, and finding its integral solutions is tantamount to determining the units $x + y\sqrt{d}$ in that ring. Fermat's

equation $x^p + y^p = z^p$ for odd prime exponents p was taken up in the 19^{th} century by Kummer in the form

$$\prod_{i=1}^{p}(x + y\zeta_p^i) = z^p$$

inside the cyclotomic number ring $\mathbf{Z}[\zeta_p]$. Euler pioneered with the arithmetic of what we now view as quadratic number rings, discovering the quadratic reciprocity law by numerical experimentation. Gauss proved the quadratic reciprocity law, and generalizations to cubic and biquadratic reciprocity, by Eisenstein and Gauss himself, were found to have their natural formulation in the quadratic rings $\mathbf{Z}[\zeta_3]$ and $\mathbf{Z}[i]$. These rings behave in many ways like the familiar ring $\mathbf{Z}$ of ordinary integers, admitting unique prime factorization, and having only finitely many units.

Arbitrary number rings are not in general so well-behaved. Kummer discovered in the 1840s that his cyclotomic number rings $\mathbf{Z}[\zeta_p]$ may not have unique factorization, and went on to develop a theory of prime *ideal* factorization. The failure of unique factorization of elements is caused by the existence of non-principal ideals in number rings, and they have a *class group* measuring the extent of non-principality.

The theory of general number rings, as developed by Dedekind and others during the 19th century, shows the potential need to enlarge number rings such as $\mathbf{Z}[\alpha]$ to the *maximal* order $\mathcal{O}_K$ contained in $K = \mathbf{Q}(\alpha)$, which is known as the *ring of integers* of the number field $\mathbf{Q}(\alpha)$. Only these *Dedekind domains* admit unique prime ideal factorization. In the case of quadratic rings $\mathbf{Z}[\sqrt{d}]$, this gave an ideal theoretic foundation to the older theory of binary quadratic forms due to Gauss, which did not explicitly mention quadratic rings.

The class group Cl_K and the unit group $\mathcal{O}_K^*$ of the ring of integers of K are the basic invariants of K needed to deal with the ideal theory of $\mathcal{O}_K$. The unit group $\mathcal{O}_K^*$ is a finitely generated abelian group by a theorem of Dirichlet [**?**, Theorem 5.13], and the class group is a finite abelian group [**?**, Corollary 5.9]. These finiteness results may be shown in

an elegant way using techniques from the geometry of numbers developed around 1900 by Minkowski. They can be applied since $\mathcal{O}_K$ can be viewed as a lattice in the Euclidean space $K \otimes_{\mathbf{Q}} \mathbf{R}$, and $\mathcal{O}_K^*$ also embeds logarithmically as a lattice in a Euclidean space. The size of the respective covolumes of these lattices is measured by the discriminant $\Delta_K \in \mathbf{Z}$ and the regulator $R_K \in \mathbf{R}$ of K.

The proofs of the finiteness results given using the geometry of numbers are often not constructive, and the actual computation of class groups and unit groups usually proceeds by factoring sufficiently many principal ideals over a well-chosen factor base of prime ideals. In order to decide that 'sufficiently many' ideals have been factored, one needs the analytic approximation of class number and regulator provided by the Dedekind zeta function ζ_K of the number field. This is a meromorphic function on $\mathbf{C}$ given by $\zeta_K(s) = \sum_{0 \neq I \subset \mathcal{O}_K} (NI)^{-s}$ for $\Re(s) > 1$. It has a simple pole at $s = 1$, and its residue

$$2^{r_1}(2\pi)^{r_2} \frac{h_K R_K}{w_K |\Delta_K|^{1/2}}$$

at this pole combines all the classical invariants of the number field K: the number of real embeddings r_1, the number of pairs of complex embeddings r_2, the class number $h_K = \#\operatorname{Cl}_K$, the regulator R_K, the number w_K of roots of unity in K, and the discriminant Δ_K. From the Euler product

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - \frac{1}{N\mathfrak{p}^s})^{-1}$$

it is clear that ζ_K encodes information on the splitting behavior in K of the primes of $\mathbf{Q}$.

1.2. 20^{th} Century Invariants

In the early 20^{th} century, Hensel and Hasse developed algebraic number theory from a local point of view. In this setting, every non-zero prime ideal $\mathfrak{p}$ of the ring of integers of K corresponds to an equivalence class of valuations $|\cdot|_{\mathfrak{p}} : K \to \mathbf{R}_{\geq 0}$, and gives rise to a completion $K_{\mathfrak{p}}$

of K at $\mathfrak{p}$ that is usually referred to as a (non-archimedean) local field. Similarly, the real and complex embeddings of K can be viewed as 'infinite' primes of K giving rise to the archimedean completions $\mathbf{R}$ and $\mathbf{C}$ of K. This point of view gives rise to the study of global invariants in terms of local data. In this way the class group Cl_K, being the quotient of the group of locally principal $\mathcal{O}_K$-ideals modulo the group of globally principal $\mathcal{O}_K$-ideals, becomes an obstruction group to a local-global principle.

Around 1940, Chevalley combined *all* completions of a number field K into a single topological ring, $\mathbb{A}_K = \prod'_{\mathfrak{p}} K_{\mathfrak{p}}$, the adele ring of K. It is the *restricted* direct product of all completions of K, both finite and infinite, consisting of those elements in the full cartesian product that are almost everywhere integral. More specifically we have,

$$\mathbb{A}_K = \{(x_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} K_{\mathfrak{p}} : |x_{\mathfrak{p}}|_{\mathfrak{p}} \leq 1 \text{ for all but finitely many } \mathfrak{p}\}. \tag{1.1}$$

The number field K embeds along the diagonal into $\mathbb{A}_K$, and becomes a discrete subgroup of $\mathbb{A}_K$ in the restricted product topology.

The unit group $\mathbb{A}_K^* = \prod'_{\mathfrak{p}} K_{\mathfrak{p}}^*$ of the adele ring is the idele group of K. It is the restricted direct product of the groups $K_{\mathfrak{p}}^*$ with respect to the unit groups $\mathcal{O}_{\mathfrak{p}}^*$ of the local ring of integers $\mathcal{O}_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$. Under the corresponding restricted product topology, K^* embeds diagonally in $\mathbb{A}_K^*$ as a discrete subgroup. The quotient $C_K = \mathbb{A}_K^*/K^*$, the *idele class group* of K, is an invariant of K that plays a key role in class field theory (Section 2.5). It is naturally a locally compact abelian group, and by the *product formula* $\prod_{\mathfrak{p}} |x|_{\mathfrak{p}} = 1$ for global elements $x \in K^*$, it comes with a well-defined multiplicative absolute value $C_K \to \mathbf{R}_{>0}$ given by $(x_{\mathfrak{p}})_{\mathfrak{p}} \mapsto \prod_{\mathfrak{p}} |x_{\mathfrak{p}}|_{\mathfrak{p}}$. The subgroup C_K^1 of idele classes of absolute value 1 is a *compact* topological group, a fact reflecting the finiteness results for class group and unit group coming out of the geometry of numbers [**?**, Chapter XII, §16-18].

Every number field K also comes with an automorphism group $\mathrm{Aut}(K)$, which is always finite, and of order equal to the degree $[K : \mathbf{Q}]$ in the case where K is Galois over $\mathbf{Q}$. The group $\mathrm{Aut}(K)$ acts on all

invariants defined so far (e.g. $\mathrm{Cl}_K, \mathcal{O}_K^*, \mathbb{A}_K^*, C_K$), as these invariants are of an "internal" nature: they are constructed out of objects that "live inside K".

Much more information is contained in the *absolute* Galois group G_K of K, which is defined as the automorphism group *over* K of an algebraic closure $\overline{K}$ of K. Being a profinite group, it naturally comes with a Krull topology (cf. Section 2.1). If we view all algebraic number fields as contained in some fixed algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$, the groups G_K are the subgroups of the absolute Galois group $G_{\mathbf{Q}}$ of the rational number field that are open and (hence) of finite index in $G_{\mathbf{Q}}$. The group G_K is also a fundamental invariant of K, and in contrast to the previous "internal" invariants, it may be considered as an "external" invariant as it does not directly come from a structure inside the number field K. In line with this, automorphisms of K do not have a natural action on G_K. More precisely, an automorphism of K gives rise to an automorphism of G_K that is only uniquely defined up to an inner automorphism of G_K.

The absolute Galois group G_K of a number field is a huge profinite group that we are currently unable to describe 'explicitly' for any number field K. The situation changes however if we pass from G_K to its maximal abelian quotient $A_K = G_K^{\mathrm{ab}}$, which describes only those extensions of K that are abelian. Automorphisms of K do have a natural action on A_K, and there is in fact an "internal" description of A_K that is provided by *class field theory*, a theory established around 1920 by Takagi and Artin. More specifically, we have the Artin reciprocity map

$$\mathbb{A}_K^*/K^* \xrightarrow{\phi} A_K = G_K^{\mathrm{ab}}$$

that provides a generalization of the older quadratic, cubic and biquadratic reciprocity laws, and shows that in abelian extensions of number fields, the splitting of the primes only depends on congruences modulo a "conductor". We will provide more details on this theory in Section 2.5.

1.3. Which Invariants Characterize Number Fields?

We now come to the basic type of question for this chapter: *to which extent is a number field characterized by its associated invariants?* This is a very natural mathematical question, and we may ask it in the case of number fields for all invariants that we have defined so far. Some of these questions turn out to be interesting, others less so. We will illustrate this by looking at the most classical invariants first.

For a number field K, the first invariants we defined were the ring of integers $\mathcal{O}_K$, its unit group $\mathcal{O}_K^*$, and its class group Cl_K. These are a commutative ring, a finitely generated abelian group and a finite abelian group, respectively. If two number fields have isomorphic rings of integers, then they are obviously isomorphic, as K is the field of fractions of its ring of integers. This is a case where an object can be recovered in a trivial way from the invariant. One may then modify the question, and forget some of the structure of the invariant, say by looking at the underlying additive group of the ring of integers. Again, we do not get anything very interesting: as an abelian group, the ring of integers is a free abelian group of rank $[K : \mathbf{Q}]$, and all information it contains on K is its degree over $\mathbf{Q}$. In this case, more interesting questions arise when viewing $\mathcal{O}_K$ as a lattice embedded in $K \otimes_{\mathbf{Q}} \mathbf{R}$, the setting of Minkowski's geometry of numbers. In this way, $\mathcal{O}_K$ is provided with a shape and a covolume, and it gives rise to questions as to whether non-isomorphic number fields of the same degree can have the same discriminant, or how the lattice shapes of rings of integers in families of number fields are distributed. These are easy questions for quadratic number fields, but not for number fields of higher degree [**?**].

For the unit group $\mathcal{O}_K^*$ of the ring of integers of a number field K, the situation is somewhat similar. As an abelian group, we know what it looks like by the following theorem.

THEOREM 1.3.1 (Dirichlet, 1846). *Let K be a number field with r_1 real embeddings and r_2 pairs of complex conjugate embeddings. Then*

the unit group of any order $\mathcal{O}$ in K has a finite cyclic torsion group $\mu(\mathcal{O})$ consisting of the roots of unity in $\mathcal{O}$, and $\mathcal{O}^*/\mu(\mathcal{O})$ is free of rank $r_1 + r_2 - 1$. Less canonically, we have an isomorphism

$$\mathcal{O}^* \cong \mu(\mathcal{O}) \times \mathbf{Z}^{r_1+r_2-1}. \tag{1.2}$$

We see that for a totally real number field K of degree n, the isomorphism type of the unit group $\mathcal{O}_K^* \cong \langle -1 \rangle \times \mathbf{Z}^{n-1}$ contains no more information than the degree of the number field, so this is not an invariant that often determines the isomorphism type of K. However, if we view $\mathcal{O}/\mu(\mathcal{O})$ as a lattice in Euclidean space, under the logarithmic map used in the standard proof of Dirichlet's unit theorem, we can ask questions just as for the additive group $\mathcal{O}_K$. Again, these are non-trivial questions as soon as we move beyond the case of quadratic fields [**?**].

The class group of a number field is a fundamental invariant that gives us information about the arithmetic of K, but it clearly does not characterize the number field K. For instance, there seem to be many number fields in small degrees with trivial class group, but we cannot even prove that there exist infinitely many pairwise non-isomorphic number fields of class number one. In this case, the *distribution* of isomorphism types of class groups in families of number fields is a question that has been studied numerically rather extensively, but so far almost all precise answers are entirely conjectural, and go under the name of *Cohen-Lenstra conjectures* [**?**]. For example, in the case of real quadratic fields of prime discriminant $p \equiv 1 \bmod 4$, we expect 75.446% of these fields to be of class number one, but as we said, we do not even know how to prove that infinitely many of them have class number one. Only in the case of imaginary quadratic fields, which are somewhat special in the sense that they have finite unit groups, the growth of the class group as a function of the discriminant is somewhat under control, albeit often in non-effective ways. We will come back to this in Chapter 3, when we deal with imaginary quadratic fields for which the class number is prime.

1.4. The Dedekind Zeta Function and the Adele Ring

The Dedekind zeta function ζ_K of a number field K is the classical invariant we defined already as $\zeta_K(s) = \sum_{0 \neq I \subset \mathcal{O}_K} (NI)^{-s}$, where N denotes the absolute ideal norm, I ranges over the nonzero ideals of $\mathcal{O}_K$ and the argument s of the function is a complex number with real part $\Re(s) > 1$. We can write $\zeta_K(s)$ as a Dirichlet series $\sum_{m=0} a_m m^{-s}$, with $a_m \in \mathbf{Z}_{\geq 0}$ the number of integral $\mathcal{O}_K$-ideals of norm m, and two of these Dirichlet series represent the same function if and only if the values of the coefficients a_m coincide for all m. Thus, two number fields having the same zeta function have the same number of integral ideals of given norm m for all $m \in \mathbf{Z}_{>0}$. This is a rather strong equivalence relation on number fields, and number fields with this property are said to be *arithmetically equivalent*.

From the values of a_m for K, one immediately reads off the degree

$$n = [K : \mathbf{Q}] = \max_{p \text{ prime}} a_p$$

and the set $S = \{p \text{ prime} : \ a_p = n\}$ of primes that split completely in K. This immediately implies that arithmetically equivalent number fields K and K' have a common normal closure N, which is the largest number field in which all primes in S split completely.

Let us define the *splitting type* of an arbitrary prime p in K as the list $(f_1, f_2, \ldots, f_g)$ of residue class field degrees $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbf{Z}/p]$ coming from the factorization $p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_g^{e_g}$ of p in K, ordered to have $f_i \leq f_{i+1}$. Then two number fields are arithmetically equivalent if and only if all rational primes p have the same splitting type in them, so an equality of zeta functions

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - \frac{1}{N\mathfrak{p}^s})^{-1}$$

only arises if the zeta functions have the "same" $\mathfrak{p}$-Euler factors.

Let two number fields K and K', inside $\overline{\mathbf{Q}}$, be arithmetically equivalent. This may of course happen because the Galois groups $H = \mathrm{Gal}(N/K)$ and $H' = \mathrm{Gal}(N/K')$ of their common normal closure N over each of them are *conjugate* subgroups of $G = \mathrm{Gal}(N/\mathbf{Q})$. In this case, K and K' are actually isomorphic. However, Gassmann [**?**] showed in 1926 that arithmetical equivalence of K and K' amounts to requiring something weaker, namely, that H and H' intersect every conjugacy class C of G in the *same* number of elements:

$$\#(C \cap H) = \#(C \cap H').$$

Such *Gassmann-equivalent* subgroups are not necessarily conjugate, and Gassmann himself found the very first examples with subgroups of index $[G : H] = [G : H'] = 180$.

Perlis [**?**] found that examples of arithmetically equivalent number fields exist in degree 7 already, and he gave an explicit family of such fields in degree 8. From the functional equation of the Dedekind zeta function, he derived that arithmetically equivalent number fields have the same discriminant, the same number of real and complex primes, and isomorphic unit groups. He was unable to prove that they also have isomorphic class groups, and in fact, later numerical work by De Smit and Perlis [**?**] showed that the class group may actually differ.

EXAMPLE 1.4.1. Let $a \in \mathbf{Z}$ be an integer for which $\pm a$ and $\pm 2a$ are non-squares in $\mathbf{Q}$. Then the polynomial $f_1(x) = x^8 - a$ is irreducible over $\mathbf{Q}$, and the number field $K = \mathbf{Q}(\alpha)$ generated by a root of f_1 has normal closure $N = \mathbf{Q}(\zeta_8, \alpha)$ of degree 32, generated over K by a primitive 8-th root of unity ζ_8. The Galois group $G = \mathrm{Gal}(N/K)$ is the affine group $\mathbf{Z}/8\mathbf{Z} \rtimes (\mathbf{Z}/8\mathbf{Z})^*$ over $\mathbf{Z}/8\mathbf{Z}$. The polynomial $f_2(x) = x^8 - 16a$ is irreducible over $\mathbf{Q}$ as well, and as $16 = (\sqrt{2})^8 = (\sqrt{-2})^8 = (1+i)^8$ is an 8-th power in $\mathbf{Q}(\zeta_8)$, its roots lie in N. The field K' generated by a root α' of f_2 is an explicit example of a number field that is arithmetically equivalent to K, but not isomorphic to K. At odd primes p, we have an

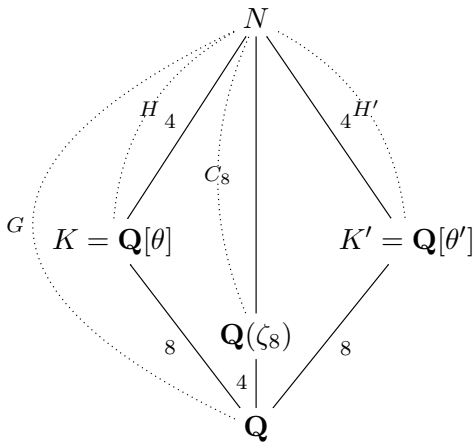


FIGURE 1.1. Perlis' example.

isomorphism

$$\mathbf{Q}_p[X]/(X^8 - a) \cong \mathbf{Q}_p[X]/(X^8 - 16a)$$

of $\mathbf{Q}_p$-algebras, as $\mathbf{Q}_p$ will contain a square root of at least one of 2, -2 and -1. In particular, the splitting types in K and K' of all odd primes p coincide.

At $p = 2$, we do have the same splitting type, but we may or may not have a local isomorphism of $\mathbf{Q}_2$-algebras. To see this, we note first that $1 + 32\mathbf{Z}_2 \subset \mathbf{Z}_2^*$ is the subgroup of 8-th powers in $\mathbf{Z}_2^*$. If we now take for a an integer $a \equiv 1 \bmod 32$, the $\mathbf{Q}_2$-algebras $\mathbf{Q}_2[X]/(X^8 - a)$ and $\mathbf{Q}_2[X]/(X^8 - 16a)$ are non-isomorphic, as they equal

$$\mathbf{Q}_2[X]/(X^8 - 1) \cong \mathbf{Q}_2 \times \mathbf{Q}_2 \times \mathbf{Q}_2(i) \times \mathbf{Q}_2(\zeta_8)$$

and

$$\mathbf{Q}_2[X]/(X^8 - 16) \cong \mathbf{Q}_2(i) \times \mathbf{Q}_2(i) \times \mathbf{Q}_2(\sqrt{2}) \times \mathbf{Q}_2(\sqrt{-2}),$$

respectively, by the factorizations

$$X^8 - 1 = (X - 1)(X + 1)(X^2 + 1)(X^4 + 1)$$

and

$$X^8 - 16 = (X^2 + 2X + 2)(X^2 - 2X + 2)(X^2 - 2)(X^2 + 2)$$

into irreducible polynomials over $\mathbf{Q}_2$. In this case the prime 2 has splitting type $(1, 1, 1, 1)$ in both K and K', but the four primes over 2 in K and K' have different ramification indices.

If we now take $a \equiv -1 \bmod 32$, the local $\mathbf{Q}_2$-algebras

$$\mathbf{Q}_2[X]/(X^8 + 1) = \mathbf{Q}_2(\zeta_{16}) \qquad \text{and} \qquad \mathbf{Q}_2[X]/(X^8 + 16)$$

are isomorphic. In this case, we have arithmetically equivalent fields for which even the adele rings $\mathbb{A}_K$ and $\mathbb{A}_{K'}$ are isomorphic, giving an example of "locally isomorphic" number fields that are not globally isomorphic.

As Iwasawa [**?**] showed, number fields K and K' have topologically isomorphic adele rings if and only if they are "locally isomorphic" at all primes p. We find that this notion, although strictly stronger than arithmetical equivalence, still does not imply global isomorphism.

1.5. The Absolute Galois Group

For the Dedekind zeta function ζ_K and the adele ring $\mathbb{A}_K$ of K, which encode a lot of information on K, it may come as a surprise that they can coincide for non-isomorphic number fields. For the absolute Galois group G_K of K, a huge profinite group that which we will consider now, the surprise is maybe not that it does characterize the number field, but the fact that we can actually *prove* such a statement without knowing very much on the global structure of this group.

At first sight, there seems to be no obvious way to construct an isomorphism of number fields $K_1 \xrightarrow{\sim} K_2$ starting from a topological isomorphism $G_{K_1} \xrightarrow{\sim} G_{K_2}$ of profinite groups. In fact, even if we have such an isomorphism $\alpha_0 : K_1 \xrightarrow{\sim} K_2$, there is no canonical way to obtain an isomorphism $G_{K_1} \xrightarrow{\sim} G_{K_2}$ from α_0. Indeed, we do know that α_0 can be extended to *some* isomorphism $\alpha : \overline{K}_1 \xrightarrow{\sim} \overline{K}_2$, which then gives rise

to an isomorphism $G_{K_1} \xrightarrow{\sim} G_{K_2}$ given by $\sigma \mapsto \alpha\sigma\alpha^{-1}$. However, there are usually many choices for the extension α of α_0, as α is only unique up to composition with an automorphism of $\overline{K}_2$ over K_2. Consequently, the isomorphism $G_{K_1} \xrightarrow{\sim} G_{K_2}$ we get from α_0 is only unique up to composition by an inner automorphism of G_{K_2}. In Figure 1.2 we exhibit the corresponding isomorphisms.

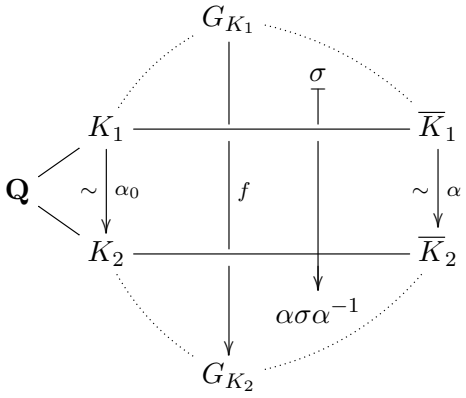


FIGURE 1.2. Isomorphisms induced by $\alpha_0 : K_1 \xrightarrow{\sim} K_2$.

The fundamental work of Neukirch [**?**, **?**], as refined by Ikeda [**?**], Neukirch [**?**], Uchida [**?**] and Iwasawa in an unpublished paper shows that, up to this intrinsic non-uniqueness, every isomorphism of absolute Galois groups of number fields "comes from" an isomorphism of number fields. This result, known as the Neukirch-Uchida theorem [**?**, 12.2.1], is the following.

THEOREM 1.5.1. *Let K_1 and K_2 be number fields, and suppose that we have a topological isomorphism of absolute Galois groups*

$$f : G_{K_1} = \mathrm{Gal}(\overline{K}_1/K_1) \xrightarrow{\sim} G_{K_2} = \mathrm{Gal}(\overline{K}_2/K_2).$$

Then there exists a field isomorphism $\alpha : \overline{K}_1 \xrightarrow{\sim} \overline{K}_2$ with restriction $\alpha_0 : K_1 \xrightarrow{\sim} K_2$ such that f is given by $f(\sigma) = \alpha\sigma\alpha^{-1}$.

The proof of the Neukirch-Uchida theorem starts with Neukirch's observation that for every prime $\mathfrak{p}$ of $\overline{K}_1$, the image $f[G_{\mathfrak{p}}]$ of the decomposition group of $\mathfrak{p}$ is the decomposition group of a *uniquely determined* prime $\alpha_*(\mathfrak{p})$ of $\overline{K}_2$. This establishes a bijection α_* between the sets of primes of the algebraic closures $\overline{K}_1$ and $\overline{K}_2$. Primes that correspond under α_* lie over a common rational prime p, and we can relate the splitting behavior of p in K_1 and its finite extensions to the splitting behavior of p in K_2 and its finite extensions. One deduces that p has an extension of degree 1 in K_1 if and only if it does so in K_2, and just as in the case of arithmetically equivalent fields, we find that *normal* number fields with isomorphic absolute Galois groups are isomorphic [**?**]. Uchida's improvement, which was subsequently simplified by Neukirch [**?**], consists in the actual construction of a map α that induces α_* and has the property stated in Theorem 1.5.1.

Even though we now know that a number field K is characterized by its absolute Galois group G_K, we still do not know what the absolute Galois group of K looks like in any way that might be called explicit. The same is true for the maximal pro-solvable quotient G_K^{solv} of G_K, for which Neukirch [**?**] had already shown that it can take over the role of G_K in the theorems above. The situation becomes however different if we replace G_K^{solv} by an even smaller quotient, the absolute abelian Galois group $A_K = G_K/\overline{[G_K, G_K]}$ of K. Here $\overline{[G_K, G_K]}$ denotes the closure of the commutator subgroup $[G_K, G_K]$ of G_K.

1.6. The Absolute Abelian Galois Group

The question as to whether the absolute abelian Galois group A_K of a number field characterizes the number field up to isomorphism was studied at the same time $1976-78$ when the Neukirch-Uchida theorem was established. As we already observed, A_K is, in contrast to G_K, an invariant that may be thought of as "internal", as it admits a class field theoretic description "in terms of K". This makes A_K more accessible

than G_K, even though the internal description of A_K as a quotient of the idele class group $\mathbb{A}_K^*/K^*$ does not easily allow us to compare absolute abelian Galois groups of number fields: the description is rather strongly tied to arithmetical properties of the field K. For this reason, one might be inclined to think that absolute abelian Galois groups *do* characterize number fields. It therefore came a bit as a surprise when Onabe [**?**, **?**] discovered that this is not the case for imaginary quadratic number fields.

Onabe based her work on earlier work of Kubota [**?**], who studied the dual group $X_K = \mathrm{Hom}(A_K, \mathbf{C}^*)$ of *continuous* characters on A_K. This Pontryagin dual of the compact group A_K is a discrete countable abelian torsion group, and Kubota had expressed the structure of the p-primary parts of X_K in terms of an infinite number of so-called *Ulm invariants*. It had been shown by Kaplansky [**?**, Theorem 14] that such invariants determine the isomorphism type of a countable reduced abelian torsion group, even though this *Ulm-Kaplansky theorem* does not provide explicit descriptions of groups in terms of their Ulm invariants.

Onabe computed the Ulm invariants of X_K for a number of small imaginary quadratic number fields K with prime class number up to 7, and concluded from this that there exist nonisomorphic imaginary quadratic number 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. As we discovered, the explicit example $K = \mathbf{Q}(\sqrt{-2})$, $K' = \mathbf{Q}(\sqrt{-5})$ of this that occurs in Onabe's main theorem [**?**, Theorem 2] is however incorrect. This is because the value of the finite Ulm invariants in [**?**, Theorem 4] is incorrect for the prime 2 in case the ground field is a special number field in the sense of our Lemma 2.3.3. As it happens, $\mathbf{Q}(\sqrt{-5})$ and the exceptional field $\mathbf{Q}(\sqrt{-2})$ 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 [**?**, Theorem 1]. It is related to the non-cyclic nature of the 2-power cyclotomic extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_{2^\infty})$.

In Chapter 3 of the present thesis, 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, and we more or less explicitly give the structure of A_K. More precisely, we show that for all imaginary quadratic number fields $K \neq \mathbf{Q}(i), \mathbf{Q}(\sqrt{-2})$, the absolute abelian Galois group A_K contains a perfectly explicit 'inertial subgroup' U_K isomorphic to

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

as a subgroup of finite index. The number fields that are said to be of "type A" in [**?**] are those fields for which A_K is *isomorphic* to this "minimal" absolute abelian Galois group G.

Just like G contains many subgroups of finite index that are isomorphic to G as topological groups, A_K can be larger than its inertial subgroup $U_K \cong G$ and still be isomorphic to G. The numerical data that we present at the end of Chapter 3 suggest that imaginary quadratic number fields K with minimal absolute abelian Galois group $A_K \cong G$ are in fact quite common: more than 97% of the 2356 imaginary quadratic number fields that have odd prime class number $h_K = p < 100$ are of this nature.

Deciding whether A_K is isomorphic to its inertial subgroup $U_K \cong G$ is a non-trivial problem that is the main topic of Chapter 3. It reduces the underlying splitting question for profinite groups to an explicit finite computation, for which we provide an algorithm in Section 3.4. It allows us to find *many* imaginary quadratic K with the same minimal absolute Galois group $A_K \cong G$, and to understand, at least heuristically, how many there are. We believe (Conjecture 3.6.1) that there are actually *infinitely many* K for which A_K is isomorphic to the minimal group G. Our belief is supported by reasonable assumptions on the average splitting behavior of exact sequences of *abelian* groups, and these assumptions are tested numerically in the same Section 3.6.

1.7. Adelic Points of Elliptic Curves

The situation for imaginary quadratic number fields is particularly easy as these fields are the only number fields (apart from $\mathbf{Q}$) that have a *finite* unit group $\mathcal{O}_K^*$. Already for real quadratic fields K, the presence of a fundamental unit ε_K of infinite order leads to considerable complications, as it is not so easy to predict the p-adic behavior of fundamental units. It is possible to extend our results to the setting of general number fields, as was shown by Gras [**?**], but one does not obtain a description of A_K that is as explicit as in the imaginary quadratic case. The lack of precision in the results is due to insufficient control of the behavior of unit groups, but one can, at least heuristically, understand this behavior, see [**?**].

In the final Chapter 4 of this thesis, we use the methods of Chapter 2 to investigate a problem that, at least at first sight, appears to be rather different: we describe the group of adelic points of an elliptic curve defined over $\mathbf{Q}$ as an abstract topological group. In the case of the inertial part U_K of the absolute abelian Galois group A_K of an imaginary quadratic number field K, which is a product of local factors at rational primes p that have a group structure that very much depends on the particular field K, the striking result is that, when the product is taken over all p, it is almost independent of K. In a similar way, the topological group $E(\mathbf{Q}_p)$ of p-adic points of an elliptic curve E defined over the rational number field $\mathbf{Q}$ can be very different for different elliptic curves E. However, we show in Theorem 4.4.2 that for an overwhelming majority of elliptic curves $E/\mathbf{Q}$, the adelic point group

$$E(\mathbb{A}_{\mathbf{Q}}) = E(\mathbf{R}) \times \prod_p E(\mathbf{Q}_p)$$

is a universal topological group

$$\mathcal{E} = \mathbf{R}/\mathbf{Z} \times \widehat{\mathbf{Z}} \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}$$

reminiscent of the universal group G we encountered in the case of absolute abelian Galois groups of imaginary quadratic fields.

Finding an elliptic curve $E/\mathbf{Q}$ which gives rise to a *different* topological group is a non-trivial problem that one can solve in a simple way using the extensive database [**?**] that was compiled by Rouse and Zureick-Brown in 2014, in the context of the classification of 2-adic Galois representations associated to non-CM elliptic curves $E/\mathbf{Q}$. It shows that there exist one-parameter families of elliptic curves over $\mathbf{Q}$ for which the adelic point group is *not* isomorphic to the generic group $\mathcal{E}$ defined above. Instead of referring to this database, we present an elementary construction of such a family.

Our result in Chapter 4 should be seen as a first step, as we stick to the basic case of elliptic curves over $\mathbf{Q}$ in this thesis. Much of what we say can be generalized without too much effort to elliptic curves over arbitrary number fields (publication in preparation), and there is also the more difficult generalization to abelian varieties of dimension bigger than 1. The 'universality' of the topological groups that occur here provides a negative answer to a question of Cornelissen and Karemaker [**?**, Section 9, Question 1], who are interested in algebraic groups $\mathbf{G}$ for which $\mathbf{G}(\mathbb{A}_K)$ determines K up to isomorphism.

CHAPTER 2

Abelian Galois Groups as $\widehat{\mathbf{Z}}$-modules

ABSTRACT. The infinite abelian Galois groups we study are in a natural way modules over the ring $\widehat{\mathbf{Z}}$ of profinite integers. This chapter presents the simple structural result for the absolute abelian Galois group of $\mathbf{Q}$ from this point of view, and then goes into the generalization to arbitrary number fields, in relation to the information that is provided by class field theory.

"For a man to conquer himself,
is the first and noblest of all victories."

Plato, 428/427 – 348/347 BC

2.1. Infinite Galois Groups

Many of the Galois groups that we will encounter are Galois groups of *infinite* algebraic extensions, and this implies that it is best to view them as *topological* groups.

If $K \subset L$ is a (possibly infinite) Galois extension, then L is a union $L = \bigcup_{i\in I} L_i$ of subfields $L_i \subset L$ that are finite Galois over K. As an automorphism of L/K is determined by its restrictions to the finite extensions L_i, the Galois group $\mathrm{Gal}(L/K)$ injects into the product $\prod_{i\in I} \mathrm{Gal}(L_i/K)$ of finite Galois groups, and its image is the projective limit

$$\varprojlim_{i\in I} \mathrm{Gal}(L_i/K) \subset \prod_{i\in I} \mathrm{Gal}(L_i/K),$$

i.e., the subgroup of the full direct product consisting of those elements that satisfy the natural compatibility conditions coming from field inclusions $L_i \subset L_j$. The product $\prod_{i\in I} \mathrm{Gal}(L_i/K)$ of finite groups carries a

topology that is non-discrete if $K \subset L$ is an infinite extension, and as the subgroup $\mathrm{Gal}(L/K)$ is "cut out" by closed conditions, such profinite Galois groups are compact topological groups.

One of the simplest examples of such an infinite Galois extension is provided by the algebraic closure $\overline{\mathbf{F}}_p$ of the field $\mathbf{F}_p$ of p elements. As we have $\overline{\mathbf{F}}_p = \bigcup_{n\geq 1} \mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$, and $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ is a cyclic group of order n generated by the Frobenius automorphism $x \mapsto x^p$, we have

$$\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p) = \varprojlim_{n\geq 1} \mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p) \cong \varprojlim_{n\geq 1} (\mathbf{Z}/n\mathbf{Z}) = \widehat{\mathbf{Z}}.$$

The procyclic group $\widehat{\mathbf{Z}}$, which occurs here as our first example of an infinite abelian Galois group, is actually a profinite *ring*, as the maps underlying the definition of $\varprojlim_{n\geq 1}(\mathbf{Z}/n\mathbf{Z})$ are also ring homomorphisms. The elements of $\widehat{\mathbf{Z}}$ are *profinite integers* that can be represented as infinite sums $x = \sum_{n=1}^{\infty} c_n n!$, with $c_n \in \mathbf{Z}$ and $0 \leq c_n \leq n$.

By the Chinese remainder theorem, the ring $\widehat{\mathbf{Z}}$ may be decomposed as an infinite product

$$\widehat{\mathbf{Z}} = \prod_p \mathbf{Z}_p \tag{2.1}$$

over all prime numbers p. Here the rings of p-adic integers

$$\mathbf{Z}_p = \varprojlim_{n\geq 1} \mathbf{Z}/p^n\mathbf{Z} = \left\{ (\alpha_n)_{n=1}^{\infty} \in \prod_{n\geq 1} \mathbf{Z}/p^n\mathbf{Z} : \forall\ n,\ \alpha_{n+1} \equiv \alpha_n \bmod p^n \right\}$$

are themselves projective limits of rings. As a group, $\mathbf{Z}_p$ is the primordial example of a pro-p-group, and every abelian pro-p-group is a module over the ring $\mathbf{Z}_p$. Indeed, let B be an abelian pro-p-group. Then we have $B = \varprojlim_i B_i$, with B_i a finite abelian p-group. Since B_i is a $(\mathbf{Z}/p^{n_i}\mathbf{Z})$-module for some n_i, the homomorphism $\mathbf{Z}_p \to \mathbf{Z}/p^{n_i}\mathbf{Z}$ makes each B_i into a $\mathbf{Z}_p$-module, and since the maps defining the projective limit $\varprojlim_i B_i$ inside $\prod_i B_i$ are $\mathbf{Z}_p$-module homomorphisms, the projective limit $\varprojlim_i B_i$ is a $\mathbf{Z}_p$-module as well.

In a similar way, an arbitrary profinite abelian group $A = \varprojlim_i A_i$, with A_i finite abelian, is a module over the ring $\widehat{\mathbf{Z}}$, as every A_i is naturally a $\widehat{\mathbf{Z}}$-module. In explicit terms, this means that the exponentiation in these groups by ordinary integers extends to a continuous exponentiation map $\widehat{\mathbf{Z}} \times A \to A$. Just as finite abelian groups are products of p-groups, profinite abelian groups can be written as products $A = \prod_p A_{(p)}$ of pro-p-groups $A_{(p)}$, with p ranging over all primes. As every $A_{(p)}$ is a $\mathbf{Z}_p$-module, their product is a module over $\prod_p \mathbf{Z}_p$, in accordance with (2.1). The possibility of decomposing $\widehat{\mathbf{Z}}$-modules into their 'p-primary parts' enables us to reduce questions on modules over $\widehat{\mathbf{Z}}$ to modules over $\mathbf{Z}_p$. As that latter ring is a discrete valuation ring, and therefore algebraically simpler than $\widehat{\mathbf{Z}}$, this is a useful reduction. We use it at Section 3.4 when dealing with actual algorithms for $\widehat{\mathbf{Z}}$-modules. Often, there is however no reason to look at a single prime p at a time, and the global picture actually remains clearer if we do not. The next section provides a first example of this phenomenon.

2.2. $A_{\mathbf{Q}}$ as $\widehat{\mathbf{Z}}$-module

For the rational number field $\mathbf{Q}$, the absolute abelian Galois group $A_{\mathbf{Q}}$ is a group that we know very explicitly by the Kronecker-Weber theorem, and it is instructive to analyze $A_{\mathbf{Q}}$ as a $\widehat{\mathbf{Z}}$-module. The Kronecker-Weber theorem states that $\mathbf{Q}^{\mathrm{ab}}$ is the maximal cyclotomic extension of $\mathbf{Q}$, and that an element $\sigma \in A_{\mathbf{Q}}$ acts on the roots of unity that generate $\mathbf{Q}^{\mathrm{ab}}$ by exponentiation. More precisely, for $\sigma \in A_{\mathbf{Q}}$ we have $\sigma(\zeta) = \zeta^u$ for all roots of unity ζ, with u a uniquely defined element in the unit group $\widehat{\mathbf{Z}}^*$ of the ring $\widehat{\mathbf{Z}}$. This yields the well-known isomorphism

$$A_{\mathbf{Q}} = \mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q}) \cong \widehat{\mathbf{Z}}^* = \prod_p \mathbf{Z}_p^*.$$

This is however not a decomposition of $A_{\mathbf{Q}}$ into p-primary parts alluded to above, as $\mathbf{Z}_p^*$ is not quite a pro-p-group for $p > 2$.

For $\mathbf{Z}_p^*$, reduction modulo p yields an exact sequence

$$1 \to 1 + p\mathbf{Z}_p \longrightarrow \mathbf{Z}_p^* \longrightarrow \mathbf{F}_p^* \to 1. \tag{2.2}$$

For $p \neq 2$, as $\mathbf{Z}_p^*$ contains a subgroup T_p consisting of the $(p-1)$-st roots of unity, we may split the sequence (2.2) by sending the elements of $\mathbf{F}_p^*$ to their Teichmüller representatives in $T_p \subset \mathbf{Z}_p^*$. This yields an isomorphism

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

of profinite groups. The subgroup $1 + p\mathbf{Z}_p$ is a free $\mathbf{Z}_p$-module of rank one, which may be generated by $1 + p$. For $p = 2$ a similar statement is true if we reduce modulo 4, as $1 + 4\mathbf{Z}_2$ is a free $\mathbf{Z}_2$-module generated by $1 + 4 = 5$, and writing $T_2 = \{\pm 1\}$ for the torsion subgroup of $\mathbf{Z}_2^*$ we again have $\mathbf{Z}_2^* \cong T_2 \times \mathbf{Z}_2$ as profinite groups. Taking the product over all p, we obtain an isomorphism

$$A_{\mathbf{Q}} \cong T_{\mathbf{Q}} \times \widehat{\mathbf{Z}}, \tag{2.3}$$

with $T_{\mathbf{Q}} = \prod_p T_p$ the product of the torsion subgroups $T_p \subset \mathbf{Q}_p^*$ of the multiplicative groups of the completions $\mathbf{Q}_p$ of $\mathbf{Q}$. More canonically, $T_{\mathbf{Q}}$ is the *closure* of the torsion subgroup of $A_{\mathbf{Q}} = \mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q})$, and the quotient $A_{\mathbf{Q}}/T_{\mathbf{Q}}$ is a free $\widehat{\mathbf{Z}}$-module of rank 1. The invariant field of $T_{\mathbf{Q}}$ inside $\mathbf{Q}^{\mathrm{ab}}$ is the unique $\widehat{\mathbf{Z}}$-extension of $\mathbf{Q}$ (see Section 2.5).

Even though it looks at first sight as if the isomorphism type of $T_{\mathbf{Q}}$ 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 non-canonical isomorphism

$$T_{\mathbf{Q}} = \prod_p T_p \cong \prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}, \tag{2.4}$$

as both of these products, when written as a countable product of cyclic groups of prime power order, have an infinite number of factors $\mathbf{Z}/\ell^k\mathbf{Z}$ 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}.

In order to compare isomorphism types of abelian groups T arising as countable products of finite abelian groups, one may write

$$T = \prod_{\ell \text{ prime}} \prod_{k=1}^{\infty} (\mathbf{Z}/\ell^k\mathbf{Z})^{e(\ell,k)} \tag{2.5}$$

for exponents $e(\ell, k)$ that can be defined in terms of T as

$$e(\ell, k) = \dim_{\mathbf{F}_\ell} T[\ell^k]/\left(T[\ell^{k-1}] + \ell T[\ell^{k+1}]\right). \tag{2.6}$$

Note that the $\mathbf{F}_\ell$-dimensions $e(\ell, k)$ are either finite, in which case $e(\ell, k)$ is a non-negative integer, or countably infinite. In the latter case we write $e(\ell, k) = \omega$, and we have

$$(\mathbf{Z}/\ell^k\mathbf{Z})^\omega = \mathrm{Map}(\mathbf{Z}_{>0}, \mathbf{Z}/\ell^k\mathbf{Z}).$$

Profinite abelian groups T written in the form (2.5) are isomorphic if and only if their exponents $e(\ell, k)$ coincide for all prime powers ℓ^k.

For arbitrary number fields K, the absolute abelian Galois group A_K is not as easily described as in the case $K = \mathbf{Q}$. Still, the direct analogue $\widehat{\mathcal{O}}^*$ of $\widehat{\mathbf{Z}}^*$, with $\widehat{\mathcal{O}}$ the profinite completion of the ring of integers $\mathcal{O}$ of K, will be a major *building block* in the description of A_K. We therefore will need the structure of $\widehat{\mathcal{O}}^*$ as a $\widehat{\mathbf{Z}}$-module, and this description is the main result of the next section.

2.3. $\widehat{\mathcal{O}}^*$ as $\widehat{\mathbf{Z}}$-module

2.3.1. Structure of $\widehat{\mathcal{O}}^*$. Let K be an arbitrary number field, and write $\widehat{\mathcal{O}} = \lim_{\leftarrow n \geq 1}(\mathcal{O}/n\mathcal{O})$ for the profinite completion of the ring of integers $\mathcal{O}$ of K. Just as $\widehat{\mathbf{Z}}$ decomposes as a product $\prod_p \mathbf{Z}_p$ of its p-adic completions, we have a decomposition $\widehat{\mathcal{O}} \cong \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$ into local rings of integers $\mathcal{O}_{\mathfrak{p}}$, with $\mathfrak{p}$ ranging over the finite primes of K. We denote by $T_{\mathfrak{p}}$ the torsion subgroup of $\mathcal{O}_{\mathfrak{p}}^*$, i.e., the subgroup of roots of unity in $K_{\mathfrak{p}}^*$,

and put

$$T_K = \prod_{\mathfrak{p}} T_{\mathfrak{p}} \subset \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^* = \widehat{\mathcal{O}}^*. \tag{2.7}$$

Then the analogue for arbitrary number fields of the isomorphism $A_{\mathbf{Q}} \cong T_{\mathbf{Q}} \times \widehat{\mathbf{Z}}$ from (2.3) is the following.

LEMMA 2.3.1. *The closure of the torsion subgroup of $\widehat{\mathcal{O}}^*$ equals the group T_K from* (2.7)*, and $\widehat{\mathcal{O}}^*/T_K$ is a free $\widehat{\mathbf{Z}}$-module of rank $[K : \mathbf{Q}]$. Less canonically, we have an isomorphism*

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

PROOF. As the finite torsion subgroup $T_{\mathfrak{p}} \subset \mathcal{O}_{\mathfrak{p}}^*$ is closed in $\mathcal{O}_{\mathfrak{p}}^*$, the first statement follows using (2.7) and the definition of the product topology on $\widehat{\mathcal{O}}^* = \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*$.

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

$$1 \to 1 + \mathfrak{p} \longrightarrow \mathcal{O}_{\mathfrak{p}}^* \longrightarrow k_{\mathfrak{p}}^* \to 1 \tag{2.8}$$

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 $\mathcal{O}_{\mathfrak{p}}^*$. 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, which is the characteristic of $k_{\mathfrak{p}}$. The kernel of reduction $1 + \mathfrak{p}$ is by [**?**, One-Unit Theorem, p. 231] a finitely generated $\mathbf{Z}_p$-module of free rank $d = [K_{\mathfrak{p}} : \mathbf{Q}_p]$ having a finite torsion group consisting of roots of unity in $T_{\mathfrak{p}}$ of p-power order.

Combining these facts, we find that $\mathcal{O}_{\mathfrak{p}}^*/T_{\mathfrak{p}}$ is a free $\mathbf{Z}_p$-module of rank d or, less canonically, that we have a local isomorphism

$$\mathcal{O}_{\mathfrak{p}}^* \cong T_{\mathfrak{p}} \times \mathbf{Z}_p^{[K_{\mathfrak{p}}:\mathbf{Q}_p]} \tag{2.9}$$

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 $[K : \mathbf{Q}]$, we obtain the desired global conclusion. □

In order to completely describe $\widehat{\mathcal{O}}^*$, we need to know now what $T_K = \prod_{\mathfrak{p}} T_{\mathfrak{p}}$ looks like as $\widehat{\mathbf{Z}}$-module.

2.3.2. Structure of T_K. In order to derive a characterization of $T_K = \prod_{\mathfrak{p}} T_{\mathfrak{p}}$ for arbitrary number fields K similar to the characterization in the previous section of the torsion part $T_{\mathbf{Q}} = \prod_p T_p \cong \prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}$ of $A_{\mathbf{Q}}$, we observe that we have an exact divisibility $\ell^k \parallel \#T_{\mathfrak{p}}$ of the order of the cyclic group $T_{\mathfrak{p}}$ 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, if we write T_K in the standard form

$$T_K = \prod_{\ell \text{ prime}} \prod_{k=1}^{\infty} (\mathbf{Z}/\ell^k\mathbf{Z})^{e(\ell,k)} \tag{2.10}$$

from (2.5), then each of the exponents $e(\ell, k)$ is either equal to zero or to ω. The prime powers $\ell^k > 1$ that *occur for* K, i.e., for which we have $e(\ell, k) = \omega$, are *all* but those for which we have an equality

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

For $K = \mathbf{Q}$ all prime powers ℓ^k occur, but for general number fields K, there are finitely many prime powers that may disappear. This is due to the fact that the infinite cyclotomic extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_{\ell^\infty})$ which has Galois group isomorphic to $\mathbf{Z}_\ell^* \cong T_\ell \times \mathbf{Z}_\ell$, can partially 'collapse' over K. As $\mathbf{Q} \subset \mathbf{Q}(\zeta_{\ell^\infty})$ is totally ramified at ℓ, it can only do so at primes ℓ that ramify in $\mathbf{Q} \subset K$.

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

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

of ℓ-power roots of unity in the field $K(\zeta_\ell)$. For almost all ℓ, including those ℓ that do not ramify in $\mathbf{Q} \subset K$, this number equals ℓ, and we call ℓ *exceptional* for K if it is divisible by ℓ^2.

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

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

of 2-power roots in $K(\zeta_4) = K(i)$. If K contains $i = \zeta_4$, or $w(2)$ is divisible by 8, we call 2 *exceptional* for K.

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 to an exponent at least 2. In the case where $w = 1$ we simply say that K has no exceptional roots of unity.

For given K, computing $w(K)$ is not difficult. Here is an easy example for quadratic number fields.

LEMMA 2.3.2. *The number of exceptional roots of unity for the quadratic number fields* $\mathbf{Q}(i), \mathbf{Q}(\sqrt{-2})$ *and* $\mathbf{Q}(\sqrt{2})$*, is* 4, 8 *and* 8*, respectively. For all other quadratic fields* K*, we have* $w(K) = 1$*.*

PROOF. Let K be quadratic. If l is an odd prime, the number field $K(\zeta_l)$ of degree dividing $2(l-1)$ cannot contain a root of unity of order l^2, which is of degree $l(l-1)$ over $\mathbf{Q}$, and we have $w_K(l) = 1$. For $K = \mathbf{Q}(i)$ we have $w_2(K) = 4$. For all other K, the quartic field $K(i)$ contains an eighth root of unity ζ_8, and is therefore equal to $K(i) = \mathbf{Q}(\zeta_8)$, if and only if we have $K = \mathbf{Q}(\sqrt{\pm 2})$. □

The prime powers $\ell^k > 1$ that do *not* occur when T_K is written as a direct product of groups $(\mathbf{Z}/\ell^k\mathbf{Z})^{\mathbf{Z}}$ are strict divisors of $w(\ell)$ at exceptional primes ℓ, with $\ell = 2$ giving rise to a special case.

THEOREM 2.3.3. *Let K be a number field, and $w = w(K)$ its number of exceptional roots of unity. Then we have a non-canonical isomorphism of profinite groups*

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

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

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

The group T_K is isomorphic to the group $T_{\mathbf{Q}}$ in (2.4) *if and only if K has no exceptional roots of unity.*

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

$$K(\zeta_\ell) \subset K(\zeta_{\ell^2}) \subset \ldots \subset K(\zeta_{\ell^k}) \subset K(\zeta_{\ell^{k+1}}) \subset \ldots \tag{2.11}$$

is a $\mathbf{Z}_\ell$-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

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

is a $\mathbf{Z}_2$-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 $(\mathbf{Z}/\ell^k\mathbf{Z})^{\mathbf{Z}}$ 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 $\prod_{n\geq 1}\mathbf{Z}/n\mathbf{Z}$ from (2.4) by the group $\prod_{n\geq 1}\mathbf{Z}/nw\mathbf{Z}$ has the effect of removing cyclic summands of order ℓ^k with $\ell^{k+1}|w$ in its standard decomposition (2.5), and this implies that the groups given in Theorem 2.3.3 are indeed isomorphic to T_K. Only for $w=1$ we obtain the group $T_{\mathbf{Q}}$ in which all prime powers ℓ^k occur. □

Now that we understand the explicit $\widehat{\mathbf{Z}}$-module structure of $\widehat{\mathcal{O}}^*$ as the product of T_K and a free module $\widehat{\mathbf{Z}}^{[K:\mathbf{Q}]}$, we have to relate $\widehat{\mathcal{O}}^*$ to the absolute abelian Galois group A_K of K. For $K=\mathbf{Q}$, the groups $\widehat{\mathcal{O}}^*=\widehat{\mathbf{Z}}^*$ and $A_{\mathbf{Q}}$ are isomorphic. For arbitrary K, the relation is given by class field theory, the theory of abelian extensions of number fields that was developed in the first half of the 20$^{\text{th}}$ century.

2.4. Class Field Theory

2.4.1. Classical Point of View. In Section 2.2 we managed to describe $A_{\mathbf{Q}}$ since by Kronecker-Weber we knew that every finite abelian extension $\mathbf{Q}\subset L$ is contained in some cyclotomic extension $\mathbf{Q}\subset\mathbf{Q}(\zeta_m)$. If we now consider abelian extensions over arbitrary number fields $K\neq\mathbf{Q}$, class field theory provides us with an analogue of Kronecker-Weber: every abelian extension $K\subset L$ is contained in a *ray class field* extension $K\subset H_{\mathfrak{m}}$. The main difference from the case where $K=\mathbf{Q}$ is that we do not in general have canonical generators of the ray class field $H_{\mathfrak{m}}$. In fact, finding such generators is known as Hilbert's 12th problem, which has remained open since 1900. However, we will use knowledge of how the primes ramify and split in the extension $H_{\mathfrak{m}}$ and the information that we can retrieve from the Galois group $\mathrm{Gal}(H_{\mathfrak{m}}/K)$, which is the *ray class group* of K of conductor $\mathfrak{m}$ denoted by $\mathrm{Cl}_{\mathfrak{m}}$. This group plays the same role as $(\mathbf{Z}/m\mathbf{Z})^*$ plays for $\mathbf{Q}\subset\mathbf{Q}(\zeta_m)$.

Let $K\subset L$ be an abelian extension. We define the *Artin map* for L/K as the homomorphism

$$\psi_{L/K}: I_K(\Delta_{L/K})\longrightarrow \mathrm{Gal}(L/K),\quad \mathfrak{p}\longmapsto \mathrm{Frob}_{\mathfrak{p}} \tag{2.12}$$

on the group of $I_K(\Delta_{L/K})$ of fractional $\mathcal{O}_K$-ideals generated by the primes $\mathfrak{p}$ that do not divide the discriminant $\Delta_{L/K}$. Here $\mathrm{Frob}_\mathfrak{p}$ is the Frobenius automorphism, which is well defined as a function of $\mathfrak{p}$ as the extension is abelian, and $\mathfrak{p}$ unramified. For an ideal $\mathfrak{a} \in I_K(\Delta_{L/K})$ we call its image under the Artin map the *Artin symbol* of $\mathfrak{a}$ in $\mathrm{Gal}(L/K)$.

A *modulus* $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ of K is a non-zero $\mathcal{O}_K$-ideal $\mathfrak{m}_0$ times a subset $\mathfrak{m}_\infty$ of the real primes of K. For this modulus we have that $x \equiv 1 \bmod^* \mathfrak{m}$ if $\mathrm{ord}_\mathfrak{p}(x-1) \geq \mathrm{ord}_\mathfrak{p}(\mathfrak{m}_0)$ for $\mathfrak{p}|\mathfrak{m}_0$ and $\sigma(x) > 0$ at the real primes $\sigma : K \to \mathbf{R}$ in $\mathfrak{m}_\infty$. The *ray* $R_\mathfrak{m}$ modulo $\mathfrak{m}$ consists of principal ideals $x\mathcal{O}_K$ generated by elements $x \equiv 1 \bmod^* \mathfrak{m}$. For an abelian extension $K \subset L$ a modulus $\mathfrak{m}$ is *admissible* if and only if all primes $\mathfrak{p}$ in the ray $R_\mathfrak{m}$ modulo $\mathfrak{m}$ split completely in L. One of the key statements of class field theory is the existence of admissible moduli for all abelian extensions, and given their existence, it is not difficult to see that there is a minimal admissible modulus (under divisibility). It is called the *conductor* $\mathfrak{f}_{L/K}$ of $K \subset L$. The primes that ramify in L are the primes that occur in the conductor.

Let $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ be an admissible modulus for $K \subset L$, and $I_\mathfrak{m}$ the group of fractional $\mathcal{O}_K$-ideals generated by the primes $\mathfrak{p}$ that are coprime to the finite part of the modulus. Then the Artin map induces a homomorphism on the *ray class group* $\mathrm{Cl}_\mathfrak{m} = I_\mathfrak{m}/R_\mathfrak{m}$ modulo $\mathfrak{m}$:

$$\psi_{L/K} : \mathrm{Cl}_\mathfrak{m} = I_\mathfrak{m}/R_\mathfrak{m} \longrightarrow \mathrm{Gal}(L/K), \quad \mathfrak{p} \longmapsto \mathrm{Frob}_\mathfrak{p}. \tag{2.13}$$

The norms of the $\mathcal{O}_L$-ideals that are coprime to $\mathfrak{m}$ are in the kernel of the Artin map (2.13), and they can be shown to generate the kernel. This implies that the *ideal group* $A_\mathfrak{m} \subset I_\mathfrak{m}$ that corresponds to L is equal to $N_{L/K}(I_{\mathfrak{m}\mathcal{O}_L}) \cdot R_\mathfrak{m}$. The *ray class field* $H_\mathfrak{m}$ modulo $\mathfrak{m}$ is the maximal abelian extension of K in which all primes in the ray $R_\mathfrak{m}$ split completely. For the extension $K \subset L = H_\mathfrak{m}$ the Artin map (2.13) is an isomorphism,

$$\mathrm{Cl}_\mathfrak{m} \cong \mathrm{Gal}(H_\mathfrak{m}/K).$$

The ray $R_{\mathfrak{m}}$ is contained in the subgroup of $P_{\mathfrak{m}} \subset I_{\mathfrak{m}}$ of principal ideals in $I_{\mathfrak{m}}$, and by the approximation theorem, the quotients $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ are for all moduli $\mathfrak{m}$ isomorphic to the class group Cl_K of K. We therefore have the exact sequence

$$\mathcal{O}_K^* \longrightarrow (\mathcal{O}_K/\mathfrak{m})^* \longrightarrow \mathrm{Cl}_{\mathfrak{m}} \longrightarrow \mathrm{Cl}_K \to 1, \tag{2.14}$$

from which we can see that the ray class group $\mathrm{Cl}_{\mathfrak{m}}$ is an extension of the class group Cl_K. The residue class in $(\mathcal{O}_K/\mathfrak{m})^*$ of $x \in \mathcal{O}_K$ coprime to the finite part of the modulus consists of its residue class modulo $\mathfrak{m}_0$ and the signs of its images for the real primes in $\mathfrak{m}_\infty$:

$$(\mathcal{O}_K/\mathfrak{m})^* = (\mathcal{O}_K/\mathfrak{m}_0)^* \times \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \langle -1 \rangle. \tag{2.15}$$

Since all ray class fields $H_{\mathfrak{m}}$ contain the Hilbert class field $H = H_1$, for their Galois groups over H we have an Artin isomorphism

$$(\mathcal{O}_K/\mathfrak{m})^*/\mathrm{im}[\mathcal{O}_K^*] \xrightarrow{\sim} \mathrm{Gal}(H_{\mathfrak{m}}/H). \tag{2.16}$$

Since we want to describe the absolute abelian Galois group $A_K = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ of K, taking the projective limit in the sequence (2.14), we have an exact sequence

$$1 \to \overline{\mathcal{O}}_K^* \longrightarrow \widehat{\mathcal{O}}_K^* \times \prod_{\mathfrak{p} \text{ real}} \langle -1 \rangle \xrightarrow{\psi} A_K \longrightarrow \mathrm{Cl}_K \to 1. \tag{2.17}$$

Here $\widehat{\mathcal{O}}_K = \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$ is the profinite completion of the ring of integers $\mathcal{O}_K$ of K of which we studied the unit group $\widehat{\mathcal{O}}^* = \widehat{\mathcal{O}}_K^* = \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*$ in the previous section, and $\overline{\mathcal{O}}_K^*$ is the closure in $\widehat{\mathcal{O}}_K^* \times \prod_{\mathfrak{p} \text{ real}} \langle -1 \rangle$ of the unit group $\mathcal{O}_K^*$ of $\mathcal{O}_K$. The image of ψ is the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/H) \subset A_K$ of K^{ab} over the Hilbert class field H of K. For an abelian extension $K \subset L$ that contains H, the image of the group $\mathcal{O}_{\mathfrak{p}}^* \subset \widehat{\mathcal{O}}_K^*$ in $\mathrm{Gal}(L/H)$ is the inertia group at $\mathfrak{p}$ in L/K.

In the case $K = \mathbf{Q}$, the group $\overline{\mathcal{O}}_K^* = \{\pm 1\}$ has order 2, there is a single real prime, and the class group Cl_K is trivial, so (2.17) easily yields the isomorphism $\widehat{\mathbf{Z}}^* \xrightarrow{\sim} A_{\mathbf{Q}} = \mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q})$. For arbitrary K, the

relation between $\mathcal{O}_K^*$ and A_K is more complicated, as $\mathcal{O}_K^*$ will usually not be finite, and Cl_K may be non-trivial.

2.4.2. Idelic Point of View. Our final exact sequence (2.17) describing A_K, which removes the need of a chosen conductor $\mathfrak{m}$, is very much in the spirit of the idelic description of class field theory. In this description, one systematically uses a single group, the *idele* group

$$\mathbb{A}_K^* = \prod\nolimits'_{\mathfrak{p}\leq\infty} K_\mathfrak{p}^* = \{(x_\mathfrak{p})_\mathfrak{p} : x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^* \text{ for almost all } \mathfrak{p}\}$$

of K, as the domain of definition of the Artin map. The definition of $\mathbb{A}_K^*$ does not depend on how we define $\mathcal{O}_\mathfrak{p}^*$ for the finitely many archimedean primes of K – one may take $\mathcal{O}_\mathfrak{p}^* = K_\mathfrak{p}^*$ for these $\mathfrak{p}$. Using the idele group, one is able to deal simultaneously with all primes of K, including those that are real or ramified.

The topology of $\mathbb{A}_K^*$ is not the restriction of the product topology, but the so-called *restricted* product topology: elements are close if their quotient is $\mathfrak{p}$-adically close to 1 at finite number of $\mathfrak{p}$, and in $\mathcal{O}_\mathfrak{p}^*$ for all other $\mathfrak{p}$. Under this topology, K^* embeds diagonally into $\mathbb{A}_K^*$ as a discrete subgroup.

To an idele $x = (x_\mathfrak{p})_\mathfrak{p}$ we associate an ideal $x\mathcal{O}_K = \prod_{\mathfrak{p}<\infty} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x_\mathfrak{p})}$, making the group of fractional $\mathcal{O}_K$-ideals I_K into a quotient of the idele group $\mathbb{A}_K^*$. If we consider a global element $x \in K^* \subset \mathbb{A}_K^*$, then the ideal $x\mathcal{O}_K$ is indeed the principal $\mathcal{O}_K$-ideal generated by x. We have the following exact sequence, which describes the *idele class group* $\mathbb{A}_K^*/K^*$ of K:

$$1 \to \overline{\mathcal{O}}_K^* \longrightarrow \prod_{\mathfrak{p}<\infty} \mathcal{O}_\mathfrak{p}^* \times \prod_{\mathfrak{p}|\infty} K_\mathfrak{p}^* \longrightarrow \mathbb{A}_K^*/K^* \longrightarrow \mathrm{Cl}_K \to 1, \tag{2.18}$$

with $\mathbb{A}_K^*/K^* \ni xK^* \mapsto [x\mathcal{O}_K]$.

No matter which of the two approaches we will choose to describe A_K, the results will be the same. This is something that becomes clear if we associate to a modulus $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ of K an open subgroup $W_\mathfrak{m} \subset \mathbb{A}_K^*$.

In order to do so, we write the modulus as a product $\prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$, with the exponent $n(\mathfrak{p})$ to be the order of $\mathfrak{m}_0$ at $\mathfrak{p}$ for finite $\mathfrak{p}$, and 0 or 1 in case $\mathfrak{p}$ is infinite. If $\mathfrak{p}$ is complex then the exponent $n(\mathfrak{p})$ is 0. Finally we define the subgroups $U_{\mathfrak{p}}^{(k)} \subset K_{\mathfrak{p}}^*$ to be:

$$U_{\mathfrak{p}}^{(k)} = \begin{cases} U_{\mathfrak{p}}, & \text{if } k = 0; \\ 1 + \mathfrak{p}^k, & \text{if } \mathfrak{p} \text{ is finite and } k > 0; \\ U_{\mathfrak{p}}^+ \subset U_{\mathfrak{p}} = \mathbf{R}^*, & \text{if } \mathfrak{p} \text{ is real and } k = 1, \end{cases}$$

where by $U_{\mathfrak{p}}^+$ we denote the subgroup of positive elements in $U_{\mathfrak{p}}$. The subgroup $W_{\mathfrak{m}} \subset \mathbb{A}_K^*$ is defined as the product $\prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(n(\mathfrak{p}))}$. By [**?**, Lemma 3.4, p. 505] we have for every modulus $\mathfrak{m}$ of K an isomorphism

$$\mathbb{A}_K^*/K^* W_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Cl}_{\mathfrak{m}}, \tag{2.19}$$

under which the residue class of a prime element at a finite prime $\mathfrak{p} \nmid \mathfrak{m}$ is mapped to the ideal class $[\mathfrak{p}] \in \mathrm{Cl}_K$.

Let $K \subset L$ be a finite abelian extension. Then for an admissible modulus $\mathfrak{m}$ of it, we may compose (2.19) with the map (2.13) to obtain an Artin map

$$\psi_{L/K} : \mathbb{A}_K^*/K^* \longrightarrow \mathrm{Gal}(L/K) \tag{2.20}$$

that has no reference to the modulus $\mathfrak{m}$. If we take the limit of (2.20) for all finite abelian extensions $K \subset L$ inside $\overline{K}$, and denote by A_K the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, we obtain the idelic Artin map

$$\psi_K : \mathbb{A}_K^*/K^* \longrightarrow A_K. \tag{2.21}$$

The map ψ_K is a continuous surjective map, and its kernel is the connected component of the unit element in $\mathbb{A}_K^*/K^*$, denoted by D_K. Thus we have the isomorphism

$$(\mathbb{A}_K^*/K^*)/D_K \xrightarrow{\sim} A_K. \tag{2.22}$$

The expression (2.22) is more involved than the corresponding identity $A_{\mathbf{Q}} = \widehat{\mathbf{Z}}^*$ for the rational number field, and the connected component D_K

is a rather complicated subgroup of $\mathbb{A}_K^*/K^*$ in the case of number fields with infinitely many units, cf. [**?**, Chapter IX, Theorem 3]. In the case of imaginary quadratic fields K that we will be dealing with in the next Chapter, D_K is simply the image of the unique archimedean component $K_{\mathfrak{p}}^* \cong \mathbf{C}^*$ of $\mathbb{A}_K^*$ in $\mathbb{A}_K^*/K^*$. In this case, the *inertial part* of A_K, i.e., the subgroup $U_K \subset A_K$ generated by all inertia groups $\mathcal{O}_{\mathfrak{p}}^* \subset \mathbb{A}_K^*/K^*$, admits a description very similar to $A_{\mathbf{Q}} = T_{\mathbf{Q}} \times \widehat{\mathbf{Z}}$, as we will show in Theorem 3.1.3.

For general K, the inertial part of A_K has the form

$$U_K = \Big(\prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*\Big)/\overline{\mathcal{O}}^*, \tag{2.23}$$

and in case K has no real primes, (2.18) gives rise to the sequence

$$1 \to U_K \longrightarrow A_K \longrightarrow \mathrm{Cl}_K \to 1. \tag{2.24}$$

2.5. $\mathbf{Z}_p$ and $\widehat{\mathbf{Z}}$-extensions of Number Fields

As we are to describe the absolute abelian Galois group A_K for certain number fields K as a $\widehat{\mathbf{Z}}$-module, or their p-primary parts as a $\mathbf{Z}_p$-module, the question naturally arises whether K admits abelian extensions with group $\mathbf{Z}_p$ or $\widehat{\mathbf{Z}}$.

In the case $K = \mathbf{Q}$, the group $A_{\mathbf{Q}}$ is isomorphic to $\widehat{\mathbf{Z}}^* = \prod_p \mathbf{Z}_p^*$, which we may rewrite as in (2.3) as $A_{\mathbf{Q}} \cong T_{\mathbf{Q}} \times \widehat{\mathbf{Z}} = T_{\mathbf{Q}} \times \prod_p \mathbf{Z}_p$. This shows that $\mathbf{Q}$ has a unique $\widehat{\mathbf{Z}}$-extension, which is the compositum over all primes p of a unique $\mathbf{Z}_p$-extension $\mathcal{Z}_p$ of $\mathbf{Q}$. We can describe this 'cyclotomic' $\mathbf{Z}_p$-extension $\mathcal{Z}_p$ of $\mathbf{Q}$ as the subfield of $\mathbf{Q}(\zeta_{p^\infty})$ left invariant by the finite torsion subgroup of $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q}) \cong \mathbf{Z}_p^*$ that we already saw in Section 2.2.

For odd p, the torsion subgroup is a cyclic group C_{p-1} of order $p-1$ consisting of the $(p-1)$-st roots of unity in $\mathbf{Z}_p^*$ indicated in the diagram of associated fields of Figure 2.1. For the prime 2, the torsion subgroup of $\mathbf{Z}_2^*$ is of order 2 and generated by -1, making $\mathbf{Q}(\zeta_{2^\infty})$ into the compositum of its maximal real subfield $\mathcal{Z}_2$ and the quadratic extension $\mathbf{Q}(i) = \mathbf{Q}(\zeta_4)$.

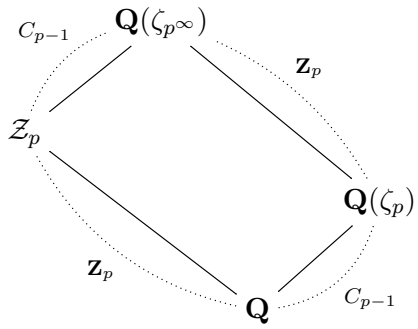


FIGURE 2.1. The unique $\mathbf{Z}_p$-extension of $\mathbf{Q}$ for p odd.

If K is any number field, its intersection (inside an algebraic closure of $\mathbf{Q}$) is a number field $K_0 = K \cap \mathcal{Z}_p$ of finite degree, and $\mathrm{Gal}(\mathcal{Z}_p/K_0)$ is, as a closed subgroup of finite index of $\mathrm{Gal}(\mathcal{Z}_p/\mathbf{Q}) = \mathbf{Z}_p$, itself isomorphic to $\mathbf{Z}_p$. This shows that the compositum $K \cdot \mathcal{Z}_p$ is a $\mathbf{Z}_p$-extension of K. It is known as the cyclotomic $\mathbf{Z}_p$-extension of K (see Figure 2.2). If K contains ζ_p (for p odd) or ζ_4 (for $p = 2$), then it is obtained by adjoining all the p-power roots of unity to K. Their compositum over all primes p gives rise to the cyclotomic $\widehat{\mathbf{Z}}$-extension of K.

In principle, class field theory tells us for any number field K how many different, or, more precisely, how many K-linearly independent $\mathbf{Z}_p$-extensions it admits. For this, it suffices to determine the $\mathbf{Z}_p$-rank of the maximal $\mathbf{Z}_p$-free quotient of the inertial part $U_K = \widehat{\mathcal{O}}_K^*/\overline{\mathcal{O}^*}$ of the absolute abelian Galois group A_K of K that we encountered in (2.23).

The free $\mathbf{Z}_p$-rank of the p-primary part of the group $\widehat{\mathcal{O}}_K^* \cong T_K \times \widehat{\mathbf{Z}}^{[K:\mathbf{Q}]}$ equals $[K : \mathbf{Q}]$, and a famous conjecture going back to Leopoldt is that, for all number fields K and all primes p, quotienting $\widehat{\mathcal{O}}_K^*$ by the closure of the subgroup of global units $\mathcal{O}_K^*$ of K, of free $\mathbf{Z}$-rank $r_1 + r_2 - 1$, will result in a group for which the p-primary part has free $\mathbf{Z}_p$-rank $[K : \mathbf{Q}] - (r_1 + r_2 - 1) = r_2 + 1$. It is however not at all obvious that the p-adic rank of $\widehat{\mathcal{O}}_K^*$, which is obviously bounded by $r_1 + r_2 - 1$, should always

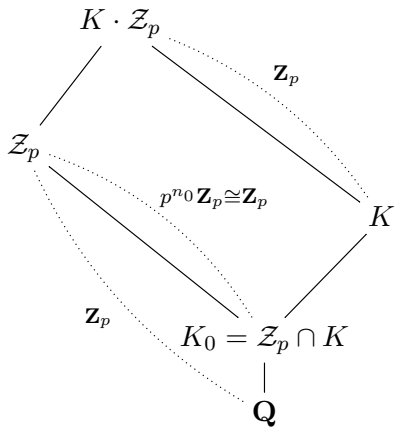


FIGURE 2.2. The cyclotomic $\mathbf{Z}_p$-extension of K.

be equal to it. Using class field theory, we may phrase the conjecture in the following way, cf. [**?**, Conjecture 1.6.4].

CONJECTURE 2.5.1 (Leopoldt). *Let K be a number field with r_2 complex primes, and p a prime number. Then K admits exactly $r_2 + 1$ linearly independent $\mathbf{Z}_p$-extensions.*

It follows from Leopoldt's conjecture that the compositum of all $\widehat{\mathbf{Z}}$-extensions of K is a Galois extension of K with group $\widehat{\mathbf{Z}}^{r_2+1}$. For general number fields K the conjecture is still open, but it has for instance been proved true (Ax-Brumer, 1965–1967, [**?**], [**?**]) for all abelian fields K.

In case K is imaginary quadratic, its unit rank is 0, over $\mathbf{Z}$ and over $\mathbf{Z}_p$, so Leopoldt's conjecture trivially holds and there are two independent $\mathbf{Z}_p$-extensions for all p. In this case, they can in fact be generated in a very explicit way, using complex multiplication, see [**?**]. We will however not need this in our explicit description of A_K for imaginary quadratic K in the next chapter.

CHAPTER 3

Imaginary Quadratic Number Fields

ABSTRACT. In this chapter, we study the structure of the absolute abelian Galois group A_K of an imaginary quadratic field K. We show that for all but two exceptional fields, A_K contains a subgroup of finite index isomorphic to $G = \widehat{\mathbf{Z}}^2 \times \prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}$. We are able to determine algorithmically whether we have $A_K \cong G$, and we will produce many different K having the 'same' minimal absolute abelian Galois group $A_K \cong G$. Based on numerical investigations, we conjecture that there are infinitely many such K.

"You will never do anything in the world
without courage.
It is the greatest quality of the mind
next to honor."

Aristotle, 384 – 322 BC

3.1. The Inertial Part of A_K

In this chapter, the field K will be an imaginary quadratic number field. For such K, the connected component D_K of the identity of the idele class group $\mathbb{A}_K^*/K^*$ in (2.22) is the subgroup $K_\infty^* \cong \mathbf{C}^* \subset \mathbb{A}_K^*/K^*$ coming from the unique infinite prime of K. In this case, it is convenient to replace the idele group $\mathbb{A}_K^*$ from the previous chapter by the group $\mathbb{A}_K^{\mathrm{fin}} = \prod'_{\mathfrak{p}<\infty} K_\mathfrak{p}$ of *finite* ideles obtained by leaving out its single archimedean component. Using the notation $\widehat{\bullet}$ as shorthand for $\bullet \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$, we have

$$\mathbb{A}_K^{\mathrm{fin}} = \widehat{K} = K \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}} = K \otimes_{\mathbf{Q}} \widehat{\mathbf{Q}} = \mathbf{Q} \otimes_{\mathbf{Z}} \widehat{\mathcal{O}}.$$

For imaginary quadratic K, the Artin isomorphism (2.22) for the absolute abelian Galois group $A_K = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ of K simply reads

$$A_K = \widehat{K}^*/K^* = \Big(\prod_{\mathfrak{p}<\infty}{}' K_{\mathfrak{p}}^*\Big)/K^*. \tag{3.1}$$

For the purposes of this chapter, which tries to describe A_K as a profinite abelian group, it is convenient to treat the isomorphism for A_K in (3.1) as an identity – exactly as we have written it down.

Under the description (3.1) and the sequence (2.24) the inertial part of A_K takes the form

$$U_K = \widehat{\mathcal{O}}^*/\mu_K = \Big(\prod_{\mathfrak{p}<\infty} \mathcal{O}_{\mathfrak{p}}^*\Big)/\mathcal{O}^*, \tag{3.2}$$

since the unit group $\mathcal{O}^*$ of $\mathcal{O}$ is finite, and equal to the group μ_K of roots of unity in K. Imaginary quadratic fields K are the only number fields different from $\mathbf{Q}$ for which the Artin map $\widehat{\mathcal{O}}^* \to A_K$ has finite kernel and cokernel, and in this case the knowledge of the $\widehat{\mathbf{Z}}$-module $\widehat{\mathcal{O}}^*$, obtained in the previous chapter, enables us to characterize A_K in a very explicit way.

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 (3.2) can be viewed as the analogue for K of the identity $A_{\mathbf{Q}} = U_{\mathbf{Q}} = \widehat{\mathbf{Z}}^*$. However, as U_K is a subgroup of index $h_K = \#\,\mathrm{Cl}_K$ in A_K, and the class number of h_K tends to infinity with the absolute value of the discriminant for imaginary quadratic fields K, it is clear that we will need more than just $U_K = \widehat{\mathcal{O}}^*/\mu_K$ in order to describe A_K.

Lemmas 2.3.1, 2.3.2 and Theorem 2.3.3 tell us what $\widehat{\mathcal{O}}^*$ looks like as a $\widehat{\mathbf{Z}}$-module. In particular, it shows that the dependence on K is limited to just two quantities: the degree $[K : \mathbf{Q}]$, which is reflected in the rank of the free $\widehat{\mathbf{Z}}$-part of $\widehat{\mathcal{O}}^*$, and the number of exceptional roots of unity of K. In particular, for an imaginary quadratic field $K \neq \mathbf{Q}(i), \mathbf{Q}(\sqrt{-2})$,

Lemmas 2.3.1, 2.3.2 and Theorem 2.3.3 tell us that

$$\widehat{\mathcal{O}}^* \cong \widehat{\mathbf{Z}}^2 \times \prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}$$

is a completely explicit $\widehat{\mathbf{Z}}$-module that is independent of K. We will now show that this is also true for its quotient $\widehat{\mathcal{O}}^*/\mu_K$, for the simple reason that this group is non-canonically isomorphic to $\widehat{\mathcal{O}}^*$ for *any* number field K. The proof below, which nowhere uses that K is imaginary quadratic, is in the spirit of Section 2.3, and uses the notation $T_K = \prod_{\mathfrak{p}} T_{\mathfrak{p}}$ from that Section.

LEMMA 3.1.1. *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 the different prime powers $\ell^k \parallel \#\mu_K$, we get cyclic extensions of different prime degrees, so there are infinitely many primes $\mathfrak{p}$ of K that are inert in all of them. For such $\mathfrak{p}$, we have $\gcd(\#\mu_K, \#T_{\mathfrak{p}}/\#\mu_K) = 1$. □

LEMMA 3.1.2. *We have a non-canonical isomorphism $T_K/\mu_K \cong T_K$.*

PROOF. Pick a prime $\mathfrak{p}_0$ of K that satisfies the conditions of Lemma 3.1.1. 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

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

can be split using the composed map

$$T_{\mathfrak{p}_0}/\mu_K \longrightarrow T_{\mathfrak{p}_0} \longrightarrow T_K \longrightarrow T_K/\mu_K.$$

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 $(\mathbf{Z}/\ell^k\mathbf{Z})^{\mathbf{Z}}$ that occur in T_K. □

Since $\widehat{\mathcal{O}}^*/\mu_K$ constitutes the inertial part U_K of A_K from (3.2), we may now rephrase the results of the last section of the previous chapter in the following way.

THEOREM 3.1.3. *For imaginary quadratic fields $K \neq \mathbf{Q}(i), \mathbf{Q}(\sqrt{-2})$, the subgroup $T_K/\mu_K \subset U_K$ is a direct summand, and we have isomorphisms*

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

of profinite groups.

For K equal to $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt{-2})$, the prime 2 is exceptional for K, and only in these two cases the groups $T_K/\mu_K \cong T_K$ are not isomorphic to the universal group

$$T = \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}, \tag{3.3}$$

as they 'lack' cyclic direct summands of order 2 and 4, respectively.

In order to describe the full group A_K from (3.1), we consider the exact sequence

$$1 \to U_K = \widehat{\mathcal{O}}^*/\mu_K \longrightarrow A_K = \widehat{K}^*/K^* \xrightarrow{\psi} \mathrm{Cl}_K \to 1 \tag{3.4}$$

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 $e_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}\, x_\mathfrak{p}$. For $K \neq \mathbf{Q}(i), \mathbf{Q}(\sqrt{-2})$ as in Theorem 3.1.3, the sequence (3.4) takes the form

$$1 \to T \times \widehat{\mathbf{Z}}^2 \longrightarrow A_K \longrightarrow \mathrm{Cl}_K \to 1. \tag{3.5}$$

The universal group T from (3.3) does not depend on K, so we immediately recover Onabe's discovery that different K can have the same absolute abelian Galois group.

THEOREM 3.1.4. *An imaginary quadratic number field K of class number 1 different from $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-2})$ has absolute abelian Galois group isomorphic to*

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

The two exceptional fields of class number 1 do give rise to different absolute abelian Galois groups. For $K = \mathbf{Q}(i)$ we obtain

$$A_{\mathbf{Q}(i)} \cong \widehat{\mathbf{Z}}^2 \times \prod_{n\geq 1} (\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4n\mathbf{Z})$$

because the presence of the 4th root of unity i prevents the unit groups $k_\mathfrak{p}^*$ of all residue class fields to have direct summands $\mathbf{Z}/2\mathbf{Z}$. For $K = \mathbf{Q}(\sqrt{-2})$ we run into the more subtle phenomenon missed by Kubota and Onabe that the number of exceptional roots equals 8, even though K itself contains only 2 roots of unity. By Lemma 2.3.2 and Theorem 2.3.3 we then have

$$A_{\mathbf{Q}(\sqrt{-2})} \cong \widehat{\mathbf{Z}}^2 \times \prod_{n\geq 1} (\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8n\mathbf{Z}),$$

since in this case the unit groups $k_\mathfrak{p}^*$ of the residue class fields containing a primitive 4th root of unity necessarily contain a primitive eighth root of unity, preventing the occurrence of direct summands $\mathbf{Z}/4\mathbf{Z}$.

In Onabe's paper [**?**, §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 different from $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-2})$ contains an open 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.

Let us now take for K any imaginary quadratic number field different from $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-2})$. Then Theorem 3.1.3 and the sequence (3.4) show that A_K is an abelian group extension of Cl_K by the minimal Galois group G from Theorem 3.1.4. If the extension (3.4) were split, we would find that A_K is isomorphic to $G \times \mathrm{Cl}_K \cong G$, since from the structure of G we have the isomorphism $(\prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}) \times \mathrm{Cl}_K \cong \prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}$. However, it turns out that splitting at this level *never* occurs for nontrivial Cl_K, in the following strong sense.

THEOREM 3.1.5. *For every imaginary quadratic number field K, the sequence*

$$1 \to \widehat{\mathcal{O}}^*/\mu_K \longrightarrow \widehat{K}^*/K^* \xrightarrow{\psi} \mathrm{Cl}_K \to 1$$

is totally nonsplit, i.e., there is no nontrivial subgroup $C \subset \mathrm{Cl}_K$ for which the associated subextension $1 \to U_K \longrightarrow \psi^{-1}[C] \longrightarrow C \to 1$ is split.

PROOF. Let $C = \langle [\mathfrak{a}] \rangle \subset \mathrm{Cl}_K$ be a subgroup of prime order p for which the subextension of (3.4) associated to C is split. Then there exists an element

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

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 [**?**, Chapter IX, Thm. 1] that α is a p-th power in K^*, and hence $\mathfrak{a}$ is a principal ideal. Contradiction. □

3.2. Galois Group Extensions

A property of $\widehat{\mathbf{Z}}$-modules is that finite abelian groups that require no more than k generators do allow extensions by free $\widehat{\mathbf{Z}}$-modules of finite rank k that are again free of rank k, just like they do with free $\mathbf{Z}$-modules in the classical setting of finitely generated abelian groups.

The standard example for $k = 1$ is the extension

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

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

$$M/M^p \xrightarrow{\sim} \mathrm{Ext}(\mathbf{Z}/p\mathbf{Z}, M) \tag{3.6}$$

by the Hom-Ext-sequence from homological algebra [**?**, Chapter III, Prop. 1.1]. We will use it in Section 3.4.

LEMMA 3.2.1. *Let B be a finite abelian group, F a free $\widehat{\mathbf{Z}}$-module of finite rank k, and*

$$1 \to F \longrightarrow E \xrightarrow{\phi} B \to 1$$

an exact sequence of $\widehat{\mathbf{Z}}$-modules. Then E is free of rank k if and only if this sequence is totally nonsplit, i.e., there is no non-trivial subgroup $B' \subset B$ for which $1 \to F \longrightarrow \phi^{-1}[B'] \longrightarrow B' \to 1$ is split.

PROOF. One may reduce the statement to the familiar case of modules over principal ideal domains by writing $\widehat{\mathbf{Z}} = \prod_p \mathbf{Z}_p$, and consider the individual p-parts of the sequence. □

At first sight, Theorem 3.1.5 seems to indicate that whenever the class number exceeds 1, the group A_K will *not* be isomorphic to the minimal Galois group $G \cong U_K$ from Theorem 3.1.4. We will see from Theorem 3.2.2 in this section that this is not the case.

In order to apply Lemma 3.2.1, we replace the extension (3.4) by the pushout under the quotient map

$$U_K = \widehat{\mathcal{O}}^*/\mu_K \to U_K/T_K = \widehat{\mathcal{O}}^*/T_K$$

from U_K to its maximal $\widehat{\mathbf{Z}}$-free quotient. This yields the exact sequence of $\widehat{\mathbf{Z}}$-modules

$$1 \to \widehat{\mathcal{O}}^*/T_K \longrightarrow \widehat{K}^*/(K^* \cdot T_K) \longrightarrow \mathrm{Cl}_K \to 1 \tag{3.7}$$

in which Cl_K is finite and $\widehat{\mathcal{O}}^*/T_K$ is free of rank 2 over $\widehat{\mathbf{Z}}$ by Lemma 2.3.1.

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 3.1 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.

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 $K \neq \mathbf{Q}(i), \mathbf{Q}(\sqrt{-2})$.

The fundamental sequence

$$1 \to \widehat{\mathcal{O}}^*/\mu_K \longrightarrow \widehat{K}^*/K^* \xrightarrow{\psi} \mathrm{Cl}_K \to 1 \tag{3.4}$$

corresponds to the tower of fields

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

By Theorem 3.1.3, 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 $\widehat{\mathbf{Z}}^2$.

The tower of field extensions

$$K \subset H \subset L$$

corresponds to the exact sequence of Galois groups (3.7).

We define L_0 as the 'maximal $\widehat{\mathbf{Z}}$-extension' of K, i.e., as the compositum of the $\mathbf{Z}_p$-extensions of K for *all* primes p. As we observed in Section 2.5, an imaginary quadratic field admits two independent $\mathbf{Z}_p$-extensions for each prime p, so $F = \mathrm{Gal}(L_0/K) \cong \widehat{\mathbf{Z}}^2$ is a free $\widehat{\mathbf{Z}}$-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 (3.7) splits. The invariant subfield of H, corresponding to it, is the intersection $L_0 \cap H$, and we denote by S_0 the Galois group $S_0 = \mathrm{Gal}(H/L_0 \cap H)$, which is a subgroup of Cl_K. In the case where (3.7) splits, we have $S_0 = \mathrm{Cl}_K$.

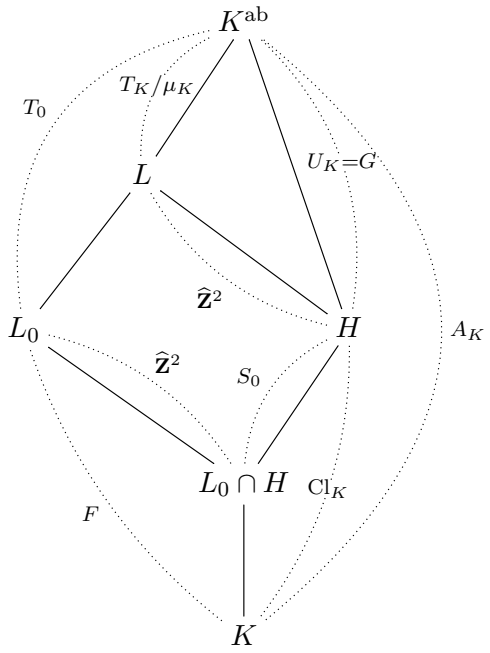


FIGURE 3.1. The structure of $A_K = \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

The totally nonsplit case occurs when H is contained in L_0, Figure 3.2, 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 $\widehat{\mathbf{Z}}$-module of rank 2, and A_K is an extension of $\widehat{\mathbf{Z}}^2$ by T_K/μ_K that is isomorphic to G.

Figure 3.2 shows that imaginary quadratic fields $K \neq \mathbf{Q}(i), \mathbf{Q}(\sqrt{-2})$ have 'minimal' absolute abelian Galois group $A_K \cong G$ in cases where the Hilbert class field extension $K \subset H$ is a subextension of the maximal $\widehat{\mathbf{Z}}$-extension $K \subset L_0$ of K. There turn out to be many such cases different from the class number one cases that we just mentioned.

THEOREM 3.2.2. *Let $K \neq \mathbf{Q}(i), \mathbf{Q}(\sqrt{-2})$ be an imaginary quadratic field for which the sequence*

$$1 \to \widehat{\mathcal{O}}^*/T_K \longrightarrow \widehat{K}^*/(K^* \cdot T_K) \longrightarrow \mathrm{Cl}_K \to 1 \tag{3.7}$$

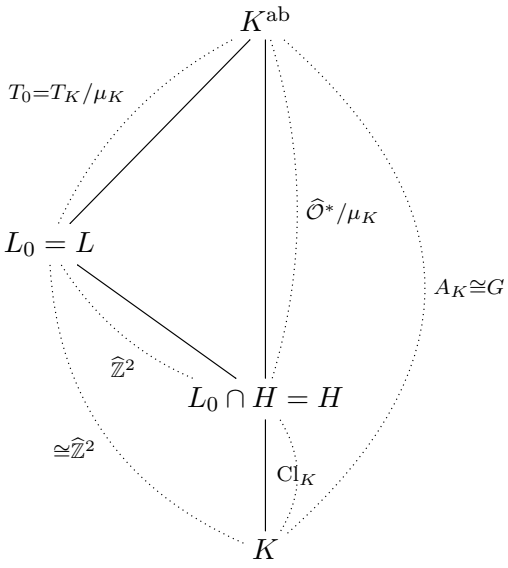


FIGURE 3.2. The structure of $A_K = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ when H is contained in L_0.

is totally nonsplit. Then the absolute abelian Galois group of K is the minimal group G occurring in Theorem 3.1.4.

PROOF. If the extension (3.7) is totally nonsplit, then $\widehat{K}^*/(K^* \cdot T_K)$ is free of rank 2 over $\widehat{\mathbf{Z}}$ by Lemma 3.2.1. In this case the exact sequence of $\widehat{\mathbf{Z}}$-modules

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

is split, and A_K is isomorphic to $\widehat{\mathbf{Z}}^2 \times (T_K/\mu_K)$. For $K \neq \mathbf{Q}(i), \mathbf{Q}(\sqrt{-2})$, we have $T_K/\mu_K \cong T$ independently of K as in (3.3), and

$$\widehat{\mathbf{Z}}^2 \times (T_K/\mu_K) \cong G = \widehat{\mathbf{Z}}^2 \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}$$

by Theorem 3.1.3. □

3.3. Non-minimal Galois Groups

We will use Theorem 3.2.2 in this chapter to find many imaginary quadratic fields K having the same minimal absolute abelian Galois group. In this section, we show how fields that do not satisfy the criteria of Theorem 3.2.2 have Galois groups A_K that are 'non-minimal' in the sense that although they contain a subgroup of finite index isomorphic to the minimal Galois group G from Theorem 3.1.4, they are themselves *not* isomorphic to G.

If K is an imaginary quadratic number field for which the sequence (3.7) is not totally nonsplit, its Hilbert class field H is not contained in the maximal $\widehat{\mathbf{Z}}$-extension L_0 of K, and (3.7) splits over the non-trivial subgroup

$$S_0 = \mathrm{Gal}(H/(H \cap L_0)) \subset \mathrm{Cl}_K\,.$$

We may identify S_0 with the Galois group $\mathrm{Gal}(L/L_0)$ in Figure 3.1.

The subgroup $T_0 = \mathrm{Gal}(K^{\mathrm{ab}}/L_0)$ is a characteristic subgroup of A_K, as $T_0 = [\ker A_K \to \mathrm{Gal}(L_0/K)]$ is the kernel of the map from A_K to its maximal $\widehat{\mathbf{Z}}$-free quotient. This means that for an imaginary quadratic number field with minimal absolute abelian Galois group isomorphic to G, the subgroup $T_0 \subset A_K$ in Figure 3.1 is necessarily isomorphic to $\prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}$.

If S_0 is not a 2-group, the field K has a non-minimal Galois group by the following Theorem.

THEOREM 3.3.1. *Let K be an imaginary quadratic number field for which the sequence*

$$1 \to \widehat{\mathcal{O}}^*/T_K \longrightarrow \widehat{K}^*/(K^* \cdot T_K) \longrightarrow \mathrm{Cl}_K \to 1 \tag{3.7}$$

splits over a subgroup of order divisible by an odd prime. Then the absolute abelian Galois group of K is not isomorphic to the minimal group G occurring in Theorem 3.1.4.

PROOF. The hypothesis means that there exists a finite idele $x \in \widehat{K}^*$ such that $(x \bmod K^* \cdot T_K) \in \widehat{K}^*/(K^* \cdot T_K)$ has odd prime order ℓ. As $\widehat{\mathcal{O}}_K^*/T_K = \ker[\widehat{K}^*/(K^* \cdot T_K) \to \mathrm{Cl}_K]$ is torsion-free, the image of $x \bmod K^* \cdot T_K$ in Cl_K is an ideal class of order ℓ. We then have inclusions

$$T = T_K/\mu_K \overset{\ell}{\subset} T' = \langle T, \overline{x} \rangle \subset T_0 \subset \widehat{K}^*/K^*,$$

and the key step in showing $A_K \ncong G$ consists in showing that $T' = \langle T, \overline{x} \rangle$ is *not* isomorphic to $\prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}$. We do this by showing that the character

$$\chi : T' \longrightarrow \frac{1}{\ell}\mathbf{Z}/\mathbf{Z}$$

defined by $\chi(\overline{x}) = \frac{1}{\ell}$ and $\chi[T] = 0$ is an ℓ-divisible character on T', i.e., for every $n \geq 1$ there exists a character $\psi : T' \to \frac{1}{\ell^{n+1}}\mathbf{Z}/\mathbf{Z}$ satisfying $\ell^n \psi = \chi$. As $T \cong \prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}$ admits no ℓ-divisible characters, this implies $T' \ncong T$. As T' is an open subgroup of finite index of T_0, we deduce that T_0 is also not isomorphic to $\prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}$, by the following Lemma.

LEMMA 3.3.2. *Let T' be an open subgroup of $\prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}$. Then T' is itself a profinite group isomorphic to $\prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}$.*

PROOF. For every positive integer N, we have

$$T' \subset \prod_{1 \leq n < N} \mathbf{Z}/n\mathbf{Z} \times \prod_{n \geq N} \mathbf{Z}/n\mathbf{Z}.$$

If we take N sufficiently large, then T' will contain the subgroup $U_N = \prod_{1 \leq n < N}\{0\} \times \prod_{n \geq N} \mathbf{Z}/n\mathbf{Z}$, as these subgroups form a basis of open neighborhoods of the zero element in $\prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}$. We therefore have $T' = X \times \prod_{n \geq N} \mathbf{Z}/n\mathbf{Z}$ for some finite subgroup $X \subset \prod_{1 \leq n < N} \mathbf{Z}/n\mathbf{Z}$, and non-canonical isomorphisms

$$T' = X \times \prod_{n \geq N} \mathbf{Z}/n\mathbf{Z} \cong X \times \prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z} \cong \prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z},$$

as we can freely add or remove finitely many cyclic components in an infinite product $\prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}$ without changing its isomorphism type. $\square$

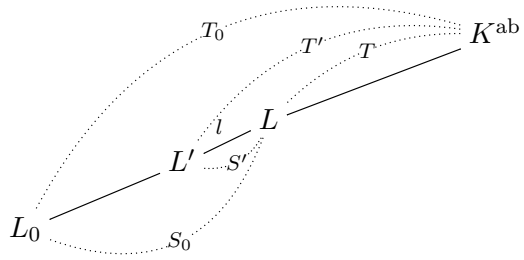


FIGURE 3.3. The diagram of $T \overset{l}{\subset} T' \subset T_0$.

Figure 3.3 summarizes the role of the various Galois groups, with $S' \subset S_0$ the subgroup of odd prime order ℓ over which the sequence (3.7) splits.

We have now reduced the proof of Theorem 3.3.1 to the following Lemma.

LEMMA 3.3.3. *Let $T = T_K/\mu_K \overset{\ell}{\subset} T' = \langle T, \overline{x} \rangle \subset T_0 \subset \widehat{K}^*/K^*$ be as above, with $x \in \widehat{K}^*$ a finite idele of odd prime order ℓ in $\widehat{K}^*/(K^* \cdot T_K)$. Then T' admits a l-divisible character.*

PROOF. As ℓ divides the class number of K, we are dealing with a field $K \neq \mathbf{Q}(\zeta_3), \mathbf{Q}(i)$ having $\mu_K = \{\pm 1\}$.

Let $\mathfrak{a}$ be the ideal generated by x. As its ideal class is of order ℓ, we have $\mathfrak{a}^l = (\alpha)$ for some $\alpha \in K^*$ that is well-defined up to multiplication by ℓ-th powers. Note that α is not an ℓ-th power in K^*. Moreover, as $x \bmod K^* \cdot T_K$ has order ℓ, we can write $x^l = t \cdot \alpha$ for some element $t = (t_{\mathfrak{p}})_{\mathfrak{p}} \in T_K$, and $\overline{x}^\ell = \overline{t} \in \widehat{K}^*/K^*$. We have $x_{\mathfrak{p}}^l = t_{\mathfrak{p}} \cdot \alpha$ with $\alpha \in K^*$ and $t_{\mathfrak{p}} \in T_{\mathfrak{p}}$ for all primes $\mathfrak{p}$.

For every integer $n \geq 1$, we now pick a prime $\mathfrak{p}$ of K such that $\mathfrak{p}$ splits completely in $K \subset K(\zeta_{\ell^n})$, but not in $K \subset K(\zeta_{\ell^{n+1}})$ and *also* not in $K(\zeta_\ell, \sqrt[\ell]{\alpha})$. This is possible because for $\ell > 2$ and $K \neq \mathbf{Q}(\zeta_3)$, the non-abelian extension $K(\zeta_\ell, \sqrt[\ell]{\alpha})$ of K of degree $\ell(\ell-1)$ has intersection $K(\zeta_\ell)$ with $K(\zeta_{\ell^{n+1}})$.

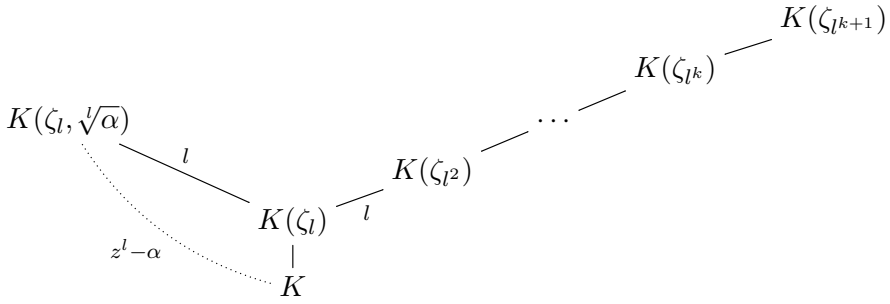


FIGURE 3.4. The splitting field of the polynomial $z^l - \alpha$ is $K(\zeta_l, \sqrt[l]{\alpha})$.

The cyclic group $T_\mathfrak{p}$ has order divisible by ℓ^n, as $K_\mathfrak{p}$ contains, by construction of $\mathfrak{p}$, an ℓ^n-th root of unity. Moreover, as α is not locally an ℓ-th power at $\mathfrak{p}$, the local root of unity $t_\mathfrak{p} \in T_\mathfrak{p}$ is not an ℓ-th power in $T_\mathfrak{p}$. As we can map $T_\mathfrak{p}$ onto a cyclic group of order ℓ^n in such a way that $t_\mathfrak{p}$ is mapped to a generator, we can define a homomorphism

$$\psi : T = T_K/\{\pm 1\} \to T_\mathfrak{p}/\{\pm 1\} \to \frac{1}{l^{n+1}}\mathbf{Z}/\mathbf{Z}$$

that satisfies $\psi(\bar{t}) = \frac{1}{l^n}$. The map ψ can be extended to $T' = \langle T, \bar{x}\rangle$ by putting $\psi(\bar{x}) = \frac{1}{l^{n+1}}$, as we have the relation $\bar{x}^\ell = \bar{t}$ in T'. The character $\ell^n\psi = \chi : T' \to \frac{1}{l}\mathbf{Z}/\mathbf{Z}$, which is independent of n, has kernel T and maps $\bar{x}$ to $\frac{1}{l}$. This shows that χ is an ℓ-divisible character on T'. So it proves Lemma 3.3.3.

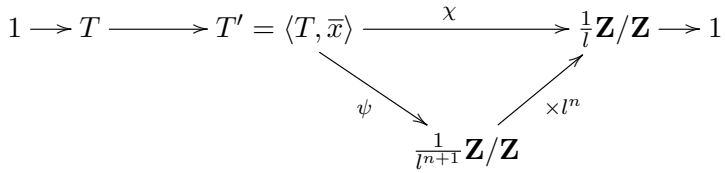


FIGURE 3.5. The l-divisible character χ.

and finishes the proof of Theorem 3.3.1. □

Our proof of Theorem 3.3.1 used in various places that ℓ is odd, so it cannot be taken over without changes to deal with the case $\ell = 2$.

3.4. Finding Minimal Galois Groups

In order to use Theorem 3.2.2 and find imaginary quadratic K for which the absolute abelian Galois group A_K is the minimal group G from Theorem 3.1.4, we need an algorithm that can effectively determine, on input K, whether the sequence of $\widehat{\mathbf{Z}}$-modules

$$1 \to \widehat{\mathcal{O}}^*/T_K \longrightarrow \widehat{K}^*/(K^* \cdot T_K) \longrightarrow \mathrm{Cl}_K \to 1 \tag{3.7}$$

from Section 3.1 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 (3.7) lying over the subgroup $\langle[\mathfrak{a}]\rangle \subset \mathrm{Cl}_K$ is nonsplit.

For the free $\widehat{\mathbf{Z}}$-module $M = \widehat{\mathcal{O}}^*/T_K$ in (3.7) we write T_p for the torsion subgroup of

$$\mathcal{O}_p^* = (\mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Z}_p)^* = \prod_{\mathfrak{p}|p} \mathcal{O}_{\mathfrak{p}}^*.$$

The p-primary part of M is the pro-p-group

$$M_p = \mathcal{O}_p^*/T_p = \prod_{\mathfrak{p}|p} (\mathcal{O}_{\mathfrak{p}}^*/T_{\mathfrak{p}}) \cong \mathbf{Z}_p^2. \tag{3.8}$$

In order to verify the hypothesis of Theorem 3.2.2, 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 (3.6) is nontrivial. This yields the following theorem.

THEOREM 3.4.1. *Let K be imaginary quadratic, and define for each prime number p dividing h_K the homomorphism*

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

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 (3.7) *is totally nonsplit if and only if all maps ϕ_p are injective.*

PROOF. Under the isomorphism (3.6), the class of the extension

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

in $\mathrm{Ext}(\mathbf{Z}/p\mathbf{Z}, M)$ corresponds by [**?**, Chapter III, Prop. 1.1] to the residue class of the element $(f^{-1}(1 \bmod p\mathbf{Z}))^p \in M/M^p$. In the case of $E[\mathfrak{a}]$, we apply this to $M = \widehat{\mathcal{O}}^*/T_K$, and choose the identification $\mathbf{Z}/p\mathbf{Z} = \langle[\mathfrak{a}]\rangle$ under which $1 \bmod p\mathbf{Z}$ is the *inverse* of $[\mathfrak{a}]$. Then $f^{-1}(1 \bmod p\mathbf{Z})$ 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 (3.4).

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 $\widehat{\mathcal{O}}^*$ that lies in the same class modulo K^* as x^p, and its image

$$(f^{-1}(1 \bmod p\mathbf{Z}))^p = x^p = x^p\alpha$$

is an element of

$$M/M^p = M_p/M_p^p = \mathcal{O}_p^*/T_p(\mathcal{O}_p^*)^p$$

that corresponds to the class of $E[\mathfrak{a}]$ in $\mathrm{Ext}(\langle[\mathfrak{a}]\rangle, \mathcal{O}^*/T_K)$.

As the idele $x = (x_\mathfrak{p})_\mathfrak{p}$ has components $x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^*$ at $\mathfrak{p} \mid p$ by the choice of $\mathfrak{a}$, we see that this image in $M_p/M_p^p = \mathcal{O}_p^*/T_p(\mathcal{O}_p^*)^p$ 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 3.4.2. In Theorem 3.4.1, 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 $K_p = K \otimes_{\mathbf{Z}} \mathbf{Z}_p$, and observe that the image of ϕ_p is in the subgroup $\mathcal{O}_p^*/T_p(\mathcal{O}_p^*)^p$ as the valuations of $\mathfrak{a}^p$ at the primes over p are divisible by p.

REMARK 3.4.3. It is possible to prove Theorem 3.4.1 without explicit reference to homological algebra. What the proof shows is that, in order to lift an ideal class of arbitrary order n under the sequence

$$1 \to \widehat{\mathcal{O}}^*/T_K \longrightarrow \widehat{K}^*/(K^* \cdot T_K) \longrightarrow \mathrm{Cl}_K \to 1, \tag{3.7}$$

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 3.1.5 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 [**?**].

Our Theorem 3.4.1 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 $\mathbf{F}_p$-vector space.

COROLLARY 3.4.4. *If* Cl_K *has* p*-rank at least* 3 *for some* p*, then the sequence* $1 \to \widehat{\mathcal{O}}^*/T_K \longrightarrow \widehat{K}^*/(K^* \cdot T_K) \longrightarrow \mathrm{Cl}_K \to 1$ *splits over some subgroup of* Cl_K *of order* p*.*

PROOF. It follows from the isomorphism in (3.8) that the image of ϕ_p lies in a group that is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^2$. If Cl_K has p-rank at

least 3, then ϕ_p will not be injective. From Theorem 3.4.1 we have that the injectivity condition is if and only if. So the result follows.

Now apply Theorem 3.4.1. □

As numerical computations in uncountable $\widehat{\mathbf{Z}}$-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 (3.7) can be found by a finite computation.

The maps ϕ_p in Theorem 3.4.1 however are linear maps between finite-dimensional $\mathbf{F}_p$-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

$$1 \to \widehat{\mathcal{O}}^*/T_K \longrightarrow \widehat{K}^*/(K^* \cdot T_K) \longrightarrow \mathrm{Cl}_K \to 1 \tag{3.7}$$

is totally nonsplit is then easily written down.

Algorithm 3.4.5.

Input: An imaginary quadratic number field K.

Output: NO if the extension (3.7) for K is not totally nonsplit, YES otherwise.

Step 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.

Step 2 For each prime p dividing h_K, compute one or two $\mathcal{O}$-ideals coprime to p, and put $n = 1$ or $n = 2$ accordingly, such that their classes in Cl_K generate $\mathrm{Cl}_K[p]$; and compute generators x_1 up to x_n for their p-th powers.

Check whether x_1 is trivial in $\mathcal{O}_p^*/T_p(\mathcal{O}_p^*)^p$.

If it is, output NO and stop.

If $n = 2$, check whether x_2 is trivial in $\mathcal{O}_p^*/T_p \cdot \langle x_1 \rangle \cdot (\mathcal{O}_p^*)^p$.

If it is, output NO and stop.

Step 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 $\mathcal{O}_p$ up to small precision. For instance, computations in $\mathbf{Z}_p^*/T_p(\mathbf{Z}_p^*)^p$ amount to computations modulo p^2 for odd p, and modulo p^3 for $p = 2$.

3.5. Minimality at 2

The splitting behavior of the sequence (3.7) depends strongly on the structure of the p-primary parts of Cl_K at the primes $p \mid h_K$. In view of Theorem 3.4.1 and Corollary 3.4.4, 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 3.6, 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 3.4.4 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 $\mathbf{F}_2$-vector space generated by the classes of the primes $\mathfrak{p}$ of K lying over the rational primes that ramify in $\mathbf{Q} \subset K$, 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 3.4.4, 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 3.4.5 by something that is much simpler.

THEOREM 3.5.1. *Let K be imaginary quadratic with even class number, and suppose that its 2-class group is cyclic. Then the sequence* (3.7) *is nonsplit over* $\mathrm{Cl}_K[2]$ *if and only if the discriminant D_K of K is of one of the following three 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 $F = \mathbf{Q}(\sqrt{p}, \sqrt{-q})$ of K, which is a quadratic extension of K with group $C_2 \times C_2$ over $\mathbf{Q}$ that is locally unramified at 2.

If we have $D_K \equiv 5 \bmod 8$, then 2 is inert in $\mathbf{Q} \subset K$, 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 3.4.1, and is not injective.

If we have $D \equiv 1 \bmod 8$ then 2 splits in $\mathbf{Q} \subset K$. In the case $p \equiv -q \equiv 1 \bmod 8$ the integers p and $-q$ are squares in $\mathbf{Z}_2^*$, 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 $\mathbf{Z}_2^*$, 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 $\mathbf{Q}_2(\sqrt{-p}) = \mathbf{Q}_2(i)$ contains a square root of $2i$, and ϕ_2 is not injective. For $p \equiv 5 \bmod 8$, the local field $\mathbf{Q}_2(\sqrt{-p}) = \mathbf{Q}_2(\sqrt{3})$ 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 3.5.2. *Let K be imaginary quadratic for which the 2-class group is noncyclic. Then the map ϕ_2 in Theorem* 3.4.1 *is not injective.*

PROOF. As every 2-torsion element in Cl_K is the class of a product of ramified primes $\mathfrak{p}$, its square can be generated by a rational number. This implies that the image of ϕ_2 is contained in the cyclic subgroup

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

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

3.6. Computational Results

In Onabe's paper [**?**], 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 (3.7), 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 3.5.1. 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 [**?**], 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 (3.7) splits mentioned explicitly, is given in Table 3.1.

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

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

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 3.1, one easily gets the impression that among all K with $h_K = p$, the fraction for which the sequence (3.7) 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 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.

In Table 3.2 we started counting for absolute discriminants exceeding $B_p \in \mathbf{Z}_{>0}$ to avoid the influence that using many very small discriminants may have on observing the asymptotic behavior. The Tables 3.3 and 3.4 make this clear, since they show how the value of $p \cdot f_p$ approximates 1, when we change B_p. Moreover we observe that for small primes the small discriminants somehow make the product $p \cdot f_p$ not to approximate 1 fast. Thus, for example, for $p = 3$ we have to start counting from discriminants greater than 10^8, for $p \cdot f_p$ to be over 0.9. On the other hand, for $p = 11$, even if we start from discriminants just greater than 1, the results are really satisfying.

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) and concluded that, at least numerically, there is no clearly visible influence; see Table 3.5.

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. The groups we examined were of the form $C_5 \times C_7 \times C_m$ with $5, 7 \nmid m$. The Tables 3.6, 3.7 and 3.8 show the numerical results of this confirmation for the primes $p = 5$ and $q = 7$. The 11, 10, 01 and 00 columns correspond to the cases where the sequence (3.7) is split over $\mathrm{Cl}_K[5]$ and $\mathrm{Cl}_K[7]$, over $\mathrm{Cl}_K[5]$ but not over $\mathrm{Cl}_K[7]$, not over $\mathrm{Cl}_K[5]$ but over $\mathrm{Cl}_K[7]$, neither over $\mathrm{Cl}_K[5]$ and $\mathrm{Cl}_K[7]$, accordingly.

Finally using our algorithm we confirm that the fraction f_p of K, with class group Cl_K of the form $C_{m \cdot p^2}$ with $p \nmid m$, is approximately equal to $1/p$; Table 3.9.

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 3.1. 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 (3.7) does not split; and the fourth column gives $-D_K$ for the fields K for which (3.7) splits.

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

TABLE 3.2. Splitting fractions at p for class number h_K divisible by $p < 100$. For the first N_p imaginary quadratic fields $K \in S_p$ of absolute discriminant $|D_K| > B_p$, we denote by f_p the fraction of K for which the sequence (3.7) is split over $\mathrm{Cl}_K[p]$. Numerically, the values for $p \cdot f_p \approx 1$ in the table show that the fraction f_p is indeed close to $1/p$.

At the following two tables the x-axis corresponds to N_p and the y-axis to $p \cdot f_p$. The symbols $-, +, \times$ corresponds to $B_p = 1, 10^5$ and 10^6 accordingly, and the "down" and "right" Y to $B_p = 10^7$ and 10^8.

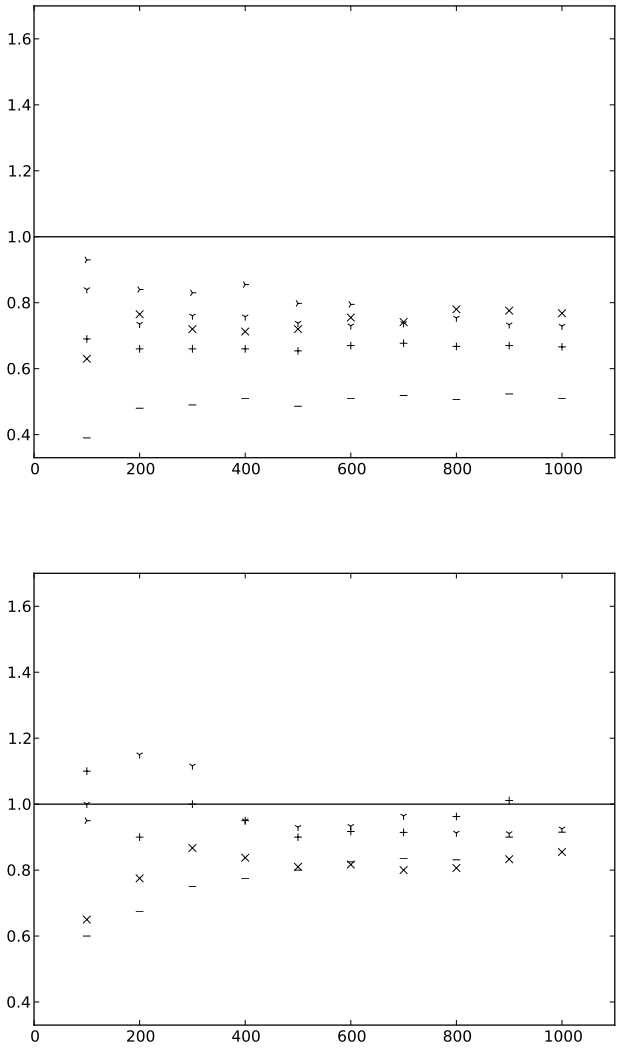


TABLE 3.3. Convergence to 1 of $p \cdot f_p$ for $p = 3$ and 5.

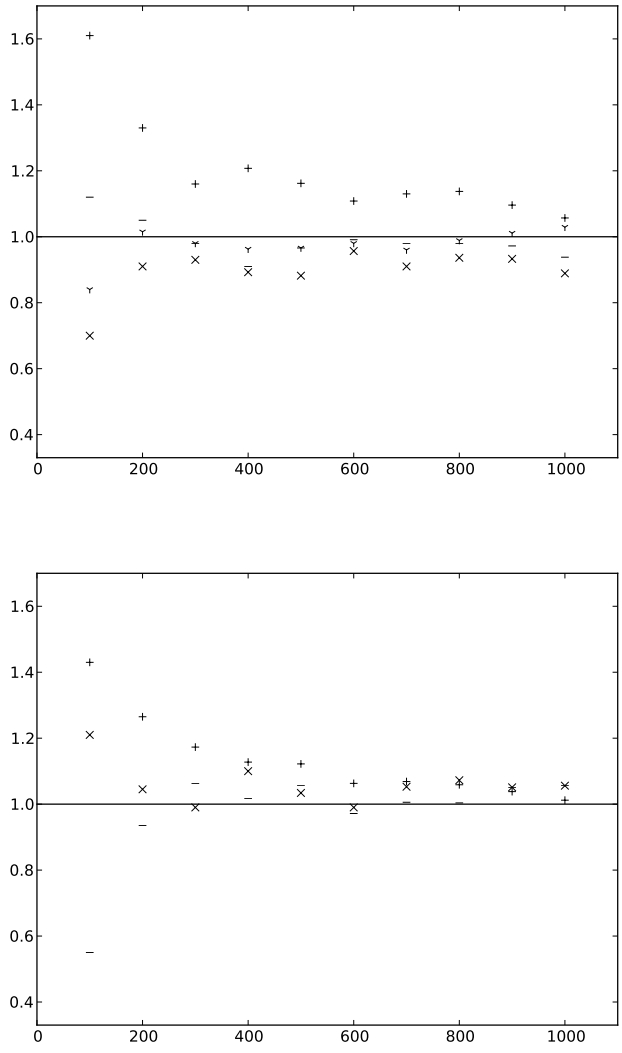


TABLE 3.4. Convergence to 1 of $p \cdot f_p$ for $p = 7$ and 11.

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 3.5. Splitting fractions at p according to local behavior at p.

B_p	11	10	01	00
10^4	0.775	1.020	1.060	0.996
10^5	0.675	0.938	1.090	1.010
10^6	1.030	0.954	1.160	0.984

TABLE 3.6. $N_p = 1400$.

B_p	11	10	01	00
10^4	0.787	0.971	1.090	1.000
10^5	0.825	0.992	0.956	1.156
10^6	0.913	0.942	1.100	1.000

TABLE 3.7. $N_p = 2400$.

B_p	11	10	01	00
10^4	0.900	0.961	1.020	1.010
10^5	0.900	0.944	1.010	1.020
10^6	0.970	0.953	1.14	0.990

TABLE 3.8. For $N_p = 2 \cdot 2400$ we observe that the approximations are better from these of Tables 3.6 and 3.7 and the best are when $B_p = 10^6$.

p	M_p	$B_p = 10^4$	$B_p = 10^5$	$B_p = 10^6$
5	100	1.070	0.935	1.100
5	200	0.978	0.957	0.995
7	100	0.964	0.931	1.030
7	200	0.911	0.900	1.020

TABLE 3.9. Once more we see that starting from fundamental discriminants $|D_K|$ greater than 10^6 gives us better approximations, and moreover if we take $M_p = 200$ we have the best results.

CHAPTER 4

Adelic Points of Elliptic Curves over Q

ABSTRACT. We apply the techniques we developed in Chapter 2 in order to explicitly determine the topological group that arises as the group of adelic points of an elliptic curve defined over the rational number field.

"The laws of nature are
but the mathematical thoughts
of God."

Euclid, lived around 300 BC

4.1. Elliptic Curves over the Adeles

The fundamental building block of all absolute abelian Galois groups A_K in Chapter 2 was the unit group $\widehat{\mathcal{O}}^*$ of the completion of the ring of integers $\widehat{\mathcal{O}}$ of the underlying number field K. We saw that, even though $\widehat{\mathcal{O}}^*$ is obtained as a product $\prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*$ of local unit groups $\mathcal{O}_{\mathfrak{p}}^*$ that vary considerably with K, the isomorphism type of the topological group $\widehat{\mathcal{O}}^*$ is to a large extent independent of K, as already the degree of the number field and its number of exceptional roots of unity (which is 'generically' equal to 1) determine the isomorphism type of $\widehat{\mathcal{O}}^*$ (Theorem 2.3.3). In the case of imaginary quadratic fields, where $\widehat{\mathcal{O}}^*$ and $U_K = \widehat{\mathcal{O}}^*/\mathcal{O}^*$ are isomorphic topological groups due to the finiteness of $\mathcal{O}^*$, this enabled us to describe $A_K = \widehat{K}^*/K^*$ very explicitly, and to find many K with isomorphic A_K.

In this chapter, we *fix* our number field to be $\mathbf{Q}$, but now consider an infinite family of objects over $\mathbf{Q}$, namely elliptic curves. There are

infinitely many different isomorphism classes of elliptic curves over $\mathbf{Q}$, but it is an open problem whether the number of different isomorphism types of point groups $E(\mathbf{Q})$ is infinite. More precisely, the group $E(\mathbf{Q})$ is a finitely generated abelian group by Mordell's theorem, and while the number of distinct isomorphism classes of torsion subgroups of $E(\mathbf{Q})$ is known to be only 15 by a celebrated theorem of Mazur, the rank of $E(\mathbf{Q})$ is not known to be uniformly bounded for all elliptic curves $E/\mathbf{Q}$. Still, it is very easy to exhibit families of elliptic curves with point groups that are isomorphic as abelian groups. This is somewhat reminiscent of the situation in Section 1.3, where we saw that many number fields with isomorphic unit groups $\mathcal{O}^*$ exist by the Dirichlet unit theorem 1.3.1.

The question that we will be investigating in this chapter, entirely in the line of Chapter 3, is whether the *adelic* point groups of elliptic curves $E/\mathbf{Q}$ can be isomorphic topological groups. In order to define these adelic point groups, we note that an elliptic curve $E/\mathbf{Q}$ is naturally an elliptic curve over the p-adic completions $\mathbf{Q}_p$ and the archimedean completion $\mathbf{Q}_\infty = \mathbf{R}$ of $\mathbf{Q}$. We call the product group

$$E(\mathbb{A}_{\mathbf{Q}}) \stackrel{\text{def}}{=} \prod_{p \leq \infty} E(\mathbf{Q}_p) = E(\mathbf{R}) \times \prod_{p \text{ prime}} E(\mathbf{Q}_p) \tag{4.1}$$

the group of *adelic points* of E. Note that, even though the elements of the $\mathbf{Q}$-algebra $\mathbb{A}_{\mathbf{Q}}$ are by their very definition 1.1 p-integral at almost all p, we do get the unrestricted product of all groups $E(\mathbf{Q}_p)$. This is because E is a smooth projective variety defined over $\mathbf{Q}$, which has $E(\mathbf{Q}_p) = E(\mathbf{Z}_p)$ at all finite primes p, as projective points may be scaled to be p-integral.

Our approach in the next two sections to describe $E(\mathbb{A}_{\mathbf{Q}})$ as a topological group will be similar to the one in Section 2.3. We first study the structure of the local point groups $E(\mathbf{Q}_p)$ for a single prime p. It will become clear that there are many possibilities for this group if we fix a large prime p and vary E. Taking the product over all p, we will prove in Lemma 4.2.2 that $E(\mathbb{A}_{\mathbf{Q}})$ is the product of $\mathbf{R}/\mathbf{Z} \times \widehat{\mathbf{Z}}$ and an infinite

product T_E of finite groups, similar to what we encountered in Lemma 2.3.1. Next, we need to determine what T_E looks like in its standard representation used in (2.10), and this leads to an analysis of the tower of division fields associated to E, as in Section 2.3.

4.2. The Structure of $E(\mathbf{Q}_p)$

For the infinite prime $p = \infty$, the structure of the group $E(\mathbf{Q}_\infty) = E(\mathbf{R})$ is well-known. It only depends on the *sign* of the discriminant $\Delta(E)$ of E, which (unlike $\Delta(E)$ itself) is independent of the model we choose for E. As topological groups, we have [**?**, Exercise 6.7 (b)]

$$E(\mathbf{R}) \cong \begin{cases} \mathbf{R}/\mathbf{Z}, & \text{if } \Delta(E) < 0; \\ \mathbf{R}/\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, & \text{if } \Delta(E) > 0. \end{cases} \tag{4.2}$$

For finite primes p, the point group $E(\mathbf{Q}_p)$ of the smooth projective curve $E/\mathbf{Q}_p$ carries a natural topology. In order to determine its structure as a topological group, we use the reduction map modulo p in the same way that we used the reduction map modulo $\mathfrak{p}$ in the exact sequence (2.8).

For our elliptic curve $E/\mathbf{Q}$, we now choose an explicit model in the form of a projective Weierstrass equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{4.3}$$

with integral coefficients $a, b \in \mathbf{Z}$ satisfying $\Delta = \Delta(E) = -(4a^3+27b^2) \neq 0$. We might even assume, analogously to [**?**, Definition p. 186], that $\mathrm{ord}_p(\Delta)$ is *minimal* among all possible short Weierstrass equations for E for each prime p, but this is actually not necessary for our purposes. Having made such a choice, we obtain a continuous reduction map

$$\phi_p : E(\mathbf{Q}_p) \longrightarrow \overline{E}(\mathbf{F}_p) \tag{4.4}$$

from the group of $\mathbf{Q}_p$-valued points to the finite set of $\mathbf{F}_p$-valued points of the curve $\overline{E}$ described by the reduced Weierstrass equation. For the primes $p \nmid 2\Delta$, the *primes of good reduction* of our model for E, the curve

$\overline{E}$ is an elliptic curve over $\mathbf{F}_p$. For such p, the reduction map ϕ_p is a homomorphism.

For the primes p of bad reduction, the curve $\overline{E}$ will have a singular point, in which case its non-singular locus $\overline{E}^{\mathrm{ns}}(\mathbf{F}_p)$ over $\mathbf{F}_p$ carries a natural group structure. We write $E_0(\mathbf{Q}_p)$ for the subgroup of $E(\mathbf{Q}_p)$ consisting of points that do not reduce to a singular point of $\overline{E}(\mathbf{F}_p)$. By [**?**, Theorem 4.1 (a)], the index of $E_0(\mathbf{Q}_p)$ in $E(\mathbf{Q}_p)$ is finite for all p. For primes of good reduction, we simply have $E_0(\mathbf{Q}_p) = E(\mathbf{Q}_p)$. On $E_0(\mathbf{Q}_p)$, the restriction of the reduction map yields a group homomorphism

$$\phi_p : E_0(\mathbf{Q}_p) \longrightarrow \overline{E}^{\mathrm{ns}}(\mathbf{F}_p) \tag{4.5}$$

for all primes p. This homomorphism is surjective, as smooth points on $\overline{E}(\mathbf{F}_p)$ can be lifted to points on $E(\mathbf{Q}_p)$ by Hensel's lemma.

LEMMA 4.2.1. *Let T_p be the torsion subgroup of $E(\mathbf{Q}_p)$. Then T_p is a finite group, and $E(\mathbf{Q}_p)/T_p$ is a free $\mathbf{Z}_p$-module of rank 1.*

If p is a prime of good reduction for E, then we have an isomorphism

$$T_p^{non\text{-}p} \cong \overline{E}(\mathbf{F}_p)^{non\text{-}p}$$

between the maximal subgroups of T_p and $\overline{E}(\mathbf{F}_p)$ that are of order coprime to p.

PROOF. On the subgroup $E_0(\mathbf{Q}_p) \subset E(\mathbf{Q}_p)$, the reduction map (4.5) gives rise to an exact sequence

$$1 \to E_1(\mathbf{Q}_p) \longrightarrow E_0(\mathbf{Q}_p) \longrightarrow \overline{E}^{\mathrm{ns}}(\mathbf{F}_p) \to 1. \tag{4.6}$$

The *kernel of reduction* $E_1(\mathbf{Q}_p)$ is a pro-p-group that we can describe as a $\mathbf{Z}_p$-module using the formal group of E as in [**?**, Chapter IV]. With our choice of model (4.3), one finds just as in [**?**, Chapter II, Theorem 4.1 and Proposition 5.4] that $E_1(\mathbf{Q}_p)$ is torsionfree, and free of rank 1 over $\mathbf{Z}_p$. As $E_1(\mathbf{Q}_p)$ is of finite index $\#\overline{E}^{\mathrm{ns}}(\mathbf{F}_p)$ in $E_0(\mathbf{Q}_p)$, and $E_0(\mathbf{Q}_p)$ is itself of finite index in $E(\mathbf{Q}_p)$, we find that the p-primary part of $E(\mathbf{Q}_p)$ is a finitely generated $\mathbf{Z}_p$-module of free rank one, whereas its non-p part

is a finite group of order coprime to p. We can non-canonically write

$$E(\mathbf{Q}_p) \cong \mathbf{Z}_p \times T_p,$$

with T_p the finite torsion group of $E(\mathbf{Q}_p)$. In case p is a prime of good reduction, we have $E(\mathbf{Q}_p) = E_0(\mathbf{Q}_p)$ and $\overline{E}^{\mathrm{ns}}(\mathbf{F}_p) = \overline{E}(\mathbf{F}_p)$, so the non-$p$-part of the sequence (4.6) yields an isomorphism

$$E(\mathbf{Q}_p)^{\text{non-}p} = T_p^{\text{non-}p} \cong \overline{E}(\mathbf{F}_p)^{\text{non-}p},$$

as was to be shown. □

Given an elliptic curve $E/\mathbf{Q}$, the preceding proof shows that we have isomorphisms of topological groups

$$E(\mathbf{Q}_p) \cong T_p \times \mathbf{Z}_p$$

for all primes p, with T_p a finite group of which we can describe the non-p-part in an easy way for $p \nmid 2\Delta$. Taking the product over all primes $p \leq \infty$, we obtain the following result.

LEMMA 4.2.2. *For the group of adelic points of an elliptic curve $E/\mathbf{Q}$, we have an isomorphism of topological groups*

$$E(\mathbb{A}_{\mathbf{Q}}) \cong E(\mathbf{R}) \times \widehat{\mathbf{Z}} \times \prod_p T_p,$$

with $T_p \subset E(\mathbf{Q}_p)$ the finite torsion subgroup of $E(\mathbf{Q}_p)$. □

Since the structure of $E(\mathbf{R})$ is known from (4.2), we need to find an explicit description of the infinite product of finite groups

$$T_E = \prod_p T_p$$

in order to finish our description of $E(\mathbb{A}_{\mathbf{Q}})$.

4.3. Torsion in $E(\mathbb{A}_{\mathbf{Q}})$

For the product $T_E = \prod_p T_p$ of local torsion groups at the finite primes p that occurs in Lemma 4.2.2, we want to determine the exponents

$e(\ell, k)$ for the number of cyclic summands of prime power order in the standard representation

$$T_E = \prod_{\ell \text{ prime}} \prod_{k=1}^{\infty} (\mathbf{Z}/\ell^k\mathbf{Z})^{e(\ell,k)} \tag{4.7}$$

of T_E. In the analogous situation of the closure T_K of the torsion subgroup of $\widehat{\mathcal{O}}^*$ in Section 2.3, we found in Theorem 2.3.3 that we had $e(\ell, k) = \omega$ for all but finitely many prime powers ℓ^k, and characterized the 'missing' prime powers in terms of the number of exceptional roots of unity in K. In the elliptic situation, the cyclotomic extension of K generated by the ℓ^k-th roots of unity will be replaced by the ℓ^k-division field

$$Z_E(\ell^k) \stackrel{\text{def}}{=} \mathbf{Q}(E[\ell^k](\overline{\mathbf{Q}})) \tag{4.8}$$

of the elliptic curve E. This is the finite Galois extension of $\mathbf{Q}$ obtained by adjoining the coordinates of all ℓ^k-torsion points of E to $\mathbf{Q}$. More precisely, we have the following.

LEMMA 4.3.1. *Let $E/\mathbf{Q}$ be an elliptic curve, and $\ell^k > 1$ a prime power for which the inclusion*

$$Z_E(\ell^k) \subset Z_E(\ell^{k+1})$$

of division fields is strict. Then we have $e(\ell, k) = \omega$ in the standard representation (4.7) *of the group T_E.*

PROOF. Let p be a prime of good reduction of E, and suppose that p splits completely in the division field $Z_E(\ell^k)$, but not in the larger division field $Z_E(\ell^{k+1})$. Then the elliptic curve $\overline{E} = (E \bmod p)$ has its full ℓ^k-torsion defined over $\mathbf{F}_p$, but not its full ℓ^{k+1}-torsion. It follows that the group $\overline{E}(\mathbf{F}_p)$, which contains a subgroup isomorphic to $(\mathbf{Z}/\ell^k\mathbf{Z})^2$ but not one isomorphic to $(\mathbf{Z}/\ell^{k+1}\mathbf{Z})^2$, has a cyclic direct summand of order ℓ^k.

The set of primes p that split completely in $Z_E(\ell^k)$, but not in $Z_E(\ell^{k+1})$, is infinite and has positive density

$$[Z_E(\ell^k) : \mathbf{Q}]^{-1} - [Z_E(\ell^{k+1}) : \mathbf{Q}]^{-1} > 0$$

by a 19th century theorem of Frobenius. Alternatively, one may invoke the Chebotarev density theorem to obtain this density.

For all primes $p \neq \ell$ of good reduction in the infinite set thus obtained, the group $\overline{E}(\mathbf{F}_p)$, and therefore also T_p, has a cyclic direct summand of order ℓ^k. This yields $e(\ell, k) = \omega$ for the group T_E in (4.7). □

It follows from Lemmas 4.2.2 and 4.3.1 that for elliptic curves E having the property that for all primes ℓ, the tower of ℓ-power division fields has strict inclusions

$$Z_E(\ell) \subsetneq Z_E(\ell^2) \subsetneq Z_E(\ell^3) \subsetneq \cdots \subsetneq Z_E(\ell^k) \subsetneq \cdots \tag{4.9}$$

at every level, the group T_E is the universal group $\prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}$ for which we have $e(\ell, k) = \omega$ in the standard representation (4.7). In this situation, the group $E(\mathbb{A}_{\mathbf{Q}})$ of adelic points of E is isomorphic to the "generic group"

$$\mathcal{E} = \mathbf{R}/\mathbf{Z} \times \widehat{\mathbf{Z}} \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}. \tag{4.10}$$

4.4. Universality of the Generic Adelic Point Group $\mathcal{E}$

In this section, we prove that for 'almost all' elliptic curves $E/\mathbf{Q}$, their adelic point group $E(\mathbb{A}_{\mathbf{Q}})$ is isomorphic to the generic group $\mathcal{E}$ in (4.10).

In order to make this 'almost all' mathematically precise, we let $C(t)$ for $t \in \mathbf{R}_{>0}$ be the finite set of elliptic curves that are given by a Weierstrass equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

as in (4.3) satisfying the inequalities $|a| \leq t^2$, $|b| \leq t^3$. Note that every elliptic curve $E/\mathbf{Q}$ is $\mathbf{Q}$-isomorphic to some elliptic curve in $C(t)$ for t sufficiently large, but that this curve is usually not unique as the coefficient pairs (a, b) and (r^4a, r^6b) for an integer $r \neq 0$ give rise to $\mathbf{Q}$-isomorphic elliptic curves. We view $C = \bigcup_{t>0} C(t)$ as the collection of all elliptic curves defined over $\mathbf{Q}$, and say that a subset $S \subset C$ has density δ if we have

$$\lim_{t\to\infty} \frac{\#(S \cap C(t))}{\#C(t)} = \delta.$$

Clearly, such densities assume values in the closed interval $[0, 1]$. If S is the collection of elliptic curves in C with some given property P, we say, somewhat informally, that *almost all elliptic curves* $E/\mathbf{Q}$ *have property* P in case S has density 1.

There are other possible ways to list elliptic curves over $\mathbf{Q}$, but with this definition, we can quote the following title of a 2010 paper by Nathan Jones [**?**] as a theorem with a precise mathematical meaning.

THEOREM 4.4.1. *Almost all elliptic curves are Serre curves.*

To understand the importance of this result in our context, we recall what it means for an elliptic curve $E/\mathbf{Q}$ to be a Serre curve. It is a maximality property for the Galois representation

$$\rho_E : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow A = \mathrm{Aut}(E(\overline{\mathbf{Q}})^{\mathrm{tor}})$$

describing the action of the absolute Galois group of $\mathbf{Q}$ by group automorphisms on the group $E(\overline{\mathbf{Q}})^{\mathrm{tor}}$ of all torsion points of E. As $E(\overline{\mathbf{Q}})^{\mathrm{tor}}$ is isomorphic to $(\mathbf{Q}/\mathbf{Z})^2 = \varinjlim_n (\frac{1}{n}\mathbf{Z}/\mathbf{Z})^2$ as an abstract abelian group, we can explicitly describe the group A as

$$A = \mathrm{Aut}\, E(\overline{\mathbf{Q}})^{\mathrm{tor}} \cong \varprojlim_n \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) = \mathrm{GL}_2(\widehat{\mathbf{Z}}),$$

and ρ_E is a continuous homomorphism of profinite groups. The *image of Galois* for the representation ρ_E is the subgroup

$$G = \rho_E[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})] \subset A.$$

It can be identified with the Galois group over $\mathbf{Q}$ of the infinite number field $\mathbf{Q}(E(\overline{\mathbf{Q}})^{\mathrm{tor}})$ obtained by taking the compositum of all division fields of E. Serre's theorem [**?**] states that this group is 'large' for most E. More precisely, if $E/\mathbf{Q}$ is without complex multiplication over $\overline{\mathbf{Q}}$ – a property that almost all elliptic curves $E/\mathbf{Q}$ have in the sense defined above – then G is an open subgroup of finite index in A. On A, we have a non-trivial quadratic character

$$\chi_2 : A = \mathrm{Aut}\, E(\overline{\mathbf{Q}})^{\mathrm{tor}} \longrightarrow \mathrm{Aut}\, E[2](\overline{\mathbf{Q}}) \cong \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \cong S_3 \to \{\pm 1\}$$

that maps an automorphism of $E(\overline{\mathbf{Q}})^{\mathrm{tor}}$ to the sign of the permutation by which it acts on the three non-trivial 2-torsion points of E. A field automorphism σ of $\overline{\mathbf{Q}}$ naturally induces a permutation of the non-trivial 2-torsion points of E, which generate the 2-division field $Z_E(2)$ of E. The sign $\varepsilon(\sigma)$ of this permutation is reflected in the action of σ on the subfield $\mathbf{Q}(\sqrt{\Delta}) \subset Z_E(2)$ that is generated by the square root of the discriminant $\Delta = \Delta_E$ of the elliptic curve E, and given by

$$\varepsilon(\sigma) = \sigma(\sqrt{\Delta})/\sqrt{\Delta}.$$

The Dirichlet character $\widehat{\mathbf{Z}}^* \to \{\pm 1\}$ corresponding to $\mathbf{Q}(\sqrt{\Delta})$ can be seen as a character

$$\chi_\Delta : A \cong \mathrm{GL}_2(\widehat{\mathbf{Z}}) \xrightarrow{\det} \widehat{\mathbf{Z}}^* \to \{\pm 1\}$$

on A. It is different from the character χ_2, which does not factor via the determinant map $A \xrightarrow{\det} \widehat{\mathbf{Z}}^*$ on A.

The *Serre character* $\chi_E : A \to \{\pm 1\}$ associated to E is the non-trivial quadratic character obtained as the product $\chi_2\chi_\Delta$. By construction, it vanishes on the image of Galois $G \subset A$, so the image of Galois is never the full group A. In the case where we have $G = \ker \chi_E$, we say that E is a *Serre curve*.

If E is a Serre curve, then the image of Galois is so close to the full group $A \cong \mathrm{GL}_2(\widehat{\mathbf{Z}})$ that for every prime power $\ell^k > 1$, the extension

$$Z_E(\ell^k) \subset Z_E(\ell^{k+1})$$

of division fields for E that occurs in Lemma 4.3.1 has its 'generic' degree ℓ^4 for odd ℓ, and at least degree ℓ^3 for $\ell = 2$. In particular, the hypothesis of Lemma 4.3.1 on E is satisfied for all prime powers ℓ^k in case E is a Serre curve. We immediately deduce the following theorem.

THEOREM 4.4.2. *For almost all elliptic curves $E/\mathbf{Q}$, the adelic point group $E(\mathbb{A}_{\mathbf{Q}})$ is isomorphic to the topological group*

$$\mathcal{E} = \mathbf{R}/\mathbf{Z} \times \widehat{\mathbf{Z}} \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}. \qquad \square$$

4.5. Existence of Non-Generic Adelic Point Groups

The hypothesis that E be a Serre curve, which guarantees that the division field extensions

$$Z_E(\ell^k) \subset Z_E(\ell^{k+1}) \tag{4.11}$$

have full degree ℓ^4 for all prime powers $\ell^k > 1$, is much stronger than what is needed in order to apply Lemma 4.3.1. In fact, one wonders for which elliptic curves there exist prime powers ℓ^k for which one encounters equality in (4.11). In the case of *odd* prime powers, equality never occurs.

THEOREM 4.5.1. *For $E/\mathbf{Q}$ an elliptic curve and ℓ an odd prime, the division field extension $Z_E(\ell^k) \subset Z_E(\ell^{k+1})$ is strict for all $k \in \mathbf{Z}_{\geq 0}$.*

PROOF. In the case $k = 0$, which is not relevant in the context of Lemma 4.3.1, the inequality $\mathbf{Q} = Z_E(1) \subset Z_E(\ell)$ is strict because $Z_E(\ell)$ contains a root of unity ζ_ℓ of odd order ℓ, and $\mathbf{Q}$ does not.

For $k = 1$, we need to show that the natural surjection

$$\pi : G_{\ell^2} = \mathrm{Gal}(Z_E(\ell^2)/\mathbf{Q}) \to G_\ell = \mathrm{Gal}(Z_E(\ell)/\mathbf{Q})$$

is not an isomorphism.

The action of G_{ℓ^2} on the ℓ^2-th roots of unity in $Z_E(\ell^2)$ leads to a surjective map $G_{\ell^2} \xrightarrow{\det} (\mathbf{Z}/\ell^2\mathbf{Z})^*$, and as ℓ is odd, we can pick an element $c \in G_{\ell^2}$ that maps to a generator of $(\mathbf{Z}/\ell^2\mathbf{Z})^*$. Its restriction $\pi(c) \in G_\ell$

then maps to a generator of $\mathbf{F}_\ell^* = (\mathbf{Z}/\ell\mathbf{Z})^*$ under the map $G_\ell \xrightarrow{\det} (\mathbf{Z}/\ell\mathbf{Z})^*$.

Suppose that π is an isomorphism. Then the order of $\pi(c)$ equals the order of c, which is divisible by the order $\ell(\ell-1)$ of $(\mathbf{Z}/\ell^2\mathbf{Z})^*$. Let $s \in G_l$ be a power of $\pi(c)$ of order ℓ. Then $s \in G_\ell \subset \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbf{F}_\ell)$, when viewed as a 2×2-matrix over the field $\mathbf{F}_\ell$, is a non-semisimple matrix with double eigenvalue 1. As $\pi(c)$ centralizes this element, its eigenvalues as an element of $\mathrm{Aut}(E[\ell])$ cannot be distinct, and we find that $\det(\pi(c))$ is a square in $\mathbf{F}_\ell^*$. Contradiction. (This neat argument is due to Hendrik Lenstra.)

Once we know that $\ker \pi$ contains a non-trivial element $x_1 \in G_{\ell^2}$, we can write it as $x_1 = 1 + \ell y_1 \in \mathrm{Aut}(E[\ell^2]) \subset \mathrm{End}(E[\ell^2])$ for some element $y_1 \in \mathrm{End}(E[\ell^2])$ with $\ell y_1 \neq 0$. Let x_k for $k \geq 2$ be an element in $G_{\ell^{k+1}} = \mathrm{Gal}(Z_E(\ell^{k+1})/\mathbf{Q})$ that restricts to x_1 on $Z_E(\ell^2)$. Then we can write $x_k = 1 + \ell y_k \in \mathrm{End}(E[\ell^{k+1}])$ for some $y_k \in \mathrm{End}(E[\ell^{k+1}])$ with $\ell y_k \neq 0$, and

$$x_k^{\ell^{k-1}} = 1 + \ell^k y_k + \ell^{k+1} z_k \in \mathrm{End}(E[\ell^{k+1}])$$

is a non-trivial element in the kernel of the natural map

$$G_{\ell^{k+1}} = \mathrm{Gal}(Z_E(\ell^{k+1})/\mathbf{Q}) \to G_{\ell^k} = \mathrm{Gal}(Z_E(\ell^k)/\mathbf{Q}).$$

Note that this is analogous to the situation for the cyclotomic $\mathbf{Z}_\ell$-extension that we had in (2.11): if $K(\zeta_\ell) \subset K(\zeta_{\ell^2})$ is a non-trivial extension, then so is $K(\zeta_{\ell^k}) \subset K(\zeta_{\ell^{k+1}})$ for $k > 1$. □

For the prime $\ell = 2$, the situation is different. There are many elliptic curves for which the previous theorem fails in the case $k = 0$, as we have $\mathbf{Q} = Z_E(2)$ in case E is defined by an affine Weierstrass equation $y^2 = f(x)$ for a cubic polynomial $f \in \mathbf{Q}[x]$ having 3 rational roots. This is however irrelevant in the context of Lemma 4.3.1.

It follows from the complete classification (for non-CM elliptic curves $E/\mathbf{Q}$) of all possible 2-adic images of the Galois representation (4.4)

from Rouse and Zureick-Brown [**?**] that there do exist infinite families of elliptic curves E for which we have $Z_E(2) = Z_E(4)$. Non-CM curves E always have $Z_E(4) \subsetneq Z_E(8)$ according to the classification, and this implies, by a slight adaptation of the argument in the proof of Theorem 4.5.1, that for such E the inclusion $Z_E(2^k) \subsetneq Z_E(2^{k+1})$ is strict for all $k \geq 2$.

We include a construction of elliptic curves with $Z_E(2) = Z_E(4)$, which is elementary and probably classical.

THEOREM 4.5.2. *For every positive rational number r, the elliptic curve E_r defined by the affine Weierstrass equation*

$$y^2 = x(x^2 - 2(1 - 4r^4)x + (1 + 4r^4)^2)$$

has division fields $Z_{E_r}(2) = Z_{E_r}(4) = \mathbf{Q}(i)$. Conversely, every elliptic curve $E/\mathbf{Q}$ with $Z_E(2) = Z_E(4) = \mathbf{Q}(i)$ is $\mathbf{Q}$-isomorphic to E_r for some rational number r.

PROOF. Let E be an elliptic curve over $\mathbf{Q}$ defined by a Weierstrass equation $y^2 = f(x)$, and suppose that we have $Z_E(2) = Z_E(4) = \mathbf{Q}(i)$. Then $f \in \mathbf{Q}[x]$ is a monic cubic polynomial with splitting field $Z_E(2) = \mathbf{Q}(i)$, so f has one rational root, and two complex conjugate roots in $\mathbf{Q}(i) \setminus \mathbf{Q}$. After translating x over the rational root, we may take 0 to be the rational root of f, leading to the model

$$f(x) = x(x - \alpha)(x - \overline{\alpha}) \tag{4.12}$$

for E for some element $\alpha \in \mathbf{Q}(i) \setminus \mathbf{Q}$. Note that in this model, the $\mathbf{Q}$-isomorphism class of E does not change if we replace α by its conjugate or multiply it by the square of a non-zero rational number.

The equality $Z_E(4) = \mathbf{Q}(i)$ means that the 4-torsion of E is defined over $\mathbf{Q}(i)$, or, equivalently, that the 2-torsion subgroup $E[2](\mathbf{Q}(i))$ of E is contained in $2 \cdot E(\mathbf{Q}(i))$. In terms of the complete 2-descent map [**?**, Proposition 1.4, p. 315] over $K = \mathbf{Q}(i)$, which embeds $E(K)/2E(K)$ in a subgroup of $K^*/(K^*)^2 \times K^*/(K^*)^2$, the inclusion $E[2](\mathbf{Q}(i)) \subset 2 \cdot E(\mathbf{Q}(i))$

amounts to the statement that all differences between the roots of f are squares in $\mathbf{Q}(i)$. In other words, we have $Z_E(2) = Z_E(4) = \mathbf{Q}(i)$ if and only if α and $\alpha - \overline{\alpha}$ are squares in $\mathbf{Q}(i)$.

Writing $\alpha = (a + bi)^2$ with $ab \neq 0$, we can scale $a + bi$ inside the $\mathbf{Q}$-isomorphism class of E by an element of $\mathbf{Q}^*$, and flip signs of a and b. Thus we may take $\alpha = (1 + qi)^2$, with q a positive rational number. The fact that $\alpha - \overline{\alpha} = 4qi = (q/2)(2 + 2i)^2$ is a square in $\mathbf{Q}(i)$ means that $q/2 = r^2$ is the square of some positive rational number r. Substituting $\alpha = (1 + 2ir^2)^2$ in the model (4.12) that we use for E, we find that E is $\mathbf{Q}$-isomorphic to

$$E_r : \quad y^2 = x(x^2 - 2(1 - 4r^4)x + (1 + 4r^4)^2) \tag{4.13}$$

for some positive rational number r. As we have shown that E_r does have $Z_{E_r}(2) = Z_{E_r}(4) = \mathbf{Q}(i)$, this proves the theorem. □

The implications of Theorem 4.5.2 for elliptic curves $E/\mathbf{Q}$ having a behavior different from the generic behavior in Theorem 4.4.2 are as follows.

THEOREM 4.5.3. *The family of elliptic curves E_r given by* (4.13) *is non-isotrivial, i.e., of non-constant j-invariant, and for none of the elliptic curves E_r with $r \in \mathbf{Q}^*$ is the adelic point group $E_r(\mathbb{A}_{\mathbf{Q}})$ isomorphic to the topological group $\mathcal{E}$ occurring in Theorem 4.4.2.*

PROOF. The non-isotriviality follows from the fact that the j-invariant

$$j(E_r) = 1728\frac{-32(1 - 4r^4)^3}{-32(1 - 4r^4)^3 + 27(1 + 4r^4)^8}$$

of E_r is not constant.

We know that an elliptic curve E for which we have a strict inequality $Z_E(2) \subsetneq Z_E(4)$ has a product of local non-archimedean torsion groups T_E for which the standard representation (4.7) has $e(2, 1) = \omega$. We will now show that the groups T_{E_r} for the elliptic curves E_r in (4.13) all have a zero number $e(2, 1) = 0$ of direct summands $\mathbf{Z}/2\mathbf{Z}$. This implies that

they are not isomorphic to the universal group $\mathcal{E}$ from Theorem 4.4.2, as desired.

For the elliptic curves E_r in (4.13) we have $Z_{E_r}(2) = Z_{E_r}(4) = \mathbf{Q}(i)$, and $E_r[2](\mathbf{Q}) = \langle (0,0) \rangle$. If $P \in E_r[4](\mathbf{Q}(i))$ is a point of order 4 for which $2P$ is a non-rational 2-torsion point on E_r, then $Q = P + P^\sigma \in E_r[4](\mathbf{Q}(i))$ is a 4-torsion point that is invariant under the complex conjugation automorphism σ of $\mathbf{Q}(i)$ and satisfies $2Q = 2P + (2P)^\sigma = (0,0)$. This shows that we have $E_r[4](\mathbf{Q}) = \langle Q \rangle \cong \mathbf{Z}/4\mathbf{Z}$.

If p is now any prime of $\mathbf{Q}$, possibly $p = \infty$, we find

$$E_r[4](\mathbf{Q}_p) = E_r[4](\mathbf{Q}_p \cap \mathbf{Q}(i)) = \begin{cases} E_r[4](\mathbf{Q}) \cong \mathbf{Z}/4\mathbf{Z}, & \text{if } i \notin \mathbf{Q}_p; \\ E_r[4](\mathbf{Q}(i)) \cong (\mathbf{Z}/4\mathbf{Z})^2, & \text{if } i \in \mathbf{Q}_p. \end{cases}$$

Thus no summand $\mathbf{Z}/2\mathbf{Z}$ ever arises, and we find $e(2,1) = 0$ as claimed. □

Abstract

The present thesis focuses on two questions that are not obviously related. Namely,

(1) *What does the absolute abelian Galois group A_K of an imaginary quadratic number field K look like, as a topological group?*
(2) *What does the adelic point group of an elliptic curve over $\mathbf{Q}$ look like, as a topological group?*

For the first question, the focus on *abelian* Galois groups provides us with *class field theory* as a tool to analyze A_K. The older work in this area, which goes back to Kubota and Onabe, provides a description of the Pontryagin dual of A_K in terms of infinite families, at each prime p, of so called *Ulm invariants* and is very indirect. Our direct class field theoretic approach shows that A_K contains a subgroup U_K of finite index isomorphic to the unit group $\widehat{\mathcal{O}}^*$ of the profinite completion $\widehat{\mathcal{O}}$ of the ring of integers of K, and provides a completely explicit description of the topological group U_K that is almost *independent* of the imaginary quadratic field K. More precisely, for *all* imaginary quadratic number fields different from $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-2})$, we have

$$U_K \cong U = \widehat{\mathbf{Z}}^2 \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}.$$

The exceptional nature of $\mathbf{Q}(\sqrt{-2})$ was missed by Kubota and Onabe, and their theorems need to be corrected in this respect.

Passing from the 'universal' subgroup U_K to A_K amounts to a group extension problem for adelic groups that may be 'solved' by passing to a suitable quotient extension involving the maximal $\widehat{\mathbf{Z}}$-free quotient

U_K/T_K of U_K. By 'solved' we mean that for each K that is sufficiently small to allow explicit class group computations for K, we obtain a practical algorithm to compute the splitting behavior of the extension. In case the quotient extension is *totally non-split*, the conclusion is that A_K is isomorphic as a topological group to the universal group U. Conversely, any splitting of the p-part of the quotient extension at an odd prime p leads to groups A_K that are *not* isomorphic to U. For the prime 2, the situation is special, but our control of it is much greater as a result of the wealth of theorems on 2-parts of quadratic class groups.

Based on numerical experimentation, we have gained a basic understanding of the distribution of isomorphism types of A_K for varying K, and this leads to challenging conjectures such as "100% of all imaginary quadratic fields of prime class number have A_K isomorphic to the universal group U".

In the case of our second question, which occurs implicitly in [**?**, Section 9, Question 1] with a view towards recovering a number field K from the adelic point group $E(\mathbb{A}_K)$ of a suitable elliptic curve over K, we can directly apply the standard tools for elliptic curves over number fields in a method that follows the lines of the determination of the structure of $\widehat{\mathcal{O}}^*$ we encountered for our first question.

It turns out that, for the case $K = \mathbf{Q}$ that is treated in Chapter 4, the adelic point group of 'almost all' elliptic curves over $\mathbf{Q}$ is isomorphic to a universal group

$$\mathcal{E} = \mathbf{R}/\mathbf{Z} \times \widehat{\mathbf{Z}} \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}$$

that is somewhat similar in nature to U. The reason for the universality of adelic point groups of elliptic curves lies in the tendency of elliptic curves to have Galois representations on their group of $\overline{\mathbf{Q}}$-valued torsion points that are very close to being maximal. For $K = \mathbf{Q}$, maximality of the Galois representation of an elliptic curve E means that E is a so-called Serre-curve, and it has been proved recently by Nathan Jones

[**?**] that 'almost all' elliptic curves over $\mathbf{Q}$ are of this nature. In fact, universality of $E(\mathbb{A}_K)$ requires much less than maximality of the Galois representation, and the result is that it actually requires some effort to construct families of elliptic curves with non-universal adelic point groups. We provide an example at the end of Chapter 4.

Résumé

Cette thèse traite de deux problèmes dont le lien n'est pas apparent :

(1) *À quoi ressemble l'abélianisé A_K du groupe de Galois absolu d'un corps quadratique imaginaire K, comme groupe topologique?*
(2) *À quoi ressemble le groupe des points adéliques d'une courbe elliptique sur $\mathbf{Q}$, comme groupe topologique?*

Pour la première question, la restriction au groupe de Galois *abélianisé* nous permet d'utiliser la *théorie du corps de classes* pour analyser A_K. Les travaux précédents dans ce domaine, qui remontent à Kubota et Onabe, décrivent le dual de Pontryagin de A_K en termes de familles infinies d'*invariants de Ulm* à chaque premier p, très indirectement. Notre approche directe par théorie du corps de classes montre que A_K contient un sous-groupe U_K d'indice fini isomorphe au groupe des unités $\widehat{\mathcal{O}}^*$ de la complétion profinie $\widehat{\mathcal{O}}$ de l'anneau des entiers de K, et décrit explicitement le groupe topologique U_K, essentiellement *indépendamment* du corps quadratique imaginaire K. Plus précisément, pour *tout* corps quadratique imaginaire différent de $\mathbf{Q}(i)$ et $\mathbf{Q}(\sqrt{-2})$, on a

$$U_K \cong U = \widehat{\mathbf{Z}}^2 \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}.$$

Le caractère exceptionnel de $\mathbf{Q}(\sqrt{-2})$ n'apparaît pas dans les travaux de Kubota et Onabe, et leurs résultats doivent être corrigés sur ce point.

Passer du sous-groupe «universel» U_K à A_K revient à un problème d'extension pour des groupes adéliques qu'il est possible de «résoudre» en passant à une extension de quotients convenables impliquant le quotient

$\widehat{\mathbf{Z}}$-libre maximal U_K/T_K de U_K. Par «résoudre», nous entendons que, pour chaque K suffisamment petit pour permettre des calculs de groupe de classes explicites, nous obtenons un algorithme praticable décidant le comportement de cette extension. Si elle est *totalement non-scindée*, alors A_K est isomorphe comme groupe topologique au groupe universel U. Réciproquement, si l'extension tensorisée par $\mathbf{Z}_p$ se scinde pour un premier p impair, alors A_K n'est *pas* isomorphe à U. Pour le premier 2, la situation est particulière, mais elle reste contrôlée grâce à l'abondance de résultats sur la 2-partie des groupes de classes de corps quadratiques.

Nos expérimentations numériques ont permis de mieux comprendre la distribution des types d'isomorphismes de A_K quand K varie, et nous conduisent à des conjectures telles que «pour 100% des corps quadratiques imaginaires K de nombre de classes premier, A_K est isomorphe au groupe universel U».

Pour notre deuxième problème, qui apparaît implicitement dans [**?**, Section 9, Question 1] (dans le but de reconstruire le corps de nombres K à partir du groupe des points adéliques $E(\mathbb{A}_K)$ d'une courbe elliptique convenable sur K), nous pouvons appliquer les techniques usuelles pour les courbes elliptiques sur les corps de nombres, en suivant les mêmes étapes que pour déterminer la structure du groupe $\widehat{\mathcal{O}}^*$ rencontré dans notre premier problème.

Il s'avère que, dans le cas $K = \mathbf{Q}$ que nous traitons au Chapitre 4, le groupe des points adéliques de «presque toutes» les courbes elliptiques sur $\mathbf{Q}$ est isomorphe à un groupe universel

$$\mathcal{E} = \mathbf{R}/\mathbf{Z} \times \widehat{\mathbf{Z}} \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}$$

de nature similaire au groupe U. Cette universalité du groupe des points adéliques des courbes elliptiques provient de la tendance qu'ont les représentations galoisiennes attachées (sur le groupe des points de torsion à

valeurs dans $\overline{\mathbf{Q}}$) à être maximales. Pour $K = \mathbf{Q}$, la représentation galoisienne est maximale si est seulement si la courbe E est une courbe de Serre, et Nathan Jones [**?**] a récemment démontré que «presque toutes» les courbes elliptiques sur $\mathbf{Q}$ sont de cette nature. En fait, l'universalité de $E(\mathbb{A}_K)$ suit d'hypothèses bien plus faibles, et il n'est pas facile de construire des familles de courbes elliptiques dont le groupe des points adéliques n'est pas universel. Nous donnons un tel exemple à la fin du Chapitre 4.

Samenvatting

Dit proefschrift is gewijd aan twee vragen die niet evident gerelateerd zijn:

(1) *Hoe ziet de absolute abelse Galois group A_K van een imaginair kwadratisch getallenlichaam K er uit, als een topologische groep?*
(2) *Hoe ziet de adelische puntengroep van een elliptische kromme over $\mathbf{Q}$ er uit, als een topologische groep?*

In het geval van de eerste vraag geeft de restrictie tot *abelse* Galoisgroepen ons de *klassenlichamentheorie* als natuurlijk instrument om A_K te analyseren. Eerder werk op dit gebied, dat teruggaat op Kubota en Onabe, geeft een beschrijving van de Pontryagin-duale van A_K in termen van oneindige families, één per priemgetal p, van zogenaamde *Ulm invarianten*, en is daarmee zeer indirect. Onze directe aanpak via de klassenlichamentheorie laat zien dat A_K een ondergroep U_K van eindige index bevat die isomorf is met de eenhedengroep $\widehat{\mathcal{O}}^*$ van de pro-eindige completering $\widehat{\mathcal{O}}$ van de ring van gehelen van K, en verschaft een geheel expliciete beschrijving van de topologische groep U_K die vrijwel *onafhankelijk* is van het imaginair kwadratische lichaam K. Preciezer geformuleerd hebben we voor *ieder* imaginair kwadratisch lichaam K verschillend van $\mathbf{Q}(i)$ en $\mathbf{Q}(\sqrt{-2})$ een isomorfisme

$$U_K \cong U = \widehat{\mathbf{Z}}^2 \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}.$$

Kubota en Onabe waren zich niet bewust van het uitzonderlijke gedrag van $\mathbf{Q}(\sqrt{-2})$, en hun stellingen moeten dan ook dienovereenkomstig gecorrigeerd worden.

Om van de 'universele' ondergroep U_K tot A_K te komen moet een adelische groepsextensie berekend worden, en dat is mogelijk voor de quotiënt-extensie behorende bij het maximale $\widehat{\mathbf{Z}}$-vrije quotiënt U_K/T_K van U_K. Met 'mogelijk' bedoelen we dat we voor iedere K die voldoende klein is om expliciete klassengroepberekeningen toe te laten een praktische algoritme krijgen om het splitsingsgedrag van de extensie te berekenen. In het geval dat de quotiënt-extensie *geheel ongesplitst* is, is de conclusie dat A_K als topologische groep isomorf is met de universele groep U. Omgekeerd leidt iedere splitsing van een p-deel van de quotiënt-extensie voor een oneven priemgetal p tot een groep A_K die *niet* isomorf is met U. De situatie is ingewikkelder voor de priem $p = 2$, maar hier is onze controle over de situatie weer groter doordat we gebruik kunnen maken van de talrijke resultaten betreffende het 2-primaire deel van kwadratische klassengroepen.

Op grond van numerieke experimenten hebben we een basisbegrip kunnen krijgen van de verdeling van isomorfietypes van A_K voor variërende K, en dit leidt tot uitdagende vermoedens zoals "voor 100% van alle imaginair kwadratische lichamen met een klassengetal dat priem is, is A_K isomorf met de universele groep U".

In het geval van onze tweede vraag, die impliciet voorkomt in [**?**, Section 9, Question 1], in de hoop om een getallenlichaam K te kunnen reconstrueren uit zijn adelische puntengroep $E(\mathbb{A}_K)$ voor een geschikt gekozen elliptische kromme E/K, kunnen we direct de standaardmethoden voor elliptische krommen over getallenlichamen toepassen op een manier die de lijnen volgt van de bepaling van de structuur van $\widehat{\mathcal{O}}^*$ zoals we die voor onze eerste vraag tegenkwamen.

Het blijkt dat, in het geval $K = \mathbf{Q}$ dat in hoofdstuk 4 behandeld wordt, de adelische puntengroep van 'bijna alle' elliptische krommen over $\mathbf{Q}$ isomorf is met de universele groep

$$\mathcal{E} = \mathbf{R}/\mathbf{Z} \times \widehat{\mathbf{Z}} \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z},$$

die wel enigszins doet denken aan de groep U.

De reden voor de universaliteit van adelische puntengroepen van elliptische krommen is gelegen in de neiging van elliptische krommen om Galoisrepresentaties op hun $\overline{\mathbf{Q}}$-waardige torsiepunten te hebben die 'zo groot mogelijk' zijn. In het geval van $K = \mathbf{Q}$ betekent 'zo groot mogelijk' voor een elliptische kromme $E/\mathbf{Q}$ dat E een zogenaamde Serre-kromme is, en Nathan Jones [**?**] heeft recent bewezen dat 'bijna alle' elliptische krommen over $\mathbf{Q}$ Serre-krommen zijn. Voor universaliteit van $E(\mathbb{A}_K)$ is in feite veel minder nodig dan maximaliteit van de Galoisrepresentatie van E, en het kost dan ook enige moeite om families van elliptische krommen op te schrijven waarvoor de adelische puntengroep *niet* universeel is. We geven een expliciet voorbeeld aan het einde van hoofdstuk 4.

Σύνοψη

Η παρούσα διδακτορική διατριβή εστιάζει σε δύο ερωτήματα τα οποία αρχικά δεν φαίνεται να συσχετίζονται. Ήτοι,

(1) *Ποιά είναι η μορφή της απόλυτης αβελιανής ομάδας Galois A_K ενός φανταστικού τετραγωνικού σώματος αριθμών K, ως τοπολογική ομάδα;*
(2) *Ποιά είναι η μορφή της ομάδας των adelic σημείων μιας ελλειπτικής καμπύλης πάνω από το $\mathbf{Q}$, ως τοπολογική ομάδα;*

Για την πρώτη ερώτηση, η εστίαση στις *αβελιανές* ομάδες Galois μας παρέχει την *θεωρία κλάσεων σωμάτων* ως εργαλείο για την ανάλυση της A_K. Οι παλαιότερες δουλειές στο θέμα αυτό των Kubota και Onabe, παρέχουν μία όχι άμεση περιγραφή του δυικού Pontryagin (Pontryagin dual) της A_K σε όρους απείρων οικογενειών, σε κάθε πρώτο p, με την επωνημία *Ulm invariants (Ulm αναλλοίωτες)*. Η αμεσότητα της προσέγγισής μας με βάση τη θεωρία κλάσεων σωμάτων, αποδεικνύει ότι η A_K περιέχει μία υποομάδα U_K πεπερασμένου δείκτη, ισομορφική με την ομάδα μονάδων $\widehat{\mathcal{O}}^*$ της προπεπερασμένης πλήρωσης του $\widehat{\mathcal{O}}$, του δακτυλίου των ακεραίων του K, και μας παρέχει μία εντελώς συγκεκριμένη περιγραφή της τοπολογικής ομάδας U_K η οποία είναι σχεδόν *ανεξάρτητη* από το φανταστικό τετραγωνικό σώμα K. Πιο συγκεκριμένα, για *όλα* τα φανταστικά τετραγωνικά σώματα αριθμών εκτός των $\mathbf{Q}(i)$ και $\mathbf{Q}(\sqrt{-2})$, έχουμε

$$U_K \cong U = \widehat{\mathbf{Z}}^2 \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}.$$

Η εξαίρετη φύση του $\mathbf{Q}(\sqrt{-2})$ έλειπε από τις εργασίες των Kubota και Onabe, και τα θεωρήματά τους έπρεπε να διορθωθούν με βάση αυτό.

Περνώντας από την «καθολική» υποομάδα U_K στην A_K, οδηγούμαστε σε ένα πρόβλημα επέκτασης ομάδας για adelic ομάδες το οποίο μπορεί να «λυθεί» περνώντας σε μία κατάλληλη επέκταση πηλίκου ομάδων το οποίο εμπλέκει το μέγιστο $\widehat{\mathbf{Z}}$-ελεύθερο πηλίκο U_K/T_K της U_K. Με τον όρο «λυθεί» εννοούμε ότι για κάθε K το οποίο είναι ικανά μικρό ώστε να επιτρέπει σαφείς υπολογισμούς κλάσεων σωμάτων για το K, αποκτούμε έναν πρακτικό αλγόριθμο για να υπολογίσουμε την splitting συμπεριφορά της επέκτασης ομάδων. Στην περίπτωση όπου η επέκταση υπολοίπου είναι *totally non-split*, το συμπέρασμα είναι πως η A_K είναι ισομορφική ως τοπολογική ομάδα με την καθολική ομάδα U. Αντίστροφα, κάθε splitting του p-μέρους του πηλίκου επέκτασης σε έναν περιττό πρώτο p οδηγεί στην ομάδα A_K η οποία *δεν* είναι ισόμορφη με την U. Για τον πρώτο 2, η κατάσταση είναι ιδιαίτερη, αλλά πιο ελεγχόμενη λόγω της πληθώρας θεωρημάτων που αφορούν τα 2-μέρη των τετραγωνικών ομάδων κλάσεων.

Βασιζόμενοι σε αριθμητικούς πειραματισμούς, έχουμε αποκτήσει μία βασική κατανόηση της κατανομής των τύπων ισομορφισμού της A_K για διάφορα K, κι αυτό οδηγεί σε προκλητικές εικασίες όπως «100% όλων των φανταστικών τετραγωνικών σωμάτων με αριθμό κλάσεων πρώτο αριθμό, έχουν A_K ισόμορφη με την καθολική ομάδα U».

Στην περίπτωση της δεύτερης ερώτησής μας, η οποία εμφανίζεται ως ερώτηση στο [**?**, Section 9, Question 1] με την οπτική της ανάκτησης ενός σώματος αριθμών K από την ομάδα των adelic σημείων $E(\mathbb{A}_K)$ μιας κατάλληλης ελλειπτικής καμπύλης πάνω από το K, μπορούμε ευθής αμέσως να εφαρμόσουμε τα καθιερωμένα εργαλεία για τις ελλειπτικές καμπύλες πάνω από σώματα αριθμών με μία μέθοδο η οποία ακολουθεί τις γραμμές του προσδιορισμού της δομής του $\widehat{\mathcal{O}}^*$ με την οποία ασχοληθήκαμε στην πρώτη ερώτησή μας.

Αποδεικνύεται ότι στην περίπτωση όπου $K = \mathbf{Q}$, η οποία αντιμετωπίζεται στο Κεφάλαιο 4, η ομάδα των adelic σημείων «σχεδόν όλων» των

ελλειπτικων καμπυλών πάνω από το $\mathbf{Q}$ είναι ισόμορφη με μία καθολική ομάδα

$$\mathcal{E} = \mathbf{R}/\mathbf{Z} \times \widehat{\mathbf{Z}} \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}$$

η οποία κατά μία έννοια είναι όμοια εκ φύσεως της U. Ο λόγος της καθολικότητας των ομάδων των adelic σημείων ελλειπτικών καμπυλών έγκειται στην τάση των ελλειπτικών καμπυλών να έχουν αναπαραστάσεις Galois στην ομάδα των σημείων πεπερασμένης τάξης που ορίζονται στο $\overline{\mathbf{Q}}$ οι οποίες είναι πολύ κοντά στο να είναι μεγιστικές. Για $K = \mathbf{Q}$, η μεγιστικότητα των αναπαραστάσεων Galois μιας ελλειπτικής καμπύλης E, σημαίνει ότι η E είναι μία καμπύλη Serre, κι έχει πρόσφατα αποδειχθεί από τον Nathan Jones [**?**] ότι «σχεδόν όλες» οι ελλειπτικές καμπύλες πάνω από το $\mathbf{Q}$ είναι καμπύλες Serre. Στην πραγματικότητα, η καθολικότητα της $E(\mathbb{A}_K)$ απαιτεί κάτι λιγότερο από την μεγιστικότητα των αναπαραστάσεων Galois, και το αποτέλεσμα είναι ότι απαιτείται κάποια προσπάθεια να κατασκευαστούν οικογένειες ελλειπτικών καμπυλών με μη-καθολική ομάδα adelic σημείων. Παρέχουμε ένα παράδειγμα τέτοιας οικογένειας στο τέλος του Κεφαλαίου 4.

Acknowledgements

Thank you Peter for you chose me, guided me, taught me, believed in me, supported me, drank with me. You are my mathematical father.

Thank you Karim for the hospitality while I was in Bordeaux, the support and the nice lunches with cider.

Thank you Prof. G. Gras for the emails we exchanged regarding the project on absolute abelian Galois groups, and for your comments being a *rapporteur* of my thesis.

Thank you Gunther for the first dinner I had at this wonderful PhD trip, in Barcelona on September 2010, and for your talk there from which the project idea regarding absolute abelian Galois groups came. I would like to thank you also for your comments being a *rapporteur* of my thesis.

Thank you Hendrik for the inspiration, your comments and ideas; Hendrik, Bart and Ronald for being members of my committee.

Thank you Aristides and Petros for your belief in me, the support and the advice; Dimitris for the support and the useful advice; Prof. D. Lappas, E. Raptis, and D. Varsos for the support all these years; Prof. A. Papaioannou for the nice conversations we had about maths and women; D. Simos, M. Fillipakis and Chrysanthi for the support all these years.

Thank you P. Bruin for you were waiting for me at the central station my very first day in Leiden, the help and support the first days there; Ronald, Filip, Jeroen, Jochen, Roberto, Erwin and Sean for the advice and the support, the beers and our conversations about maths and music.

Thank you all guys from the number theory and geometry group: Lenny, Marco, Bas, Robin, Bart, Cecilia, Krzysztof, ..., for the nice times.

Thank you Dino and Val for being music-mates during these years, and you guys from music club: Mois, Andrea, B.J. Teddy, ...

Thank you Marianne and Kathelijne for all the administration stuff. Many thanks Kathelijne for your support the last months there.

Thank you Julio and Michiel for your support, your belief in me, the crazy nights we had and the conversations about women; Liu and Djordjo for the great times of basketball or not and your support; Samuele and Alberto for your support and the nice times we had.

Thank you Giannis for you put my mind in order when I was 16 and showed me the way to find my path in the world of mathematics.

Thank you Chrysa for the support the first hard months in Leiden, and for the dreams we had and lived.

Thank you Konstantina for the support and the understanding while we were in different places, for the dreams we shared and lived.

Thank you Artemis and Victoria for your belief in me and your support all these years. Remember to chase your dreams!

Thank you George and Thodoris for your support, your poems and paintings, our philosophical conversations with rakes.

Thank you Thomas, Aunt Litsa, Dimis, Olga and Daniel for your support all the years, your belief in me; Elena and Dimitris for the support, the nice times and for every minute on skype and on phone we had.

Thank you my friend Sakis for you are my precious friend in life, you were always there for me, you believe in me, and you didn't let me sell my Les Paul while I was in Bordeaux; Tasos and grandma for you were always there and supported me all the years.

Thank you Andreas and Angeliki, my friend in life and my sister, for you believe in me. Your support is priceless.

My mother, my father, without you, without your support, without you to believe in me, your strength, your sacrifices, your wisdom, your kindness, your love, I wouldn't be here today. Thank you!

Curriculum Vitae

Athanasios Angelakis was born in Amarousio of Attica in Athens, Greece on June 4, 1979.

He graduated from the 21st Lyceum of Athens, and entered the Mathematics Department of the National-Kapodistrian University of Athens in 1998. He worked as private tutor during his studies, graduated in 2006 and joined the air-force of the army, becoming a class B Meteorologist.

In 2008 he entered the Master of Sciences program of the National Technical University of Athens, where he graduated in 2010 under the supervision of Aristides Kontogeorgis with a thesis entitled *Counting points of Elliptic Curves over Finite Fields*. During these years he was working as a bartender in his favorite Blues Bar.

In October 2010, Athanasios started his PhD-studies with an Erasmus Mundus Algant-DOC fellowship under the supervision of P. Stevenhagen (Leiden) and K. Belabas (Bordeaux). Since the end of his fellowship in January 2014, he has been working as a senior researcher in the Telecommunication consulting company Enomix, while being a member of the 3rd research team of the National Technical University of Athens working on the project *Algebraic Modeling of Computational Structures*.

Athanasios holds several distinctions in Martial Arts, Basketball and Free Diving. He is a self-taught guitarist who composed many songs, played in several bands and gave various live performances.