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 [**Len08**] 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 [**Ste08**, Theorem 5.13], and the class group is a finite abelian group [**Ste08**, 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 [**CF10**, 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 [**BH13**].

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 [**BH13**].

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* [**CL84**]. 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 [**Gas26**] 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 [**Per77**] 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 [**dSP94**] 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

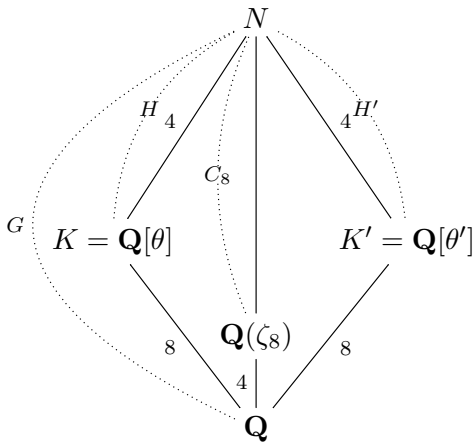

FIGURE 1.1. Perlis' example.

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 [**Iwa53**] 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.

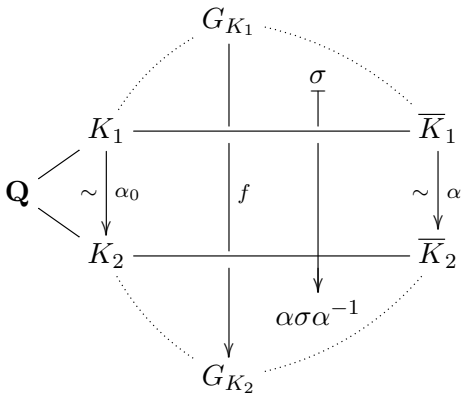

FIGURE 1.2. Isomorphisms induced by $\alpha_0 : K_1 \xrightarrow{\sim} K_2$.

The fundamental work of Neukirch [**Neu69a**, **Neu69b**], as refined by Ikeda [**Ike77**], Neukirch [**Neu77**], Uchida [**Uch76**] 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 [**NSW08**, 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 [**Neu69b**]. Uchida's improvement, which was subsequently simplified by Neukirch [**Neu77**], 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 [**Neu69a**] 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 [**Ona76**, **Ona78**] discovered that this is not the case for imaginary quadratic number fields.

Onabe based her work on earlier work of Kubota [**Kub57**], 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 [**Kap54**, 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 [**Ona76**, Theorem 2] is however incorrect. This is because the value of the finite Ulm invariants in [**Kub57**, 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 [**Wan50**] occurring in Kubota's paper [**Kub57**, 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 [**Ona76**] 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 [**Gra**], 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 [**Gra14**].

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 [**RZB14**] 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 [**CK14**, Section 9, Question 1], who are interested in algebraic groups $\mathbf{G}$ for which $\mathbf{G}(\mathbb{A}_K)$ determines K up to isomorphism.