Semi-galois Categories III: Witt vectors by deformations of modular functions

Takeo Uramoto
Institute of Mathematics for Industry, Kyushu University

Abstract
Based on our previous work on an arithmetic analogue of Christol’s theorem, this paper studies in more detail the structure of the Λ-ring \( E_K = K \otimes W^a_{O_K}(O_K) \) of algebraic Witt vectors for number fields \( K \). First developing general results concerning \( E_K \), we apply them to the case when \( K \) is an imaginary quadratic field. The main results include the “modularity theorem” for algebraic Witt vectors, which claims that certain deformation families \( f : M_2(\hat{\mathbb{Z}}) \times \mathfrak{H} \to \mathbb{C} \) of modular functions of finite level always define algebraic Witt vectors \( \hat{\xi} = f \) by their special values, and conversely, every algebraic Witt vector \( \xi \in E_K \) is realized in this way, that is, \( \xi = f \) for some deformation family \( f : M_2(\hat{\mathbb{Z}}) \times \mathfrak{H} \to \mathbb{C} \). This gives a rather explicit description of the Λ-ring \( E_K \) for imaginary quadratic fields \( K \), which is stated as the identity \( E_K = M_K \) between the Λ-ring \( E_K \) and the \( K \)-algebra \( M_K \) of modular vectors \( \hat{f} \).

1 Introduction
This paper is a continuation of our previous work on arithmetic analogue of Christol’s theorem \[16\]. This theorem claims that a (generalized) Witt vector \( \xi \in W_{O_K}(O_K) \) is integral over the ring \( O_K \) of integers in a number field \( K \) if and only if the orbit of \( \xi \) under the action of the Frobenius lifts \( \psi_p : W_{O_K}(O_K) \to W_{O_K}(O_K) \) is finite (cf. Theorem 3.4, \[16\]); we then deduced that, with the aid of the work of Borger and de Smit \[3\], which heavily relies on class field theory, this is also precisely when the ghost components \( \xi_a \) of \( \xi \) are periodic with respect to some modulus \( \mathfrak{f} \) of \( K \) (cf. Corollary 2, \[16\]). With this background, the major goal of the current paper is then to study in more detail the structure of the Λ-ring \( E_K := K \otimes W^a_{O_K}(O_K) \) (where \( W^a_{O_K}(O_K) \) is the Λ-ring of integral Witt vectors) in the case where \( K \) is an imaginary quadratic field; in particular, we prove that the Λ-ring \( E_K \) coincides as a \( K \)-subalgebra of \( (K^{ab})^{\mathbb{Z}_K} \) with the \( K \)-algebra \( M_K \) of modular vectors—i.e. those vectors \( \hat{f} \in (K^{ab})^{\mathbb{Z}_K} \) whose components \( \hat{f}_a \) are given by special values of certain deformation families \( f : M_2(\hat{\mathbb{Z}}) \times \mathfrak{H} \to \mathbb{C} \) of modular functions—i.e. the fiber \( f_m := f(m, -) : \mathfrak{H} \to \mathbb{C} \) at each \( m \in M_2(\hat{\mathbb{Z}}) \) is a modular function of finite level, and these \( f_m \) satisfy certain correlation—prototypical examples of such deformation families of modular functions are given by Fricke functions \( f_a(a \in \mathbb{Q}^2/\mathbb{Z}^2) \); cf. \[4.1\] In summary, the following is our major result, which we call the modularity theorem (cf. \[4.2\] \[4.3\]):

**Theorem 1.0.1** (modularity theorem). We have the following identity as \( K \)-subalgebras of \( (K^{ab})^{\mathbb{Z}_K} \):

\[
E_K = M_K. 
\]
Background To be precise, for a flat $O_K$-algebra $A$, recall that the ring $W_{O_K}(A)$ of (generalized) \textit{Witt vectors} with coefficients in $A$ \cite{1} is defined as the intersection $W_{O_K}(A) := \bigcap_n U_n(A)$ of the following $O_K$-algebras $U_n(A) \subseteq A^{I_K}$ given by induction on $n \geq 0$ (cf. §2.1 \cite{10}; also see Remark 5, §2.2 \cite{10} for some intuition on Witt vectors as “smooth” functions on $I_K$ with respect to \textit{arithmetic derivatives} in the sense of Buium \cite{6}):

$$U_0(A) := A^{I_K}$$

$$U_{n+1}(A) := \{ \xi \in U_n(A) \mid \forall p \in P_K, \psi_p \xi - \xi N^p \in p U_n(A) \}$$

(1.2) (1.3)

where $P_K$ and $I_K$ denote the set of maximal ideals of $O_K$ and the monoid of nonzero ideals of $O_K$ respectively; $A^{I_K}$ denotes the $I_K$-times product of $A$; $Np$ denotes the absolute norm of $p \in P_K$; and $\psi_p : A^{I_K} \to A^{I_K}$ denotes the shift $(\xi_a) \mapsto (\xi_{pa})$. In the case when $K$ is the rational number field $\mathbb{Q}$, say, this ring $W_{O_K}(A)$ is isomorphic to the usual ring $W_{\mathbb{Z}}(A)$ of \textit{big Witt vectors}; and the usual ring $W_p(A)$ of $p$-\textit{typical Witt vectors} can be constructed in a similar way. While these rings of big and $p$-typical Witt vectors are conventionally constructed using Witt polynomials, Buium \cite{1} recasted these constructions of Witt vectors putting his focus on Frobenius lifts, and constructed the ring of Witt vectors as the universal ring among those rings which are equipped with commuting family of Frobenius lifts, or $\Lambda$-rings; this construction naturally allows us to extend the base ring from $\mathbb{Z}$ to arbitrary Dedekind domains $O$ with finite residue fields (or more): He proved the existence of such a universal ring for this generalized setting by the above inductive construction. The basic theory of these generalized Witt vectors was developed in \cite{1}; our major concern in this paper is to study the structure of the rings of these generalized Witt vectors.

In particular, among generalized Witt vectors $\xi \in W_{O_K}(O_K)$ with coefficients in the ring $O_K$ of algebraic integers, those $\xi \in W_{O_K}(O_K)$ which are integral over $O_K$—i.e. \textit{integral Witt vectors}—were proved to be relevant to class field theory of the number field $K$, as discussed in our previous work \cite{10} based on \cite{2,3}; see also \cite{4}. In fact, on the one hand, it was proved in \cite{3} that the category $\mathcal{C}_K$ of those (generalized) $\Lambda$-rings which are finite etale over $K$ and have \textit{integral models} (§2 \cite{10}) is dually equivalent to the category $\mathcal{B}_f DR_K$ of finite $DR_K$-sets, where $DR_K$ is the profinite monoid called the \textit{Deligne-Ribet monoid} and given by inverse limit of ray class monoids $DR_f$ ($f \in I_K$); in this proof, class field theory was used in an essential way, which suggests an inherent connection between class field theory and (generalized) $\Lambda$-rings. Motivated by this duality \cite{3}, our previous work \cite{10} then related integral Witt vectors to the objects of $\mathcal{C}_K$; to be precise, we proved that for any integral Witt vector $\xi \in W_{O_K}(O_K)$, the $\Lambda$-ring $X_\xi = K \otimes O_K(\xi)$ generated by the orbit $I_K \xi$ of $\xi$ under the action of the Frobenius lifts $\psi_p$ is finite etale over $K$ and has an integral model, or in other words, forms an object of $\mathcal{C}_K$ (cf. Proposition 4 \cite{10})—indeed as further proved in this paper, these types of objects $X_\xi$ are universal in $\mathcal{C}_K$ (cf. \cite{3}). Technically speaking, our major result there, i.e. an arithmetic analogue of Christol’s theorem (Theorem 3.4 \cite{10}), is necessary to prove the finiteness of $X_\xi$ over $K$. (However, this theorem itself is of independent interest in that it gives a natural arithmetic (or $\mathbb{F}_1$-) analogue of Christol’s theorem [2,8] on formal power series $\xi \in \mathbb{F}_q[[t]]$ over finite field $\mathbb{F}_q$; cf. §3 \cite{10}.)

\textbf{Contributions} As a natural continuation of \cite{10}, the current paper then studies in more detail the structure of the ring $W_{O_K}(O_K)$ of integral Witt vectors and the $K$-algebra $E_K := K \otimes W_{O_K}(O_K)$ whose elements we call \textit{algebraic Witt} vectors. In particular, after developing some general basic results about the $K$-algebra $E_K$ (\cite{33}), we then apply them to the case when $K$ is the rational number field $\mathbb{Q}$ (\cite{33,33}) and an imaginary quadratic field (\cite{33}). The major results of this paper are those given
in \[\mathfrak{I}\] where, as briefly summarized above, we relate algebraic Witt vectors \(\xi \in E_K\) with certain deformation families of modular functions.

To be more specific, the subject of \[\mathfrak{I}\] is to classify and study the structure of the galois objects of \(\mathcal{C}_K\) (cf. §3.2 [15]), which provides a general basis for the study in \[\mathfrak{I}\]. In particular, we see that, for each finite set \(\Xi \subseteq W^n_{O_K}(O_K)\) of integral Witt vectors, we can construct a \(\Lambda\)-ring \(X_{\Xi}\), which is an object of \(\mathcal{C}_K\) as in the case of singleton \(\Xi = \{\xi\}\) mentioned above. Concerning this construction, we prove in \[\mathfrak{I}\] that \(X_{\Xi}\) is a galois object of \(\mathcal{C}_K\) for every \(\Xi \subseteq W^n_{O_K}(O_K)\), and conversely, every galois object of \(\mathcal{C}_K\) is of this form up to isomorphism. That is, the galois objects of \(\mathcal{C}_K\) are precisely those of the form \(X_{\Xi}\) for some finite \(\Xi \subseteq W^n_{O_K}(O_K)\). This particularly implies that the direct limit of the galois objects of \(\mathcal{C}_K\) is naturally isomorphic to our \(K\)-algebra \(E_K = K \otimes W^n_{O_K}(O_K)\); this gives a characterization of the \(K\)-algebra \(E_K\) of algebraic Witt vectors as the universal ring among those \(\Lambda\)-rings finite etale over \(K\) and having integral models (i.e. universal with respect to the objects of \(\mathcal{C}_K\)). For the purpose of \[\mathfrak{I}\], the rest of \[\mathfrak{I}\] (i.e. \[\mathfrak{3.2}\] and \[\mathfrak{3.3}\]) is somewhat optional, but the results there will be of independent interest. In \[\mathfrak{3.2}\] on the one hand, we study the structure of the galois objects of \(\mathcal{C}_K\); by the result in \[\mathfrak{3.1}\] this means that we study the \(\Lambda\)-rings of the form \(X_{\Xi}\) for some \(\Xi \subseteq W^n_{O_K}(O_K)\). In this subsection, we particularly determine the state complexity of integral Witt vectors \(\xi \in W^n_{O_K}(O_K)\), i.e. the minimum size \(c_\xi\) of deterministic finite automata (DFAs) that generate \(\xi\) (cf. §3.1 [16]); we prove that the state complexity \(c_\xi\) for \(\xi \in W^n_{O_K}(O_K)\) is equal to the dimension \(\dim_K X_{\xi}\) of the \(\Lambda\)-ring \(X_{\xi}\) over \(K\). (This is a \(\mathbb{F}_1\)-anologue of Bridy’s result [5] on formal power series \(\xi \in \mathbb{F}_q[[t]]\); cf. \[\mathfrak{3.2}\].) In \[\mathfrak{3.3}\] on the other hand, we determine the structure of \(W^n_{O_K}(O_K)\) and \(E_K\) for the case when \(K\) is the rational number field \(\mathbb{Q}\) as an immediate consequence of the result in \[\mathfrak{3.1}\] and the result in \[\mathfrak{2}\], we show that the \(\Lambda\)-ring \(W^n_{\mathbb{Z}}(\mathbb{Z})\) of integral Witt vectors is isomorphic to the group-ring \(\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]\), hence, \(E_K\) is isomorphic to the group-algebra \(\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]\). In more elementary words, this isomorphism \(E_K \simeq \mathbb{Q}[\mathbb{Q}/\mathbb{Z}]\) shows that the algebraic (resp. integral) Witt vectors \(\xi = (\xi_n)_{n \in \mathbb{N}} \in E_K\) are precisely the \(\mathbb{Q}\)-linear (resp. \(\mathbb{Z}\)-linear) combinations of the vectors \(\zeta(\gamma) \in (\mathbb{Q}_a^{ab})^{\mathbb{N}}\) of the form \(\zeta(\gamma) = (e^{2\pi i \gamma \gamma})_n\) for \(\gamma \in \mathbb{Q}/\mathbb{Z}\).

The subject of \[\mathfrak{4}\] is then to proceed this study to the case where \(K\) is an imaginary quadratic field. To be more specific, we prove in \[\mathfrak{4.1}\] that the algebraic Witt vectors \(\xi \in E_K\) are precisely the modular vectors, i.e. the vectors \(\hat{f} \in (K^{ab})^{I_K}\) whose components \(\hat{f}_a\) are defined by special values of certain deformation families \(f : M_2(\mathbb{Z}) \times \mathfrak{I} \to \mathbb{C}\) of modular functions, which we shall call Witt deformation families of modular functions (because their special values eventually define algebraic Witt vectors). Briefly, a Witt deformation (family) of modular function is defined as a continuous function \(f : M_2(\mathbb{Z}) \times \mathfrak{I} \to \mathbb{C}\) such that the fiber \(f_m := f(m, -) : \mathfrak{I} \to \mathbb{C}\) at each \(m \in M_2(\mathbb{Z})\) is a modular function of finite level, where the fibers \(f_m\) satisfy some few conditions (cf. Definition \[\mathfrak{1.1.2}\] \[\mathfrak{4.1}\]), including e.g. the property that \(f_{m_1}(\gamma^{-1}\gamma) = f_m(\gamma)\) for \(\gamma \in SL_2(\mathbb{Z}) = \Gamma\) in particular. Concerning this, we see that each Witt deformation \(f : M_2(\mathbb{Z}) \times \mathfrak{I} \to \mathbb{C}\) of modular functions defines a modular vector \(\hat{f} \in (K^{ab})^{I_K}\) in a natural (but non-trivial) way that heavily relies on the work of Connes, Marcolli and Ramachandran [10], Connes and Marcolli [9], Laca, Larsen, and Neshveyev [12] and Yalkinoglu [19]. Briefly speaking, this construction \(f \mapsto \hat{f}\) is based on the isomorphisms between the above-mentioned Deligne-Ribet monoid \(DR_K\) and the (moduli) space \(\text{Lat}^1_K\) of 1-dimensional \(K\)-lattices [10][12][19], and between the (moduli) space \(\text{Lat}^2_Q\) of 2-dimensional \(\mathbb{Q}\)-lattices and the quotient space \(\Gamma \setminus (M_2(\mathbb{Z}) \times \mathfrak{I})\) [9] (cf. \[\mathfrak{2.2}\]). Since \(K\) is now imaginary quadratic, hence, of degree 2 over \(\mathbb{Q}\), we have a natural embedding \(\text{Lat}^1_K \to \text{Lat}^2_Q\); and then composed with the isomorphisms \(DR_K \simeq \text{Lat}^1_K\) and \(\text{Lat}^2_Q \simeq \Gamma \setminus (M_2(\mathbb{Z}) \times \mathfrak{I})\), as well as the canonical embedding \(I_K \to DR_K\), each Witt deformation \(f : M_2(\mathbb{Z}) \times \mathfrak{I} \to \mathbb{C}\) then induces a function \(\hat{f} : I_K \to \mathbb{C}\) as...
follows:

\[
\hat{f} : I_K \hookrightarrow DR_K \xrightarrow{\cong} Lat^1_K \xrightarrow{\cong} \text{Lat}^2_\mathbb{Q} \cong \Gamma(M_2(\hat{\mathbb{Z}}) \times I) \xrightarrow{f} \mathbb{C}.
\] (1.4)

We can see that \(\hat{f}\) takes its values in \(K^{ab}\); hence defines a vector \(\hat{f} \in (K^{ab})^{I_K}\) which is what we call the modular vector associated to \(f\); the \(K\)-subalgebra \(M_K \subseteq (K^{ab})^{I_K}\) is defined as that consisting of modular vectors in this sense. The major result of \(\S 4\) is the “modularity theorem” claiming the identity \(E_K = M_K\) as \(K\)-subalgebras of \((K^{ab})^{I_K}\) (\(\S 1.2\)). In other words, for every Witt deformation \(f : M_2(\mathbb{Z}) \times I \to \mathbb{C}\), the associated modular vector \(\hat{f}\) defines an algebraic Witt vector, i.e. \(\hat{f} \in E_K\); and conversely, every algebraic Witt vector \(\xi \in E_K\) is realized in this way, i.e. \(\xi = \hat{f}\) for some Witt deformation \(f : M_2(\mathbb{Z}) \times I \to \mathbb{C}\). This identity \(E_K = M_K\) relates the geometry of \(\Lambda\)-rings in \(\mathcal{C}_K\) and that of modular functions. Moreover, in the last subsection (\(\S 4.3\)) we prove that \(E_K = M_K\) is generated as a \(K\)-algebra by the modular vectors \(\hat{f}_a\) naturally arising from the Fricke functions \(f_a\) (\(a \in \mathbb{Q}^2/\mathbb{Z}^2\)).

Acknowledgement We are grateful to James Borger for fruitful discussions, which motivated us to prove Proposition 3.1.3 instead of considering the existence of cyclic Witt vectors, cf. Remark 3.1.7 and to Naoya Yanamaka and Hayato Saigo for their support and encouragement. We are also thankful to an anonymous reviewer for his/her patient proofreading, in particular, alerting us to an error in Lemma 4.4.2 in [17]; to Yasuhiro Ishitsuka for alerting us to an error in Proposition 3 [16] (cf. corrigendum given in [18]). This work was done during the author was a member of Nagahama Institute for Bio-Science and Technology, to whom we are grateful for their hospitality. This work was supported by JSPS KAKENHI Grant number JP16K21115.

2 Preliminaries

This section summarizes necessary terminology and results from [16] [9] [10] [12] [19]. But in order to avoid duplications, we refer the reader to §2 – §4 [16] for the detailed definitions of basic concepts and results in [16], say, Witt vectors (Definition 1, pp. 543), \(\Lambda\)-rings (Definition 2, pp. 544), integral models of finite etale \(\Lambda\)-rings over \(K\) (Remark 4, pp. 544) and our arithmetic analogue of Christol’s theorem (Theorem 3.4, pp. 557) in particular. Also, for the categorical concepts and results on semi-galois categories, we refer the reader to [15].

But, before proceeding to the main part, let us include here the following corrigendum to [16]:

Corrigendum to [16] Yasuhiro Ishitsuka alerted us that the proof of Proposition 3, §3.2, pp.552 [16] is valid only for the case when \(K\) is of class number one; to be specific, an error occurs in the last part of the proof claiming that \(b/p \in O_K\) for \(p \neq q\), which is invalid for our choice of \(\pi \in \mathfrak{p}\) in general because, when \(\mathfrak{p}\) is not principal, \(\pi \in \mathfrak{p}\) would belong in some \(q \neq \mathfrak{p}\) too. We are thankful to him for pointing this out. Thus we restrict Proposition 3 [16] only to the case when \(K\) is of class number one.

Accordingly, we repair here our proof of the main result of [16], which depended on Proposition 3. Note that Proposition 3 was used in the proofs of Lemma 3.2 (pp.554) and Lemma 3.4 (pp.555). However, in the proof of Lemma 3.2, on the one hand, we actually need only Lemma 3.1. On the other hand, Lemma 3.4 could be also proved without Proposition 3 as follows[4]. The notations are

[4] This salvage of Lemma 3.4 is optional in that, as discussed in [18], the full statement of Lemma 3.4 was in fact unnecessary for the current paper and [16]. Nevertheless we include it here for future reference.
Therefore, we have some \( \psi \), from which we deduce \( \eta \).

For the base case \( n = 0 \), there is nothing to prove. For induction, assume that the claim is true up to \( n \), with which we show that \( N^*\xi \in U_{OL,n+1}(OL) \) for \( \xi \in U_{OK,n+1}(OL) \). Take \( \xi \in U_{OK,n+1}(OL) \) and let us put \( \zeta := N^*\xi \in O^*_L \).

First, by \( U_{OK,n+1}(OL) \subseteq U_{OK,n}(OL) \) and induction hypothesis, we indeed have \( \zeta \in U_{OK,n}(OL) \); then, to show \( \zeta \in U_{OL,n+1}(OL) \), we need prove that \( \psi_\mathfrak{p}\zeta - \zeta^{N\mathfrak{P}} \in \mathfrak{P}U_{OL,n}(OL) \) for every \( \mathfrak{P} \in P_L \).

To this end we note that, by \( \xi \in U_{OK,n+1}(OL) \), we have \( \psi_\mathfrak{p}\xi - \xi^{N\mathfrak{P}} \in \mathfrak{P}U_{OK,n}(OL) \) for \( \mathfrak{p} := \mathfrak{P} \cap OK \), from which we deduce \( \psi_\mathfrak{p}\xi - \xi^{(N\mathfrak{P})f} \in \mathfrak{P}U_{OK,n}(OL) \) where \( f \) denotes the inertia degree for \( \mathfrak{P} | \mathfrak{p} \).

Therefore, we have some \( r_i \in \mathfrak{p} \) and \( \eta^{(i)} \in U_{OK,n}(OL) \) such that:

\[
\psi_\mathfrak{p}\xi - \zeta^{(N\mathfrak{P})f} = \sum_{i=1}^{m} r_i \cdot \eta^{(i)}. \tag{2.1}
\]

Applying \( N^* \) to the both side of this equality, and noting that \( N^*(\psi_\mathfrak{p}\xi) = \psi_\mathfrak{P}(N^*\xi) = \psi_\mathfrak{P}\zeta \) and \( (N\mathfrak{P})f = N\mathfrak{P} \), we obtain:

\[
\psi_\mathfrak{P}\zeta - \zeta^{N\mathfrak{P}} = \sum_{i=1}^{m} r_i \cdot N^*\eta^{(i)}. \tag{2.2}
\]

By induction hypothesis applied to \( \eta^{(i)} \in U_{OK,n}(OL) \), we know that \( N^*\eta^{(i)} \in U_{OL,n}(OL) \); also by \( r_i \in \mathfrak{p} \subseteq \mathfrak{P} \), we then obtain \( \psi_\mathfrak{P}\zeta - \zeta^{N\mathfrak{P}} \in \mathfrak{P}U_{OL,n}(OL) \), which is what we needed to prove.

With this modification, our main result (i.e. Theorem 3.4) of \cite{16} remains valid.

### 2.1 The category \( \mathcal{C}_K \)

Here we recall some basic facts concerning the semi-galois category \( \mathcal{C}_K \) constructed by Borger and de Smit \cite{3} for a number field \( K \). Let \( K \) be a number field and \( OK \) the ring of integers in \( K \). We denote by \( PK \) and \( IK \) the set of non-zero prime ideals of \( OK \) and the monoid of non-zero ideals of \( OK \) respectively. For each \( \mathfrak{p} \in PK \), we denote by \( k_\mathfrak{p} \) the residue field \( k_\mathfrak{p} := OK / \mathfrak{p} \) and by \( N\mathfrak{p} \) the absolute norm \( N\mathfrak{p} := \#k_\mathfrak{p} \).

**Definition 2.1.1 (the category \( \mathcal{C}_K \)).** The objects of the category \( \mathcal{C}_K \) are the \( \Lambda \)-rings that are finite etale over \( K \) and have integral models (cf. Remark 4, pp.544 \cite{16}); the arrows of \( \mathcal{C}_K \) are the \( \Lambda \)-ring homomorphisms over \( K \) between them.

The category \( \mathcal{C}_K \) is equipped with a functor \( F_K : \mathcal{C}_K^{op} \to \text{Sets} \) that assigns to each object \( X \in \mathcal{C}_K \) the finite set \( F_K(X) := \text{Hom}_K(X, \bar{K}) \) of the \( K \)-algebra homomorphisms from the underlying \( K \)-algebra \( X \) to the algebraic closure \( \bar{K} \) of \( K \); and to each arrow \( f : X \to Y \) of \( \Lambda \)-rings the pullback \( f^* : \text{Hom}_K(Y, \bar{K}) \to \text{Hom}_K(X, \bar{K}) \). With this functor \( F_K \), we can see that the pair \( (\mathcal{C}_K^{op}, F_K) \) forms a semi-galois category. Therefore, by the general results developed in \cite{16}, the semi-galois category
\( (\mathcal{C}_K^p, F_K) \) should be canonically equivalent to the semi-galois category \( \langle B, M, F_M \rangle \) of finite \( M \)-sets with \( M \) being the fundamental monoid \( M = \pi_1(\mathcal{C}_K^p, F_K) \) (cf. Definition 4, §2.2 [15]).

But in the current situation, Borger and de Smit [3] could give a more explicit description of this equivalence. To be specific, recall that by definition an object \( X \in \mathcal{C}_K \) is a finite etale \( \Lambda \)-ring over \( K \), i.e., a finite etale \( K \)-algebra equipped with commuting family of Frobenius lifts \( \psi_p : X \to X \) for each \( p \in P_K \); thus, the finite set \( F_K(X) = \text{Hom}_K(X, \bar{K}) \) is equipped with a continuous action of the absolute galois group \( G_K \) of \( K \) as well as the action of the monoid \( I_K \) by natural pullbacks of \( \psi_a : X \to X \) for \( a \in I_K \) (see Remark 2, §2.2 [16] for this notation \( \psi_a \)); and the actions of \( G_K \) and \( I_K \) commute with each other. Therefore, the finite set \( F_K(X) \) forms a finite \((G_K \times I_K)\)-set with respect to this action. To be specific, the action of the monoid \( G_K \times I_K \) on the finite set \( F_K(X) \) is given as follows:

\[
F_K(X) \times (G_K \times I_K) \to F_K(X) \quad (s, (\sigma, a)) \mapsto \sigma \circ s \circ \psi_a.
\]

Of course, the objects of \( \mathcal{C}_K \) are not just finite etale \( \Lambda \)-rings over \( K \) but have integral models (cf. Remark 4, §2.2 [16]); Borger and de Smit [3] gave a characterization of when a finite etale \( \Lambda \)-ring \( X \) has an integral model in terms of the corresponding finite \((G_K \times I_K)\)-set \( F_K(X) \). As proved there, the Deligne-Ribet monoid \( DR_K \) (after their work [11] where this profinite monoid appeared) comes into play for this characterization: As we recall below, we have a canonical map \( G_K \times I_K \to DR_K \); and it was proved in [3] that a finite etale \( \Lambda \)-ring \( X \) over \( K \) has an integral model (i.e. is an object of \( \mathcal{C}_K \)) if and only if the \((G_K \times I_K)\)-action on \( F_K(X) \) factors through this map \( G_K \times I_K \to DR_K \) (Theorem 1.2 [3]).

To be precise, the Deligne-Ribet monoid \( DR_K \) is defined as the inverse limit of the ray class monoids, i.e. the finite monoids \( DR_\mathfrak{f} \) given for each \( \mathfrak{f} \in I_K \) as the quotient monoid \( DR_\mathfrak{f} := I_K/\sim_\mathfrak{f} \) of the monoid \( I_K \) by the following congruence relation \( \sim_\mathfrak{f} \) on \( I_K \): for \( a, b \in I_K \),

\[
a \sim_\mathfrak{f} b \iff ab^{-1} = (t) \text{ for } \exists \mathfrak{t} \in K_+ \cap (1 + \mathfrak{f}^{-1}); \tag{2.3}
\]

where \( K_+ \) denotes the totally positive elements of \( K \). This congruence relation \( \sim_\mathfrak{f} \) is of finite index, and thus, the ray class monoid \( DR_\mathfrak{f} \) is a finite monoid. To form an inverse system of the ray class monoids \( DR_\mathfrak{f} \), note that if \( \mathfrak{f} \mid \mathfrak{f}' \) then \( a \sim_{\mathfrak{f}'} b \) implies \( a \sim_\mathfrak{f} b \); therefore, we have a canonical monoid surjection \( DR_\mathfrak{f}' \to DR_\mathfrak{f} \) by the assignment \([a]_\mathfrak{f}' \mapsto [a]_\mathfrak{f}\) where \([a]_\mathfrak{f} \in DR_\mathfrak{f} \) denotes the equivalence class of \( a \in I_K \) in \( DR_\mathfrak{f} \). With respect to these surjections \( DR_\mathfrak{f}' \to DR_\mathfrak{f} \), the ray class monoids \( DR_\mathfrak{f} (\mathfrak{f} \in I_K) \) constitute an inverse system of finite monoids; and the Deligne-Ribet monoid \( DR_K \) is then defined as the inverse limit of this system:

**Definition 2.1.2** (the Deligne-Ribet monoid \( DR_K \)). The Deligne-Ribet monoid \( DR_K \) is the profinite monoid defined as the following inverse limit of the above inverse system of the ray class monoids \( DR_\mathfrak{f} \):

\[
DR_K := \lim_{\mathfrak{f} \in I_K} DR_\mathfrak{f}. \tag{2.4}
\]

**Remark 2.1.3.** By definition, \( DR_K \) is commutative; also, for each \( \mathfrak{f} \in I_K \), we can identify \( DR_\mathfrak{f} = C_\mathfrak{f} \), where \( DR_\mathfrak{f} \) is the unit group of \( DR_\mathfrak{f} \) and \( C_\mathfrak{f} \) is the strict ray class group with the conductor \( \mathfrak{f} \cdot \infty \) (cf. 2.6, [11]). Taking inverse limit, we then have an isomorphism \( DR_K \cong \varprojlim C_\mathfrak{f} \cong G_K^{\text{op}} \), where the second isomorphism is the class-field-theory isomorphism.
The above-mentioned map $G_K \times I_K \to DR_K$ is then given, on the second factor, as the canonical map $I_K \to DR_K$; and on the first factor, as the composition $G_K \to G_K^a \simeq \lim_i C^i \simeq DR_K \subseteq DR_K$. With this, we restate here the result of Borger and de Smit [3]:

**Theorem 2.1.4** (Theorem 1.2 [3]). A finite etale $\Lambda$-ring $X$ over $K$ has an integral model if and only if the $(G_K \times I_K)$-action on the finite set $F_K(X)$ factors through the map $G_K \times I_K \to DR_K$ given above; in other words, this means that the fundamental monoid $\pi_1(\mathcal{C}_K^\text{op}, F_K)$ is isomorphic to $DR_K$ and we have the following equivalence of categories:

$$
\mathcal{C}_K^\text{op} \xrightarrow{\approx} \mathcal{B}_f DR_K
$$

**Remark 2.1.5** (every component of $X \in \mathcal{C}_K$ is abelian). Recall that, since the underlying $K$-algebra of each object $X \in \mathcal{C}_K$ is finite etale over $K$, we have an isomorphism $X \simeq L_1 \times \cdots \times L_n$ for some finite extensions $L_i/K$ of number fields. As described above, moreover, since the action of $G_K$ onto $F_K(X)$ factors through the abelianization $G_K \to G_K^a$, it follows that every component $L_i$ of $X$ must be abelian over $K$. (See §3 [3] for a reason of this fact; this is not true for finite etale $\Lambda$-rings without integral models.) We shall use this fact throughout this paper.

**Remark 2.1.6** (the case of $K = \mathbb{Q}$). In [2], preceding [3], the authors studied the case when $K$ is the rational number field $\mathbb{Q}$. In this case, it is shown that the Deligne-Ribet monoid $DR_\mathbb{Q}$ is isomorphic to the multiplicative monoid $\hat{\mathbb{Z}}$ of profinite integers. In particular, the monoid $I_\mathbb{Q}$ is identified with the multiplicative monoid $\mathbb{N}$ of positive integers; and we can see that $DR_N$ for $N \in \mathbb{N}$ is isomorphic to the multiplicative monoid $\mathbb{Z}/N\mathbb{Z}$.

**Remark 2.1.7** (galois objects). The major subject of [3] is to classify the galois objects of $\mathcal{C}_K$ in terms of integral Witt vectors. For this reason, we recall here a few basic facts about galois objects of the semi-galois category $\mathcal{C}_K$; nevertheless, instead of recalling the fully general facts on galois objects (cf. §3.2 [15]), it is sufficient for our purpose to see some description of the galois objects of $\mathcal{B}_f DR_K$. In this category $\mathcal{B}_f DR_K$, the galois objects are precisely the rooted $DR_K$-sets, i.e., those $DR_K$-sets $S \in \mathcal{B}_f DR_K$ which have some $s_0 \in S$ such that $S = s_0 \cdot DR_K$; in this case, $s_0 \in S$ is called a root of $S$. (In general, rooted objects are not galois; but in the current situation, $DR_K$ is commutative: from this, it follows that rooted objects in $\mathcal{B}_f DR_K$ are always galois.) In terms of $\Lambda$-rings $X \in \mathcal{C}_K$, this means that $X \in \mathcal{C}_K$ is galois if and only if there exists $s_0 \in F_K(X) = \text{Hom}_K(X, K)$ such that every $s \in F_K(X)$ can be written as $s = \sigma \circ s_0 \circ \psi_a$ for some $\sigma \in G_K$ and $a \in I_K$. We shall use this fact for the study in [3].

### 2.2 The moduli spaces of lattices

The Deligne-Ribet monoid $DR_K$ was defined as the inverse limit $\lim_f DR_f$ of the ray class monoids $DR_f$ ($f \in I_K$); but as proved by Yalkinoglu [19], this profinite monoid $DR_K$ has yet another aspect as the “moduli space” of 1-dimensional $K$-lattices up to some scaling [10] [12]. In the case when $K$ is an imaginary quadratic field in particular, such $K$-lattices are naturally 2-dimensional $\mathbb{Q}$-lattices; therefore, $DR_K$ then has a natural embedding to the space $\text{Lat}_2^K$ of 2-dimensional $\mathbb{Q}$-lattices up to scaling, which is further proved isomorphic to a certain quotient space $\Gamma \backslash (M_2(\hat{\mathbb{Z}}) \times \delta)$. In this subsection, we recall these facts essentially from [10] [11] [19] [12] which will provide a key for relating Witt vectors to modular functions.
Throughout this subsection, let us suppose that $K$ is an imaginary quadratic field, and also let $O_K = \mathbb{Z}\tau + \mathbb{Z}$ with $\tau \in \mathcal{H}$, where $\mathcal{H}$ denotes the upper half plane in $\mathbb{C}$. For a number field $K$, we denote by $\mathbb{A}_K$ the ring of adeles of $K$; by $\mathbb{A}_{K, fin}$ the ring of finite adeles; and also, by $\mathcal{O}_K$ the ring of finite integral adeles. In general, for a ring $R$, we denote by $R^*$ the invertible elements. Finally, $[-] : \mathbb{A}_K^* \rightarrow G_K^{ab}$ denotes the Artin map.

We start with relating $DR_K$ with 1-dimensional $K$-lattices, which is defined as follows:

**Definition 2.2.1** ($K$-lattices; [10]). A (1-dimensional) $K$-lattice is a pair $(\Lambda, \phi)$ of a finitely generated $O_K$-submodule $\Lambda$ of $\mathbb{C}$ such that $K \otimes_{O_K} \Lambda \simeq K$ and a $O_K$-linear homomorphism $\phi : K/O_K \rightarrow \Lambda$.  

**Example 2.2.2** (cf. Lemma 2.4 [10]). Fractional ideals of $K$ are “prototypical” examples of $K$-lattices in the sense that, up to scaling by some $\lambda \in \mathbb{C}^*$, every $K$-lattice $\Lambda \subseteq \mathbb{C}$ becomes a fractional ideal as $\lambda \Lambda \subseteq K$. Such a scaling factor $\lambda \in \mathbb{C}^*$ is unique modulo $K^*$.

**Proposition 2.2.3** (cf. Proposition 2.6 [10]). There are bijective correspondences (1) between $\mathcal{O}_K \times \hat{\mathcal{O}}_K (\mathbb{A}_K^*/K^*)$ and the set of $K$-lattices, and (2) between $\mathcal{O}_K \times \hat{\mathcal{O}}_K (\mathbb{A}_{K, fin}^*/K^*)$ and the set of $K$-lattices up to scaling.

**Proof.** For this result, the reader is referred to [10]; we just describe the correspondence. For $[\rho, t] \in \mathcal{O}_K \times \hat{\mathcal{O}}_K (\mathbb{A}_K^*/K^*)$, the correspondence is given by $[\rho, t] \mapsto (\Lambda_t, \phi_{(\rho, t)})$, where $\Lambda_t := t_{\infty}^{-1}(t_f \mathcal{O}_K \cap K)$ with $t_f, t_{\infty}$ denoting the non-archimedian and archimedian components of $t = (t_f, t_{\infty}) \in \mathbb{A}_K^*$ and $\phi_{(\rho, t)} : K/O_K \rightarrow K \Lambda_t/\Lambda_t$ is given by the following composition (the upper row):

$$
\begin{array}{ccc}
K/O_K & \longrightarrow & K/O_K \\
\simeq & & \simeq \\
\mathbb{A}_{K, fin}/\hat{\mathcal{O}}_K & \rho & \mathbb{A}_{K, fin}/\hat{\mathcal{O}}_K \\
t_f & \Lambda_t & \Lambda_t/\Lambda_t \\
\end{array}
$$

(2.5)

where $\rho, t_f$, and $t_{\infty}^{-1}$ denote the maps given by the straightforward multiplications. Based on this, the second correspondence is given just by forgetting the scaling factor $t_{\infty}$.  

**Proposition 2.2.4** ($DR_K$ as moduli space). There is a bijective correspondence between $DR_K$ and the set of $K$-lattices up to scaling.

**Proof.** This is given as a combination of the above results of [10] and that of [19] together with the class field theory isomorphism $[-] : \mathbb{A}_{K, fin}^*/K^* \simeq G_K^{ab}$. That is, by Proposition 8.2 [19], we have an isomorphism $DR_K \simeq \hat{\mathcal{O}}_K \times \hat{\mathcal{O}}_K G_K^{ab}$; then, by combining with $G_K^{ab} \simeq \mathbb{A}_{K, fin}^*/K^*$, this induces an isomorphism $DR_K \simeq \hat{\mathcal{O}}_K \times \hat{\mathcal{O}}_K (\mathbb{A}_{K, fin}^*/K^*)$. As proved above, the latter corresponds to the set of $K$-lattices up to scaling, hence the claim.  

In what follows, we shall denote by $Lat^1_K$ the set of $K$-lattices up to scaling; for each $K$-lattice $(\Lambda, \phi)$, we shall denote by $[\Lambda, \phi] \in Lat^1_K$ the equivalence class (up to scaling) of $(\Lambda, \phi)$. So far, we proved the following isomorphisms:

$$
DR_K \simeq \hat{\mathcal{O}}_K \times \hat{\mathcal{O}}_K (\mathbb{A}_{K, fin}^*/K^*) \simeq Lat^1_K.
$$

(2.6)
Moreover, since $K$ is now imaginary quadratic, hence, of degree 2 over $\mathbb{Q}$, we can then think of $K$-lattices as 2-dimensional $\mathbb{Q}$-lattices in the following sense:

**Definition 2.2.5 (2-dimensional $\mathbb{Q}$-lattice).** A (2-dimensional) $\mathbb{Q}$-lattice is a pair $(\Lambda, \phi)$ of a lattice $\Lambda$ in $\mathbb{C}$ and a homomorphism $\phi : \mathbb{Q}^2/\mathbb{Z}^2 \to \mathbb{Q}\Lambda/\Lambda$.

Recall that we now have $O_K = \mathbb{Z}\tau + \mathbb{Z}$ for $\tau \in \mathfrak{H}$, hence, $K = \mathbb{Q}\tau + \mathbb{Q}$; this choice of the basis $(\tau, 1)^t$ of $K$ over $\mathbb{Q}$ gives an isomorphism $K \simeq \mathbb{Q}^2$, with $O_K \simeq \mathbb{Z}^2$. Also, note that for a $K$-lattice $\Lambda \subseteq \mathbb{C}$, we have $K\Lambda = \mathbb{Q}\Lambda \subseteq \mathbb{C}$. By these identifications, each $K$-lattice $(\Lambda, \phi)$ naturally defines a (2-dimensional) $\mathbb{Q}$-lattice $(\Lambda', \phi')$, where $\phi' : \mathbb{Q}^2/\mathbb{Z}^2 \to \mathbb{Q}\Lambda'/\Lambda'$ is given by:

$$\phi' : \mathbb{Q}^2/\mathbb{Z}^2 \simeq K/O_K \xrightarrow{\phi} K\Lambda/\Lambda = \mathbb{Q}\Lambda/\Lambda. \quad (2.7)$$

In this sense, we identify $K$-lattices $(\Lambda, \phi)$ with (2-dimensional) $\mathbb{Q}$-lattices; and denote by the same symbol $(\Lambda, \phi)$.

In general, as in the case of $K$-lattices, 2-dimensional $\mathbb{Q}$-lattices can be classified with a certain "moduli space"; the following proposition essentially due to [9] gives a description of the space: (In what follows, we simply denote $\Gamma := SL_2(\mathbb{Z})$.)

**Proposition 2.2.6 ([9]).** There is a bijective correspondence between $\Gamma \backslash (M_2(\hat{\mathbb{Z}}) \times GL_2^+(\mathbb{R}))$ and the set of $\mathbb{Q}$-lattices. By this correspondence, we have a bijective correspondence between $\Gamma \backslash (M_2(\hat{\mathbb{Z}}) \times \mathfrak{H})$ and the set of $\mathbb{Q}$-lattices up to scaling by $\mathbb{C}^\ast$ as well.

**Proof.** The proof is essentially due to [9]; but we need modify the constructions there so that our constructions below get compatible with the conventions in [14]. With this slight modification, the proof in [4] works well. To be more specific, for each $(m, \alpha) \in M_2(\hat{\mathbb{Z}}) \times GL_2^+(\mathbb{R})$, the corresponding $\mathbb{Q}$-lattice is defined by $(m, \alpha) \mapsto (\Lambda_\alpha, m\alpha)$, where $\Lambda_\alpha := \mathbb{Z}^2 \cdot \alpha \cdot (i, 1)^t$ regarding $\mathbb{Z}^2$ as consisting of row vectors, and $m\alpha : \mathbb{Q}^2/\mathbb{Z}^2 \to \mathbb{Q}\Lambda_\alpha/\Lambda_\alpha$ is given by $a \mapsto a \cdot m\alpha \cdot (i, 1)^t$ for $a = (a_1, a_2) \in \mathbb{Q}^2/\mathbb{Z}^2$. (Here $M_2(\hat{\mathbb{Z}})$ acts on $\mathbb{Q}^2/\mathbb{Z}^2$ as $\mathbb{Q}^2/\mathbb{Z}^2 \simeq A_2^2/\mathbb{Z}^2/\mathbb{Z}^2$.) The group $\Gamma = SL_2(\mathbb{Z})$ acts on $M_2(\hat{\mathbb{Z}}) \times GL_2^+(\mathbb{R})$ by $(\gamma, (m, \alpha)) \mapsto (m\gamma^{-1}, \gamma\alpha)$. With this definition, the above correspondence $(m, \alpha) \mapsto (\Lambda_\alpha, m\alpha)$ induces a bijection from $\Gamma \backslash (M_2(\hat{\mathbb{Z}}) \times GL_2^+(\mathbb{R}))$ to the set of $\mathbb{Q}$-lattices.

Concerning the second claim, note that the action of scaling $\lambda = s + it \in \mathbb{C}^\ast$ on $\Lambda_\alpha$ corresponds to the action of the following matrix on the right of $\alpha \in GL_2^+(\mathbb{R})$:

$$\lambda = \begin{pmatrix} s & -t \\ t & s \end{pmatrix}. \quad (2.8)$$

Also the quotient $GL_2^+(\mathbb{R})/\mathbb{C}^\ast$ by this action of $\mathbb{C}^\ast$ can be identified with the upper half plane $\mathfrak{H}$ via the following correspondence $GL_2^+(\mathbb{R}) \to \mathfrak{H}$:

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \mapsto \quad \alpha(i) := \frac{ai + b}{ci + d}. \quad (2.9)$$

By this identification, we eventually obtain a bijection from $\Gamma \backslash (M_2(\hat{\mathbb{Z}}) \times \mathfrak{H})$ to the set of $\mathbb{Q}$-lattices up to scaling.

**Remark 2.2.7 (basis of $\Lambda_\alpha$).** Suppose that $\alpha \in GL_2^+(\mathbb{R})$ is given as follows:

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \quad (2.10)$$


Then the basis of $\Lambda_\alpha$ is given by $(ai+b, ci+d)$; that is, $\Lambda_\alpha = \mathbb{Z}(ai+b) + \mathbb{Z}(ci+d)$. Also, note that $\tau_\alpha := \alpha(i) = (ai+b)/(ci+d)$ corresponds to this lattice $\Lambda_\alpha$ up to scaling.

Let $\text{Lat}_X^2$ denote the set of 2-dimensional $\mathbb{Q}$-lattices up to scaling. In the above lemma, we have constructed the isomorphism $\text{Lat}_X^2 \simeq \Gamma\backslash ([M_2(\mathbb{Z}) \times \mathfrak{f}]$; and we also have a natural embedding of sets $\text{Lat}_K^1 \hookrightarrow \text{Lat}_X^2$ in the sense mentioned above. Consequently, we have constructed the following sequence of maps:

$$DR_K \simeq \hat{O}_K \times \hat{O}_K \simeq \Gamma\backslash ([M_2(\mathbb{Z}) \times \mathfrak{f}]$$

We will use this sequence of maps in §3 to relate Witt vectors with modular functions.

### 3 Galois objects of $\mathcal{E}_K$

In this section, before proceeding to our major subject in §4, we develop some general facts about the $\Lambda$-ring $K \otimes W^n_{O_K}(O_K)$ of algebraic Witt vectors. The first subsection (§3.1) gives a classification of galois objects of $\mathcal{E}_K$; from which we deduce the universality of $K \otimes W^n_{O_K}(O_K)$ with respect to the $\Lambda$-rings in $\mathcal{E}_K$; the second subsection (§3.2) studies the structure of the galois objects of $\mathcal{E}_K$, where we particularly determine the state complexity of integral Witt vectors; the last subsection (§3.3) gives a presentation of $W^n_{O_K}(O_K)$ and $K \otimes W^n_{O_K}(O_K)$ when $K$ is the rational number field $\mathbb{Q}$, which are proved isomorphic to the group-rings $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ and $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ respectively. After developing these basic results, the next section (§4) then proceeds to our major subject, where we study these rings when $K$ is an imaginary quadratic field.

#### 3.1 Classification of galois objects

The subject of this subsection is to classify the galois objects in $\mathcal{E}_K$ in terms of integral Witt vectors; in this section, let $E_K$ denote the direct limit of the galois objects of $\mathcal{E}_K$ (see §3.1 [15] for the inverse system of galois objects of $\mathcal{E}_K$). We prove that $E_K$ is naturally isomorphic to $K \otimes W^n_{O_K}(O_K)$; this gives a characterization of our $\Lambda$-ring $K \otimes W^n_{O_K}(O_K)$ of algebraic Witt vectors, which gives a basis of our study in §4.

To this end we need the following construction:

**Definition 3.1.1 (\(\Lambda\)-ring $X_\Xi$).** Let $\Xi \subseteq W^n_{O_K}(O_K)$ be a finite subset. Then the associated $\Lambda$-ring $X_\Xi$ is defined as follows:

$$X_\Xi := K \otimes O_K[I_K \Xi],$$

where $I_K \Xi$ is the orbit of $\Xi$ under the action of $\psi_a$s ($a \in I_K$).

We show that these $\Lambda$-rings are always galois objects of $\mathcal{E}_K$; and conversely, every galois object of $\mathcal{E}_K$ is of this form up to isomorphism:

**Proposition 3.1.2.** For any finite set $\Xi \subseteq W^n_{O_K}(O_K)$, the associated $\Lambda$-ring $X_\Xi$ is a galois object with its root given by $X_\Xi \ni \eta \mapsto \eta_1 \in K$.

**Proof.** The proof of the first claim that $X_\Xi$ has an integral model (i.e. is an object of $\mathcal{E}_K$) follows similarly to that of Proposition 4. [16] We prove that $X_\Xi$ is a galois object with the homomorphism
Given by \( s \in G_K \eta \) every component being abelian, we can take a finite abelian subfield \( \bar{\eta} \) for every \( s \in G_K \) (cf. Remark 2.1.7). (In this proof, let us denote \( X := X_{\bar{\eta}} \) for simplicity.)

To see this, let us first consider a monoid congruence \( \equiv \) on \( I_K \) defined by \( a \equiv b \) if and only if \( \psi_a \xi = \psi_b \xi \) for every \( \xi \in \Xi \), which is of finite index since the orbit of \( \Xi \) under the action of \( \psi_a \)'s \( (a \in I_K) \) is finite (cf. Theorem 3.4 [16]). Let \( I_K = J_1 \sqcup \cdots \sqcup J_N \) be the \( \equiv \)-class decomposition; and choose their representatives, say \( a_i \in J_i \) for \( i = 1, \cdots, N \). Also, since \( X \) is finite over \( K \) with each component being abelian, we can take a finite abelian subfield \( \bar{K} / L / K \) so that the image \( s(X) \) for every \( s : X \to \bar{K} \) is contained in \( L \). Then let us define a homomorphism \( t : X \to L \times \cdots \times L \) by \( t(\eta) := (\eta_{a_1}, \cdots, \eta_{a_N}) \), which is injective. In fact, note first that if \( a \equiv b \) then \( \eta_a = \eta_b \) for every \( \eta \in \Xi \) by the fact that \( \Xi \) is generated by the orbit \( I_K \Xi \) and by definition of \( \equiv \). Therefore, the values of \( \eta_a \) are determined by those of \( \eta_{a_i} \) for \( i = 1, \cdots, N \); hence \( t : X \to L \times \cdots \times L \) is injective. This means that the \( G_K \)-set \( \text{Hom}_K(X, \bar{K}) \) is a quotient of \( \prod \text{Hom}_K(L, \bar{K}) \) induced from \( t : X \to L \times \cdots \times L \); and by construction, this proves the claim that every \( s \in \text{Hom}_K(X, \bar{K}) \) is given by \( s = \sigma \circ s_1 \circ \psi_a \), for some \( i \).

**Proposition 3.1.3.** Every galois object \( X \in \mathcal{C}_K \) is isomorphic to \( X_{\Xi} \) for some finite subset \( \Xi \subseteq W_{O_K}^a (O_{\bar{K}}) \).

**Proof.** Let \( s : X \to \bar{K} \) be a root of \( X \) and \( A \subseteq X \) be its integral model. For each \( \xi \in X \) we define \( \xi^s = (\xi_a^s) \in \bar{K}^A \) by \( \xi_a^s := s(\psi_a \xi) \). It is not difficult to see that \( \xi^s \in W_{O_K}^a (O_{\bar{K}}) \) for every \( \xi \in A \) because \( A \) is an integral model. Also, since \( X = K \otimes A \) and \( A \) is finite over \( O_K \), there exist some \( \xi_1, \cdots, \xi_n \in A \) that generate \( X \) over \( K \). Let \( \Xi := \{ \xi_1^s, \cdots, \xi_n^s \} \subseteq W_{O_K}^a (O_{\bar{K}}) \). We prove that \( X \) is isomorphic to \( \Xi \). Notice that the assignment \( \xi \mapsto \xi^s \) for every \( \xi \in X \) defines a \( \Lambda \)-ring homomorphism \( X \to \Xi \), which is clearly surjective. To show its injectivity, note that since \( s \) is a root of the galois object \( X \), every homomorphism \( s' : X \to \bar{K} \) is a composition \( s' = s \circ f \) for some \( f \in \text{End}(X) \). Also, by the fact that \( \text{End}(X) \) is generated by \( \psi_a \)'s, this implies that the values \( \xi_a^s = s(\psi_a \xi) \) determines \( \xi \in X \); hence, \( \xi \mapsto \xi^s \) is indeed injective.

Therefore, the galois objects in \( \mathcal{C}_K \) are precisely of the form \( X_{\Xi} \) for some finite \( \Xi \subseteq W_{O_K}^a (O_{\bar{K}}) \). Consequently, we obtain the following presentation of the \( K \)-algebra \( E_K \) in terms of integral Witt vectors:

**Theorem 3.1.4.** We have a canonical isomorphism of \( \Lambda \)-rings:

\[
E_K \simeq K \otimes W_{O_K}^a (O_{\bar{K}}).
\]

(In particular, \( W_{O_K}^a (O_{\bar{K}}) \) is isomorphic to the direct limit of the maximal integral models of galois objects of \( \mathcal{C}_K \).

**Proof.** This isomorphism \( E_K \to K \otimes W_{O_K}^a (O_{\bar{K}}) \) is given as (the direct limit of) the isomorphisms \( X \to X_{\Xi} \) constructed in the above proposition for galois objects \( X \).

**Remark 3.1.5.** In what follows we identify \( E_K \) with \( K \otimes W_{O_K}^a (O_{\bar{K}}) \) in the sense of this isomorphism, and often call \( E_K \) as the \( K \)-algebra of algebraic Witt vectors.

**Corollary 3.1.6.** The \( K \)-algebra \( E_K = K \otimes W_{O_K}^a (O_{\bar{K}}) \) is isomorphic to the \( K \)-algebra of all locally constant \( K \)-valued \( G_K \)-equivariant functions on \( DR_K \), symbolically, \( E_K = \text{Hom}_{C_K}(DR_K, \bar{K}) \).

11
Proof. This is a direct consequence of Theorem 3.1.4 above, and see also Theorem 10.1 [19] due to Neshveyev. To be more precise, Theorem 10.1 [19] claims that $E_K$ is isomorphic to the $\mathbb{K}$-algebra of such functions. Since we proved that $E_K$ is also isomorphic to $\mathbb{K} \otimes W^n_{O_K}(O_K)$, the composition of these isomorphisms shows the claim of this corollary.

Remark 3.1.7 (cyclic Witt vector). We are concerned with whether every galois object $X \in \mathcal{C}_K$ is actually isomorphic to $X_\xi$ for some $\xi \in W^n_{O_K}(O_K)$, that is, whether we can take $\Xi \subseteq W^n_{O_K}(O_K)$ in Proposition 3.1.3 as a singleton $\Xi = \{\xi\}$. This is true for e.g. the (cofinal) galois objects of the form $Q[x]/(x^n - 1)$ of $\mathcal{C}_Q$; but we do not know whether every galois object $X$ has such a $\xi$ in general, which we shall call a cyclic Witt vector for $X$ (a la, cyclic vectors for differential modules known in differential galois theory).

Remark 3.1.8 (galois correspondence). Although we do not give a proof here, it would be meaningful to mention a certain galois correspondence that naturally extends the usual galois correspondence of galois theory for number fields. To be specific, our galois correspondence is the one between the following objects:

1. $\Lambda$-subalgebras of $E_K$;
2. profinite quotients of $DR_K$;
3. semi-galois full subcategories of $\mathcal{C}_K$.

This follows from the presentation of $E_K = \text{Hom}_{G_K}(DR_K, \bar{K})$ and $DR_K = \text{Hom}_K(E_K, \bar{K})$ as well as the duality between $DR_K$ and $\mathcal{C}_K$.

3.2 The structure of galois objects

As we proved in the above subsection, the galois objects of $\mathcal{C}_K$ are precisely those of the form $X_\Xi$ for some finite $\Xi \subseteq W^n_{O_K}(O_K)$. In this subsection, we then study the structure of the galois objects $X_\Xi$ and represent $X_\Xi$ in terms of $\xi \in \Xi$. Starting from some general facts about galois objects in $\mathcal{C}_K$, we describe the components $L_i$ of $X_\Xi \simeq L_1 \times \cdots \times L_r$ and also determine the state complexity of integral Witt vectors $\xi \in W^n_{O_K}(O_K)$, which is a natural analogue of Bridy’s result [5] on formal power series $\xi \in \mathbb{F}_q[[t]]$ algebraic over $\mathbb{F}_q[t]$.

To this end, we need to prepare some general lemmas:

Lemma 3.2.1. Let $X \in \mathcal{C}_K$. If $p$ is an automorphism on $X$, then the action of $p$ on $F_K(X)$ is equal to that of some $\sigma \in G_K$.

Proof. The proof is done by completion and Theorem 1.1, [4]. Let $A \subseteq X$ be the maximal integral model of $X$ and $K_p$ be the completion of $K$ at $p$; also let $X_p = K_p \otimes X$ and $A_p = O_{K_p} \otimes A$. Then $X_p$ together with $\psi_p$ is a $\Lambda_p$-ring with integral model $A_p$. Since $\psi_p$ is an automorphism on $X_p$, the set $S_{unr} := \cap_{n=0}^\infty Sp^n$, where $S := F_{K_p}(X_p)$, is equal to $S$ itself. This implies that, by Theorem 1.1, [4], the action of $p$ on $S_{unr} = S$ is equal to the Frobenius $\sigma_p \in G_K$ (where $I_p \leq G_K$, denotes the inertia subgroup).

Lemma 3.2.2. Let $X \in \mathcal{C}_K$ be a galois object. If $f \in \text{End}(X)$ is an automorphism of the $\Lambda$-ring $X$, then the action of $f$ on $F_K(X)$ by pullback is equal to the action of some $\sigma \in G_K$. 12
Proof. Let \( f \in \text{End}(X) \) be an automorphism. Since \( X \) is galois and \( I_K \) is dense in \( DR_K \), the action of \( f \) on \( F_K(X) \) by pullback is equal to that of \( \psi_a \) for some \( a \in I_K \). (To see this, recall the definition of galois objects, Definition 12, §3.2 [15], and the fact that the galois objects of \( \mathcal{B}_f DR_K \) are those \( DR_K \)-sets which are of the form of finite quotients \( DR_K \twoheadrightarrow H \), cf. Lemma 17, §4.1 [15].) Now since \( f \) is an automorphism, so is the action of \( \psi_a \). Hence, if \( a = p_1 \cdots p_n \), the actions of \( \psi_{p_i} \)'s are all automorphisms as well. By the above lemma, the actions of \( \psi_{p_i} \)'s come from some \( \sigma_i \in G_K \); hence, so is the action of \( \psi_a = \psi_{p_1} \cdots \psi_{p_n} \), which is equal to that of \( f \). \( \square \)

To proceed further, let us recall the following notion from semigroup theory:

**Definition 3.2.3** (\( J \)-equivalence). Let \( M \) be a commutative monoid. For two elements \( s, s' \in M \), we denote as \( s \preceq_J s' \) if we have an inclusion of the (two-sided) ideals \( sM \subseteq s'M \), or in other words, there exists \( m \in M \) such that \( s = s'm \). Furthermore, we denote as \( s \sim_J s' \) and say that \( s \) and \( s' \) are \( J \)-equivalent if \( s \preceq_J s' \) and \( s' \preceq_J s \). The set of \( J \)-equivalent classes is denoted as \( M/J \).

**Lemma 3.2.4.** Let \( X \in \mathcal{C}_K \) be galois with \( s_1 : X \rightarrow \bar{K} \subseteq F_K(X) \) its root. Then, \( f, f' \in \text{End}(X) \) are \( J \)-equivalent in the (commutative) monoid \( \text{End}(X) \) if and only if the corresponding \( s_1 \circ f, s_1 \circ f' \in F_K(X) \) belong to the same \( G_K \)-component.

**Proof.** For the reason mentioned in the above lemma, we may put \( f = \psi_a \) and \( f' = \psi_{a'} \) for some \( a, a' \in I_K \). First suppose that \( s_a := s_1 \circ \psi_a \) and \( s_{a'} := s_1 \circ \psi_{a'} \) belong to the same \( G_K \)-component in \( F_K(X) \); that is, \( s_a = \sigma \circ s_{a'} \) for some \( \sigma \in G_K \). By the density of \( I_K \) in \( DR_K \), the action of \( \sigma \) is equal to the action of \( \psi_b \) for some \( b \in I_K \), which means that \( s_a = s_{a'b} \). Hence, we have \( \psi_a \preceq_J \psi_a' \) in \( \text{End}(X) \). (This is because \( (X, s_1) \) is now galois, thus the assignment \( \text{End}(X) \ni f \mapsto s_1 \circ f \in F_K(X) \) is injective; cf. Proposition 4, §3.2 [15].) The converse inequality \( \psi_a' \preceq_J \psi_a \) is similar, thus, \( \psi_a \) and \( \psi_{a'} \) are \( J \)-equivalent. Second suppose that \( \psi_a \) and \( \psi_{a'} \) are \( J \)-equivalent in \( \text{End}(X) \), whence \( \psi_a = \psi_{a'b} \) and \( \psi_{a'} = \psi_{a'b'} \) for some \( b, b' \in I_K \). Dually, i.e. in terms of the \( DR_K \)-set \( F_K(X) \), this means that \( s_a \) and \( s_{a'} \) are mutually accessible by the action of \( DR_K \), that is, \( s_a \cdot DR_K = s_{a'} \cdot DR_K \). We put \( S := s_a \cdot DR_K = s_{a'} \cdot DR_K \). Then, note that this \( S \) forms a rooted \( DR_K \)-set, hence, galois in \( \mathcal{B}_f DR_K \) (cf. Remark 2.1.7 [13] 2.1); and also that, by \( \psi_a = \psi_{a'b} \) and \( \psi_{a'} = \psi_{a'b'} \), one sees that the actions of \( \psi_b, \psi_{b'} \) on \( S \) are (mutually inverse) automorphisms. Thus, by Lemma 3.2.2 applied to (the \( \Lambda \)-ring in \( \mathcal{C}_K \) dual to) this galois object \( S \in \mathcal{B}_f DR_K \), it follows that the actions of \( \psi_b, \psi_{b'} \) on \( S \) are equal to those of some \( \sigma, \sigma' \in G_K \), which implies that \( s_a = s_{a'b} \) and \( s_{a'} = s_{a'b'} \) belong to the same \( G_K \)-component. This completes the proof. \( \square \)

Now we study the structure of the galois objects \( X_\xi \in W_{O_K}(O_K) \). (For simplicity, we shall study the structure of \( X_\Xi \) only for singleton \( \Xi = \{ \xi \} \), but a similar result holds in general.) Since \( X_\xi \) is finite etale over \( K \), we have an isomorphism \( X_\xi \simeq L_1 \times \cdots \times L_r \) for some finite extensions \( L_i/K \). However, we do not yet quite know what and how many components \( L_i \) each \( X_\xi \) has. In the following, we first discuss this problem. In this relation, let us denote by \( M_\xi \) the quotient monoid \( I_K/\equiv_\xi \), where \( a \equiv_\xi b \) if and only if \( \psi_\xi a = \psi_\xi b \); by Theorem 3.2, [10], \( M_\xi \) is a finite monoid.

**Proposition 3.2.5.** For any \( \xi \in W_{O_K}(O_K) \) we have the following isomorphism:

\[
X_\xi \simeq \prod_{[a] \in M_\xi/\mathcal{J}} K(\xi_{ab}; b \in I_K).
\]

In particular, the number of components is equal to \( \#(M_\xi/\mathcal{J}) \).
Proof. For short let us put the right-hand side as \( Y_\xi := \prod_{i \in M_{\xi} / J} K(\xi_{ab}; b \in I_K) \); we construct the target isomorphism \( f : X_\xi \to Y_\xi \). Let \( M_{\xi} / J = \{[a_1], \ldots, [a_r]\} \), and for each \([a_i] \in M_{\xi} / J\), denote its representative as \( a_i \in I_K \). Then we can define \( f : X_\xi \to Y_\xi \) by \( f(\eta) := (\eta_{a_i})^\sigma_{a_i}, \) for every \( \iota \). To prove the lemma, note first that this \( f \) is injective: If \( f(\eta) = f(\eta') \) then \( \eta_{a_i} = \eta'_{a_i} \) for every \( i = 1, \ldots, r \). But for each \( a \in I_K \) we have \([a] = [a_i] \) for some \( i \); this means that, for every \( \xi \in X_\xi \), we have \( \xi_a = \xi_{a_i} \), for some \( \sigma \in G_K \). (In fact \([a] = [a_i] \) implies \( a = a_i b \) and \( a_i = a_i b' \) for some \( b, b' \in I_K \) in \( M_{\xi} \), whence \( \psi_a = \psi_{a_i}, \psi_b \) and \( \psi_i = \psi_i \psi_{b'} \) on \( X_\xi \); then apply Lemma 3.2.4 to the root \( s_1 : X_\xi \to \eta \to \xi \in I_K \).) Thus \( c \eta = c \eta_{a_i} = c \eta_{a_i} \), \( c \eta' = c \eta_i \) for every \( a \in I_K \), which implies \( c \eta = c \eta' \) as requested.

Finally, we see that \( f \) is surjective. First note that, since \( X_\xi \) is finite etale over \( K \), we have an isomorphism \( X_\xi \simeq L_1 \times \cdots \times L_m \) for some finite extensions \( L_i / K \); and each \( L_i \) is obtained as the image of \( X_\xi \) under some \( s_i : X_\xi \to \bar{K} \in F_K(X_\xi) \). As shown in Proposition 3.1.2, each \( s_i \in F_K(X_\xi) \) is given as \( s_i(\eta) = \eta_{a_i} \) (\( \forall \eta \in X_\xi \)) for some \( a_i \in I_K \) and \( \sigma_i \in G_K \). Namely, \( s_i \) is \( G_K \)-equivalent to \( s_i^\prime \), \( s_i^\prime \) is \( F_K(X_\xi) \) given by \( s_i^\prime(\eta) = \eta_{a_i} \). So, the image \( L_i \) of \( X_\xi \) under \( s_i \) is isomorphic to \( K(\eta_{a_i} ; \eta \in X_\xi) \), which is further isomorphic to \( K(\xi_{a_i} ; b \in I_K) \) because \( \xi \) is generated by \( \psi_{b, \xi} \)'s \( \langle b \in I_K \rangle \) over \( K \). By Lemma 3.2.4, the two maps \( s_i \) and \( s_i^\prime \) are \( G_K \)-equivalent if and only if \([a_i] = [a_i] \). This means that the \( G_K \)-equivalence classes of \( s \in F_K(X_\xi) \) are classified precisely by the set \( \{ [a_i] \mid \sigma_i \in G_K \} \). Therefore, one concludes that \( m = r \) and \( L_i \simeq K(\xi_{a_i} ; b \in I_K) \), which completes the proof. \( \square \)

Finally, we determine the state complexity of integral Witt vectors \( \xi \in W_{O_K}^d(O_K) \) (cf Definition 3.2.6) as a natural analogue of the result of Bridy [5] for formal power series \( \xi \in F_q[[t]] \), where using the Riemann-Roch theorem he gave a sharp estimate of the state complexity of a formal power series \( \xi \in F_q[[t]] \) algebraic over \( F_q(t) \) in terms of the dimension \( \dim_{F_q(t)} X_\xi \) of the function field \( X_\xi \) of the curve generated by \( \xi \) over \( F_q(t) \). Analogously, we now show that the state complexity of an integral Witt vector \( \xi \in W_{O_K}^d(O_K) \) is equal to the dimension \( \dim_{K(X_\xi)} \bar{\xi} \) of the \( \Lambda \)-ring \( X_\xi \). In fact, this holds for general \( \Xi \subseteq W_{O_K}^d(O_K) \). To be precise, the state complexity of a finite set \( \Xi \subseteq W_{O_K}^d(O_K) \) is defined as follows: (See §3 [16] for the concept of DFA’s and DFAN’s (i.e. deterministic finite automata with output), and how they generate integral Witt vectors.)

Definition 3.2.6 (state complexity). Let \( \Xi \subseteq W_{O_K}^d(O_K) \) be any finite set of integral Witt vectors. We say that a DFA \( \Xi \) generates \( \Xi \) if for every \( \xi \in \Xi \) there exists an output function \( \tau : S_\Xi \to O_K \) such that \( \Xi \tau \) generates \( \xi \). The state complexity of \( \Xi \), denoted by \( c_\Xi \), is then defined as the minimum size \( \min \#S_\Xi \) of the state set \( S_\Xi \) of those DFA \( \Xi \) which can generate \( \Xi \).

Proposition 3.2.7 (estimate of state complexity). For any finite \( \Xi \subseteq W_{O_K}^d(O_K) \), we have the following identity:

\[
c_\Xi = \dim_K X_\Xi. \tag{3.4}
\]

In particular, \( c_\Xi = \dim_K X_\Xi \) for \( \xi \in W_{O_K}^d(O_K) \).

Proof. Firstly note that we have \( \dim_K X_\Xi = \#F_K(X_\Xi) \). Also it is easy to see that \( F_K(X_\Xi) \) forms (the state set of) a DFA over \( K \) that generates \( \Xi \); thus we have the one-side inequality:

\[
c_\Xi \leq \#F_K(X_\Xi) \tag{3.5}
\]

\[
= \dim_K X_\Xi. \tag{3.6}
\]
To prove the inverse inequality, note that by Proposition 3.1.2 we know that \( X_{\Xi} \) is a galois object; hence, \(#F_K(X_{\Xi}) = #\text{End}(X_{\Xi})\). Therefore, it suffices to prove:

\[
c_{\Xi} \geq #\text{End}(X_{\Xi}).
\] (3.7)

To this end, let \( A = (S, \delta, s_0) \) be a minimum DFA generating \( \Xi \). Then, by the minimality, every \( s \in S \) is represented as \( s = s_0 \cdot u \) for some \( u = p_1 \cdots p_n \in P^*_K \). Also, we can see that if \( s_0 \cdot u = s_0 \cdot v \) for \( u, v \in P^*_K \), then \( \psi_{a_n} = \psi_{a_n} \xi \) for every \( \xi \in \Xi \), where \( a_w = p_1 \cdots p_n \in I_K \) for \( w = p_1 \cdots p_n \in P^*_K \).

In fact, for each \( \xi \in \Xi \) there exists an output function \( \tau : S \rightarrow O_K \) such that for every \( w \in P^*_K \):

\[
(\psi_{a_n} \xi)_{a_w} = \xi_{a_w},
\]

\[
= \tau((s_0 \cdot u) \cdot w),
\]

\[
= \tau((s_0 \cdot v) \cdot w)
\]

\[
= (\psi_{a_n} \xi)_{a_w},
\]

which means that \( \psi_{a_n} \xi = \psi_{a_n} \xi \). Since \( X_{\Xi} \) is generated by \( I_K \Xi \), this then implies that \( \psi_{a_n} = \psi_{a_n} \) on \( X_{\Xi} \); hence, the assignment \( s \mapsto \psi_{a_n} \in #\text{End}(X_{\Xi}) \) is well-defined. Furthermore, by the fact that \( I_K \rightarrow DR_K \) is dense, this assignment \( S \rightarrow #\text{End}(X_{\Xi}) \) is in fact surjective, which proves the desired inequality \( c_{\Xi} = #S \geq #\text{End}(X_{\Xi}) \).

**Remark 3.2.8.** Note that the identity \( c_{\Xi} = \dim_K X_{\Xi} \) relates seemingly unrelated quantities, namely the state complexity \( c_{\Xi} \) and the dimension \( \dim_K X_{\Xi} \) of the \( K \)-algebra \( X_{\Xi} \). In fact, while the former is just the size of the orbit \( I_K \xi \) under the action of the Frobenius \( \psi_p \), the latter is the quantity relevant to the algebraic degree of its coefficients \( \xi_a \)'s. As we discuss below, this identity seems related to the difficulty of actually constructing integral Witt vectors; to our thought, this is because there must be some geometric reason for why the coefficients \( \xi_a \)'s of integral Witt vectors \( \xi \) distribute as they do. Concerning this, it will be meaningful to remark that the \( j \)-invariants \( j(a) \) in the theory of complex multiplication actually constitute an example of integral Witt vector; this is proved from their reciprocity law (cf. §4.1).

### 3.3 The structure of \( W^a_Z(\mathbb{Z}) \)

As an immediate consequence of the above general development, applied to the case \( K = \mathbb{Q} \), this section concludes with a presentation of the ring \( W^a_Z(\mathbb{Z}) \), which asserts that \( W^a_Z(\mathbb{Z}) \) is isomorphic to the group-ring \( \mathbb{Z}[Q/\mathbb{Z}] \). After this presentation we proceed to the case when \( K \) is an imaginary quadratic field.

**Corollary 3.3.1.** The ring \( W^a_Z(\mathbb{Z}) \) is isomorphic to the group-ring \( \mathbb{Z}[Q/\mathbb{Z}] \).

**Proof.** We first see that \( E_Q = \mathbb{Q} \otimes W^a_Z(\mathbb{Z}) \) is isomorphic to the group-ring \( \mathbb{Q}[Q/\mathbb{Z}] \). In fact, by the result of Borger and de Smit [2] combined with our result in §4.1, we know that \( E_Q \) is isomorphic to the \( \mathbb{Q} \)-algebra given by the direct limit \( \lim_{\leftarrow n} \mathbb{Q}[x]/(x^n - 1) = \bigcup_n \mathbb{Q}[x]/(x^n - 1) \); here this direct limit of \( \mathbb{Q} \)-algebras \( \mathbb{Q}[x]/(x^n - 1) \) is given by the following embeddings, for positive integers \( n, m \):

\[
\mathbb{Q}[x]/(x^n - 1) \rightarrow \mathbb{Q}[x]/(x^{nm} - 1)
\]

\[
x \mapsto x^m.
\] (3.12) (3.13)
The group-ring \( \mathbb{Q}[\mathbb{Q}/\mathbb{Z}] \), on the other hand, is also isomorphic to this \( \mathbb{Q} \)-algebra \( \bigcup_n \mathbb{Q}[x]/(x^n - 1) \) by the correspondence:

\[
\mathbb{Q}[\mathbb{Q}/\mathbb{Z}] \rightarrow \bigcup_n \mathbb{Q}[x]/(x^n - 1) \quad (3.14)
\]

\[
1/N \mapsto x \in \mathbb{Q}[x]/(x^N - 1). \quad (3.15)
\]

Hence we have \( E_{\mathbb{Q}} \simeq \mathbb{Q}[\mathbb{Q}/\mathbb{Z}] \). Finally we see that, in this isomorphism, the subring \( \mathbb{W}^a(\bar{\mathbb{Z}}) \subseteq E_{\mathbb{Q}} \) corresponds to \( \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \subseteq \mathbb{Q}[\mathbb{Q}/\mathbb{Z}] \). Indeed, as proved in Theorem 3.4 [2], the maximal integral model of the \( \Lambda \)-ring \( \mathbb{Q}[x]/(x^n - 1) \) is \( \mathbb{Z}[x]/(x^n - 1) \) for each \( n \); and thus, the subring \( \bigcup_n \mathbb{Z}[x]/(x^n - 1) \subseteq \bigcup_n \mathbb{Q}[x]/(x^n - 1) \) corresponds to \( \mathbb{W}^a(\bar{\mathbb{Z}}) \subseteq E_{\mathbb{Q}} \). On the other hand, we see that \( \bigcup_n \mathbb{Z}[x]/(x^n - 1) \) corresponds to \( \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \) under the above isomorphism \( \mathbb{Q}[\mathbb{Q}/\mathbb{Z}] \simeq \bigcup_n \mathbb{Q}[x]/(x^n - 1) \). Consequently, we obtain the desired isomorphism \( \mathbb{W}^a(\bar{\mathbb{Z}}) \simeq \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \). This completes the proof.

\[ \boxdot \]

**Remark 3.3.2.** More explicitly, in the above isomorphism \( \mathbb{W}^a(\bar{\mathbb{Z}}) \simeq \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \), each \( \gamma \in \mathbb{Q}/\mathbb{Z} \subseteq \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \) corresponds to the following Witt vector \( \zeta^{(\gamma)} \in \mathbb{W}^a(\bar{\mathbb{Z}}) \subseteq (\mathbb{Q}^{ab})^N \):

\[
\zeta^{(\gamma)} := (e^{2\pi i \gamma n})_{n \in \mathbb{N}}. \quad (3.16)
\]

Therefore we can conclude that, in general, the integral Witt vectors \( \xi \in \mathbb{W}^a(\bar{\mathbb{Z}}) \) are precisely the \( \mathbb{Z} \)-linear combinations of these \( \zeta^{(\gamma)}, \gamma \in \mathbb{Q}/\mathbb{Z} \) (while the algebraic Witt vectors \( \xi \in E_{\mathbb{Q}} \) are the \( \mathbb{Q} \)-linear combinations of \( \zeta^{(\gamma)} \)'s). This provides a complete classification of the integral Witt vectors over \( \mathbb{Z} \).

### 4 The modularity theorem

In some sense, the above isomorphism \( E_{\mathbb{Q}} \simeq \mathbb{Q}[\mathbb{Q}/\mathbb{Z}] \) clarifies how the coefficients \( \xi_n \) of an algebraic Witt vector \( \xi \) over \( \mathbb{Q} \) are correlated; they are essentially correlated as special values \( e^{2\pi i \gamma n} \) for fixed \( \gamma \in \mathbb{Q}/\mathbb{Z} \) of the function \( e^z \).

The purpose of this section is to prove an analogue of this result in the case where \( K \) is an imaginary quadratic field. To be precise, this section proves that the \( K \)-algebra \( E_K = K \otimes_{O_K} (O_K) \) for an imaginary quadratic field \( K \) is isomorphic to (or actually coincides with) the \( K \)-algebra \( M_K \) that consists of *modular vectors*; technically speaking, modular vectors are defined by special values of certain deformations of modular functions (§4.1). Our target theorem, which we call the *modularity theorem*, exhibits that such vectors arising from deformations of modular functions always define algebraic Witt vectors, and conversely, every algebraic Witt vector arises in this way (§4.2). After this, we then give a specific set of generators of \( E_K = M_K \) arising from the Fricke functions \( f_a \) (cf. §4.3).

#### 4.1 Modular vectors

Before developing general results, let us start with some motivating observation. As mentioned in Remark 3.2.8, the \( j \)-function, i.e. a prototypical example of modular function, naturally induces an example of integral Witt vector; indeed, as we see below, this fact follows from Hasse’s *reciprocity law* of the \( j \)-invariants \( j(a) \) (cf. 14). This basic observation gives us yet another way to look at integral Witt vectors and the \( j \)-function; and then, leads us to the general consideration of *modular vectors* developed below.
To be more specific, the $j$-function induces an integral Witt vector $\iota \in W^n_{\Omega_K}(O_K)$ by its special values in the following way:

**Proposition 4.1.1.** Define $\iota = (\iota_a) \in O_{H_K}^I$ by $\iota_a := j(a^{-1})$ for each $a \in I_K$; and let $H_K$ denote the Hilbert class field of $K$. Then $\iota$ is an integral Witt vector with coefficients in $O_{H_K}$:

$$\iota = (\iota_a) \in W^n_{\Omega_K}(O_{H_K}).$$

**Proof.** To see this, recall first that every prime $p \in P_K$ is unramified in $H_K$; therefore $H_K$ in itself forms an object of $\mathcal{C}_K$ together with the Frobenius automorphisms $\sigma_p \in Gal(H_K/K)$ ($p \in P_K$) as the $\Lambda$-structure $\psi_p$; there, $O_{H_K}$ is the maximal integral model.

With this in mind, take the natural embedding $s : H_K = K(j(1)) \hookrightarrow K \subseteq \mathbb{C}$; and for $\xi = j(1) \in O_{H_K}$, consider $\xi^a \in \hat{K}^{t\bar{\iota}}$ as in Proposition 3.1.3. Then, as discussed there, we have $\xi^a \in W^n_{\Omega_K}(O_K)$ because $j(1) \in O_{H_K}$. To be more specific, the component $\xi^a$s of $\xi^a \in W^n_{\Omega_K}(O_K)$ at each $a \in I_K$ is given by $s(\psi_a \xi)$; but by construction of $\xi = j(1) \in H_K$ and Hasse’s reciprocity law (i.e. $j(b)^{ap} = j(p^{-1}b)$ for $p \in P_K$ and fractional ideals $b$ of $K$), this means that $\xi^a = j(a^{-1}) = \iota_a$ for any $a \in I_K$, hence the claim. \hfill \Box

While algebraic (or integral) Witt vectors are defined in a purely algebraic way, this proposition indicates us an analytic way to construct a prototypical example of them. In fact we now see that this observation is a special case of a more general relationship between algebraic Witt vectors and modular functions; the following concept of Witt deformation family of modular functions is a key to explain this general relationship. In what follows, let us denote by $\mathfrak{f} = \bigcup N \mathfrak{f}_N$ the field of modular functions of finite level rational over $\mathbb{Q}^a$, where $\mathfrak{f}_N$ is the field of modular functions of level $N$ rational over $\mathbb{Q}(e^{2\pi i/N})$ in the sense of §6.2, pp.137 [14], i.e. $\mathfrak{f}_N = \mathbb{Q}(f_a \mid a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2)$ with $f_a$ Fricke functions (cf. Example 4.1.5). (Recall that the field of all modular functions of finite level is equal to $\mathbb{C} \otimes \mathfrak{f}$; cf. Proposition 6.1, [14].)

**Definition 4.1.2** (Witt deformation family of modular functions). A Witt deformation family of modular functions (or simply, a Witt deformation of modular functions) is a continuous function $^2f : M_2(\hat{\mathbb{Z}}) \times \mathfrak{f} \to \mathbb{C}$ satisfying the following axioms:

1. for each $m \in M_2(\hat{\mathbb{Z}})$, the fiber $f_m := f(m, -) : \mathfrak{f} \to \mathbb{C}$ is a modular function in $\mathfrak{f}$;

2. for each $m \in M_2(\hat{\mathbb{Z}})$ and $u \in GL_2(\hat{\mathbb{Z}})$, we have:

$$f_{mu} = f_m^u;$$

where $f_m \mapsto f_m^u$ denotes the action of $u \in GL_2(\hat{\mathbb{Z}})$ onto the modular field $\mathfrak{f}$ (cf. §6.6 [14]);

3. the function $f : M_2(\hat{\mathbb{Z}}) \times \mathfrak{f} \to \mathbb{C}$ factors through the projection $p_N : M_2(\mathbb{Z}) \to M_2(\mathbb{Z}/N\mathbb{Z})$ for some $N$ as follows:

$$M_2(\hat{\mathbb{Z}}) \times \mathfrak{f} \xrightarrow{f} \mathbb{C} \quad \text{ (4.3)}$$

\[\text{p}_N \times \text{id}_N\]

$M_2(\mathbb{Z}/N\mathbb{Z}) \times \mathfrak{f}$

---

2To be more precise, $f : M_2(\hat{\mathbb{Z}}) \times \mathfrak{f} \to \mathbb{C}$ is actually a partial function or a function to $\mathbb{C} \cup \infty$ in general; but in this paper we shall denote $f$ as a function to $\mathbb{C}$ just for simplicity.
Remark 4.1.3. In relation to the Bost-Connes system \[10\], the concept of Witt deformation is based on a slight modification of the arithmetic subalgebra constructed in Definition 2.22 \[10\]. Modulo this modification, our modularity theorem in \([5,2]\) can be seen (almost) as the claim that the arithmetic subalgebra given loc. cit. (or its commutative subalgebra) coincides with that constructed in \([10]\). For this proof to work well, however, we needed to modify the constructions in \([10, 9]\); hence our construction is slightly different from there. Despite of this modification, it would be meaningful to have in mind the relationship between our result and the works on Bost-Connes systems \([10, 12, 19]\) particularly when we try to extend the results developed in this paper to number fields of higher degree; in particular the results of \([12, 19]\) and ours in \([3]\) hold for arbitrary number fields.

Example 4.1.4 (j-function). The j-function \(j\) naturally defines the simplest Witt deformation family of modular functions, denoted by the same symbol \(j: M_2(\hat{\mathbb{Z}}) \times \mathfrak{H} \to \mathbb{C}\): for each \((m, \tau) \in M_2(\hat{\mathbb{Z}}) \times \mathfrak{H}\),

\[ j(m, \tau) := j(\tau).\]  

(4.4)

The fact that this \(j: M_2(\hat{\mathbb{Z}}) \times \mathfrak{H} \to \mathbb{C}\) indeed defines a Witt deformation follows readily from the definition of the action of \(GL_2(\mathbb{A}_{Q,f}) = GL_2(\hat{\mathbb{Z}})GL_2^+ (\mathbb{Q})\) on \(j\), in particular, \(j^u = j\) for \(u \in GL_2(\hat{\mathbb{Z}})\) (cf. §6.6, \[13\]).

Example 4.1.5 (Fricke functions). The Fricke functions are modular functions \(f_a : \mathfrak{H} \to \mathbb{C}\) indexed by row vectors \(a \in \mathbb{Q}^2/\mathbb{Z}^2 \setminus \{0\}\), and defined as follows (cf. pp.133 \[13\]): for \(w_1, w_2\) with \(w_1/w_2 \in \mathfrak{H}\),

\[ f_a(w_1/w_2) = \frac{g_2(w_1, w_2)g_3(w_1, w_2)}{\Delta(w_1, w_2)} p(a_1 w_1 + a_2 w_2; w_1, w_2).\]  

(4.5)

Each Fricke function \(f_a\) naturally defines a Witt deformation family \(\chi_a\) of modular functions by:

\[ \chi_a : M_2(\hat{\mathbb{Z}}) \times \mathfrak{H} \to \mathbb{C} \]  

\[ (m, \tau) \mapsto f_{am}(\tau) \]  

(4.6)

(4.7)

(In some sense this \(\chi_a\) “deforms” the Fricke functions \(f_a\) by the action of \(m \in M_2(\hat{\mathbb{Z}})\) on the index \(a \in \mathbb{Q}^2/\mathbb{Z}^2\) ) The fact that this \(\chi_a : M_2(\hat{\mathbb{Z}}) \times \mathfrak{H} \to \mathbb{C}\) indeed defines a Witt deformation of modular functions can be proved, again, using the definition of the action of \(GL_2(\mathbb{A}_{Q,f}) = GL_2(\hat{\mathbb{Z}})GL_2^+ (\mathbb{Q})\) on \(f_a\)’s: That is, for \(ua \in GL_2(\hat{\mathbb{Z}})GL_2^+ (\mathbb{Q}) = GL_2(\mathbb{A}_{Q,f})\), one has \(f_{ua}^{(u)} = f_{aa} \circ \alpha\) (cf. §6.6, \[13\]).

We demonstrate in Theorem \([4.3.1]\) that these functions (Example \([4.1.4, 4.1.5]\) are typical and provide enough generators of modular vectors (cf. Definition \([4.1.7]\) ), but we have yet another class of examples as follows, which is useful in our constructions (in Lemma \([4.2.4, 4.2.5]\) ) of modular vectors:

Example 4.1.6 (characteristic functions). Let \(N \geq 1\) be a positive integer and \(S \subseteq M_2(\mathbb{Z}/N\mathbb{Z})\) be a subset that is closed under the right action of \(GL_2(\mathbb{Z}/N\mathbb{Z}).\) Denoting by \(\chi_S : M_2(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{C}\) the characteristic function of \(S\), let us define the function \(f^{(S)} : M_2(\hat{\mathbb{Z}}) \times \mathfrak{H} \to \mathbb{C}\) as the composition:

\[ f^{(S)} : M_2(\hat{\mathbb{Z}}) \times \mathfrak{H} \xrightarrow{\pi_1} M_2(\mathbb{Z}) \to M_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\chi_S} \mathbb{C} \]  

(4.8)

where \(\pi_1\) denotes the projection onto the first component. Then this \(f^{(S)}\) gives a Witt deformation, whose fiber \(f_m : \mathfrak{H} \to \mathbb{C}\) at each \(m \in M_2(\hat{\mathbb{Z}})\) is either 0 or 1, the constant functions.
Definition 4.1.7 (modular vector). Let \( f : M_2(\mathbb{Z}) \times S \to \mathbb{C} \) be a Witt deformation of modular functions such that the fiber \( f_m : S \to \mathbb{C} \) of each \( m \in M_2(\mathbb{Z}) \) is defined as a finite value at \( \tau_K \in \mathfrak{H} \) with \( O_K = \mathbb{Z}\tau_K + \mathbb{Z} \). Then the modular vector \( \hat{f} \in \mathcal{C}^{IK} \) associated to \( f \) (at \( K \)) is the function \( \hat{f} : I_K \to \mathbb{C} \) defined by the following composition:

\[
\hat{f} : I_K \hookrightarrow DR_K \cong \hat{O}_K \times \hat{\varphi}_K (\mathfrak{a}_{K,f}/K^*) \cong \text{Lat}_{1,K}^I \hookrightarrow \text{Lat}_Q^2 \cong \Gamma \backslash (M_2(\mathbb{Z}) \times S) \xrightarrow{\hat{f}} \mathbb{C}. \tag{4.9}
\]

Note that \( f \) induces a function on \( \Gamma \backslash (M_2(\mathbb{Z}) \times S) \) thanks to the second condition of Witt deformation, and \( \hat{f} \) in fact takes its values in \( K^{ab} \), which follows from Lemma 4.1.9 below. Modular vectors in this sense themselves constitute a \( \mathbb{Q} \)-algebra; to make it a \( K \)-algebra, we define the \( K \)-algebra \( M_K \) of modular vectors as follows (and abusively, we shall call the elements of \( M_K \) as well modular vectors):

\[
M_K := K \otimes \mathbb{Q} \{ \hat{f} \in (K^{ab})^{IK} | f : M_2(\mathbb{Z}) \times S \to \mathbb{C} \text{ is a Witt deformation.} \}. \tag{4.10}
\]

Remark 4.1.8. Instead, we may allow the fibers \( f_m \) of Witt deformations \( f : M_2(\mathbb{Z}) \times S \to \mathbb{C} \) to be modular functions in \( K \otimes \mathbb{Q} \mathfrak{H} \); then the modular vectors \( \hat{f} \) constitute a \( K \)-algebra in themselves, which is equal to \( (1.10) \). We may use the term “Witt deformations” in this extended sense too.

Concerning modular vectors, we first see more explicitly the coefficients \( \hat{f}_a \) of modular vectors \( \hat{f} = (f_a) \) in terms of the values of the Witt deformation \( f : M_2(\mathbb{Z}) \times S \to \mathbb{C} \) of modular functions:

Lemma 4.1.9. Let \( f : M_2(\mathbb{Z}) \times S \to \mathbb{C} \) be a Witt deformation of modular functions. Then, for each \( a \in I_K \), the component \( \hat{f}_a \in \mathbb{C} \) at \( a \) of the associated modular vector \( \hat{f} = (f_a) \in \mathcal{C}^{IK} \) is in fact in \( K^{ab} \) and given by the following equation:

\[
\hat{f}_a = f(m_a, \tau_{a^{-1}}); \tag{4.11}
\]

where, on one hand, if we denote as \( a^{-1} = Zw_1 + Zw_2 \) with \( w_1, w_2 \in S \), we define \( \tau_{a^{-1}} := w_1/w_2 \); on the other hand, \( m_a \in M_2(\mathbb{Z}) \) is such that the following diagram commutes with some \( \alpha \in GL_2^+ (\mathbb{R}) \) (i.e. such that \( \mathbb{Z}^2 \cdot \alpha \cdot (i, 1)^t = a^{-1} \); cf. (4.12):

\[
\begin{array}{ccc}
\mathbb{Q}^2/\mathbb{Z}^2 & \xrightarrow{m_a} & \mathbb{Q}^2/\mathbb{Z}^2 \\
\downarrow q & & \downarrow q \alpha \cdot (i, 1)^t & = \\
K/O_K & \xrightarrow{=} & K a^{-1}/a^{-1} \\
\end{array}
\tag{4.12}
\]

where \( K/O_K \to Ka^{-1}/a^{-1} \) is a natural inclusion.

Proof. The proof is just based on a careful chase of the composition (4.11). Firstly, the composition \( I_K \hookrightarrow DR_K \cong \hat{O}_K \times \hat{\varphi}_K (\mathfrak{a}_{K,f}/K^*) \) sends the ideal \( a \in I_K \) (denoting \( a = \rho \hat{O}_K \cap K \) for some \( \rho \in \hat{O}_K \)) to \( [\rho, \rho^{-1}] \in \hat{O}_K \times \hat{\varphi}_K (\mathfrak{a}_{K,f}/K^*) \) (cf. Proposition 4.2 and Proposition 8.2, [19]); secondly, one sees that the further composition with the maps \( \hat{O}_K \times \hat{\varphi}_K (\mathfrak{a}_{K,f}/K^*) \to \text{Lat}_K^1 \to \text{Lat}_Q^2 \) sends \( [\rho, \rho^{-1}] \) to \( [a^{-1}, \phi_a] \in \text{Lat}_Q^2 \), where \( \phi_a : \mathbb{Q}^2/\mathbb{Z}^2 \to \mathbb{Q}

\]

\[
\begin{array}{ccc}
\phi_a : \mathbb{Q}^2/\mathbb{Z}^2 & \xrightarrow{q} & K/O_K \xrightarrow{=} K a^{-1}/a^{-1} \\
\end{array}
\tag{4.13}
\]
where the second arrow $K/O_K \to Ka^{-1}/a^{-1}$ is a natural inclusion. Therefore, by the construction of the isomorphism $\text{Lat}_Q \simeq \Gamma\langle M_2(\mathbb{Z}) \times \mathfrak{f} \rangle$ (cf. §22), this $[a^{-1}, \phi_a] \in \text{Lat}_Q^2$ indeed corresponds to $[m_a, \tau_a^{-1}] \in \Gamma \backslash (M_2(\mathbb{Z}) \times \mathfrak{f})$ for the $m_a \in M_2(\mathbb{Z})$ and $\tau_a^{-1} \in \mathfrak{f}$ described above. This completes the proof.

**Example 4.1.10** (the modular vector for $j$). Let $j : M_2(\mathbb{Z}) \times \mathfrak{f} \to \mathbb{C}$ be the Witt deformation of modular functions given in Example 4.1.4. Then Lemma 4.1.9 shows that the associated modular vector $\hat{j}$ is given by $\hat{j}_a = j(a^{-1})$. Therefore, this $\hat{j}$ is equal to $\iota$ constructed in Proposition 4.1.1 and as observed there, this vector $\hat{j} = \iota$ is a member of $\mathbb{W}^a_\hat{\iota}(O_K)$, hence, of the $K$-algebra $E_K$ in particular. This example shows that some modular vector (i.e. $\hat{j} \in M_K$) indeed defines an algebraic Witt vector (i.e. $\hat{j} = \iota \in E_K$).

The goal of the next subsection is to show that this example is a special case of a more general relationship between modular vectors and algebraic Witt vectors: we prove that these two concepts actually coincide.

### 4.2 The modularity theorem

This section proves that the $K$-algebra $M_K$ of modular vectors coincides with the $K$-algebra $E_K$ of algebraic Witt vectors, which we call the modularity theorem. In other words, this theorem claims that every modular vector $\hat{f}$ defines an algebraic Witt vector, i.e. $\hat{f} \in E_K$, and conversely, every algebraic Witt vector $\xi \in E_K$ is realized as a modular vector, i.e. $\xi = \hat{f}$ for some Witt deformation $\hat{f} : M_2(\mathbb{Z}) \times \mathfrak{f} \to \mathbb{C}$ of modular functions. To be precise:

**Theorem 4.2.1** (modularity theorem). *We have the following identity as $K$-subalgebras of $(K^{ab})^{I_K}$:*

$$E_K = M_K.$$  \hspace{1cm} (4.14)

Our proof of this theorem consists of two steps. We first prove the inclusion $M_K \subseteq E_K$, which is based on Corollary 3.1.6 and Shimura’s reciprocity law. After that, we prove the converse inclusion $E_K \subseteq M_K$, which is based on the characterization of $E_K$ by simple conditions due to Neshveyev, Theorem 10.1, §10 [19].

To be specific, recall that Corollary 3.1.6 proved that the $K$-algebra $E_K$ is identified with that of locally constant $K^{ab}$-valued $G_K^{ab}$-equivariant functions on $DR_K$, i.e. $E_K = \text{Hom}_{G_K^{ab}}(DR_K, K^{ab})$; in the proof of the inclusion $M_K \subseteq E_K$, we see that every modular vector $\hat{f}$ defines a locally constant ($K^{ab}$-valued) $G_K^{ab}$-equivariant function on $DR_K$, by which we deduce the inclusion $M_K \subseteq E_K$. On the other hand, the $K$-algebra $E_K$ was characterized by Neshveyev, §10 [19] as the $K$-subalgebra $E$ of $C(D\hat{R}_K)$— the $\mathbb{C}$-algebra of continuous functions on $D\hat{R}_K$— that satisfies the following conditions (cf. pp.408, [19]; note that $D\hat{R}_K$ is homeomorphic to $Y_K$ in [19]):

1. every function in $E$ is locally constant on $D\hat{R}_K$;
2. $E$ separates the points of $D\hat{R}_K$;
3. $E$ contains the idempotents $\rho^a$ for each $a \in I_K$ (cf. Lemma 4.2.4);
4. every function in $E$ is $K^{ab}$-valued and $G_K^{ab}$-equivariant.
In other words, if $E$ is a $K$-subalgebra of $E_K$ and satisfies the second and the third conditions here, one actually has the identity $E = E_K$. Therefore, after the proof of the inclusion $M_K \subseteq E_K$, the remained task for the proof of the identity $E_K = M_K$ is only to prove that $M_K$ satisfies the second and the third conditions here. Our proof of the target identity $E_K = M_K$ will follow this line of argument.

Now let us start proving the inclusion $M_K \subseteq E_K$. To this end, we prepare the following lemma, which is used to prove that modular vectors $\tilde{f}$ define $K^{ab}$-valued $G_K^{ab}$-equivariant functions on $\mathcal{D}R_2$.

In what follows, recall that every fractional ideal $\Lambda$ of $K$ can be given as $\Lambda = t\mathcal{O}_K \cap K$ for some $t \in \mathcal{A}_{K,f}$; then, for such $\Lambda$ and each $s \in \mathcal{A}_{K,f}$, let us denote $s^{-1}\Lambda := s^{-1}t\mathcal{O}_K \cap K$.

**Lemma 4.2.2.** Let $(\Lambda, \phi) \in \mathcal{L}at_f^1$ be a $K$-lattice such that $\Lambda$ is a fractional ideal of $K$ and corresponds to $[m, \tau] \in \Gamma \backslash (M_2(\mathbb{Z}) \times \mathfrak{f})$; also let $s \in \mathcal{A}_{K,f}^* / K^*$ and $(s^{-1}\Lambda, s^{-1}\phi) \in \mathcal{L}at_1^1$ corresponds to $[m, \tau]$. Moreover, let $f : M_2(\mathbb{Z}) \times \mathfrak{f} \to \mathbb{C}$ be a Witt deformation of modular functions. Then $f_m(\tau) \in K^{ab}$, and the following identity holds:

$$ (f_m(\tau))^s = f_{m_s}(\tau_s). $$

(4.15)

**Proof.** Throughout this proof, let us denote $\Lambda_s := s^{-1}\Lambda$ and $\phi_s := s^{-1}\phi$ for short. Moreover let $\Lambda = Zw_1 + Zw_2 = Z^2 \cdot \phi \cdot (i, 1)^t$ and $\Lambda_s = Zw_1 + Zw_2 = Z^2 \cdot \phi \cdot (i, 1)^t$ with $\tau = w_1 / w_2$, $\tau_s = w_1 / w_2 \in \mathfrak{f}$ and $\alpha, \alpha_s \in GL_2^+ (\mathbb{R})$; also let $\beta \in GL_2^+ (\mathbb{Q})$ be such that $(w_1, w_2) = \beta (w_1, w_2)^t$, whence $\alpha_s = \beta^{-1} \alpha$ and $\tau = \alpha(1), \tau_s = \alpha_s(1)$. Define the embedding $q_\Lambda : \mathcal{A}_{K,f} \to M_2(\mathbb{R}_Q)$ with respect to the basis of $\Lambda$ in the sense of §4.4 [11] that $q_\Lambda (\mu) (w_1, w_2)^t = (\mu w_1, \mu w_2)^t$ for $\mu \in K$. Then, for each prime $p$, we have:

$$ Z_p^2 \left( \begin{array}{c} w'_1 \\ w'_2 \end{array} \right) = (\Lambda_s)_p $$

(4.16)

$$ = \Lambda_p s^{-1}_p $$

(4.17)

$$ = Z_p^2 \left( \begin{array}{c} w_1 s^{-1}_p \\ w_2 s^{-1}_p \end{array} \right) $$

(4.18)

$$ = Z_p^2 q_\Lambda (s_p)^{-1} \left( \begin{array}{c} w_1 \\ w_2 \end{array} \right) $$

(4.19)

$$ = Z_p^2 q_\Lambda (s_p)^{-1} \beta \left( \begin{array}{c} w'_1 \\ w'_2 \end{array} \right). $$

(4.20)

Since this holds for each prime $p$, we have some $u \in GL_2 (\mathbb{Z})$ such that $q_\Lambda (s)^{-1} \beta = u$; therefore, $q_\Lambda (s)^{-1} = u \beta^{-1}$. With this in mind, we first compute $(f_m(\tau))^s$. By Shimura’s reciprocity law and $q_\Lambda (s) = u \beta^{-1}$, we have:

$$ (f_m(\tau))^s = f_m (q_\Lambda (s)^{-1} (\tau)) $$

(4.21)

$$ = f_{m_s} \circ \beta^{-1} (\tau). $$

(4.22)

To prove that the last one is equal to $f_{m_s}(\tau_s)$, consider the following composition:

$$ \mathbb{Q}^2 / \mathbb{Z}^2 \xrightarrow{m} \mathbb{Q}^2 / \mathbb{Z}^2 \mathcal{O}(i, 1)^t \xrightarrow{q_\Lambda / \Lambda} \mathbb{Q} \Lambda / \Lambda \xrightarrow{s^{-1}} \mathbb{Q} \Lambda_s / \Lambda_s. $$

(4.23)
here the last arrow is defined by the following; suppose $\Lambda = t\hat{O}_K \cap K$ for $t \in \mathbb{A}_{K,f}$. Then:

\[ \frac{Q\Lambda}{\Lambda} \xrightarrow{s^{-1}} \frac{Q\Lambda_s}{\Lambda_s} \]

\[ \xrightarrow{=} \]

\[ \frac{K\Lambda}{\Lambda} \xrightarrow{=} \frac{K\Lambda_s}{\Lambda_s} \]

\[ \xrightarrow{\sim} \]

\[ \frac{\mathbb{A}_{K,f}/t\hat{O}_K}{s^{-1}} \xrightarrow{s^{-1}} \frac{\mathbb{A}_{K,f}/s^{-1}t\hat{O}_K}{s^{-1}} \]

Recall that $q_\Lambda(s)$ is defined with respect to the basis of $\Lambda = \mathbb{Z}^2 \cdot \alpha \cdot (i, 1)^t$. Therefore, we have the following commutative diagram: (recall also that $\Lambda_s = \mathbb{Z}^2 \cdot \alpha_s \cdot (i, 1)^t$ with $\alpha_s = \beta^{-1}\alpha$; and we write just by $\alpha : \mathbb{Q}^2/\mathbb{Z}^2 \to \mathbb{Q}\Lambda/\Lambda$ to mean the composition $\alpha \cdot (i, 1)^t \cdot \mathbb{Q}^2/\mathbb{Z}^2 \to \mathbb{Q}\alpha/\mathbb{Z}^2 \alpha \to \mathbb{Q}\Lambda/\Lambda$.)

\[ \frac{Q\Lambda/\Lambda}{\alpha^{-1}} \xrightarrow{s^{-1}} \frac{Q\Lambda_s/\Lambda_s}{\alpha} \]

\[ \xrightarrow{\sim} \]

\[ \frac{\mathbb{Q}^2/\mathbb{Z}^2}{q_\Lambda(s)^{-1}} \xrightarrow{\mathbb{Q}^2/\mathbb{Z}^2/\beta^{-1}} \]

This diagram shows that the composition (4.23) is equal to the following:

\[ \mathbb{Q}^2/\mathbb{Z}^2 \xrightarrow{m} \mathbb{Q}^2/\mathbb{Z}^2 \xrightarrow{q_\Lambda(s)^{-1}} \mathbb{Q}^2/\mathbb{Z}^2/\beta^{-1} \xrightarrow{\alpha} \mathbb{Q}\Lambda/\Lambda. \]

Therefore, $m_s\alpha_s = mq_\Lambda(s)^{-1}\alpha = mu\beta^{-1}\alpha$; and hence we have: (note that $\tau = \alpha(i)$ and $\tau_s = \alpha_s(i)$ by definition above.)

\[ f_{mu} \circ \beta^{-1}(\tau) = f_{mu} \circ \beta^{-1}\alpha(i) \]

\[ = f_{mu}(\alpha_s(i)) \]

\[ = f_{mu}(\tau_s). \]

\[ f_{mu} \circ \beta^{-1}(\tau) = f_{mu}(\tau_s). \]

Consequently, we proved that $(f_m(\tau))^{\bullet} = f_m(\tau_s)$ as requested. This completes the proof.

With this lemma, we first prove the one-side inclusion for the target equality $E_K = M_K$:

**Lemma 4.2.3.** We have the following inclusion:

\[ M_K \subseteq E_K. \]

**Proof.** Let $f : M_2(\hat{\mathbb{Z}}) \times \mathfrak{H} \to \mathbb{C}$ be a Witt deformation of modular functions with $\hat{f} \in M_K$ being the associated modular vector. Firstly we see that the associated function $\hat{f} : DR_K \to \mathbb{C}$ is locally constant. (Here recall that $\hat{f} : I_K \to K^{ab} \in M_K$ is defined as a restriction of a (continuous) function $\hat{f} : DR_K \to \mathbb{C}$ onto the dense subset $I_K \subseteq DR_K$; cf. Definition [1.1.7].) Since $f : M_2(\hat{\mathbb{Z}}) \times \mathfrak{H} \to \mathbb{C}$ by definition factors through some projection $p_N : M_2(\hat{\mathbb{Z}}) \to M_2(\mathbb{Z}/\mathbb{N}\mathbb{Z})$, this function $\hat{f} : DR_K \to \mathbb{C}$ also factors through the projection $DR_K \to DR_{NO_K}$; this readily follows from the isomorphism
\( DR_{NO_K} \cong (O_K/NO_K) \times (O_K/NO_K)^*, C_{NO_K} \), cf. Proposition 7.2 [19]. Hence, \( \hat{f} : DR_K \to \mathbb{C} \) is indeed locally constant on \( DR_K \).

Secondly, to see that \( \hat{f} : DR_K \to \mathbb{C} \) is \( G_{K}^{ab} \)-equivariant, we remark that the action of \([s] \in G_{K}^{ab}\) for \( s \in \mathbb{A}_{K.f}^* \) on the element of \( DR_K \) that corresponds to \( [\rho, t] \in \hat{O}_K \times \hat{O}_K \) under the homeomorphism \( \psi : DR_K \to \hat{O}_K \times \hat{O}_K \) \( (\mathbb{A}_{K,f}^*/K^*) \) corresponds to \( [\rho, s^{-1}t] \) (i.e. not \( [\rho, st] \)); that is, we have \( (\psi^{-1}(\rho, t))[s] = \psi^{-1}(\rho, s^{-1}t) \); this follows from the construction of the homeomorphism \( \hat{\Psi} : \hat{O}_K \times \hat{O}_K \) \( G_{K}^{ab} \to DR_K \) of §8.1 [19]. Thus, if \( \psi^{-1}(\rho, t) \in DR_K \) corresponds to \([m, \tau] \in \Gamma \backslash (\mathbb{M}_2(\hat{\mathbb{Z}}) \times \hat{\mathbb{Z}}) \) under the correspondence \( DR_K \to \Gamma \backslash (\mathbb{M}_2(\hat{\mathbb{Z}}) \times \hat{\mathbb{Z}}) \) (cf. (4.9)), then \( (\psi^{-1}(\rho, t))[s] = \psi^{-1}(\rho, s^{-1}t) \in DR_K \) corresponds to \([m_s, \tau_s] \) (in the sense of the notation in Lemma 4.2.2). Therefore, we have:

\[
\hat{f}((\psi^{-1}(\rho, t))[s]) \quad (4.31)
\]

\[
\hat{f}(\psi^{-1}(\rho, s^{-1}t)) \quad (4.32)
\]

\[
(f_m(\tau))[s] \quad (4.33)
\]

\[
(\hat{f}(\psi^{-1}(\rho, t))[s]) \quad (4.34)
\]

In the third equality, we used Lemma 4.2.2, this shows that \( \hat{f} : DR_K \to \mathbb{C} \) is indeed \( G_{K}^{ab} \)-equivariant. Therefore \( \hat{f} \) is \( K^{ab} \)-valued locally constant \( G_{K}^{ab} \)-equivariant function on \( DR_K \), hence \( \hat{f} \in E_K \). This completes the proof.

Now we have the inclusion \( M_K \subseteq E_K \). Thus, in order to prove our target identity \( E_K = M_K \), it suffices to prove that \( M_K \) satisfies the above-mentioned two conditions (2) and (3). In the following we first prove the third condition (3), and then prove the second (2), which will complete the proof of our target theorem.

**Lemma 4.2.4.** For each \( a \in I_K \), let us define \( \rho^a \in (K^{ab})^{I_K} \) as follows:

\[
\rho^a(b) := \begin{cases} 
1 & \text{if } a | b \\
0 & \text{otherwise}
\end{cases} \quad (4.35)
\]

Then \( \rho^a \in M_K \) for every \( a \in I_K \).

**Proof.** This function \( \rho^a \) corresponds to the characteristic function of \( aDR_K \), which we now show belongs to \( M_K \). Let us fix \( s_a \in \hat{O}_K \) such that \( a = s_a \hat{O}_K \cap K \). Under the homeomorphism \( DR_K \cong \hat{O}_K \times \hat{O}_K \) \( (\mathbb{A}_{K,f}^*/K^*) \) of [19], the subspace \( aDR_K \subseteq DR_K \) corresponds to \( a\hat{O}_K \times \hat{O}_K \) \( (\mathbb{A}_{K,f}^*/K^*) \); and note that, under the further composition \( \hat{O}_K \times \hat{O}_K \) \( (\mathbb{A}_{K,f}^*/K^*) \to \text{Lat}_1^{\hat{\mathbb{K}}_2} \to \text{Lat}_2^{\hat{\mathbb{K}}_2} \to \Gamma \backslash (\mathbb{M}_2(\hat{\mathbb{Z}}) \times \hat{\mathbb{Z}}) \), this subspace is eventually mapped into \( \Gamma \backslash (q_\tau(s_a)\mathbb{M}_2(\hat{\mathbb{Z}}) \times \hat{\mathbb{Z}}) \), where \( q_\tau : \mathbb{A}_{K,f}^* \to \mathbb{M}_2(\hat{\mathbb{K}}_2) \) denotes the embedding determined by \( O_K = \mathbb{Z}\tau + \mathbb{Z} \). Let us define the function \( f^a : \mathbb{M}_2(\hat{\mathbb{Z}}) \times \hat{\mathbb{Z}} \to \mathbb{C} \) as the characteristic function of the subspace \( q_\tau(s_a)\mathbb{M}_2(\hat{\mathbb{Z}}) \times \hat{\mathbb{Z}} \subseteq \mathbb{M}_2(\hat{\mathbb{Z}}) \times \hat{\mathbb{Z}} \). It is clear that \( f^a \) satisfies the conditions (1), (2) of Witt deformations of modular functions. In order to see that \( f^a \) also satisfies the condition (3), we note that \( f^a \) factors through \( p_{N(a)} : \mathbb{M}_2(\hat{\mathbb{Z}}) \to \mathbb{M}_2(\mathbb{Z}/N(a)\mathbb{Z}) \), where \( N(a) \) is the absolute norm of \( a \). In fact, this follows from the fact that the kernel of \( p_{N(a)} \) is \( N(a)\mathbb{M}_2(\hat{\mathbb{Z}}) \), which is included in \( q_\tau(s_a)\mathbb{M}_2(\hat{\mathbb{Z}}) \). From these facts, we find that \( f^a \) is in fact a Witt deformation of modular functions; and by construction, it is clear that \( f^a = \rho^a \). This implies that \( \rho^a \in M_K \) as requested. This completes the proof. \( \square \)
Lemma 4.2.5. The functions in $M_K$ are enough to separate the points of $DR_K$. 

Proof. Let $x \neq y \in DR_K$ be distinct points. Since $DR_K$ is the inverse limit of $DR_f$’s for $f \in I_K$, there exists $\bar{f} \in I_K$ such that $x$ and $y$ still represent distinct elements of $DR_{\bar{f}}$ under the projection $DR_K \to DR_{\bar{f}}$; also since the ideals $NO_K$ for positive integers $N$ are cofinal in $I_K$, we may suppose $f = NO_K$. In this proof let us denote by $\bar{x}, \bar{y} \in DR_f$ those in $DR_{\bar{f}}$ represented by $x, y \in DR_K$ under the projection $DR_K \to DR_f$. Here recall the decomposition $DR_f = \bigsqcup_{\rho \mid f} C_{\rho,f}$ (see (4.4) in pp. 394 [19]). If $x$ and $y$ belong to distinct components, then the characteristic functions defined above are enough to separate $x, y$.

So we suppose that $\bar{x}, \bar{y}$ belong to the same component $C_{\rho,f}$ for some $\rho \mid f$ but represent distinct elements. This implies that there exist $[\rho, s], [\rho, t] \in \hat{O}_K \times \hat{O}_K (\bar{K}_K, f) \subset DR_{\bar{f}}$; also, by $\bar{x} \neq \bar{y} \in C_{\rho,f} \subset DR_f$, the actions of $[\rho, s], [\rho, t] \in Gal(K^{ab}/K)$ are not identical on $C_{\rho,f}$. Thus by the corollary in §3, Chapter 10 [13], we can find $a \in (N^{-1}Z^2/Z^2) : q_{\tau_K}(\rho) \simeq N^{-1}d/O_K$ so that $(f_a(\tau_K))^{[s]} \neq (f_a(\tau_K))^{[t]}$. (To be precise, when $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}((\sqrt{-3}))$, we replace $f_a$’s in Example [4.3.5] with the functions $f'_a$’s or $f''_a$’s given in §6.1 [14].) With these data, let us now define a function $f : M_2(\hat{Z}) \times \mathcal{S} \to \mathbb{C}$ as follows: (Here $q_{\tau_K} : K_{K,f} \to M_2(\mathbb{A}_{K,f}^1)$ denotes the embedding determined by $O_K = \mathbb{Z}_{\tau K} + \mathbb{Z}$.)

$$f(m, \tau) := \begin{cases} 0 & \text{if } m \not\in q_{\tau_K}(\rho)M_2(\hat{Z}) \subset M_2(\hat{Z}) \\ f_{am'}(\tau) & \text{if } m = q_{\tau_K}(\rho)m' \text{ for } \exists! m' \in M_2(\hat{Z}) \end{cases} \quad (4.36)$$

By the same argument as above and $a \in (N^{-1}Z^2/Z^2) : q_{\tau_K}(\rho)$, we see that this function $f$ factors through the quotient $M_2(\hat{Z}) \to M_2(\mathbb{Z}/NZ)$; and $f$ defines a Witt deformation of modular functions. We now show that the modular vector $\hat{f}$ associated to this $f$ separates $x$ and $y$. Note that, since $f$ factors through $M_2(\hat{Z}) \to M_2(\mathbb{Z}/NZ)$, the function $\hat{f} : DR_K \to \mathbb{C}$ also factors through $DR_K \to DR_f = DR_{NO_K}$. (Again recall that we have $DR_{NO_K} \simeq (O_K/NO_K) \times (O_K/NO_K)$, $C_{NO_K}$; cf. Proposition 7.2 [19].) Then, by construction and the $G_K^{ab}$-equivariance (cf. Lemma 4.2.3) of this function $\hat{f} : DR_K \simeq \hat{O}_K \times \hat{O}_K (\bar{K}_K, f) \to \mathbb{C}$, we have:

$$\hat{f}(x) = \hat{f}(\rho, s) = (\hat{f}(\rho, 1))^{[s]} = (f_a(\tau_K))^{[s]} \neq (f_a(\tau_K))^{[t]} = (\hat{f}(\rho, 1))^{[t]} = \hat{f}(\rho, t) = \hat{f}(y). \quad (4.37)$$

This completes the proof.

Corollary 4.2.6. We have the following inclusion:

$$E_K \subseteq M_K; \quad (4.38)$$

hence $E_K = M_K$.

Proof. In the above developments, we have proved that $M_K$ is a $K$-subalgebra of $E_K$, separates the points of $DR_K$, and contains the idempotents $\rho^a$ for $a \in I_K$. Therefore, by Theorem 10.1 [19], we conclude the target identity $E_K = M_K$. \qed
4.3 Explicit generators

To further clarify the description of $E_K$ as $M_K$ (Theorem 4.2.1), we conclude this paper by giving a set of explicit generators of $M_K = E_K$. To be more specific we demonstrate that the galois objects $X_{\mathfrak{E}(N)}$ generated by the modular vectors $\mathfrak{E}(N) := \{ \hat{\chi}_a \in M_K \mid a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2 \}$ $(N \geq 1)$ are cofinal among the galois objects of $\mathfrak{E}_K$; in particular, as we discuss below, this implies that $E_K = M_K$ is generated by the modular vectors $\hat{\chi}_a$ coming from the Fricke functions $f_a$. (For $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$, we replace $f_a$'s with $f_{\alpha}^2$'s and $f_{\beta}^3$'s in §6.1 [14].)

Throughout this subsection, we abusively denote for brevity as $f_a = \chi_a : M_2(\hat{\mathbb{Z}}) \times \mathfrak{S} \ni (m, \tau) \mapsto f_a m(\tau) \in \mathbb{C}$, thus $\hat{f}_a = \hat{\chi}_a$; again recall that we put $f_0 := j$. To prove the following theorem is our major goal in this subsection:

**Theorem 4.3.1** (Fricke functions are enough to generate $E_K$). The $K$-algebra $E_K$ is generated as a $K$-algebra by the modular vectors $f_a$ for $a \in \mathbb{Q}^2/\mathbb{Z}^2$. That is:

$$E_K = K[\hat{f}_a \mid a \in \mathbb{Q}^2/\mathbb{Z}^2].$$  \hfill (4.39)

The proof of this theorem is based on three lemmas: With the first two lemmas (Lemma 4.3.2, Lemma 4.3.3) we see that, for every positive integer $N$, the monoid congruence $a \sim_{NO_K} b$ on $I_K$ (cf. (2.3)) coincides with the monoid congruence $a =_{\mathfrak{E}(N)} b$ (cf. §3.1), which implies that the galois objects $X_{\mathfrak{E}(N)}$ are cofinal in all the galois objects in $\mathfrak{E}_K$; the last lemma (Lemma 4.3.5) then proves that $X_{\mathfrak{E}(N)}$ is generated by $\mathfrak{E}(N)$ (less than the orbit $I_K \mathfrak{E}(N)$). Since $E_K$ is the direct limit (i.e. the union) of the galois objects of $\mathfrak{E}_K$, hence of $X_{\mathfrak{E}(N)}$'s, these three lemmas will conclude the target theorem.

We start with the following lemma:

**Lemma 4.3.2.** Let $N$ be a positive integer. Then, for any $a, b \in I_K$ (not necessarily prime to $N$), $a =_{\mathfrak{E}(N)} b$ implies the equality $(a, NO_K) = (b, NO_K)$ of greatest common divisors.

**Proof.** Assume $(a, NO_K) \neq (b, NO_K)$, from which we deduce $a \neq_{\mathfrak{E}(N)} b$. By this assumption we have $p \mid NO_K$ such that $v_p(a) \neq v_p(b)$, and without loss of generality, we may assume $v_p(a) < v_p(b)$ and $v_p(a) < v_p(NO_K)$. We need to prove that there exists $a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2$ such that $\psi_a \hat{f}_a \neq \psi_b \hat{f}_a$, whence $a \neq_{\mathfrak{E}(N)} b$; so, more specifically, we prove $\hat{f}_a (p^e a) \neq \hat{f}_a (p^f b)$ for some $a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2$, where $e := \max\{0, v_p(NO_K) - v_p(b)\} < v_p(NO_K) - v_p(a)$.

To prove $\hat{f}_a(p^e a) \neq \hat{f}_a(p^f b)$, $K$-algebra $K_{\mathfrak{E}(N)}$ for $a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2$, it suffices to find $a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2$ such that $\hat{f}_a(p^e a)$ and $\hat{f}_a(p^f b)$ generate different fields over $H_K$. To this end recall Corollary in §3, Chapter 10, [13], which shows that the ray class field $K_\ell$ over $K$ with conductor $\ell := NO_K/\ell \in I_K$ (for $\ell \mid NO_K$) can be given as:

$$K_{NO_K/\ell} = H_K(f_a(\tau_K) \mid a \in (N^{-1}\mathbb{Z}^2/\mathbb{Z}^2) \cdot q_{\tau_K}(\rho_\ell)),$$  \hfill (4.40)

where $\rho_\ell \in \hat{O}_K$ is taken so that $\ell = \rho_\ell \hat{O}_K$; moreover, we can choose a single $a_\ell := (N^{-1}\mathbb{Z}^2/\mathbb{Z}^2) \cdot q_{\tau_K}(\rho_\ell)$, where we put $\rho := \rho_\ell = \rho_{\ell(p^a, NO_K)}$.

Then we take $a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2$ so that $a \cdot q_{\tau_K}(\rho) = a'$, with which we prove that $H_K(\hat{f}_a(p^e a)) \neq H_K(\hat{f}_a(p^f b))$ by showing that $p$ is ramified in the former, while unramified in the latter. (This will complete the proof of this lemma.) To see this, let us take $[\rho, s], [\lambda, t] \in \hat{O}_K \times \hat{O}_K (\hat{K}_{\ell,f}/K^*)$ such
that the images of \([\rho, s], [\lambda, t]\) under the composition \(\widehat{\Theta}_K \times \widehat{\Theta}_K\) \((K^R_K/K^*) \simeq DR_K \to DR_{NO_K}\) are equal to \([p^a], [p^b] \in DR_{NO_K}\) respectively; here \(\rho\) is the same as taken in the above. In particular \((p^a, NO_K) = \rho\widehat{O}_K \cap K\) and \((p^b, NO_K) = \lambda\widehat{O}_K \cap K\). As discussed in Lemma 4.2.5 too, recall also that the function \(\widehat{f}_a : DR_K \to \mathbb{C}\) factors through \(DR_K \to DR_{NO_K}\) for \(a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2\). Then, with these data we have:

\[
\widehat{f}_a(p^a) = \widehat{f}_a(p^b) (4.41)
\]

\[
= (f_{aq_K}(\rho)(\tau_K))^{|s|^{-1}}; (4.42)
\]

Thus we have \(H_K(\widehat{f}_a(p^a)) = H_K(f_{aq_K}(\rho)(\tau_K))\) and \(H_K(\widehat{f}_a(p^b)) = H_K(f_{aq_K}(\lambda)(\tau_K))\). On one hand, by construction of \(a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2\), we have \(H_K(\widehat{f}_a(p^a)) = K_{NO_K}(p^a, NO_K)\); in particular, since \(\nu_p(NO_K (p^a, NO_K)) \neq 0\), we see that \(p\) ramifies in \(H_K(\widehat{f}_a(p^a)) = K_{NO_K}(p^a, NO_K)\). On the other hand, concerning \(H_K(\widehat{f}_a(p^b))\), we have \(\nu_p(NO_K(p^b, NO_K)) = 0\); also, since \(aq_K(\lambda) \in (N^{-1}\mathbb{Z}^2/\mathbb{Z}^2)\cdot q_K(\lambda)\), the field \(H_K(\widehat{f}_a(p^b))\) is a subfield of the ray class field \(K_{NO_K}(p^b, NO_K)\) over \(K\) whose conductor is not divisible by \(p\). Therefore, \(p\) is unramified in \(H_K(\widehat{f}_a(p^b))\) as requested. This completes the proof.

**Lemma 4.3.3 (modular description of the congruence \(\sim_{NO_K}\)).** Let \(N\) be a positive integer. Then \(a \sim_{NO_K} b\) if and only if \(a \equiv_{\Xi(N)} b\) for any \(a, b \in I_K\).

**Proof.** We start with proving the only-if part. To this end, recall that for each \(a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2\), the function \(f_a(\chi_a) : M_2(\mathbb{Z}) \times \widehat{\mathfrak{g}} \to \mathbb{C}\) factors through the projection \(M_2(\mathbb{Z}) \to M_2(\mathbb{Z}/N\mathbb{Z})\); and that the composition \(DR_K \to \Gamma(M_2(\mathbb{Z}) \times \widehat{\mathfrak{g}}) \to \Gamma(M_2(\mathbb{Z}/N\mathbb{Z}) \times \widehat{\mathfrak{g}})\) factors through \(DR_K \to DR_{NO_K}\). In other words, the modular vectors \(f_a's\) for \(a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2\) belong to \(Hom_{\mathfrak{g}}(DR_{NO_K}, K)\), i.e. the galois object \(X_{NO_K}\) dual to \(DR_{NO_K}\). Also \(a \sim_{NO_K} b\) implies the identity \(\psi_a = \psi_b\) on \(X_{NO_K}\). Therefore, since \(\widehat{f}_a \in X_{NO_K}\) for \(a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2\), we have \(\psi_a\widehat{f}_a = \psi_b\widehat{f}_a\) for every \(a \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2\), namely \(a \equiv_{\Xi(N)} b\).

Next we prove the if part along the same line as Lemma 4.2.5. To this end, note first that, by assumption and Lemma 4.3.2 we have the equality \((a, NO_K) = (b, NO_K)\) of the greatest common divisors, which we denote by \(\mathfrak{d}\); then, the \(\sim_{NO_K}\)-classes \([a]\) and \([b]\) \(\in DR_{NO_K}\) belong to the same component of the decomposition \(DR_{NO_K} = \bigsqcup_{b|NO_K} C_{NO_K}/b\). Again, as discussed in Lemma 4.2.5 there exist \([\rho, s], [\rho, t] \in \widehat{O}_K \times \widehat{O}_K\) \((K^R_K/K^*) \simeq DR_K \to DR_{NO_K}\) such that \(\mathfrak{d} = \rho\widehat{O}_K \cap K\) and \([\rho, s], [\rho, t]\) are mapped into \([a]\), \([b]\) \(\in DR_{NO_K}\) respectively under the composition \(\widehat{O}_K \times \widehat{O}_K\) \((K^R_K/K^*) \simeq DR_K \to DR_{NO_K}\). Thus, to see the target congruence \(a \sim_{NO_K} b\), it suffices to prove that \([s], [t] \in Gal(K^{ab}/K)\) define the same action on the ray class field \(K_{NO_K}/b\) over \(K\).

We prove this by showing contradiction; suppose that \([s], [t]\) are not identical on \(K_{NO_K}/b\). When this could be the case, as seen in Lemma 4.2.5 there exists \(a \in (N^{-1}\mathbb{Z}^2/\mathbb{Z}^2) \cdot q_{K}(\rho) \simeq N^{-1}\mathfrak{d}/O_K\) such that \((f_a(\tau_K))^{|s|^{-1}} \neq (f_a(\tau_K))^{|t|^{-1}}\); take \(a' \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2\) such that \(a'=q_K(\rho) = a\). By construction, the ideal classes \([a],[b]\) \(\in DR_{NO_K}\) are the same respectively as the images of \([\rho, s], [\rho, t]\). Therefore, noting that \(\widehat{f}_a : DR_K \to \mathbb{C}\) factors through \(DR_K \to DR_{NO_K}\) for each \(a'' \in N^{-1}\mathbb{Z}^2/\mathbb{Z}^2\), we have
\( \hat{f}_a'(a) = \hat{f}_a'(b) \) and \( \hat{f}_a'(b) = \hat{f}_a'(t) \). On the other hand, by assumption, we have:

\[
\hat{f}_a'(a) = \hat{f}_a'(b) = (f_\alpha(\tau_K))^{[\sigma]^{-1}} \neq (f_\alpha(\tau_K))^{[\tau]^{-1}} = \hat{f}_a'(b) = \hat{f}_a'(a). \tag{4.45}
\]

Thus \( \psi_a \hat{f}_a'(1) \neq \psi_b \hat{f}_a'(1) \); however this contradicts to the assumption \( a \equiv_{\Xi(N)} b \), whence \( \psi_a \hat{f}_a' = \psi_b \hat{f}_a' \) must hold for \( a' \in N^{-1}Z^2/Z^2 \). Therefore, \([s],[t] \) are identical on \( K_{NOK}/b \) and thus \( a \sim_{NOK} b \) as requested.

**Corollary 4.3.4.** We have an isomorphism of \( \Lambda \)-rings:

\[
X_{\Xi(N)} \cong X_{NOK}. \tag{4.46}
\]

**Proof.** The galois object \( X_{\Xi(N)} \) is dual to \( I_K/\equiv_{\Xi(N)} \), while \( X_{NOK} \) is dual to \( I_K/\sim_{NOK} \). Now as proved above, we know that \( \equiv_{\Xi(N)} \) is equal to \( \sim_{NOK} \), hence the claim.

Finally we need the following:

**Lemma 4.3.5.** We have the equality:

\[
X_{\Xi(N)} = K[\hat{f}_a | a \in N^{-1}Z^2/Z^2]. \tag{4.47}
\]

**Proof.** It suffices to see that \( \psi_a \hat{f}_a = \hat{f}_a'[s]a \); namely \( \hat{f}_a(ac) = (\hat{f}_a[\sigma](s))^{[\sigma]} \) for each \( c \in I_K \), since \( a \cdot q_\tau(s_a) \in N^{-1}Z^2/Z^2 \) for any \( a \in N^{-1}Z^2/Z^2 \) and the right-hand-side is closed under the action of \( G_{ab}^K \). But this can be proved as \( \hat{f}_a(ac) = \hat{f}_a(s_a^s c, s_a^s s_a^{-1} s_a^{-1}) = (\hat{f}_a[\sigma](s))^{[\sigma]} = (\hat{f}_a[\sigma](s))^{[\sigma]} \), where we choose \( s_a \in \mathbb{A}^*_K \) so that \( a = s_a \hat{O}_K \cap K \), hence the claim. (To be more specific, the first equality is described in the proof of Lemma 4.1.9; the second equality uses the \( G_{ab}^K \)-equivariance of \( \hat{f}_a \) and follows from the construction of \( \hat{O}_K \times \hat{O}_K \) \( \mathbb{A}^*_K / K^* \to \Gamma \langle \mathbb{M}_2(\mathbb{Z}) \times S \rangle \) in \S 2.2; the last equality again uses the argument described in Lemma 4.1.9.)

This completes the proof of Theorem 4.3.1.

**References**

[1] J. Borger. The basic geometry of Witt vectors I, the affine case. *Algebra and Number Theory*, 5(2):231–285, 2011.

[2] J. Borger and B. de Smit. Galois theory and integral models of \( \lambda \)-rings. *Bulletin of London Mathematical Society*, 40(3):439–446, 2008.

[3] J. Borger and B. de Smit. Lambda actions of rings of integers, 2011. arXiv:1105.4662.

[4] J. Borger and B. de Smit. Explicit class field theory and the algebraic geometry of \( \lambda \)-rings, 2018. arXiv:1809.02295v1.

[5] A. Bridy. Automatic sequences and curves over finite fields. *Algebra and Number Theory*, 11(3):685–712, 2017.

[6] A. Buium. Geometry of \( p \)-jets. *Duke Mathematical Journal*, 82(2):349–367, 1996.
[7] G. Christol. Ensembles presque periodiques k-reconnaissables. Theoret. Comput. Sci., 9(1):pp.141–145, 1979.

[8] G. Christol, T. Kamae, M. France, and G. Gauzy. Suites algebriques, automates et substitutions. Bull. Soc. Math. France, 108:pp.401–409, 1980.

[9] A. Connes and M. Marcolli. Noncommutative Geometry, Quantum Fields and Motives. American Mathematical Society Colloquium Publications. American Mathematical Society, 2008.

[10] A. Connes, M. Marcolli, and N. Ramachandran. KMS states and complex multiplication. Sel. Math. New Ser., 11:325–347, 2005.

[11] P. Deligne and K. Ribet. Values of Abelian L-functions at negative integers over totally real fields. Inventiones mathematicae, 59:227–286, 1980.

[12] M. Laca, S. Larsen, N, and S. Neshveyev. On Bost-Connes systems for number fields. J. Number Theory, 129(2):325–338, 2009.

[13] S. Lang. Elliptic Functions. Springer, 1987.

[14] G. Shimura. Introduction to the arithmetic theory of automorphic functions. Princeton University Press, 1971.

[15] T. Uramoto. Semi-galois Categories I: The Classical Eilenberg Variety Theory, 2017. arXiv:1512.04389v4 (Extended version of LICS’16 paper).

[16] T. Uramoto. Semi-galois Categories II: An arithmetic analogue of Christol’s theorem. J. Algebra, 508(2018):539–568, 2018.

[17] T. Uramoto. Semi-galois Categories III: Witt vectors by deformations of modular functions, 2021. arXiv:2007.13367v4.

[18] T. Uramoto. Semi-galois Categories III: Witt vectors by deformations of modular functions, 2021. arXiv:2007.13367v6.

[19] B. Yalkinoglu. On arithmetic models and functoriality of Bost-Connes systems. with an appendix by Sergey Neshveyev. Invent. Math., 191(2):383–425, 2013.