EXPLICIT CLASS FIELD THEORY AND THE ALGEBRAIC GEOMETRY OF Λ-RINGS

JAMES BORGER, BART DE SMIT

ABSTRACT. We consider generalized Λ-structures on algebras and schemes over the ring of integers O_K of a number field K. When $K = \mathbb{Q}$, these agree with the λ-ring structures of algebraic K-theory. We then study reduced finite flat Λ-rings over O_K and show that the maximal ones are classified in a Galois theoretic manner by the ray class monoid of Deligne and Ribet. Second, we show that the periodic loci on any Λ-scheme of finite type over O_K generate a canonical family of abelian extensions of K. This raises the possibility that Λ-schemes could provide a framework for explicit class field theory, and we show that the classical explicit class field theories for the rational numbers and imaginary quadratic fields can be set naturally in this framework. This approach has the further merit of allowing for some precise questions in the spirit of Hilbert's 12th Problem.

In an interlude which might be of independent interest, we define rings of periodic big Witt vectors and relate them to the global class field theoretical mathematics of the rest of the paper.

CONTENTS

1. Introduction

Let A be a Dedekind domain with fraction field K. Let P be a set of maximal ideals of A such that for each $\mathfrak{p} \in P$, the residue field $k(\mathfrak{p}) = A/\mathfrak{p}$ has finite cardinality $N(\mathfrak{p})$. We will be most interested in the case where K is a number field or local field, A is the full ring of integers O_K of K, and P is the set M_K of all maximal ideals of O_K.

Let B be a (commutative) A-algebra. Then for each $\mathfrak{p} \in P$ the algebra $B/\mathfrak{p}B = B \otimes_A k(\mathfrak{p})$ over $k(\mathfrak{p})$ has a natural $k(\mathfrak{p})$-algebra endomorphism $F_\mathfrak{p} \colon x \mapsto x^{N(\mathfrak{p})}$, which is called the Frobenius endomorphism. By a Frobenius lift on B at $\mathfrak{p}$ we mean an A-algebra endomorphism $\psi_\mathfrak{p} \colon B \to B$ such that $\psi_\mathfrak{p} \otimes k(\mathfrak{p}) = F_\mathfrak{p}$.

We define a $\Lambda_{A,P}$-structure on B to be a set map $P \to \mathrm{End}_{A\text{-alg}}(E)$, denoted $\mathfrak{p} \mapsto \psi_\mathfrak{p}$, such that

(1) $\psi_\mathfrak{p}$ is a Frobenius lift at $\mathfrak{p}$ for each $\mathfrak{p} \in P$.
(2) $\psi_\mathfrak{p} \circ \psi_\mathfrak{q} = \psi_\mathfrak{q} \circ \psi_\mathfrak{p}$ for all $\mathfrak{p}, \mathfrak{q} \in P$.

By a $\Lambda_{A,P}$-*ring* we mean an A-algebra with $\Lambda_{A,P}$-structure. (In fact, this definition of $\Lambda_{A,P}$-structure is well-behaved only when B is torsion free as an A-module, but since all the $\Lambda_{A,P}$-rings in this paper have that property, we will use the simple definition given above. For the general one, see [3].)

For example, if A is the ring of integers of a number field K and B is the ring of integers of a subfield L of the strict Hilbert class field of K, then B has a unique $\Lambda_{A,P}$-structure: $\psi_\mathfrak{p}$ is the Artin symbol of $\mathfrak{p}$ in the field extension $K \subseteq L$.

Observe that if $\mathfrak{p}$ satisfies $B \otimes_A k(\mathfrak{p}) = 0$, then the lifting condition (1) is vacuous. In particular, if B is an algebra over K, then any commuting collection of K-automorphisms of B indexed by the maximal ideals of P is a $\Lambda_{A,P}$-structure on B. At a different extreme, if P consists of one maximal ideal, for example if A is a local ring, then the commutation condition (2) is vacuous.

When $A = \mathbb{Z}$ and $P = M_\mathbb{Q}$, Wilkerson and Joyal have shown that a $\Lambda_{A,P}$-structure on a ring without $\mathbb{Z}$-torsion is the same as a λ-ring structure in the sense of algebraic K-theory [23][15]. For instance, for any abelian group M we have a natural $\Lambda_{\mathbb{Z},P}$-structure on the group ring $\mathbb{Z}[M]$ given by $\psi_{(p)}(m) = m^p$ for $m \in M$ and prime p. In an earlier paper [7], we showed that a $\Lambda_{\mathbb{Z},P}$-ring that is reduced and finite flat over $\mathbb{Z}$ is a sub-$\Lambda_{\mathbb{Z},P}$-ring of $\mathbb{Z}[C]^n$ for some finite cyclic group C and integer $n \geqslant 0$. The proof uses the explicit description of ray class fields over $\mathbb{Q}$ as cyclotomic fields.

Over a general number field, class field theory is less explicit, and the generalizations we present in the present paper are consequently less explicit. However, we can still give a very similar criterion for a finite étale K-algebra E with $\Lambda_{A,P}$-structure to admit an integral $\Lambda_{A,P}$-model, by which we mean a sub-$\Lambda_{A,P}$-ring $B \subseteq E$ which is finite flat as an A-module such that the induced map $K \otimes_A B \to E$ is a bijection. See theorem 1.2 below.

Let Id_P denote the set of non-zero ideals of A divisible only by the primes in P. It as a monoid under ideal multiplication, the free commutative monoid on the set P. Let K^{sep} be a separable closure of K, and let G_K denote the Galois group of K^{sep} over K. It is a profinite group. By a G_K-set X we mean a finite discrete set with a continuous G_K-action. By Grothendieck's formulation of Galois theory, a finite étale K-algebra E is determined by the G_K-set S consisting of all K-algebra homomorphisms $E \to K^{\mathrm{sep}}$. Giving a $\Lambda_{A,P}$-structure on E then translates to giving a monoid map $\mathrm{Id}_P \to \mathrm{Map}_{G_K}(S, S)$. By giving Id_P the discrete topology, we see that the category of $\Lambda_{A,P}$-rings whose underlying A-algebra is a finite étale K-algebra is anti-equivalent to the category of finite discrete sets with a continuous action of the monoid $G_K \times \mathrm{Id}_P$.

Let us first consider the case where A is a complete discrete valuation ring and P consists of the single maximal ideal $\mathfrak{p}$. Then Id_P is isomorphic as a monoid to the monoid of non-negative integers under addition. Let $I_K \subseteq G_K$ be the inertia subgroup. Then I_K is normal in G_K and G_K/I_K is the absolute Galois group of $k(\mathfrak{p})$, which contains the Frobenius element $F \in G_K/I_K$ given by $x \mapsto x^{N(\mathfrak{p})}$. Thus, F acts on any G_K-set on which I_K acts trivially.

Theorem 1.1. *Suppose that A is a complete discrete valuation ring and that P consists of the single maximal ideal $\mathfrak{p}$. Let E be a finite étale K-algebra with a $\Lambda_{A,P}$-structure, and let S be the set of K-algebra maps from E to K^{sep}. Then K has an integral $\Lambda_{A,P}$-model if and only if the action of $G_K \times \mathrm{Id}_P$ on S satisfies the following two conditions:*

 (1) *the group I_K acts trivially on $S_{\mathrm{unr}} = \bigcap_{n \geqslant 0} \mathfrak{p}^n S$;*
 (2) *the elements $\mathfrak{p} \in \mathrm{Id}_P$ and $F \in G_K/I_K$ act in the same way on S_{unr}.*

See section 3 for the proof.

Next, consider the global case, where A is the ring of integers in a number field.

In order to express our result, let us first recall the definition of the ray class monoid. A cycle of K is a formal product $\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$, where the product ranges over all primes of K, both finite and infinite, all $n_{\mathfrak{p}}$ are non-negative integers, only finitely many of which are non-zero, and we have $n_{\mathfrak{p}} \in \{0, 1\}$ for real primes $\mathfrak{p}$, and $n_{\mathfrak{p}} = 0$ for complex primes $\mathfrak{p}$. The finite part of $\mathfrak{f}$ is $\mathfrak{f}_{\mathrm{fin}} = \prod_{\mathfrak{p} < \infty} \mathfrak{p}^{n_{\mathfrak{p}}}$, which can be viewed as an ideal of A. We write $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}) = n_{\mathfrak{p}}$.

For a cycle $\mathfrak{f}$, we say that two integral ideals $\mathfrak{a}, \mathfrak{b}$ are $\mathfrak{f}$-*equivalent*, and write $\mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{b}$, if the following two conditions are satisfied:

 (1) $\mathfrak{a}$ and $\mathfrak{b}$ have the same greatest common divisor $\mathfrak{d}$ with $\mathfrak{f}_{\mathrm{fin}}$
 (2) $\mathfrak{a}\mathfrak{d}^{-1}$ and $\mathfrak{b}\mathfrak{d}^{-1}$ represent the same class in the ray class group $\mathrm{Cl}(\mathfrak{f}\mathfrak{d}^{-1})$ of conductor $\mathfrak{f}\mathfrak{d}^{-1}$.

This is an equivalence relation, and we write $\mathrm{DR}_P(\mathfrak{f})$ for the quotient $\mathrm{Id}_P/\sim_{\mathfrak{f}}$. Because $\sim_{\mathfrak{f}}$ is preserved by multiplication of ideals, $\mathrm{DR}_P(\mathfrak{f})$ inherits a unique monoid structure from Id_P. We call it the *ray class monoid (or Deligne–Ribet monoid)* of conductor $\mathfrak{f}$ supported at P. It was introduced in Deligne–Ribet [11] in the case where $P = M_K$ and every real place divides $\mathfrak{f}$. For alternative definitions of $\mathfrak{f}$-equivalence and $\mathrm{DR}_P(\mathfrak{f})$, see section 4.

Let us say that P is *Chebotarev dense* if any element of any ray class group $\mathrm{Cl}(\mathfrak{f})$ can be represented by an ideal supported at P, or equivalently by infinitely many such ideals. For example, by Chebotarev's theorem, any set P consisting of all but finitely many maximal ideals is Chebotarev dense. Whenever P is Chebotarev dense, any element of $\mathrm{Cl}(\mathfrak{f})$ can be written as the class of an ideal supported at P, and hence gives a well-defined element of $\mathrm{DR}_P(\mathfrak{f})$. This defines a map $\mathrm{Cl}(\mathfrak{f}) \to \mathrm{DR}_P(\mathfrak{f})$, which is in fact injective. Composing with the Artin symbol defines a map

(1.1.1) $$ G_K \longrightarrow \mathrm{Cl}(\mathfrak{f}) \longrightarrow \mathrm{DR}_P(\mathfrak{f}), $$

and hence a surjective map

(1.1.2) $$ G_K \times \mathrm{Id}_P \longrightarrow \mathrm{DR}_P(\mathfrak{f}) $$

whose restriction to the first factor is the map (1.1.1) and whose restriction to the second factor is the canonical quotient map $\mathrm{Id}_P \to \mathrm{DR}_P(\mathfrak{f})$.

Theorem 1.2. *Suppose that K is a number field and that P is Chebotarev dense. Let E be a finite étale K-algebra with a $\Lambda_{A,P}$-structure, and let S be the set of K-algebra maps from E to K^{sep}. Then E has an integral $\Lambda_{A,P}$-model if and only if there is a cycle $\mathfrak{f}$ of K such that the action of $G_K \times \mathrm{Id}_P$ on S factors (necessarily uniquely) through the map $G_K \times \mathrm{Id}_P \longrightarrow \mathrm{DR}_P(\mathfrak{f})$ above.*

It follows that the category of such $\Lambda_{A,P}$-rings is anti-equivalent to the category of finite discrete sets with a continuous action by the profinite monoid $\lim_{\mathfrak{f}} \mathrm{DR}_P(\mathfrak{f})$, where the inverse limit is taken over all cycles $\mathfrak{f}$ with respect to the canonical surjective maps $\mathrm{DR}(\mathfrak{f}) \to \mathrm{DR}(\mathfrak{f}')$ when $\mathfrak{f}' \mid \mathfrak{f}$. When $K = \mathbb{Q}$, $A = \mathbb{Z}$, and $P = M_{\mathbb{Q}}$, this limit is the monoid $\hat{\mathbb{Z}}^{\circ}$ of all profinite integers under multiplication. In this case, the theorem above reduces to the first theorem of our earlier paper [7]. It was Lenstra who suggested that the ray class monoid could play this role over general number fields.

When E admits an integral $\Lambda_{A,P}$-model, there must be a maximal one. (See section 2.) In the example above, $\mathbb{Z}[x]/(x^n - 1)$ is the maximal integral model of $\mathbb{Q}[x]/(x^n - 1)$. This is the second theorem in [7]. In general, let us write $R_{A,P}(\mathfrak{f})$ for the maximal integral $\Lambda_{A,P}$-model associated to the free $\mathrm{DR}_P(\mathfrak{f})$-set on one generator, namely $\mathrm{DR}_P(\mathfrak{f})$. We call $R_{A,P}(\mathfrak{f})$ the *ray class algebra* of conductor $\mathfrak{f}$—just as $K(\mathfrak{f})$, the ray class field of conductor $\mathfrak{f}$, is the extension of K corresponding to the free $\mathrm{Cl}(\mathfrak{f})$-set on one generator. The ray class algebra is an order in a product of ray class fields:

$$K \otimes_A R_{A,P}(\mathfrak{f}) = \prod_{\mathfrak{d} \mid \mathfrak{f}, \mathfrak{d} \in \mathrm{Id}_P} K(\mathfrak{f}\mathfrak{d}^{-1}).$$

It is typically smaller than the maximal order in the non-Λ sense. For example,

$$R_{\mathbb{Z}, M_{\mathbb{Q}}}(n\infty) = \mathbb{Z}[x]/(x^n - 1) \subsetneq \prod_{d \mid n} \mathbb{Z}[\zeta_d].$$

The theorems in [7] for $K = \mathbb{Q}$, however, give us something more than the abstract existence theorem above. They give explicit presentations of the ray class algebras $R_{\mathbb{Z}, M_{\mathbb{Q}}}(n\infty)$, namely $\mathbb{Z}[x]/(x^n - 1)$. More importantly, the presentations are all as quotients of a single finitely generated Λ-ring—in this case $\mathbb{Z}[x^{\pm 1}]$, or $\mathbb{Z}[x]$, where each ψ_p is defined by $\psi_p(x) = x^p$. One can view this as a Λ-refinement of the Kronecker–Weber theorem, telling us that the function algebra $\mathcal{O}(\mu_n)$ of the n-torsion subscheme $\mu_n \subset \mathbb{G}_{\mathrm{m}} = \mathrm{Spec}\,\mathbb{Z}[x^{\pm 1}]$ is isomorphic as a $\Lambda_{\mathbb{Z}, M_{\mathbb{Q}}}$-ring to the ray class algebra $R_{\mathbb{Z}, M_{\mathbb{Q}}}(n\infty)$; this is instead of the statement that its set of $\bar{\mathbb{Q}}$-points, $\mu_n(\bar{\mathbb{Q}})$, generates the ray class field $\mathbb{Q}(n\infty)$. This refinement gives us Frobenius lifts at all primes, even those dividing the conductor, by treating integral structures with more care. But the ray class algebras will have zero divisors and be non-normal over the primes dividing the conductor, which some might consider a drawback. Then again, they are normal in a Λ-ring theoretic sense, by definition.

It is natural to ask whether something like this holds for number fields K larger than $\mathbb{Q}$. Do the ray class algebras $R_{A,P}(\mathfrak{f})$ have a common origin in the algebraic geometry of $\Lambda_{A,P}$-rings? If so, this would give a systematic way of generating ray class algebras and hence ray class fields. Or more modestly, is it at least true that the known explicit class field theories admit a Λ-refinement as above? There is also a converse question: when does a $\Lambda_{A,P}$-structure on an A-scheme X give rise to a family of abelian extensions, as the $\Lambda_{\mathbb{Z}, M_{\mathbb{Q}}}$-structure on $\mathbb{G}_{\mathrm{m}}$ does?

The converse is the easier direction, and we will consider it first. Let X be a (flat and separated) A-scheme with a $\Lambda_{A,P}$-structure, by which we mean a commuting family of Frobenius lifts $\psi_{\mathfrak{p}} \colon X \to X$, for $\mathfrak{p} \in P$. If we are going to follow the model of $\mu_n \subseteq \mathbb{G}_{\mathrm{m}}$ and produce abelian extensions of our number field K by finding finite flat sub-$\Lambda_{A,P}$-schemes $Z \subseteq X$ and applying the theorem above, then by this theorem, there must exist a cycle $\mathfrak{f}$ such that the Frobenius operators $\psi_{\mathfrak{a}}$ on Z are $\mathfrak{f}$-periodic in $\mathfrak{a}$, meaning that they depend only on the class of $\mathfrak{a}$ in $\mathrm{DR}_P(\mathfrak{f})$. So it is natural to consider the largest such subscheme, the locus $X(\mathfrak{f}) \subseteq X$ where the operations $\psi_{\mathfrak{a}}$ depend only the class of $\mathfrak{a}$ in $\mathrm{DR}_P(\mathfrak{f})$. We call $X(\mathfrak{f})$ the $\mathfrak{f}$-periodic

locus. It is defined by a large equalizer diagram; so it does indeed exist and is a closed subscheme of X.

For example, in the cyclotomic setting with the $\Lambda_{\mathbb{Z}, M_{\mathbb{Q}}}$-scheme $X = \mathbb{G}_{\mathrm{m}}$ as above and $\mathfrak{f} = n\infty$, with $n \geqslant 1$, the $\mathfrak{f}$-periodicity condition is $\psi_{(m+n)} = \psi_{(m)}$ for all $m \geqslant 1$. In other words, it is that the operators $\psi_{(m)}$ are periodic in m with period dividing n. It follows that the $\mathfrak{f}$-periodic locus is just the n-torsion locus μ_n. In general, while the $\mathfrak{f}$-periodic locus is similar in spirit to the $\mathfrak{f}$-torsion locus when X is a group, they can be different: for example if X is still $\mathbb{G}_{\mathrm{m}}$ but $\mathfrak{f}$ is trivial at ∞, so $\mathfrak{f} = (n)$, then the periodic locus must also be invariant under the involution $x \mapsto x^{\pm 1}$ and is hence just μ_2 if n is even, or μ_1 if n is odd.

But the definition of $X(\mathfrak{f})$ does not even require X to be a group. Thus the group scheme structure in the traditional frameworks for explicit class field theory is replaced by a Λ-structure in ours. This will allow us some flexibility that is not available when working with group schemes. For example, we can divide out a CM elliptic curve, say, by its automorphism group. Although the group structure is lost, the Λ-structure is retained and hence we can still speak of the periodic locus on the quotient. Note that whereas in the group-scheme setting, the abelian nature of the Galois theory comes from the torsion locus being of rank 1 over some commutative ring of complex multiplications and then from the commutativity of the general linear group GL_1, in our setting, it comes from the assumption that the Frobenius lifts $\psi_{\mathfrak{p}}$ commute with each other and then from Chebotarev's theorem.

We can now state the answer to the converse question:

Theorem 1.3. *Let X be a $\Lambda_{A,P}$-scheme of finite type over A, as above, and assume P is Chebotarev dense. Then possibly after inverting some primes, $X(\mathfrak{f})$ is an affine $\Lambda_{A,P}$-scheme which is reduced and finite flat over A.*

The idea of the proof is that for primes $\mathfrak{p} \nmid \mathfrak{f}$, the endomorphism $\psi_{\mathfrak{p}}$ is an automorphism of finite order because the class $[\mathfrak{p}] \in \mathrm{DR}_P(\mathfrak{f})$ is invertible and hence has finite order; therefore the Frobenius endomorphism of the fiber of X over $\mathfrak{p}$ is an automorphism of finite order, and so the fiber is finite and geometrically reduced. Then apply the semicontinuity theorems of scheme theory. For details, see theorem 8.4.

It then follows from theorem 1.2 that $\mathcal{O}(X(\mathfrak{f})_K)$, the function algebra of the generic fiber of $X(\mathfrak{f})$, is a finite product of abelian extensions of K of conductor dividing $\mathfrak{f}$. Thus any $\Lambda_{A,P}$-scheme X of finite type (still flat and separated) gives rise to a uniform geometric way of constructing abelian extensions indexed by cycles $\mathfrak{f}$. It will not always produce arbitrarily large abelian extensions—for example, the Chebyshev line below will only produce the ray class fields over $\mathbb{Q}$ with trivial conductor at infinity, namely $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

We can now state some precise versions of our original question of whether the ray class algebras have a common origin in Λ-algebraic geometry. It is cleaner to restrict to cycles $\mathfrak{f}$ of a fixed type away from P, and in particular of a fixed type at infinity. So fix a cycle $\mathfrak{r}$ supported away from P, and let $Z(P, \mathfrak{r})$ denote the set of cycles $\mathfrak{f}$ which agree with $\mathfrak{r}$ away from the primes in P. We will refer to the triple $(A, P, \mathfrak{r})$ as the *context*.

(Q1) Does there exist a $\Lambda_{A,P}$-scheme X of finite type such that for all $\mathfrak{f} \in Z(P, \mathfrak{r})$, the direct factors of the étale K-algebra $\mathcal{O}(X(\mathfrak{f})_K)$ generate the ray class field $K(\mathfrak{f})$?

The Kronecker–Weber theorem states that the answer is positive in the cyclotomic context $(\mathbb{Z}, M_{\mathbb{Q}}, \infty)$, with X being $\mathbb{G}_{\mathrm{m}}$ with the usual $\Lambda_{\mathbb{Z}, M_{\mathbb{Q}}}$-structure defined above. We will show it is true in two other classical contexts of explicit

class field theory, namely the real-cyclotomic context $(\mathbb{Z}, M_\mathbb{Q}, (1))$ and the context $(O_K, M_K, (1))$ where K is an imaginary quadratic field.

In fact, we will show a stronger Λ-refinement holds. The strongest question one might ask is the following:

(Q2) Does there exist a $\Lambda_{A,P}$-scheme X of finite type such that for all $\mathfrak{f} \in Z(P, \mathfrak{r})$, the function algebra $\mathcal{O}(X(\mathfrak{f}))$ of the periodic locus is isomorphic to the ray class algebra $R_{A,P}(\mathfrak{f})$?

As mentioned above, the answer is positive in the cyclotomic context with $X = \mathbb{G}_\mathrm{m}$. But it appears to be slightly too much to ask for in general. For instance, consider the real-cyclotomic context $(\mathbb{Z}, M_\mathbb{Q}, (1))$, and let $X = \mathbb{G}_\mathrm{m}/(x \mapsto x^{-1}) \cong \mathbb{A}_\mathbb{Z}^1$. Then the $\Lambda_{\mathbb{Z}, M_\mathbb{Q}}$-structure on $\mathbb{G}_\mathrm{m}$ descends to one on X. The operations $\psi_{(p)}$ are given by Chebyshev polynomials $\psi_{(p)}(y) \in \mathbb{Z}[y]$ determined by $\psi_{(p)}(x + x^{-1}) = x^p + x^{-p}$. Then for any $n \geqslant 1$, the periodic locus $X(n)$ does indeed generate the real ray class fields,

$$\mathbb{Q}(X(n)(\bar{\mathbb{Q}})) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}),$$

but $\mathcal{O}(X(n))$ does not generally agree with the full ray class algebra $R_{\mathbb{Z}, P}(n)$. It is however only of index 2 in it, once n is even, and this error even disappears in the limit as n grows. So in the real-cyclotomic context, the answer to (Q2) is as about as close to being positive without being so (at least for the given X!). This discrepancy is no doubt due to the nontrivial isotropy groups of the points $\pm 1 \in \mathbb{G}_\mathrm{m}$ under the involution $x \mapsto x^{-1}$, and it may very well disappear in a proper stack-theoretic treatment.

But if we stay in the world of schemes, we need to control it. So given a finite reduced $\Lambda_{A,P}$-ring B, let $\tilde{B}$ denote the maximal integral $\Lambda_{A,P}$-model in $K \otimes_A B$. It is the Λ-analogue of the integral closure of B.

(Q3) Does there exist a $\Lambda_{A,P}$-scheme X of finite type such that for all $\mathfrak{f} \in Z(P, \mathfrak{r})$,
(i) the function algebra $\mathcal{O}(X(\mathfrak{f}))$ is of finite index in $\mathcal{O}(X(\mathfrak{f}))^\sim$,
(ii) the morphism of pro-rings

$$\left(\mathcal{O}(X(\mathfrak{f})) \right)_{\mathfrak{f} \in Z(P, \mathfrak{r})} \longrightarrow \left(\mathcal{O}(X(\mathfrak{f}))^\sim \right)_{\mathfrak{f} \in Z(P, \mathfrak{r})}$$

is an isomorphism, and
(iii) $\mathcal{O}(X(\mathfrak{f}))^\sim$ is isomorphic to $R_A(\mathfrak{f})$ as a $\Lambda_{A,P}$-ring?

Theorem 1.4. *The answer to (Q3) is positive in the following contexts $(A, P, \mathfrak{r})$ with the $\Lambda_{A,P}$-schemes X:*

(1) $(\mathbb{Z}, M_\mathbb{Q}, \infty)$ *and* $X = \mathbb{G}_{\mathrm{m}/\mathbb{Z}}$ *with the $\Lambda_{\mathbb{Z}, M_\mathbb{Q}}$-structure above*
(2) $(\mathbb{Z}, M_\mathbb{Q}, (1))$ *and* $X = \mathbb{A}_\mathbb{Z}^1$ *with the Chebyshev $\Lambda_{\mathbb{Z}, M_\mathbb{Q}}$-structure*
(3) $(O_K, M_K, (1))$, *where K is imaginary quadratic with Hilbert class field H, and X is $\mathbb{P}_{O_H}^1$, viewed as a scheme over O_K, with the Lattès Λ_{O_K, M_K}-structure defined in (11.2).*

The Λ-scheme $\mathbb{P}_{O_H}^1$ in the imaginary quadratic context plays the role of the target of the Weber functions $E \to E/\mathrm{Aut}(E) \cong \mathbb{P}_\mathbb{C}^1$ in the traditional treatments of explicit class field theory of imaginary quadratic fields. There are, however, a number of subtleties in constructing this Λ-structure. For instance, CM elliptic curves are only defined over H and not K, there can be more than one of them, but it might be that none of them has good reduction everywhere. These problems were completely clarified in Gurney's thesis [14]. He also gave an account of class field theory for imaginary quadratic fields from the point of view of the Λ-structure on $\mathbb{P}_{O_H}^1$, but he stopped at considering the field extensions generated by the preimages $\psi_\mathfrak{f}^{-1}(\infty)$. In either approach, the package of elliptic curves with complex multiplication and their Weber functions is replaced by the single Λ_{O_K, M_K}-scheme $\mathbb{P}_{O_H}^1$.

We emphasize that $\mathbb{P}^1_{O_H}$ is not so interesting from a cohomological or motivic point of view—there are no interesting Galois representations in the cohomology. All the richness is in the Λ-structure.

It would be interesting to know if something similar holds for other number fields, starting with CM fields. One virtue of the questions above is that they allow for negative answers, which would also be interesting. In the final section, we will raise some further questions in this direction.

It is a pleasure to thank Lance Gurney and Hendrik Lenstra for several helpful discussions.

Part 1. Finite Λ-rings and class field theory

2. Maximal Λ-orders

2.1. *Maximal Λ-orders.* Let A' be a sub-A-algebra of K, and let E be a finite K-algebra with $\Lambda_{A,P}$-structure. A sub-A'-algebra $B \subseteq E$ with a $\Lambda_{A,P}$-structure is said to be a $\Lambda_{A,P}$-*order (over A')* if it is finite over A'. We say it is *maximal (in E)* if it contains all others. Maximal $\Lambda_{A,P}$-orders always exist, by an elementary argument ([7], prop. 1.1), since maximal orders in the ordinary sense exist and since A' is noetherian.

We will say a finite flat A'-algebra B with a $\Lambda_{A,P}$-structure is *normal* (or $\Lambda_{A,P}$-*normal over A'*) if it is maximal in $K \otimes_{A'} B$, in the sense above.

We will need the following basic facts:

Proposition 2.2. *Let B be a finite flat A'-algebra with $\Lambda_{A,P}$-structure.*
  (1) *B is $\Lambda_{A,P}$-normal over A' if $O_{K_{\mathfrak{p}}} \otimes_{A'} B$ is $\Lambda_{O_{K_{\mathfrak{p}}},\mathfrak{p}}$-normal over $O_{K_{\mathfrak{p}}}$ for all maximal ideals $\mathfrak{p}$ of A'.*
  (2) *If B is $\Lambda_{A,P}$-normal over A', and G is a group acting on B by $\Lambda_{A,P}$-automorphisms, then the invariant subring B^G is $\Lambda_{A,P}$-normal over A'.*
  (3) *If B is a product $B_1 \times B_2$ of $\Lambda_{A,P}$-rings, then B is $\Lambda_{A,P}$-normal over A' if and only if B_1 and B_2 are.*

Proof. (1): Let $C \subseteq K \otimes_{A'} B$ be a $\Lambda_{A,P}$-order over A' containing B. Then for any maximal ideal $\mathfrak{p} \subset A'$, the base change $O_{K_{\mathfrak{p}}} \otimes_{A'} C$ is a $\Lambda_{O_{K_{\mathfrak{p}}},\mathfrak{p}}$-order over $O_{K_{\mathfrak{p}}}$. Therefore it agrees with $O_{K_{\mathfrak{p}}} \otimes_{A'} B$. Since this holds for all maximal ideals $\mathfrak{p} \subset A'$, the ring C agrees with B. Therefore B is maximal.

(2): Let $C \subseteq K \otimes_{A'} B^G$ be a $\Lambda_{A,P}$-order over A' containing B^G. Then C is contained in $K \otimes_{A'} B$ and hence, by the maximality of B, is contained in B. But since C is contained in $K \otimes_{A'} B^G$, it is also G-invariant. Therefore we have $C \subseteq B^G$.

(3): Let $C \subseteq K \otimes_{A'} (B_1 \times B_2)$ be a $\Lambda_{A,P}$-order over A' containing $B_1 \times B_2$. Put $C_i = C \otimes_{B_1 \times B_2} B_i$, for $i = 1, 2$. Then each C_i is a $\Lambda_{A,P}$-order over A' in $K \otimes_{A'} B_i$. By the maximality of B_i, we have $C_i = B_i$. Therefore we have

$$C = C_1 \times C_2 = B_1 \times B_2.$$

Thus $B_1 \times B_2$ is maximal. $\qquad\square$

3. The local case

In this section, A will be a complete discrete valuation ring with maximal ideal $\mathfrak{p}$, and P will be the singleton set $\{\mathfrak{p}\}$. So Id_P is the multiplicative monoid of all nonzero ideals of A. Write $k = k(\mathfrak{p})$ and $\Lambda_{A,\mathfrak{p}} = \Lambda_{A,P}$.

Proposition 3.1. *Let B be a finite étale A-algebra. Then B has a unique $\Lambda_{A,\mathfrak{p}}$-structure, and the induced action of $G_K \times \mathrm{Id}_P$ on $S = \mathrm{Hom}_{K\text{-alg}}(B \otimes_A K, K^{\mathrm{sep}})$ has the property that the inertia group I_K acts trivially and that the element $\mathfrak{p} \in \mathrm{Id}_P$ and the Frobenius element $F \in G_K/I_K$ act on S in the same way.*

Proof. Because B is étale, $k \otimes_A B$ is a product of finite fields. Since B is complete in its $\mathfrak{p}$-adic topology, idempotents of $B/\mathfrak{p}B$ lift to B, so that B is a finite product of rings of integers in finite unramified extensions of K. Therefore the inertia group $I_K \subseteq G_K$ acts trivially on $S = \operatorname{Hom}_{A\text{-alg}}(B, K^{\text{sep}})$. Every finite unramified field extension L of K is Galois with an abelian Galois group, and its rings of integers has a unique Frobenius lift. It follows that when B is unramified over A, it has a unique $\Lambda_{A,\mathfrak{p}}$-structure.   □

3.2. *Structure of finite étale K-algebras with $\Lambda_{A,\mathfrak{p}}$-structure.* Let E be a finite étale K-algebra with a $\Lambda_{A,\mathfrak{p}}$-structure, and write

$$S = \operatorname{Hom}_{K\text{-alg}}(E, K^{\text{sep}}).$$

Put $S_0 = \bigcap_{n \geqslant 0} \mathfrak{p}^n S$ and for $i = 1, 2, \ldots$, let

$$S_i = \{s \in S \colon \ s \notin S_{i-1} \text{ and } \mathfrak{p}s \in S_{i-1}\}.$$

Then each S_i is a sub-G_K-set of S. Since S is finite, there exists an $n \geqslant 0$ such that $S_{n+1} = \varnothing$. Then we have the decomposition

$$S = S_0 \sqcup S_1 \sqcup \cdots \sqcup S_n.$$

Let $E_i = \operatorname{Map}_{G_K}(S_i, K^{\text{sep}})$ be the corresponding finite étale K-algebra for each i. Then the maps $S_n \to \cdots \to S_1 \to S_0 \circlearrowleft$ given by multiplication by $\mathfrak{p}$ give rise to a diagram of K-algebras

$$f_0 \circlearrowright E_0 \xrightarrow{f_1} E_1 \xrightarrow{f_2} \cdots \xrightarrow{f_n} E_n$$

Since $S = S_0 \sqcup S_1 \sqcup \cdots \sqcup S_n$ is a decomposition of G as a G_K-set, we have a corresponding product decomposition of the finite étale K-algebras $E = E_0 \times E_1 \times \cdots \times E_n$. In terms of this decomposition, ψ_p is given by

$$(3.2.3) \qquad \psi_{\mathfrak{p}}(e_0, e_1, \ldots, e_n) = (f_0(e_0), f_1(e_0), \ldots, f_n(e_{n-1})).$$

Since S_0 is closed under multiplication by $\mathfrak{p}$, the quotient ring E_0 of E is a quotient $\Lambda_{A,\mathfrak{p}}$-ring of E, with Frobenius lift f_0.

We will now construct a splitting of this quotient map $E \to E_0$ in the category of $\Lambda_{A,\mathfrak{p}}$-rings. Note that we have $\mathfrak{p}^k S = S_0$ for sufficiently large k; so we have $\mathfrak{p}S_0 = S_0$ and hence $\mathfrak{p}$ act as a bijection on S_0. Thus, f_0 is an automorphism of E_0. For $s \in S_i$ we have $\mathfrak{p}^i s \in S_0$. Again since $\mathfrak{p}$ acts bijectively on S_0, we can define a map $S \longrightarrow S_0$ by sending $s \in S_i$ to the unique element s' of S_0 such that $\mathfrak{p}^i s' = \mathfrak{p}^i s$. This map commutes with the $G_K \times \operatorname{Id}_P$-action, and it is a retraction of the inclusion $S_0 \to S$. This induces our desired splitting $E_0 \to E$. In other words, E_0 is not only a quotient $\Lambda_{A,\mathfrak{p}}$-ring of E, but also a sub-$\Lambda_{A,\mathfrak{p}}$-ring:

$$j \colon E_0 \longrightarrow E$$
$$e_0 \longmapsto (e_0, f_1 f_0^{-1} e_0, f_2 f_1 f_0^{-2} e_0, \ldots, f_{n-1} \cdots f_1 f_0^{-n+1} e_0).$$

3.3. *Proof of theorem 1.1.* Suppose that E has an integral $\Lambda_{A,\mathfrak{p}}$-model B, that is,

   (i) B is finitely generated as an A-module and has rank $\dim_K(E)$,
   (ii) $\psi_{\mathfrak{p}}(B) \subseteq B$,
   (iii) $\psi_{\mathfrak{p}} \otimes_A k$ is the Frobenius map $x \mapsto x^{N(\mathfrak{p})}$ on $B \otimes_A k$.

Let B_0 denote the image of B under the quotient map $E \to E_0$ (in the notation of 3.2). Then B_0 is an integral $\Lambda_{A,\mathfrak{p}}$-model of E_0. Since f_0 is an automorphism of E_0, the ring B_0 and its subring $f_0(B_0)$ have the same discriminant. Thus, $f_0(B_0) = B_0$ and hence f_0 is an automorphism of B_0. This implies that the map $x \mapsto x^{N(\mathfrak{p})}$ on $B_0 \otimes_A k$ is an automorphism, and so B_0 is étale over A. Conditions (1) and (2) of theorem 1.1 now follow by proposition 3.1.

For the converse, suppose that conditions (1) and (2) hold. We will produce an integral $\Lambda_{A,\mathfrak{p}}$-model of $E = E_0 \times \cdots \times E_n$. Let R_i be the integral closure of A in E_i. Since I_K acts trivially on $S_{\text{unr}} = S_0$, the A-algebra R_0 is finite étale and hence has a unique $\Lambda_{A,\mathfrak{p}}$-structure by proposition 3.1. Our integral model $B \subseteq E$ will be of the form

$$(3.3.4) \qquad\qquad B = j(R_0) \oplus (0 \times \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n),$$

where each $\mathfrak{a}_i$ is an ideal in R_i and j is the map defined in 3.2. Observe that any B of this form is a subring of E. For it to be a sub-$\Lambda_{A,\mathfrak{p}}$-ring, we need to have $\psi_{\mathfrak{p}}(a) \equiv a^{N(\mathfrak{p})} \bmod \mathfrak{p}B$ for all $a \in B$. Since both sides of this congruence are additive in a, it is enough to consider elements a in each of the summands in (3.3.4). It holds for the summand $j(R_0)$ because j is a $\Lambda_{A,\mathfrak{p}}$-morphism. So by (3.2.3), a sufficient condition for B to be a sub-$\Lambda_{A,\mathfrak{p}}$-ring is $f_i(\mathfrak{a}_{i-1}) \subseteq \mathfrak{p}\mathfrak{a}_i$ and $\mathfrak{a}_i^{N(\mathfrak{p})} \subseteq \mathfrak{p}\mathfrak{a}_i$ for $i = 1, \ldots, n$, where we take $\mathfrak{a}_0 = 0$. This holds if, for instance, $\mathfrak{a}_i = \mathfrak{p}^{n-i+1}R_i$. So for this choice, B is an integral $\Lambda_{A,\mathfrak{p}}$-model of E. $\qquad\square$

3.4. *Remark.* Note that the integral model produced in the proof above is not always the maximal one. For instance, if C_n denotes a cyclic group of order n, then on the group algebra $\mathbb{Q}_2[C_4]$ with its usual $\Lambda_{\mathbb{Z}_2,2}$-structure, the proof produces a strict subring of $\mathbb{Z}_2[C_4]$ and hence cannot be not maximal. (In fact, $\mathbb{Z}_2[C_4]$ is the maximal integral model, as is shown in [7]).

It can also happen that, for group algebras, the integral model supplied by the proof is strictly larger than the integral group algebra. An example is $\mathbb{Q}_2[C_2 \times C_2]$.

3.5. *Remark.* It is possible to express theorem 1.1 in a more Galois-theoretic way, similar to the statement of theorem 1.2. We can define an inverse system of finite quotients $G_{N,n}$ of the monoid $G_K \times \text{Id}_P$ with the property that E has an integral $\Lambda_{A,\mathfrak{p}}$-model if and only if the action of $G_K \times \text{Id}_P$ on S factors through some $G_{N,n}$.

The quotients $G_{N,n}$ are defined as follows. Let N be an open normal subgroup of G_K, and let n be an integer $\geqslant 0$. Define a relation on $G_K \times \text{Id}_P$ by $(g, \mathfrak{p}^a) \sim (h, \mathfrak{p}^b)$ if either or both of the following conditions hold:
  (1) $a = b$ and $g \equiv h \bmod N$
  (2) $a, b \geqslant n$ and $gF^a \equiv hF^b \bmod NI_K$.
This is easily seen to be an equivalence relation which is stable under the monoid operation. We then define $G_{N,n}$ to be the quotient monoid. Observe that we have a decomposition of G_K-sets:

$$(3.5.5) \qquad\qquad G_{N,n} = \underbrace{G_K/N \sqcup \cdots \sqcup G_K/N}_{n \text{ times}} \sqcup\, G_K/NI_K.$$

For $N' \subseteq N$ and $n' \geqslant n$, we have evident transition maps $G_{N',n'} \to G_{N,n}$. If we consider the inverse limit

$$\hat{G} = \lim_{N,n} G_{N,n},$$

then the re-expression of theorem 1.1 is that E has an integral $\Lambda_{A,\mathfrak{p}}$-model if and only if the action of $G_K \times \text{Id}_P$ on S factors (necessarily uniquely) through a continuous action of $\hat{G}$. One might call $\hat{G}$ the $\Lambda_{A,\mathfrak{p}}$-algebraic fundamental monoid of $\text{Spec}\, O_K$ with ramification allowed along $\text{Spec}\, k$.

3.6. *Remark.* In the global case considered in the rest of this paper, we will see that only abelian field extensions arise from integral Λ-models. But in the local case, we can get nonabelian extensions. In fact, we can get arbitrary extensions. Indeed, any given extension L of K is a direct factor of the K-algebra $L_{\text{unr}} \times L$, which has a $\Lambda_{A,\mathfrak{p}}$-structure admitting an integral model. For instance, one can take $\psi_{\mathfrak{p}}(e_0, e_1) = (F(e_0), e_0)$.

4. The ray class monoid

Fix the following notation:

$$K = \text{a finite extension of } \mathbb{Q}$$
$$O_K = \text{the ring of integers in } K$$
$$M_K = \text{the set of maximal ideals of } O_K$$
$$A = \text{a Dedekind domain whose fraction field is } K$$
$$P = \text{a set of maximal ideals of } A$$
$$\mathrm{Id}_P = \text{the monoid of nonzero ideals of } A \text{ supported at } P$$
$$\mathfrak{f} = \text{a cycle (or modulus) on } K$$
$$\mathfrak{f}_P = \text{the part of } \mathfrak{f} \text{ supported at } P$$
$$\mathfrak{f}^P = \text{the part of } \mathfrak{f} \text{ supported away from } P$$
$$\mathfrak{f}_{\mathrm{fin}} = \text{the part of } \mathfrak{f} \text{ supported at the finite primes}$$
$$\mathfrak{f}_\infty = \text{the part of } \mathfrak{f} \text{ supported at the real places}$$
$$\mathrm{Id}_P(\mathfrak{f}) = \text{the submonoid of } \mathrm{Id}_P \text{ of ideals prime to } \mathfrak{f}_{\mathrm{fin}}$$
$$\mathrm{Cl}(\mathfrak{f}) = \text{the ray class group of } K \text{ of conductor } \mathfrak{f}$$
$$\mathrm{Cl}_P(\mathfrak{f}) = \text{the image of the canonical map } \mathrm{Id}_P(\mathfrak{f}) \to \mathrm{Cl}(\mathfrak{f})$$
$$R^\circ = R \text{ viewed as a monoid under multiplication, for any ring } R$$

Observe that, up to canonical isomorphism, the constructions above depend only on the places of K corresponding to P, and so they depend on A only in that these places must come from maximal ideals of A. Therefore we can take $A = O_K$ without changing anything above.

4.1. *Structure of the ray class monoid.* There is a bijection

$$(4.1.6) \qquad \coprod_{\mathfrak{d} \in \mathrm{Id}_P, \, \mathfrak{d} \mid \mathfrak{f}} \mathrm{Cl}_P(\mathfrak{f}\mathfrak{d}^{-1}) \xrightarrow{\sim} \mathrm{DR}_P(\mathfrak{f}),$$

sending an ideal class $[\mathfrak{a}] \in \mathrm{Cl}_P(\mathfrak{f}\mathfrak{d}^{-1})$ in the summand of index $\mathfrak{d}$ to the class $[\mathfrak{d}\mathfrak{a}] \in \mathrm{DR}_P(\mathfrak{f})$. Thus we have

$$(4.1.7) \qquad \coprod_{\mathfrak{d} \in \mathrm{Id}_P, \, \mathfrak{d} \mid \mathfrak{f}} [\mathfrak{d}]\mathrm{Cl}_P(\mathfrak{f}\mathfrak{d}^{-1}) = \mathrm{DR}_P(\mathfrak{f}).$$

The multiplication law on $\mathrm{DR}_P(\mathfrak{f})$ is given in terms of the left-hand side by the formula

$$(4.1.8) \qquad [\mathfrak{d}][\mathfrak{a}] \cdot [\mathfrak{d}'][\mathfrak{a}'] = [\mathfrak{d}''][\mathfrak{a}''],$$

where $\mathfrak{d}'' = \gcd(\mathfrak{d}\mathfrak{d}', \mathfrak{f})$ and $\mathfrak{a}''$ satisfies $\mathfrak{d}''\mathfrak{a}'' = \mathfrak{d}\mathfrak{a}\mathfrak{d}'\mathfrak{a}'$. It follows, for example, that the submonoid $\mathrm{DR}_P(\mathfrak{f})^* \subseteq \mathrm{DR}_P(\mathfrak{f})$ of invertible elements agrees with the part of the ray class group supported at P:

$$\mathrm{DR}_P(\mathfrak{f})^* = \mathrm{Cl}_P(\mathfrak{f}).$$

When P is Chebotarev dense, we have $\mathrm{Cl}_P(\mathfrak{f}) = \mathrm{Cl}(\mathfrak{f})$, and so the invertible part of $\mathrm{DR}_P(\mathfrak{f})$ is independent of P. Observe however that this is not the case for the noninvertible part. For example, if $K = \mathbb{Q}$ and $\mathfrak{f} = (n)\infty$, then we have

$$(4.1.9) \qquad \mathrm{DR}_P(\mathfrak{f}) = (\mathbb{Z}/n_P\mathbb{Z})^\circ \times (\mathbb{Z}/n^P\mathbb{Z})^*,$$

where n_P is the factor of n supported at P and n^P is that supported away from P. The invertible part is $(\mathbb{Z}/n_P\mathbb{Z})^* \times (\mathbb{Z}/n^P\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z})^*$, which does not depend on P, but the non-invertible part does.

4.2.   *Change of conductor.* Suppose $\mathfrak{f} \mid \mathfrak{f}'$. Then we have the implication

$$\mathfrak{b} \sim_{\mathfrak{f}'} \mathfrak{c} \Rightarrow \mathfrak{b} \sim_{\mathfrak{f}} \mathfrak{c}.$$

which induces a monoid map

$$(4.2.10) \qquad \mathrm{DR}_P(\mathfrak{f}') \to \mathrm{DR}_P(\mathfrak{f}),$$

which we call the canonical map.

There is also a map in the other direction. Write $\mathfrak{f}' = \mathfrak{f}\mathfrak{a}$. Then by the equivalence

$$\mathfrak{b} \sim_{\mathfrak{f}} \mathfrak{c} \Leftrightarrow \mathfrak{a}\mathfrak{b} \sim_{\mathfrak{a}\mathfrak{f}} \mathfrak{a}\mathfrak{c},$$

there is a well-defined injective map

$$(4.2.11) \qquad \mathrm{DR}_P(\mathfrak{f}) \longrightarrow \mathrm{DR}_P(\mathfrak{f}'), \quad [\mathfrak{b}] \mapsto [\mathfrak{a}\mathfrak{b}].$$

It is not a monoid map, but it is an equivariant map of $\mathrm{DR}_P(\mathfrak{f}')$-sets. The composition with the canonical projection $\mathrm{DR}_P(\mathfrak{f}') \to \mathrm{DR}_P(\mathfrak{f})$ on either the left or the right, is given by multiplication by the class of $\mathfrak{a}$.

We conclude this section with two more descriptions of $\mathfrak{f}$-equivalence and the ray class monoid, although they only have small parts in this paper. The first is the one that appears in Deligne–Ribet [11], and a form of the second was pointed out to us by Bora Yalkinoglu.

Proposition 4.3. *Two ideals $\mathfrak{a}, \mathfrak{b}$ of O_K are $\mathfrak{f}$-equivalent if and only if $\mathfrak{a} = x\mathfrak{b}$ for some element $x \in 1 + \mathfrak{f}_{\mathrm{fin}}\mathfrak{b}^{-1}$ which is positive at all real places dividing $\mathfrak{f}$.*

Proof. Let $\mathfrak{d} = \gcd(\mathfrak{f}, \mathfrak{b})$. By definition, we have $\mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{b}$ if and only if there exists an element $x \in K^*$ satisfying the following:

  (1) $\mathfrak{a}\mathfrak{d}^{-1} = x\mathfrak{b}\mathfrak{d}^{-1}$
  (2) $x \equiv 1 \bmod \mathfrak{p}^{n_{\mathfrak{p}}}$, where $n_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}\mathfrak{d}^{-1})$, whenever $n_{\mathfrak{p}} \geqslant 1$
  (3) x is positive at all real places dividing $\mathfrak{f}\mathfrak{d}^{-1}$.

Observe that (1) is equivalent to $\mathfrak{a} = x\mathfrak{b}$ and that (3) is equivalent to the positivity condition in the statement of the proposition. It is therefore enough to show that, under (1), condition (2) is equivalent to $x \in 1 + \mathfrak{f}_{\mathrm{fin}}\mathfrak{b}^{-1}$, or equivalently to the condition that that for all $\mathfrak{p}$, we have $x \equiv 1 \bmod \mathfrak{p}^{m_{\mathfrak{p}}}$, where $m_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}\mathfrak{b}^{-1})$. So fix a prime $\mathfrak{p}$. In the case $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}) \geqslant \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})$, we have $n_{\mathfrak{p}} = m_{\mathfrak{p}}$ and so this condition is indeed equivalent to (2).

Now consider the remaining case $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}) < \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})$. Then we have $n_{\mathfrak{p}} = 0$ and $m_{\mathfrak{p}} < 0$. Because $n_{\mathfrak{p}} = 0$, condition (2) is vacuous. Therefore it is enough to show that $x \equiv 1 \bmod \mathfrak{p}^{m_{\mathfrak{p}}}$ necessarily holds. Since $\gcd(\mathfrak{f}, \mathfrak{b}) = \gcd(\mathfrak{f}, \mathfrak{a})$, we have $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}) < \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ and hence

$$\mathrm{ord}_{\mathfrak{p}}(x - 1) \geqslant \min\{\mathrm{ord}_{\mathfrak{p}}(x), 0\} = \min\{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}^{-1}), 0\} \geqslant \min\{m_{\mathfrak{p}}, 0\} = m_{\mathfrak{p}}.$$

$\square$

Proposition 4.4. *Assume that P is Chebotarev dense. Then there is an isomorphism*

$$(4.4.12) \qquad (O_K/\mathfrak{f}_P)^{\circ} \oplus_{(O_K/\mathfrak{f}_P)*} \mathrm{Cl}(\mathfrak{f}) \overset{\sim}{\longrightarrow} \mathrm{DR}_P(\mathfrak{f}),$$

which is given by the canonical inclusion $\mathrm{Cl}(\mathfrak{f}) \to \mathrm{DR}_P(\mathfrak{f})$ on the second factor and which on the first factor sends the residue class of any element $x \in O_K$ with $(x) \in \mathrm{Id}_P$ to the class $[(x)] \in \mathrm{DR}_P(\mathfrak{f})$.

The notation $A \oplus_G B$ above refers to the push out in the category of commutative monoids, which when G is a group is the quotient of $A \oplus B = A \times B$ by the action of G given by $g \cdot (a, b) = (ga, g^{-1}b)$.

Proof. First observe that this morphism is well defined. Indeed, any element $x \in (O_K/\mathfrak{f}_P)^*$ is the image of an element $\tilde{x} \in O_K$ relatively prime to $\mathfrak{f}_P$, and its class $[(\tilde{x})]$ in $\mathrm{DR}_P(\mathfrak{f})$ is indeed the image of its class in the ray class group $\mathrm{Cl}(\mathfrak{f})$.

The fact that this morphism is an isomorphism is a consequence of the following equalities, which will be justified below, and where $\mathfrak{d}$ runs over Id_P with $\mathfrak{d} \mid \mathfrak{f}$:

$$(4.4.13) \qquad \mathrm{DR}_P(\mathfrak{f}) = \coprod_{\mathfrak{d}}[\mathfrak{d}]\mathrm{Cl}_P(\mathfrak{f}\mathfrak{d}^{-1}) = \coprod_{\mathfrak{d}}[\mathfrak{d}]\mathrm{Cl}(\mathfrak{f}\mathfrak{d}^{-1})$$

Let us simplify the right-hand side further and show

$$(4.4.14) \qquad [\mathfrak{d}]\mathrm{Cl}(\mathfrak{f}\mathfrak{d}^{-1}) = \mathrm{Cl}(\mathfrak{f})/(1 + \mathfrak{f}_{\mathrm{fin}}\mathfrak{d}^{-1}/\mathfrak{f}_{\mathrm{fin}}).$$

We use the adèlic description of ray class groups: $\mathrm{Cl}(\mathfrak{m}) = \mathbb{A}_K^*/K^*U_{\mathfrak{m}}$. Then we have the exact sequence

$$U_{\mathfrak{f}\mathfrak{d}^{-1}}/U_{\mathfrak{f}} \longrightarrow \mathrm{Cl}(\mathfrak{f}) \longrightarrow \mathrm{Cl}(\mathfrak{f}\mathfrak{d}^{-1}) \longrightarrow 1.$$

Since the archimedean parts of $\mathfrak{f}\mathfrak{d}^{-1}$ and $\mathfrak{f}$ agree, we have

$$U_{\mathfrak{f}\mathfrak{d}^{-1}}/U_{\mathfrak{f}} = U_{\mathfrak{f}_{\mathrm{fin}}\mathfrak{d}^{-1}}/U_{\mathfrak{f}_{\mathrm{fin}}} = 1 + \mathfrak{f}_{\mathrm{fin}}\mathfrak{d}^{-1}/\mathfrak{f}_{\mathrm{fin}}.$$

Equation (4.4.14) follows.

Combining this with (4.4.13), we have

$$\begin{aligned}
\mathrm{DR}_P(\mathfrak{f}) &= \coprod_{\mathfrak{d}}[\mathfrak{d}]\mathrm{Cl}(\mathfrak{f})/(1 + \mathfrak{f}_{\mathrm{fin}}\mathfrak{d}^{-1}/\mathfrak{f}_{\mathrm{fin}}) \\
&= \coprod_{\mathfrak{d}}[\mathfrak{d}](O_K/\mathfrak{f}_{\mathrm{fin}}\mathfrak{d}^{-1})^* \oplus_{(O_K/\mathfrak{f}_{\mathrm{fin}})^*} \mathrm{Cl}(\mathfrak{f}) \\
&= \Big(\coprod_{\mathfrak{d}}[\mathfrak{d}](O_K/\mathfrak{f}_{\mathrm{fin}}\mathfrak{d}^{-1})^*\Big) \oplus_{(O_K/\mathfrak{f}_{\mathrm{fin}})^*} \mathrm{Cl}(\mathfrak{f}) \\
&= \big((O_K/\mathfrak{f}_P)^\circ \times (O_K/\mathfrak{f}^P)^*\big) \oplus_{(O_K/\mathfrak{f}_{\mathrm{fin}})^*} \mathrm{Cl}(\mathfrak{f}) \\
&= \big((O_K/\mathfrak{f}_P)^\circ \times (O_K/\mathfrak{f}^P)^*\big) \oplus_{(O_K/\mathfrak{f}_P)^* \times (O_K/\mathfrak{f}^P)^*} \mathrm{Cl}(\mathfrak{f}) \\
&= (O_K/\mathfrak{f}_P)^\circ \oplus_{(O_K/\mathfrak{f}_P)^*} \mathrm{Cl}(\mathfrak{f}).
\end{aligned}$$

$\square$

4.5. *Examples.* If K has class number 1 and P is still Chebotarev dense, then we have

$$(4.5.15) \qquad \mathrm{DR}_P(\mathfrak{f}) = (O_K/\mathfrak{f}_P)^\circ \oplus_{O_{K,\mathfrak{f}_\infty}^*} (O_K/\mathfrak{f}_{\mathrm{fin}}^P)^*,$$

where $O_{K,\mathfrak{f}_\infty}^*$ is the subgroup of O_K^* consisting of units which are positive at all places dividing $\mathfrak{f}_\infty$. At a different extreme, if K is arbitrary but $P = M_K$, then in the limit we have

$$(4.5.16) \qquad \varprojlim_{\mathfrak{f}} \mathrm{DR}_P(\mathfrak{f}) = \hat{O}_K^\circ \oplus_{\hat{O}_K^*} G_K^{\mathrm{ab}}.$$

If K has class number 1 and $P = M_K$, then we have

$$\mathrm{DR}_P(\mathfrak{f}) = (O_K/\mathfrak{f}_{\mathrm{fin}})^\circ/O_{K,\mathfrak{f}_\infty}^*.$$

5. GLOBAL ARGUMENTS

The purpose of this section is to prove theorem 1.2 from the introduction. It will follow immediately from proposition 5.2 and theorem 5.5 below.

We continue with the notation of the previous section. Also fix the following notation:

$E = $ a finite étale K-algebra with a $\Lambda_{A,P}$-structure

$S = \mathrm{Hom}_K(E, K^{\mathrm{sep}})$, with its continuous action of $G_K \times \mathrm{Id}_P$.

Define $\mathfrak{r} \in \mathrm{Id}_P$ by setting

$$(5.0.17) \qquad \mathrm{ord}_{\mathfrak{p}}(\mathfrak{r}) = \inf\{i \geqslant 0 \colon \ \mathfrak{p}^{i+1}S = \mathfrak{p}^i S\}$$

for each prime $\mathfrak{p} \in P$. This is well defined because $\mathfrak{p}S = S$ whenever $\mathfrak{p}$ is unramified in B, by proposition 3.1.

Lemma 5.1. *Assume that E has an integral $\Lambda_{A,P}$-model B. Let $\mathfrak{d}$ be an ideal in Id_P, and put $\mathfrak{b} = \gcd(\mathfrak{d}, \mathfrak{r})$. Then $\mathfrak{d}S$ equals $\mathfrak{b}S$, and this G_K-set is unramified at all primes dividing $\mathfrak{d}\mathfrak{b}^{-1}$.*

Proof. Observe that for any prime $\mathfrak{p} \mid \mathfrak{d}\mathfrak{b}^{-1}$, we have $\mathfrak{p}\mathfrak{b}S = \mathfrak{b}S$. Indeed, we have $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{r})$ and hence $\mathfrak{p}^{1+\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})}S = \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})}S$, by the definition of $\mathfrak{r}$. Then $\mathfrak{p}\mathfrak{b}S = \mathfrak{b}S$ follows.

This implies by induction that $\mathfrak{d}S = \mathfrak{b}S$. It also implies that for each prime $\mathfrak{p} \mid \mathfrak{d}\mathfrak{b}^{-1}$, the action of $\mathfrak{p}$ on $\mathfrak{b}S = \mathfrak{d}S$ is bijective. Therefore by theorem 1.1(1), this G_K-set is unramified at all primes $\mathfrak{p} \mid \mathfrak{d}\mathfrak{b}^{-1}$. $\qquad\square$

Proposition 5.2. *If E has an integral $\Lambda_{A,P}$-model and P is Chebotarev dense, then the action of G_K on S factors through the abelianization of G_K.*

Proof. Let B be an integral $\Lambda_{A,P}$-model of E. For each prime $\mathfrak{p} \in P$ we consider the completion $A_{\mathfrak{p}}$, and its fraction field $K_{\mathfrak{p}}$. Then we obtain an $\Lambda_{A_{\mathfrak{p}},\mathfrak{p}}$-structure on the finite étale $K_{\mathfrak{p}}$-algebra $E_{\mathfrak{p}} = E \otimes_K K_{\mathfrak{p}}$, and then $B \otimes_A A_{\mathfrak{p}}$ is an integral $\Lambda_{A_{\mathfrak{p}},\mathfrak{p}}$-model of $E_{\mathfrak{p}}$. Fixing an embedding $K^{\mathrm{sep}} \to K_{\mathfrak{p}}^{\mathrm{sep}}$ for each $\mathfrak{p}$ we can view $G_{\mathfrak{p}}$ as a subgroup of G_K. The finite étale $K_{\mathfrak{p}}$-algebra $E_{\mathfrak{p}}$ then corresponds to the $G_{\mathfrak{p}}$-set that one gets by restricting the action of G_K on S to $G_{\mathfrak{p}}$.

Now let $\bar{G}$ be the image of the action map $G_K \to \mathrm{Map}(S, S)$. Because P is Chebotarev dense, for each $g \in \bar{G}$ there is a prime $\mathfrak{p} = \mathfrak{p}_g$ in P such that

(1) B is unramified at $\mathfrak{p}$,
(2) the image of $F_{\mathfrak{p}} \in G_{\mathfrak{p}}/I_{\mathfrak{p}}$ under the induced map $G_{\mathfrak{p}}/I_{\mathfrak{p}} \to \bar{G}$ is g.

By proposition 3.1, the action of g on S is the same as the action of $\mathfrak{p}_g$ on S. But by the definition of $\Lambda_{A,P}$-structure, the $\mathfrak{p}_g$ commute with each other. Therefore $\bar{G}$ is abelian. $\qquad\square$

5.3.   *Conductors.* By class field theory, any continuous action of the abelianization of G_K on a finite discrete set T factors, by the Artin map, through the ray class group $\mathrm{Cl}(c(T))$ for a minimal cycle $c(T)$ on K, which we call the conductor of T.

Lemma 5.4. *Assume that E has an integral $\Lambda_{A,P}$-model B and that the action of G_K on S factors through its abelianization. Let $\mathfrak{f}$ be a cycle on K, and let $\mathfrak{r}$ be as in (5.0.17). Then following are equivalent:*

(1) *the action of $G_K \times \mathrm{Id}_P$ on S factors through an action of $\mathrm{DR}_P(\mathfrak{f})$,*
(2) *$\mathfrak{r}$ divides $\mathfrak{f}$, and for each ideal $\mathfrak{d} \mid \mathfrak{f}$ we have $c(\mathfrak{d}S) \mid \mathfrak{f}\mathfrak{d}^{-1}$,*
(3) *$\mathfrak{r}$ divides $\mathfrak{f}$, and for each ideal $\mathfrak{d} \mid \mathfrak{r}$ we have $c(\mathfrak{d}S) \mid \mathfrak{f}\mathfrak{d}^{-1}$,*
(4) *the least common multiple $\mathrm{lcm}_{\mathfrak{d}\mid\mathfrak{r}}\big(\mathfrak{d}\, c(\mathfrak{d}S)\big)$ divides $\mathfrak{f}$.*

Proof. (1)$\Rightarrow$(2): To show $\mathfrak{r} \mid \mathfrak{f}$, we will show that for all $\mathfrak{p} \in P$, we have $\mathfrak{p}^n S \subseteq \mathfrak{p}^{n+1}S$, where $n = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f})$. Using the decomposition (4.1.7), we see $[\mathfrak{p}]^{n+1}\mathrm{DR}_P(\mathfrak{f}) = [\mathfrak{p}]^n \mathrm{DR}_P(\mathfrak{f})$ and hence $[\mathfrak{p}]^n = [\mathfrak{p}]^{n+1}x$ for some $x \in \mathrm{DR}_P(\mathfrak{f})$. Then because the action of Id_P is assumed to factor through $\mathrm{DR}_P(\mathfrak{f})$, we have $\mathfrak{p}^n S = \mathfrak{p}^{n+1}xS \subseteq \mathfrak{p}^{n+1}S$.

Second, the condition $c(\mathfrak{d}S) \mid \mathfrak{f}\mathfrak{d}^{-1}$ of (2) is equivalent to the condition that the action of G_K on $\mathfrak{d}S$ factors through the Artin map $G_K \to \mathrm{Cl}(\mathfrak{f}\mathfrak{d}^{-1})$. But this holds by the assumption (1) and the decomposition (4.1.7).

(2)$\Rightarrow$(1): Consider an element $(\sigma, \mathfrak{a}) \in G_K \times \mathrm{Id}_P$. We will show its action on S depends only on its class in $\mathrm{DR}_P(\mathfrak{f})$. First observe that by the assumption

$c(\mathfrak{d}S) \mid \mathfrak{f}\mathfrak{d}^{-1}$, taken when $\mathfrak{d} = (1)$, we have $c(S) \mid \mathfrak{f}$. This implies that the action of G_K factors through the Artin map $G_K \to \mathrm{Cl}(\mathfrak{f})$, and so it is enough to show that the action of $\mathfrak{a}$ depends only on its class $[\mathfrak{a}] \in \mathrm{DR}_P(\mathfrak{f})$. Now put $\mathfrak{d} = \gcd(\mathfrak{a}, \mathfrak{f})$ and $\mathfrak{a}' = \mathfrak{a}\mathfrak{d}^{-1}$. Then we have $\mathfrak{a}' \in \mathrm{Id}_P(\mathfrak{f})$. Therefore, because of (4.1.7), it is enough to show that the action of $\mathfrak{a}' \in \mathrm{Id}_P(\mathfrak{f})$ on $\mathfrak{d}S$ depends only on its class $[\mathfrak{a}'] \in \mathrm{Cl}_P(\mathfrak{f}\mathfrak{d}^{-1})$. In particular, it is enough to show

$$(5.4.18) \qquad\qquad \mathfrak{a}'\mathfrak{d}s = F_{\mathfrak{a}'}\mathfrak{d}s,$$

for all $s \in S$, where $F_{\mathfrak{a}'} \in G_K$ is an element mapping to $[\mathfrak{a}']$ under the Artin map $G_K \to \mathrm{Cl}(\mathfrak{f})$. To do this, it is enough to consider the case where $\mathfrak{a}'$ is a prime $\mathfrak{p} \in \mathrm{Id}_P(\mathfrak{f})$. Now by our assumption $\mathfrak{r} \mid \mathfrak{f}$, we have $\mathfrak{p} \nmid \mathfrak{r}$ and hence $\mathfrak{p}$ acts bijectively on S. Therefore by theorem 1.1, we have

$$\mathfrak{p}s = F_{\mathfrak{p}}s,$$

for all $s \in S$. This implies (5.4.18) and hence (1).

(2) $\Leftrightarrow$ (3): The implication (2) $\Rightarrow$ (3) is clear. So consider the other direction. Given an ideal $\mathfrak{d} \mid \mathfrak{f}$, let $\mathfrak{b}$ denote $\gcd(\mathfrak{d}, \mathfrak{r})$. Then by lemma 5.1, we have equivalences

$$c(\mathfrak{d}S) \mid \mathfrak{f}\mathfrak{d}^{-1} \Leftrightarrow c(\mathfrak{b}S) \mid \mathfrak{f}\mathfrak{d}^{-1} \Leftrightarrow c(\mathfrak{b}S) \mid \mathfrak{f}\mathfrak{d}^{-1}\mathfrak{d}\mathfrak{b}^{-1} \Leftrightarrow c(\mathfrak{b}S) \mid \mathfrak{f}\mathfrak{b}^{-1}.$$

Therefore since $\mathfrak{b}$ is a divisor of $\mathfrak{r}$, the condition $c(\mathfrak{d}S) \mid \mathfrak{f}\mathfrak{d}^{-1}$ holds for all $\mathfrak{d} \mid \mathfrak{f}$ if it holds for all $\mathfrak{d} \mid \mathfrak{r}$.

(3) $\Leftrightarrow$ (4): Clear. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Theorem 5.5. *Let $\mathfrak{f}$ be a cycle on K. Then the action of $G_K \times \mathrm{Id}_P$ on S factors (necessarily uniquely) through the map $G_K \times \mathrm{Id}_P \longrightarrow \mathrm{DR}_P(\mathfrak{f})$ of (1.1.2) if and only if the following hold:*

(1) *the action of G_K on S factors through its abelianization,*
(2) *$\mathrm{lcm}_{\mathfrak{d}\mid\mathfrak{r}}\big(\mathfrak{d}\, c(\mathfrak{d}S)\big)$ divides $\mathfrak{f}$,*
(3) *E has an integral $\Lambda_{A,P}$-model.*

If P is Chebotarev dense, then condition (1) can be removed.

Proof. If (1)–(3) hold, then by lemma 5.4, the action of $G_K \times \mathrm{Id}_P$ on S factors through $\mathrm{DR}_P(\mathfrak{f})$; and if P is Chebotarev dense, then (1) can be removed because, by proposition 5.2, it follows from (3).

Let us now consider the converse direction. Suppose that the $G_K \times \mathrm{Id}_P$-action on S factors through $\mathrm{DR}_P(\mathfrak{f})$. Then (1) holds because $\mathrm{DR}_P(\mathfrak{f})$ is commutative. Further, (3) implies (2) by lemma 5.4. Therefore it is enough to show (3).

For each $\mathfrak{p} \in P$, let $B_{\mathfrak{p}}$ denote the maximal sub-$\Lambda_{A_{\mathfrak{p}},\mathfrak{p}}$-ring of $E \otimes_K K_{\mathfrak{p}}$ which is finite over $A_{\mathfrak{p}}$. As mentioned in 3.4, it always exists. We will show that $B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} K_{\mathfrak{p}}$ agrees with $E_{\mathfrak{p}}$. To do this, it is enough to show that $E \otimes_K K_{\mathfrak{p}}$ has an integral $\Lambda_{A_{\mathfrak{p}},\mathfrak{p}}$-model. So write $\mathfrak{f} = \mathfrak{p}^n\mathfrak{f}'$ with $n = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f})$. Then $[\mathfrak{p}^k] \in [\mathfrak{p}^n]\mathrm{Cl}(\mathfrak{f}') \subseteq \mathrm{DR}(\mathfrak{f})$ for all $k \geqslant n$. This implies, by say (4.1.8), that the action of $\mathfrak{p}$ on $\bigcap_i \mathfrak{p}^iS = \mathfrak{p}^nS$ is given by the Artin symbol of $[\mathfrak{p}] \in \mathrm{Cl}(\mathfrak{f}')$, which by our local result, theorem 1.1, guarantees existence of an integral $\Lambda_{A_{\mathfrak{p}},\mathfrak{p}}$-model.

Now let R denote the integral closure of A in E, and let B denote the set of elements $a \in R$ such that the image of a in $E \otimes_K K_{\mathfrak{p}}$ lies in $B_{\mathfrak{p}}$ for all $\mathfrak{p} \in P$. We will show that B is what we seek, an integral $\Lambda_{A,P}$-model for E.

For all $\mathfrak{p} \nmid \mathfrak{f}$, we are in the unramified case, and so $B_{\mathfrak{p}}$ is $R \otimes_A \mathcal{O}_{\mathfrak{p}}$, by proposition 3.1. It follows that B is of finite index in R. Therefore, since R is finite and flat over A and we have $E = R \otimes_A K$, the same hold for B. Further, B is closed under all $\psi_{\mathfrak{q}}$ with $\mathfrak{q} \in P$. Indeed it is enough to show $\psi_{\mathfrak{q}}(B_{\mathfrak{p}}) \subseteq B_{\mathfrak{p}}$ for all $\mathfrak{p}, \mathfrak{q} \in P$; and this holds because is a $\psi_{\mathfrak{q}}(B_{\mathfrak{p}})$ sub-$\Lambda_{A_{\mathfrak{p}},\mathfrak{p}}$-ring of $E_{\mathfrak{p}}$ which is finite over $A_{\mathfrak{p}}$, and so it is contained in the maximal one $B_{\mathfrak{p}}$. Finally, for each $\mathfrak{p} \in P$, the

induced endomorphism $\psi_{\mathfrak{p}}$ of B is a Frobenius lift, because $B \otimes_A \mathcal{O}_{\mathfrak{p}}$ is a $\Lambda_{A_{\mathfrak{p}}, \mathfrak{p}}$-ring. Therefore B is an integral $\Lambda_{A,P}$-model for E. This establishes (3) and, hence, (1) and (2) as explained above. $\qquad\square$

Corollary 5.6. *If P is Chebotarev dense, there is a contravariant equivalence between the category of finite étale $\Lambda_{A,P}$-rings over K which admit an integral model and the category of finite discrete sets with a continuous action of the profinite monoid* $\lim_{\mathfrak{f}} \mathrm{DR}_P(\mathfrak{f})$.

Part 2. **Periodic loci and explicit class field theory**

6. Λ-SCHEMES

Below X will denote a flat A-scheme.

6.1. *Λ-schemes.* Let $\mathfrak{p}$ be a maximal ideal of A. As in the affine case, the fiber $X \times_{\mathrm{Spec}\, A} \mathrm{Spec}\, k(\mathfrak{p})$ has a natural $k(\mathfrak{p})$-scheme endomorphism $F_{\mathfrak{p}}$ which is the identity map on the underlying topological space and such that for each affine open subscheme $\mathrm{Spec}\, B$, the induced the endomorphism of B is the affine Frobenius map $x \mapsto x^{N(\mathfrak{p})}$.

Let $\mathrm{End}_A(X)$ denote the monoid of A-scheme endomorphisms of X. An endomorphism $\psi \in \mathrm{End}_A(X)$ is said to be a *Frobenius lift* at $\mathfrak{p}$ if the induced endomorphism on the fiber $X \times_{\mathrm{Spec}\, A} \mathrm{Spec}\, k(\mathfrak{p})$ agrees with $F_{\mathfrak{p}}$. A $\Lambda_{A,P}$-*structure* on a flat A-scheme X is defined to be a set map $P \to \mathrm{End}_A(X)$, denoted $\mathfrak{p} \mapsto \psi_{\mathfrak{p}}$ such that $\psi_{\mathfrak{p}}$ is a Frobenius lift at $\mathfrak{p}$ for each $\mathfrak{p} \in P$ and such that $\psi_{\mathfrak{p}} \circ \psi_{\mathfrak{q}} = \psi_{\mathfrak{q}} \circ \psi_{\mathfrak{p}}$ for all $\mathfrak{p}, \mathfrak{q} \in P$. We will call an A-scheme with $\Lambda_{A,P}$-structure a $\Lambda_{A,P}$-*scheme*. (When X is not flat over A, this definition still makes sense; but as in the affine case, it is not well behaved. In general, one should define it to be an action of the Witt vector monad $W_{A,P}^*$ as in the introduction to [4]. We will only consider Λ-structures on flat schemes in this paper; so the simplified definition above is good enough here.)

For any ideal $\mathfrak{a} \in \mathrm{Id}_P$ with prime factorization $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, let $\psi_{\mathfrak{a}}$ denote the composition $\psi_{\mathfrak{p}_1} \circ \cdots \circ \psi_{\mathfrak{p}_n}$. It is independent of the order of the factors because the operators $\psi_{\mathfrak{p}}$ commute with each other.

A morphism $X \to Y$ of $\Lambda_{A,P}$-schemes is a morphism $f \colon X \to Y$ of A-schemes such that $f \circ \psi_{\mathfrak{p}} = \psi_{\mathfrak{p}} \circ f$, for all $\mathfrak{p} \in P$. In this way, $\Lambda_{A,P}$-schemes form a category.

6.2. *Examples.* The multiplicative group $X = \mathbb{G}_{\mathrm{m}}$ over A has a $\Lambda_{A,P}$-structure given by $\psi_{\mathfrak{p}}(x) = x^{N(\mathfrak{p})}$. This extends uniquely to $\Lambda_{A,P}$-structures on $\mathbb{A}^1$ and $\mathbb{P}^1$. More generally, projective n-space $\mathbb{P}^n$ has a $\Lambda_{A,P}$-structure where $\psi_{\mathfrak{p}}$ raises the homogeneous coordinates to the $N(\mathfrak{p})$ power.

Any product of $\Lambda_{A,P}$-schemes is again a $\Lambda_{A,P}$-scheme, where the ψ-operators act componentwise. In a similar way, coproducts of $\Lambda_{A,P}$-schemes are $\Lambda_{A,P}$-schemes.

7. PERIODIC Λ-SCHEMES

Let $\mathfrak{f}$ be a cycle on K.

7.1. *Periodic Λ-schemes.* We will say that a $\Lambda_{A,P}$-scheme X is $\mathfrak{f}$-*periodic* if for all $\mathfrak{f}$-equivalent ideals $\mathfrak{a}, \mathfrak{b} \in \mathrm{Id}_P$, the two maps $\psi_{\mathfrak{a}}, \psi_{\mathfrak{b}} \colon X \to X$ are equal—in other words, the monoid map $\mathrm{Id}_P \to \mathrm{End}_A(X)$ factors through $\mathrm{DR}_P(\mathfrak{f})$.

7.2. *Examples.* Suppose that $A = \mathbb{Z}$, $P = M_{\mathbb{Q}}$, and $\mathfrak{f} = (n)\infty$ with n positive. Then $\mathfrak{f}$-periodicity means that $\psi_{(a)} = \psi_{(a+n)}$ for all integers $a \geqslant 1$. In other words, the sequence of Frobenius lifts $\psi_{(a)}$ is periodic in $a \geqslant 1$ with period dividing n, which is the reason for the name. Representation rings of finite groups, with their usual λ-ring structure in algebraic K-theory, are periodic. In fact, periodicity was first introduced in this context by Davydov [10].

On the other hand, when A is general but $\mathfrak{f}$ is (1), then $\mathfrak{f}$-periodicity means that $\psi_{\mathfrak{a}}$ depends only on the class of $\mathfrak{a}$ in the class group $\mathrm{Cl}(1)$. If $\mathfrak{f}$ is instead the product of all real places, then it means that $\psi_{\mathfrak{a}}$ depends only on the class of $\mathfrak{a}$ in the narrow class group $\mathrm{Cl}(\mathfrak{f})$. In particular, if either of these class groups is trivial, then every $\psi_{\mathfrak{a}}$ is the identity map, and so any (flat) A-scheme has at most one $\Lambda_{A,P}$-structure with that type of periodicity.

If we are in the intersection of the two cases above, a (1)-periodic $\Lambda_{\mathbb{Z},P}$-ring is just a λ-ring in which all the Adams operations are the identity. Elliott [12] has proved that this is equivalent to being a binomial ring, a notion which dates back to Berthelot's exposé in SGA6 [1], p. 323.

Proposition 7.3. *Let X be a separated flat $\mathfrak{f}$-periodic $\Lambda_{A,P}$-scheme of finite type.*
  (1) *If P is infinite, then X is affine, reduced, and quasi-finite over A, with étale generic fiber X_K.*
  (2) *If P is Chebotarev dense, then the generic fiber's function algebra $\mathcal{O}(X_K)$ is a product of subextensions of the ray class field $K(\mathfrak{f})$.*

Proof. (1): Let us first show that X is reduced and quasi-finite over A. By periodicity, for every $\mathfrak{p} \in P$ satisfying $\mathfrak{p} \nmid \mathfrak{f}$, the Frobenius lift $\psi_{\mathfrak{p}}$ on X is an automorphism of finite order. Therefore the Frobenius map $F_{\mathfrak{p}}$ on the fiber $k(\mathfrak{p}) \otimes X$ is an automorphism of finite order, and so the fiber is both geometrically reduced and finite over $k(\mathfrak{p})$. Since P is infinite and since the set of prime ideals of A with geometrically reduced fibers forms a constructible subset of $\mathrm{Spec}\, A$, by EGA IV (9.7.7) [13], the generic fiber $X \times_{\mathrm{Spec}\, A} \mathrm{Spec}\, K$ must be geometrically reduced. Similarly, since infinitely many fibers are finite, the generic fiber is also finite, by EGA IV (9.2.6.2) [13]. We now use the flatness of X over A to pass from the generic fiber to all of X. It is clear that flatness implies X is reduced. For quasi-finiteness, apply EGA IV (14.2.4) [13].

Therefore X is reduced and is quasi-finite over A. Affineness then follows from Zariski's Main Theorem, as we now explain. Let D denote the integral closure of A in $\mathcal{O}(X)$. Let X' denote $\mathrm{Spec}\, D$, called the normalization of A in X in the Stacks Project [2, Tag 035H]. Then $\mathcal{O}(X)$ is reduced and is flat over A, and hence so is D. It is also finite over A, by [2, Tag 03GR]. Since X is quasi-finite, the canonical map $X \to X'$ is an open immersion by Zariski's Main Theorem [2, Tag 03GW]. Finally, since X' is finite flat over A, which is a Dedekind domain, its Krull dimension is 1 and hence its open subscheme X must be affine [2, Tag 09N9].

Thus we can write $X = \mathrm{Spec}\, B$, where B is an $\mathfrak{f}$-periodic $\Lambda_{A,P}$-ring which is reduced and is flat, quasi-finite, and of finite type over A. It follows that $K \otimes_A B$ is étale over K.

(2): It follows from statement (1) that there is a nonzero element $t \in A$ such that $B[1/t]$ is a finite product $\prod_i D_i$, where each D_i is the integral closure of $A[1/t]$ in a finite extension L_i of K: Indeed, since B is of finite type over A and since $B \otimes_A K$ is finite over K, there is an element $t \in A$ such that $B[1/t]$ is finite flat over $A[1/t]$. Since B is reduced, so is $B[1/t]$, and hence the discriminant ideal of $B[1/t]$ over $A[1/t]$ is nonzero. Then by scaling t so that it lies in the discriminant ideal, and is nonzero, we may assume that $B[1/t]$ is finite étale over $A[1/t]$. It then follows that $B[1/t]$ is the integral closure of $A[1/t]$ in $K \otimes_A B$ and is hence of the required form.

Now let P_t denote the set of primes $\mathfrak{p}$ in P that do not divide t. Then we can consider P_t as a set of primes of $A[1/t]$; and since P is Chebotarev dense, so is P_t. Applying proposition 5.2 to the $\Lambda_{A[1/t],P_t}$-ring $B[1/t]$, we see each field $K \otimes_A D_i$ is an abelian extension of K. Since the Frobenius elements act on each D_i with period $\mathfrak{f}$, the conductor of $K \otimes_A D_i$ divides $\mathfrak{f}$. $\square$

7.4. *Ray class algebras.* These are Λ-ring analogues of the ray class fields of K.

We can view $\mathrm{DR}_P(\mathfrak{f})$ as a pointed $\mathrm{DR}_P(\mathfrak{f})$-set: the distinguished point is the identity element, and the action is translation. By theorem 5.5, the corresponding $\Lambda_{A,P}$-ring over K has an integral model. Define $R_{A,P}(\mathfrak{f})$, the *ray class algebra of conductor* $\mathfrak{f}$, to be the maximal $\Lambda_{A,P}$-order in this K-algebra. Thus we have
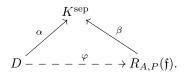
$$K \otimes_A R_{A,P}(\mathfrak{f}) = \prod_{\substack{\mathfrak{d} \in \mathrm{Id}_P \\ \mathfrak{d} | \mathfrak{f}_{\mathrm{fin}}}} K(\mathfrak{f}\mathfrak{d}^{-1}),$$

where $K(\mathfrak{f}\mathfrak{d}^{-1})$ is the ray class field of K with conductor $\mathfrak{f}\mathfrak{d}^{-1}$. Under this identification, the map $\beta\colon R_{A,P}(\mathfrak{f}) \to K^{\mathrm{sep}}$ coming from the distinguished point of $\mathrm{DR}_P(\mathfrak{f})$ is the projection to the component with $\mathfrak{d} = (1)$.

In our previous paper [7], we considered the case where $A = \mathbb{Z}$ and P is all maximal ideals. There we showed that the ray class algebra of conductor $(n)\infty$ is $\mathbb{Z}[x]/(x^n - 1)$, or more naturally, the group ring on the cyclic group $\mu_n(K^{\mathrm{sep}})$ of n-th roots of unity in K^{sep}.

Observe that the ray class algebra is not usually a domain, and in particular the map $\beta\colon R_{A,P}(\mathfrak{f}) \to K(\mathfrak{f})$ to the ray class field is not usually injective. Also, unlike the ray class field, it depends not only on $\mathfrak{f}$ but also on A and P. On the other hand, $K \otimes_A R_{A,P}(\mathfrak{f})$ is independent of A.

If P is Chebotarev dense, the ray class algebra $R_{A,P}(\mathfrak{f})$ satisfies the following maximality property: if D is a reduced finite flat $\mathfrak{f}$-periodic $\Lambda_{A,P}$-ring equipped with a map $\alpha\colon D \to K^{\mathrm{sep}}$ of A-algebras, then there is a unique map $\varphi\colon D \to R_{A,P}(\mathfrak{f})$ of $\Lambda_{A,P}$-rings making the following diagram commute:

$$
\begin{array}{ccc}
 & K^{\mathrm{sep}} & \\
 {}^{\alpha}\nearrow & & \nwarrow{}^{\beta} \\
 D \dashrightarrow{\ \varphi\ } & & R_{A,P}(\mathfrak{f}).
\end{array}
$$

This is simply because, under the anti-equivalence with $\mathrm{DR}_P(\mathfrak{f})$-sets, $R_{A,P}(\mathfrak{f})$ corresponds to $\mathrm{DR}_P(\mathfrak{f})$, which is the free $\mathrm{DR}_P(\mathfrak{f})$-set on one generator.

7.5. *Change of $\mathfrak{f}$.* Suppose $\mathfrak{f}' = \mathfrak{f}\mathfrak{a}$. Then the maps $\mathrm{DR}_P(\mathfrak{f}') \to \mathrm{DR}_P(\mathfrak{f})$ and $\mathrm{DR}_P(\mathfrak{f}) \longrightarrow \mathrm{DR}_P(\mathfrak{f}')$ of 4.2 induce an inclusion

$$(7.5.19) \qquad\qquad u\colon R_{A,P}(\mathfrak{f}) \longrightarrow R_{A,P}(\mathfrak{f}')$$

and a surjection

$$(7.5.20) \qquad\qquad v\colon R_{A,P}(\mathfrak{f}') \longrightarrow R_{A,P}(\mathfrak{f})$$

of $\Lambda_{A,P}$-rings, and the compositions $u \circ v$ and $u \circ v$ agree with the two $\psi_{\mathfrak{a}}$ endomorphisms.

In the case where $K = \mathbb{Q}$, P is all maximal ideals, $\mathfrak{f} = (n)\infty$, and $\mathfrak{f}' = (n')\infty$, these maps can be identified with the maps on group rings corresponding to the inclusion $\mu_n(K^{\mathrm{sep}}) \subseteq \mu_{n'}(K^{\mathrm{sep}})$, in the case of u, and the n'/n-th power map $\mu_{n'}(K^{\mathrm{sep}}) \to \mu_n(K^{\mathrm{sep}})$, in the case of v.

8. Periodic loci and abelian extensions

Let $\mathfrak{f}$ be a cycle on K. Let X be a separated (flat) $\Lambda_{A,P}$-scheme.

8.1. *Periodic locus $X(\mathfrak{f})$.* Define the $\mathfrak{f}$-periodic locus $X(\mathfrak{f})$ of X to be the scheme-theoretic intersection

$$X(\mathfrak{f}) = \bigcap_{\substack{\mathfrak{a},\mathfrak{b}\in\mathrm{Id}_P \\ \mathfrak{a}\sim_\mathfrak{f}\mathfrak{b}}} X(\psi_\mathfrak{a} = \psi_\mathfrak{b}),$$

where $X(\psi_\mathfrak{a} = \psi_\mathfrak{b})$ denotes the equalizer of the two maps $\psi_\mathfrak{a}, \psi_\mathfrak{b}\colon X \to X$. Since X is separated, $X(\mathfrak{f})$ is a closed subscheme. The functor $X(\mathfrak{f})$ represents is

$$X(\mathfrak{f})(C) = \{x \in X(C) : \psi_\mathfrak{a}(x) = \psi_\mathfrak{b}(x) \text{ for all } \mathfrak{a},\mathfrak{b} \in \mathrm{Id}_P \text{ with } \mathfrak{a} \sim_\mathfrak{f} \mathfrak{b}\}.$$

We emphasize that $X(\mathfrak{f})$ depends on P as well as $\mathfrak{f}$, although the notation does not reflect this.

Observe that $X(\mathfrak{f})$ is functorial in X. It also behaves well under change of $\mathfrak{f}$: if $\mathfrak{f}'$ is another cycle and $\mathfrak{f} \mid \mathfrak{f}'$, then we have

$$X(\mathfrak{f}) \subseteq X(\mathfrak{f}').$$

Finally, let $X(\mathfrak{f})_{\mathrm{fl}}$ denote the maximal A-flat subscheme of $X(\mathfrak{f})$. It is the closed subscheme of $X(\mathfrak{f})$ defined by the ideal sheaf of A-torsion elements. Although the actual periodic locus $X(\mathfrak{f})$ is more fundamental than $X(\mathfrak{f})_{\mathrm{fl}}$, for the purposes of this paper it is enough to consider $X(\mathfrak{f})_{\mathrm{fl}}$, and doing so will allow us to avoid the subtleties of Λ-rings with torsion.

Proposition 8.2. *For any ideal $\mathfrak{a} \in \mathrm{Id}_P$, we have the subscheme inclusion*

$$(8.2.21) \qquad\qquad X(\mathfrak{a}\mathfrak{f}) \subseteq \psi_\mathfrak{a}^{-1}(X(\mathfrak{f})).$$

Proof. Let x be a point of $X(\mathfrak{a}\mathfrak{f})$ with coordinates in some ring R. Let $\mathfrak{b}$ and $\mathfrak{c}$ be $\mathfrak{f}$-equivalent ideals in Id_P. Then we have $\mathfrak{a}\mathfrak{b} \sim_{\mathfrak{a}\mathfrak{f}} \mathfrak{a}\mathfrak{c}$ and hence

$$\psi_\mathfrak{b}\big(\psi_\mathfrak{a}(x)\big) = \psi_{\mathfrak{a}\mathfrak{b}}(x) = \psi_{\mathfrak{a}\mathfrak{c}}(x) = \psi_\mathfrak{c}\big(\psi_\mathfrak{a}(x)\big).$$

It follows that $\psi_\mathfrak{a}(x) \in X(\mathfrak{f})$, and this implies (8.2.21). $\qquad\square$

8.3. *Torsion locus $X[\mathfrak{f}]$.* Write $\mathfrak{f} = \mathfrak{f}_{\mathrm{fin}}\mathfrak{f}_\infty$. Then we define the $\mathfrak{f}$-*torsion* locus by

$$X[\mathfrak{f}] = \psi_{\mathfrak{f}_{\mathrm{fin}}}^{-1}(X(\mathfrak{f}_\infty)).$$

It follows from proposition 8.2 that we have an inclusion of subschemes

$$(8.3.22) \qquad\qquad X(\mathfrak{f}) \subseteq X[\mathfrak{f}].$$

For example, if $A = \mathbb{Z}$, $P = M_\mathbb{Q}$, and $\mathfrak{f} = (n)\infty$, then this inclusion is an equality because both sides are μ_n. If however $\mathfrak{f} = (n)$, then the $\mathfrak{f}$-torsion locus is again μ_n, but the $\mathfrak{f}$-periodic locus $\mathbb{G}_\mathrm{m}(\mathfrak{f})$ is μ_m, where $m = \gcd(2, n)$. So the containment (8.3.22) can be far from an equality.

Summing up the results above with the previous section, we have the following:

Theorem 8.4. *If X is of finite type over A and P is Chebotarev dense, then we have the following:*

(1) *The flat $\mathfrak{f}$-periodic locus $X(\mathfrak{f})_{\mathrm{fl}}$ is a closed $\mathfrak{f}$-periodic sub-$\Lambda_{A,P}$-scheme of X, and it is the maximal flat closed subscheme with these properties.*

(2) *We have $X(\mathfrak{f})_{\mathrm{fl}} = \mathrm{Spec}\,B$, where B is a finitely generated A-algebra, and $K \otimes_A B$ is a finite product of abelian extensions of K of conductor dividing $\mathfrak{f}$.*

(3) *If X is proper, then B is a finite A-algebra.*

Proof. (1) By functoriality, the subscheme $X(\mathfrak{f})$ is stable under the operators $\psi_\mathfrak{p}$, for all $\mathfrak{p} \in P$. Again by functoriality, $X(\mathfrak{f})_{\mathrm{fl}}$ is also stable under them. Since the $\psi_\mathfrak{p}$ are Frobenius lifts on X, so are the endomorphisms they induce on the closed subscheme $X(\mathfrak{f})_{\mathrm{fl}}$. Since $X(\mathfrak{f})_{\mathrm{fl}}$ is flat, this defines a $\Lambda_{A,P}$-structure on $X(\mathfrak{f})_{\mathrm{fl}}$. It is obviously $\mathfrak{f}$-periodic. Maximality is also clear.

(2) This follows from proposition 7.3.

(3) When X is proper, so is $X(\mathfrak{f})_{\mathrm{fl}}$, since it is a closed subscheme of X. It therefore must be finite over A because it is flat and generically finite. $\square$

8.5. *Conjecture.* Let $\mathfrak{r}$ denote the product of all the real places. If X is proper and nonempty, we conjecture that $X(\mathfrak{r})$ is nonempty.

When $K = \mathbb{Q}$, this was proved in [5]. It is possible, however, to give an easier argument that avoids the deep theorems in étale cohomology and p-adic Hodge theory used there. One would expect this argument to go through for general K.

8.6. *Computing the periodic locus.* Is there an algorithm to find equations describing $X(\mathfrak{f})$, given equations for X and formulas for the Frobenius lifts $\psi_{\mathfrak{p}}$? Without such an algorithm, our approach to generating abelian extensions would not be so explicit. But it also might be an indication that, for theoretical purposes, there really is more freedom in this approach.

9. Interlude on periodic Witt vectors

In this section, we define periodic Witt vectors and show how they recover the ray class algebras of the previous section. It will not be used elsewhere in the paper.
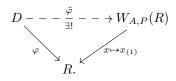
9.1. *P-typical Witt vector rings $W_{A,P}(R)$.* Let us review the generalized Witt vector rings as defined in the first section of [3]. Let R be a flat A-algebra. Then the monoid Id_P acts on the product A-algebra R^{Id_P} (the so-called ghost ring) by translation in the exponent. Explicitly, if $x_{\mathfrak{a}}$ denotes the $\mathfrak{a}$-th component of a vector $x \in R^{\mathrm{Id}_P}$, then $\psi_{\mathfrak{b}} \colon R^{\mathrm{Id}_P} \to R^{\mathrm{Id}_P}$ is defined by the formula

$$\big(\psi_{\mathfrak{b}}(x)\big)_{\mathfrak{a}} = x_{\mathfrak{a}\mathfrak{b}}.$$

Now consider the set of sub-A-algebras $D \subseteq R^{\mathrm{Id}_P}$ such that D is taken to itself by the action of Id_P and such that for each prime $\mathfrak{p} \in P$, the induced endomorphism $\psi_{\mathfrak{p}} \colon D \to D$ is a Frobenius lift at $\mathfrak{p}$. An elementary argument shows that this collection of subrings has a maximal element $W_{A,P}(R)$. It is called the ring of P-typical Witt vectors with entries in R. It recovers the usual p-typical Witt vector functor (restricted to torsion-free rings) when A is $\mathbb{Z}$ and P consists of the single maximal ideal $p\mathbb{Z}$; it recovers the big Witt vector functor when instead P consists of all maximal ideals of $\mathbb{Z}$.

This construction is functorial in R, and one can show that the functor $W_{A,P}$ is representable by a flat A-algebra $\Lambda_{A,P}$. (Incidentally, this shows that $W_{A,P}$ extends to a functor on all A-algebras, namely the one represented by $\Lambda_{A,P}$. Thus we can extend the theory of Λ-structures and Witt vectors to A-algebras with torsion, but we will not need this generality here.) The endomorphisms $\psi_{\mathfrak{a}}$ of the functor $W_{A,P}$ induce endomorphisms of $\Lambda_{A,P}$. They are in fact Frobenius lifts, and hence $\Lambda_{A,P}$ is a $\Lambda_{A,P}$-ring.

9.2. *Universal property of Witt vector rings.* The Witt vector functor is the right adjoint of the forgetful functor from $\Lambda_{A,P}$-rings to A-algebras. Let us spell out the universal property for future reference. Let R be a flat A-algebra, let D be a flat $\Lambda_{A,P}$-ring, and let $\varphi \colon D \to R$ be an A-algebra map. Then φ lifts to a unique $\Lambda_{A,P}$-ring map $\tilde{\varphi}$ to the Witt vector ring:

$$
\begin{array}{ccc}
D & \xdashrightarrow[\exists!]{\tilde{\varphi}} & W_{A,P}(R) \\
& {\scriptstyle \varphi} \searrow \quad \swarrow {\scriptstyle x \mapsto x_{(1)}} & \\
& R. &
\end{array}
$$

Indeed, it lifts to a unique Id_P-equivariant morphism $D \to R^{\mathrm{Id}_P}$, given by $a \mapsto x$, where $x_{\mathfrak{a}} = \varphi(\psi_{\mathfrak{a}}(a))$. It remains to check that the image S of this map lies in $W_{A,P}(R)$. But S is torsion free, as a subalgebra of R^{Id_P}; it has an action of Id_P, as the image of an equivariant map of rings with an Id_P-action; and it satisfies the Frobenius lift condition because it is an Id_P-equivariant quotient of D, which satisfies the Frobenius lift condition. Therefore S is contained in $W_{A,P}(R)$ by the maximality property of $W_{A,P}(R)$.

9.3. $\mathfrak{f}$-*periodic Witt vector rings* $W^{(\mathfrak{f})}(R)$. Let $\mathfrak{f}$ be a cycle on K. We define the set of $\mathfrak{f}$-periodic Witt vectors with entries in an A-algebra R as follows

$$(9.3.23) \qquad W_{A,P}^{(\mathfrak{f})}(R) := \{x \in W_{A,P}(R) : \psi_{\mathfrak{a}}(x) = \psi_{\mathfrak{b}}(x) \text{ whenever } \mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{b}\}.$$

In other words, if we view the functor $W_{A,P}$ as a scheme, then $W_{A,P}^{(\mathfrak{f})}(R)$ is the set of R-valued points on its $\mathfrak{f}$-periodic locus.

When R is flat, the periodic Witt vectors can be described simply in terms of their ghost components:

$$(9.3.24) \qquad W_{A,P}^{(\mathfrak{f})}(R) = \{x \in W_{A,P}(R) : x_{\mathfrak{a}} = x_{\mathfrak{b}} \text{ whenever } \mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{b}\}.$$

Indeed, this follows from the implication $\mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{b} \Rightarrow \mathfrak{a}\mathfrak{c} \sim_{\mathfrak{f}} \mathfrak{b}\mathfrak{c}$. In other words, we have

$$(9.3.25) \qquad W_{A,P}^{(\mathfrak{f})}(R) = W_{A,P}(R) \cap R^{\mathrm{DR}_P(\mathfrak{f})},$$

as subrings of the ghost ring R^{Id_P}.

9.4. *Example.* Suppose $A = \mathbb{Z}$, $P = M_{\mathbb{Q}}$, and $\mathfrak{f} = (n)\infty$ where $n \geqslant 1$. Then an $\mathfrak{f}$-periodic Witt vector with entries in a torsion-free ring R is just a big Witt vector whose ghost components are periodic with period dividing n. This is the reason for the name. For example, if ζ_n is an n-th root of unity, then the Teichmüller element

$$[\zeta_n] := \langle \zeta_n, \zeta_n^2, \zeta_n^3, \dots \rangle$$

is $n\infty$-periodic. (This is even true when R is not torsion free, by functoriality and because the universal ring with an n-th root of unity is $\mathbb{Z}[x]/(x^n - 1)$, which is torsion free.)

Proposition 9.5. $W_{A,P}^{(\mathfrak{f})}(R)$ *is an* $\mathfrak{f}$-*periodic sub-*$\Lambda_{A,P}$-*ring of* $W_{A,P}(R)$, *for any flat* A-*algebra* R.

Proof. It is clearly a sub-A-algebra of $W_{A,P}(R)$. It is also preserved by all $\psi_{\mathfrak{p}}$ operators ($\mathfrak{p} \in P$) because of the implication $\mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{b} \Rightarrow \mathfrak{p}\mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{p}\mathfrak{b}$. The family of operators $\psi_{\mathfrak{a}}$ is also $\mathfrak{f}$-periodic on $W_{A,P}^{(\mathfrak{f})}(R)$ by definition.

So all that remains is to check the Frobenius lift property. For $\mathfrak{p} \in P$ and any $x \in W_{A,P}^{(\mathfrak{f})}(R)$, we have

$$\psi_{\mathfrak{p}}(x) - x^{N(\mathfrak{p})} \in \mathfrak{p}W_{A,P}(R) \cap W_{A,P}^{(\mathfrak{f})}(R).$$

Thus it is enough to show that the containment

$$(9.5.26) \qquad \mathfrak{p}W_{A,P}^{(\mathfrak{f})}(R) \subseteq \mathfrak{p}W_{A,P}(R) \cap W_{A,P}^{(\mathfrak{f})}(R)$$

is an equality. This follows from the diagram

$$
\begin{array}{ccccc}
0 \longrightarrow & W^{(\mathfrak{f})}(R) & \longrightarrow & W(R) & \overset{\gamma}{\longrightarrow} & \prod_{\mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{b}} R \\
& \uparrow & & \uparrow & & \uparrow \\
0 \longrightarrow & \mathfrak{p} \otimes_A W^{(\mathfrak{f})}(R) & \longrightarrow & \mathfrak{p} \otimes_A W(R) & \overset{\mathfrak{p} \otimes \gamma}{\longrightarrow} & \mathfrak{p} \otimes_A \prod_{\mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{b}} R
\end{array}
$$

of exact sequences, where $\gamma(x) = (\ldots, x_{\mathfrak{a}} - x_{\mathfrak{b}}, \ldots)$. The vertical arrows are the evident multiplication maps $a \otimes b \mapsto ab$; they are injective because all modules on the top row are flat. This plus the exactness of the bottom row implies that (9.5.26) is an equality. $\qquad\square$

9.6. *Remark: Plethysic algebra.* The formal concepts above can be expressed in the language of plethystic algebra [8]. Let $\Lambda_{A,P}$ be the A-algebra representing the functor $W_{A,P}$, and let $\Lambda_{A,P}^{(\mathfrak{f})}$ be the one representing the functor $W_{A,P}^{(\mathfrak{f})}$. Then the inclusion of functors $W_{A,P}^{(\mathfrak{f})} \subseteq W_{A,P}$ induces a surjection $\Lambda_{A,P} \to \Lambda_{A,P}^{(\mathfrak{f})}$. It is not hard to show that this has the structure of a morphism of A-plethories and an action of $\Lambda_{A,P}^{(\mathfrak{f})}$ is the same as an $\mathfrak{f}$-periodic $\Lambda_{A,P}$-structure. It follows that the forgetful functor from $\mathfrak{f}$-periodic $\Lambda_{A,P}$-rings to all $\Lambda_{A,P}$-rings has both a left and a right adjoint. The right adjoint outputs the $\mathfrak{f}$-periodic elements of the given $\Lambda_{A,P}$-ring. This provides one approach to Λ-structures and Witt vectors that works smoothly in the presence of torsion.

9.7. *Universal property of periodic Witt vector rings.* Let R be a flat A-algebra, let D be a flat $\mathfrak{f}$-periodic $\Lambda_{A,P}$-ring, and let $\varphi \colon D \to R$ be an A-algebra map. Then φ lifts to a unique $\Lambda_{A,P}$-ring map to the $\mathfrak{f}$-periodic Witt vector ring:

$$
\begin{array}{ccc}
D & \xdashrightarrow[\;\exists!\;]{\tilde{\varphi}} & W_{A,P}^{(\mathfrak{f})}(R) \\
& {\scriptstyle \varphi}\searrow \quad \swarrow {\scriptstyle x \mapsto x_{(1)}} & \\
& R. &
\end{array}
$$

Indeed, by the universal property of Witt vectors (9.2), it lifts to a unique $\Lambda_{A,P}$-map $D \to W_{A,P}(R)$. But since D is $\mathfrak{f}$-periodic, the image is contained in $W_{A,P}^{(\mathfrak{f})}(R)$.

Proposition 9.8. *Let K^{sep} be a separable closure of K, and let A^{int} denote the integral closure of A in K^{sep}. Let $R_{A,P}(\mathfrak{f})$ denote the ray class $\Lambda_{A,P}$-ring of conductor $\mathfrak{f}$, as defined in 7.4. Then we have an isomorphism*

$$(9.8.27) \qquad \tilde{\beta} \colon R_{A,P}(\mathfrak{f}) \xrightarrow{\sim} W_{A,P}^{(\mathfrak{f})}(A^{\mathrm{int}})$$

of $\Lambda_{A,P}$-rings, where the map $\tilde{\beta}$ is the lift, in the sense of 9.7, of the projection $\beta \colon R_{A,P}(\mathfrak{f}) \to A^{\mathrm{int}}$ defined in 7.4.

Proof. The $\Lambda_{A,P}$-rings $R_{A,P}(\mathfrak{f})$ and $W_{A,P}^{(\mathfrak{f})}(A^{\mathrm{int}})$ are characterized by the same universal property, except that the one for $R_{A,P}(\mathfrak{f})$ is restricted to algebras D that are reduced and finite flat over A. So it is enough to show that $W_{A,P}^{(\mathfrak{f})}(A^{\mathrm{int}})$ is itself reduced and finite flat over A. Since it is a subalgebra of $\prod_{\mathrm{DR}_P(\mathfrak{f})} A^{\mathrm{int}}$ by definition, it is reduced and flat. So it is enough to show that it is finite over A.

First, observe that we have

$$(9.8.28) \qquad \mathrm{colim}_L\, W_{A,P}^{(\mathfrak{f})}(L \cap A^{\mathrm{int}}) = W_{A,P}^{(\mathfrak{f})}(A^{\mathrm{int}}),$$

where L runs over the finite extensions of K contained in K^{sep}. Indeed, for any $x \in W_{A,P}^{(\mathfrak{f})}(A^{\mathrm{int}})$, let L denote the extension $K(\ldots, x_{\mathfrak{a}}, \ldots)$, where the $x_{\mathfrak{a}}$ are the (ghost) components of x. It follows that $x \in W_{A,P}(L) \cap W_{A,P}(A^{\mathrm{int}})$. Because $W_{A,P}$ is representable, we also have

$$W_{A,P}(L) \cap W_{A,P}(A^{\mathrm{int}}) = W_{A,P}(L \cap A^{\mathrm{int}}),$$

and hence $x \in W_{A,P}(L \cap A^{\mathrm{int}})$. Because x is also $\mathfrak{f}$-periodic, we have

$$x \in W_{A,P}^{(\mathfrak{f})}(L \cap A^{\mathrm{int}}),$$

as desired. It remains to show that L is a finite extension of K. This holds because x is $\mathfrak{f}$-periodic and $\mathrm{DR}_P(\mathfrak{f})$ is finite, and so x has only finitely many distinct ghost components. This proves (9.8.28).

Therefore it is enough to prove that $W_{A,P}^{(\mathfrak{f})}(L \cap A^{\mathrm{int}})$ has bounded rank as L runs over all finite extensions of K. By proposition 9.5, $W_{A,P}^{(\mathfrak{f})}(L \cap A^{\mathrm{int}})$ is a flat reduced $\mathfrak{f}$-periodic $\Lambda_{A,P}$-ring. Being a subring of $\prod_{\mathrm{DR}_P(\mathfrak{f})} L \cap A^{\mathrm{int}}$, it is also finitely generated as an A-module. Therefore by theorem 5.5, it is contained in the product ring $\prod_{\mathfrak{d}} K(\mathfrak{f}\mathfrak{d}^{-1}) \cap A^{\mathrm{int}}$, where $\mathfrak{d}$ runs over Id_P with $\mathfrak{d} \mid \mathfrak{f}_{\mathrm{fin}}$. Therefore its rank as L varies is bounded. $\qquad\square$

9.9. *Example.* If $A = \mathbb{Z}$, $P = M_{\mathbb{Q}}$, and $\mathfrak{f} = (n)\infty$ with $n \geqslant 1$, then for any primitive n-th root of unity ζ_n, there is an isomorphism

$$\mathbb{Z}[x]/(x^n - 1) \xrightarrow{\sim} W_{\mathbb{Z},P}^{(n\infty)}(O_{\bar{\mathbb{Q}}})$$

given by $x \mapsto [\zeta_n]$. Given the above, this is the second theorem of our first paper [7].

On the other hand, if $\mathfrak{f} = (1)$ but K is arbitrary and $P = M_K$, then we have

$$W_{O_K,P}^{(1)}(O_{\bar{K}}) = O_H$$

where H is the Hilbert class field of K. More generally, if $\mathfrak{f}$ is supported at infinity, then $W_{O_K,P}^{(\mathfrak{f})}(O_{\bar{K}})$ is the ring of integers in the corresponding narrow Hilbert class field.

Corollary 9.10. *The periodic Witt vector ring is generically a product of ray class fields:*

$$(9.10.29) \qquad K \otimes_A W_{A,P}^{(\mathfrak{f})}(A^{\mathrm{int}}) = \prod_{\substack{\mathfrak{d} \in \mathrm{Id}_P \\ \mathfrak{d} \mid \mathfrak{f}_{\mathrm{fin}}}} K(\mathfrak{f}\mathfrak{d}^{-1}).$$

The ray class field $K(\mathfrak{f})$ is the image of the projection

$$(9.10.30) \qquad K \otimes_A W_{A,P}^{(\mathfrak{f})}(A^{\mathrm{int}}) \longrightarrow K^{\mathrm{sep}}, \quad x \mapsto x_{(1)}.$$

9.11. *Remark: Periodic Witt vectors and explicit class field theory.* It follows from corollary 9.10 that any ray class field $K(\mathfrak{f})$ is generated by the first coordinate $x_{(1)}$ of the $\mathfrak{f}$-periodic A^{int}-points x on the affine scheme $W_{A,P} = \mathrm{Spec}(\Lambda_{A,P})$. We emphasize however that $W_{A,P}$ is not of finite type, and so this does not give an explicit method of producing a polynomial whose roots generate $K(\mathfrak{f})$. In fact, the periodic locus $W_{A,P}^{(\mathfrak{f})}$ is itself not even of finite type. For instance, if $K = \mathbb{Q}$, $P = M_{\mathbb{Q}}$, and $\mathfrak{f} = \infty$, then $\Lambda_{A,P}^{(\mathfrak{f})}$ is isomorphic to the binomial ring, the subring of $\mathbb{Q}[x]$ generated by the binomial coefficients $\binom{x}{n}$, and this is not finitely generated as a ring. Therefore to find a point of $W_{A,P}^{(\mathfrak{f})}$, one has to solve infinitely many simultaneous polynomial equations with coefficients in A.

To be sure, $K \otimes_A \Lambda_{A,P}^{(\mathfrak{f})}$ is finitely generated as a K-algebra, because on K-algebras it represents the periodic ghost functor $R \mapsto R^{\mathrm{DR}_P(\mathfrak{f})}$ and $\mathrm{DR}_P(\mathfrak{f})$ is finite. Therefore a periodic Witt vector is determined by finitely many components, namely its ghost components. However to give a criterion for a periodic ghost vector to be a Witt vector, we need infinitely many congruences between polynomials in the ghost components. If we add variables to express these congruences as equations, we will need infinitely many new variables.

10. $K = \mathbb{Q}$: THE TORIC LINE AND THE CHEBYSHEV LINE

In this section, we consider the case where A is $\mathbb{Z}$ and P is the set of all maximal ideals of $\mathbb{Z}$. For any integer $n \geqslant 1$, let us write $\psi_n = \psi_{(n)}$ and $\Lambda = \Lambda_{\mathbb{Z},P}$.

10.1. *The toric line and cyclotomic extensions.* Define the toric Λ-structure on $\mathbb{G}_{\mathrm{m}} = \operatorname{Spec} \mathbb{Z}[x^{\pm 1}]$ to be the one given by $\psi_p(x) = x^p$, for all primes numbers p. (We use this name because it is a particular case of the natural Λ-structure on any toric variety.) Observe that it extends uniquely to the affine and projective lines.

For each cycle of the form $(n)\infty$, with $n \geqslant 1$, the periodic locus $\mathbb{G}_{\mathrm{m}}(n\infty)$ is simply $\mu_n = \operatorname{Spec} \mathbb{Z}[x]/(x^n - 1)$. In other words, the containment (8.3.22) is an equality. Thus we have

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{G}_{\mathrm{m}}(n\infty) = \coprod_{d|n} \operatorname{Spec} \mathbb{Q}(\zeta_d).$$

So in this case, the $n\infty$-periodic locus of the Λ-scheme $\mathbb{G}_{\mathrm{m}}$ does in fact generate the ray class field of conductor $n\infty$.

10.2. *The Chebyshev line and real-cyclotomic extensions.* The toric Λ-ring $\mathbb{Z}[x^{\pm 1}]$ above has an automorphism σ defined by $\sigma(x) = x^{-1}$. The fixed subring is easily seen to be a sub-Λ-ring and freely generated as a ring by $y = x + x^{-1}$. The elements $\psi_p(y) \in \mathbb{Z}[y]$ are given by Chebyshev polynomials

$$\psi_n(y) = 2 + \prod_{i=0}^{n-1} (y - \zeta_n^i - \zeta_n^{-i}),$$

where ζ_n is a primitive n-th root of unity. For example, we have

$$\psi_2(y) = y^2 - 2, \qquad \psi_3(y) = y^3 - 3y, \qquad \psi_5(y) = y^5 - 5y^3 + 5y, \qquad \ldots.$$

This gives the affine line $Y = \operatorname{Spec} \mathbb{Z}[y]$ a Λ-scheme structure. We call it the Chebyshev Λ-structure. It also extends uniquely to the projective line. (Incidentally, $\mathbb{Z}[y]$ is isomorphic as a Λ-ring to the Grothendieck group of the Lie algebra $\mathfrak{sl}_2$. By Clauwens's theorem [9], this and the toric Λ-structure are the only two Λ-structures on the affine line, up to isomorphism.)

Now consider a cycle $\mathfrak{f}$ with trivial infinite part. Write $\mathfrak{f} = (n)$, where $n \geqslant 1$, and write $Y(n) = Y(\mathfrak{f})$ for the periodic locus. We have

$$Y[1] = Y(1) = \operatorname{Spec} \mathbb{Z}[y]/(y - 2),$$

and hence the n-torsion locus is

$$Y[n] = \psi_n^{-1}(\operatorname{Spec} \mathbb{Z}[y]/(y - 2))$$

or more simply, $Y[n] = \psi_n^{-1}(2)$. Observe that $Y[n]$ is not reduced when $n \geqslant 3$: for instance if n is odd, we have

$$\psi_n(y) - 2 = \prod_{i=0}^{n-1} (y - \zeta_n^i - \zeta_n^{-i}) = (y - 2) \prod_{i=1}^{\frac{n-1}{2}} (y - \zeta_n^i - \zeta_n^{-i})^2.$$

However the periodic locus is reduced. In fact, we have

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}(Y(n)) = \prod_{d|n} \mathbb{Q}(\zeta_d + \zeta_d^{-1}),$$

by the following more precise integral result:

Proposition 10.3. (1) *The periodic locus $Y(n)$ is flat and reduced, and the inclusion*

$$i : Y(n) \to Y[n]_{\mathrm{red}}$$

is an isomorphism.

(2) *The map $\mathcal{O}(Y(n)) \to \mathbb{Z}[x]/(x^n - 1)$ is injective. If n is odd, its image is the subring of invariants under the involution $\sigma : x \mapsto x^{-1}$. If n is even, its image is the span of $\{1, x + x^{-1}, \ldots, x^{n/2-1} + x^{1-n/2}, 2x^{n/2}\}$.*

Proof. (1): Consider the differences of Chebyshev polynomials

$$P_{a,b}(y) := \psi_a(y) - \psi_b(y) \in \mathbb{Z}[y].$$

Then the periodic locus $Y(n)$ is $\operatorname{Spec} \mathbb{Z}[y]/I$, where

$$I = \big(P_{a,b}(y) \mid a \equiv \pm b \bmod n, \ a,b \geqslant 1\big).$$

Let $Q(y)$ denote the product of the monic irreducible factors of $(\psi_n(y) - 2)$, each taken only with multiplicity 1. If n is odd, we have

$$Q(y) = \prod_{i=0}^{\frac{n-1}{2}} (y - \zeta_n^i - \zeta_n^{-i}).$$

and if n is even, we have

$$Q(y) = \prod_{i=0}^{\frac{n}{2}} (y - \zeta_n^i - \zeta_n^{-i}).$$

Then we have

$$I \subseteq (Q(y))$$

since each $P_{a,b}(y)$ vanishes at $y = \zeta_n^i + \zeta_n^{-i}$, for each i. Therefore to prove (1), it is enough to show this containment is an equality.

Since $\mathbb{Z}[x^{\pm 1}]$ is a faithfully flat extension of $\mathbb{Z}[y]$, it is enough to show this after base change to $\mathbb{Z}[x^{\pm 1}]$. In other words, it is enough to show

$$Q(x + x^{-1}) \in \big(P_{a,b}(x + x^{-1}) \mid a \equiv \pm b \mod n\big).$$

We have

$$P_{a,b}(x + x^{-1}) = x^a + x^{-a} - x^b - x^{-b} = x^{-a}(x^{a+b} - 1)(x^{a-b} - 1).$$

Therefore we have

$$\big(P_{n+1,1}(x + x^{-1})\big) = \big((x^n - 1)(x^{n+2} - 1)\big),$$
$$\big(P_{n+2,2}(x + x^{-1})\big) = \big((x^n - 1)(x^{n+4} - 1)\big)$$

and hence

$$\big(P_{n+1,1}(x + x^{-1}), P_{n+2,2}(x + x^{-1})\big) = \big(x^n - 1\big)\big((x^2 - 1), (x^n - 1)\big).$$

If n is odd, then we have

$$\big(x^n - 1\big)\big((x^2 - 1), (x^n - 1)\big) = \big((x^n - 1)(x - 1)\big) = \big(Q(x + x^{-1})\big).$$

Similarly, if n is even

$$\big(x^n - 1\big)\big((x^2 - 1), (x^n - 1)\big) = \big((x^n - 1)(x^2 - 1)\big) = \big(Q(x + x^{-1})\big).$$

Thus in either case, we have

$$Q(x + x^{-1}) \in \big(P_{n+1,1}(x + x^{-1}), P_{n+2,2}(x + x^{-1})\big)$$
$$\subseteq \big(P_{a,b}(y) \mid a \equiv \pm b \bmod n, \ a,b \geqslant 1\big).$$

(2): Suppose a polynomial $f(y) \in \mathbb{Z}[y]$ maps to zero in $\mathbb{Z}[x]/(x^n - 1)$. Then we have $f(\zeta_n^i + \zeta_n^{-i}) = 0$ for all i. Therefore we have $(y - \zeta_n^i - \zeta_n^{-i}) \mid f(y)$. Thus if n is odd, we have

$$\prod_{i=0}^{\frac{n-1}{2}} (y - \zeta_n^i - \zeta_n^{-1}) \mid f(y)$$

and if n is even,

$$\prod_{i=0}^{\frac{n}{2}} (y - \zeta_n^i - \zeta_n^{-1}) \mid f(y).$$

In either case, we have $Q(y) \mid f(y)$. Therefore the map $\mathbb{Z}[y]/(Q(y)) \to \mathbb{Z}[x]/(x^n-1)$ is injective.

Let us now consider surjectivity. When n is odd, the set

$$\{1, x + x^{-1}, \ldots, x^{\frac{n-1}{2}} + x^{-\frac{n-1}{2}}\}$$

is a $\mathbb{Z}$-basis for the subring $\left(\mathbb{Z}[x]/(x^n-1)\right)^\sigma$ of σ-invariants, and this is contained in the image of $\mathbb{Z}[y]$. When n is even, $\{1, x + x^{-1}, \ldots, x^{n/2-1} + x^{1-n/2}, x^{n/2}\}$ is a $\mathbb{Z}$-basis. All these elements but $x^{n/2}$ lie in the image of $\mathbb{Z}[y]$. However $2x^{n/2}$ does lie in the image. □

Corollary 10.4. *The map*

$$\mathcal{O}(Y(n)) \longrightarrow R_{\mathbb{Z},P}(n)$$

to the ray class algebra given by the point $\zeta_n + \zeta_n^{-1} \in Y(n)(O_{\bar{\mathbb{Q}}})$ is injective. If n is odd, it is surjective; if n is even, its cokernel is a group of order 2 generated by the class of $[-1] = \langle \ldots, (-1)^d, \ldots \rangle \in \prod_{d|n} \mathbb{Q}(\zeta_{n/d} + \zeta_{n/d}^{-1})$.

Proof. By the map $\mathbb{Z}[x]/(x^n-1) \to O_{\bar{\mathbb{Q}}}$ given by $x \mapsto \zeta_n$ results in a diagram

$$
\begin{array}{ccc}
\mathbb{Z}[x]/(x^n-1) & \longrightarrow & R_{\mathbb{Z},P}(n\infty) \\
\uparrow & & \uparrow \\
\left(\mathbb{Z}[x]/(x^n-1)\right)^\sigma & \longrightarrow & R_{\mathbb{Z},P}(n).
\end{array}
$$

By the second theorem in our first paper [7], the top map is an isomorphism. Since taking maximal Λ-orders commutes with taking group invariants, by part (2) of proposition 2.2, the bottom arrow is also an isomorphism. Observe that when n is even, the image of $x^{n/2}$ is $[-1]$. Now invoke proposition 10.3. □

11. K IMAGINARY QUADRATIC: CM ELLIPTIC CURVES AND THE LATTÈS SCHEME

Let K be an imaginary quadratic field. For convenience, let us fix an embedding $K \subset \mathbb{C}$. In this section, we show how explicit class field theory over K, due to Kronecker and his followers, can be set naturally in the framework of this paper. This builds on Gurney's thesis [14]. The arguments are similar in spirit to those in the real-cyclotomic context in the previous section.

Let us write

$$\Lambda = \Lambda_{O_K, M_K} \quad \text{and} \quad \Lambda_{\mathfrak{p}} = \Lambda_{O_{K_{\mathfrak{p}}}, \mathfrak{p}},$$

where $\mathfrak{p} \in P$ is any given prime.

11.1. *The moduli space of CM elliptic curves.* Let R be an O_K-algebra. Then a *CM elliptic curve* over R is an elliptic curve E over R together with a ring map $O_K \to \mathrm{End}_R(E)$ such that the induced action of O_K on the tangent space $T_0(E)$ agrees with the O_K-algebra structure map $O_K \to R = \mathrm{End}_R(T_0(E))$. Let $\mathcal{M}_{\mathrm{CM}}(R)$ denote the category whose objects are the CM elliptic curves over R and whose morphisms are the O_K-equivariant isomorphisms of elliptic curves. Since all morphisms are isomorphisms, $\mathcal{M}_{\mathrm{CM}}(R)$ is a groupoid by definition. As the O_K-algebra R varies, the usual base-change maps make $\mathcal{M}_{\mathrm{CM}}$ a fibered category over the category of affine O_K-schemes. Further, this fibered category satisfies effective descent for the fppf topology because all ingredients in its definition can be expressed in terms which are fppf-local. In other words, $\mathcal{M}_{\mathrm{CM}}$ is a stack. (See [16] the theory of stacks.) Let $\mathcal{E} \to \mathcal{M}_{\mathrm{CM}}$ denote the universal object. Then $\mathcal{E}(R)$ is the groupoid of pairs (E, x), where E is a CM elliptic curve over R, and x is a point of $E(R)$.

Both $\mathcal{E}$ and $\mathcal{M}_{\mathrm{CM}}$ have certain endomorphisms $\psi_{\mathfrak{a}}$, for any integral ideal $\mathfrak{a} \subseteq O_K$, defined as follows. On $\mathcal{M}_{\mathrm{CM}}$, the map $\psi_{\mathfrak{a}}$ is defined by

$$\psi_{\mathfrak{a}} : E \mapsto \mathfrak{a}^{-1} \otimes E,$$

where the elliptic curve $\mathfrak{a}^{-1} \otimes E$ is the Serre tensor product [19], defined as a functor by

$$\left(\mathfrak{a}^{-1} \otimes E\right)(C) := \mathfrak{a}^{-1} \otimes_{O_K} \left(E(C)\right),$$

for any algebra C over the base R of E. (This is again an elliptic curve: since $\mathfrak{a}^{-1}$ is a direct summand of O_K^2, the functor $\mathfrak{a}^{-1} \otimes E$ is a direct summand of the abelian variety E^2.) In particular, if $R = \mathbb{C}$ and the period lattice of E is L, so that $E(\mathbb{C}) = \mathbb{C}/L$, then $\mathfrak{a}^{-1} \otimes E$ is the elliptic curve with period lattice $\mathfrak{a}^{-1} \otimes_{O_K} L$, up to canonical isomorphism.

Using the isogeny $E \to \mathfrak{a}^{-1} \otimes E$ defined by $x \mapsto 1 \otimes x$, we can then define the endomorphism $\psi_{\mathfrak{a}} : \mathcal{E} \to \mathcal{E}$ by

$$\psi_{\mathfrak{a}} : (E, x) \mapsto (\mathfrak{a}^{-1} \otimes E, 1 \otimes x).$$

Observe that it lies over the endomorphism $\psi_{\mathfrak{a}}$ of $\mathcal{M}_{\mathrm{CM}}$.

The $\psi_{\mathfrak{a}}$ operators should be thought of as providing a Λ-structure on $\mathcal{M}_{\mathrm{CM}}$ and $\mathcal{E}$, but $\mathcal{M}_{\mathrm{CM}}$ and $\mathcal{E}$ are stacks and we will not define what Λ-structures on stacks are here. Let us just say that the $\psi_{\mathfrak{a}}$ operators, whether on $\mathcal{M}_{\mathrm{CM}}$ or $\mathcal{E}$, commute up to a coherent family of canonical isomorphisms coming from the usual associators $(U \otimes V) \otimes W \to U \otimes (V \otimes W)$ on the category of O_K-modules. Similarly, if $\mathfrak{a}$ is a prime $\mathfrak{p}$, then the reduction of $\psi_{\mathfrak{p}}$ modulo $\mathfrak{p}$ agrees with the $N(\mathfrak{p})$-power Frobenius map $F_{\mathfrak{p}}$, in the sense that for any elliptic curve E over an $\mathbb{F}_p$-algebra, there is unique isomorphism $\psi_{\mathfrak{p}}(E) \to F_{\mathfrak{p}}(E)$ compatible with the canonical maps from E.

11.2. *Lattès scheme.* We follow Gurney's thesis [14]. Let $\mathcal{L}$ denote the coarse space underlying $\mathcal{E}$. It is the functor defined, for any O_K-algebra C, by
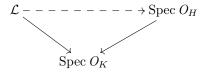
$$\mathcal{L}(C) = \{\text{local-isomorphism classes of triples } (C', E, x)\},$$

where C' is an fppf cover of C, and E is a CM elliptic curve over C', and $x \in E(C')$ and where two pairs (C_1', E_1, x_1) and (C_2', E_2, x_2) are in the same local-isomorphism class if C_1' and C_2' have a common fppf cover C'' such that when pulled back to C'', there is an isomorphism between E_1 and E_2 identifying x_1 and x_2. Observe that if $C = \mathbb{C}$ (or any algebraically closed field), we have

$$\mathcal{L}(\mathbb{C}) = \{\text{isomorphism classes of pairs } (E, x)\},$$

where E is a CM elliptic curve over $\mathbb{C}$ and $x \in E(\mathbb{C})$. Thus $\mathcal{L}(\mathbb{C})$ is the union of h_K copies of $\mathbb{P}^1(\mathbb{C})$, where h_K is the class number of K.

The functor $\mathcal{L}$ is an O_K-scheme (see 4.3.10 of [14]), which we call the *Lattès scheme*, and unless we say otherwise we will view it as an O_K-scheme. Note however that the structure map $\mathcal{L} \to \operatorname{Spec} O_K$ factors naturally through the coarse space underlying $\mathcal{M}_{\mathrm{CM}}$, which Gurney shows (2.6.10 of [14]) is $\operatorname{Spec} O_H$, where H is the Hilbert class field of K in $\mathbb{C}$:

$$\mathcal{L} \dashrightarrow \operatorname{Spec} O_H$$
$$\searrow \quad \swarrow$$
$$\operatorname{Spec} O_K$$

So one can also view $\mathcal{L}$ as an O_H-scheme, and sometimes we will.

For example, given any CM elliptic curve E over R, we have an identification

$$(11.2.31) \qquad\qquad \mathcal{L} \times_{\operatorname{Spec}(O_H)} \operatorname{Spec}(R) = E/O_K^*.$$

(This can in fact serve as an alternative definition of $\mathcal{L}$.) The universal map $\mathcal{E} \to \mathcal{L}$ is then nothing more than the classical Weber function expressed in our language. Gurney (4.3.16 of [14]) proves there exists an isomorphism $\mathcal{L} \to \mathbb{P}^1_{O_H}$ of O_H-schemes. (The fact that $\mathcal{L}$ is a $\mathbb{P}^1$-bundle over O_H is expected, but the fact that it is the trivial bundle requires more work.) It follows that as an O_K-scheme, $\mathcal{L}$ has geometrically disconnected fibers if $h_K > 1$. We also emphasize that there appears to be no canonical isomorphism $\mathcal{L} \to \mathbb{P}^1_{O_H}$. There is a canonical O_H-point $\infty \in \mathcal{L}(O_H)$, which corresponds to pairs of the form $(E, 0)$. The isomorphism $\mathcal{L} \to \mathbb{P}^1_{O_H}$ would then typically be chosen to send ∞ to ∞, but we cannot make any further restrictions, it seems. So the isomorphism $\mathcal{L} \to \mathbb{P}^1_{O_H}$ is canonically defined only up to the action of the stabilizer group of ∞, the semi-direct product $O_H \rtimes O_H^*$.

The endomorphisms $\psi_{\mathfrak{a}}$ of $\mathcal{E}$ induce endomorphisms $\psi_{\mathfrak{a}} : \mathcal{L} \to \mathcal{L}$ (morphisms of O_K-schemes). Then $\psi_{\mathfrak{p}}$ for $\mathfrak{p}$ prime reduces to the $N(\mathfrak{p})$-power Frobenius map $F_{\mathfrak{p}}$ modulo $\mathfrak{p}$, and hence the $\psi_{\mathfrak{a}}$ define a Λ-structure on $\mathcal{L}$. (See 4.3.11 of [14].) Further the map $\mathcal{L} \to \operatorname{Spec} O_H$ above is a morphism of Λ-schemes, where O_H is given its unique Λ-ring structure.

When expressed in terms of $\mathbb{P}^1_{O_H}$, the endomorphisms $\psi_{\mathfrak{a}}$ are often call the Lattès functions, as for example in Milnor's book [17] (page 72), which explains the name.

Proposition 11.3. (1) $\mathcal{L}[\mathfrak{f}](\mathbb{C})$ *is the set of isomorphism classes of pairs* (E, x), *where E is a complex CM elliptic curve and $x \in E[\mathfrak{f}](\mathbb{C})$.*

(2) *The action of Id_P on $\mathcal{L}[\mathfrak{f}](\mathbb{C})$, where $\mathfrak{a}$ acts as $\psi_{\mathfrak{a}}$, factors through an action (necessarily unique) of $\operatorname{DR}_P(\mathfrak{f})$ on $\mathcal{L}[\mathfrak{f}](\mathbb{C})$. The resulting $\operatorname{DR}_P(\mathfrak{f})$-set is a torsor generated by any class of the form (E_0, x_0), where E_0 is a CM elliptic curve and x_0 is a generator of $E_0[\mathfrak{f}](\mathbb{C})$ as an O_K-module.*

Proof. (1): Any point of $y \in \mathcal{L}(\mathbb{C})$ is the isomorphism class of a pair (E, x), where E is a complex CM elliptic curve and $x \in E(\mathbb{C})$. Under $\psi_{\mathfrak{f}}$, the pair (E, x) maps to $(\mathfrak{f}^{-1} \otimes E, 1 \otimes x)$. So if y lies in the $\mathfrak{f}$-torsion locus $\mathcal{L}[\mathfrak{f}](\mathbb{C})$, the object $(\mathfrak{f}^{-1} \otimes E, 1 \otimes x)$ must be isomorphic to one of the form $(E', 0)$. Therefore the point $1 \otimes x \in (\mathfrak{f}^{-1} \otimes E)(\mathbb{C})$ is 0, and hence x is an $\mathfrak{f}$-torsion point of E.

(2): Let us first show that the orbit of (E_0, x_0) under Id_P is all of $\mathcal{L}[\mathfrak{f}](\mathbb{C})$. Let (E, x) be an element of $\mathcal{L}[\mathfrak{f}](\mathbb{C})$. Then there is an integral ideal $\mathfrak{a} \subseteq O_K$ such that there exists an isomorphism of elliptic curves $f : \mathfrak{a}^{-1} \otimes E_0 \to E$. We can choose $\mathfrak{a}$ such that it is coprime to $\mathfrak{f}$. It follows that the image $1 \otimes x_0 \in \mathfrak{a}^{-1} \otimes E_0(\mathbb{C})$ of x_0 is a generator of $(\mathfrak{a}^{-1} \otimes E_0)[\mathfrak{f}](\mathbb{C})$, and hence that $f(1 \otimes x_0)$ is a generator of $E[\mathfrak{f}](\mathbb{C})$. In other words, there exists an element $b \in O_K$ such that $bf(1 \otimes x_0) = x$. Then we have

$$\psi_{b\mathfrak{a}}(E_0, x_0) = (b^{-1}\mathfrak{a}^{-1} \otimes E_0, 1 \otimes x_0) \cong (\mathfrak{a}^{-1} \otimes E_0, b \otimes x_0)$$
$$\cong (E, f(b \otimes x_0)) = (E, bf(1 \otimes x_0)) = (E, x).$$

Therefore (E_0, x_0) generates $\mathcal{L}[\mathfrak{f}](\mathbb{C})$ as a $\operatorname{DR}_P(\mathfrak{f})$-set.

It remains to show

$$\mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{b} \iff \psi_{\mathfrak{a}}((E_0, x_0)) = \psi_{\mathfrak{b}}((E_0, x_0)),$$

for any two ideals $\mathfrak{a}, \mathfrak{b} \in \operatorname{Id}_P$.

First consider the direction $\Rightarrow$. The equality $\psi_{\mathfrak{a}}((E_0, x_0)) = \psi_{\mathfrak{b}}((E_0, x_0))$ is equivalent to the existence of an isomorphism $(\mathfrak{a}^{-1} \otimes E_0, 1 \otimes x_0) \cong (\mathfrak{b}^{-1} \otimes E_0, 1 \otimes x_0)$. Since $\mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{b}$, by 4.3, there exists an element $t \in K$ such that $\mathfrak{a} = \mathfrak{b}t$ and $t - 1 \in \mathfrak{f}\mathfrak{b}^{-1}$. So it is enough to show that the isomorphism

$$(11.3.32) \qquad\qquad \mathfrak{a}^{-1} \otimes E_0 \xrightarrow{t \otimes 1} \mathfrak{b}^{-1} \otimes E_0$$

given by multiplication by $t \otimes 1$, sends $1 \otimes x_0$ on the left to $1 \otimes x_0$ on the right. In other words, it is enough to show that the two elements $1 \otimes x_0, t \otimes x_0 \in \mathfrak{b}^{-1} \otimes E_0(\mathbb{C})$ agree.

We give an argument using period lattices. Write $E_0(\mathbb{C}) = \mathbb{C}/\mathfrak{c}$, where $\mathfrak{c}$ is a fractional ideal of K, and let $y \in \mathbb{C}$ be a coset representative of $x_0 \in \mathbb{C}/\mathfrak{c}$. Then the morphism (11.3.32) above is identified with

$$\mathbb{C}/\mathfrak{a}^{-1}\mathfrak{c} \xrightarrow{t} \mathbb{C}/\mathfrak{b}^{-1}\mathfrak{c}.$$

So what we want to show is equivalent to the congruence

$$ty \equiv y \mod \mathfrak{b}^{-1}\mathfrak{c}.$$

But since x_0 is an $\mathfrak{f}$-torsion element of $\mathbb{C}/\mathfrak{c}$, we have $y \in \mathfrak{f}^{-1}\mathfrak{c}$, and hence we have

$$(t-1)y \in \mathfrak{f}\mathfrak{b}^{-1} \cdot \mathfrak{f}^{-1}\mathfrak{c} = \mathfrak{b}^{-1}\mathfrak{c},$$

as desired.

Now consider the direction $\Leftarrow$. So assume $\psi_{\mathfrak{a}}(E_0, x_0) \cong \psi_{\mathfrak{b}}(E_0, x_0)$. This means there is an isomorphism

$$\mathbb{C}/\mathfrak{a}^{-1}\mathfrak{c} \xrightarrow{t} \mathbb{C}/\mathfrak{b}^{-1}\mathfrak{c},$$

given by multiplication by some element $t \in K^*$ with $(t) = \mathfrak{a}\mathfrak{b}^{-1}$, such that $tx_0 = x_0$. Therefore the diagram

$$
\begin{array}{ccc}
\mathfrak{f}^{-1}\mathfrak{c}/\mathfrak{c} & \xrightarrow{\mathrm{id}} & \mathfrak{f}^{-1}\mathfrak{c}/\mathfrak{c} \\
\downarrow & & \downarrow \\
\mathbb{C}/\mathfrak{a}^{-1}\mathfrak{c} & \xrightarrow{t} & \mathbb{C}/\mathfrak{b}^{-1}\mathfrak{c}
\end{array}
$$

commutes, since the two ways around the diagram agree on x_0, which is a generator of $\mathfrak{f}^{-1}\mathfrak{c}/\mathfrak{c}$. Therefore the difference map $t-1 \colon \mathfrak{f}^{-1}\mathfrak{c}/\mathfrak{c} \to \mathbb{C}/\mathfrak{b}^{-1}\mathfrak{c}$ is zero. This implies $(t-1)\mathfrak{f}^{-1}\mathfrak{c} \subseteq \mathfrak{b}^{-1}\mathfrak{c}$ and hence $t - 1 \in \mathfrak{f}\mathfrak{b}^{-1}$. It follows from 4.3 that $\mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{b}$. $\qquad\square$

Proposition 11.4. *Let $\mathfrak{f}$ be an integral ideal in O_K. Then we have equalities*

$$\mathcal{L}(\mathfrak{f})_{\mathrm{fl}} = \mathcal{L}(\mathfrak{f})_{\mathrm{red}} = \mathcal{L}[\mathfrak{f}]_{\mathrm{red}}$$

of closed subschemes of $\mathcal{L}$.

Proof. We have the following diagram of containments of closed subschemes of $\mathcal{L}$:

$$
\begin{array}{ccccc}
\mathcal{L}(\mathfrak{f})_{\mathrm{red}} & \xrightarrow{\ \alpha\ } & \mathcal{L}(\mathfrak{f})_{\mathrm{fl}} & \longrightarrow & \mathcal{L}(\mathfrak{f}) \\
\downarrow{\scriptstyle\beta} & & \downarrow & & \downarrow \\
\mathcal{L}[\mathfrak{f}]_{\mathrm{red}} & \longrightarrow & \mathcal{L}[\mathfrak{f}]_{\mathrm{fl}} & \longrightarrow & \mathcal{L}[\mathfrak{f}]
\end{array}
$$

(As an aside, we note that $\mathcal{L}[\mathfrak{f}]$ is finite flat of degree $N(\mathfrak{f})$ over O_H, by 4.3.11 of [14], and hence $\mathcal{L}[\mathfrak{f}]_{\mathrm{fl}} = \mathcal{L}[\mathfrak{f}]$.) Observe that α is an isomorphism, by (7.3), and so it is enough to show that β is an isomorphism. It is enough to show this after base change to $\mathbb{C}$, since β is a closed immersion and $\mathcal{L}[\mathfrak{f}]_{\mathrm{red}}$ is flat over O_K. Further, since the schemes in question are of finite type, it is enough to show that β induces a surjection on complex points, or in other words that the inclusion

$$\mathcal{L}(\mathfrak{f})(\mathbb{C}) \hookrightarrow \mathcal{L}[\mathfrak{f}](\mathbb{C})$$

is surjective. But this follows from 11.3, which says that $\mathcal{L}[\mathfrak{f}](\mathbb{C})$ is $\mathfrak{f}$-periodic. $\qquad\square$

Corollary 11.5. *The map $\mathcal{E}[\mathfrak{f}] \to \mathcal{L}$ factors through the closed subscheme $\mathcal{L}(\mathfrak{f})_{\mathrm{fl}}$ of $\mathcal{L}$.*

Proof. By functoriality, it factors through $\mathcal{L}[\mathfrak{f}]$. Because $\mathcal{E}[\mathfrak{f}]$ is reduced, it factors further through $\mathcal{L}[\mathfrak{f}]_{\mathrm{red}}$. Therefore, by 11.4, it factors through $\mathcal{L}(\mathfrak{f})_{\mathrm{fl}}$. $\qquad\square$

Proposition 11.6. *Let R be a flat O_K-algebra over which there is a CM elliptic curve E. Fix an ideal $\mathfrak{f} \subseteq O_K$, and write $G = O_K^*$. Let $\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}$ denote the base change of $\mathcal{L}(\mathfrak{f})_{\mathrm{fl}}$ from O_H to R. Then we have the following:*

(1) *The map $\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}) \to \mathcal{O}(E[\mathfrak{f}])^G$ induced by corollary 11.5 is injective.*

(2) *Its cokernel is a finitely generated R/nR-module, where n is the order of O_K^*.*

(3) *For any sufficiently divisible integer m, there exists a (unique) morphism making the following diagram commute:*

$$
\begin{array}{ccc}
\mathcal{O}(\mathcal{L}_R(m\mathfrak{f})_{\mathrm{fl}}) & \rightarrowtail & \mathcal{O}(E[m\mathfrak{f}])^G \\
\downarrow & \swarrow \quad & \downarrow \\
\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}) & \rightarrowtail & \mathcal{O}(E[\mathfrak{f}])^G.
\end{array}
$$

Proof. Write $\mathcal{L}_R = E/G \cong \mathbb{P}_R^1$. Then $\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}$ is a closed subscheme of $\mathcal{L}_R$, and by 11.5, we have the following containment of closed subschemes of E:

$$
E[\mathfrak{f}] \subseteq \mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_R} E.
$$

Let $I_{\mathfrak{f}}(R)$ denote the deal sheaf on $\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_R} E$ corresponding to $E[\mathfrak{f}]$; so we have the short exact sequence

(11.6.33) $$0 \longrightarrow I_{\mathfrak{f}}(R) \longrightarrow \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_R} E) \longrightarrow \mathcal{O}(E[\mathfrak{f}]) \longrightarrow 0.$$

Its long exact sequence of group cohomology begins

(11.6.34) $$0 \longrightarrow I_{\mathfrak{f}}(R)^G \longrightarrow \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_R} E)^G \longrightarrow \mathcal{O}(E[\mathfrak{f}])^G \longrightarrow H^1(G, I_{\mathfrak{f}}(R)).$$

We would like to simplify this sequence using the fact that the map

(11.6.35) $$\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}) \to \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_R} E)^G$$

is an isomorphism, which we will now show. We have the following diagram of G-equivariant quasi-coherent sheaves on $\mathcal{L}_R$ (dropping the usual direct-image notation for simplicity):

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{O}_{\mathcal{L}_R} & \longrightarrow & \mathcal{O}_E & \longrightarrow & M & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{O}_{\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}} & \longrightarrow & \mathcal{O}_{\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_R} E} & \longrightarrow & \bar{M} & \longrightarrow & 0,
\end{array}
$$

where the rows are exact, M and $\bar{M}$ being defined to be the cokernels as shown. We know $\mathcal{O}_{\mathcal{L}_R} = \mathcal{O}_E^G$, and so we have $(\mathbb{Q} \otimes_{\mathbb{Z}} M)^G = 0$ and hence $(\mathbb{Q} \otimes_{\mathbb{Z}} \bar{M})^G = 0$. Therefore the map (11.6.35) becomes an isomorphism after tensoring with $\mathbb{Q}$. To show it is an isomorphism, it is therefore enough to show it is surjective. Also observe that both sides are torsion free. So let b be a G-invariant element of $\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_R} E)$. Then we have $b = a/n$, for some $a \in \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}})$ and some integer $n \geqslant 1$. Therefore a becomes a multiple of n in $\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_R} E)$. But because $\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_R} E$ is faithfully flat over $\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}$, it must be a multiple of n already in $\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}})$. Therefore b is in $\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}})$, and so the map (11.6.35) is surjective, and hence an isomorphism.

Thus we can rewrite the long exact sequence (11.6.34) as

(11.6.36) $$0 \longrightarrow I_{\mathfrak{f}}(R)^G \longrightarrow \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}) \longrightarrow \mathcal{O}(E[\mathfrak{f}])^G \longrightarrow H^1(G, I_{\mathfrak{f}}(R)).$$

Using this sequence, we will prove parts (1)–(3).

(1): We will show $I_{\mathfrak{f}}(R)^G = 0$. First, observe that $I_{\mathfrak{f}}(R)^G$ is a flat-local construction in R: if R'/R is flat, we have $I_{\mathfrak{f}}(R') = R' \otimes_R I_{\mathfrak{f}}(R)$ and hence

$$
I_{\mathfrak{f}}(R')^G = (R' \otimes_R I_{\mathfrak{f}}(R))^G = R' \otimes_R I_{\mathfrak{f}}(R)^G
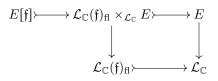$$

since taking invariants under the action of a finite group commutes with flat base change.

Second, since $I_{\mathfrak{f}}(R)$ is a submodule of $\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}})$, which by construction is flat over O_K, its invariant subgroup $I_{\mathfrak{f}}(R)^G$ is also flat over O_K and hence maps injectively to

$$\mathbb{C} \otimes_{O_K} I_{\mathfrak{f}}(R)^G = (\mathbb{C} \otimes_{O_K} R) \otimes_R I_{\mathfrak{f}}(R)^G = I_{\mathfrak{f}}(\mathbb{C} \otimes_{O_K} R)^G.$$

Therefore to show $I_{\mathfrak{f}}(R)^G = 0$, it is enough to do it in the case where R is a $\mathbb{C}$-algebra; and because any $\mathbb{C}$-algebra is flat over $\mathbb{C}$, we can apply the flat-local property again and conclude that it is enough to assume $R = \mathbb{C}$, which we will now do.

Summing up, we have the diagram

$$
\begin{array}{ccc}
E[\mathfrak{f}] \rightarrowtail \mathcal{L}_{\mathbb{C}}(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_{\mathbb{C}}} E & \longrightarrow & E \\
\downarrow & & \downarrow \\
\mathcal{L}_{\mathbb{C}}(\mathfrak{f})_{\mathrm{fl}} & \longrightarrow & \mathcal{L}_{\mathbb{C}}
\end{array}
$$

where $E \to \mathcal{L}_{\mathbb{C}}$ is a G-Galois cover of complex curves, the horizontal maps are closed immersions, and $E[\mathfrak{f}]$ and $\mathcal{L}_{\mathbb{C}}(\mathfrak{f})_{\mathrm{fl}}$ are reduced. Write $I_{\mathfrak{f}}(\mathbb{C}) = \bigoplus_Z I_Z$, where Z runs over the G-orbits of $E[\mathfrak{f}](\mathbb{C})$ and the ideal I_Z of $\mathcal{O}(\mathcal{L}_{\mathbb{C}}(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_{\mathbb{C}}} E)$ is the part of $I_{\mathfrak{f}}(\mathbb{C})$ supported at Z. It is then enough to show $I_Z^G = 0$ for each Z. So consider the filtration of I_Z by its powers:

$$I_Z \supseteq I_Z^2 \supseteq \cdots \supseteq I_Z^e = \{0\},$$

where e is the ramification index of E over $\mathcal{L}$ at Z, or equivalently the order of the stabilizer subgroup $H \subseteq G$ of a point $x \in Z$. Then it is enough to show $(I_Z^n/I_Z^{n+1})^G = 0$ for $n = 1, \dots, e-1$.

This holds vacuously if $e = 1$. So assume $e > 1$. For $n \leqslant e-1$, the G-representation I_Z^n/I_Z^{n+1} is the induced representation $\mathrm{Ind}_H^G(U^{\otimes n})$ where and $U = I_x/I_x^2$ is the cotangent space of E at x. Therefore we have

$$(I_Z^n/I_Z^{n+1})^G = (U^{\otimes n})^H.$$

Observe that as a representation of H, the cotangent space U is isomorphic to the restriction to H of the representation of $G = O_K^*$ on $\mathbb{C}$ given by usual multiplication. Therefore $U^{\otimes n}$ is the one-dimensional representation on which a generator $\zeta \in H$ acts as multiplication by ζ^n. But since $n < e$, and since e is the order of H, we have $\zeta^n \neq 1$. Therefore ζ acts nontrivially on $U^{\otimes n}$ and hence we have

$$(I_Z^n/I_Z^{n+1})^G = (U^{\otimes n})^H = 0,$$

as desired.

(2): By general properties of group cohomology, $H^1(G, I_{\mathfrak{f}}(R))$ is an R-module of exponent dividing n, and hence an R/nR-module. The cokernel in question is a sub-R-module of $H^1(G, I_{\mathfrak{f}}(R))$ and is therefore also an R/nR-module. It remains to show it is finitely generated. Since it is a quotient of $\mathcal{O}(E[\mathfrak{f}])^G$, it is enough to show that $\mathcal{O}(E[\mathfrak{f}])^G$ is finitely generated, and hence enough to show this locally on R. But locally E descends to some finitely generated O_K-algebra over which R is flat. Since the formation of $\mathcal{O}(E[\mathfrak{f}])^G$ commutes with flat base change, it is enough to show finite generation in the case where R is a finitely generated O_K-algebra. Here it holds because $E[\mathfrak{f}]$ is finite flat and R is noetherian.

(3): Write $I_{\mathfrak{f}} = I_{\mathfrak{f}}(R)$. Then by part (1), for any $m \geqslant 1$, we have a morphism of exact sequences

$$
\begin{array}{ccccccc}
0 & \longrightarrow & \mathcal{O}(\mathcal{L}_R(m\mathfrak{f})_{\mathrm{fl}}) & \longrightarrow & \mathcal{O}(E[m\mathfrak{f}])^G & \longrightarrow & H^1(G, I_{m\mathfrak{f}}) \\
& & \downarrow & & \downarrow & & \downarrow{\scriptstyle\alpha} \\
0 & \longrightarrow & \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}) & \longrightarrow & \mathcal{O}(E[\mathfrak{f}])^G & \longrightarrow & H^1(G, I_{\mathfrak{f}}).
\end{array}
$$

To prove (3), it is enough to show the map α above is zero for sufficiently divisible m. Since $I_{\mathfrak{f}}$ is torsion free, it is enough by lemma 11.7 below to show that the map $I_{m\mathfrak{f}} \to I_{\mathfrak{f}}$ is zero modulo n for sufficiently divisible m. Further, by part (2), it is enough to show this instead modulo each prime dividing n—that is, it is enough to show that for each prime $p \mid n$, there exists an integer m such that the map $I_{m\mathfrak{f}} \to I_{\mathfrak{f}}$ is zero modulo p.

So fix a prime $p \mid n$. Let E_p denote the reduction of E modulo p, which is an elliptic curve over R/pR. Then for any $j \geqslant 0$, we have a morphism of short exact sequences

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & I_{p^j\mathfrak{f}}/pI_{p^j\mathfrak{f}} & \longrightarrow & \mathcal{O}(\mathcal{L}_R(p^j\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_R} E_p) & \longrightarrow & \mathcal{O}(E_p[p^f\mathfrak{f}]) & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I_{\mathfrak{f}}/pI_{\mathfrak{f}} & \longrightarrow & \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}_R} E_p) & \longrightarrow & \mathcal{O}(E_p[\mathfrak{f}]) & \longrightarrow & 0.
\end{array}
$$

(Left-exactness is because $E[\mathfrak{f}]$ and $E[p^j\mathfrak{f}]$ are flat.) Now whether the fibers of E_p are supersingular or ordinary, the closed subschemes $E_p[p^j\mathfrak{f}]$ contain arbitrary nilpotent thickenings of $E_p[\mathfrak{f}]$, for large enough j. Since $\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}} E_p$ is a nilpotent thickening of $E_p[\mathfrak{f}]$, we can take j such that $E_p[p^j\mathfrak{f}]$ contains $\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}} \times_{\mathcal{L}} E_p$. Thus the map

$$I_{p^j\mathfrak{f}}/pI_{p^j\mathfrak{f}} \longrightarrow I_{\mathfrak{f}}/pI_{\mathfrak{f}}$$

is zero, and hence so is the map $I_{p^j\mathfrak{f}} \to I_{\mathfrak{f}}/pI_{\mathfrak{f}}$, as desired. $\qquad\square$

Lemma 11.7. *Let G be a finite group, and let n denote its order. Let $M \to N$ be a morphism of G-modules which vanishes modulo n, and assume N is n-torsion free. Then the induced map $H^i(G, M) \to H^i(G, N)$ is zero, for all $i \geqslant 1$.*

Proof. Since our given map $M \to N$ vanishes modulo n and N is n-torsion free, it factors as

$$
\begin{array}{ccc}
 & M & \\
 & \vdots \quad \searrow & \\
 & \downarrow & \\
 N & \xrightarrow{\ n\ } & N.
\end{array}
$$

Hence the induced map on cohomology factors similarly

$$
\begin{array}{ccc}
 & H^i(G, M) & \\
 & \vdots \quad \searrow & \\
 & \downarrow & \\
 H^i(G, N) & \xrightarrow{\ n\ } & H^i(G, N)
\end{array}
$$

However $H^i(G, N)$ is a n-torsion group for $i \geqslant 1$, because G has exponent dividing n. Therefore the bottom map is zero and hence so is the diagonal map. $\qquad\square$

Corollary 11.8. *With the notation of proposition 11.6, the map*

$$\left(\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}) \right)_{\hat{\mathfrak{f}}} \longrightarrow \left(\mathcal{O}(E[\mathfrak{f}])^G \right)_{\hat{\mathfrak{f}}}$$

of pro-rings is an isomorphism.

Proposition 11.9. *Let $\mathfrak{p}$ be a prime of O_K, let R be a finite unramified extension of $O_{K_\mathfrak{p}}$, and let E be a CM elliptic curve over R. Then for any integer $r \geqslant 0$, $\mathcal{O}(E[\mathfrak{p}^r])$ is $\Lambda_\mathfrak{p}$-normal over $O_{K_\mathfrak{p}}$.*

Proof. We follow (3.1) of [7], which is the analogous result for $\mathbb{G}_\mathrm{m}$.

For $r = 0$, it is clear. So we may assume that $r \geqslant 1$ and, by induction, that $\mathcal{O}(E[\mathfrak{p}^{r-1}])$ is $\Lambda_\mathfrak{p}$-normal over $O_{K_\mathfrak{p}}$.

The $\mathfrak{p}^r$-torsion $E[\mathfrak{p}^r]$ can be obtained by gluing the $\mathfrak{p}^{r-1}$-torsion $E[\mathfrak{p}^{r-1}]$ and the locus of exact order $\mathfrak{p}^r$, as follows. Let D_r denote $\mathcal{O}(E[\mathfrak{p}^r])$. Let π be a generator of $\mathfrak{p}O_{K_\mathfrak{p}}$, and consider the Lubin–Tate polynomial $h(z) \in R[z]$ for E with respect to the uniformizer π and some fixed local coordinate. So we have $h(z) = zg(z)$, where $g(z)$ is a monic Eisenstein polynomial with $g(0) = \pi$. Then D_r is identified with $R[z]/(h^{\circ r}(z))$. Because $h^{\circ r}(z) = h^{\circ r-1}(z) \cdot g(h^{\circ r-1}(z))$, we have the following diagram of quotients of $R[z]$:

$$
\begin{array}{ccc}
R[z]/(h^{\circ r}(z)) & \longrightarrow & R[z]/(h^{\circ r-1}(z)) \\
\downarrow & & \downarrow \\
R[z]/(g(h^{\circ r-1}(z))) & \longrightarrow & R[z]/(h^{\circ r-1}(z), g(h^{\circ r-1}(z))).
\end{array}
$$

Observe that $g(h^{\circ r-1}(z))$ is a monic Eisenstein polynomial. For degree reasons, it does not divide $h^{\circ r-1}(z)$, and so the least common multiple of these two polynomials is their product. Therefore we have

$$(h^{\circ r}(z)) = (h^{\circ r-1}(z)) \cap (g(h^{\circ r-1}(z))),$$

and hence the diagram above is a pull-back diagram. Further, if we put $B_r = R[z]/(g(h^{\circ r-1}(z)))$, then B_r is the ring of integers in a totally ramified extension of $K_\mathfrak{p}$. Let $\pi_r \in B_r$ denote the corresponding uniformizer, namely the coset of z. Thus we have a pull-back diagram

$$
\begin{array}{ccc}
D_r & \twoheadrightarrow & D_{r-1} \\
\downarrow & & \downarrow \\
B_r & \twoheadrightarrow & \bar{B}_r,
\end{array}
$$

where $\bar{B}_r = B_r/(h^{\circ r-1}(\pi_r))$. Further observe that the element $h^{\circ r-1}(\pi_r) \in B_r$ is a root of $g(z)$, which is an Eisenstein polynomial of degree $q - 1$, where we write $q = N(\mathfrak{p})$. Therefore we have $v_\mathfrak{p}(h^{\circ r-1}(\pi_r)) = 1/(q-1)$, where $v_\mathfrak{p}$ is the valuation normalized such that $v_\mathfrak{p}(\pi) = 1$.

Now suppose C is a sub-$\Lambda_\mathfrak{p}$-ring of $K_\mathfrak{p} \otimes_{O_{K_\mathfrak{p}}} D_r$ which is finite over $O_{K_\mathfrak{p}}$. The maximality statement we wish to prove is that C is contained in $D_r = B_r \times_{\bar{B}_r} D_{r-1}$. By induction, D_{r-1} is $\Lambda_\mathfrak{p}$-normal over $O_{K_\mathfrak{p}}$, and hence the image of C in $K_\mathfrak{p} \otimes_{O_{K_\mathfrak{p}}} D_{r-1}$ is contained in D_{r-1}. Similarly, since B_r is a maximal order in the usual sense, the image of C in $K_\mathfrak{p} \otimes_{O_{K_\mathfrak{p}}} B_r$ is contained in B_r. Putting the two together, we have the containment $C \subseteq B_r \times D_{r-1}$.

To show $C \subseteq B_r \times_{\bar{B}_r} D_{r-1}$, let us suppose that this does not hold. Then there is an element $(b, \overline{f(z)}) \in C \subseteq B_r \times D_{r-1}$ such that b and $\overline{f(z)}$ do not become equal in $\bar{B}_r$. In other words, we have

$$v_\mathfrak{p}(b - f(\pi_r)) < 1/(q-1).$$

Further we can choose $(b, \overline{f(z)}) \in C$ such that $v_\mathfrak{p}(b - f(\pi_r))$ is as small as possible. Write $a = v_\mathfrak{p}(b - f(\pi_r))$. Since C is a sub-$\Lambda_\mathfrak{p}$-ring of $K_\mathfrak{p} \otimes_{O_{K_\mathfrak{p}}} D_r$, we know

$$(b, \overline{f(z)})^q - \psi_\mathfrak{p}((b, \overline{f(z)})) \in \pi C$$

The left side can be simplified using the fact $\psi_{\mathfrak{p}}(z) = h(z)$ on D_r:

$$(b, \overline{f(z)})^q - \psi_{\mathfrak{p}}((b, \overline{f(z)})) = (b^q - f^*(h(\pi_r)), \overline{f(z)}^q - \overline{f^*(h(z))})$$

where $f^*(z)$ the polynomial obtained by applying the Frobenius map to each coefficient of $f(z)$. Therefore by the minimality of a, we have

$$a \leqslant v_{\mathfrak{p}}\left(\frac{b^q - f^*(h(\pi_r))}{\pi} - \frac{f(z)^q - f^*(h(z))}{\pi}\Big|_{z=\pi_r}\right) = v_{\mathfrak{p}}\left(\frac{b^q - f(\pi_r)^q}{\pi}\right)$$

$$= v_{\mathfrak{p}}\left(\frac{(b - f(\pi_r))^q}{\pi} + (b - f(\pi_r)) \cdot c(b, f(\pi_r))\right)$$

where $c(X, Y)$ denotes the polynomial

$$\frac{(X^q - Y^q) - (X - Y)^q}{\pi(X - Y)} \in O_{K_{\mathfrak{p}}}[X, Y].$$

But again by the minimality of a, we know $a \leqslant v_{\mathfrak{p}}(b - f(\pi_r))$. Therefore we have

$$a \leqslant v_{\mathfrak{p}}\left(\frac{(b - f(\pi_r))^q}{\pi}\right) = qa - 1$$

and hence $a \geqslant 1/(q - 1)$. This contradicts the assumption $a < 1/(q - 1)$. □

Lemma 11.10. *Let $A = O_K[1/t]$, for some $t \in O_K$, and let R be a Λ-ring, finite étale over A, over which there exists a CM elliptic curve E. Then for any ideal $\mathfrak{f} \subseteq O_K$, the Λ-ring $\mathcal{O}(E[\mathfrak{f}])$ is Λ-normal over A.*

Proof. Let S denote the maximal Λ-order over A in $K \otimes_{O_K} \mathcal{O}(E[\mathfrak{f}])$. Then we have an inclusion $\mathcal{O}(E[\mathfrak{f}]) \subseteq S$ of finite flat A-algebras. Therefore it is an equality if $O_{K_{\mathfrak{p}}} \otimes_A \mathcal{O}(E[\mathfrak{f}]) = O_{K_{\mathfrak{p}}} \otimes_A S$ for all primes $\mathfrak{p} \nmid t$. Thus it is enough to show that $O_{K_{\mathfrak{p}}} \otimes_A \mathcal{O}(E[\mathfrak{f}])$ is $\Lambda_{\mathfrak{p}}$-normal over $O_{K_{\mathfrak{p}}}$ for all $\mathfrak{p} \nmid t$.

Write $\mathfrak{f} = \mathfrak{p}^r \mathfrak{g}$, where $\mathfrak{p} \nmid \mathfrak{g}$. Then putting $R_{\mathfrak{p}} = O_{K_{\mathfrak{p}}} \otimes_A R$, we have

$$O_{K_{\mathfrak{p}}} \otimes_A \mathcal{O}(E[\mathfrak{f}]) = O_{K_{\mathfrak{p}}} \otimes_A (\mathcal{O}(E[\mathfrak{p}^r]) \otimes_R \mathcal{O}(E[\mathfrak{g}]))$$
$$= (O_{K_{\mathfrak{p}}} \otimes_A \mathcal{O}(E[\mathfrak{p}^r])) \otimes_{R_{\mathfrak{p}}} (O_{K_{\mathfrak{p}}} \otimes_A \mathcal{O}(E[\mathfrak{g}]))$$
$$= \mathcal{O}(E_{R_{\mathfrak{p}}}[\mathfrak{p}^r]) \otimes_{R_{\mathfrak{p}}} \mathcal{O}(E_{R_{\mathfrak{p}}}[\mathfrak{g}])$$
$$= \prod_{R'} \mathcal{O}(E_{R'}[\mathfrak{p}^r]),$$

where R' runs over all irreducible direct factors of the finite étale $O_{K_{\mathfrak{p}}}$-algebra $\mathcal{O}(E_{R_{\mathfrak{p}}}[\mathfrak{g}])$. Therefore it is enough to show that each $\mathcal{O}(E_{R'}[\mathfrak{p}^r])$ is $\Lambda_{\mathfrak{p}}$-normal over $O_{K_{\mathfrak{p}}}$. But this follows from 11.9. □

Proposition 11.11. *Let $A = O_K[1/t]$, for some $t \in O_K$. Put $R = O_H[1/t]$ and assume there exists a CM elliptic curve E over R. Write $G = O_K^*$. Then the maximal Λ-order in $K \otimes_A \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\text{fl}})$ over A is $\mathcal{O}(E[\mathfrak{f}])^G$.*

Proof. By lemma 11.10 and part (2) of proposition 2.2, the G-invariant subring $\mathcal{O}(E[\mathfrak{f}])^G$ is Λ-normal over A. Since $K \otimes_A \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\text{fl}}) = K \otimes_A \mathcal{O}(E[\mathfrak{f}])^G$, by part (2) of proposition 11.6, we can conclude that $\mathcal{O}(E[\mathfrak{f}])^G$ is the maximal Λ-order over A in $K \otimes_A \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\text{fl}})$. □

Theorem 11.12. *Let $\mathcal{O}(\mathcal{L}(\mathfrak{f})_{\text{fl}})^{\sim}$ denote the maximal Λ-order over O_K in $K \otimes_{O_K} \mathcal{O}(\mathcal{L}(\mathfrak{f})_{\text{fl}})$. Then*

(1) *$\mathcal{O}(\mathcal{L}(\mathfrak{f})_{\text{fl}})^{\sim}$ is isomorphic as a Λ-ring to the ray class algebra $R_{O_K, P}(\mathfrak{f})$.*
(2) *The map*

$$\left(\mathcal{O}(\mathcal{L}(\mathfrak{f})_{\text{fl}})\right)_{\hat{\mathfrak{f}}} \longrightarrow \left(\mathcal{O}(\mathcal{L}(\mathfrak{f})_{\text{fl}})^{\sim}\right)_{\hat{\mathfrak{f}}}$$

is an isomorphism of pro-rings.

(3) *If a prime number divides the index $[\mathcal{O}(\mathcal{L}(\mathfrak{f})_{\mathrm{fl}})^{\sim} : \mathcal{O}(\mathcal{L}(\mathfrak{f})_{\mathrm{fl}})]$ then it divides the order of the unit group O_K^*.*

Proof. (1): Since $\mathcal{O}(\mathcal{L}(\mathfrak{f})_{\mathrm{fl}})^{\sim}$ is the maximal Λ-order over O_K in $K \otimes_{O_K} \mathcal{O}(\mathcal{L}(\mathfrak{f})_{\mathrm{fl}})$, and since $R_{O_K,P}(\mathfrak{f})$ is that in $K \otimes_{O_K} R_{O_K,P}(\mathfrak{f})$, it is enough to show there is an isomorphism

$$\mathcal{L}(\mathfrak{f})(\bar{\mathbb{Q}}) \cong \mathrm{DR}_P(\mathfrak{f})$$

of Id_P-sets, but this is follows immediately from part (2) of proposition 11.3.

(2): Since the rings

$$A = O_K[\mathfrak{q}^{-1}]$$

for any two primes $\mathfrak{q} \subset O_K$ form a cover of O_K, it is enough to prove the map of pro-rings is an isomorphism after base change from O_K to any two such A. By Shimura's theorem ([14], prop. 4.2.2), there are at least two primes $\mathfrak{q} \subset O_K$ such that there exists a CM elliptic curve over $R = O_H \otimes_{O_K} A$. (In fact, he proves there are infinitely many.) So fixing A and a CM elliptic curve E over $O_H \otimes_{O_K} A$, it is enough to show that

$$(11.12.37) \qquad \left(A \otimes_{O_K} \mathcal{O}(\mathcal{L}(\mathfrak{f})_{\mathrm{fl}}) \right)_{\mathfrak{f}} \longrightarrow \left(A \otimes_{O_K} \mathcal{O}(\mathcal{L}(\mathfrak{f})_{\mathrm{fl}})^{\sim} \right)_{\mathfrak{f}}$$

is an isomorphism of pro-rings.

But we also have

$$A \otimes_{O_K} \mathcal{O}(\mathcal{L}(\mathfrak{f})_{\mathrm{fl}}) = R \otimes_{O_H} \mathcal{O}(\mathcal{L}(\mathfrak{f})_{\mathrm{fl}}) = \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}})$$

and hence by part (1) of proposition 2.2

$$\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}})^{\sim} = A \otimes_{O_K} \mathcal{O}(\mathcal{L}(\mathfrak{f})_{\mathrm{fl}})^{\sim}.$$

Therefore (11.12.37) can be rewritten as

$$(11.12.38) \qquad \left(\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}) \right)_{\mathfrak{f}} \longrightarrow \left(\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}})^{\sim} \right)_{\mathfrak{f}}.$$

We know further that the map

$$\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}})^{\sim} \longrightarrow \mathcal{O}(E[\mathfrak{f}])^G$$

is an isomorphism by 11.11. So the map (11.12.38) can in turn be rewritten as

$$(11.12.39) \qquad \left(\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}) \right)_{\mathfrak{f}} \longrightarrow \left(\mathcal{O}(E[\mathfrak{f}])^G \right)_{\mathfrak{f}},$$

and this is an isomorphism of pro-rings by 11.8.

(3): It is enough to show these properties locally on O_K. So as above, it is enough to show them after base change to $A = O_K[\mathfrak{q}^{-1}]$, where $\mathfrak{q}$ is a prime of O_K such that there is a CM elliptic curve E over $R = O_H \otimes_{O_K} A$.

Then the map $A \otimes_{O_K} \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}) \to A \otimes_{O_K} \mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}})^{\sim}$ is identified with

$$\mathcal{O}(\mathcal{L}_R(\mathfrak{f})_{\mathrm{fl}}) \longrightarrow \mathcal{O}(E[\mathfrak{f}])^G.$$

By part (2) of proposition 11.6, the image of this map is of finite index divisible only by the primes dividing the order of O_K^*. $\qquad\square$

12. FURTHER QUESTIONS

Is it possible to use Λ-schemes of finite type to generate other large abelian extensions, beyond the Kroneckerian explicit class field theories? We will formulate a range of such questions in this section, some of which it is reasonable to hope have a positive answer and some which are more ambitious.

12.1. *Λ-geometric field extensions.* So far, we have mostly been interested in what in the introduction we called Λ-*refinements* of explicit class field theories—that is, in generating ray class algebras instead of abelian field extensions. But hungry for positive answers, we will give weaker, field-theoretic formulations here.

Let K be a number field, and write

$$\Lambda = \Lambda_{O_K, M_K} \quad \text{and} \quad R(\mathfrak{f}) = R_{O_K, M_K}(\mathfrak{f}).$$

For any separated Λ-scheme X of finite type over O_K, consider the extension of K obtained by adjoining the coordinates of the $\mathfrak{f}$-periodic points, for all cycles $\mathfrak{f}$:

$$K(X) := \bigcup_{\mathfrak{f}} K(X(\mathfrak{f})(\bar{K})).$$

For instance, we have the following:

(1) If $K = \mathbb{Q}$ and X is $\mathbb{G}_{\mathrm{m}}$ with the toric Λ-structure, then Then $K(X)$ is the maximal abelian extension $\bigcup_n \mathbb{Q}(\zeta_n)$.

(2) If $K = \mathbb{Q}$ and $X = \mathbb{A}^1$ with the Chebyshev Λ-structure, then $K(X)$ is the maximal totally real abelian extension $\bigcup_n \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

(3) K is imaginary quadratic, X is $\mathbb{P}^1_{O_H}$ with the Lattès Λ-structure. Then $K(X)$ is the maximal abelian extension of K.

(4) If K is general and $X = \operatorname{Spec} R(\mathfrak{f})$, then $K(X)$ is the ray class field $K(\mathfrak{f})$.

(5) $K(X_1 \sqcup X_2)$ is the compositum $K(X_1)K(X_2)$

Let us say that an abelian extension L/K is *Λ-geometric* if there exists an X as above such that $L \subseteq K(X)$. First observe that any finite extension of a Λ-geometric extension is Λ-geometric, by (4) and (5) above. Therefore there is no maximal Λ-geometric extension unless, as in the examples above, the maximal abelian extension itself is Λ-geometric.

(Q4) Are there number fields other than $\mathbb{Q}$ and imaginary quadratic fields for which the maximal abelian extension is Λ-geometric?

It is natural to consider Shimura's generalization of Kronecker's theory to CM fields and abelian varieties. We expect that it can be realized in our framework, or at least that some version of it. But note that, assuming $[K : \mathbb{Q}] > 2$, the maximal abelian extension generated by Shimura's method is an infinite subextension of the maximal abelian extension itself—the relative Galois group is an infinite group of exponent 2. (See [20][18][22].)

(Q5) Let K be a CM field of degree greater than 2. Is Shimura's extension Λ-geometric? If so, is there an infinite extension of it which is Λ-geometric?

12.2. *Production of Λ-schemes from ray class algebras.* It appears difficult to find Λ-schemes of finite type which generate large infinite abelian extensions. Every example we know ultimately comes from varieties with complex multiplication. Here we will consider an alternative—the possibility of manufacturing Λ-schemes of finite type by interpolating the ray class schemes $\operatorname{Spec}(R(\mathfrak{f}))$, in the way that $\mathbb{G}_{\mathrm{m}}$ can be viewed as interpolating the μ_n as n varies. This raises some questions which have the flavor of algebraic number theory more than the geometric questions above, and hence have a special appeal.

Let $\mathfrak{r}$ be a product of real places of K, and let X a reduced Λ-scheme of finite type over O_K. Assume further that the union

$$\bigcup_{\mathfrak{f} \in Z(P, \mathfrak{r})} X(\mathfrak{f})$$

of the closed subschemes $X(\mathfrak{f})$ is Zariski dense in X. If it is not, replace X with the closure. Then all the information needed to construct X is in principle available

inside the function algebra of

$$\text{colim}_{\mathfrak{f} \in Z(P,\mathfrak{r})} X(\mathfrak{f}).$$

To be sure, this ind-scheme and X are quite far apart, much as an abelian variety and its p-divisible groups are. But pressing on, if X satisfies the property in (Q2) in the introduction, then this colimit would be isomorphic to

$$\text{colim}_{\mathfrak{f} \in Z(P,\mathfrak{r})} \left(\text{Spec } R(\mathfrak{f}) \right),$$

and so all the information need to construct X is in principle available in projective limit

$$R^{[\mathfrak{r}]} = \lim_{\mathfrak{f} \in Z(P,\mathfrak{r})} R(\mathfrak{f}),$$

which can be viewed as a construction purely in the world of algebraic number theory in that it depends only on K and $\mathfrak{r}$ and not on any variety X.

For example in the cyclotomic context, where $K = \mathbb{Q}$ and $\mathfrak{r} = \infty$, the injective map

$$\mathbb{Z}[x^{\pm 1}] \longrightarrow \lim_n \mathbb{Z}[x]/(x^n - 1) = R^{[\infty]}$$

realizes the function algebra of $\mathbb{G}_m$ as a dense finitely generated sub-Λ-ring of $R^{[\infty]}$.

We can ask whether similar subrings exist for general K:

(Q6) Does $R^{[\mathfrak{r}]}$ have a dense sub-O_K-algebra which is finitely generated as an O_K-algebra? Does it have a dense sub-Λ-ring which is finitely generated as an O_K-algebra?

It might be possible to cook up such a subring purely algebraically, instead of going through geometry.

12.3. *The cotangent space.* One first step in finding such a subring might be to guess its dimension by looking at the cotangent space of the ray class algebras at a point modulo $\mathfrak{p}$. For example, the cotangent space of μ_{p^n} modulo p at the origin is 1-dimensional, at least if $n \geqslant 1$.

For any ideal $\mathfrak{a} \in \text{Id}_{M_K}$ (and $\mathfrak{r}$ still a product of real places), let $I_\mathfrak{a}$ denote the kernel of the morphism

(12.3.40) $R(\mathfrak{r}\mathfrak{a}) \xrightarrow{\psi_\mathfrak{a}} R(\mathfrak{r}) = O_{K(\mathfrak{r})}.$

So we have an exact sequence

$$0 \longrightarrow I_\mathfrak{a} \longrightarrow R(\mathfrak{r}\mathfrak{a}) \xrightarrow{\psi_\mathfrak{a}} O_{K(\mathfrak{r})} \longrightarrow 0.$$

Therefore $I_\mathfrak{a}/I_\mathfrak{a}^2$ is naturally an $O_{K(\mathfrak{r})}$-module. It is finitely generated since $R(\mathfrak{r}\mathfrak{a})$ is noetherian, being finite over $\mathbb{Z}$.

(Q7) Given a maximal ideal $\mathfrak{q} \subset O_{K(\mathfrak{r})}$ with residue field k, is the dimension

$$\dim_k(k \otimes_{O_{K(\mathfrak{r})}} I_\mathfrak{a}/I_\mathfrak{a}^2)$$

constant for large $\mathfrak{a}$?

If so, can it be expressed in terms of the classical algebraic number theoretic invariants of K? One might hope it is the number of places of K at infinity.

REFERENCES

[1] *Théorie des intersections et théorème de Riemann-Roch.* Lecture Notes in Mathematics, Vol. 225. Springer-Verlag, Berlin-New York, 1971. Séminaire de Géométrie Algébrique du Bois-Marie 1966–1967 (SGA 6), Dirigé par P. Berthelot, A. Grothendieck et L. Illusie. Avec la collaboration de D. Ferrand, J. P. Jouanolou, O. Jussila, S. Kleiman, M. Raynaud et J. P. Serre.
[2] Stacks Project. http://stacks.math.columbia.edu, 2017.
[3] James Borger. Basic geometry of Witt vectors, I: The affine case. arXiv:0801.1691v5.
[4] James Borger. Basic geometry of Witt vectors, II: Spaces. arXiv:1006.0092v1.

[5] James Borger. Λ-rings and the field with one element. arXiv:0906.3146v1.

[6] James Borger and Bart de Smit. Lambda actions of rings of integers. arXiv:1105.4662.

[7] James Borger and Bart de Smit. Galois theory and integral models of Λ-rings. *Bull. Lond. Math. Soc.*, 40(3):439–446, 2008.

[8] James Borger and Ben Wieland. Plethystic algebra. *Adv. Math.*, 194(2):246–283, 2005.

[9] F. J. B. J. Clauwens. Commuting polynomials and λ-ring structures on **Z**[x]. *J. Pure Appl. Algebra*, 95(3):261–269, 1994.

[10] A. A. Davydov. Periodic λ-rings and periods of finite groups. *Mat. Sb.*, 188(8):75–82, 1997.

[11] Pierre Deligne and Kenneth A. Ribet. Values of abelian *L*-functions at negative integers over totally real fields. *Invent. Math.*, 59(3):227–286, 1980.

[12] Jesse Elliott. Binomial rings, integer-valued polynomials, and λ-rings. *J. Pure Appl. Algebra*, 207(1):165–185, 2006.

[13] Alexander Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III. *Inst. Hautes Études Sci. Publ. Math.*, (28):255, 1966.

[14] Lance Gurney. *Elliptic curves with complex multiplication and Λ-structures*. PhD thesis, Australian National University, 2015.

[15] André Joyal. δ-anneaux et λ-anneaux. *C. R. Math. Rep. Acad. Sci. Canada*, 7(4):227–232, 1985.

[16] Gérard Laumon and Laurent Moret-Bailly. *Champs algébriques*, volume 39 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, 2000.

[17] John Milnor. *Dynamics in one complex variable*, volume 160 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, third edition, 2006.

[18] A. I. Ovseevič c. Abelian extensions of fields of CM type. *Funkcional. Anal. i Priložen.*, 8(1):16–24, 1974.

[19] J.-P. Serre. Complex multiplication. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 292–296. Thompson, Washington, D.C., 1967.

[20] Goro Shimura. On the class-fields obtained by complex multiplication of abelian varieties. *Osaka Math. J.*, 14:33–44, 1962.

[21] Takeo Uramoto. Semi-galois Categories II: An arithmetic analogue of Christol's theorem. arXiv:1710.01021v3.

[22] Wafa Wei. Moduli fields of CM-motives applied to Hilbert's 12-th problem. `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.57.5573`.

[23] Clarence Wilkerson. Lambda-rings, binomial domains, and vector bundles over **C**P(∞). *Comm. Algebra*, 10(3):311–328, 1982.

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

Email address: `james.borger@anu.edu.au`, `desmit@math.leidenuniv.nl`