ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION AND Λ-STRUCTURES

Lance Rory Gurney

July 2015

Thesis submitted for the degree Doctor of Philosophy
of the Australian National University

DECLARATION

The work in this thesis is my own except where otherwise stated.

Lance Rory Gurney

The tears stream down my cheeks from my unblinking eyes. What makes me weep so? From time to time. There is nothing saddening here. Perhaps it is liquefied brain.

— Samuel Beckett, The Unnamable.

ABSTRACT

This thesis examines the relationship between elliptic curves with complex multiplication and Lambda structures. Our main result is to show that the moduli stack of elliptic curves with complex multiplication, and the universal elliptic curve with complex multiplication over it, both admit Lambda structures and that the structure morphism is a Lambda morphism. This implies that elliptic curves with complex multiplication can be canonically lifted to the Witt vectors of the base (these are big and global Witt vectors). We also show that elliptic curves with complex multiplication of Shimura type are precisely those admitting Lambda structures. Along the way, we present a detailed study of families of elliptic curves with complex multiplication over arbitrary bases, give new derivations of the local reciprocity map and the global reciprocity map associated to an imaginary quadratic field, construct a new flat, affine and pro-smooth rigidification of the moduli stack of elliptic curves with complex multiplication and exhibit a relationship between perfect Lambda schemes and periods, both p-adic and analytic.

ACKNOWLEDGEMENTS

I would like to thank my mum and dad, Ruth and Henry, and my brothers, Callum and Scott, who, despite giving up years ago wondering when I was going to get a proper job, have constantly supported and encouraged me in my mathematical endeavours.

I would like to thank the *Bonney Street Babes* — Shellaine, Cassie, Harriet (and Seb!) — without whom this long and sometimes tiresome journey would not have been as fun, bright, wonderful and full of love.

Finally, I would like to thank Jim Borger. Jim has been my supervisor through my honours, masters and finally doctoral studies. It goes without saying that I would not be the mathematician I am today if had not had the benefit of his mathematical insight, patience and absolute generosity and for that I am truly thankful. But Jim was not only my supervisor, he has also been a good friend, and as I step out into mathematical wilderness on my own I don't think I could have ask for a better person to lead me there.

CONTENTS

INTRODUCTION

This thesis began as an attempt to answer the question:

> Q: What do elliptic curves with complex multiplication and Λ-structures have to do with one another?

The reader is probably somewhat familiar with first term, less likely so with the second. Even if he or she is familiar with both, why such a question might have an answer worth finding is probably not clear at all. So we will begin by explaining how both of these terms are related to a third: class field theory.

Let us remind the reader of the relationship between elliptic curves with complex multiplication and class field theory. For all that follows we fix an imaginary quadratic field K, with ring of integers $\mathrm{O_K}$. If L/K is a finite extension, an elliptic curve with complex multiplication by $\mathrm{O_K}$ over L, here on called a CM elliptic curve over L, is an elliptic curve E/L with the property that its ring of endomorphisms $\mathrm{End_L(E)}$ is isomorphic to $\mathrm{O_K}$. For a general elliptic curve E/L, the Tate module $\mathrm{T(E)} = \lim_n \mathrm{E}[n](\mathrm{L^{sep}})$ is a rank two $\widehat{\mathbf{Z}}$-module equipped with an action of $\mathrm{G(L^{sep}/L)}$. However, when E/L is a CM elliptic curve, this rank two $\widehat{\mathbf{Z}}$-module becomes a rank one $\widehat{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathrm{O_K}$-module and so the action of $\mathrm{G(L^{sep}/L)}$ is defined by a character

$$\rho_{\mathrm{E/L}} : \mathrm{G(L^{ab}/L)} = \mathrm{G(L^{sep}/L)^{ab}} \to (\widehat{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathrm{O_K})^{\times}.$$

In particular, it follows that extensions of L generated by torsion points of E are abelian over L. It is then known that if one can find a CM elliptic curve E/K defined over K itself, the resulting character

$$\rho_{\mathrm{E/K}} : \mathrm{G(K^{ab}/K)} \to (\widehat{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathrm{O_K})^{\times}$$

is injective from which it follows that every abelian extension of K is realised as a sub-extension of one generated by the torsion points of E — thus realising the class field theory of K.

In general there do not exist CM elliptic curves defined over K. The smallest field of definition of a CM elliptic curve is the Hilbert class field H/K (the maximal abelian, everywhere unramified extension of K). If E/H is such a curve then the extensions of H generated by its torsion points are abelian over H, but they are not necessarily abelian over K. If one is still interested in the class field theory of K, this problem can be overcome by considering certain $\mathrm{O_K^\times} = \mathrm{Aut_H(E)}$ invariant maps

$$w : \mathrm{E} \to \mathbf{P}^1_{\mathrm{H}},$$

called Weber functions. The extensions of K generated by the co-ordinates of the images of torsion points of E under a fixed Weber function are abelian, and every abelian extension of K is a sub-extension of one of these — again realising the class field theory of K. Therefore, if one is interested in the class field theory of K one need go no further than CM elliptic curves.

Now let us explain the relationship between Λ-structures and class field theory. First, a Λ-structure on a flat $\mathrm{Spec(O_K)}$-scheme X (we will say more about the non-flat case later) is nothing more than a commuting family endomorphisms

$$\psi^{\mathfrak{a}} : \mathrm{X} \to \mathrm{X}$$

indexed by the non-zero ideals $\mathfrak{a}$ of $\mathrm{O_K}$ such that for any two ideals $\mathfrak{a}, \mathfrak{b}$ we have $\psi^{\mathfrak{a}} \circ \psi^{\mathfrak{b}} = \psi^{\mathfrak{a}\mathfrak{b}}$ and with the property that for each prime ideal $\mathfrak{p}$, the restriction of $\psi^{\mathfrak{p}}$ to the fibre $\mathrm{X_\mathfrak{p}} := \mathrm{X} \times_{\mathrm{Spec(O_K)}} \mathrm{Spec(O_K/\mathfrak{p})}$ is the $\mathrm{N}\mathfrak{p}$-power Frobenius endomorphism

$$\mathrm{Fr}^{\mathrm{N}\mathfrak{p}} : \mathrm{X_\mathfrak{p}} \to \mathrm{X_\mathfrak{p}}.$$

We call the endomorphisms $\psi^{\mathfrak{a}}$ (for all $\mathfrak{a}$) a commuting family of Frobenius lifts. The resulting notion of a Λ-morphism of Λ-schemes $f : \mathrm{X} \to \mathrm{Y}$ being one that commutes with the Frobenius lifts. The $\mathrm{O_K}$-scheme $\mathrm{Spec(O_K)}$ has a unique Λ-structure with Frobenius lifts all equal to the identity and if L/K is an abelian extension with ring of integers $\mathrm{O_L}$ then (ignoring the ramified primes) the finite locally free $\mathrm{O_K}$-scheme $\mathrm{Spec(O_L)}$ admits a unique Λ-structure as well. More generally, if S is any finite locally free $\mathrm{Spec(O_K)}$-scheme equipped with a Λ-structure then the extension of K generated by the co-ordinates of S (in any affine embedding) is an abelian extension of K. The link between Λ-structures

and class field theory appears. These observations also have the following implication. If X a Λ-scheme over $\mathrm{Spec}(\mathrm{O_K})$ and $0_\mathrm{X} : \mathrm{Spec}(\mathrm{O_K}) \to \mathrm{X}$ a Λ-morphism then (under certain hypotheses) for each ideal $\mathfrak{a}$ the scheme $\mathrm{X}[\mathfrak{a}] := \psi^{\mathfrak{a}*}(0_\mathrm{X}) \subset \mathrm{X}$ is a finite locally free Λ-scheme over $\mathrm{Spec}(\mathrm{O_K})$. Therefore, the extension of K generated by the coordinates of $\mathrm{X}[\mathfrak{a}]$ will be abelian.

With this in hand, let us return to CM elliptic curves. It now turns out that if E/K is a CM elliptic curve, writing $\mathscr{E} \to \mathrm{Spec}(\mathrm{O_K})$ for the Néron model of E/K, the flat $\mathrm{O_K}$-scheme $\mathscr{E}$ admits a unique Λ-structure (ignoring the primes of bad reduction for E/K) and the morphism

$$0_\mathscr{E} : \mathrm{Spec}(\mathrm{O_K}) \to \mathscr{E}$$

is a Λ-morphism. Moreover, for each integer $n \geq 0$, viewing $(n) \subset \mathrm{O_K}$ as an ideal, we have that $\psi^{(n)*}(0_\mathscr{E}) = \mathscr{E}[n]$ is the n-torsion of $\mathscr{E}$ which is now a finite locally free Λ-scheme. It is now also natural to ask whether in general there exist CM elliptic curves E/H defined over the Hilbert class field whose Néron models admit Λ-structures and this turns out to be a subtle question.

At this point, we should note that everything we have said so far is the work of others. Indeed, the theory of complex multiplication and its relationship with class field theory is classical and has a very long history and to give a list of names would be very difficult. The theory of Λ-schemes and Λ-structures is due to Borger ([**4**], [**5**]), and the relationship between Λ-structures and class field theory is due to Borger-de Smit ([**7**], [**8**]) and indeed it was my advisor James Borger who originally posed the question at the beginning of this introduction and the more specific one asking for the existence of CM elliptic curves E/H over the Hilbert class field with Λ-structures. This second question we can now answer:

0.0.1 Theorem. — (i) *There always exists a* CM *elliptic curve* E/H *over the Hilbert class field whose Néron model admits a* Λ*-structure.*

(ii) *The Néron model of a* CM *elliptic curve* E/H *admits a* Λ*-structure if and only if the extension of* K *generated by its torsion is abelian over* K.

CM elliptic curves (over arbitrary abelian extensions of K) with the property that the extensions generated by their torsion is abelian over K were introduced originally by Shimura and are now called CM elliptic curves of Shimura type. Indeed, it is using results of Shimura that, after proving (ii) we are able to prove (i). It worth pointing out that CM elliptic curves of Shimura type have been studied by several authors, with particular reference to their L-functions

and the Birch-Swinnerton-Dyer Conjecture. Indeed, the papers of Coates-Wiles [**13**] and Rubin [**30**] concern curves of this type.

Let us now also answer the question posed in the first paragraph:

> Q: What do elliptic curves with complex multiplication and Λ-structures have to do with one another?
>
> A: Everything!

The central theorem we aim to prove is the following and explains our answer to the question above.

0.0.2 Theorem. — *Let $\mathscr{M}_{\mathrm{CM}}$ denote the moduli stack of* CM *elliptic curves and let $\mathscr{E} \to \mathscr{M}_{\mathrm{CM}}$ denote the universal* CM *elliptic curve. Then both $\mathscr{E}$ and $\mathscr{M}_{\mathrm{CM}}$ admit canonical Λ-structures and the morphism $\mathscr{E} \to \mathscr{M}_{\mathrm{CM}}$ is a Λ-morphism.*

The reader will probably have noticed that we have not even defined what it means for a general (non-flat) scheme, let alone a stack, to have a Λ-structure and in fact we do not propose to define Λ-structures on stacks in this thesis (not because it isn't possible to do so, only because doing so would lead us into the nightmarish realm of 2-monads on 2-categories). In any case, the definition of Λ-structure we have given for a flat $\mathrm{O_K}$-scheme admits an obvious naive generalisation — that of a commuting family of Frobenius lifts — though it is not the correct one. Before we explain the correct definition, and the actual meaning of (0.0.2), let us describe the naive Λ-structure on $\mathscr{M}_{\mathrm{CM}}$.

If S is an $\mathrm{O_K}$-scheme then $\mathscr{M}_{\mathrm{CM}}(\mathrm{S})$ is the category of CM elliptic curves E over S. In particular, the objects $\mathrm{E/S} \in \mathscr{M}_{\mathrm{CM}}(\mathrm{S})$ are $\mathrm{O_K}$-modules and for each non-zero ideal $\mathfrak{a} \subset \mathrm{O_K}$ it is possible to make sense of the $\mathrm{O_K}$-module $\mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}$ which is again a CM elliptic curve over S. This defines for each ideal $\mathfrak{a}$ an endofunctor

$$- \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} : \mathscr{M}_{\mathrm{CM}} \to \mathscr{M}_{\mathrm{CM}} : \mathrm{E} \mapsto \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1},$$

and for different ideals $\mathfrak{a}$ these endo-functors all 'commute' in the obvious sense. More important is the following fact: if $\mathfrak{p} \subset \mathrm{O_K}$ is prime and S is an $\mathrm{O_K}$-scheme of characteristic $\mathfrak{p}$, i.e. the morphism $\mathrm{S} \to \mathrm{Spec}(\mathrm{O_K})$ factors through $\mathrm{Spec}(\mathrm{O_K}/\mathfrak{p})$, then for all CM elliptic curves E/S there is a canonical isomorphism

$$\mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1} \xrightarrow{\sim} \mathrm{Fr}^{\mathrm{N}\mathfrak{p}*}(\mathrm{E})$$

between $E \otimes_{O_K} \mathfrak{p}^{-1}$ and the pull-back of E along the $N\mathfrak{p}$-power Frobenius $Fr^{N\mathfrak{p}} : S \to S$ (this construction in its simplest form is due to Serre). In other words, the functor $- \otimes_{O_K} \mathfrak{p}^{-1}$ is a lift of the $N\mathfrak{p}$-power Frobenius and we have defined a naive Λ-structure on $\mathscr{M}_{CM}$.

However, as we have already noted, the naive notion of a Λ-structure as a commuting family of Frobenius lifts is not the correct one. Let us now at least say enough about the non-naive notion of Λ-structure so that we may explain to the reader some of the actual meaning of (0.0.2).

There is a functor

$$W^* : \mathrm{Sch}_{O_K} \to \mathrm{Sch}_{O_K} : X \mapsto W^*(X)$$

sending an O_K-scheme X to its scheme $W^*(X)$ of (big O_K-typical) Witt vectors (technically speaking $W^*(X)$ is actually an ind-scheme, but for the purposes of this introduction we will ignore this fact). We will not say much here about the geometry of the Witt vectors $W^*(X)$ themselves, other than to remark that they have many miraculous properties, chief among which is that if X is an O_K-scheme of characteristic $\mathfrak{p}$ for some prime of O_K, then (very roughly speaking) the Witt vectors $W^*(X)$ of X have characteristic 0. The properties of the Witt vectors $W^*(X)$ which are of interest to us presently are the following:

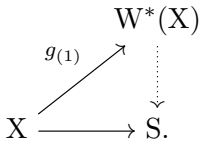
(i) $W^*(X)$ possesses a family of commuting Frobenius lifts

$$\psi^{\mathfrak{a}} : W^*(X) \to W^*(X)$$

indexed by the ideals $\mathfrak{a}$ of O_K (i.e. a naive Λ-structure),

(ii) there is a morphism $g_{(1)} : X \to W^*(X)$, and

(iii) for all flat Λ-schemes S (the definition of which we have given) and all morphisms $X \to S$ there is a unique morphism $W^*(X) \to S$ compatible with the Frobenius lifts on $W^*(X)$ and S such that the following diagram commutes

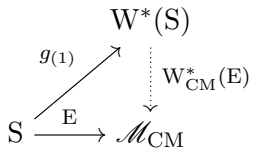


(0.0.2.1)

If we now let S be an arbitrary O_K-scheme, the diagram (0.0.2.1) can be taken as the *definition* of a Λ-structure on S: a Λ-structure on an O_K-scheme S is, for each morphism $X \to S$, a *canonical lifting* $W^*(X) \to S$ of that morphism making the diagram (0.0.2.1) commute (together with certain iterated compatibilities which we will not give here). It is not unreasonable to make

the comparison between the construction of Serre-Tate of the canonical lift to the (p-typical) Witt vectors of ordinary elliptic curve over a finite field.

We can now give the reader a better sense of the meaning of (0.0.2). If S is an $\mathrm{O_K}$-scheme and E/S is a CM elliptic curve, i.e. if one is given a morphism $\mathrm{S} \xrightarrow{\mathrm{E}} \mathscr{M}_{\mathrm{CM}}$, then there is a functorially defined CM elliptic curve $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})$ over the (big $\mathrm{O_K}$-typical) Witt vectors $\mathrm{W}^*(\mathrm{S})$ of S, i.e. there is a morphism $\mathrm{W}^*(\mathrm{S}) \xrightarrow{\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})} \mathscr{M}_{\mathrm{CM}}$, together with a canonical isomorphism $g^*_{(1)}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})) \xrightarrow{\sim} \mathrm{E}$. This to say we have a 'commutative' diagram:



and this is what we mean when we say that $\mathscr{M}_{\mathrm{CM}}$ admits a Λ-structure. It follows that CM elliptic curves can be lifted canonically to the Witt vectors of the base. We would like to point out that the base S here is arbitrary.

We shall not anything more about (0.0.2) here, nor the Λ-structure on $\mathscr{E}$. However, what (0.0.2) does do is equip $\mathscr{E} \to \mathscr{M}_{\mathrm{CM}}$ with an incredible amount of very rich structure — structure which is of interest in and of itself in the world of Λ-geometry, but which can also be exploited to prove new results in both the theory of CM elliptic curves and the arithmetic of imaginary quadratic fields. The following result is an example of this phenomenon:

0.0.3 Theorem. — *Let* $\mathrm{K}(\mathfrak{f})$ *be the ray class field of conductor* $\mathfrak{f}$ *and let* $\mathrm{E}/\mathrm{K}(\mathfrak{f})$ *be a* CM *elliptic curve of Shimura type. If the* $\mathfrak{f}$*-torsion* $\mathrm{E}[\mathfrak{f}]$ *is constant then* $\mathrm{E}/\mathrm{K}(\mathfrak{f})$ *admits a global minimal model away from* $\mathfrak{f}$*. In particular, if* $\mathfrak{f} = \mathrm{O_K}$ *so that* $\mathrm{K}(\mathfrak{f}) = \mathrm{H}$ *then* every CM *elliptic curve* E/H *of Shimura admits a* global *minimal model.*

In the special case when $\mathrm{disc}(\mathrm{K}/\mathbf{Q})$ is prime and $\mathfrak{f} = \mathrm{O_K}$ this result was proven by Gross (Corollary 4.4 [**22**]),

We now give an overview of the chapters:

Chapter 1: We recall the local and global reciprocity maps, define Lubin–Tate modules and study their moduli stack $\mathscr{M}_{\mathrm{LT}}$. We show that $\mathscr{M}_{\mathrm{LT}}$ admits a certain torsor structure and using this explain how to derive the local reciprocity map directly from $\mathscr{M}_{\mathrm{LT}}$ using only its formal properties. We then give

an overview of a certain special case of global reciprocity, and present some basic constructions regarding local systems of rank one.

Chapter 2: We undertake a quite detailed study of CM elliptic curves over arbitrary bases and their moduli stack $\mathscr{M}_{\mathrm{CM}}$. We show that $\mathscr{M}_{\mathrm{CM}}$ admits a certain torsor structure analogous to that of $\mathscr{M}_{\mathrm{LT}}$. We also give CM analogues of some classical theorems for general elliptic curves and, in a similar vein to Lubin-Tate modules, we explain how to derive a certain global reciprocity map directly from $\mathscr{M}_{\mathrm{CM}}$ using only its formal properties. Using this we classify all CM elliptic curves over fields (of arbitrary characteristic) in terms of their associated Galois representations. Finally, we consider the moduli stacks with level structure and consider their representability in the fine and coarse setting.

Chapter 3: We give a short overview of the general theory of Λ-schemes, Witt vectors and arithmetic jets. We then prove a handful of (slightly technical) new results for later use.

Chapter 4: Here we prove the main theorem regarding lifting CM elliptic curves over arbitrary bases to their big $\mathrm{O_K}$-typical Witt vectors. We then prove that a CM elliptic curve is of Shimura type if and only if its Néron model admits a Λ-structure. We then consider the minimal models of CM elliptic curves of Shimura type and prove their global existence under certain hypotheses. Next we consider quotients of CM elliptic curves by their groups of automorphisms and prove that (suitable reinterpreted) they always exist and we show that the quotient of the universal CM elliptic curve descends to the coarse space of the moduli stack of CM elliptic curves. We show how this descended curve admits a canonical Λ-structure and allows one to construct the ray class fields of K in a choice free, integral and coherent manner and we also show show that this descended curve is nothing but a (global) projective line. We then construct a flat, affine and pro-smooth cover of the moduli stack of CM elliptic curves, which comes equipped with a Λ-structure compatible with that on $\mathscr{M}_{\mathrm{CM}}$. Finally, we exhibit an interesting relationship between certain deformations of CM elliptic curves with Λ-structures and their Tate modules.

Appendix: We give an abstract and formal definition of smooth formal groups, we consider the general properties of 'Serre's tensor product' and we give a short overview of Faltings' generalised Cartier duality, needed to prove certain results in Chapter 1. Finally, we prove a strengthening of an old principal ideal theorem for arbitrary number fields.

FOUNDATIONS, CONVENTIONS AND TERMINOLOGY

0.1. Sheaves

0.1.1. In order to have a nice common ground for all the objects we would like to work with, we shall here define the basic categories of (pre)sheaves in which all objects we consider will live. We have decided to not to bother ourselves with set theoretic issues of 'size' (which really only come up when one tries to sheafify wild presheaves for large topologies [**37**] — something we will have no need to do), however the concerned reader may add the word 'universe' whenever he or she sees fit.

Let Aff denote the category of affine schemes and PSh the category of presheaves of sets on Aff, i.e. the category of functors

$$\mathrm{X} : \mathrm{Aff}^{\circ} \to \mathrm{Set}.$$

We write Sch for the category of schemes and as usual we embed Aff and Sch in PSh by sending a scheme to the functor it represents.

We shall be working with sheaves for the fpqc and étale topologies on Aff which we now recall. The covers of an affine scheme S for the fpqc (resp. étale) topology are given by flat (resp. étale) families $(\mathrm{S}_i \to \mathrm{S})_{i\in \mathrm{I}}$ indexed by a finite set I which are covers in the usual sense. A sheaf for the fpqc topology will just be called a sheaf and the category of such sheaves will be denoted $\mathrm{Sh} \subset \mathrm{PSh}$. A sheaf for the étale topology will be called an ét-sheaf and we write $\mathrm{Sh}^{\text{ét}} \subset \mathrm{PSh}$ for the corresponding category. We have the inclusions

$$\mathrm{Aff} \subset \mathrm{Sch} \subset \mathrm{Sh} \subset \mathrm{Sh}^{\text{ét}} \subset \mathrm{PSh}.$$

0.1.2. If $f : \mathrm{S}' \to \mathrm{S}$ is a morphism of presheaves and $\mathrm{X} \to \mathrm{S}$ is an S-presheaf then we denote the fibre product by $\mathrm{X} \times_{\mathrm{S}} \mathrm{S}'$, $f^*(\mathrm{X})$, or when f is clear by $\mathrm{X}_{\mathrm{S}'}$. Viewed as a functor $f^* : \mathrm{PSh}_{\mathrm{S}} \to \mathrm{PSh}_{\mathrm{S}'}$, the right adjoint to f^* is denoted by f_* and the left adjoint by $f_!$. Recall that if $\mathrm{X}' \to \mathrm{S}'$ is an S'-presheaf then $f_!(\mathrm{X}')$ is the S-presheaf $\mathrm{X}' \to \mathrm{S}' \xrightarrow{f} \mathrm{S}$ and f_* is the S-presheaf defined by

$$\mathrm{Spec}(\mathrm{A}) \mapsto \mathrm{Hom}_{\mathrm{S}'}(\mathrm{Spec}(\mathrm{A}), f_*(\mathrm{X}')) = \mathrm{Hom}_{\mathrm{S}'}(f^*(\mathrm{Spec}(\mathrm{A})), \mathrm{X}').$$

The functor $f_!$ will be used rarely, and only in the case when f is an isomorphism, in which case it is isomorphic to g^* where $g = f^{-1}$.

0.1.3 Example. — An important family of sheaves for the fpqc topology are the ind-affine schemes, the category of which we denote by IndAff. Recall an ind-affine scheme X is a pre-sheaf X which can be written as filtered a colimit $X = \operatorname{colim}_i \operatorname{Spec}(A_i)$ of affine schemes (it follows automatically from this that it is a sheaf). One of the main examples we work with is the following: if $S = \operatorname{Spec}(A)$ is an affine scheme and I is an ideal we write $\operatorname{Spf}_I(A)$ (or just $\operatorname{Spf}(A)$ when I is clear from the context) for the ind-affine scheme $\operatorname{colim}_n \operatorname{Spec}(A/I^{n+1})$. If $X \to \operatorname{Spec}(A)$ is a presheaf over $\operatorname{Spec}(A)$ we say that X is I-adic or that I is locally nilpotent on X if the morphism $X \to \operatorname{Spec}(A)$ factors through $\operatorname{Spf}(A) \subset \operatorname{Spec}(A)$. If $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is an affine $\operatorname{Spec}(A)$-scheme then $\operatorname{Spec}(B)$ is I-adic if and only if the ideal $IB \subset B$ is nilpotent.

0.1.4. If A is a set and S is an ét-sheaf then we write

$$\underline{A}_S = \coprod_{a \in A} S$$

for the constant ét-sheaf over S associated to A. If S is actually a sheaf, so is $\underline{A}_S$. When S is a fixed base (usually the spectrum of some Dedekind domain) we will drop the sub-script and just write $\underline{A}$.

0.1.5. By a cover of a sheaf S (resp. ét-sheaf) we just mean a family $(S_i \to S)_{i \in I}$ of morphisms of sheaves (resp. ét-sheaves) such that $\coprod_{i \in I} S_i \to S$ is an epimorphism. When referring to properties or making claims which are compatible with base change we will use the word local to mean after base change along a cover.

0.1.6. We say that a morphism of pre-sheaves $f : X \to S$ is representable, or that X is representable over S, if for each affine scheme $S' \to S$ the pre-sheaf $X \times_S S'$ is (representable by) a scheme. In general, for a morphism of sheaves (or ét-sheaves) to be representable is not local. However, it is the case for f which are representable by open immersions, or when f is representable by affine morphisms. In both of these cases we will just say that f is open immersion, or that f is affine. Similarly for any other condition of f that includes affine in its definition: finite, finite locally free, a closed immersion and so on.

0.1.7 Proposition. — *If $f : X \to Y$ is a finite locally free étale morphism of* ét*-sheaves then the inclusion of the image $f(X) \to Y$ in $\mathrm{Sh}^{\text{ét}}$ is an open and closed immersion, the inclusion of the complement $Y - f(X) \to Y$ is also an open and closed immersion and $Y \amalg (Y - f(X)) = Y$. Moreover, if X and Y are sheaves, so are the* ét*-sheaves $f(X)$ and $Y - f(X)$.*

The following result will be used often (it follows from Théorème 2.1 of Exposé VIII in [**3**]) cited as 'by descent':

0.1.8 Proposition. — *Let* $\mathrm{X} \to \mathrm{S}$ *be a morphism of (*ét*-)sheaves and let* $\mathrm{S}' \to \mathrm{S}$ *be an epimorphism of (*ét*-)sheaves. Then* $\mathrm{X} \to \mathrm{S}$ *is affine if and only if* $\mathrm{X} \times_{\mathrm{S}} \mathrm{S}' \to \mathrm{S}'$ *is affine.*

0.1.9. We now say a little about what we mean by a quasi-coherent $\mathscr{O}_{\mathrm{S}}$-module on a sheaf S. We have the relatively representable sheaf of rings

$$\mathscr{O}_{\mathrm{S}} := \mathbf{A}^1_{\mathrm{S}} = \mathrm{Spec}(\mathbf{Z}[\mathrm{T}]) \times_{\mathrm{Spec}(\mathbf{Z})} \mathrm{S} \tag{0.1.9.1}$$

and the abelian category of $\mathscr{O}_{\mathrm{S}}$-modules $\mathrm{Mod}(\mathscr{O}_{\mathrm{S}})$. For any map of sheaves $f : \mathrm{S}' \to \mathrm{S}$, as $\mathscr{O}_{\mathrm{S}} \times_{\mathrm{S}} \mathrm{S}' = \mathscr{O}_{\mathrm{S}'}$, we obtain the functor

$$f^* : \mathrm{Mod}(\mathscr{O}_{\mathrm{S}}) \to \mathrm{Mod}(\mathscr{O}_{\mathrm{S}'}) : \mathscr{M} \mapsto \mathscr{M} \times_{\mathrm{S}} \mathrm{S}' = \mathscr{M}_{\mathrm{S}'}.$$

Note that this functor is exact for any map f.

The category of quasi-coherent sheaves $\mathrm{QCoh}(\mathscr{O}_{\mathrm{S}}) \subset \mathrm{Mod}(\mathscr{O}_{\mathrm{S}})$ is the full sub-category of $\mathscr{O}_{\mathrm{S}}$-modules $\mathscr{M}$ such that there exists a cover $(\mathrm{S}_i \to \mathrm{S})_{i \in \mathrm{I}}$ and for each $i \in \mathrm{I}$ an exact sequence

$$\mathscr{O}_{\mathrm{S}_i}^{\mathrm{M}_i} \to \mathscr{O}_{\mathrm{S}_i}^{\mathrm{N}_i} \to \mathscr{M}_{\mathrm{S}_i} \to 0$$

where M_i and N_i are sets. When S is a scheme this category coincides with the usual category of quasi-coherent sheaves over S and the functor f^* defined above has its usual meaning. However, the inclusion $\mathrm{QCoh}(\mathscr{O}_{\mathrm{S}}) \subset \mathrm{Mod}(\mathscr{O}_{\mathrm{S}})$ is not exact (to be precise it does not preserve kernels). This explains why $f^* : \mathrm{Mod}(\mathscr{O}_{\mathrm{S}}) \to \mathrm{Mod}(\mathscr{O}_{\mathrm{S}'})$ is exact for any f while the same is not true for $\mathrm{QCoh}(\mathscr{O}_{\mathrm{S}}) \to \mathrm{QCoh}(\mathscr{O}_{\mathrm{S}})$.

We shall be almost exclusively concerned with locally free finite rank $\mathscr{O}_{\mathrm{S}}$-modules — or what is the same vector bundles — the equivalence between which is a tautology with our definition $\mathscr{O}_{\mathrm{S}} := \mathbf{A}^1_{\mathrm{S}}$.

0.2. Group actions

0.2.1. Let $\mathrm{A} \to \mathrm{B}$ be a homomorphism of rings and let G be some group of A-automorphisms of B. The example to have in mind here is a Galois extension of fields $\mathrm{K} \to \mathrm{L}$ and $\mathrm{G} = \mathrm{G}(\mathrm{L}/\mathrm{K})$.

Given $\sigma \in \mathrm{G}$, in order to avoid the cumbersome notation $\mathrm{Spec}(\sigma) : \mathrm{Spec}(\mathrm{B}) \to \mathrm{Spec}(\mathrm{B})$, we will just write $\sigma : \mathrm{Spec}(\mathrm{B}) \to \mathrm{Spec}(\mathrm{B})$. However, associating an affine scheme to a ring is contravariant, so that this notation becomes confusing when considering compositions $\sigma \circ \tau$ of elements in G. In order to avoid problems here, we make the convention that the product of two elements of $\sigma, \tau \in \mathrm{G}$, will be denoted by $\sigma\tau$ so that $\sigma\tau \in \mathrm{G}$ is the automorphism

$$\mathrm{B} \xrightarrow{\tau} \mathrm{B} \xrightarrow{\sigma} \mathrm{B}.$$

We will only use the composition symbol $\circ$ when viewing σ and τ as automorphisms of Spec(B) so that $\sigma \circ \tau$ will denote the Spec(A)-automorphism of Spec(B)

$$\mathrm{Spec(B)} \xrightarrow{\tau} \mathrm{Spec(B)} \xrightarrow{\sigma} \mathrm{Spec(B)}.$$

With this convention the following three symbols denote the same Spec(A)-automorphism of Spec(B)

$$\sigma \circ \tau = \mathrm{Spec}(\tau\sigma) = \tau\sigma : \mathrm{Spec(B)} \to \mathrm{Spec(B)}.$$

0.3. Stacks

0.3.1. Let C be a site (the examples we have in mind are C = Aff, IndAff, Sh). A fibred category over C is a category $\mathscr{X}$ equipped with a functor

$$p : \mathscr{X} \to \mathrm{C}$$

together with, for each morphism $f : \mathrm{S}' \to \mathrm{S}$ of C, a pull-back functor $f^* : \mathscr{X}(\mathrm{S}) \to \mathscr{X}(\mathrm{S}')$ where $\mathscr{X}(\mathrm{S})$ denotes the fibre of p over S (objects of $\mathscr{X}$ mapping to S and morphisms those mapping to $\mathrm{id_S}$) together with various natural transformations between their compositions satisfying certain identities. There is also the notion of a morphism of fibred categories $f : \mathscr{X}' \to \mathscr{X}$ being a functor (strictly) compatible with the functors from $\mathscr{X}'$ and $\mathscr{X}$ to C together with certain compatibility relations between the pull-back functors of $\mathscr{X}'$ and $\mathscr{X}$. Finally, a stack over C is a fibred category whose objects and morphisms satisfy descent with respect to the topology on C.

To keep things (relatively) concrete we shall say the following for C = Aff with the fpqc topology — it will also apply when working with other sites C.

The main point we want to make is that when defining stacks $\mathscr{X} \to \mathrm{Aff}$ we shall often skip the details and define only the fibres $\mathscr{X}(\mathrm{S})$ for $\mathrm{S} \in \mathrm{Aff}$ and the pull-back functors $f^* : \mathscr{X}(\mathrm{S}) \to \mathscr{X}(\mathrm{S}')$ for $f : \mathrm{S}' \to \mathrm{S}$ in Aff (and sometimes not even these when they are clear). Similarly a morphism of stacks will be defined only on the fibres, the various compatibilities which must be satisfied will be obvious from the context.

0.3.2. To each sheaf X there is an associated stack $\mathrm{Aff}_{/\mathrm{X}} \to \mathrm{Aff}$ and for each morphism $f : \mathrm{X} \to \mathrm{Y}$ a morphism

$$\mathrm{Aff}_{/\mathrm{X}} \to \mathrm{Aff}_{/\mathrm{Y}} : (\mathrm{S} \to \mathrm{X}) \mapsto (\mathrm{S} \to \mathrm{X} \xrightarrow{f} \mathrm{Y}).$$

Moreover, every morphism of stacks

$$\mathrm{Aff}_{/\mathrm{X}} \to \mathrm{Aff}_{/\mathrm{Y}}$$

is uniquely isomorphic to one of this form. In other words, when considering sheaves as the more general objects stacks, via $\mathrm{X} \mapsto \mathrm{Aff}_{/\mathrm{S}}$, we do not lose or gain anything especially important and so when considering a sheaf as a stack we shall continue to denote it by X.

0.3.3. Finally, if $\mathscr{X} \to \mathrm{Aff}$ is a stack and $\mathrm{S} \in \mathrm{Aff}$ we write $\mathscr{X}(\mathrm{S})/\sim$ for the set of isomorphism classes of objects of $\mathscr{X}(\mathrm{S})$. The pull-back maps $f^* : \mathscr{X}(\mathrm{S}) \to \mathscr{X}(\mathrm{S}')$ for $f : \mathrm{S}' \to \mathrm{S}$ define maps $\mathscr{X}(\mathrm{S})/\sim \to \mathscr{X}(\mathrm{S}')/\sim$ and this defines a (separated) pre-sheaf

$$\mathrm{Aff}^\circ \to \mathrm{Set} : \mathrm{S} \mapsto \mathscr{X}(\mathrm{S})/\sim$$

whose sheafification $\mathrm{C}(\mathscr{X}) = \mathrm{X}$ (which will be denoted by the print form of the cursive letter denoting the stack) is called the coarse sheaf associated to $\mathscr{X}$. There is an induced morphism $c_{\mathscr{X}} : \mathscr{X} \to \mathrm{X}$ and for each sheaf Y and each morphism $f : \mathscr{X} \to \mathrm{Y}$ there is a unique morphism $f' : \mathrm{X} \to \mathrm{Y}$ such that $f' \circ c_{\mathscr{X}} = f$.

0.4. Dedekind domains

Here we fix some general notation for Dedekind domains and various related objects.

0.4.1. Let O be a Dedekind domain with field of fractions K and finite residue fields. An integral ideal of O is any non-zero ideal and a prime ideal will mean a non-trivial prime ideal. We write Id_O (resp. Prin_O) for the monoid of integral (resp. and principal) ideals of O and Id_K (resp. Prin_K) for the group of fractional (resp. principal) ideals of O. If $\mathfrak{a}, \mathfrak{b} \in \mathrm{Id}_\mathrm{O}$ we write $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ so that $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime if and only if $(\mathfrak{a}, \mathfrak{b}) = \mathrm{O}$. We write CL_O for the class group of O, i.e. the group of isomorphism classes of rank one projective O-modules.

Let $\mathfrak{f}$ be an integral ideal. We write $\mathrm{Id}_\mathrm{O}^{(\mathfrak{f})} \subset \mathrm{Id}_\mathrm{O}$ (resp. $\mathrm{Id}_\mathrm{K}^{(\mathfrak{f})} \subset \mathrm{Id}_\mathrm{K}$) for the sub-monoid (resp. sub-group generated) by the prime ideals prime to $\mathfrak{f}$. If $a \in \mathrm{K}^\times$ then we say $a = 1 \bmod \mathfrak{f}$ to mean that the ideal $(a-1)$ can be written as $\mathfrak{f}\mathfrak{a}\mathfrak{b}^{-1}$ where $\mathfrak{a}, \mathfrak{b} \subset \mathrm{O}$ are ideals (if $a = 1$ we allow $\mathfrak{a} = (0)$) with $\mathfrak{b} \neq (0)$ and $(\mathfrak{b}, \mathfrak{f}) = \mathrm{O}$. If $\mathfrak{f}|\mathfrak{g}$ is another ideal then we write $\mathrm{Prin}_{1 \bmod \mathfrak{f}}^{(\mathfrak{g})}$ to denote the group of principal fractional ideals $\mathfrak{a} = (a)$ prime to $\mathfrak{g}$ with $a = 1 \bmod \mathfrak{f}$.

We write $\mathrm{N}\mathfrak{f}$ for the cardinality of $\mathrm{O}/\mathfrak{f}$ and if $\mathfrak{f} = \mathfrak{p}$ is prime we write $\mathbf{F}_\mathfrak{p} = \mathrm{O}/\mathfrak{p}$. If A is an $\mathbf{F}_\mathfrak{p}$-algebra then we write $\mathrm{Fr}^{\mathrm{N}\mathfrak{p}} : \mathrm{A} \to \mathrm{A}$ for the $\mathrm{N}\mathfrak{p}$-power Frobenius endomorphism.

We write $\mathrm{O}^{\times,\mathfrak{f}}$ for the kernel of the homomorphism $\mathrm{O}^\times \to (\mathrm{O}/\mathfrak{f})^\times$ and we say that $\mathfrak{f}$ separates units if this homomorphism is injective (this is not often the case, but will be used constantly in the text).

We write $\mathrm{O}[\mathfrak{f}^{-1}]$ for the sub-O-algebra of K generated by the elements of $\mathfrak{f}^{-1} \subset \mathrm{K}$. If $\mathrm{X} \to \mathrm{Spec}(\mathrm{O})$ is any $\mathrm{Spec}(\mathrm{O})$-sheaf then we write $\mathrm{X}[\mathfrak{f}^{-1}] = \mathrm{X} \times_{\mathrm{Spec}(\mathrm{O})} \mathrm{Spec}(\mathrm{O}[\mathfrak{f}^{-1}])$. We say that $\mathfrak{f}$ is invertible on X if $\mathrm{X}[\mathfrak{f}^{-1}] = \mathrm{X}$. If $\mathfrak{p}$ is a prime ideal we say that X has characteristic $\mathfrak{p}$ if the structure map $\mathrm{X} \to \mathrm{Spec}(\mathrm{O})$ factors through $\mathrm{Spec}(\mathbf{F}_\mathfrak{p}) \to \mathrm{Spec}(\mathrm{O})$.

If $\mathfrak{p}$ is a prime we write

$$\mathrm{Spf}_{\mathfrak{p}}(\mathrm{O}) = \operatorname*{colim}_{n\geq 0} \mathrm{Spec}(\mathrm{O}/\mathfrak{p}^{n+1}) \subset \mathrm{Spec}(\mathrm{O}).$$

We say that X is $\mathfrak{p}$-adic, or that $\mathfrak{p}$ is nilpotent on S, if the structure morphism $\mathrm{X} \to \mathrm{Spec}(\mathrm{O})$ factors through $\mathrm{Spf}_{\mathfrak{p}}(\mathrm{O}) \subset \mathrm{Spec}(\mathrm{O})$. For an affine Spec(O)-scheme Spec(A) to be $\mathfrak{p}$-adic is equivalent to the ideal $\mathfrak{p}\mathrm{A}$ being nilpotent.

CHAPTER 1

LOCAL AND GLOBAL RECIPROCITY

In §§1.1 and 1.3 of this chapter we recall the local and global reciprocity maps of class field theory. In §1.2 we define Lubin–Tate O-modules (in families) for a non-archimedian local field K with ring of integers O and show that the moduli stack $\mathscr{M}_{\mathrm{LT}}$ of Lubin–Tate O-modules is a torsor under the stack $\mathscr{CL}_{\mathrm{O}}$ of rank one O-local systems (1.2.13). We show how using this structure one can derive the local reciprocity map directly from the stack $\mathscr{M}_{\mathrm{LT}}$ using only the formal properties of Lubin–Tate O-modules (1.2.20). The construction we give is an analogue, for non-archimedian local fields, of the derivation of the global reciprocity map for imaginary quadratic fields using CM elliptic curves (which we address in Chapter 2). In §1.4 we recall how, for global fields K equipped with a certain special place ∞ and associated ring of integers $\mathrm{O_K}$, the reciprocity map associated to the maximal abelian extension of K which is totally split at ∞ can be reinterpreted in terms of certain class groups associated to $\mathrm{O_K}$ (such pairs (K, ∞) were first considered by Drinfel'd [**18**]). Finally, in §1.5 we define and give the basic properties of rank one $\mathrm{O_K}$-local systems, their level-$\mathfrak{f}$ structures and moduli for use in the later chapters.

The only new results (or perhaps observations) in this chapter are the $\mathscr{CL}_{\mathrm{O}}$-torsor structure on $\mathscr{M}_{\mathrm{LT}}$ (which in any case we prove using results of Faltings) and the derivation of the local reciprocity map directly from $\mathscr{M}_{\mathrm{LT}}$.

1.1. The local reciprocity map

The purpose of this section is to recall the basic properties of local fields and the local reciprocity map. Everything here is contained in Chapters I and VI of [**1**]).

1.1.1. Let K be a local field. There are two cases and for each we fix the following notation:

(i) K is archimedian and is isomorphic to $\mathbf{R}$ or $\mathbf{C}$. We write $|-|_{\mathrm{K}}$ for the usual absolute value if $\mathrm{K} \xrightarrow{\sim} \mathbf{R}$ and the square of the usual absolute value if $\mathrm{K} \xrightarrow{\sim} \mathbf{C}$.

(ii) K is non-archimedian and is the field of fractions of a discrete valuation ring $O \subset K$ with maximal ideal $\mathfrak{p}$ and finite residue field $\mathbf{F}_\mathfrak{p}$. We equip it with the absolute value $|a|_K = N\mathfrak{p}^{-v_\mathfrak{p}(a)}$ where $a \cdot O = \mathfrak{p}^{v_\mathfrak{p}(a)} \subset K$).

We also fix maximal abelian and separable extensions $K \subset K^{ab} \subset K^{sep}$. If K is non-archimedian these extensions are not complete but from the point of view of Galois theory nothing is lost.

1.1.2. Let K be a non-archimedian local field and let $K \subset L \subset K^{sep}$ be a (not necessarily finite) Galois extension of K. Write $O_L \subset L$ for the ring of integers of L, $\mathfrak{p}_L \subset K$ for its unique maximal ideal and $\mathbf{F}_{\mathfrak{p}_L} = O_L/\mathfrak{p}_L$ for its residue field. The reduction homomorphism $G(L/K) \to G(\mathbf{F}_{\mathfrak{p}_L}/\mathbf{F}_\mathfrak{p})$ is surjective and is bijective whenever L/K is unramified. In this case we write $\sigma_{L/K} \in G(L/K)$ for the unique element lifting the $N\mathfrak{p}$-power Frobenius automorphism of $\mathbf{F}_{\mathfrak{p}_L}$. We denote by $K \subset K^{ur} \subset K^{sep}$ the maximal unramified extension of K. The map

$$\widehat{\mathbf{Z}} \to G(K^{ur}/K) : n \mapsto \sigma^n_{K^{ur}/K}$$

is a continuous isomorphism whose inverse is denoted by $v_K : G(K^{ur}/K) \to \widehat{\mathbf{Z}}$. If L/K^{ur} is any extension we also write $v_K : G(L/K) \to \widehat{\mathbf{Z}}$ for the map $\sigma \mapsto v_K(\sigma|_{K^{ur}})$ and define $W(L/K) := v_K^{-1}(\mathbf{Z}) \subset G(L/K)$ (this is the 'Weil group').

1.1.3 Theorem. — *There is a unique isomorphism*

$$K^\times \to W(K^{ab}/K) : a \mapsto (a, K^{ab}/K) \tag{1.1.3.1}$$

such that

(i) *for all finite extensions* $K \subset L \subset K^{ab}$ *, the kernel of the composition* $a \mapsto (a, K^{ab}/K)|_L$ *is* $N_{L/K}(L^\times)$ *and the induced map*

$$K^\times/N_{L/K}(L^\times) \to G(L/K)$$

is an isomorphism, and

(ii) *the diagram*

$$\begin{array}{ccc} K^\times & \xrightarrow{(-,K^{ab}/K)} & W(K^{ab}/K) \\ {\scriptstyle v_\mathfrak{p}}\downarrow & & \downarrow \\ \mathbf{Z} & \xrightarrow{n\mapsto\sigma^n_{K^{ur}/K}} & W(K^{ur}/K) \end{array}$$

commutes.

Proof. — Uniqueness and existence are Proposition 6, §2.8 of Chapter VI and Theorem 2, §2.2 Chapter VI of [**1**] respectively. □

1.1.4. We list the following further property of the reciprocity homomorphism (see §2 Chapter VI of [**1**]): If K'/K is any finite separable extension and K'^{ab}/K' a maximal abelian extension of K', then the diagram

$$\begin{array}{ccc} K'^{\times} & \xrightarrow{(-,K'^{ab}/K')} & W(K'^{ab}/K') \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow \\ K^{\times} & \xrightarrow{(-,K^{ab}/K)} & W(K^{ab}/K) \end{array}$$

commutes.

1.1.5. We also recall the reciprocity map $(-, K^{ab}/K)$ associated to an archimedian local field K. It is the unique continuous homomorphism

$$(-, K^{ab}/K) : K^{\times} \to G(K^{ab}/K)$$

sending -1 to the unique generator of $G(K^{ab}/K)$ which is either trivial (if $K \xrightarrow{\sim} \mathbf{C}$) or cyclic of order two (if $K \xrightarrow{\sim} \mathbf{R}$).

1.2. The local reciprocity map and Lubin–Tate O-modules

We now define rank one O-local systems over $\mathfrak{p}$-adic sheaves and their moduli stack $\mathscr{CL}_O$. We then define and study families of Lubin–Tate O-modules over $\mathfrak{p}$-adic sheaves and show that $\mathscr{CL}_O$ acts on the moduli stack $\mathscr{M}_{LT}$ of Lubin–Tate O-modules, making it a torsor under $\mathscr{CL}_O$ (see (1.2.13) and (1.2.15)). Finally, we explain in (1.2.19) how this action, combined with the basic properties of Lubin–Tate O-modules, allows one to construct the reciprocity map of (1.1.3).

1.2.1. We shall be working with the category of $\mathfrak{p}$-adic sheaves, i.e. sheaves $S \to \mathrm{Spf}(O) = \mathrm{colim}_n \mathrm{Spec}(O/\mathfrak{p}^{n+1})$. If $S \to \mathrm{Spf}(O)$ is a $\mathfrak{p}$-adic sheaf then we write $S_n = S \times_{\mathrm{Spf}(O)} \mathrm{Spec}(O/\mathfrak{p}^{n+1})$ so that $S = \mathrm{colim}_{n\geq 0} S_n$. Unless otherwise stated S denotes a $\mathfrak{p}$-adic sheaf.

1.2.2. For each $\mathfrak{p}$-adic sheaf S we write $\widehat{O}_S$ for the pro-constant sheaf of rings

$$\widehat{O}_S := \lim_n \underline{O/\mathfrak{p}^{n+1}}_S.$$

If L is any finitely generated O-module then we write $\widehat{L}_S$ for the pro-constant sheaf of $\widehat{O}_S$-modules

$$\widehat{L}_S := \lim_n \underline{L/\mathfrak{p}^{n+1}L}_S.$$

If F and G are two $\widehat{O}_S$-modules over S we write $F \otimes_O G$ for the $\widehat{O}_S$-module $F \otimes_{\widehat{O}_S} G$ and $\underline{\mathrm{Hom}}^O_S(F, G)$ for the sheaf of $\widehat{O}_S$-homomorphisms $F \to G$. Moreover, if $G = \widehat{L}_S$ for some finite rank projective O-module L we shall just write $F \otimes_O L$ for $F \otimes_{\widehat{O}_S} \widehat{L}_S$.

1.2.3. A rank one O-local system over a $\mathfrak{p}$-adic sheaf S is a sheaf $\mathscr{L}$ of $\widehat{\mathrm{O}}_{\mathrm{S}}$-modules with the property that there exists a cover $(\mathrm{S}_i \to \mathrm{S})_{i\in \mathrm{I}}$ and rank one projective O-modules $(\mathrm{L}_i)_{i\in \mathrm{I}}$ such that $\mathscr{L} \times_{\mathrm{S}} \mathrm{S}_i \xrightarrow{\sim} \underline{\widehat{\mathrm{L}}_i}_{\mathrm{S}_i}$. We denote by $\mathscr{C}\mathscr{L}_{\mathrm{O}}$ the moduli stack of rank one O-local systems over $\mathrm{Sh}_{\mathrm{Spf(O)}}$. We list the following (usual) constructions and properties of O-local systems:

(i) The tensor product $\mathscr{L} \otimes_{\mathrm{O}} \mathscr{L}'$ of two rank one O-local systems $\mathscr{L}$ and $\mathscr{L}'$ (in the category of $\widehat{\mathrm{O}}_{\mathrm{S}}$-modules) is again a rank one O-local system.

(ii) The sheaf of $\widehat{\mathrm{O}}_{\mathrm{S}}$-homomorphisms $\underline{\mathrm{Hom}}^{\mathrm{O}}_{\mathrm{S}}(\mathscr{L}, \mathscr{L}')$ is again a rank one O-local system and defining $\mathscr{L}^\vee := \underline{\mathrm{Hom}}^{\mathrm{O}}_{\mathrm{S}}(\mathscr{L}, \widehat{\mathrm{O}}_{\mathrm{S}})$ we have $\underline{\mathrm{Hom}}^{\mathrm{O}}_{\mathrm{S}}(\mathscr{L}, \mathscr{L}') \xrightarrow{\sim} \mathscr{L}' \otimes_{\mathrm{O}} \mathscr{L}^\vee$.

(iii) The sheaf of automorphisms $\underline{\mathrm{Aut}}^{\mathrm{O}}_{\mathrm{S}}(\mathscr{L})$ of a rank one $\widehat{\mathrm{O}}_{\mathrm{S}}$-local system $\mathscr{L}$ is isomorphic to $\widehat{\mathrm{O}}^\times_{\mathrm{S}} := \lim_n \underline{(\mathrm{O}/\mathfrak{p}^{n+1})^\times}_{\mathrm{S}}$.

(iv) The sheaf of $\widehat{\mathrm{O}}_{\mathrm{S}}$-isomorphisms $\underline{\mathrm{Isom}}_{\mathrm{S}}(\mathscr{L}, \mathscr{L}')$ is pro-finite and étale over S and is an $\widehat{\mathrm{O}}^\times_{\mathrm{S}}$-torsor over S. We denote by $\rho_{\mathscr{L}/\mathrm{S}} \in \mathrm{H}^1(\mathrm{S}, \widehat{\mathrm{O}}^\times_{\mathrm{S}})$ the class of the torsor $\underline{\mathrm{Isom}}_{\mathrm{S}}(\mathscr{L}, \widehat{\mathrm{O}}_{\mathrm{S}})$ so that the map

$$\mathscr{L} \mapsto \rho_{\mathscr{L}/\mathrm{S}} \in \mathrm{H}^1(\mathrm{S}, \widehat{\mathrm{O}}^\times_{\mathrm{S}})$$

defines a bijection between isomorphism classes of rank one O-local systems over S and $\mathrm{H}^1(\mathrm{S}, \widehat{\mathrm{O}}^\times_{\mathrm{S}})$.

1.2.4. Let $\widehat{\mathrm{O}}_{\mathrm{S}} \to \mathscr{O}_{\mathrm{S}}$ be the unique homomorphism whose pull-back to $\mathrm{S}_n = \mathrm{S} \times_{\mathrm{Spf(O)}} \mathrm{Spec}(\mathrm{O}/\mathfrak{p}^{n+1})$ is

$$\widehat{\mathrm{O}}_{\mathrm{S}_n} \to \underline{\mathrm{O}/\mathfrak{p}^{n+1}}_{\mathrm{S}_n} \to \mathscr{O}_{\mathrm{S}_n}$$

where the second map is induced by the structure map $\mathrm{S}_n \to \mathrm{Spec}(\mathrm{O}/\mathfrak{p}^{n+1})$.

A strict formal O-module over S is a formal group F over S equipped with the structure of a $\widehat{\mathrm{O}}_{\mathrm{S}}$-module which is strict with respect to the homomorphism $\widehat{\mathrm{O}}_{\mathrm{S}} \to \mathscr{O}_{\mathrm{S}}$ (cf. (A.2.4)). Recall that this means that the two actions of $\widehat{\mathrm{O}}_{\mathrm{S}}$ on the $\mathscr{O}_{\mathrm{S}}$-module $\underline{\mathrm{Lie}}_{\mathrm{F/S}}$, coming from the action of $\widehat{\mathrm{O}}_{\mathrm{S}}$ on F and the homomorphism $\widehat{\mathrm{O}}_{\mathrm{S}} \to \mathscr{O}_{\mathrm{S}}$, coincide.

If $\mathscr{L}$ is a rank one O-local system over S then $\mathscr{L}$ (as an $\widehat{\mathrm{O}}_{\mathrm{S}}$-module) satisfies condition (P) of (A.2.1) as locally it is isomorphic to $\widehat{\mathrm{O}}_{\mathrm{S}}$. So we may apply (A.2.5) to see that if F is a strict formal O-module over S and $\mathscr{L}$ is a rank one O-local system over S then $\mathrm{F} \otimes_{\mathrm{O}} \mathscr{L}$ is again a strict formal O-module over S (of the same dimension as F).

Finally, we define the $\mathfrak{p}^n$-torsion of a strict formal O-module F over S to be the kernel of the homomorphism

$$i_{\mathfrak{p}^n} : \mathrm{F} \to \mathrm{F} \otimes_{\mathrm{O}} \mathfrak{p}^{-n}$$

induced by the inclusion $\mathrm{O} \to \mathfrak{p}^{-n}$.

1.2.5 Proposition. — *Let* F *be a strict formal* O*-module of dimension one over* S*. Then*

(i) *locally on* S *there exists an isomorphism* $\rho : \mathrm{F} \xrightarrow{\sim} \widehat{\mathbf{A}}^1_{\mathrm{S}}$ *with the property that for all* $\zeta \in \mu_{\mathrm{N}\mathfrak{p}-1} \subset \mathrm{O}^\times$ *we have* $\rho \circ [\zeta]_{\mathrm{F}} = \zeta \cdot \rho$,
(ii) $\operatorname{colim}_n \mathrm{F}[\mathfrak{p}^n] = \mathrm{F}$, *and*
(iii) $\ker(\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}_{\mathrm{F}_0/\mathrm{S}_0}) \subset \mathrm{F}_0[\mathfrak{p}^n]$.

Proof. — The claims are local on S so that we assume that $\mathrm{S} = \mathrm{Spec}(\mathrm{A})$, $\mathfrak{p}^r\mathrm{A} = (0)$ for some $r \geq 1$ as S is $\mathfrak{p}$-adic, and by (A.1.7) we may also assume that $\mathrm{F} = \widehat{\mathbf{A}}^1_{\mathrm{S}}$.

(i) This is Lemma 4.1.2 of [**26**].

Before we show (ii) and (iii) let us fix some notation and make some reductions. If $a \in \mathrm{O}$ let us write $[a](\mathrm{T}) \in \mathrm{A}[[\mathrm{T}]]$ for the power series defining the multiplication by a map

$$a : \mathrm{F} = \widehat{\mathbf{A}}^1_{\mathrm{S}} \to \mathrm{F} = \widehat{\mathbf{A}}^1_{\mathrm{S}}.$$

We also choose a generator $(\pi) = \mathfrak{p}$ so that $\ker(\pi^n) = \mathrm{F}[\mathfrak{p}^n]$ for all $n \geq 0$. Considering the coefficients of the series

$$[\pi](\mathrm{T}) = c_1\mathrm{T} + c_2\mathrm{T}^2 + \cdots \in \mathrm{A}[[\mathrm{T}]],$$

the strictness of the action of $\widehat{\mathrm{O}}_{\mathrm{S}}$ shows that $c_1 = \pi$ and by (i) we may assume that $[\zeta](\mathrm{T}) = \zeta\mathrm{T}$ for $\zeta \in \mu_{\mathrm{N}\mathfrak{p}-1} \subset \mathrm{O}^\times$. The relation

$$\zeta[\pi](\mathrm{T}) = [\zeta]([\pi](\mathrm{T})) = [\pi]([\zeta](\mathrm{T})) = [\pi](\zeta\mathrm{T})$$

for all $\zeta \in \mu_{\mathrm{N}\mathfrak{p}-1}$ then shows that $c_2 = \cdots = c_{\mathrm{N}\mathfrak{p}-1} = 0$. Thus we may assume that

$$[\pi](\mathrm{T}) = \pi\mathrm{T} \bmod \mathrm{T}^{\mathrm{N}\mathfrak{p}}.$$

We note that as $\mathfrak{p}^r\mathrm{A} = (0)$ we have

$$[\pi^r](\mathrm{T}) = 0 \bmod \mathrm{T}^{\mathrm{N}\mathfrak{p}}.$$

(ii) It is enough to show that for all A-algebras B and $b \in \mathrm{F}(\mathrm{Spec}(\mathrm{B})) = \widehat{\mathbf{A}}^1_{\mathrm{S}}(\mathrm{Spec}(\mathrm{B})) = \mathrm{nil}(\mathrm{B})$ there is an n such that $[\pi^n](b) = 0$. However, as $[\pi^r](\mathrm{T}) = 0 \bmod \mathrm{T}^{\mathrm{N}\mathfrak{p}}$ we see that $[\pi^{rm}](b) = 0$ whenever $b^{m\mathrm{N}\mathfrak{p}} = 0$ which shows the claim.

(iii) We may assume that $\mathrm{S} = \mathrm{S} \times_{\mathrm{Spf}(\mathrm{O})} \mathrm{Spec}(\mathrm{O}/\mathfrak{p}) = \mathrm{S}_0$ so that $\mathfrak{p}\mathrm{A} = 0$. Then

$$[\pi](\mathrm{T}) = c_{\mathrm{N}\mathfrak{p}}\mathrm{T}^{\mathrm{N}\mathfrak{p}} \bmod \mathrm{T}^{\mathrm{N}\mathfrak{p}+1}$$

and hence

$$[\pi^n](\mathrm{T}) = c_{\mathrm{N}\mathfrak{p}}^{\frac{\mathrm{N}\mathfrak{p}^n-1}{\mathrm{N}\mathfrak{p}-1}}\mathrm{T}^{\mathrm{N}\mathfrak{p}^n} \bmod \mathrm{T}^{\mathrm{N}\mathfrak{p}^n+1}.$$

Thus if $\mathrm{Spec}(\mathrm{B})$ is an affine $\mathfrak{p}$-adic $\mathrm{Spec}(\mathrm{A})$-scheme and if $b \in \mathrm{nil}(\mathrm{B})$ satisfies $\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}_{\mathrm{B}}(b) = b^{\mathrm{N}\mathfrak{p}^n} = 0$ we have

$$[\pi^n](b) = 0 \bmod b^{\mathrm{N}\mathfrak{p}^n} = 0$$

and therefore $\ker(\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}_{\mathrm{F}/\mathrm{S}}) \subset \mathrm{F}[\mathfrak{p}^n]$ for all $n \geq 1$. □

1.2.6. A Lubin–Tate O-module over S is a strict formal O-module F over S of dimension one (cf. (A.1.8)) with the property that the homomorphism $i_{\mathfrak{p}} : \mathrm{F} \to \mathrm{F} \otimes_{\mathrm{O}} \mathfrak{p}^{-1}$ is finite locally free of degree $\mathrm{N}\mathfrak{p}$ (in particular it is affine and faithfully flat). A morphism of Lubin–Tate O-modules is just a homomorphism of the underlying $\widehat{\mathrm{O}}_{\mathrm{S}}$-modules. We denote by $\mathscr{M}_{\mathrm{LT}}$ the moduli stack of Lubin–Tate O-modules over $\mathrm{Sh}_{\mathrm{Spf(O)}}$.

1.2.7 Proposition. — *If* F/S *is a Lubin–Tate* O*-module and* $\mathscr{L}/\mathrm{S}$ *is an* O*-local system then* $\mathrm{F} \otimes_{\mathrm{O}} \mathscr{L}/\mathrm{S}$ *is a Lubin–Tate* O*-module.*

Proof. — We have that $\mathrm{F} \otimes_{\mathrm{O}} \mathscr{L}$ is a strict O-module of dimension one by (A.2.5). The homomorphism

$$i_{\mathfrak{p}} : \mathrm{F} \otimes_{\mathrm{O}} \mathscr{L} \to (\mathrm{F} \otimes_{\mathrm{O}} \mathscr{L}) \otimes_{\mathrm{O}} \mathfrak{p}^{-1}$$

is finite locally free of degree $\mathrm{N}\mathfrak{p}$ as this can be checked locally, e.g. when $\mathscr{L} \xrightarrow{\sim} \widehat{\mathrm{O}}_{\mathrm{S}}$, and in this case it is obvious. □

1.2.8 Corollary. — *For each pair* $\mathscr{L}, \mathscr{L}'$ *of rank one* O*-local systems over* S *and each pair* F, F' *of Lubin–Tate* O*-modules over* S *the natural map*

$$\underline{\mathrm{Hom}}^{\mathrm{O}}_{\mathrm{S}}(\mathrm{F}, \mathrm{F}') \otimes_{\mathrm{O}} \underline{\mathrm{Hom}}^{\mathrm{O}_{\mathrm{K}}}_{\mathrm{S}}(\mathscr{L}, \mathscr{L}') \to \underline{\mathrm{Hom}}^{\mathrm{O}}_{\mathrm{S}}(\mathrm{F} \otimes_{\mathrm{O}_{\mathrm{K}}} \mathscr{L}, \mathrm{F}' \otimes_{\mathrm{O}_{\mathrm{K}}} \mathscr{L}')$$

is an isomorphism.

Proof. — This follows from (A.2.3). □

1.2.9 Lemma. — *Let* S *be a sheaf of characteristic* $\mathfrak{p}$*,* $n \geq 0$ *and* F *be a Lubin–Tate* O*-module over* S*. Then* $\mathrm{F}[\mathfrak{p}^n] = \ker(\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}_{\mathrm{F/S}})$.

Proof. — We may work locally on S and so assume that $\mathrm{S} = \mathrm{Spec(A)}$ and that $\mathrm{F} = \widehat{\mathbf{A}}^1_{\mathrm{S}}$. By (iii) of (1.2.5) we have $\ker(\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}_{\mathrm{F/S}}) \subset \mathrm{F}[\mathfrak{p}^n]$. As $\mathrm{F} = \widehat{\mathbf{A}}^1_{\mathrm{S}}$, it follows that $\ker(\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}_{\mathrm{F/S}})$ is finite locally free of rank $\mathrm{N}\mathfrak{p}^n$ over S. As $\mathrm{F}[\mathfrak{p}^n]$ is also finite locally free of rank $\mathrm{N}\mathfrak{p}^n$ the closed immersion $\ker(\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}_{\mathrm{F/S}}) \subset \mathrm{F}[\mathfrak{p}^n]$ must be an isomorphism. □

1.2.10 Corollary. — *For each* $n \geq 0$ *there is a unique isomorphism of functors*

$$\nu_{\mathfrak{p}^n} : - \otimes_{\mathrm{O}} \mathfrak{p}^{-n} \xrightarrow{\sim} \mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n *}(-)$$

on $\mathscr{M}_{\mathrm{LT}} \times_{\mathrm{Spf(O)}} \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}})$ *such that for all Lubin–Tate* O*-modules* F *over characteristic* $\mathfrak{p}$*-sheaves* S *the diagram*

$$\begin{array}{ccc} & \mathrm{F} & \\ {\scriptstyle i_{\mathfrak{p}^n}}\swarrow & & \searrow{\scriptstyle \mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}_{\mathrm{F/S}}} \\ \mathrm{F} \otimes_{\mathrm{O}} \mathfrak{p}^{-n} & \xrightarrow[\sim]{\nu_{\mathfrak{p}^n}} & \mathrm{Fr}^{\mathrm{N}\mathfrak{p} *}(\mathrm{F}) \end{array}$$

commutes.

Proof. — For any Lubin–Tate O-module F/S the two homomorphisms $i_{\mathfrak{p}^n}$ and $\mathrm{Fr}^{\mathrm{N}\mathfrak{p}}_{\mathrm{F/S}}$ are epimorphisms with the same kernel (1.2.9) and the claim follows. □

1.2.11 Remark. — The result (1.2.10) can be read as saying that the moduli stack $\mathscr{M}_{\mathrm{LT}}$ admits an endomorphism $-\otimes_{\mathrm{O}}\mathfrak{p}^{-1}:\mathscr{M}_{\mathrm{LT}}\to\mathscr{M}_{\mathrm{LT}}$ which (upto canonical isomorphism) lifts the N$\mathfrak{p}$-power Frobenius endomorphism. This kind of structure is very closely related to the notions of Λ-structures, Witt vectors and arithmetic jets (due to Borger and Buium) which we define and study in Chapter 3. It is essentially the topic of Chapter 4 to study and exploit this relationship in the context of CM elliptic curves (for which we prove an analogue of (1.2.10) in Chapter 2, see (2.2.13)).

1.2.12 Proposition. — (i) *If* F *is a Lubin–Tate* O*-module over* S *the natural homomorphism*

$$\widehat{\mathrm{O}}_{\mathrm{S}}\to\underline{\mathrm{End}}^{\mathrm{O}}_{\mathrm{S}}(\mathrm{F})$$

is an isomorphism.

(ii) *If* F,F' *are a pair of Lubin–Tate* O*-modules over* S *then* $\underline{\mathrm{Hom}}^{\mathrm{O}}_{\mathrm{S}}(\mathrm{F},\mathrm{F}')$ *is an* O*-local system over* S *and the evaluation homomorphism*

$$\mathrm{F}\otimes_{\mathrm{O}}\underline{\mathrm{Hom}}^{\mathrm{O}}_{\mathrm{S}}(\mathrm{F},\mathrm{F}')\to\mathrm{F}'$$

is an isomorphism.

Proof. — The proof of these statements is an application of Faltings' generalised Cartier duality [**20**]. It would take us too far afield to give the proof here and so we defer it to the appendix (see (i) and (ii) of (A.3.7)). □

1.2.13 Proposition. — *The functor*

$$\mathscr{M}_{\mathrm{LT}}\times\mathscr{C}\mathscr{L}_{\mathrm{O}}\to\mathscr{M}_{\mathrm{LT}}\times\mathscr{M}_{\mathrm{LT}}:(\mathrm{F},\mathscr{L})\mapsto(\mathrm{F},\mathrm{F}\otimes_{\mathrm{O}}\mathscr{L})$$

is an equivalence of stacks.

Proof. — As with (1.2.12), the proof of this statement will be given in the appendix (see (iii) of (A.3.7)). □

1.2.14 Remark. — It would be preferable to have elementary proofs of (1.2.12) and (1.2.13) which do not rely on the machinery of Faltings' generalised Cartier duality.

1.2.15 Example. — Let us now at least tell the reader that there do exist Lubin–Tate O-modules. First, if $\mathrm{O}=\mathbf{Z}_p$ then the p-power torsion in $\mathbf{G}_{\mathrm{m}/\mathrm{Spf}(\mathrm{O})}$:

$$\mu_{p^\infty}=\operatorname*{colim}_n\mu_{p^n}\subset\mathbf{G}_{\mathrm{m}/\mathrm{Spf}(\mathrm{O})}$$

is a Lubin-Tate $\mathbf{Z}_p$-module and it also has the property that the multiplication by p map $p:\mu_{p^\infty}\to\mu_{p^\infty}$ reduces to the p-power Frobenius after base change along $\mathrm{Spec}(\mathbf{F}_p)\to\mathrm{Spf}(\mathbf{Z}_p)$.

In fact, for any O, given a generator π of the prime ideal $\mathfrak{p}$, there is a unique (upto isomorphism) Lubin–Tate O-module F_π over $\mathrm{Spf}(\mathrm{O})$ with the property that the endomorphism $\pi : \mathrm{F}_\pi \to \mathrm{F}_\pi$ reduces to the $\mathrm{N}\mathfrak{p}$-power Frobenius map after base change along $\mathrm{Spec}(\mathbf{F}_\mathfrak{p}) \to \mathrm{Spf}(\mathrm{O})$ (see §3.5 Chapter VI [**1**]). Moreover, there exists a unique isomorphism $\mathrm{F}_\pi \xrightarrow{\sim} \widehat{\mathbf{A}}^1_{\mathrm{Spf}(\mathrm{O})}$ under which the multiplication by π is represented by the power series $[\pi](\mathrm{T}) = \pi\mathrm{T} + \mathrm{T}^{\mathrm{N}\mathfrak{p}}$.

A consequence of this is that the morphism $\mathscr{M}_{\mathrm{LT}} \to \mathrm{Spf}(\mathrm{O})$ admits a section. The statement of (1.2.13) above can now be interpreted as saying that $\mathscr{M}_{\mathrm{LT}}$ is (in a stack theoretic sense) a torsor under the (stack theoretic) group $\mathscr{C}\mathscr{L}_{\mathrm{O}}$ albeit a trivial one:

1.2.16 Corollary. — *Fixing a Lubin–Tate* O*-module* F *over* $\mathrm{Spf}(\mathrm{O})$ *the functor*

$$\mathscr{C}\mathscr{L}_{\mathrm{O}} \to \mathscr{M}_{\mathrm{LT}} : \mathscr{L}/\mathrm{S} \mapsto \mathrm{F}_\mathrm{S} \otimes_{\mathrm{O}} \mathscr{L}/\mathrm{S}$$

is an equivalence of stacks.

1.2.17 Corollary. — *Let* $\mathrm{S}_0 \to \mathrm{S}$ *be a nilpotent immersion of* $\mathfrak{p}$*-adic sheaves. The functor*

$$\mathscr{M}_{\mathrm{LT}}(\mathrm{S}) \to \mathscr{M}_{\mathrm{LT}}(\mathrm{S}_0) : \mathrm{F} \mapsto \mathrm{F}_{\mathrm{S}_0}$$

is an equivalence of categories.

Proof. — This follows from (1.2.16) and the corresponding obvious claim for $\mathscr{C}\mathscr{L}_{\mathrm{O}}$ (which is a moduli space of pro-étale objects). □

1.2.18 Corollary. — *Let* $f : \mathrm{F} \to \mathrm{F}'$ *be a homomorphism of Lubin–Tate* O*-modules over* S*. Then there is a unique decomposition* $\mathrm{S} = \mathrm{S}_{(0)} \amalg_{0 \le n < \infty} \mathrm{S}_{\mathfrak{p}^n}$ *such that* $f_{\mathrm{S}_{(0)}}$ *is the zero map and such that* $\ker(f_{\mathrm{S}_{\mathfrak{p}^n}}) = \mathrm{F}_{\mathrm{S}_{\mathfrak{p}^n}}[\mathfrak{p}^n]$ *for* $0 \le n < \infty$.

Proof. — We have $\mathrm{F}' \xrightarrow{\sim} \mathrm{F} \otimes_{\mathrm{O}} \mathscr{L}$ for some rank one O-local system $\mathscr{L}$ by (1.2.13) and the homomorphism

$$f : \mathrm{F} \to \mathrm{F} \otimes_{\mathrm{O}} \mathscr{L}$$

is of the form $\mathrm{id}_\mathrm{F} \otimes_{\mathrm{O}} h$ for some homomorphism

$$h : \widehat{\mathrm{O}}_\mathrm{S} \to \mathscr{L}$$

by (i) of (A.2.3).

Define the sub-sheaves $\mathrm{S}_{(0)} \subset \mathrm{S}$ (resp. $\mathrm{S}_{\mathfrak{p}^n} \subset \mathrm{S}$ for $0 \le n < \infty$) by the property that $h_{\mathrm{S}_{(0)}}$ is the zero map (resp. $h_{\mathrm{S}_{\mathfrak{p}^n}}$ factors as

$$\widehat{\mathrm{O}}_{\mathrm{S}_{\mathfrak{p}^n}} \xrightarrow{\sim} \mathfrak{p}^n \otimes_{\mathrm{O}} \mathscr{L}_{\mathrm{S}_{\mathfrak{p}^n}} \to \mathscr{L}_{\mathrm{S}_{\mathfrak{p}^n}}$$

where the second map is multiplication). These definitions combined with $f = \mathrm{id}_\mathrm{F} \otimes_{\mathrm{O}} h$ show that $f_{\mathrm{S}_{(0)}}$ is the zero map that $f_{\mathrm{S}_{\mathfrak{p}^n}} = \mathrm{id}_{\mathrm{F}_{\mathrm{S}_{\mathfrak{p}^n}}} \otimes_{\mathrm{O}} h_{\mathrm{S}_{\mathfrak{p}^n}}$ factors as

$$\mathrm{F}_{\mathrm{S}_{\mathfrak{p}^n}} \xrightarrow{\sim} \mathrm{F}'_{\mathrm{S}_{\mathfrak{p}^n}} \otimes_{\mathrm{O}} \mathfrak{p}^n \to \mathrm{F}'_{\mathrm{S}_{\mathfrak{p}^n}}$$

where the second map is multiplication and hence $\ker(f_{\mathrm{S}_n}) = \mathrm{F}_{\mathrm{S}_n}[\mathfrak{p}^n]$. Moreover, it is clear that $\mathrm{S}_{(0)}$ and all the $\mathrm{S}_{\mathfrak{p}^n}$ for $0 \leq n < \infty$ are disjoint and so to prove our claim we need to show that $\mathrm{S}_{(0)} \amalg_{0 \leq n < \infty} \mathrm{S}_{\mathfrak{p}^n} \to \mathrm{S}$ is an epimorphism.

For this we may localise S and assume that $\mathscr{L} = \widehat{\mathrm{O}}_{\mathrm{S}}$ and $h = a \in \mathrm{O} \subset \widehat{\mathrm{O}}_{\mathrm{S}}(\mathrm{S})$. Then either $a = 0$, in which case h is the zero map so that $\mathrm{S}_{(0)} \xrightarrow{\sim} \mathrm{S}$, or $a \neq 0$, in which case $a \cdot \mathrm{O} = \mathfrak{p}^n$ for some integer $n \geq 0$ and $h = a$ factors as

$$\widehat{\mathrm{O}}_{\mathrm{S}} \xrightarrow{\sim} \widehat{\mathrm{O}}_{\mathrm{S}} \otimes_{\mathrm{O}} \mathfrak{p}^n \to \widehat{\mathrm{O}}_{\mathrm{S}},$$

so that $\mathrm{S}_{\mathfrak{p}^n} \xrightarrow{\sim} \mathrm{S}$. It follows that $\mathrm{S}_{(0)} \amalg_{0 \leq i < \infty} \mathrm{S}_{\mathfrak{p}^n} = \mathrm{S}$. □

1.2.19. Classically one relates the reciprocity map of the local field K to Lubin–Tate O-modules as follows. Write $\mathrm{S} = \mathrm{Spf}(\mathrm{O}_{\mathrm{K}^{\mathrm{sep}}})$ and let F be the unique Lubin–Tate O-module over $\mathrm{Spf}(\mathrm{O})$ such that $\pi : \mathrm{F} \to \mathrm{F}$ reduces to the $\mathrm{N}\mathfrak{p}$-power Frobenius after base change to $\mathrm{Spec}(\mathbf{F}_{\mathfrak{p}})$. Then for each $r \geq 0$, the $\mathrm{O}/\mathfrak{p}^r$-module $\mathrm{F}[\mathfrak{p}^r](\mathrm{S})$ is free of rank one and $\mathrm{colim}_r(\mathrm{F}[\mathfrak{p}^r](\mathrm{S})) \xrightarrow{\sim} \mathrm{K}/\mathrm{O}$ (non-canonically). We then obtain the character

$$\rho_\pi : \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K}) \to \lim_r \mathrm{Aut}_{\mathrm{O}}(\mathrm{F}[\mathfrak{p}^r](\mathrm{S})) = \lim_r (\mathrm{O}/\mathfrak{p}^r)^\times = \mathrm{O}^\times$$

defining the action of $\mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$ on $\mathrm{colim}_r(\mathrm{F}[\mathfrak{p}^r](\mathrm{S}))$. The relationship between the character ρ_π and the reciprocity map (1.1.3.1) is that for all $\sigma \in \mathrm{W}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$ we have

$$\sigma|_{\mathrm{K}^{\mathrm{ab}}} = (\pi^{v_{\mathrm{K}}(\sigma)} \rho_\pi(\sigma)^{-1}, \mathrm{K}^{\mathrm{ab}}/\mathrm{K}) \tag{1.2.19.1}$$

(see §3.7 Chapter VI of [**1**]).

We would now like to show how one can construct the reciprocity map of local class field theory in a slightly more abstract but direct way using only the Frobenius lift property (1.2.10) of Lubin–Tate O-modules and the $\mathscr{C}\mathscr{L}_{\mathrm{O}_{\mathrm{K}}}$-torsor structure of $\mathscr{M}_{\mathrm{LT}}$. Write $\overline{\mathrm{S}} = \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}}^{\mathrm{sep}}) \subset \mathrm{S} = \mathrm{Spf}(\mathrm{O}_{\mathrm{K}^{\mathrm{sep}}})$ and for a Lubin–Tate O-module $\mathrm{F} \to \mathrm{S}$ write $\overline{\mathrm{F}} = \mathrm{F} \times_{\mathrm{S}} \overline{\mathrm{S}}$ and $\mathrm{F}_r = \mathrm{F}[\mathfrak{p}^r]$ for each $r \geq 0$.

1.2.20 Proposition. — *Let $\sigma \in \mathrm{W}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$ satisfy $v_{\mathrm{K}}(\sigma) = n \geq 0$. Then*

(i) *for each Lubin–Tate* O*-module* F *over* S *there is a unique isomorphism $\nu_\sigma : \mathrm{F} \otimes_{\mathrm{O}} \mathfrak{p}^{-n} \xrightarrow{\sim} \sigma^*(\mathrm{F})$ whose pull-back along $\overline{\mathrm{S}} \to \mathrm{S}$ is the isomorphism $\nu_{\mathfrak{p}^n} : \overline{\mathrm{F}} \otimes_{\mathrm{O}} \mathfrak{p}^{-n} \xrightarrow{\sim} \mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n *}(\overline{\mathrm{F}})$ of* (1.2.10),

(ii) *there is a generator $\chi_{\mathrm{K}}(\sigma) \in \mathrm{K}^\times$ of $\mathfrak{p}^n$, independent of* F*, such that for all $r \geq 0$, the isomorphism induced by ν_σ on the* S*-points of the $\mathfrak{p}^r$-torsion of* F

$$\mathrm{F}_r(\mathrm{S}) \otimes_{\mathrm{O}} \mathfrak{p}^{-n} \xrightarrow{\sim} \sigma^*(\mathrm{F}_r)(\mathrm{S})$$

is equal to

$$\mathrm{F}_r(\mathrm{S}) \otimes_{\mathrm{O}} \mathfrak{p}^{-n} \xrightarrow{\mathrm{F}_r(\sigma) \otimes \chi_{\mathrm{K}}(\sigma)} \mathrm{F}_r(\sigma_!(\mathrm{S})) = \sigma^*(\mathrm{F}_r)(\mathrm{S}),$$

(iii) *if $\tau \in \mathrm{W}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$ also satisfies $v_{\mathrm{K}}(\tau) \geq 0$ then in the notation of* (ii) *we have $\chi_{\mathrm{K}}(\sigma\tau) = \chi_{\mathrm{K}}(\sigma)\chi_{\mathrm{K}}(\tau)$, and*

(iv) *$\sigma|_{\mathrm{K}^{\mathrm{ab}}} = (\chi_{\mathrm{K}}(\sigma), \mathrm{K}^{\mathrm{ab}}/\mathrm{K})$.*

Proof. — (i) The existence of $\nu_{\mathfrak{p}^n}$ follows from (1.2.17) applied to the nilpotent immersion $\mathrm{S}_{\mathfrak{p}} \to \mathrm{S}$ and the fact that the restriction of σ to $\overline{\mathrm{S}}$ is equal to $\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}$.

(ii) For all $r \geq 0$ we have that $\mathrm{F}_r(\mathrm{S})$ is a free rank one $\mathrm{O}_{\mathrm{K}}/\mathfrak{p}^r$-module and so writing $\nu_{\sigma,r}$ for the restriction of ν_σ to the S-valued points of the $\mathfrak{p}^r$-torsion, we set

$$\begin{aligned} \chi_{\mathrm{K},r}(\sigma) = \mathrm{F}_r(\sigma)^{-1} \circ \nu_{\sigma,r} &\in \mathrm{Isom}_{\mathrm{O}}(\mathrm{F}_r(\mathrm{S}) \otimes_{\mathrm{O}} \mathfrak{p}^{-n}, \mathrm{F}_r(\mathrm{S})) \\ &= \mathrm{Isom}_{\mathrm{O}}(\mathrm{F}_r(\mathrm{S}), \mathrm{F}_r(\mathrm{S}) \otimes_{\mathrm{O}} \mathfrak{p}^n) \\ &\subset \mathfrak{p}^n \otimes_{\mathrm{O}} \mathrm{O}/\mathfrak{p}^r. \end{aligned}$$

Then $\chi_{\mathrm{K}}(\sigma)$ is given by the limit $\lim_r \chi_{\mathrm{K},r}(\sigma) \in \lim_r \mathfrak{p}^n \otimes_{\mathrm{O}} \mathrm{O}/\mathfrak{p}^r = \mathfrak{p}^n$. It is a generator of $\mathfrak{p}^n$ as $\chi_{\mathrm{K},r}(\sigma)$ is a generator of the free rank one $\mathrm{O}/\mathfrak{p}^r$-module $\mathrm{O}/\mathfrak{p}^r \otimes_{\mathrm{O}} \mathfrak{p}^n$ for all $r \geq 0$.

First, it is clear that $\chi_{\mathrm{K}}(\sigma)$ depends only on the isomorphism class of F. However, by (1.2.13), every other Lubin–Tate O-module over S is of the form $\mathrm{F} \otimes_{\mathrm{O}} \mathscr{L}$ for some rank one O-local system $\mathscr{L}$. But every rank one O-local system $\mathscr{L}$ over $\mathrm{Spf}(\mathrm{O}_{\mathrm{K}^{\mathrm{sep}}})$ is pro-constant and isomorphic to $\widehat{\mathrm{O}}_{\mathrm{S}}$. Therefore, all Lubin–Tate O-modules over S are isomorphic and $\chi_{\mathrm{K}}(\sigma)$ is independent of the Lubin–Tate O-module F over S (admittedly there is only one!).

(iii) Write $m = v_{\mathrm{K}}(\tau)$. Then the two isomorphisms

$$\nu_{\sigma\tau} \quad \text{and} \quad \tau^*(\nu_\sigma) \circ (\nu_\tau \otimes_{\mathrm{O}} \mathfrak{p}^{-m})$$

between

$$\mathrm{F} \otimes_{\mathrm{O}} \mathfrak{p}^{-n-m} \xrightarrow{\sim} (\sigma \circ \tau)^*(\mathrm{F}) = \tau^*(\sigma^*(\mathrm{F})))$$

both pull-back to the isomorphism $\nu_{\mathfrak{p}^{n+m}}$ of (1.2.10) along $\overline{\mathrm{S}} \to \mathrm{S}$. By the uniqueness in (i) we get

$$\nu_{\sigma\tau} = \tau^*(\nu_\sigma) \circ (\nu_\tau \otimes_{\mathrm{O}} \mathfrak{p}^{-m})$$

from which we find the relation $\chi_{\mathrm{K}}(\sigma\tau) = \chi_{\mathrm{K}}(\sigma)\chi_{\mathrm{K}}(\tau)$.

(iv) With notation as in (1.2.19) take $\mathrm{F} = \mathrm{F}_\pi \times_{\mathrm{Spf}(\mathrm{O})} \mathrm{S}$. As $\pi^n : \mathrm{F}_\pi \to \mathrm{F}_\pi$ lifts the $\mathrm{N}\mathfrak{p}^n$-power Frobenius endomorphism of $\mathrm{F}_\pi \times_{\mathrm{Spf}(\mathrm{O})} \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}})$ the (unique) isomorphism

$$\nu_\sigma : \mathrm{F} \otimes_{\mathrm{O}} \mathfrak{p}^{-n} \xrightarrow{\sim} \sigma^*(\mathrm{F})$$

of (i) is given by

$$\mathrm{F} \otimes_{\mathrm{O}} \mathfrak{p}^{-n} \xrightarrow{\pi^n} \mathrm{F} \xrightarrow{d_\sigma} \sigma^*(\mathrm{F}) \tag{1.2.20.1}$$

where $d_\sigma : \mathrm{F} \xrightarrow{\sim} \sigma^*(\mathrm{F})$ is the descent isomorphism (coming from the fact that $\mathrm{F} = \mathrm{F}_\pi \times_{\mathrm{Spf}(\mathrm{O})} \mathrm{S}$ is defined over $\mathrm{Spf}(\mathrm{O})$). The isomorphism d_σ on the S-points of the $\mathfrak{p}^r$-torsion is given by

$$\mathrm{F}_r(\mathrm{S}) \xrightarrow{\rho_\pi(\sigma)^{-1} \cdot \mathrm{F}_r(\sigma)} \mathrm{F}_r(\sigma_!(\mathrm{S})) = \sigma^*(\mathrm{F}_r)(\mathrm{S})$$

so that ν_σ on the S-points of the $\mathfrak{p}^r$ torsion is given by (cf. (1.2.20.1))

$$\mathrm{F}_r(\mathrm{S}) \otimes_{\mathrm{O}} \mathfrak{p}^{-n} \xrightarrow{1 \otimes \pi^n} \mathrm{F}_r(\mathrm{S}) \xrightarrow{\rho_\pi(\sigma)^{-1} \cdot \mathrm{F}_r(\sigma)} \mathrm{F}_r(\sigma_!(\mathrm{S})) = \sigma^*(\mathrm{F}_r)(\mathrm{S}).$$

Therefore $\chi_{\mathrm{K}}(\sigma) = \pi^n \rho_\pi(\sigma)^{-1}$ and by (1.2.19.1) we get

$$\sigma|_{\mathrm{K}^{\mathrm{ab}}} = (\pi^n \rho_\pi(\sigma)^{-1}, \mathrm{K}^{\mathrm{ab}}/\mathrm{K}) = (\chi_{\mathrm{K}}(\sigma), \mathrm{K}^{\mathrm{ab}}/\mathrm{K}).$$

□

1.2.21 Remark. — From (i), (ii) and (iii) of (1.2.20) we see that we can associate to any element of $\sigma \in v_{\mathrm{K}}^{-1}(\mathbf{N}_{\geq 0}) \subset \mathrm{W}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$ an element $\chi_{\mathrm{K}}(\sigma) \in \mathrm{K}^\times$ and that this association is multiplicative. It therefore extends to a homomorphism

$$\mathrm{W}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K}) \to \mathrm{K}^\times : \sigma \mapsto \chi_{\mathrm{K}}(\sigma) \tag{1.2.21.1}$$

and (iv) of (1.2.20) states that this map satisfies

$$\sigma|_{\mathrm{K}^{\mathrm{ab}}} = (\chi_{\mathrm{K}}(\sigma), \mathrm{K}^{\mathrm{ab}}/\mathrm{K})$$

for all $\sigma \in \mathrm{W}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$. Thus we have derived the local reciprocity map (1.1.3.1) using nothing more than the basic properties of Lubin–Tate O-modules (in particular, the Frobenius lifting property (1.2.10) and the $\mathscr{C}\mathscr{L}_{\mathrm{O}}$-torsor structure of $\mathscr{M}_{\mathrm{LT}}$ (1.2.13)).

1.2.22 Remark. — If $\mathrm{K} \subset \mathrm{L} \subset \mathrm{K}^{\mathrm{sep}}$ is a finite extension and $\mathrm{F}/\mathrm{Spf}(\mathrm{O}_{\mathrm{L}})$ is a Lubin–Tate O-module let us write

$$\rho_{\mathrm{F}/\mathrm{O}_{\mathrm{L}}} : \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{L}) \to \mathrm{O}^\times$$

for the (continuous) character defining the action of G on

$$\operatorname*{colim}_r(\mathrm{F}[\mathfrak{p}^r](\mathrm{Spf}(\mathrm{O}_{\mathrm{K}^{\mathrm{sep}}}))) \xrightarrow{\sim} \mathrm{K}/\mathrm{O}.$$

Then a continuous character $\rho : \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{L}) \to \mathrm{O}^\times$ is of the form $\rho_{\mathrm{F}/\mathrm{O}_{\mathrm{L}}}$ if and only if the diagram

$$\begin{array}{ccc} \mathrm{W}(\mathrm{K}^{\mathrm{sep}}/\mathrm{L}) & \xrightarrow{\rho_{\mathrm{F}/\mathrm{O}_{\mathrm{L}}}^{-1}} & \mathrm{O}^\times \\ & \searrow^{\chi_{\mathrm{K}}} & \downarrow \\ & & \mathrm{K}^\times \end{array}$$

commutes where the right vertical map is the inclusion. We mention this mainly as it is analogous to the classification of elliptic curves with complex multiplication over fields in terms of their associated characters we will give in Chapter 2 (see (iii) of (2.5.10)).

1.2.23 Remark. — Of course, the theory of Lubin–Tate O-modules and the local reciprocity map are themselves not particularly complicated and one can derive the reciprocity map in any number of ways. We believe the this approach above has some advantages over the classical one, first and foremost it is choice free, and secondly one gets the whole of the local reciprocity map right of the bat, rather than first finding a character

$$\rho_\pi : \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K}) \to \mathrm{O}^\times$$

which one then restricts to $\mathrm{W}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K}) \subset \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$, takes the reciprocal of and then multiplies by the character

$$\mathrm{W}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K}) \to \mathrm{K}^{\times} : \sigma \mapsto \pi^{v_{\mathrm{K}}(\sigma)}.$$

The derivation of the local reciprocity map we have given is also analogous to the derivation (2.5.9) of the global reciprocity map for imaginary quadratic fields which we will give using CM elliptic curves in Chapter 2. Moreover, in the case of CM elliptic curves and imaginary quadratic fields, the situation is somewhat more delicate — one cannot just find CM elliptic curves with suitable properties from which one can construct the global reciprocity map in the same way one can with Lubin–Tate O-modules.

1.3. The global reciprocity map

In this section we recall the basic objects required to define, and then we recall, the global reciprocity map (1.3.3) associated to a global field K.

1.3.1. Let K be a global field and fix maximal abelian and separable extensions $\mathrm{K} \subset \mathrm{K}^{\mathrm{ab}} \subset \mathrm{K}^{\mathrm{sep}}$. Write $\mathscr{P}_{\mathrm{K}}$ for the set of places of K, and as usual, if K is a number field we identify the non-archimedian places $v \in \mathscr{P}_{\mathrm{K}}$ with the prime ideals $\mathfrak{p} \subset \mathrm{O}_{\mathrm{K}}$ of the ring of integers of K. For $v \in \mathrm{K}$ we write K_v for the completion of K with respect to v and if v is archimedian $\mathrm{O}_{\mathrm{K}_v} \subset \mathrm{K}_v$ for the ring of local integers. We write $\mathscr{P}_{\mathrm{K}}^{\mathrm{arch}} \subset \mathscr{P}_{\mathrm{K}}$ for the subset of archimedian places (which is of course empty if K is a function field).

Let $\mathrm{K} \subset \mathrm{L} \subset \mathrm{K}^{\mathrm{sep}}$ be a finite Galois extension. If $w \in \mathscr{P}_{\mathrm{L}}$ is a non-archimedian place and the extension L/K is unramified at w then we write $\sigma_{\mathrm{L/K},w} \in \mathrm{G}(\mathrm{L/K})$, or just σ_w, for the Frobenius element associated to w. If L/K is abelian (so that $\sigma_{\mathrm{L/K},w}$ depends only on $w|_{\mathrm{K}} = v \in \mathscr{P}_{\mathrm{K}}$) then we write $\sigma_{\mathrm{L/K},v}$, or again just σ_v, for $\sigma_{\mathrm{L/K},w}$.

1.3.2. For each finite set $\mathrm{S} \subset \mathscr{P}_{\mathrm{K}}$ containing all archimedian places of K we write $\mathrm{I}_{\mathrm{K,S}}$ for the topological group

$$\mathrm{I}_{\mathrm{K,S}} = \prod_{v \in \mathscr{P}_{\mathrm{K}} - \mathrm{S}} \mathrm{O}_{\mathrm{K}_v}^{\times} \times \prod_{v \in \mathrm{S}} \mathrm{K}_v^{\times}$$

(the topology being the product topology). For $\mathrm{S} \subset \mathrm{S}' \subset \mathscr{P}_{\mathrm{K}}$ the inclusions $\mathrm{I}_{\mathrm{K,S}} \subset \mathrm{I}_{\mathrm{K,S}'}$ are open and the group of idèles of K is the topological group

$$\mathrm{I}_{\mathrm{K}} = \operatorname*{colim}_{\mathrm{S}} \mathrm{I}_{\mathrm{K,S}}$$

(the topology being the colimit topology). The diagonal embedding $\mathrm{K}^{\times} \to \mathrm{I}_{\mathrm{K}}$ makes $\mathrm{K}^{\times}$ a discrete subgroup of I_{K} and the idèle class group of K is the quotient $\mathrm{C}_{\mathrm{K}} = \mathrm{I}_{\mathrm{K}}/\mathrm{K}^{\times}$. The embeddings $\mathrm{K}_v^{\times} \to \mathrm{I}_{\mathrm{K}} \to \mathrm{C}_{\mathrm{K}}$ for each place v of K make $\mathrm{K}_v^{\times}$ a closed subgroup of I_{K} and C_{K}.

1.3.3 Theorem. — *There is a unique continuous homomorphism*

$$\mathrm{C_K} \to \mathrm{G}(\mathrm{K}^{\mathrm{ab}}/\mathrm{K}) : s \mapsto (s, \mathrm{K}^{\mathrm{ab}}/\mathrm{K})$$

such that for each place v of K *and each* K*-linear embedding* $\mathrm{K}^{\mathrm{ab}} \to \mathrm{K}_v^{\mathrm{ab}}$ *the following diagram commutes*

$$\begin{array}{ccc} \mathrm{C_K} & \xrightarrow{(-,\mathrm{K}^{\mathrm{ab}}/\mathrm{K})} & \mathrm{G}(\mathrm{K}^{\mathrm{ab}}/\mathrm{K}) \\ \uparrow & & \uparrow \\ \mathrm{K}_v^{\times} & \xrightarrow{(-,\mathrm{K}_v^{\mathrm{ab}}/\mathrm{K}_v)} & \mathrm{G}(\mathrm{K}_v^{\mathrm{ab}}/\mathrm{K}_v). \end{array}$$

Proof. — See §§4–6 Chapter VII of [**1**]. □

1.3.4. We list the following further properties of the reciprocity map (see §§4–6 Chapter VII of [**1**]).

(a) If K'/K is any finite Galois extension, with maximal abelian extension $\mathrm{K}'^{\mathrm{ab}}$, the diagram

$$\begin{array}{ccc} \mathrm{C}_{\mathrm{K}'} & \xrightarrow{(-,\mathrm{K}'^{\mathrm{ab}}/\mathrm{K}')} & \mathrm{G}(\mathrm{K}'^{\mathrm{ab}}/\mathrm{K}') \\ {\scriptstyle \mathrm{N}_{\mathrm{K}'/\mathrm{K}}}\downarrow & & \downarrow \\ \mathrm{C_K} & \xrightarrow{(-,\mathrm{K}^{\mathrm{ab}}/\mathrm{K})} & \mathrm{G}(\mathrm{K}^{\mathrm{ab}}/\mathrm{K}) \end{array}$$

commutes (where $\mathrm{N}_{\mathrm{K}'/\mathrm{K}}$ denotes the map induced by the norm $\mathrm{I}_{\mathrm{K}'} \to \mathrm{I_K}$).

(b) The kernel of the reciprocity map is $\mathrm{C}_{\mathrm{K}}^{\circ} \subset \mathrm{C_K}$ (a superscript $\circ$ denotes the connected component of the identity of a topological group). If K is a function field then $\mathrm{C}_{\mathrm{K}}^{\circ}$ is trivial and $(-, \mathrm{K}^{\mathrm{ab}}/\mathrm{K})$ is injective. If K is a number field then $\mathrm{C}_{\mathrm{K}}^{\circ}$ is the closure of the sub-group

$$\prod_{v \in \mathscr{P}_{\mathrm{K}}^{\mathrm{arch}}} \mathrm{K}_v^{\times,\circ} \subset \mathrm{C_K}$$

and $(-, \mathrm{K}^{\mathrm{ab}}/\mathrm{K})$ is surjective. We note that if $\mathscr{P}_{\mathrm{K}}^{\mathrm{arch}} = \{\infty\}$ contains only one place then $\mathrm{K}_{\infty}^{\times,\circ} = \mathrm{C}_{\mathrm{K}}^{\circ}$ and we obtain a topological isomorphism

$$\mathrm{C_K}/\mathrm{K}_{\infty}^{\times,\circ} \xrightarrow{\sim} \mathrm{G}(\mathrm{K}^{\mathrm{ab}}/\mathrm{K}).$$

1.4. Global fields with a single 'infinite' place and class groups

In this section we describe a variant of the reciprocity map associated to the maximal abelian extension K^{∞} of a global field K which is totally split at a fixed place ∞ satisfying $\mathscr{P}_{\mathrm{K}}^{\mathrm{arch}} \subset \{\infty\}$. If K is a function field then any place ∞ satisfies the above property and if K is a number field then the only possibilities are $\mathrm{K} = \mathbf{Q}$ or K an imaginary quadratic and in each case ∞ equal to the unique archimedian place of K.

As mentioned in the introduction to this chapter, the fact that such pairs (K, ∞) should be considered along similar lines is due to Drinfel'd [**18**] and essentially all we are doing here is collecting the relevant facts for use in the later chapters. It is worth noting here that the abelian extensions of K contained in K^∞ have a long history mainly due to the fact that they are amenable to explicit computation via the use of Drinfel'd modules in case K is a function field, tori if $K = \mathbf{Q}$ and CM elliptic curves if K is an imaginary quadratic field (what Drinfel'd originally called 'elliptic modules of rank one'). While we are only concerned with the final case in this thesis, the abstract theory we describe below is valid for arbitrary pairs (K, ∞).

1.4.1. Let K be a global field, and fix a place ∞ of K such that $\mathscr{P}_K^{\mathrm{arch}} \subset \{\infty\}$. We call ∞ the infinite place, and the places in $\mathscr{P}_K - \infty$ the finite places and denote them by $\mathscr{P}_K^{\mathrm{fin}}$. As every place $v \neq \infty$ is non-archimedian the subset $O_K = \{a \in K : |a|_v \leq 1 \text{ for all } v \neq \infty\} \subset K$ is a Dedekind domain, and its prime ideals are in bijection with the set $\mathscr{P}_K^{\mathrm{fin}}$.

The group of units $O_K^\times$ is finite and we denote its order by w. We want to point out that for what follows in this section, and in the following chapters, this fact is quite crucial. It implies in particular that given any ideal $\mathfrak{f}$ there is an ideal $\mathfrak{f}|\mathfrak{f}'$ with the property that $\mathfrak{f}'$ separates units, i.e. the homomorphism

$$O_K^\times \to (O_K/\mathfrak{f}')^\times$$

is injective or what is the same $O_K^{\times,\mathfrak{f}'} = \{1\}$ (of course, if $\mathfrak{f} \neq O_K$ any high power of $\mathfrak{f}$ will do).

1.4.2. We write A_{O_K} for the topological ring

$$\lim_{\mathfrak{a}} O_K/\mathfrak{a} = \prod_{\mathfrak{p}} O_{K_\mathfrak{p}},$$

the topology being the product topology or the inverse limit topology induced by the discrete topologies on the finite sets $O_K/\mathfrak{a}$ (they are the same). We also view

$$A_{O_K}^\times = \lim_{\mathfrak{a}} (O_K/\mathfrak{a})^\times = \prod O_{K_\mathfrak{p}}^\times$$

as a topological group via the topology induced from A_{O_K}, the product topology or the inverse limit topology (again they are one and the same). For each integral ideal $\mathfrak{f}$ we denote by $A_{O_K}^{\times,\mathfrak{f}}$ the open subgroup

$$\ker(A_{O_K}^\times \to (O_K/\mathfrak{f})^\times).$$

For each integral ideal $\mathfrak{a}$ we equip

$$A_{O_K}[\mathfrak{a}^{-1}]^\times := \prod_{\mathfrak{p}|\mathfrak{a}} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\nmid\mathfrak{a}} O_{K_\mathfrak{p}}^\times$$

with the product topology. If $\mathfrak{a}|\mathfrak{b}$ the inclusion $\mathrm{A}_{\mathrm{O_K}}[\mathfrak{a}^{-1}]^\times \subset \mathrm{A}_{\mathrm{O_K}}[\mathfrak{b}^{-1}]^\times$ is open and we equip

$$(\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^\times = \operatorname*{colim}_{\mathfrak{a}} \mathrm{A}_{\mathrm{O_K}}[\mathfrak{a}^{-1}]^\times$$

with the colimit topology. The natural map

$$\mathrm{I_K} \to (\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^\times,$$

induced by forgetting the component at ∞, is continuous and surjective and induces topological isomorphism

$$\mathrm{I_K}/\mathrm{K}_\infty^\times \xrightarrow{\sim} (\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^\times.$$

1.4.3. We will now relate the group $(\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^\times$ to certain class groups associated to $\mathrm{O_K}$. So let $\mathfrak{f} \in \mathrm{Id}_{\mathrm{O_K}}$ and let L be a projective rank one $\mathrm{O_K}$-module. A level-$\mathfrak{f}$ structure on L is a surjective homomorphism $a : \mathrm{L} \to \mathrm{O_K}/\mathfrak{f}$. An $\mathfrak{f}$-isomorphism $f : (\mathrm{L}, a) \xrightarrow{\sim} (\mathrm{L}', a')$ between a pair of projective rank one $\mathrm{O_K}$-modules with level-$\mathfrak{f}$ structures is an $\mathrm{O_K}$-isomorphism $f : \mathrm{L} \to \mathrm{L}'$ such that $h \circ a' = a$. We denote by $\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}$ the set of $\mathfrak{f}$-isomorphism classes of rank one projective $\mathrm{O_K}$-modules with level-$\mathfrak{f}$ structure. Equipping it with the product

$$(\mathrm{L}, a) \cdot (\mathrm{L}', a') = (\mathrm{L} \otimes_{\mathrm{O_K}} \mathrm{L}', a \otimes_{\mathrm{O_K}} a'),$$

$\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}$ becomes a group, which we call the ray class group of conductor $\mathfrak{f}$.

If $\mathfrak{a}$ is any fractional ideal prime to $\mathfrak{f}$, the multiplication map

$$\mathfrak{a} \otimes_{\mathrm{O_K}} \mathrm{O_K}/\mathfrak{f} \xrightarrow{\sim} \mathrm{O_K}/\mathfrak{f}$$

is well defined, and an isomorphism, so that setting $f : \mathfrak{a} \to \mathrm{O_K}/\mathfrak{f}$ to be the composition

$$\mathfrak{a} \to \mathfrak{a} \otimes_{\mathrm{O_K}} \mathrm{O_K}/\mathfrak{f} \xrightarrow{\sim} \mathrm{O_K}/\mathfrak{f} \tag{1.4.3.1}$$

equips $\mathfrak{a}$ with a level-$\mathfrak{f}$ structure. We write $[\mathfrak{a}]_\mathfrak{f} = (\mathfrak{a}, f) \in \mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}$ for the corresponding class. This defines a surjective homomorphism

$$\mathrm{Id}_{\mathrm{K}}^{(\mathfrak{f})} \to \mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})} : \mathfrak{a} \mapsto [\mathfrak{a}]_\mathfrak{f}$$

whose kernel is the group $\mathrm{Prin}_{1 \bmod \mathfrak{f}}^{(\mathfrak{f})}$ of principal fractional ideals $\mathfrak{a} = \mathrm{O_K} \bmod \mathfrak{f}$ admitting a generator $a \in \mathrm{K}^\times$ with $a = 1 \bmod \mathfrak{f}$. If $\mathfrak{f}|\mathfrak{f}'$ then

$$\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f}')} \to \mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})} : (\mathrm{L}, a) \mapsto (\mathrm{L}, a \bmod \mathfrak{f})$$

defines a surjective homomorphism and we define the topological group

$$\mathrm{CL}_{\mathrm{O_K},\infty} = \lim_{\mathfrak{f}} \mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}$$

(the topology being the inverse limit of the discrete topologies on the $\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}$). Finally, if $\mathfrak{f} = \mathrm{O_K}$ then we identify $\mathrm{CL}_{\mathrm{O_K}}^{\mathrm{O_K}}$ with the class group $\mathrm{CL}_{\mathrm{O_K}}$ of $\mathrm{O_K}$.

1.4.4. Given an element $s \in (\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^\times$, we write $(s) \in \mathrm{Id_K}$ for the fractional ideal

$$(s) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(s)}.$$

For each integral ideal $\mathfrak{f}$, we equip $(s)^{-1}$ with the level-$\mathfrak{f}$ structure

$$(s)^{-1} \xrightarrow{s} \mathrm{A}_{\mathrm{O_K}} \to \mathrm{O_K}/\mathfrak{f}$$

and write $[s]_{\mathfrak{f}} \in \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}$ for the corresponding class. This defines a continuous surjective homomorphism

$$(\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^\times \to \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}} : s \mapsto [s]_{\mathfrak{f}}$$

with kernel $\mathrm{K}^\times \cdot \mathrm{A}^{\times,\mathfrak{f}}_{\mathrm{O_K}}$. Finally, if $\mathfrak{f}|\mathfrak{f}'$ the image of $[s]_{\mathfrak{f}'}$ under $\mathrm{CL}^{(\mathfrak{f}')}_{\mathrm{O_K}} \to \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}$ is $[s]_{\mathfrak{f}}$ and so taking the limit over $\mathfrak{f}$ we obtain a homomorphism

$$[-] : (\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^\times \to \mathrm{CL}_{\mathrm{O_K},\infty} = \lim_{\mathfrak{f}} \mathrm{CL}_{\mathrm{O_K}}(\mathfrak{f}) : s \mapsto [s] = \lim_{\mathfrak{f}} [s]_{\mathfrak{f}}. \quad (1.4.4.1)$$

1.4.5 Proposition. — *The map $[-]$ is continuous and the sequence*

$$0 \to \mathrm{K}^\times \to (\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^\times \xrightarrow{[-]} \mathrm{CL}_{\mathrm{O_K},\infty} \to 0$$

is exact.

Proof. — It is clear that $s \mapsto [s]$ is continuous (as $s \mapsto [s]_{\mathfrak{f}}$ is continuous for each $\mathfrak{f}$) and if we can show that $\ker(s \mapsto [s]) = \mathrm{K}^\times$ then the surjectivity of $s \mapsto [s]$ follows as $s \mapsto [s]_{\mathfrak{f}}$ is surjective for each $\mathfrak{f}$ and $(\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^\times/\mathrm{K}^\times = \mathrm{C_K}/\mathrm{K}^\times_\infty$ is compact.

The kernel of $s \mapsto [s]$ is equal to

$$\bigcap_{\mathfrak{f}} \ker(s \mapsto [s]_{\mathfrak{f}}) = \bigcap_{\mathfrak{f}} (\mathrm{K}^\times \cdot \mathrm{A}^{\times,\mathfrak{f}}_{\mathrm{O_K}}).$$

If s is an element of this kernel then for all integral ideals $\mathfrak{f}$ we can write $s = a_{\mathfrak{f}} s_{\mathfrak{f}}$ where $a_{\mathfrak{f}} \in \mathrm{K}^\times$ and $s_{\mathfrak{f}} \in \mathrm{A}^{\times,\mathfrak{f}}_{\mathrm{O_K}}$. The elements $a_{\mathfrak{f}}$ and $s_{\mathfrak{f}}$ are unique upto scaling by an element of $\mathrm{O}^{\times,\mathfrak{f}}_{\mathrm{K}}$ so that if $\mathfrak{f}$ separates units both $a_{\mathfrak{f}}$ and $s_{\mathfrak{f}}$ are unique, and moreover equal to $a_{\mathfrak{f}'}$ and $s_{\mathfrak{f}'}$ for any integral ideal $\mathfrak{f}'$ divisible by $\mathfrak{f}$. Fixing such an $\mathfrak{f}$ it follows that

$$s_{\mathfrak{f}} \in \bigcap_{\mathfrak{f}|\mathfrak{f}'} \mathrm{A}^{\times,\mathfrak{f}'}_{\mathrm{O_K}} = \{1\}$$

so that $s = a_{\mathfrak{f}} s_{\mathfrak{f}} = a_{\mathfrak{f}} \in \mathrm{K}^\times$ and we are done. □

1.4.6 Remark. — The exactness of the sequence (1.4.5) is the first result of many that will rely crucially on the fact that the unit group $\mathrm{O}^\times_{\mathrm{K}}$ is finite.

1.4.7. We write $\mathrm{K}^{\infty}/\mathrm{K}$ for the maximal abelian extension of K which is totally split at ∞. The kernel of the surjective map

$$\mathrm{C_K} \to \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K})$$

is precisely $\mathrm{K}_{\infty}^{\times}$ (cf. (b) of (1.3.4)) so that we obtain continuous isomorphisms

$$(\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^{\times}/\mathrm{K}^{\times} = \mathrm{I_K}/(\mathrm{K}^{\times}\mathrm{K}_{\infty}^{\times}) = \mathrm{C_K}/\mathrm{K}_{\infty}^{\times} \to \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K}).$$

Let us write

$$(-, \mathrm{K}^{\infty}/\mathrm{K}) : (\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^{\times}/\mathrm{K}^{\times} \xrightarrow{\sim} \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K}). \tag{1.4.7.1}$$

for this isomorphism and also

$$\theta_{\mathrm{K}} : \mathrm{CL}_{\mathrm{O_K},\infty} \xrightarrow{\sim} \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K}) \tag{1.4.7.2}$$

for the isomorphism

$$\mathrm{CL}_{\mathrm{O_K},\infty} \xleftarrow{\sim} (\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^{\times}/\mathrm{K}^{\times} \xrightarrow{(-,\mathrm{K}^{\infty}/\mathrm{K})} \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K})$$

so that for all $s \in (\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K}^{\times})/\mathrm{K}^{\times}$ we have

$$\theta_{\mathrm{K}}([s]) = (s, \mathrm{K}^{\infty}/\mathrm{K}).$$

If $\mathfrak{f}$ is an integral ideal of $\mathrm{O_K}$ then, under θ_{K}, the kernel of the homomorphism

$$\mathrm{CL}_{\mathrm{O_K},\infty} \to \mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}$$

corresponds to the subgroup $\mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K}(\mathfrak{f})) \subset \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K})$ of automorphisms fixing a certain finite abelian extension $\mathrm{K} \subset \mathrm{K}(\mathfrak{f}) \subset \mathrm{K}^{\infty}$ which we call the ray class field of conductor $\mathfrak{f}$. By definition the map (1.4.7.2) induces an isomorphism

$$\theta_{\mathrm{K},\mathfrak{f}} : \mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})} \xrightarrow{\sim} \mathrm{G}(\mathrm{K}(\mathfrak{f})/\mathrm{K}). \tag{1.4.7.3}$$

The extension $\mathrm{K}(\mathfrak{f})/\mathrm{K}$ is unramified away from $\mathfrak{f}$ and if $\mathfrak{p}$ is prime to $\mathfrak{f}$ then

$$\theta_{\mathrm{K},\mathfrak{f}}([\mathfrak{p}]_{\mathfrak{f}}^{-1}) = \theta_{\mathrm{K},\mathfrak{f}}([\pi]_{\mathfrak{f}}) = \sigma_{\mathrm{K}(\mathfrak{f})/\mathrm{K},\mathfrak{p}}$$

where $\pi \in \mathrm{K}_{\mathfrak{p}}^{\times} \subset (\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^{\times}$ is any local uniformiser. In particular, when $\mathfrak{f} = \mathrm{O_K}$ the field $\mathrm{H} := \mathrm{K}(\mathrm{O_K})$ is called the Hilbert class field. It is unramified everywhere and the isomorphism

$$\theta_{\mathrm{K},\mathrm{O_K}} : \mathrm{CL}_{\mathrm{O_K}} \xrightarrow{\sim} \mathrm{G}(\mathrm{H}/\mathrm{K})$$

maps the class of the inverse of each prime ideal $[\mathfrak{p}^{-1}] \in \mathrm{CL}_{\mathrm{O_K}}$ to the Frobenius element $\sigma_{\mathrm{H}/\mathrm{K},\mathfrak{p}}$.

1.4.8 Remark. — For future reference we make the following observations.

(a) The composition

$$\mathrm{A}_{\mathrm{O_K}}^{\times,\mathfrak{f}}/\mathrm{O}_{\mathrm{K}}^{\times,\mathfrak{f}} \to (\mathrm{A} \otimes_{\mathrm{O_K}} \mathrm{K}^{\times})/\mathrm{K}^{\times} \overset{[-]}{\to} \mathrm{CL}_{\mathrm{O_K},\infty} \overset{\theta_{\mathrm{K}}}{\to} \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K})$$

induces an isomorphism

$$\mathrm{A}_{\mathrm{O_K}}^{\times,\mathfrak{f}}/\mathrm{O}_{\mathrm{K}}^{\times,\mathfrak{f}} \xrightarrow{\sim} \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K}(\mathfrak{f})) \subset \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K}). \tag{1.4.8.1}$$

In particular, when $\mathfrak{f}$ separates units we have $\mathrm{O}_{\mathrm{K}}^{\times,\mathfrak{f}} = \{1\}$ so that (1.4.8.1) becomes

$$\mathrm{A}_{\mathrm{O_K}}^{\times,\mathfrak{f}} \xrightarrow{\sim} \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K}(\mathfrak{f})).$$

(b) For each prime $\mathfrak{p}$ of $\mathrm{O_K}$ and each K-linear embedding $\mathrm{K}^{\mathrm{sep}} \to \mathrm{K}_{\mathfrak{p}}^{\mathrm{sep}}$, the map

$$\mathrm{K}_{\mathfrak{p}}^{\times} \overset{(-,\mathrm{K}_{\mathfrak{p}}^{\mathrm{ab}}/\mathrm{K}_{\mathfrak{p}})}{\longrightarrow} \mathrm{G}(\mathrm{K}_{\mathfrak{p}}^{\mathrm{sep}}/\mathrm{K}_{\mathfrak{p}}) \to \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K}) \overset{-|_{\mathrm{K}^{\infty}}}{\to} \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K}) \overset{\theta_{\mathrm{K}}^{-1}}{\to} \mathrm{CL}_{\mathrm{O_K},\infty}$$

is given by

$$a \mapsto [a] \tag{1.4.8.2}$$

where we view $a \in \mathrm{K}_{\mathfrak{p}}^{\times} \subset (\mathrm{A}_{\mathrm{O_K}} \otimes_{\mathrm{O_K}} \mathrm{K})^{\times}$.

1.5. Class stacks

We now extend the definition of the level-$\mathfrak{f}$ structures on $\mathrm{O_K}$-modules to level-$\mathfrak{f}$ structures on $\mathrm{O_K}$-local systems over sheaves and give several basic results concerning them and their moduli stacks.

1.5.1. So let S be a sheaf over $\mathrm{Spec}(\mathrm{O_K})$ (this is technically not important for what follows) and consider the constant sheaf of rings $\underline{\mathrm{O_K}}_{\mathrm{S}}$ on S associated to $\mathrm{O_K}$. If L is any $\mathrm{O_K}$-module we write $\underline{\mathrm{L}}_{\mathrm{S}}$ for the corresponding constant $\underline{\mathrm{O_K}}_{\mathrm{S}}$-module. If F and G are two $\underline{\mathrm{O_K}}_{\mathrm{S}}$-modules over S we write $\mathrm{F} \otimes_{\mathrm{O_K}} \mathrm{G}$ for the tensor product $\mathrm{F} \otimes_{\underline{\mathrm{O_K}}_{\mathrm{S}}} \mathrm{G}$ and if $\mathrm{G} = \underline{\mathrm{L}}_{\mathrm{S}}$ for some $\mathrm{O_K}$-module L we just write $\mathrm{F} \otimes_{\mathrm{O_K}} \mathrm{L}$. We also write $\underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{F},\mathrm{G})$ for the sheaf of $\underline{\mathrm{O_K}}_{\mathrm{S}}$-homomorphisms $\mathrm{F} \to \mathrm{G}$.

1.5.2. A rank one $\mathrm{O_K}$-local system on S is a sheaf of $\underline{\mathrm{O_K}}_{\mathrm{S}}$-modules $\mathscr{L}$ over S such that there exists a cover $(\mathrm{S}_i \to \mathrm{S})_{i\in\mathrm{I}}$, rank one projective $\mathrm{O_K}$-modules $(\mathrm{L}_i)_{i\in\mathrm{I}}$ and $\underline{\mathrm{O_K}}_{\mathrm{S}}$-isomorphisms $\mathscr{L} \times_{\mathrm{S}} \mathrm{S}_i \xrightarrow{\sim} \underline{\mathrm{L}_i}_{\mathrm{S}_i}$. The moduli stack of rank one $\mathrm{O_K}$-local systems over $\mathrm{Sh}_{\mathrm{O_K}}$ is denoted by $\mathscr{C}\mathscr{L}_{\mathrm{O_K}}$. We list the following (usual) constructions and properties of $\mathrm{O_K}$-local systems.

(i) The tensor product $\mathscr{L} \otimes_{\mathrm{O_K}} \mathscr{L}'$ of two rank one $\mathrm{O_K}$-local systems $\mathscr{L}$ and $\mathscr{L}'$ is again a rank one $\mathrm{O_K}$-local system.

(ii) The sheaf of $\underline{\mathrm{O_K}}_{\mathrm{S}}$-homomorphisms $\underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L},\mathscr{L}')$ is again a rank one $\mathrm{O_K}$-local system and defining $\mathscr{L}^{\vee} := \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L},\underline{\mathrm{O_K}}_{\mathrm{S}})$ we have $\mathscr{L}' \otimes_{\mathrm{O_K}} \mathscr{L}^{\vee} \xrightarrow{\sim} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L},\mathscr{L}')$.

(iii) The sheaf of automorphisms $\underline{\mathrm{Aut}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L})$ of a rank one $\mathrm{O_K}$-local system $\mathscr{L}$ is isomorphic to $\underline{\mathrm{O_K}}_{\mathrm{S}}^{\times}$.

(iv) The sheaf of $\mathrm{O_K}$-isomorphisms $\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L},\mathscr{L}')$ is finite and étale over S and $\mathscr{L}$ and $\mathscr{L}'$ are locally isomorphic on S if and only if $\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L},\mathscr{L}') \to \mathrm{S}$ is an epimorphism if and only if the action of $\underline{\mathrm{O_K}}_{\mathrm{S}}^{\times}$ on $\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L},\mathscr{L}') \to \mathrm{S}$ makes it a torsor.

(v) Every rank one $\mathrm{O_K}$-local system is, locally on S, isomorphic $\underline{\mathrm{L}}_{\mathrm{S}}$ for some rank one projective $\mathrm{O_K}$-module L whose corresponding class in $\mathrm{CL}_{\mathrm{O_K}}$ is independent of the choice of L. Thus given an $\mathrm{O_K}$-local system $\mathscr{L}$ on S one obtains a section $c_{\mathscr{L}/\mathrm{S}} \in \underline{\mathrm{CL}_{\mathrm{O_K}}}(\mathrm{S})$, or what is the same a map

$$c_{\mathscr{L}/\mathrm{S}} : \mathrm{S} \to \underline{\mathrm{CL}_{\mathrm{O_K}}}$$

from S to the constant sheaf over $\mathrm{Spec}(\mathrm{O_K})$ associated to the group $\mathrm{CL}_{\mathrm{O_K}}$. Moreover, if one chooses representatives L of each class $[\mathrm{L}] \in \mathrm{CL}_{\mathrm{O_K}}$ and considers the rank one $\mathrm{O_K}$-local system over $\underline{\mathrm{CL}_{\mathrm{O_K}}}$:

$$[\mathrm{L}]^{\mathrm{univ}} := \coprod_{[\mathrm{L}]\in \mathrm{CL}_{\mathrm{O_K}}} \underline{\mathrm{L}} \to \coprod_{[\mathrm{L}]\in \mathrm{CL}_{\mathrm{O_K}}} \mathrm{Spec}(\mathrm{O_K}) = \underline{\mathrm{CL}_{\mathrm{O_K}}}$$

then $\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L}, c_{\mathscr{L}/\mathrm{S}}^{*}([\mathrm{L}]^{\mathrm{univ}}))$ is an $\underline{\mathrm{O_K}}_{\mathrm{S}}^{\times}$-torsor whose corresponding class in $\mathrm{H}^1(\mathrm{S}, \underline{\mathrm{O_K}}_{\mathrm{S}}^{\times})$ we denote by $\rho_{\mathscr{L}/\mathrm{S}}$. The resulting map

$$\mathscr{L} \mapsto (c_{\mathscr{L}/\mathrm{S}}, \rho_{\mathscr{L}/\mathrm{S}}) \in \underline{\mathrm{CL}_{\mathrm{O_K}}}(\mathrm{S}) \times \mathrm{H}^1(\mathrm{S}, \underline{\mathrm{O_K}}_{\mathrm{S}}^{\times})$$

defines a bijection between isomorphism classes of rank one $\mathrm{O_K}$-local systems over S and the set $\underline{\mathrm{CL}_{\mathrm{O_K}}}(\mathrm{S}) \times \mathrm{H}^1(\mathrm{S}, \underline{\mathrm{O_K}}_{\mathrm{S}}^{\times})$.

1.5.3. If $\mathfrak{f}$ is an integral ideal of $\mathrm{O_K}$ a level-$\mathfrak{f}$ structure on a rank one $\mathrm{O_K}$-local system $\mathscr{L}$ over S is an epimorphism of $\underline{\mathrm{O_K}}_{\mathrm{S}}$-modules $\alpha : \mathscr{L} \xrightarrow{\sim} \underline{\mathrm{O_K}/\mathfrak{f}}_{\mathrm{S}}$. An $\mathfrak{f}$-isomorphism $f : (\mathscr{L},\alpha) \xrightarrow{\sim} (\mathscr{L}',\alpha')$ of rank one $\mathrm{O_K}$-local systems of over S equipped level-$\mathfrak{f}$ structures is an $\mathrm{O_K}$-linear isomorphism $f : \mathscr{L} \xrightarrow{\sim} \mathscr{L}'$ such that $\alpha' \circ f = \alpha$. With this definition every $(\mathscr{L},\alpha)$ is, locally on S, of the form $(\underline{\mathrm{L}}_{\mathrm{S}}, \underline{a}_{\mathrm{S}})$ for some $(\mathrm{L}, a) \in \mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}$. When working with rank one $\mathrm{O_K}$-local systems we will often drop explicit reference to the level-$\mathfrak{f}$ structure when it is clear from context. We list the following (usual) constructions and properties of $\mathrm{O_K}$-local systems with level-$\mathfrak{f}$ structure.

(i) The tensor product $\mathscr{L} \otimes_{\mathrm{O_K}} \mathscr{L}'$ of two rank one O-local systems $(\mathscr{L},\alpha)$ and $(\mathscr{L}',\alpha')$ equipped with level-$\mathfrak{f}$ structures is again a rank one $\mathrm{O_K}$-local system with level-$\mathfrak{f}$ structure given by $\alpha \otimes_{\mathrm{O_K}} \alpha'$.

(ii) The sheaf of $\underline{\mathrm{O_K}}_{\mathrm{S}}$-homomorphisms $\underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L},\mathscr{L}')$ is again a rank one $\mathrm{O_K}$-local system with level-$\mathfrak{f}$ structure given by

$$\underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L} \otimes_{\mathrm{O_K}} \mathrm{O_K}/\mathfrak{f}, \mathscr{L}' \otimes_{\mathrm{O_K}} \mathrm{O_K}/\mathfrak{f}) \xrightarrow{\sim} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\underline{\mathrm{O_K}/\mathfrak{f}}_{\mathrm{S}}, \underline{\mathrm{O_K}/\mathfrak{f}}_{\mathrm{S}}) = \underline{\mathrm{O_K}/\mathfrak{f}}_{\mathrm{S}},$$

and equipping $\mathscr{L}^\vee := \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L}, \underline{\mathrm{O_K}}_{\mathrm{S}})$ with this level-$\mathfrak{f}$ structure makes $\mathscr{L}' \otimes_{\mathrm{O_K}} \mathscr{L}^\vee \xrightarrow{\sim} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L}, \mathscr{L}')$ is an $\mathfrak{f}$-isomorphism.

(iii) The sheaf of $\mathfrak{f}$-automorphisms $\underline{\mathrm{Aut}}_{\mathrm{S}}^{(\mathfrak{f})}(\mathscr{L})$ of a rank one $\mathrm{O_K}$-local system $(\mathscr{L}, \alpha)$ with level-$\mathfrak{f}$ structure is equal to $\underline{(\mathrm{O_K}/\mathfrak{f})^\times}_{\mathrm{S}}$ and in particular is trivial if $\mathfrak{f}$ separates units.

(iv) The sheaf of $\mathfrak{f}$-isomorphisms $\underline{\mathrm{Isom}}_{\mathrm{S}}^{(\mathfrak{f})}(\mathscr{L}, \mathscr{L}')$ between two rank one $\mathrm{O_K}$-local systems with level-$\mathfrak{f}$ structure is finite and étale over S and $\mathscr{L}$ and $\mathscr{L}'$ are locally $\mathfrak{f}$-isomorphic if and only if $\underline{\mathrm{Isom}}_{\mathrm{S}}^{(\mathfrak{f})}(\mathscr{L}, \mathscr{L}')$ is an $\underline{\mathrm{O_K}^{\times,\mathfrak{f}}}_{\mathrm{S}}$-torsor.

(v) Every rank one $\mathrm{O_K}$-local system with level-$\mathfrak{f}$ structure is, locally on S, $\mathfrak{f}$-isomorphic $(\underline{\mathrm{L}}_{\mathrm{S}}, \underline{a}_{\mathrm{S}})$ for some rank one projective $\mathrm{O_K}$-module with level-$\mathfrak{f}$ structure (L, a) whose corresponding class in $\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}$ is independent of the choice of L. Thus given an $\mathrm{O_K}$-local system $\mathscr{L}$ on S one obtains a section $c_{\mathscr{L}/\mathrm{S},\mathfrak{f}} \in \underline{\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}}(\mathrm{S})$, or what is the same a map

$$c_{\mathscr{L}/\mathrm{S},\mathfrak{f}} : \mathrm{S} \to \underline{\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}}$$

from S to the constant sheaf over $\mathrm{Spec}(\mathrm{O_K})$ associated to the group $\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}$. Moreover, if one chooses representatives (L, a) of each class $[\mathrm{L}, a] \in \mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}$ and considers the rank one $\mathrm{O_K}$-local system with level-$\mathfrak{f}$ structure over $\underline{\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}}$:

$$[\mathrm{L}, a]^{\mathrm{univ}} := \coprod_{[\mathrm{L},a] \in \mathrm{CL}_{\mathrm{O_K}}} (\underline{\mathrm{L}}, \underline{a}) \to \coprod_{[\mathrm{L},a] \in \mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}} \mathrm{Spec}(\mathrm{O_K}) = \underline{\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}}$$

then $\underline{\mathrm{Isom}}_{\mathrm{S}}^{(\mathfrak{f})}(\mathscr{L}, c_{\mathscr{L}/\mathrm{S}}^*([\mathrm{L}, a]^{\mathrm{univ}}))$ is an $\underline{\mathrm{O_K}^{\times,\mathfrak{f}}}_{\mathrm{S}}$-torsor whose corresponding class in $\mathrm{H}^1(\mathrm{S}, \underline{\mathrm{O_K}^{\times,\mathfrak{f}}}_{\mathrm{S}})$ we denote by $\rho_{\mathscr{L}/\mathrm{S},\mathfrak{f}}$. The resulting map

$$\mathscr{L} \mapsto (c_{\mathscr{L}/\mathrm{S},\mathfrak{f}}, \rho_{\mathscr{L}/\mathrm{S},\mathfrak{f}}) \in \underline{\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}}(\mathrm{S}) \times \mathrm{H}^1(\mathrm{S}, \underline{\mathrm{O_K}^\times}_{\mathrm{S}})$$

defines a bijection between isomorphisms classes of rank one $\mathrm{O_K}$-local systems over S and the set $\underline{\mathrm{CL}_{\mathrm{O_K}}}(\mathrm{S}) \times \mathrm{H}^1(\mathrm{S}, \underline{\mathrm{O_K}^{\times,\mathfrak{f}}}_{\mathrm{S}})$. In particular, if $\mathfrak{f}$ separates units then $\mathrm{H}^1(\mathrm{S}, \underline{\mathrm{O_K}^{\times,\mathfrak{f}}}_{\mathrm{S}}) = 0$ and the map

$$\mathscr{L} \mapsto c_{\mathscr{L}/\mathrm{S},\mathfrak{f}} \in \underline{\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}}(\mathrm{S})$$

defines a bijection between $\mathfrak{f}$-isomorphism classes of rank one $\mathrm{O_K}$-local systems with level-$\mathfrak{f}$ structure over S and elements of $\underline{\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}}$.

(vi) If $\mathfrak{f}$ separates units, $(\mathscr{L}, \alpha)$ is an $\mathrm{O_K}$-local system equipped with a level-$\mathfrak{f}$ structure and S is connected, then $(\mathscr{L}, \alpha) \xrightarrow{\sim} (\underline{\mathrm{L}}_{\mathrm{S}}, \underline{a}_{\mathrm{S}})$ for some rank one projective $\mathrm{O_K}$-module with level-$\mathfrak{f}$ structure and in particular, $\mathscr{L}$ is constant.

1.5.4 Corollary. — *The map*

$$\mathscr{C}\mathscr{L}^{(\mathfrak{f})}_{\mathrm{O_K}} \to \underline{\mathrm{CL}}^{(\mathfrak{f})}_{\mathrm{O_K}} : \mathscr{L}/\mathrm{S} \mapsto c_{\mathscr{L}/\mathrm{S}} \in \underline{\mathrm{CL}}^{(\mathfrak{f})}_{\mathrm{O_K}}(\mathrm{S})$$

identifies $\underline{\mathrm{CL}}^{(\mathfrak{f})}_{\mathrm{O_K}}$ *with the coarse sheaf of* $\mathscr{C}\mathscr{L}^{(\mathfrak{f})}_{\mathrm{O_K}}$ *and is an equivalence whenever* $\mathfrak{f}$*-separates units.*

Proof. — This follows from the remarks (1.5.3). □

CHAPTER 2

ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

In this chapter we develop the general theory of (families of) elliptic curves with complex multiplication by the ring of integers $\mathrm{O_K}$ of a fixed imaginary quadratic field K, here on called just CM elliptic curves. In §1 we recall several standard results from the theory of (families of general) elliptic curves. In §2 we define the notion of a family $\mathrm{E} \to \mathrm{S}$ of CM elliptic curves, the corresponding moduli stack $\mathscr{M}_{\mathrm{CM}}$, and we show that (just as with Lubin–Tate O-modules) the moduli stack $\mathscr{C}\mathscr{L}_{\mathrm{O_K}}$ of rank one $\mathrm{O_K}$-local systems acts in a natural way on the moduli stack $\mathscr{M}_{\mathrm{CM}}$ of CM elliptic curves. We then describe, for a prime $\mathfrak{p} \subset \mathrm{O_K}$, the properties of the $\mathfrak{p}$-power torsion subgroups $\mathrm{E}[\mathfrak{p}^\infty] \subset \mathrm{E}$ of a family of CM elliptic curves and show that when S is a $\mathfrak{p}$-adic sheaf $\mathrm{E}[\mathfrak{p}^\infty]$ is a Lubin–Tate $\mathrm{O_{K_\mathfrak{p}}}$-module. In §3 we consider CM elliptic curves over complex and $\mathfrak{p}$-adic bases and give CM analogues of the classification of elliptic curves over complex bases, and theorem of Serre-Tate describing deformations of elliptic curves over $\mathfrak{p}$-adic bases. In §4 we show that any two CM elliptic curves over the same base are locally isogenous and from this deduce that the action of $\mathscr{C}\mathscr{L}_{\mathrm{O_K}}$ on $\mathscr{M}_{\mathrm{CM}}$ gives $\mathscr{M}_{\mathrm{CM}}$ the structure of a torsor. In §5 we derive the global reciprocity map associated to the maximal abelian extension of K (totally split at ∞ – but this is a vacuous condition) directly from the stack $\mathscr{M}_{\mathrm{CM}}$ in a manner quite analogous to the derivation of the local reciprocity map via the moduli stack of Lubin–Tate O-modules. We then classify all CM elliptic curves over fields (both of characteristic zero and finite characteristic) and prove some results regarding good reduction. In §5 we define level-$\mathfrak{f}$ structures for CM elliptic curves and consider the corresponding moduli stacks $\mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})}$. As with $\mathscr{M}_{\mathrm{CM}}$ and $\mathscr{C}\mathscr{L}_{\mathrm{O_K}}$, we show that $\mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})}$ is a torsor under $\mathscr{C}\mathscr{L}_{\mathrm{O_K}}^{(\mathfrak{f})}$ (at least after inverting $\mathfrak{f}$). Using this we show that the coarse sheaf of $\mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})}$ is isomorphic to $\mathrm{Spec}(\mathrm{O_{K(\mathfrak{f})}}[\mathfrak{f}^{-1}])$ where $\mathrm{K}(\mathfrak{f})$ is the ray class field of conductor $\mathfrak{f}$.

We should point out that, aside from the $\mathscr{C}\mathscr{L}_{\mathrm{O_K}}$-torsor structure of $\mathscr{M}_{\mathrm{CM}}$, consistently working over a general base (instead of a field) and our derivation of the reciprocity map, almost everything in this chapter is probably more or less already known. This combined with the fact that $\mathscr{M}_{\mathrm{CM}}$ is zero dimensional

over $\mathrm{Spec}(\mathrm{O_K})$, the advantages of our general approach may be somewhat unclear. However, while $\mathscr{M}_{\mathrm{CM}}$ is geometrically rather simple, it is arithmetically quite complicated and the general approach we take in this chapter will allow for great deal of flexibility later when we wish to study some of its finer arithmetic properties.

2.1. General elliptic curves

We now recall the definition of a family of elliptic curves over a sheaf S and recall several standard results. In particular, the fact that the moduli stack of elliptic curves is indeed a stack, the rigidity principal for homomorphisms, the representability of Isom sheaves, Grothendieck's formal GAGA, the classification of elliptic curves over complex schemes S in terms of rank two $\mathbf{Z}$-local systems over S^{an}, the Serre-Tate theorem, and the criterion of good reduction.

2.1.1. Let S be a sheaf. An elliptic curve over S is a sheaf of groups $\mathrm{E} \to \mathrm{S}$ which is relatively representable, smooth of relative dimension one, proper and geometrically connected. A morphism is of course a homomorphism of the underlying (sheaves of) groups over S. For many more general properties and constructions related to families of elliptic curves $\mathrm{E} \to \mathrm{S}$ we refer the reader to the wonderful book of Katz-Mazur [**24**].

If S is a sheaf we write $\mathrm{Ell}(\mathrm{S})$ for the category of elliptic curves over S and we denote by $\mathscr{M}_{\mathrm{Ell}}$ the fibred category over Sh whose fibre over a sheaf S is the category elliptic curves E/S together with their isomorphisms.

2.1.2 Proposition. — *The fibred category $\mathscr{M}_{\mathrm{Ell}}$ is a stack over* Sh.

Sketch. — If S is an affine scheme and $f : \mathrm{E} \to \mathrm{S}$ is a family of elliptic curves let $\mathscr{I}_{\mathrm{E/S}} \subset \mathscr{O}_{\mathrm{E}}$ denote the ideal sheaf defining the zero section $\mathrm{S} \to \mathrm{E}$ (it is a locally free rank one $\mathscr{O}_{\mathrm{E}}$-module). The quasi-coherent $\mathscr{O}_{\mathrm{S}}$-module $\mathscr{W}_{\mathrm{E/S}} = f_*(\mathscr{I}_{\mathrm{E/S}}^{-3})$ is a vector bundle of rank three, the morphism

$$f^* f_*(\mathscr{I}_{\mathrm{E/S}}^{-3}) \to \mathscr{I}_{\mathrm{E/S}}^{-3}$$

is an epimorphism and defines a closed immersion $w_{\mathrm{E/S}} : \mathrm{E} \to \mathbf{P}(\mathscr{W}_{\mathrm{E/S}})$. Both the vector bundle $\mathscr{W}_{\mathrm{E/S}}$ and the morphism $w_{\mathrm{E/S}}$ are functorial in S so that by descent if $\mathrm{E} \to \mathrm{S}$ is any family of elliptic curves over a sheaf S then there is a unique vector bundle $\mathscr{W}_{\mathrm{E/S}}$ of rank three over S together with a closed immersion $w_{\mathrm{E/S}} : \mathrm{E} \to \mathbf{P}_{\mathrm{S}}(\mathscr{W}_{\mathrm{E/S}})$ compatible with those defined when S is affine.

Now if S is an sheaf and $(f_i : \mathrm{E}_i \to \mathrm{S}_i)_{i \in \mathrm{I}}$ is a family of elliptic curves equipped with descent data relative to a cover $(\mathrm{S}_i)_{i \in \mathrm{I}}$ of S then the E_i descend to a *sheaf* of groups $\mathrm{E} \to \mathrm{S}$, the vector bundles $\mathscr{W}_{\mathrm{E}_i/\mathrm{S}_i}$ to a vector bundle $\mathscr{W}_{\mathrm{E/S}}$ and the closed immersions $w_{\mathrm{E}_i} : \mathrm{E}_i \to \mathbf{P}(\mathscr{W}_{\mathrm{E}_i/\mathrm{S}_i})$ to a closed immersion

$$w_{\mathrm{E/S}} : \mathrm{E} \to \mathbf{P}(\mathscr{W}_{\mathrm{E/S}}).$$

This shows that the morphism $p : \mathrm{E} \to \mathrm{S}$ is representable (in fact projective) and by descent it follows that $\mathrm{E} \to \mathrm{S}$ is also smooth of relative dimension one, proper, and geometrically connected so that $\mathrm{E} \to \mathrm{S}$ is an elliptic curve over S. □

2.1.3. Here we recall several useful properties enjoyed by homomorphisms of elliptic curves.

2.1.4 Proposition. — *Let* S *be a sheaf and let* $\mathrm{E} \to \mathrm{S}$ *be a family of elliptic curves. For each* $n \geq 1$ *multiplication map* $n : \mathrm{E} \to \mathrm{E}$ *is finite locally free of degree* n^2*.*

Proof. — This is Theorem 2.3.1 of [**24**]. □

***2.1.5 Proposition* (Rigidity).** — *If* $f : \mathrm{E} \to \mathrm{E}'$ *is a homomorphism of elliptic curves over a sheaf* S *there is a unique decomposition* $\mathrm{S} = \amalg_{n \geq 0} \mathrm{S}_{(n)}$ *with the property that* $f \times_{\mathrm{S}} \mathrm{S}_{(0)}$ *is the zero map and such that* $f \times_{\mathrm{S}} \mathrm{S}_{(n)}$ *is finite locally free of degree* n *for* $n \geq 1$*. In particular, if* $f, g : \mathrm{E} \to \mathrm{E}'$ *are a pair of homomorphisms of elliptic curves and* $\mathrm{S}' \to \mathrm{S}$ *is a morphism of sheaves which is surjective on geometric points then* $f = g$ *if and only if* $f \times_{\mathrm{S}} \mathrm{S}' = g \times_{\mathrm{S}} \mathrm{S}'$*.*

Proof. — The first statement is Theorem 2.4.2 of [**24**]. For the second statement the only if direction is clear, so assume that $f \times_{\mathrm{S}} \mathrm{S}' = g \times_{\mathrm{S}} \mathrm{S}'$. The claim is local on S and S' and so we may assume that they are affine schemes. If $\mathrm{S}_{(0)} \subset \mathrm{S}$ and $\mathrm{S}'_{(0)} \subset \mathrm{S}'$ denote the open and closed sub-schemes where $f - g$ and $f \times_{\mathrm{S}} \mathrm{S}' - g \times_{\mathrm{S}} \mathrm{S}'$ are equal to the zero map respectively, then $\mathrm{S}'_{(0)} \to \mathrm{S}$ factors through $\mathrm{S}_{(0)}$. However, $\mathrm{S}'_{(0)} = \mathrm{S}'$, so that as $\mathrm{S}' \to \mathrm{S}$ is surjective on geometric points, it follows that $\mathrm{S}_{(0)} = \mathrm{S}$. □

2.1.6 Remark. — We will make much use of (2.1.5) and when doing so just say 'by rigidity'.

2.1.7 Proposition. — *For each pair of elliptic curves* E *and* E' *over a sheaf* S *the sheaf* $\underline{\mathrm{Isom}}_{\mathrm{S}}(\mathrm{E}, \mathrm{E}')$ *is finite and unramified over* S*.*

Proof. — The claim is local on S so we may assume that S is an affine scheme and this is Proposition 5.3 (i) of [**15**]. □

2.1.8. Let A be a noetherian ring complete with respect to the I-adic topology for $\mathrm{I} \subset \mathrm{A}$ an ideal and write $\mathrm{Spf}(\mathrm{A}) = \mathrm{colim}_{n \geq 0} \mathrm{Spec}(\mathrm{A}/\mathrm{I}^{n+1}) \subset \mathrm{Spec}(\mathrm{A})$.

***2.1.9 Theorem* (Formal GAGA).** — *The functor*

$$\mathrm{Ell}(\mathrm{Spec}(\mathrm{A})) \to \mathrm{Ell}(\mathrm{Spf}(\mathrm{A})) : \mathrm{E}/\mathrm{Spec}(\mathrm{A}) \mapsto \mathrm{E} \times_{\mathrm{Spec}(\mathrm{A})} \mathrm{Spf}(\mathrm{A})$$

induced by base change is an equivalence of categories.

Proof. — This is an easy application Grothendieck's formal GAGA (in particular Corollaire 2 and Théorème 4 of [**23**]). □

2.1.10. The following is taken from Nº 2 of [**16**]. Let S be a locally finitely presented $\mathrm{Spec}(\mathbf{C})$-scheme and let $f : \mathrm{E} \to \mathrm{S}$ be an elliptic curve. The analytification $f^{\mathrm{an}} : \mathrm{E}^{\mathrm{an}} \to \mathrm{S}^{\mathrm{an}}$ is an analytic space over S^{an} which is smooth of relative dimension one and proper with connected fibres. There is a canonical exact sequence, the exponential sequence, of sheaves on the big analytic site of X^{an}

$$0 \to \mathrm{T}_{\mathbf{Z}}(\mathrm{E}) \to \underline{\mathrm{Lie}}_{\mathrm{E}^{\mathrm{an}}/\mathrm{S}^{\mathrm{an}}} \to \mathrm{E}^{\mathrm{an}} \to 0$$

(we view $\underline{\mathrm{Lie}}_{\mathrm{S}^{\mathrm{an}}/\mathrm{E}^{\mathrm{an}}}$ as a rank one locally free sheaf of $\mathscr{O}_{\mathrm{S}^{\mathrm{an}}}$-modules on the *big* analytic site of S) with $\mathrm{T}_{\mathbf{Z}}(\mathrm{E})$ a rank two $\mathbf{Z}$-local system on S^{an}. Denote by $\mathrm{Lat}(\mathrm{S}^{\mathrm{an}})$ the category of pairs $(\mathrm{T} \subset \mathscr{V})$ where $\mathscr{V}$ is a locally free rank one $\mathscr{O}_{\mathrm{S}^{\mathrm{an}}}$-module and $\mathrm{T} \subset \mathscr{V}$ is a rank two $\mathbf{Z}$-local system which is fibre-wise over S^{an} discrete in $\mathscr{V}$.

2.1.11 Proposition. — *The functor*

$$\mathrm{Ell}(\mathrm{S}) \to \mathrm{Lat}(\mathrm{S}^{\mathrm{an}}) : \mathrm{E}/\mathrm{S} \mapsto (\mathrm{T}_{\mathbf{Z}}(\mathrm{E}/\mathrm{S}) \subset \underline{\mathrm{Lie}}_{\mathrm{E}^{\mathrm{an}}/\mathrm{S}^{\mathrm{an}}})$$

is an equivalence of categories.

2.1.12. Let p be a rational prime and S a p-adic sheaf (i.e. a sheaf over $\mathrm{Spf}(\mathbf{Z}_p) = \mathrm{colim}_n \mathrm{Spec}(\mathbf{Z}/p^{n+1})$). A p-divisible group over S is an sheaf of groups $\mathrm{F} \to \mathrm{S}$ such that the multiplication map $p : \mathrm{F} \to \mathrm{F}$ is representable, finite locally free and faithfully flat and such that $\mathrm{colim}_n \ker(p^n) = \mathrm{F}$. If E is an elliptic curve over S we write $\mathrm{E}[p^\infty]$ for the p-divisible group $\mathrm{colim}_n \mathrm{E}[p^n]$.

Let $\mathrm{S}_0 \to \mathrm{S}$ be a nilpotent closed immersion of p-adic sheaves and consider the category $\mathrm{D}(\mathrm{S}, \mathrm{S}_0)$ whose objects are triples $(\mathrm{E}/\mathrm{S}_0, \mathrm{F}/\mathrm{S}, \rho)$ with

(i) $\mathrm{E}_0/\mathrm{S}_0$ an elliptic curve,
(ii) F/S is a p-divisible group, and
(iii) $\rho : \mathrm{E}_0[p^\infty] \xrightarrow{\sim} \mathrm{F} \times_{\mathrm{S}} \mathrm{S}_0$ an isomorphism of p-divisible groups,

and whose morphisms $(\mathrm{E}_0/\mathrm{S}_0, \mathrm{F}/\mathrm{S}, \rho) \to (\mathrm{E}'/\mathrm{S}_0, \mathrm{F}', \rho')$ are pairs (f, g) where $f : \mathrm{E} \to \mathrm{E}'$ is a morphism of elliptic curves, $g : \mathrm{F} \to \mathrm{F}'$ is a morphism of p-divisible groups such that

$$(g \times_{\mathrm{S}} \mathrm{S}_0) \circ \rho = \rho' \circ f|_{\mathrm{E}[p^\infty]}.$$

***2.1.13 Theorem* (Serre-Tate).** — *The functor*

$$\mathrm{Ell}(\mathrm{S}) \to \mathrm{D}_p(\mathrm{S}, \mathrm{S}_0) : \mathrm{E}/\mathrm{S} \mapsto (\mathrm{E} \times_{\mathrm{S}} \mathrm{S}_0/\mathrm{S}_0, \mathrm{E}[p^\infty]/\mathrm{S}, \mathrm{id}_{\mathrm{E}[p^\infty]}|_{\mathrm{S}_0})$$

is an equivalence of categories.

Proof. — A short argument using (2.1.2) reduces us to the case where S is an affine scheme and this case is the content of the Appendix of [**19**]. □

2.1.14. Let S be a Dedekind scheme, i.e. a one dimensional, regular and irreducible scheme. Let $f : \mathrm{Spec}(\mathrm{K}) \to \mathrm{S}$ be its generic point and let $\mathrm{E}/\mathrm{Spec}(\mathrm{K})$.

***2.1.15 Theorem* (Néron models).** — *The functor* $\mathrm{X}/\mathrm{S} \mapsto \mathrm{E}(\mathrm{X} \times_{\mathrm{S}} \mathrm{Spec}(\mathrm{K}))$ *on* smooth *schemes over* S *is representable by a smooth, one dimensional group scheme* $\mathrm{Nér}_{\mathrm{S}}(\mathrm{E})/\mathrm{S}$. *Moreover, if* $\mathrm{S}' \to \mathrm{S}$ *is an étale map of Dedekind schemes and* $\mathrm{Spec}(\mathrm{K}') \to \mathrm{S}'$ *is the generic point of* S' *then*

$$\mathrm{Nér}_{\mathrm{S}}(\mathrm{E}) \times_{\mathrm{S}} \mathrm{S}' = \mathrm{Nér}_{\mathrm{S}'}(\mathrm{E} \times_{\mathrm{Spec}(\mathrm{K})} \mathrm{Spec}(\mathrm{K}')).$$

Proof. — Representability of the functor is Theorem 3 §1.4 Chapter 1 of [**9**] and compatibility with étale base change is Proposition 2 (b) §1.2 of [**9**]. □

2.1.16 Theorem. — *Let* $\mathrm{L}/\mathbf{Q}$ *be a finite extension, v a place over* $\mathbf{Q}^{\mathrm{sep}}$ *lying over the prime* $\mathfrak{p}$ *of* O_{L} *with residue characteristic* $p > 0$ *and let* E/L *be an elliptic curve. Then* $\mathrm{Nér}_{\mathrm{O}_{\mathrm{L},\mathfrak{p}}}(\mathrm{E}) \to \mathrm{Spec}(\mathrm{O}_{\mathrm{L},\mathfrak{p}})$ *is an elliptic curve if, for some prime* $l \neq p$, *the action of the inertia group* $\mathrm{I}_v \subset \mathrm{G}(\mathbf{Q}^{\mathrm{sep}}/\mathrm{L})$ *on* $\mathrm{E}[l^\infty](\mathbf{Q}^{\mathrm{sep}})$ *is trivial.*

Proof. — This follows from Theorem 1 of [**31**]. □

2.2. Elliptic curves with complex multiplication

In this section we define families of elliptic curves with complex multiplication by the ring of integers O_{K} of an imaginary quadratic field K or, for short, CM elliptic curves. We give analogues for CM elliptic curves of several of the results of (1.2) given for Lubin–Tate O-modules. In particular, we consider the moduli stack $\mathscr{M}_{\mathrm{CM}}$ of CM elliptic curves and show that the stack $\mathscr{CL}_{\mathrm{O}_{\mathrm{K}}}$ of rank one O_{K}-local system acts on $\mathscr{M}_{\mathrm{CM}}$.

2.2.1. For the remainder of this chapter we fix an imaginary quadratic field $\mathrm{K} = \mathbf{Q}(\sqrt{-d})$ for $d \in \mathbf{N}$ square free and with ring of integers O_{K}. We note that K has only one archimedian place ∞ and so (K, ∞) satisfies the conditions of (1.4.1) and we shall make use and notation (and in later sections theory) set up in §1.4 of Chapter 1. As $\mathrm{K}_\infty \xrightarrow{\sim} \mathbf{C}$ is algebraically closed every finite extension of K is totally split at infinity so that $\mathrm{K}^\infty = \mathrm{K}^{\mathrm{ab}}$, although we shall continue to use the notation K^∞. The unit group $\mathrm{O}_{\mathrm{K}}^\times$ is finite and is equal to $\{\pm 1\}$ unless $\mathrm{K} = \mathbf{Q}(\mu_n)$ for $n = 4, 6$ in which case $\mathrm{O}_{\mathrm{K}}^\times = \mu_n$. The unique non-trivial automorphism of $\mathrm{K}/\mathbf{Q}$ is denoted by $a \mapsto \overline{a}$. We shall be working solely in the category $\mathrm{Sh}_{\mathrm{O}_{\mathrm{K}}}$ and so by a sheaf S we will mean a sheaf over $\mathrm{Spec}(\mathrm{O}_{\mathrm{K}})$. In particular, to simplify some of the notation we will write $\mathrm{X} \times \mathrm{Y}$ for the product $\mathrm{X} \times_{\mathrm{Spec}(\mathrm{O}_{\mathrm{K}})} \mathrm{Y}$ in $\mathrm{Sh}_{\mathrm{O}_{\mathrm{K}}}$.

2.2.2. An elliptic curve with complex multiplication by $\mathrm{O_K}$ over S, or for short a CM elliptic curve over S, is an elliptic curve $\mathrm{E} \to \mathrm{S}$ (2.1.1) equipped an $\underline{\mathrm{O_K}}_{\mathrm{S}}$-module structure which is strict with respect to the morphism $\underline{\mathrm{O_K}}_{\mathrm{S}} \to \mathscr{O}_{\mathrm{S}}$ coming from the structure map $\mathrm{S} \to \mathrm{Spec}(\mathrm{O_K})$ (cf. (A.2.4)). A morphism of CM elliptic curves over S is just a homomorphism of $\underline{\mathrm{O_K}}_{\mathrm{S}}$-modules. For $a \in \underline{\mathrm{O_K}}_{\mathrm{S}}(\mathrm{S})$ we write $[a]_{\mathrm{E}} : \mathrm{E} \to \mathrm{E}$, or just $a : \mathrm{E} \to \mathrm{E}$, for the corresponding endomorphism (in particular for $a \in \mathrm{O_K} \subset \underline{\mathrm{O_K}}_{\mathrm{S}}(\mathrm{S})$).

Finally, we write $\mathrm{CM}(\mathrm{S})$ for the category of CM elliptic curves over a sheaf S and we write $\mathscr{M}_{\mathrm{CM}}$ for the stack over $\mathrm{Sh}_{\mathrm{O_K}}$ whose fibre over S is the category of CM elliptic curves over S together with their isomorphisms.

2.2.3 Proposition. — *For any* CM *elliptic curve* $\mathrm{E/S}$ *the morphism*

$$\underline{\mathrm{O_K}}_{\mathrm{S}} \to \underline{\mathrm{End}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E})$$

is an isomorphism.

Proof. — The claim is local on S so may assume that S is an affine scheme. That $\underline{\mathrm{O_K}}_{\mathrm{S}} \to \underline{\mathrm{End}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E})$ is injective follows from the fact that both $\underline{\mathbf{Z}}_{\mathrm{S}} \subset \underline{\mathrm{O_K}}_{\mathrm{S}}$ and $\underline{\mathbf{Z}}_{\mathrm{S}} \to \underline{\mathrm{End}}_{\mathrm{S}}(\mathrm{E})$ are monomorphisms. By Corollary 1, §4 of [**31**] the map $\underline{\mathrm{O_K}}_{\mathrm{S}} \to \underline{\mathrm{End}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E})$ is an isomorphism when evaluated on any closed point $\mathrm{Spec}(k) \to \mathrm{S}$. Therefore, if $f : \mathrm{E} \to \mathrm{E}$ is any morphism, for each closed point $h : \mathrm{Spec}(k) \to \mathrm{S}$ there is an element $\alpha_h \in \mathrm{O_K}$ such that $(f - [\alpha_h]_{\mathrm{E}})|_{\mathrm{Spec}(k)} = 0$ and by rigidity (2.1.3) there is an open (and closed) neighbourhood $\mathrm{Spec}(k) \to \mathrm{U} \subset \mathrm{S}$ such that $(f - [\alpha_h]_{\mathrm{E}})|_{\mathrm{U}} = 0$. It follows that

$$\underline{\mathrm{O_K}}_{\mathrm{S}} \to \underline{\mathrm{End}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E})$$

is an epimorphism and so is an isomorphism. □

2.2.4 Proposition. — *Let* $\mathrm{E/S}$ *be a* CM *elliptic curve and* $\mathscr{L}/\mathrm{S}$ *a rank one* $\mathrm{O_K}$*-local system. Then* $\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}$ *is a* CM *elliptic curve over* S*.*

Proof. — The claims are all local on S so we may assume that S is an affine scheme. It follows from (A.2.6) that, at least locally on S, $\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}$ is representable by a proper, smooth, geometrically connected group scheme. It follows from (A.2.3) that, when this is the case, the Lie algebra of $\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}$ is locally free of rank one so that the relative dimension of $\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L} \to \mathrm{S}$ is also one. Therefore $\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}$ is, locally on S, an elliptic curve so that it is in fact an elliptic curve over S as the moduli stack of elliptic curves is a stack. Finally, $\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}$ has an obvious structure of an $\underline{\mathrm{O_K}}_{\mathrm{S}}$-module and it follows from (A.2.3) that it is strict. □

2.2.5 Remark. — By (2.2.4) above we find a functor

$$\mathscr{M}_{\mathrm{CM}} \times \mathscr{C}\mathscr{L}_{\mathrm{O_K}} \to \mathscr{M}_{\mathrm{CM}} : (\mathrm{E/S}, \mathscr{L}/\mathrm{S}) \mapsto \mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}/\mathrm{S}$$

which we may view as defining an action of $\mathscr{CL}_{\mathrm{O_K}}$ on $\mathscr{M}_{\mathrm{CM}}$. We will show later (see (2.4.4)) that, as with Lubin–Tate O-modules, this makes $\mathscr{M}_{\mathrm{CM}}$ a torsor under $\mathscr{CL}_{\mathrm{O_K}}$.

2.2.6 Corollary. — *For each pair $\mathscr{L}, \mathscr{L}'$ of rank one $\mathrm{O_K}$-local systems over* S *and each pair* E, E' *of* CM *elliptic curves over* S *the natural map*

$$\underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}') \otimes_{\mathrm{O_K}} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L}, \mathscr{L}') \to \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}, \mathrm{E}' \otimes_{\mathrm{O_K}} \mathscr{L}')$$

is an isomorphism.

Proof. — This follows from (A.2.3). □

2.2.7 Remark. — The isomorphism of (2.2.6) together with (2.2.3) gives the particularly simple formula when $\mathrm{E} = \mathrm{E}'$ and $\mathscr{L} = \underline{\mathrm{O_K}}_{\mathrm{S}}$ and $\mathscr{L}' = \underline{\mathrm{L}}_{\mathrm{S}}$:

$$\underline{\mathrm{L}}_{\mathrm{S}} \xrightarrow{\sim} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E} \otimes_{\mathrm{O_K}} \mathrm{L}) : l \mapsto \mathrm{id}_{\mathrm{E}} \otimes_{\mathrm{O_K}} l.$$

2.2.8. For each integral ideal $\mathfrak{a} \subset \mathrm{O_K}$ we write

$$i_{\mathfrak{a}} : \mathrm{E} \to \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}$$

for the homomorphism induced by the inclusion $\mathrm{O_K} \to \mathfrak{a}^{-1}$. We define the $\mathfrak{a}$-torsion in E to be $\mathrm{E}[\mathfrak{a}] = \ker(i_{\mathfrak{a}})$. We have $\mathrm{E}[\mathfrak{a}] = \cap_{a \in \mathfrak{a}} \ker(a)$ so that $\mathrm{E}[\mathfrak{a}] = \ker(a)$ if $\mathfrak{a} = (a)$ is principal.

2.2.9 Proposition. — *The homomorphism $i_{\mathfrak{a}} : \mathrm{E} \to \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}$ is finite locally free of degree* $\mathrm{N}\mathfrak{a}$.

Proof. — If S is empty or if $\mathfrak{a} = \mathrm{O_K}$ the claim is obvious so we assume that $\mathrm{S} \neq \emptyset$ and that $\mathfrak{a} \neq \mathrm{O_K}$. Using (2.2.7), the morphism $i_{\mathfrak{a}}$ is equal to the zero map only if $\mathrm{S} = \emptyset$, and it is an isomorphism if and only if $\mathfrak{a} = \mathrm{O_K}$ or $\mathrm{S} = \emptyset$. Therefore, as $\mathfrak{a} \neq \mathrm{O_K}$ and $\mathrm{S} \neq \emptyset$, the morphism $i_{\mathfrak{a}}$ is finite locally free of degree greater than one.

As tensoring with rank one $\mathrm{O_K}$-local systems is exact (A.2.2) the kernel of $i_{\mathfrak{a}} \otimes_{\mathrm{O_K}} \mathfrak{b}^{-1}$ is $\mathrm{E}[\mathfrak{a}] \otimes_{\mathrm{O_K}} \mathfrak{b}^{-1}$ and as $\mathrm{O_K}/\mathfrak{a} \otimes_{\mathrm{O_K}} \mathfrak{b}^{-1} \xrightarrow{\sim} \mathrm{O_K}/\mathfrak{a}$ (non-canonically) for all pairs of integral ideals $\mathfrak{a}, \mathfrak{b}$ we have

$$\mathrm{E}[\mathfrak{a}] \otimes_{\mathrm{O_K}} \mathfrak{b}^{-1} \xrightarrow{\sim} \mathrm{E}[\mathfrak{a}].$$

Therefore $\deg(i_{\mathfrak{a}} \otimes_{\mathrm{O_K}} \mathfrak{b}^{-1}) = \deg(i_{\mathfrak{a}})$ and

$$\deg(i_{\mathfrak{a}\mathfrak{b}}) = \deg((i_{\mathfrak{b}} \otimes_{\mathrm{O_K}} \mathfrak{b}^{-1}) \circ i_{\mathfrak{b}}) = \deg(i_{\mathfrak{a}}) \deg(i_{\mathfrak{b}}).$$

As $\mathrm{N}\mathfrak{a}\mathfrak{b} = \mathrm{N}\mathfrak{a}\mathrm{N}\mathfrak{b}$ and $\deg(i_{\mathfrak{a}\mathfrak{b}}) = \deg(i_{\mathfrak{a}}) \deg(i_{\mathfrak{b}})$ we may assume that $\mathfrak{a} = \mathfrak{p}$ is a prime ideal in which case we find

$$\deg(i_{\mathfrak{p}}) \deg(i_{\overline{\mathfrak{p}}}) = \deg(i_{\mathfrak{p}\overline{\mathfrak{p}}}) = \deg([\mathrm{N}\mathfrak{p}]_{\mathrm{E}}) = \mathrm{N}\mathfrak{p}^2.$$

If $\mathfrak{p} = \overline{\mathfrak{p}}$ then $\deg(i_{\mathfrak{p}})^2 = \mathrm{N}\mathfrak{p}^2$ and so $\deg(i_{\mathfrak{p}}) = \mathrm{N}\mathfrak{p}$ and if $\mathfrak{p} \neq \overline{\mathfrak{p}}$ then, as $\mathrm{N}\mathfrak{p}$ is prime and as both $\deg(i_{\mathfrak{p}}), \deg(i_{\overline{\mathfrak{p}}}) \neq 1$, it also follows that $\deg(i_{\mathfrak{p}}) = \mathrm{N}\mathfrak{p}$. □

2.2.10. We associate the following sheaves of groups to E/S:

(i) For each maximal ideal $\mathfrak{p} \subset \mathrm{O_K}$ the $\mathfrak{p}$-divisible group of E is the ind-finite locally free group scheme $\mathrm{E}[\mathfrak{p}^\infty] := \operatorname{colim}_n \mathrm{E}[\mathfrak{p}^n]$. It is a $\lim_n \underline{\mathrm{O_K}/\mathfrak{p}^n}_{\mathrm{S}}$-module.

(ii) The torsion subgroup of E/S is

$$\mathrm{E}[\mathrm{tors}] := \operatorname*{colim}_{\mathfrak{a}} \mathrm{E}[\mathfrak{a}] = \bigoplus_{\mathfrak{p}} \mathrm{E}[\mathfrak{p}^\infty].$$

It is a $\lim_{\mathfrak{a}} \underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{S}}$-module.

(iii) The formal group of E/S is $\widehat{\mathrm{E}} := \operatorname{colim}_k \mathrm{Inf}_{\mathrm{S}}^{(k)}(\mathrm{E})$ (cf. A.1.2). It is a strict formal $\underline{\mathrm{O_K}}_{\mathrm{S}}$-module of dimension one.

2.2.11 Proposition. — *Let* E/S *be a* CM *elliptic curve and* $\mathfrak{p} \subset \mathrm{O_K}$ *a prime ideal. Then*

(i) $\mathfrak{p}$ *is invertible on* S *if and only if* $\mathrm{E}[\mathfrak{p}]$ *is finite and étale over* S. *In this case,* $\mathrm{E}[\mathfrak{p}^\infty]$ *is étale over* S *and is locally isomorphic to the constant* $\lim_n \underline{\mathrm{O_K}/\mathfrak{p}^n}_{\mathrm{S}}$*-module*

$$\operatorname*{colim}_n \underline{\mathfrak{p}^{-n}/\mathrm{O_K}}_{\mathrm{S}} = \underline{\mathrm{K}_{\mathfrak{p}}/\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}}_{\mathrm{S}},$$

and

(ii) $\mathfrak{p}$ *is locally nilpotent on* S *if and only if* $\mathrm{E}[\mathfrak{p}^\infty] = \widehat{\mathrm{E}}$. *In this case,* $\mathrm{E}[\mathfrak{p}^\infty]$ *is a Lubin–Tate* $\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}$*-module over* S.

Proof. — The claims are true if and only if they are locally on S and so we may assume that S is an affine scheme.

(i) As $i_{\mathfrak{p}^n}$ is finite locally free of degree $\mathrm{N}\mathfrak{p}^n$ (in particular, faithfully flat) its kernel $\mathrm{E}[\mathfrak{p}^n]$ is étale over S if and only if the morphism $\mathrm{E} \to \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-n}$ is étale, or equivalently, induces an isomorphism $\underline{\mathrm{Lie}}_{\mathrm{E/S}} \to \underline{\mathrm{Lie}}_{\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{p}^{-1}/\mathrm{S}} = \underline{\mathrm{Lie}}_{\mathrm{E/S}} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1}$ and this is true if and only if $\mathfrak{p}$ is invertible on S.

For the second claim we may, after localising S, assume that $\mathrm{E}[\mathfrak{p}^\infty]$ is constant and hence that $\mathrm{E}[\mathfrak{p}^n]$ is constant for all $n \geq 0$. For each $n \geq 0$ let E_n be a finite $\mathrm{O_K}$-module with $\mathrm{E}[\mathfrak{p}^n] \xrightarrow{\sim} \underline{\mathrm{E}_n}_{\mathrm{S}}$ for $n \geq 0$. For $n \geq 0$, E_n is an $\mathrm{O_K}/\mathfrak{p}^n$-module and the $\mathfrak{p}^n$-torsion of $\operatorname{colim}_n \mathrm{E}_n$ is equal to E_n. As $\#\mathrm{E}_{n+1} = \mathrm{N}\mathfrak{p}^{n+1}$ if E_{n+1} is not a free rank one $\mathrm{O_K}/\mathfrak{p}^{n+1}$-module it must consist of $\mathfrak{p}^n$-torsion and therefore $\mathrm{E}_{n+1} \subset \mathrm{E}_n$ but $\#\mathrm{E}_n = \mathrm{N}\mathfrak{p}^n$ so that this is impossible. It follows that for each $n \geq 0$ the $\mathrm{O_K}/\mathfrak{p}^n$-module E_n is free of rank one and the inclusions $\mathrm{E}_n \to \mathrm{E}_{n+1}$ identify E_n with the $\mathfrak{p}^n$-torsion of E_{n+1}. Therefore, we may fix isomorphisms $\mathrm{E}_n \xrightarrow{\sim} \mathfrak{p}^{-n}/\mathrm{O_K}$ for all $n \geq 0$ with the property that the inclusions $\mathrm{E}_n \subset \mathrm{E}_{n+1}$ become the natural inclusions $\mathfrak{p}^{-n}/\mathrm{O_K} \subset \mathfrak{p}^{-n-1}/\mathrm{O_K}$. Thus

$$\mathrm{E}[\mathfrak{p}^\infty] \xrightarrow{\sim} \operatorname*{colim}_n \underline{\mathfrak{p}^{-n}/\mathrm{O_K}}_{\mathrm{S}}.$$

(ii) First assume that $\widehat{\mathrm{E}} = \mathrm{E}[\mathfrak{p}^\infty]$. Then $\mathrm{S} \to \mathrm{Spec}(\mathrm{O_K})$ factors through

$$\mathrm{Spf}(\mathrm{O_{K_\mathfrak{p}}}) = \operatorname*{colim}_n \mathrm{Spec}(\mathrm{O_K}/\mathfrak{p}^{n+1}) \to \mathrm{Spec}(\mathrm{O_K})$$

if and only if $\mathrm{S} \times \mathrm{Spec}(\mathrm{O_K}[\mathfrak{p}^{-1}]) = \emptyset$. Thus we may assume that $\mathrm{S} = \mathrm{S} \times \mathrm{Spec}(\mathrm{O_K}[\mathfrak{p}^{-1}])$ and show that it is empty. By (i) the sheaf $\widehat{\mathrm{E}} = \mathrm{E}[\mathfrak{p}^\infty]$ is étale over S. In this case it follows that, for all $k \geq 0$, the scheme $\mathrm{Inf}^{(k)}_{\mathrm{S}}(\mathrm{E})$ is unramified over S as it is a sub-scheme of the étale scheme $\widehat{\mathrm{E}} = \mathrm{E}[\mathfrak{p}^\infty]$. Therefore, the morphism defining the zero section $\mathrm{S} \to \mathrm{Inf}^{(k)}_{\mathrm{S}}(\mathrm{E})$ is both a nilpotent immersion and an open immersion which is possible if and only if $\mathrm{S} = \mathrm{Inf}^{(k)}_{\mathrm{S}}(\mathrm{E})$ and this is possible if and only if $\mathrm{S} = \emptyset$.

Conversely, assume that $\mathrm{S} \to \mathrm{Spec}(\mathrm{O_K})$ factors through $\mathrm{Spf}(\mathrm{O_{K_\mathfrak{p}}}) \subset \mathrm{Spec}(\mathrm{O_K})$ and write $\widehat{\mathrm{E}}[\mathfrak{p}^n] = \ker(\widehat{\mathrm{E}} \to \widehat{\mathrm{E}} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-n})$. As S is affine it follows that $\mathfrak{p}$ is nilpotent on S and as the action of $\underline{\mathrm{O_K}}_{\mathrm{S}}$ on $\widehat{\mathrm{E}}$ is strict it follows that

$$\operatorname*{colim}_n \widehat{\mathrm{E}}[\mathfrak{p}^n] = \widehat{\mathrm{E}}$$

(just as in the proof of (ii) of (1.2.5)). In particular, $\widehat{\mathrm{E}} \subset \mathrm{E}[\mathfrak{p}^\infty]$ and the strict $\underline{\mathrm{O_K}}_{\mathrm{S}}$-module structure on $\widehat{\mathrm{E}}$ extends uniquely to a strict $\lim_n \underline{\mathrm{O_K}/\mathfrak{p}^n}_{\mathrm{S}}$-module structure.

We are now reduced to showing that for each $r \geq 0$ the zero section $\mathrm{S} \to \mathrm{E}[\mathfrak{p}^r]$ is a nilpotent immersion as this will give $\mathrm{E}[\mathfrak{p}^r] \subset \widehat{\mathrm{E}}$. As $\mathrm{S} \times \mathrm{Spec}(\mathbf{F}_\mathfrak{p}) \to \mathrm{S}$ is a nilpotent immersion, we may replace S by $\mathrm{S} \times \mathrm{Spec}(\mathbf{F}_\mathfrak{p})$ and assume that S has characteristic $\mathfrak{p}$. From (iii) of (1.2.5) we find closed immersions

$$\ker(\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^r}_{\widehat{\mathrm{E}}/\mathrm{S}}) \subset \widehat{\mathrm{E}}[\mathfrak{p}^r] \subset \mathrm{E}[\mathfrak{p}^r].$$

But, as $\widehat{\mathrm{E}}$ is a smooth formal group of dimension one, $\ker(\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^r}_{\widehat{\mathrm{E}}/\mathrm{S}})$ is finite locally free of rank $\mathrm{N}\mathfrak{p}^r$, as is $\mathrm{E}[\mathfrak{p}^r]$. Therefore the closed immersion

$$\ker(\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^r}_{\widehat{\mathrm{E}}/\mathrm{S}}) \subset \mathrm{E}[\mathfrak{p}^r]$$

is an isomorphism. It follows that $\mathrm{S} \to \mathrm{E}[\mathfrak{p}^r]$ is a nilpotent immersion, so that $\mathrm{E}[\mathfrak{p}^r] \subset \widehat{\mathrm{E}}$, and therefore

$$\widehat{\mathrm{E}} = \mathrm{E}[\mathfrak{p}^\infty].$$

This proves the first claim. For the second, the sheaf of groups $\widehat{\mathrm{E}} = \mathrm{E}[\mathfrak{p}^\infty]$ is a strict formal $\widehat{\mathrm{O_{K_\mathfrak{p}}}_{\mathrm{S}}}$-module of dimension one. Moreover, as $\widehat{\mathrm{E}} = \mathrm{E}[\mathfrak{p}^\infty]$ we have

$$\ker(i_\mathfrak{p} : \widehat{\mathrm{E}} \to \widehat{\mathrm{E}} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1}) = \mathrm{E}[\mathfrak{p}]$$

so that

$$i_\mathfrak{p} : \widehat{\mathrm{E}} \to \widehat{\mathrm{E}} \otimes_{\mathrm{O_{K_\mathfrak{p}}}} \mathfrak{p}^{-1}$$

is finite locally free of degree $\mathrm{N}\mathfrak{p}$. This is precisely the definition of a Lubin–Tate $\mathrm{O_{K_\mathfrak{p}}}$-module (1.2.6). □

2.2.12 Corollary. — *Let* E/S *be a* CM *elliptic curve.*

(i) *The morphism* $\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}[\mathfrak{a}], \underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{S}}) \to \mathrm{S}$ *is affine and étale, factors through* $\mathrm{S}[\mathfrak{a}^{-1}] = \mathrm{S} \times \mathrm{Spec}(\mathrm{O_K}[\mathfrak{a}^{-1}]) \subset \mathrm{S}$ *and defines an affine étale cover*

$$\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}[\mathfrak{a}], \underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{S}}) \to \mathrm{S}[\mathfrak{a}^{-1}].$$

(ii) *If* $\mathrm{P} \subset \mathrm{Id}_{\mathrm{O_K}}$ *is any set of ideals which do not admit a common divisor the family*

$$(\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}[\mathfrak{a}], \underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{S}}) \to \mathrm{S})_{\mathfrak{a}\in\mathrm{P}}$$

is an affine étale cover of S.

Proof. — (i) If there exists an isomorphism $\mathrm{E_T}[\mathfrak{a}] \xrightarrow{\sim} \underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{T}}$ over some affine S-scheme T then $\mathrm{E_T}[\mathfrak{a}]$ is étale, so that by (i) of (2.2.11) the map $\mathrm{T} \to \mathrm{S}$ factors through the affine étale sub-scheme $\mathrm{S}[\mathfrak{a}^{-1}] \subset \mathrm{S}$. It follows that $\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}[\mathfrak{a}], \underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{S}}) \to \mathrm{S}$ factors through $\mathrm{S}[\mathfrak{a}^{-1}]$ and so base changing along $\mathrm{S}[\mathfrak{a}^{-1}] \to \mathrm{S}$ we may assume $\mathfrak{a}$ is invertible on S.

Applying (i) of (2.2.11) to the prime power divisors of $\mathfrak{a}$ we find that $\mathrm{E}[\mathfrak{a}]$ is locally isomorphic to $\underline{\mathfrak{a}^{-1}/\mathrm{O_K}}_{\mathrm{S}}$ which is isomorphic to $\underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{S}}$. This shows that

$$\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}[\mathfrak{a}], \underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{S}}) \to \mathrm{S}$$

is an epimorphism so that by descent, to show that it is finite and étale, we may assume that $\mathrm{E}[\mathfrak{a}] = \underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{S}}$. In this case we have

$$\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{S}}, \underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{S}}) = \underline{(\mathrm{O_K}/\mathfrak{a})^{\times}}_{\mathrm{S}}$$

and the claim is clear.

(ii) The hypothesis on P implies that $(\mathrm{S}[\mathfrak{a}^{-1}] \to \mathrm{S})_{\mathfrak{a}\in\mathrm{P}}$ is a cover of S so that this follows from (i). □

2.2.13 Corollary. — *For each* $n \geq 0$ *there is a unique isomorphism of functors*

$$\nu_{\mathfrak{p}^n} : - \otimes_{\mathrm{O_K}} \mathfrak{p}^{-n} \xrightarrow{\sim} \mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n *}(-)$$

on $\mathscr{M}_{\mathrm{CM}} \times \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}})$ *such that for all* CM *elliptic curves* E *over characteristic* $\mathfrak{p}$*-sheaves* S *the diagram*

$$\begin{array}{ccc} & \mathrm{E} & \\ {\scriptstyle i_{\mathfrak{p}^n}}\swarrow & & \searrow{\scriptstyle \mathrm{Fr}_{\mathrm{E/S}}^{\mathrm{N}\mathfrak{p}^n}} \\ \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-n} & \xrightarrow[\sim]{\nu_{\mathfrak{p}^n}} & \mathrm{Fr}^{\mathrm{N}\mathfrak{p}*}(\mathrm{E}) \end{array}$$

commutes.

Proof. — The two homomorphisms $i_{\mathfrak{p}^n}$ and $\mathrm{Fr}_{\mathrm{E/S}}^{\mathrm{N}\mathfrak{p}^n}$ are finite locally free of degree $\mathrm{N}\mathfrak{p}^n$ so we need only show that their kernels are equal. As $\mathfrak{p}$ is nilpotent on S, we have $\widehat{\mathrm{E}} = \mathrm{E}[\mathfrak{p}^\infty]$ and $\widehat{\mathrm{E}}$ is a Lubin–Tate $\mathrm{O_{K_\mathfrak{p}}}$-module by (ii) of (2.2.11) so that by (1.2.9) we find

$$\ker(\mathrm{Fr}_{\mathrm{E/S}}^{\mathrm{N}\mathfrak{p}^n}) = \ker(\mathrm{Fr}_{\widehat{\mathrm{E}}/\mathrm{S}}^{\mathrm{N}\mathfrak{p}^n}) = \widehat{\mathrm{E}}[\mathfrak{p}^n] = \mathrm{E}[\mathfrak{p}^n] = \ker(i_{\mathfrak{p}^n}).$$

□

2.2.14 Remark. — The above (2.2.13) is the first indication that the moduli stack $\mathscr{M}_{\mathrm{CM}}$ should admit a Λ-structure.

2.2.15 Corollary. — *Let $f : \mathrm{E} \to \mathrm{E}'$ be a homomorphism of* CM *elliptic curves over* S. *Then there is a unique decomposition $\mathrm{S} = \amalg_{\mathfrak{a} \subset \mathrm{O_K}} \mathrm{S}_{(\mathfrak{a})}$ such $f_{\mathrm{S}_{(0)}}$ is the zero map and such that $\ker(f_{\mathrm{S}_{(\mathfrak{a})}}) = \mathrm{E}_{\mathrm{S}_{(\mathfrak{a})}}[\mathfrak{a}]$ for all $(0) \neq \mathfrak{a} \subset \mathrm{O_K}$.*

Proof. — By rigidity we may decompose S as $\mathrm{S}_{(0)} \amalg \mathrm{S}_{\mathrm{isog}}$ where $f_{\mathrm{S}_{(0)}}$ is the zero map and where $f_{\mathrm{S}_{\mathrm{isog}}}$ is finite locally free of positive degree. Thus we may replace S by $\mathrm{S}_{\mathrm{isog}}$ and assume that f is finite locally free. Then $\ker(f) \subset \mathrm{E}[\mathrm{tors}]$ and

$$\ker(f) = \bigoplus_{\mathfrak{p}} \ker(f_{\mathfrak{p}})$$

where $f_{\mathfrak{p}} : \mathrm{E}[\mathfrak{p}^\infty] \to \mathrm{E}'[\mathfrak{p}^\infty]$ is the restriction of f to the $\mathfrak{p}$-divisible groups. As $\ker(f)$ is finite locally free so is $\ker(f_{\mathfrak{p}})$ for all prime ideals $\mathfrak{p}$.

The claim is local so we may reduce to the case where $\mathrm{S} = \mathrm{Spec}(\mathrm{A})$ is an affine scheme and, by passage to the limit, to when S finitely presented over $\mathrm{Spec}(\mathrm{O_K})$. As S is noetherian it admits a finite cover by connected affine schemes and so we may assume that S is connected. In this case, the finite locally free group schemes $\ker(f_{\mathfrak{p}})$ have constant degree and we are reduced to showing that, locally on S, there exists an integer $n \geq 0$ such that $\ker(f_{\mathfrak{p}}) = \mathrm{E}[\mathfrak{p}^n]$.

We continue to localise S and so assume that $\mathrm{S} = \mathrm{Spec}(\mathrm{A})$ for A a local noetherian ring with maximal ideal I and by descent that A is I-adically complete. As E and $\mathrm{E}[\mathfrak{p}^n]$ and $\ker(\mathfrak{f}_{\mathfrak{p}})$ are all proper over S to check that $\ker(f_{\mathfrak{p}}) = \mathrm{E}[\mathfrak{p}^n]$ for some n we may, by Grothendieck's formal GAGA, replace S by $\mathrm{Spec}(\mathrm{A}/\mathrm{I}^r)$ for each $r \geq 0$ and assume that $\mathrm{S} = \mathrm{Spec}(\mathrm{A})$ where A is an artinian local ring. If $\mathfrak{p}$ is invertible in A then $\mathrm{E}[\mathfrak{p}^\infty]$ is locally isomorphic to the constant group scheme

$$\underline{\mathrm{K}_{\mathfrak{p}}/\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}}_{\mathrm{S}}$$

by (2.2.11), from this and the corresponding fact for $\mathrm{K}_{\mathfrak{p}}/\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}$, we see that any finite locally free $\underline{\mathrm{O}_{\mathrm{K}}}_{\mathrm{S}}$-sub-module of $\mathrm{E}[\mathfrak{p}^\infty]$ is of the form $\mathrm{E}[\mathfrak{p}^n]$ for some $n \geq 0$. On the other hand, if $\mathfrak{p}$ is nilpotent in A, then $\ker(f_{\mathfrak{p}})$ is the kernel of the homomorphism $f_{\mathfrak{p}} : \mathrm{E}[\mathfrak{p}^\infty] \to \mathrm{E}'[\mathfrak{p}^\infty]$ of Lubin–Tate $\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}$-modules and so the claim follows from (1.2.18). □

2.3. Complex and $\mathfrak{p}$-adic bases

In this section we give CM analogues of the classification of elliptic curves over complex schemes in terms of lattices, and of the Serre-Tate theorem. We use this to show there exists a CM elliptic curve $\mathrm{E} \to \mathrm{Spec}(\mathrm{O}_{\mathrm{K}^{\mathrm{sep}}})$ (2.3.3),

that deformations of CM elliptic curves over $\mathfrak{p}$-adic bases always exist and are unique (2.3.6).

2.3.1. Let us first consider complex bases. We fix a homomorphism $\mathrm{O_K} \to \mathbf{C}$ so that we may view $\mathrm{Spec}(\mathbf{C})$ as a $\mathrm{Spec}(\mathrm{O_K})$-scheme. Let S be a locally finitely presented $\mathrm{Spec}(\mathbf{C})$-scheme and E/S a CM elliptic curve. Consider the exponential sequence associated to the analytification $\mathrm{E^{an}/S^{an}}$ (cf. (2.1.10))

$$0 \to \mathrm{T_{\mathbf{Z}}(E/S)} \to \underline{\mathrm{Lie}}_{\mathrm{E^{an}/S^{an}}} \to \mathrm{E^{an}} \to 0.$$

The strictness of the $\underline{\mathrm{O_K}}_{\mathrm{S}}$-action on E implies that the homomorphism

$$\underline{\mathrm{Lie}}_{\mathrm{E^{an}/S^{an}}} \to \mathrm{E^{an}}$$

is a homomorphism of $\underline{\mathrm{O_K}}_{\mathrm{S^{an}}}$-modules. This makes the rank two $\underline{\mathbf{Z}}_{\mathrm{S^{an}}}$-local system $\mathrm{T_{\mathbf{Z}}(E/S)}$ a rank one $\mathrm{O_K}$-local system, which we shall denote by $\mathrm{T_{O_K}(E/S)}$, and the homomorphism

$$\mathrm{T_{O_K}(E/S)} \otimes_{\underline{\mathrm{O_K}}_{\mathrm{S^{an}}}} \mathscr{O}_{\mathrm{S^{an}}} \to \underline{\mathrm{Lie}}_{\mathrm{E^{an}/S^{an}}}$$

is now an isomorphism. As the automorphism sheaf of any rank one $\mathrm{O_K}$-local system over S or $\mathrm{S^{an}}$ is just the constant sheaf associated to the finite group $\mathrm{O_K^\times}$ (from which one sees that every $\mathrm{O_K}$-local system over S or $\mathrm{S^{an}}$ is just a sum of finite étale S-schemes, or finite covering spaces of $\mathrm{S^{an}}$) by GAGA the functor sending a rank one $\mathrm{O_K}$-local system on S to the corresponding rank one $\mathrm{O_K}$-local system on $\mathrm{S^{an}}$ is an equivalence. Therefore:

2.3.2 Proposition. — *The functor*

$$\mathrm{E/S} \mapsto \mathrm{T_{O_K}(E/S)}$$

is an equivalence between the category of CM *elliptic curves* E/S *and the rank one* $\mathrm{O_K}$*-local systems over* S*.*

Proof. — This follows from (2.1.11) and the remarks above. □

2.3.3 Corollary. — *There exists a* CM *elliptic curve* E *over* $\mathrm{Spec}(\mathrm{O_{K^{sep}}})$*.*

Proof. — By (2.3.2) we see that there exists a CM elliptic curve $\mathrm{E/Spec}(\mathbf{C})$. Writing $\mathrm{Spec}(\mathbf{C}) = \lim_\lambda \mathrm{Spec}(\mathrm{A}_\lambda)$ as a filtered inverse limit of finite type affine Spec(K)-schemes by passage to the limit we find a CM elliptic curve $\mathrm{E}_\lambda/\mathrm{Spec}(\mathrm{A}_\lambda)$ for some λ. As $\mathrm{Spec}(\mathrm{A}_\lambda)$ is of finite type over Spec(K) it admits a closed point $\mathrm{Spec(L)} \to \mathrm{Spec}(\mathrm{A}_\lambda)$ with L/K finite and we find a CM elliptic curve $\mathrm{E}_\lambda \times_{\mathrm{Spec}(\mathrm{A}_\lambda)} \mathrm{Spec(L)}$ over Spec(L).

We now show (essentially following the arguments of [**31**] only for the sake of completeness) that for any CM elliptic curve $\mathrm{E} \to \mathrm{Spec(L)}$ over a finite extension L/K there is a finite extension L′/L such that $\mathrm{E} \times_{\mathrm{Spec(L)}} \mathrm{Spec}(\mathrm{L}')$ has good reduction everywhere. As E has bad reduction at only finitely many primes, it is enough to show that for each prime $\mathfrak{p}$ of L there is a finite extension L′/L such that $\mathrm{E} \times_{\mathrm{Spec(L)}} \mathrm{Spec}(\mathrm{L}')$ admits good reduction at all primes of L′

over $\mathfrak{p}$, as then E will obtain good reduction over the compositum of these finitely many fields.

So fix a prime $\mathfrak{p}$ lying over the rational prime p and let $\ell \neq p$ be another rational prime. Let $\rho_\ell : \mathrm{G}(\mathrm{L}^{\mathrm{sep}}/\mathrm{L})^{\mathrm{ab}} = \mathrm{G}(\mathrm{L}^{\mathrm{ab}}/\mathrm{L}) \to (\mathrm{O_K} \otimes_{\mathbf{Z}} \mathbf{Z}_\ell)^\times$ be the character defining the $\mathrm{O_K} \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$-linear action of $\mathrm{G}(\mathrm{L}^{\mathrm{sep}}/\mathrm{L})$ on

$$\mathrm{E}[\ell^\infty](\mathrm{Spec}(\mathrm{L}^{\mathrm{sep}})) \xrightarrow{\sim} \mathrm{O_K} \otimes_{\mathbf{Z}} \mathbf{Q}_\ell/\mathbf{Z}_\ell.$$

First we claim that for each place v of $\mathrm{L}^{\mathrm{sep}}$ lying over $\mathfrak{p}$ the restriction of ρ_ℓ to the inertia group $\mathrm{I}_v \subset \mathrm{G}(\mathrm{L}^{\mathrm{sep}}/\mathrm{L})$ at v has finite image and that this image is independent of v. As the target of ρ_ℓ is commutative and as the image of $\mathrm{I}_v(\mathrm{L}^{\mathrm{sep}}/\mathrm{L})$ in $\mathrm{G}(\mathrm{L}^{\mathrm{sep}}/\mathrm{L}) = \mathrm{G}(\mathrm{L}^{\mathrm{ab}}/\mathrm{L})$ is the inertia subgroup $\mathrm{I}_\mathfrak{p} \subset \mathrm{G}(\mathrm{L}^{\mathrm{ab}}/\mathrm{L})$ at $\mathfrak{p}$, which is independent of v, it is enough to show that $\rho_\ell(\mathrm{I}_\mathfrak{p})$ is finite. But it is well known that $\mathrm{I}_\mathfrak{p}$ admits an open subgroup of finite index which is pro-p and that $(\mathrm{O_K} \otimes_{\mathbf{Z}} \mathbf{Z}_\ell)^\times$ admits an open subgroup of finite index which is pro-ℓ. Therefore, as ρ_ℓ is continuous and $\ell \neq p$ the image of the inertia group $\rho_\ell(\mathrm{I}_\mathfrak{p})$ must be finite. It now follows that there is an integer $n \geq 0$ with the property that

$$\rho_\ell(\mathrm{I}_\mathfrak{p}) \to (\mathrm{O_K} \otimes_{\mathbf{Z}} \mathbf{Z}_\ell)^\times \to (\mathrm{O_K} \otimes_{\mathbf{Z}} \mathbf{Z}/\ell^n)^\times$$

is injective. Taking $\mathrm{L}' = \mathrm{L}(\mathrm{E}[\ell^n])$, the action of the inertia group $\mathrm{I}_v(\mathrm{L}^{\mathrm{sep}}/\mathrm{L}') \subset \mathrm{G}(\mathrm{L}^{\mathrm{sep}}/\mathrm{L}')$ at any place v lying over $\mathfrak{p}$ on $\mathrm{E}'[\ell^\infty](\mathrm{Spec}(\mathrm{L}^{\mathrm{sep}})) = \mathrm{E}'[\ell^\infty](\mathrm{Spec}(\mathrm{L}^{\mathrm{sep}}))$ is trivial and we now apply (2.1.16) to deduce that $\mathrm{E}'/\mathrm{Spec}(\mathrm{L}')$ has good reduction at all places of L' lying over $\mathfrak{p}$. □

2.3.4. Now let us consider $\mathfrak{p}$-adic bases. Fix a prime ideal $\mathfrak{p}$ of $\mathrm{O_K}$ and let $\mathrm{S}_0 \to \mathrm{S}$ be a nilpotent thickening of $\mathfrak{p}$-adic sheaves and denote by $\mathrm{D}_\mathfrak{p}(\mathrm{S}, \mathrm{S}_0)$ the category whose objects are triples $(\mathrm{E}_0/\mathrm{S}_0, \mathrm{F}/\mathrm{S}, \rho)$ where

(i) E/S_0 is a CM elliptic curve,
(ii) F/S is a Lubin–Tate $\mathrm{O}_{\mathrm{K}_\mathfrak{p}}$-module, and
(iii) $\rho : \mathrm{F} \times_{\mathrm{S}} \mathrm{S}_0 \xrightarrow{\sim} \mathrm{E}[\mathfrak{p}^\infty]$ is an isomorphism of Lubin–Tate $\mathrm{O}_{\mathrm{K}_\mathfrak{p}}$-modules,

and whose morphisms $(\mathrm{E}_0/\mathrm{S}_0, \mathrm{F}/\mathrm{S}, \rho) \to (\mathrm{E}'_0/\mathrm{S}_0, \mathrm{F}'/\mathrm{S}, \rho')$ are given by pairs $(g_0, g_\mathfrak{p})$ where $g_0 : \mathrm{E}_0 \to \mathrm{E}'_0$ is a homomorphism of CM elliptic curves, $g_\mathfrak{p} : \mathrm{F} \to \mathrm{F}'$ is a homomorphism of Lubin–Tate $\mathrm{O}_{\mathrm{K}_\mathfrak{p}}$-modules such that $\rho' \circ (g_\mathfrak{p} \times_{\mathrm{S}} \mathrm{S}_0) = (g_0|_{\mathrm{E}[\mathfrak{p}^\infty]}) \circ \rho$. There is an obvious functor

$$\mathrm{CM}(\mathrm{S}) \to \mathrm{D}_\mathfrak{p}(\mathrm{S}_0, \mathrm{S}) : \mathrm{E}/\mathrm{S} \mapsto (\mathrm{E} \times_{\mathrm{S}} \mathrm{S}_0, \mathrm{E}[\mathfrak{p}^\infty], \mathrm{id}_{\mathrm{E}[\mathfrak{p}^\infty] \times_{\mathrm{S}} \mathrm{S}_0}).$$

The following is the theorem of Serre-Tate (2.1.13) adapted for CM elliptic curves.

2.3.5 Proposition. — *The functor* $\mathrm{CM}(\mathrm{S}) \to \mathrm{D}_\mathfrak{p}(\mathrm{S}_0, \mathrm{S})$ *is an equivalence of categories.*

Proof. — Let p be the rational prime lying under $\mathfrak{p}$. We will show that to each object $(\mathrm{E}_0/\mathrm{S}_0, \mathrm{F}/\mathrm{S}, \rho)$ of $\mathrm{D}_\mathfrak{p}(\mathrm{S}_0, \mathrm{S})$ (resp. morphism) one can functorially define a element of $\mathrm{D}_p(\mathrm{S}_0, \mathrm{S})$ (resp. morphism) (cf. (2.1.12)). If $\overline{\mathfrak{p}} = \mathfrak{p}$

then this is clear as $\mathrm{E}_0[\mathfrak{p}^\infty] = \mathrm{E}[p^\infty]$. On the other hand if $\overline{\mathfrak{p}} \neq \mathfrak{p}$ then $\mathrm{E}_0[p^\infty] = \mathrm{E}_0[\mathfrak{p}^\infty] \times_{\mathrm{S}_0} \mathrm{E}_0[\overline{\mathfrak{p}}^\infty]$ and $\mathrm{E}_0[\overline{\mathfrak{p}}^\infty]$ is étale over S_0 so that there is a unique deformation of $\mathrm{E}_0[\overline{\mathfrak{p}}^\infty]$ along $\mathrm{S}_0 \to \mathrm{S}$ and the product over S of this deformation with F will give the desired deformation of $\mathrm{E}_0[p^\infty]$. Regarding morphisms $(g_0, g_\mathfrak{p})$ the restriction $g_0|_{\mathrm{E}[\overline{\mathfrak{p}}^\infty]}$ lifts uniquely and the product of this with $g_\mathfrak{p}$ defines the map on morphisms.

In both cases this defines a functor $\mathrm{D}_\mathfrak{p}(\mathrm{S}_0, \mathrm{S}) \to \mathrm{D}_p(\mathrm{S}_0, \mathrm{S})$ and by the classical Serre-Tate theorem a functor $\mathrm{D}_\mathfrak{p}(\mathrm{S}_0, \mathrm{S}) \to \mathrm{Ell}(\mathrm{S})$. By functoriality, if E/S is the image of $(\mathrm{E}_0/\mathrm{S}_0, \mathrm{F}/\mathrm{S}, \rho)$ then E/S admits the structure of an $\underline{\mathrm{O}_{\mathrm{K}_\mathrm{S}}}$-module (deforming the corresponding structure on $\mathrm{E}_0/\mathrm{S}_0$). Moreover, the action of $\underline{\mathrm{O}_{\mathrm{K}_\mathrm{S}}}$ on the Lie algebra of E/S is strict as we have identifications of $\underline{\mathrm{O}_{\mathrm{K}_\mathrm{S}}}$-modules

$$\underline{\mathrm{Lie}}_{\mathrm{E}/\mathrm{S}} = \underline{\mathrm{Lie}}_{\mathrm{E}[p^\infty]/\mathrm{S}} = \underline{\mathrm{Lie}}_{\mathrm{E}[\mathfrak{p}^\infty]/\mathrm{S}} = \underline{\mathrm{Lie}}_{\mathrm{F}/\mathrm{S}}$$

and the action of $\underline{\mathrm{O}_{\mathrm{K}_\mathrm{S}}}$ on F is strict. In particular, the functor $\mathrm{D}_\mathfrak{p}(\mathrm{S}_0, \mathrm{S}) \to \mathrm{Ell}(\mathrm{S})$ factors as

$$\mathrm{D}_\mathfrak{p}(\mathrm{S}_0, \mathrm{S}) \to \mathrm{CM}(\mathrm{S})$$

and it is easily seen to be quasi-inverse to $\mathrm{CM}(\mathrm{S}) \to \mathrm{D}_\mathfrak{p}(\mathrm{S}_0, \mathrm{S})$. □

2.3.6 Corollary. — *If* $\mathrm{S}_0 \to \mathrm{S}$ *is a nilpotent immersion of* $\mathfrak{p}$*-adic sheaves the functor*

$$\mathrm{CM}(\mathrm{S}) \to \mathrm{CM}(\mathrm{S}_0) : \mathrm{E}/\mathrm{S} \mapsto \mathrm{E} \times_\mathrm{S} \mathrm{S}_0/\mathrm{S}_0$$

is an equivalence of categories.

Proof. — This follows from (2.3.5) combined with (1.2.17). □

2.3.7 Corollary. — *Let* S *be a* $\mathfrak{p}$*-adic affine scheme and let* E/S *be a* CM *elliptic curve. Then there exists a affine scheme* $\widetilde{\mathrm{S}}$*, flat over* $\mathrm{Spec}(\mathrm{O}_\mathrm{K})$*, a morphism* $\mathrm{S} \to \widetilde{\mathrm{S}}$*, and a* CM *elliptic curve* $\widetilde{\mathrm{E}}/\widetilde{\mathrm{S}}$ *such that* $\widetilde{\mathrm{E}} \times_{\widetilde{\mathrm{S}}} \mathrm{S} \xrightarrow{\sim} \mathrm{E}$.

Proof. — By passage to the limit we may assume that $\mathrm{S} = \mathrm{Spec}(\mathrm{A})$ with A a finite type O_K-algebra. We then choose a surjection $\mathrm{A}' \to \mathrm{A}$ where A' is a flat O_K-algebra. Letting I be the kernel of $\mathrm{A}' \to \mathrm{A}$ we write $\widetilde{\mathrm{S}} = \mathrm{Spec}(\lim_n \mathrm{A}'/\mathrm{I}^n) = \mathrm{Spec}(\widehat{\mathrm{A}}')$, $\widetilde{\mathrm{S}}_n = \mathrm{Spec}(\mathrm{A}'/\mathrm{I}^n)$ and $\widetilde{\mathrm{S}}_\infty = \mathrm{colim}_n \mathrm{Spec}(\mathrm{A}'/\mathrm{I}^n)$. We will show that there exists a CM elliptic curve $\widetilde{\mathrm{E}}/\widetilde{\mathrm{S}}$ with $\widetilde{\mathrm{E}} \times_{\widetilde{\mathrm{S}}} \mathrm{S} \xrightarrow{\sim} \mathrm{E}$ which, as $\widetilde{\mathrm{S}} = \mathrm{Spec}(\widehat{\mathrm{A}}')$ is flat over $\mathrm{Spec}(\mathrm{O}_\mathrm{K})$, will prove the claim.

For each $n \geq 0$ there is a unique $\widetilde{\mathrm{E}}_n/\widetilde{\mathrm{S}}_n$ equipped with an isomorphism $\widetilde{\mathrm{E}}_n \times_{\widetilde{\mathrm{S}}_n} \mathrm{S} \xrightarrow{\sim} \mathrm{E}$ by (2.3.6). Therefore there is a unique CM elliptic curve $\widetilde{\mathrm{E}}_\infty$ over the ind-scheme $\widetilde{\mathrm{S}}_\infty = \mathrm{colim}_n \widetilde{\mathrm{S}}_n$ with $\widetilde{\mathrm{E}}_\infty \times_{\widetilde{\mathrm{S}}_\infty} \mathrm{S} = \mathrm{E}$. By (2.1.8) there is a unique elliptic curve $\widetilde{\mathrm{E}}$ over $\widetilde{\mathrm{S}} = \mathrm{Spec}(\widehat{\mathrm{A}}')$ with $\widetilde{\mathrm{E}} \times_{\widetilde{\mathrm{S}}} \mathrm{S} = \mathrm{E}$ and moreover it admits an action of $\underline{\mathrm{O}_{\mathrm{K}_\mathrm{S}}}$ compatible with that on $\widetilde{\mathrm{E}}_n$ over $\widetilde{\mathrm{S}}_n$ which (taking n large) shows that the action is strict so that $\widetilde{\mathrm{E}}/\widetilde{\mathrm{S}}$ is a CM elliptic curve. □

2.4. Isogenies and the action of $\mathscr{CL}_{\mathrm{O_K}}$ on $\mathscr{M}_{\mathrm{CM}}$

In this section we continue the study of the action of $\mathscr{CL}_{\mathrm{O_K}}$ on $\mathscr{M}_{\mathrm{CM}}$. We show that all pairs of CM elliptic curves over a fixed base are locally isogenous (2.4.1) and from this deduce that the action of $\mathscr{CL}_{\mathrm{O_K}}$ on $\mathscr{M}_{\mathrm{CM}}$ makes it a torsor (2.4.4).

2.4.1 Lemma. — *Let* $\mathrm{E}, \mathrm{E}'/\mathrm{S}$ *be a pair of* CM *elliptic curves. Then the family*

$$(\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}' \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}) \to \mathrm{S})_{\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}}$$

is a finite étale cover of S.

Proof. — The claim is local so we may assume that S is an affine scheme and by passage to the limit that S is finitely presented over $\mathrm{Spec}(\mathrm{O_K})$. For every pair of CM elliptic curves $\mathrm{E}, \mathrm{E}'/\mathrm{S}$ the inclusion

$$\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}') \to \underline{\mathrm{Isom}}_{\mathrm{S}}(\mathrm{E}, \mathrm{E}')$$

is easily seen to be a closed immersion and so it follows from (2.1.7) that $\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}') \to \mathrm{S}$ is finite and unramified. Therefore, for each integral ideal $\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}$ the sheaf $\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}' \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1})$ is finite and unramified over S. It follows from (2.3.6) that the maximal open sub-scheme of $\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}' \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1})$ which is étale over S contains all of the special fibres and is therefore equal to all of $\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}' \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1})$. As the morphisms $(\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}' \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}) \to \mathrm{S})_{\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}}$ are finite étale this family forms a cover of S if and only if it is a cover after base change to each generic point of S. So we way assume that S is either flat over $\mathrm{Spec}(\mathrm{O_K})$ (if a generic point has characteristic 0) or that S is $\mathfrak{p}$-adic for some prime $\mathfrak{p}$ (if a generic point has characteristic $\mathfrak{p}$). Let us reduce the second case to the first and assume that S is $\mathfrak{p}$-adic.

Applying (2.3.7) to E and E′, then taking the product of the flat $\mathrm{Spec}(\mathrm{O_K})$-schemes over which E and E′ can be extended, we find a flat $\mathrm{Spec}(\mathrm{O_K})$-scheme $\widetilde{\mathrm{S}}$, a morphism $\mathrm{S} \to \widetilde{\mathrm{S}}$ and a pair of CM elliptic curves $\widetilde{\mathrm{E}}$ and $\widetilde{\mathrm{E}}'$ over $\widetilde{\mathrm{S}}$ whose pull-backs to S are isomorphic to E and E′. We now see that the claim we wish to prove is true for $\mathrm{E}, \mathrm{E}'/\mathrm{S}$ if it is true for $\widetilde{\mathrm{E}}, \widetilde{\mathrm{E}}'/\widetilde{\mathrm{S}}$. As the generic points of $\widetilde{\mathrm{S}}$ are all of characteristic 0, we have reduced the second case to the first and we may assume that $\mathrm{S} = \mathrm{Spec}(\mathrm{F})$ where F is a field of characteristic 0.

By passage to the limit we may assume that F has finite transcendence degree over K, that there is a morphism $\mathrm{F} \to \mathbf{C}$ and by base change that $\mathrm{F} = \mathbf{C}$. The claim now follows from (2.3.2), the fact that all $\mathrm{O_K}$-local systems over $\mathrm{Spec}(\mathbf{C})$ are constant, and the fact that if L and L′ are two rank one $\mathrm{O_K}$-modules there always exists some $\mathfrak{a} \subset \mathrm{O_K}$ and an isomorphism $\mathrm{L}' \xrightarrow{\sim} \mathrm{L} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}$. □

2.4.2 Proposition. — *For each pair* $\mathrm{E}, \mathrm{E}'/\mathrm{S}$ *of* CM *elliptic curves over* S *the sheaf* $\underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}')$ *is a rank one* $\mathrm{O_K}$*-local system and the evaluation*

homomorphism

$$\mathrm{E} \otimes_{\mathrm{O_K}} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}') \to \mathrm{E}'$$

is an isomorphism.

Proof. — The claim is local and by (2.4.1) the set of S-sheaves

$$(\underline{\mathrm{Isom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}' \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}) \to \mathrm{S})_{\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}}$$

is a finite étale cover, so replacing S with any one of them we may assume that $\mathrm{E}' = \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}$ for some integral ideal $\mathfrak{a}$. Composing the evaluation homomorphism with $\mathrm{id}_{\mathrm{E}} \otimes_{\mathrm{O_K}} i$, where $i : \underline{\mathfrak{a}}_{\mathrm{S}}^{-1} \xrightarrow{\sim} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1})$ is the isomorphism of (2.2.6), the resulting map

$$\mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \xrightarrow{\sim} \mathrm{E} \otimes_{\mathrm{O_K}} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}) \to \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}$$

is an isomorphism (in particular it is the identity) and so the second map is an isomorphism and we are done. □

2.4.3 Corollary. — *Let* $\mathrm{E}, \mathrm{E}'/\mathrm{S}$ *be a pair of* CM *elliptic curves. Then* E *and* E' *are isomorphic if and only if they are isogenous and locally isomorphic.*

Proof. — The only if direction is clear. Conversely, let $f : \mathrm{E} \to \mathrm{E}'$ be an isogeny and assume that E and E' are locally isomorphic. As the cover $\amalg_{\mathfrak{a} \subset \mathrm{O_K}} \mathrm{S}_{(\mathfrak{a})} = \mathrm{S}$ in (2.2.15) is by open and closed sub-sheaves, E and E' are isomorphic over S if and only if they are after base change to each $\mathrm{S}_{(\mathfrak{a})}$. Therefore we may assume that $\ker(f) = \mathrm{E}[\mathfrak{a}] = \ker(i_{\mathfrak{a}})$, so that f factors as $\mathrm{E} \to \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \xrightarrow{\sim} \mathrm{E}'$. Now as E and $\mathrm{E}' \xrightarrow{\sim} \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}$ are locally isomorphic it follows that $\underline{\mathrm{O_K}}_{\mathrm{S}}$ and $\underline{\mathfrak{a}^{-1}}_{\mathrm{S}}$ are locally isomorphic. Any such and isomorphism is locally constant from which it follows that there exists an isomorphism $\mathfrak{a}^{-1} \xrightarrow{\sim} \mathrm{O_K}$ and we get

$$\mathrm{E}' \xrightarrow{\sim} \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \xrightarrow{\sim} \mathrm{E}.$$

□

2.4.4 Theorem. — *The functor*

$$\mathscr{M}_{\mathrm{CM}} \times \mathscr{C}\mathscr{L}_{\mathrm{O_K}} \to \mathscr{M}_{\mathrm{CM}} \times \mathscr{M}_{\mathrm{CM}} : (\mathrm{E}, \mathscr{L}) \mapsto (\mathrm{E}, \mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L})$$

is an equivalence of stacks and $\mathscr{M}_{\mathrm{CM}}$ *is locally (over* $\mathrm{Spec}(\mathrm{O_K})$*) equivalent to* $\mathscr{C}\mathscr{L}_{\mathrm{O_K}}$*.*

Proof. — The functor in question is essentially surjective as, given any pair $(\mathrm{E}/\mathrm{S}, \mathrm{E}'/\mathrm{S}) \in \mathscr{M}_{\mathrm{CM}}(\mathrm{S}) \times \mathscr{M}_{\mathrm{CM}}(\mathrm{S})$, by (2.4.2) we have

$$(\mathrm{E}/\mathrm{S}, \mathrm{E}'/\mathrm{S}) \xrightarrow{\sim} (\mathrm{E}/\mathrm{S}, \mathrm{E} \otimes_{\mathrm{O_K}} \underline{\mathrm{Hom}}_{\mathrm{S}}(\mathrm{E}, \mathrm{E}')/\mathrm{S}).$$

Full faithfulness is the bijectivity of the map

$$\mathrm{Isom}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}') \times \mathrm{Isom}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L}, \mathscr{L}') \to \mathrm{Isom}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}') \times \mathrm{Isom}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}, \mathrm{E}' \otimes_{\mathrm{O_K}} \mathscr{L}').$$

If $\mathrm{Isom}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E},\mathrm{E}') = \emptyset$ this is clear. If $\mathrm{Isom}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E},\mathrm{E}') \neq \emptyset$ we may assume that $\mathrm{E} = \mathrm{E}'$ and instead show that

$$\mathrm{Isom}_{\mathrm{S}}^{\mathrm{O_K}}(\mathscr{L},\mathscr{L}') \to \mathrm{Isom}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}\otimes_{\mathrm{O_K}}\mathscr{L},\mathrm{E}\otimes_{\mathrm{O_K}}\mathscr{L}')$$

is bijective but this follows from (2.2.6).

For the second statement, if $\mathrm{E}/\mathrm{Spec}(\mathrm{O}_{\mathrm{K}}^{\mathrm{sep}})$ is any CM elliptic curve (2.3.3) the functor

$$\mathscr{CL}_{\mathrm{O_K}} \times \mathrm{Spec}(\mathrm{O}_{\mathrm{K}^{\mathrm{sep}}}) \to \mathscr{M}_{\mathrm{CM}} \times \mathrm{Spec}(\mathrm{O}_{\mathrm{K}^{\mathrm{sep}}})$$

sending a rank one $\mathrm{O_K}$-local system $\mathscr{L}$ over a $\mathrm{Spec}(\mathrm{O}_{\mathrm{K}}^{\mathrm{sep}})$-sheaf $p : \mathrm{S} \to \mathrm{Spec}(\mathrm{O}_{\mathrm{K}^{\mathrm{sep}}})$ to $p^*(\mathrm{E})\otimes_{\mathrm{O_K}}\mathscr{L}$ is the desired local equivalence. □

2.4.5 Remark. — One might ask whether, as in the analogous situation of Lubin–Tate O-modules (1.2.16), there exists a CM elliptic curve over $\mathscr{E}/\mathrm{Spec}(\mathrm{O_K})$ inducing a trivialisation of the $\mathscr{CL}_{\mathrm{O_K}}$-torsor $\mathscr{M}_{\mathrm{CM}}$, i.e. an equivalence of stacks:

$$\mathscr{CL}_{\mathrm{O_K}} \xrightarrow{\sim} \mathscr{M}_{\mathrm{CM}} : \mathscr{L}/\mathrm{S} \mapsto \mathrm{E_S}\otimes_{\mathrm{O_K}}\mathscr{L}/\mathrm{S}$$

We shall show later (see (4.2.5)) that in general this is not the case (and for non-trivial reasons).

2.4.6 Corollary. — *Let* E *and* E′ *be a pair of* CM *elliptic curves over* S *and assume that* $\mathfrak{a}$ *is invertible on* S. *Then the homomorphism*

$$\underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E},\mathrm{E}') \to \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}[\mathfrak{a}],\mathrm{E}'[\mathfrak{a}])$$

is an epimorphism.

Proof. — We may work locally on S and so assume that $\mathrm{E}' \xrightarrow{\sim} \mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{b}^{-1}$. We may find a $k \in \mathrm{K}^\times$ such that $\mathfrak{b}(k)$ is prime to $\mathfrak{a}$ and using the isomorphism $k : \mathfrak{b} \xrightarrow{\sim} \mathfrak{b}(k)$ we may assume $\mathfrak{b}$ is prime to $\mathfrak{a}$. In this case, the restriction of $i_{\mathfrak{b}}$ to the $\mathfrak{a}$-torsion defines an isomorphism $\mathrm{E}[\mathfrak{a}] \xrightarrow{\sim} \mathrm{E}[\mathfrak{a}]\otimes_{\mathrm{O_K}}\mathfrak{b}^{-1}$ which, as $\mathrm{E}[\mathfrak{a}]$ and $\mathrm{E}[\mathfrak{a}]\otimes_{\mathrm{O_K}}\mathfrak{b}^{-1}$ are locally isomorphic to $\underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{S}}$, induces an isomorphism

$$\underline{\mathrm{O_K}/\mathfrak{a}}_{\mathrm{S}} \xrightarrow{\sim} \underline{\mathrm{Hom}}_{\mathrm{S}}(\mathrm{E}[\mathfrak{a}],\mathrm{E}[\mathfrak{a}]\otimes_{\mathrm{O_K}}\mathfrak{b}^{-1}) : a \mapsto a\cdot i_{\mathfrak{b}}$$

and it follows that

$$\underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E},\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{b}^{-1}) \to \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}[\mathfrak{a}],\mathrm{E}[\mathfrak{a}]\otimes_{\mathrm{O_K}}\mathfrak{b}^{-1})$$

is an epimorphism as the image contains $i_{\mathfrak{b}}$. □

2.5. The global reciprocity map and CM elliptic curves

We now consider CM elliptic curves over Spec(F) where F is a field of arbitrary characteristic. First, we define a homomorphism $[-]_F$ from the Galois group $G(F^{sep}/F)$ into a certain class group (which depends only on the characteristic of the field F) (2.5.1). We then prove a relation between this homomorphism $[-]_F$ and the character $\rho_{E/F}$ defining the action of $G(F^{sep}/F)$ on the torsion of a CM elliptic curve E/Spec(F) (2.5.4). Moreover, we show the character $\rho_{E/F}$ determines E/Spec(F) upto isogeny (2.5.7) and we use the homomorphism $[-]_F$ to classify exactly which characters ρ of $G(F^{sep}/F)$ are of the form $\rho_{E/F}$ for some CM elliptic curve E/Spec(F) (2.5.8). In (2.5.9) we compute the homomorphisms $[-]_F$ when $F = K$, $F = K_{\mathfrak{p}}$ and $F = \mathbf{F}_{\mathfrak{p}}$ for $\mathfrak{p}$ a prime. In particular, for $F = K$ the homomorphism $[-]_K$ takes the form

$$[-]_K : G(K^{sep}/K) \to CL_{O_K,\infty}$$

and we show that for $\sigma \in G(K^{sep}/K)$ we have

$$\theta_K([\sigma]_K) = \sigma|_{K^\infty} \tag{2.5.0.1}$$

where $\theta_K : CL_{O_K,\infty} \to G(K^\infty/K)$ is reciprocity map (1.4.7.2). This fact is, at least in spirit, equivalent to the main theorem of complex multiplication (see Theorem 5.4 of [**33**]). The method we use to derive this fact is quite similar to (and in fact reliant on) the method used to prove (1.2.20) for Lubin–Tate O-modules in Chapter 1. Finally, we use these results to derive a sharpening of the criterion of good reduction adapted to CM elliptic curves (2.5.12).

The results of this section are, at least when F is a finite extension of K, probably more or less known when translated into the language of algebraic Hecke characters though the proofs we give are, to the best of the author's knowledge, original. We would like to emphasise that the rather abstract approach taken – which eschews Hecke characters – works for all fields F simultaneously and allows for more conceptual proofs.

2.5.1. Let F be a field over O_K with separable closure F^{sep}, let $S = Spec(F^{sep})$ and let $\mathfrak{f} \in Id_{O_K}$ be invertible on Spec(F). By (2.3.3) there exists a CM elliptic curve E/S. Moreover, if E′/S is another CM elliptic curve then there exists a rank one projective O_K-module L and an isomorphism $f : E \otimes_{O_K} L \xrightarrow{\sim} E'$. Of course, we could take $L = \mathrm{Hom}_{O_K}(E, E')$ and f the evaluation map, but for what follows it will be more useful to work with arbitrary modules L and isomorphisms $f : E \otimes_{O_K} L \xrightarrow{\sim} E'$.

In particular, for each $\sigma \in G(F^{sep}/F)$ there is a rank one projective O_K-module L_σ and an isomorphism

$$f_\sigma : E \otimes_{O_K} L_\sigma \xrightarrow{\sim} \sigma^*(E).$$

This isomorphism, restricted to the $S = \mathrm{Spec}(F^{\mathrm{sep}})$-points of the $\mathfrak{f}$-torsion, is then given by

$$E[\mathfrak{f}](S) \otimes_{O_K} L_\sigma \overset{E[\mathfrak{f}](\sigma)\otimes\lambda_\sigma}{\longrightarrow} E[\mathfrak{f}](\sigma_!(S)) = \sigma^*(E)[\mathfrak{f}](S)$$

for a unique level-$\mathfrak{f}$ structure $\lambda_\sigma : L_\sigma \to O_K/\mathfrak{f}$ on L_σ. It is clear from this construction that the class

$$[\sigma]_{F,\mathfrak{f}} := (L_\sigma, \lambda_\sigma) \in \mathrm{CL}^{(\mathfrak{f})}_{O_K}$$

is independent of the choice of L_σ and the isomorphism $f_\sigma : E \otimes_{O_K} L_\sigma \overset{\sim}{\longrightarrow} \sigma^*(E)$. Moreover, as every other CM elliptic curve E'/S is of the form $E \otimes_{O_K} \mathfrak{a}$ for some ideal $\mathfrak{a}$, having chosen L_σ and an isomorphism $f_\sigma : E \otimes_{O_K} L_\sigma \overset{\sim}{\longrightarrow} \sigma^*(E)$, the map $f_\sigma \otimes_{O_K} \mathfrak{a}$ defines an isomorphism

$$(E \otimes_{O_K} \mathfrak{a}) \otimes_{O_K} L_\sigma = E \otimes_{O_K} L_\sigma \otimes_{O_K} \mathfrak{a} \overset{f_\sigma \otimes_{O_K} \mathfrak{a}}{\longrightarrow} \sigma^*(E) \otimes_{O_K} \mathfrak{a} = \sigma^*(E \otimes_{O_K} \mathfrak{a})$$

which induces on the S-valued points of the $\mathfrak{f}$-torsion

$$(E \otimes_{O_K} \mathfrak{a})[\mathfrak{f}](S) \otimes_{O_K} L_\sigma \overset{(E\otimes_{O_K}\mathfrak{a})[\mathfrak{f}](\sigma)\otimes\lambda_\sigma}{\longrightarrow} (E \otimes_{O_K} \mathfrak{a})[\mathfrak{f}](\sigma_!(S)).$$

Therefore the class $[\sigma]_{F,\mathfrak{f}}$ is also independent of the choice of E/S.

If $F \to F'$ is a field extension and

$$\mathrm{res} : G(F'^{\mathrm{sep}}/F') \to G(F^{\mathrm{sep}}/F)$$

denotes the restriction map then it follows easy from the definitions that

$$[-]_{F',\mathfrak{f}} = [-]_{F,\mathfrak{f}} \circ \mathrm{res}. \tag{2.5.1.1}$$

This relation implies that once we known $[-]_F$ for $F = K$, and $F = \mathbf{F}_\mathfrak{p}$ for each prime ideal $\mathfrak{p}$, we essentially know $[-]_F$ for any field F. The computation of the map $[-]_F$ for these values of F will be given in (2.5.9).

If $\tau \in G(F^{\mathrm{sep}}/F)$ then the composition

$$E \otimes_{O_K} L_\sigma \otimes_{O_K} L_\tau \overset{f_\sigma \otimes_{O_K} \mathrm{id}_{L_\tau}}{\longrightarrow} \sigma^*(E) \otimes_{O_K} L_\tau \overset{\sigma^*(f_\tau)}{\longrightarrow} \sigma^*(\tau^*(E))$$

induces on the S-points of the $\mathfrak{f}$-torsion the map

$$(E[\mathfrak{f}](\sigma^{-1}\circ\tau\circ\sigma)\otimes_{O_K}\lambda_\tau)\circ(E[\mathfrak{f}](\sigma)\otimes_{O_K}\lambda_\sigma\otimes_{O_K}\mathrm{id}_{L_\tau}) = E[\mathfrak{f}](\tau\circ\sigma)\otimes_{O_K}\lambda_\sigma\otimes_{O_K}\lambda_\tau$$

so that

$$[\sigma\tau]_{F,\mathfrak{f}} = (L_\tau \otimes_{O_K} L_\sigma, \lambda_\tau \otimes_{O_K} \lambda_\sigma) = (L_\tau, \lambda_\tau)(L_\sigma, \lambda_\sigma) = [\sigma]_{F,\mathfrak{f}}[\tau]_{F,\mathfrak{f}}.$$

In other words, $[-]_{F,\mathfrak{f}} : G(F^{\mathrm{sep}}/F) \to \mathrm{CL}^{(\mathfrak{f})}_{O_K}$ is a homomorphism.

2.5.2. The homomorphism of (1.4.4.1)

$$[-]_{\mathfrak{f}} : (\mathrm{A} \otimes_{\mathrm{O_K}} \mathrm{K})^{\times} \to \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}$$

restricted to $\mathrm{A}^{\times}_{\mathrm{O_K}}$ factors through the quotient $\mathrm{A}^{\times}_{\mathrm{O_K}} \to (\mathrm{O_K}/\mathfrak{f})^{\times}$ and we denote the resulting map by the same symbol

$$[-]_{\mathfrak{f}} : (\mathrm{O_K}/\mathfrak{f})^{\times} \to \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}.$$

Note that $\ker([-]_{\mathfrak{f}}) = \mathrm{im}(\mathrm{O}^{\times}_{\mathrm{K}} \to (\mathrm{O_K}/\mathfrak{f})^{\times}) \subset (\mathrm{O_K}/\mathfrak{f})^{\times}$.

2.5.3. Now let E/F be a CM elliptic curve and denote by

$$\rho_{\mathrm{E/F},\mathfrak{f}} : \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}) \to (\mathrm{O_K}/\mathfrak{f})^{\times}$$

the character defining the action of $\mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F})$ on the rank one $\mathrm{O_K}/\mathfrak{f}$-module $\mathrm{E}[\mathfrak{f}](\mathrm{S}) = \mathrm{E}[\mathfrak{f}](\mathrm{Spec}(\mathrm{F}^{\mathrm{sep}}))$, i.e.

$$\mathrm{E}[\mathfrak{f}](\sigma) = \rho_{\mathrm{E/F},\mathfrak{f}}(\sigma) : \mathrm{E}[\mathfrak{f}](\mathrm{S}) \to \mathrm{E}[\mathfrak{f}](\mathrm{S}).$$

We also note for future reference that as $(\mathrm{O_K}/\mathfrak{f})^{\times} = \mathrm{Aut}_{\mathrm{O_K}}(\mathrm{E}[\mathfrak{f}](\mathrm{S}))$ is abelian for each $\mathfrak{f}$ it follows that the extension $\mathrm{F}(\mathrm{E}[\mathfrak{f}])/\mathrm{F}$ generated by the $\mathfrak{f}$-torsion is an abelian extension of F. Moreover (as is obvious) the character $\rho_{\mathrm{E/F},\mathfrak{f}}$ is continuous, as it vanishes on the open subgroup of $\mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F})$ fixing $\mathrm{F}(\mathrm{E}[\mathfrak{f}])$.

2.5.4 Proposition. — (i) *The homomorphism* $[-]_{\mathrm{F},\mathfrak{f}}$ *is continuous and* (ii) *if* E/F *is a* CM *elliptic curve the diagram*

$$\begin{array}{ccc} \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}) & \xrightarrow{\rho^{-1}_{\mathrm{E/F},\mathfrak{f}}} & (\mathrm{O_K}/\mathfrak{f})^{\times} \\ & \searrow^{[-]_{\mathrm{F},\mathfrak{f}}} & \downarrow{\scriptstyle [-]_{\mathfrak{f}}} \\ & & \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}} \end{array}$$

commutes.

Proof. — (i) We shall reduce this claim to the second. By passage to the limit (applied to any CM elliptic curve over $\mathrm{Spec}(\mathrm{F}^{\mathrm{sep}})$) we may find a CM elliptic curve $\mathrm{E}/\mathrm{Spec}(\mathrm{F}')$ for some finite extension F'/F. If the diagram

$$\begin{array}{ccc} \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}') & \xrightarrow{\rho^{-1}_{\mathrm{E/F}',\mathfrak{f}}} & (\mathrm{O_K}/\mathfrak{f})^{\times} \\ \downarrow & & \downarrow{\scriptstyle [-]_{\mathfrak{f}}} \\ \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}) & \xrightarrow{[-]_{\mathrm{F},\mathfrak{f}}} & \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}} \end{array} \tag{2.5.4.1}$$

commutes then, as the composition along the top and right is continuous, it follows that $[-]_{\mathrm{F},\mathfrak{f}}|_{\mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}')}$ is continuous. But $\mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}') \subset \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F})$ is open and of finite index and $\mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}$ is discrete so it follows that $[-]_{\mathrm{F},\mathfrak{f}}$ is continuous.

As $[-]_{\mathrm{F},\mathfrak{f}} = [-]_{\mathrm{F},\mathfrak{f}}|_{\mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}')}$ (2.5.1.1), the commutativity of (2.5.4.1) is equivalent to the commutativity of the diagram

$$\begin{array}{ccc} \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}') & \xrightarrow{\rho^{-1}_{\mathrm{E}/\mathrm{F}',\mathfrak{f}}} & (\mathrm{O}_{\mathrm{K}}/\mathfrak{f})^{\times} \\ & \searrow^{[-]_{\mathrm{F}',\mathfrak{f}}} & \downarrow{\scriptstyle [-]_{\mathfrak{f}}} \\ & & \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O}_{\mathrm{K}}} \end{array}$$

and so we may assume that $\mathrm{F} = \mathrm{F}'$ and instead prove (ii).

(ii) Write $\mathrm{E}_{\mathrm{F}^{\mathrm{sep}}} = \mathrm{E} \times_{\mathrm{Spec}(\mathrm{F})} \mathrm{Spec}(\mathrm{F}^{\mathrm{sep}})$ and let

$$d_{\sigma} : \mathrm{E}_{\mathrm{F}^{\mathrm{sep}}} \to \sigma^{*}(\mathrm{E}_{\mathrm{F}^{\mathrm{sep}}})$$

be the descent isomorphism i.e. (the isomorphism coming from the fact that $\mathrm{E} = \mathrm{E} \times_{\mathrm{Spec}(\mathrm{F})} \mathrm{Spec}(\mathrm{F}^{\mathrm{sep}})$ descends to $\mathrm{Spec}(\mathrm{F})$). Then d_{σ} induces on the S-points of the $\mathfrak{f}$-torsion the map

$$\mathrm{E}[\mathfrak{f}](\mathrm{S}) \xrightarrow{\rho_{\mathrm{E}/\mathrm{F},\mathfrak{f}}(\sigma)^{-1}\cdot \mathrm{E}[\mathfrak{f}](\sigma)} \mathrm{E}[\mathfrak{f}](\sigma_{!}(\mathrm{S})) = \sigma^{*}(\mathrm{E}[\mathfrak{f}])(\mathrm{S})$$

and therefore

$$[\sigma]_{\mathrm{F},\mathfrak{f}} = (\mathrm{O}_{\mathrm{K}}, \mathrm{O}_{\mathrm{K}} \xrightarrow{\rho_{\mathrm{E}/\mathrm{F},\mathfrak{f}}(\sigma)^{-1}} \mathrm{O}_{\mathrm{K}}/\mathfrak{f}) = [\rho_{\mathrm{E}/\mathrm{F},\mathfrak{f}}(\sigma)^{-1}]_{\mathfrak{f}} \in \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O}_{\mathrm{K}}}$$

□

2.5.5 Proposition. — *Let* E/F *be a* CM *elliptic curve.*

(i) *Let* $\mathscr{L} \in \mathscr{CL}_{\mathrm{O}_{\mathrm{K}}}(\mathrm{Spec}(\mathrm{F}))$ *and*

$$\rho_{\mathscr{L}/\mathrm{F}} : \mathrm{G}(\mathrm{G}^{\mathrm{sep}}/\mathrm{F}) \to \mathrm{Aut}_{\mathrm{O}_{\mathrm{K}}}(\mathscr{L}(\mathrm{Spec}(\mathrm{F}^{\mathrm{sep}}))) = \mathrm{O}_{\mathrm{K}}^{\times}$$

be the associated character. Then $\rho_{\mathrm{E}\otimes_{\mathrm{O}_{\mathrm{K}}}\mathscr{L}/\mathrm{F}} = \rho_{\mathrm{E}/\mathrm{F},\mathfrak{f}}\rho_{\mathscr{L}/\mathrm{F}}$.

(ii) *If* $\tau : \mathrm{F} \to \mathrm{F}$ *is any* O_{K}*-linear automorphism then*

$$\rho_{\tau^{*}(\mathrm{E})/\mathrm{F}}(\sigma) = \rho_{\mathrm{E}/\mathrm{F},\mathfrak{f}}(\widetilde{\tau}^{-1}\sigma\widetilde{\tau})$$

for each $\sigma \in \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F})$*, where* $\widetilde{\tau}$ *denotes any extension of* τ *to* $\mathrm{F}^{\mathrm{sep}}$.

Proof. — These are immediate from the definition of $\rho_{\mathrm{E}/\mathrm{F},\mathfrak{f}}$ as the character defining the action of $\mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F})$ on $\mathrm{E}[\mathfrak{f}](\mathrm{S}) = \mathrm{E}[\mathfrak{f}](\mathrm{Spec}(\mathrm{F}^{\mathrm{sep}}))$. □

2.5.6. For what follows we let $\mathfrak{f} \in \mathrm{Id}_{\mathrm{O}_{\mathrm{K}}}$ vary over the integral ideals of O_{K} which are invertible on $\mathrm{Spec}(\mathrm{F})$. We now take the limit over $\mathfrak{f}$ to define the homomorphisms $[-]_{\mathrm{F}}$, $\rho_{\mathrm{E}/\mathrm{F}}$ and $[-]$ by

$$[-]_{\mathrm{F}} := \varprojlim_{\mathfrak{f}} [-]_{\mathrm{F},\mathfrak{f}} : \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}) \to \varprojlim_{\mathfrak{f}} \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O}_{\mathrm{K}}},$$

$$\rho_{\mathrm{E}/\mathrm{F}} := \varprojlim_{\mathfrak{f}} \rho_{\mathrm{E}/\mathrm{F},\mathfrak{f}} : \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}) \to \varprojlim_{\mathfrak{f}} (\mathrm{O}_{\mathrm{K}}/\mathfrak{f})^{\times},$$

and

$$[-] := \varprojlim_{\mathfrak{f}} [-]_{\mathfrak{f}} : \varprojlim_{\mathfrak{f}} (\mathrm{O}_{\mathrm{K}}/\mathfrak{f})^{\times} \to \varprojlim_{\mathfrak{f}} \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O}_{\mathrm{K}}}.$$

We find immediately from (ii) of (2.5.4) that

$$[-]_{\mathrm{F}} = [\rho_{\mathrm{E/F}}^{-1}]. \tag{2.5.6.1}$$

2.5.7 Proposition. — *Let* $\mathrm{E}, \mathrm{E}'/\mathrm{F}$ *be a pair of* CM *elliptic curves. The following are equivalent:*

(i) $\rho_{\mathrm{E/F}} = \rho_{\mathrm{E}'/\mathrm{F}}$,
(ii) *the character* ρ *defining the action of* $\mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F})$ *on*

$$\underline{\mathrm{Hom}}^{\mathrm{O_K}}_{\mathrm{Spec(F)}}(\mathrm{E}, \mathrm{E}')(\mathrm{Spec}(\mathrm{F}^{\mathrm{sep}}))$$

is trivial,
(iii) *the étale* $\mathrm{Spec}(\mathrm{F})$*-scheme* $\underline{\mathrm{Hom}}^{\mathrm{O_K}}_{\mathrm{Spec(F)}}(\mathrm{E}, \mathrm{E}')$ *is constant,*
(iv) E *and* E' *are isogenous.*

Proof. — Let $\rho : \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}) \to \mathrm{O_K^\times}$ be the character defining the action of $\mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F})$ on the $\mathrm{Spec}(\mathrm{F}^{\mathrm{sep}})$-valued points of the rank one $\mathrm{O_K}$-local system $\underline{\mathrm{Hom}}^{\mathrm{O_K}}_{\mathrm{Spec(F)}}(\mathrm{E}, \mathrm{E}')$.

(i) implies (ii): The isomorphism

$$\mathrm{E} \otimes_{\mathrm{O_K}} \underline{\mathrm{Hom}}_{\mathrm{Spec(F)}^{\mathrm{O_K}}}(\mathrm{E}, \mathrm{E}') \xrightarrow{\sim} \mathrm{E}'$$

combined with (i) of (2.5.5) gives $\rho_{\mathrm{E}'/\mathrm{F}} = \rho \cdot \rho_{\mathrm{E/F}}$ so that ρ is trivial if and only if $\rho_{\mathrm{E/F}} = \rho_{\mathrm{E}'/\mathrm{F}}$.

(ii) implies (iii): This is clear from the definition of ρ.

(iii) implies (iv): If $\underline{\mathrm{Hom}}^{\mathrm{O_K}}_{\mathrm{Spec(F)}}(\mathrm{E}, \mathrm{E}')$ is constant any non-zero $\mathrm{Spec}(\mathrm{F})$-section defines an isogeny $\mathrm{E} \to \mathrm{E}'$.

(iv) implies (i): If $f : \mathrm{E} \to \mathrm{E}'$ is an isogeny then $\ker(f) = \mathrm{E}[\mathfrak{a}] = \ker(i_{\mathfrak{a}})$ for some integral ideal $\mathfrak{a}$ by (2.2.15). Therefore $\mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \xrightarrow{\sim} \mathrm{E}'$ and by (i) of (2.5.5) we then get

$$\rho_{\mathrm{E}'/\mathrm{F}} = \rho_{\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{a}^{-1}/\mathrm{F}} = \rho_{\mathrm{E/F}}.$$

□

2.5.8 Proposition. — *Let*

$$\rho = \lim_{\mathfrak{f}} \rho_{\mathfrak{f}} : \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}) \to \lim_{\mathfrak{f}} (\mathrm{O_K}/\mathfrak{f})^\times$$

be a continuous homomorphism. Then there exists a CM *elliptic curve* E/F *with* $\rho_{\mathrm{E/F}} = \rho$ *if and only if the diagram*

$$\begin{array}{ccc} \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}) & \xrightarrow{\rho^{-1}} & \lim_{\mathfrak{f}} (\mathrm{O_K}/\mathfrak{f})^\times \\ & \searrow^{[-]_{\mathrm{F}}} & \downarrow{\scriptstyle [-]} \\ & & \lim_{\mathfrak{f}} \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}} \end{array}$$

commutes.

Proof. — The only if claim is (2.5.6.1). Conversely, by passage to the limit there exists a CM elliptic curve $\mathrm{E}'/\mathrm{Spec}(\mathrm{F}')$ where $\mathrm{F} \subset \mathrm{F}'$ is a finite extension. As the compositions of $\rho_{\mathrm{E}'/\mathrm{F}'}$ and $\rho|_{\mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}')}$ with

$$[-] : \lim_{\mathfrak{f}} (\mathrm{O}_{\mathrm{K}}/\mathfrak{f})^{\times} \to \lim_{\mathfrak{f}} \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O}_{\mathrm{K}}}$$

coincide and $\ker([-]) = \mathrm{O}_{\mathrm{K}}^{\times}$, the difference defines a character

$$\rho^{-1}_{\mathrm{E}'/\mathrm{F}'} \cdot \rho|_{\mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}')} : \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}') \to \mathrm{O}_{\mathrm{K}}^{\times} = \ker([-]) \subset \lim_{\mathfrak{f}} (\mathrm{O}_{\mathrm{K}}/\mathfrak{f})^{\times}. \quad (2.5.8.1)$$

Replacing E' by the tensor product of E' with any rank one O_{K}-local system with associated character (2.5.8.1) we may assume that $\rho_{\mathrm{E}'/\mathrm{F}'} = \rho|_{\mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}')}$.

Let $\upsilon \in \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}')$ and $\widetilde{\sigma} \in \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F})$ with $\widetilde{\sigma}|_{\mathrm{F}'} = \sigma$. We have by (ii) of (2.5.5)

$$\rho_{\sigma^*(\mathrm{E}')/\mathrm{F}'}(\upsilon) = \rho_{\mathrm{E}'/\mathrm{F}'}(\sigma^{-1}\upsilon\sigma) = \rho(\sigma^{-1}\upsilon\sigma) = \rho(\upsilon) = \rho_{\mathrm{E}'/\mathrm{F}'}(\upsilon).$$

Therefore $\rho_{\sigma^*(\mathrm{E}')/\mathrm{F}'} = \rho_{\mathrm{E}'/\mathrm{F}'}$ and by (ii) of (2.5.7) E' and $\sigma^*(\mathrm{E}')$ are isogenous.

For all $\mathfrak{f}$ invertible on $\mathrm{Spec}(\mathrm{F})$ we have

$$[\widetilde{\sigma}]_{\mathrm{F},\mathfrak{f}} = [\rho_{\mathfrak{f}}(\sigma)^{-1}]_{\mathfrak{f}} = (\mathrm{O}_{\mathrm{K}}, \mathrm{O}_{\mathrm{K}} \overset{\rho_{\mathfrak{f}}(\sigma)^{-1}}{\to} \mathrm{O}_{\mathrm{K}}/\mathfrak{f}).$$

This implies that, writing $\mathrm{E}'_{\mathrm{F}^{\mathrm{sep}}} = \mathrm{E} \times_{\mathrm{Spec}(\mathrm{F})} \mathrm{Spec}(\mathrm{F}^{\mathrm{sep}})$, the CM elliptic curves $\mathrm{E}'_{\mathrm{F}^{\mathrm{sep}}}$ and $\widetilde{\sigma}^*(\mathrm{E}_{\mathrm{F}^{\mathrm{sep}}})$ are isomorphic. As $\widetilde{\sigma}|_{\mathrm{F}} = \sigma$ this implies that E' and $\sigma^*(\mathrm{E}')$ are locally isomorphic. But E and E' are also isogenous and so by (2.4.3) they are isomorphic.

Now fix an integral ideal $\mathfrak{f}$ which separates units and is also invertible on $\mathrm{Spec}(\mathrm{F})$. As $[\widetilde{\sigma}]_{\mathrm{F},\mathfrak{f}} = [\rho_{\mathfrak{f}}(\widetilde{\sigma})^{-1}]$, and as $\mathfrak{f}$ separates units, there is a unique isomorphism

$$r_{\widetilde{\sigma}} : \mathrm{E}' \xrightarrow{\sim} \sigma^*(\mathrm{E}')$$

which on S-valued points of the $\mathfrak{f}$-torsion is the map

$$\mathrm{E}'[\mathfrak{f}](\mathrm{S}) \overset{\rho_{\mathfrak{f}}(\sigma)^{-1}\cdot \mathrm{E}'[\mathfrak{f}](\widetilde{\sigma})}{\longrightarrow} \mathrm{E}'[\mathfrak{f}](\sigma_!(\mathrm{S})) = \sigma^*(\mathrm{E})[\mathfrak{f}](\mathrm{S}) \quad (2.5.8.2)$$

where we view $\widetilde{\sigma}$ as a $\mathrm{Spec}(\mathrm{F}')$-morphism

$$\widetilde{\sigma} : \sigma_!(\mathrm{S}) \to \mathrm{S}.$$

If $\tau \in \mathrm{G}(\mathrm{F}'/\mathrm{F})$ and $\widetilde{\tau} \in \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F})$ satisfies $\widetilde{\tau}|_{\mathrm{F}'} = \tau$ then the defining property (2.5.8.2) of the isomorphism

$$r_{\widetilde{\sigma}\widetilde{\tau}} : \mathrm{E}' \xrightarrow{\sim} (\tau \circ \sigma)^*(\mathrm{E}')$$

is also satisfied by

$$\sigma^*(r_{\widetilde{\tau}}) \circ r_{\widetilde{\sigma}} : \mathrm{E}' \xrightarrow{\sim} (\tau \circ \sigma)^*(\mathrm{E}')$$

and so we get

$$r_{\widetilde{\sigma}\widetilde{\tau}} = \sigma^*(r_{\widetilde{\tau}}) \circ r_{\widetilde{\sigma}}. \quad (2.5.8.3)$$

Moreover, if $\widetilde{\sigma} \in \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}') \subset \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F})$ then $r_{\widetilde{\sigma}}$ induces on the S-points of the $\mathfrak{f}$-torsion the map

$$\mathrm{E}'[\mathfrak{f}](\mathrm{S}) \overset{\rho_{\mathfrak{f}}(\widetilde{\sigma})\cdot \mathrm{E}'[\mathfrak{f}](\widetilde{\sigma})}{\longrightarrow} \mathrm{E}[\mathfrak{f}](\mathrm{S}).$$

However, by definition

$$\mathrm{E}'[\mathfrak{f}](\widetilde{\sigma}) = \rho_{\mathrm{E}'/\mathrm{F}',\mathfrak{f}}(\widetilde{\sigma})$$

so that $r_{\widetilde{\sigma}}$ induces on the S-valued points of the $\mathfrak{f}$-torsion the map

$$\rho_{\mathrm{E}'/\mathrm{F}',\mathfrak{f}}(\widetilde{\sigma})^{-1}\mathrm{E}[\mathfrak{f}](\widetilde{\sigma}) = \rho_{\mathrm{E}'/\mathrm{F}',\mathfrak{f}}(\widetilde{\sigma})^{-1}\rho_{\mathrm{E}'/\mathrm{F}',\mathfrak{f}}(\widetilde{\sigma}) = \mathrm{id}_{\mathrm{E}[\mathfrak{f}](\mathrm{S})}.$$

The uniqueness of $r_{\widetilde{\sigma}}$ now shows that $r_{\widetilde{\sigma}} = \mathrm{id}_{\mathrm{E}'}$.

This combined with the relation (2.5.8.3) shows that for all $\widetilde{\sigma} \in \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F})$ the isomorphism $r_{\widetilde{\sigma}} = r_\sigma$ depends only on $\sigma = \widetilde{\sigma}|_{\mathrm{F}}$, has $r_{\mathrm{id}_{\mathrm{F}'}} = \mathrm{id}_{\mathrm{E}'}$ and satisfies

$$r_{\sigma\tau} = \sigma^*(r_\tau) \circ r_\sigma.$$

In other words, we have Galois descent data on $\mathrm{E}' \to \mathrm{Spec}(\mathrm{F}')$ relative to $\mathrm{Spec}(\mathrm{F}') \to \mathrm{Spec}(\mathrm{F})$ and by construction the descended CM elliptic curve $\mathrm{E}/\mathrm{Spec}(\mathrm{F})$ has $\rho_{\mathrm{E}/\mathrm{F}} = \rho$. □

2.5.9 Proposition. — (i) *When* $\mathrm{F} = \mathbf{F}_{\mathfrak{p}}$, *in the notation of* (1.4.7), *we have for all* $n \in \widehat{\mathbf{Z}}$*:*

$$[\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}]_{\mathbf{F}_{\mathfrak{p}}} = \lim_{(\mathfrak{f},\mathfrak{p})=\mathrm{O}_{\mathrm{K}}} [\mathfrak{p}]_{\mathfrak{f}}^{-n} \in \lim_{(\mathfrak{f},\mathfrak{p})=\mathrm{O}_{\mathrm{K}}} \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O}_{\mathrm{K}}}.$$

(ii) *When* $\mathrm{F} = \mathrm{K}_{\mathfrak{p}}$, *we have for all* $\sigma \in \mathrm{G}(\mathrm{K}_{\mathfrak{p}}^{\mathrm{sep}}/\mathrm{K})$*:*

$$\sigma|_{\mathrm{K}^\infty} = \theta_{\mathrm{K}}([\sigma]_{\mathrm{K}_{\mathfrak{p}}})$$

where the restriction $|_{\mathrm{K}^\infty}$ *is along any* K*-linear embedding* $\mathrm{K}^\infty \to \mathrm{K}_{\mathfrak{p}}^{\mathrm{sep}}$.

(iii) *When* $\mathrm{F} = \mathrm{K}$ *we have for all* $\sigma \in \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$*:*

$$\sigma|_{\mathrm{K}^\infty} = \theta_{\mathrm{K}}([\sigma]_{\mathrm{K}}).$$

Proof. — (i) As $\mathrm{G}(\mathbf{F}_{\mathfrak{p}}^{\mathrm{sep}}/\mathbf{F}_{\mathfrak{p}})$ is topologically generated by $\mathrm{Fr}^{\mathrm{N}\mathfrak{p}}$, by continuity it is enough to show that $[\mathrm{Fr}^{\mathrm{N}\mathfrak{p}}]_{\mathbf{F}_{\mathfrak{p}},\mathfrak{f}} = [\mathfrak{p}]_{\mathfrak{f}}^{-1}$ for all $\mathfrak{f}$ prime to $\mathfrak{p}$. Write $\mathrm{S} = \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}}^{\mathrm{sep}})$, let E/S be a CM elliptic curve and consider the isomorphism

$$\nu_{\mathfrak{p}} : \mathrm{E} \otimes_{\mathrm{O}_{\mathrm{K}}} \mathfrak{p}^{-1} \xrightarrow{\sim} \mathrm{Fr}^{\mathrm{N}\mathfrak{p}*}(\mathrm{E})$$

of (2.2.13). By the definition of $\nu_{\mathfrak{p}}$, the composition

$$\mathrm{E} \xrightarrow{i_{\mathfrak{p}}} \mathrm{E} \otimes_{\mathrm{O}_{\mathrm{K}}} \mathfrak{p}^{-1} \xrightarrow{\sim} \mathrm{Fr}^{\mathrm{N}\mathfrak{p}^*}(\mathrm{E})$$

is equal to the $\mathrm{N}\mathfrak{p}$-power relative Frobenius of E which induces the map

$$\mathrm{E}[\mathfrak{f}](\mathrm{S}) \overset{\mathrm{E}[\mathfrak{f}](\mathrm{Fr}^{\mathrm{N}\mathfrak{p}})}{\longrightarrow} \mathrm{E}[\mathfrak{f}](\mathrm{Fr}_!^{\mathrm{N}\mathfrak{p}}(\mathrm{S}))$$

on the S-points of the $\mathfrak{f}$-torsion. Therefore, the map $\nu_{\mathfrak{p}}$ induces on the S-valued points of the $\mathfrak{f}$-torsion the map

$$\mathrm{E}[\mathfrak{f}](\mathrm{S}) \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1} \overset{\mathrm{E}[\mathfrak{f}](\mathrm{Fr}^{\mathrm{N}\mathfrak{p}})\otimes f}{\longrightarrow} \mathrm{E}[\mathfrak{f}](\mathrm{Fr}_!^{\mathrm{N}\mathfrak{p}}(\mathrm{S}))$$

where f is level-$\mathfrak{f}$ structure defined by (1.4.3.1). Hence

$$[\mathrm{Fr}^{\mathrm{N}\mathfrak{p}}]_{\mathbf{F}_{\mathfrak{p}},\mathfrak{f}} = [\mathfrak{p}^{-1}]_{\mathfrak{f}} = [\mathfrak{p}]_{\mathfrak{f}}^{-1}.$$

(ii) Write $\mathrm{T} = \mathrm{Spec}(\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}^{\mathrm{sep}}})$, $\mathrm{T}_{\mathfrak{p}} = \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}}^{\mathrm{sep}}) \subset \mathrm{T}$, let $\mathscr{E}/\mathrm{T}$ be a CM elliptic curve, write $\mathscr{E}_{\mathfrak{p}} = \mathscr{E} \times_{\mathrm{T}} \mathrm{T}_{\mathfrak{p}}$. By continuity it is enough to prove the claim for $\sigma \in \mathrm{W}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K}) = v_{\mathrm{K}}^{-1}(\mathbf{Z})$ and by multiplicativity for σ with $v_{\mathrm{K}}(\sigma) = n \geq 0$. Let σ be such an element.

As $\mathrm{T} = \mathrm{Spec}(\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}^{\mathrm{sep}}})$ admits no non-constant finite étale covers, the sheaf

$$\underline{\mathrm{Isom}}_{\mathrm{T}}^{\mathrm{O_K}}(\mathscr{E} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1}, \sigma^*(\mathscr{E}))$$

is finite and constant. Moreover, as T is connected and σ acts by $\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}$ on the residue field $\mathbf{F}_{\mathfrak{p}}^{\mathrm{sep}}$ of $\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}^{\mathrm{sep}}}$, there exists a unique isomorphism

$$\nu_\sigma : \mathscr{E} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-n} \overset{\sim}{\longrightarrow} \sigma^*(\mathscr{E})$$

lifting the isomorphism

$$\nu_{\mathfrak{p}} : \mathscr{E}_{\mathfrak{p}} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-n} \overset{\sim}{\longrightarrow} \mathrm{Fr}^{\mathrm{N}\mathfrak{p}*}(\mathscr{E}_{\mathfrak{p}})$$

of (2.6.5). We now compute the action of ν_σ on the T-points of the $\mathfrak{f}$-torsion of $\mathscr{E}/\mathrm{T}$.

First let $\mathfrak{f}$ be prime to $\mathfrak{p}$. As $\mathscr{E}[\mathfrak{f}]$ is finite étale, we have $\mathscr{E}[\mathfrak{f}](\mathrm{T}) = \mathscr{E}[\mathfrak{f}](\mathrm{T}_{\mathfrak{p}})$ compatibly with the actions of σ and $\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}$. It now follows from (i) that the map induced by ν_σ on the S-points of the $\mathfrak{f}$-torsion is

$$\mathscr{E}[\mathfrak{f}](\mathrm{T}) \otimes_{\mathrm{O_K}} \mathfrak{p}^{-n} \overset{\mathscr{E}[\mathfrak{f}](\sigma)\otimes f}{\to} \mathscr{E}[\mathfrak{f}](\sigma_!(\mathrm{T})) = \sigma^*(\mathscr{E})[\mathfrak{f}](\mathrm{T})$$

where f is level-$\mathfrak{f}$ structure defined by (1.4.7).

Now let $\mathfrak{f} = \mathfrak{p}^r$ for some $r \geq 0$. Setting $\mathscr{E}_r := \mathscr{E}[\mathfrak{p}^r]$ and

$$\mathrm{T}_\infty = \mathrm{Spf}(\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}^{\mathrm{sep}}}) = \operatorname*{colim}_n \mathrm{Spec}(\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}^{\mathrm{sep}}}/\mathfrak{p}^{n+1}),$$

we obtain the commutative diagram

$$\begin{array}{ccc} \mathscr{E}_r(\mathrm{T}) \otimes_{\mathrm{O_K}} \mathfrak{p}^{-n} & \longrightarrow & \sigma^*(\mathscr{E}_r)(\mathrm{T}) \\ \downarrow & & \downarrow \\ \mathscr{E}_r(\mathrm{T}_\infty) \otimes_{\mathrm{O_K}} \mathfrak{p}^{-n} & \longrightarrow & \sigma^*(\mathscr{E}_r)(\mathrm{T}_\infty). \end{array} \tag{2.5.9.1}$$

whose columns are isomorphisms as $\mathscr{E}_r$ is finite locally free over S. Now consider $\mathrm{F} = \mathscr{E}[\mathfrak{p}^\infty] \times_{\mathrm{T}} \mathrm{T}_\infty$ and set $\mathrm{F}_r = \mathrm{F}[\mathfrak{p}^r]$. Then F is a Lubin–Tate $\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}$-module over the $\mathfrak{p}$-adic sheaf T_∞ by (2.2.11) and the map on the bottom row

of (2.5.9.1) is equal to

$$\nu_\sigma : \mathrm{F}_r(\mathrm{T}_\infty) \otimes_{\mathrm{O}_{\mathrm{K}_\mathfrak{p}}} \mathfrak{p}^{-n} \xrightarrow{\sim} \sigma^*(\mathrm{F}_r)(\mathrm{T}_\infty)$$

where ν_σ is the unique map in (i) of (1.2.20). It follows from (iii) of (1.2.20) that this map is given by

$$\mathrm{F}_r(\sigma) \otimes_{\mathrm{O}_{\mathrm{K}_\mathfrak{p}}} \chi_{\mathrm{K}_\mathfrak{p}}(\sigma) : \mathrm{F}_r(\mathrm{T}_\infty) \otimes_{\mathrm{O}_{\mathrm{K}_\mathfrak{p}}} \mathfrak{p}^{-n} \xrightarrow{\sim} \mathrm{F}[\mathfrak{p}^r](\sigma_!(\mathrm{T}_\infty)) = \sigma^*(\mathrm{F}[\mathfrak{p}^r])(\mathrm{T}_\infty)$$

where $\sigma|_{\mathrm{K}_\mathfrak{p}^{\mathrm{ab}}} = (\chi_{\mathrm{K}_\mathfrak{p}}(\sigma), \mathrm{K}_\mathfrak{p}^{\mathrm{ab}}/\mathrm{K}_\mathfrak{p})$. Therefore the map in the top row of (2.5.9.1) is given by $\mathscr{E}_r(\sigma) \otimes_{\mathrm{O}_\mathrm{K}} \chi_{\mathrm{K}_\mathfrak{p}}(\sigma)$.

Writing $\mathrm{S} = \mathrm{Spec}(\mathrm{K}_\mathfrak{p}^{\mathrm{sep}})$ and considering the generic fibre $\mathrm{E} := \mathscr{E} \times_\mathrm{T} \mathrm{S}$, and arbitrary $\mathfrak{f}$, the computations above show that the map induced by ν_σ

$$\mathrm{E}[\mathfrak{f}](\mathrm{S}) \otimes_{\mathrm{O}_\mathrm{K}} \mathfrak{p}^{-n} \xrightarrow{\sim} \mathrm{E}[\mathfrak{f}](\sigma_!(\mathrm{S})) = \sigma^*(\mathrm{E}[\mathfrak{p}^r])(\mathrm{S})$$

is given by $\mathrm{E}(\sigma) \otimes \chi_{\mathrm{K}_\mathfrak{p}}(\sigma)$ where we view $\chi_{\mathrm{K}_\mathfrak{p}}(\sigma)$ as

$$\mathfrak{p}^{-n} \xrightarrow{\chi_{\mathrm{K}_\mathfrak{p}}(\sigma)} \mathrm{A}_{\mathrm{O}_\mathrm{K}} \to \mathrm{O}_\mathrm{K}/\mathfrak{f}.$$

Therefore

$$[\sigma]_{\mathrm{K}_\mathfrak{p},\mathfrak{f}} = (\mathfrak{p}^{-n}, \mathfrak{p}^{-n} \xrightarrow{\chi_{\mathrm{K}_\mathfrak{p}}(\sigma)} \mathrm{A}_{\mathrm{O}_\mathrm{K}} \to \mathrm{O}_\mathrm{K}/\mathfrak{f}) = [\chi_{\mathrm{K}_\mathfrak{p}}(\sigma)]_\mathfrak{f}.$$

Taking limits we find $[\sigma]_{\mathrm{K}_\mathfrak{p}} = [\chi_{\mathrm{K}_\mathfrak{p}}(\sigma)]$ and by (1.4.8.2) we get

$$\sigma|_{\mathrm{K}^\infty} = \theta_\mathrm{K}([\sigma]_{\mathrm{K}_\mathfrak{p}})$$

where the restriction is along any K-embedding $\mathrm{K}^\infty \to \mathrm{K}_\mathfrak{p}^{\mathrm{sep}}$.

(iii) We see from (ii) that for all primes $\mathfrak{p}$ and all embeddings $\mathrm{K}^{\mathrm{sep}} \to \mathrm{K}_\mathfrak{p}^{\mathrm{sep}}$ and all $\sigma \in \mathrm{G}(\mathrm{K}_\mathfrak{p}^{\mathrm{sep}}/\mathrm{K})$, writing $\tau = \sigma|_{\mathrm{K}^{\mathrm{sep}}}$

$$\tau|_{\mathrm{K}^\infty} = (\sigma|_{\mathrm{K}^{\mathrm{sep}}})|_{\mathrm{K}^\infty} = \sigma|_{\mathrm{K}^\infty} = \theta_\mathrm{K}([\sigma]_{\mathrm{K}_\mathfrak{p}}) = \theta_\mathrm{K}([\sigma|_{\mathrm{K}^{\mathrm{sep}}}]_\mathrm{K}) = \theta_\mathrm{K}([\tau]_\mathrm{K}).$$

However, the sub-group of $\mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$ generated by elements of the form $\tau = \sigma|_{\mathrm{K}^{\mathrm{sep}}}$ (for varying primes $\mathfrak{p}$ and embeddings $\mathrm{K}^{\mathrm{sep}} \to \mathrm{K}_\mathfrak{p}^{\mathrm{sep}}$) is dense. It follows, by continuity and multiplicativity, that for all $\tau \in \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$ we have

$$\tau|_{\mathrm{K}^\infty} = \theta_\mathrm{K}([\tau]_\mathrm{K}).$$

□

2.5.10. The homomorphisms $[-]_\mathrm{F}$ can be (trivially) reinterpreted idèlically using the isomorphism (1.4.7.2)

$$\mathrm{CL}_{\mathrm{O}_\mathrm{K},\infty} \xrightarrow{h_\mathrm{K}^{-1}} (\mathrm{A} \otimes_{\mathrm{O}_\mathrm{K}} \mathrm{K})^\times/\mathrm{K}^\times$$

and we do so only to make clear the relationship with the map (1.2.21.1). Let us do so here for h_K and so define $\chi_\mathrm{K} = [-]_\mathrm{K} \circ h_\mathrm{K}^{-1}$.

(i) For all $\sigma \in \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$ we have $\sigma|_{\mathrm{K}^\infty} = (\chi_\mathrm{K}(\sigma), \mathrm{K}^\infty/\mathrm{K})$ (cf. (iv) of (1.2.20)).

(ii) For each prime $\mathfrak{p}$, each $\sigma \in \mathrm{W}(\mathrm{K}_{\mathfrak{p}}^{\mathrm{sep}}/\mathrm{K}_{\mathfrak{p}}) \subset \mathrm{G}(\mathrm{K}_{\mathfrak{p}}^{\mathrm{sep}}/\mathrm{K})$ and each K-linear $\mathrm{K}^{\mathrm{sep}} \to \mathrm{K}_{\mathfrak{p}}^{\mathrm{sep}}$ we have

$$\chi_{\mathrm{K}}(\sigma|_{\mathrm{K}^{\mathrm{sep}}}) = \chi_{\mathrm{K}_{\mathfrak{p}}}(\sigma) \in \mathrm{K}_{\mathfrak{p}}^{\times} \subset (\mathrm{A}_{\mathrm{O}_{\mathrm{K}}} \otimes_{\mathrm{O}_{\mathrm{K}}} \mathrm{K})^{\times}/\mathrm{K}^{\times}$$

where $\chi_{\mathrm{K}_{\mathfrak{p}}}$ is the homomorphism of (1.2.21.1).

(iii) If $\mathrm{K} \subset \mathrm{L} \subset \mathrm{K}^{\mathrm{sep}}$ is a finite extension of K and $\rho : \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{L}) \to \mathrm{A}_{\mathrm{O}_{\mathrm{K}}}^{\times}$ is a continuous character then there exists a CM elliptic curve E/Spec(L) with $\rho_{\mathrm{E/L}} = \rho$ if and only if the following diagram commutes

$$\begin{array}{ccc} \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{L}) & \xrightarrow{\rho_{\mathrm{E/L}}^{-1}} & \mathrm{A}_{\mathrm{O}_{\mathrm{K}}}^{\times} \\ & \searrow^{\chi_{\mathrm{K}}|_{\mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{L})}} & \downarrow \\ & & (\mathrm{A}_{\mathrm{O}_{\mathrm{K}}} \otimes_{\mathrm{O}_{\mathrm{K}}} \mathrm{K})^{\times}/\mathrm{K}^{\times} \end{array}$$

where the right vertical arrow is the obvious map.

2.5.11 Remark. — Let L/K be a finite Galois extension and let E/L be a CM elliptic curve. We now give a simple description of the algebraic Hecke character of E/L, which is a certain continuous homomorphism

$$\psi_{\mathrm{E/L}} : \mathrm{I}_{\mathrm{L}} \to \mathrm{K}^{\times}$$

satisfying $\psi_{\mathrm{E/L}}|_{\mathrm{L}^{\times}} = \mathrm{N}_{\mathrm{L/K}}$ (for the definition of $\psi_{\mathrm{E/L}}$ see §7 of [**31**]).

View the homomorphism

$$\rho_{\mathrm{E/L}} : \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{L}) \to \mathrm{A}_{\mathrm{O}_{\mathrm{K}}}^{\times}$$

as a homomorphism

$$\rho_{\mathrm{E/L}} : \mathrm{G}(\mathrm{L}^{\mathrm{ab}}/\mathrm{L}) = \mathrm{G}(\mathrm{L}^{\mathrm{sep}}/\mathrm{L})^{\mathrm{ab}} \to \mathrm{A}_{\mathrm{O}_{\mathrm{K}}}^{\times}$$

and for $s \in \mathrm{I}_{\mathrm{L}}$ write s_{fin} for the element of $(\mathrm{A}_{\mathrm{O}_{\mathrm{K}}} \otimes_{\mathrm{O}_{\mathrm{K}}} \mathrm{L})^{\times}$ obtained by forgetting the components of s at the places of L lying over ∞. Then we claim that algebraic Hecke character $\psi_{\mathrm{E/L}}$ associated to E/L is given by

$$\psi_{\mathrm{E/L}} : \mathrm{I}_{\mathrm{L}} \to (\mathrm{A}_{\mathrm{O}_{\mathrm{K}}} \otimes_{\mathrm{O}_{\mathrm{K}}} \mathrm{K})^{\times} : s \mapsto \rho_{\mathrm{E/L}}((s^{-1}, \mathrm{L}^{\mathrm{ab}}/\mathrm{L})) \cdot \mathrm{N}_{\mathrm{L/K}}(s_{\mathrm{fin}}). \quad (2.5.11.1)$$

We will not prove this but let us show that the map $\psi_{\mathrm{E/L}}$ defined by (2.5.11.1) satisfies $\psi_{\mathrm{E/L}}|_{\mathrm{L}^{\times}} = \mathrm{N}_{\mathrm{L/K}}$ and $\psi_{\mathrm{E/L}}(\mathrm{I}_{\mathrm{L}}) \subset \mathrm{K}^{\times} \subset (\mathrm{A}_{\mathrm{O}_{\mathrm{K}}} \otimes_{\mathrm{O}_{\mathrm{K}}} \mathrm{K})^{\times}$.

For $a \in \mathrm{L}^{\times} \subset \mathrm{I}_{\mathrm{L}}$ we have

$$\rho_{\mathrm{E/L}}(a) = \rho_{\mathrm{E/L}}((a^{-1}, \mathrm{L}^{\mathrm{ab}}/\mathrm{L})) \cdot \mathrm{N}_{\mathrm{L/K}}(a_{\mathrm{fin}}) = 1 \cdot \mathrm{N}_{\mathrm{L/K}}(a)$$

so that $\rho_{\mathrm{E/L}}|_{\mathrm{L}^{\times}} = \mathrm{N}_{\mathrm{L/K}}$. Now computing the composition

$$\mathrm{I}_{\mathrm{L}} \overset{\rho_{\mathrm{E/L}}}{\to} (\mathrm{A} \otimes_{\mathrm{O}_{\mathrm{K}}} \mathrm{K})^{\times} \overset{[-]}{\to} \mathrm{CL}_{\mathrm{O}_{\mathrm{K}},\infty}$$

we find:

$$\begin{aligned}
[\rho_{\mathrm{E/L}}((s^{-1},\mathrm{L}^{\mathrm{ab}}/\mathrm{L}))\cdot \mathrm{N}_{\mathrm{L/K}}(s_{\mathrm{fin}})] &= [\rho_{\mathrm{E/L}}((s^{-1},\mathrm{L}^{\mathrm{ab}}/\mathrm{L}))]\cdot[\mathrm{N}_{\mathrm{L/K}}(s_{\mathrm{fin}})]\\
&= [(s^{-1},\mathrm{L}^{\mathrm{ab}}/\mathrm{L})]_{\mathrm{L}}\cdot[\mathrm{N}_{\mathrm{L/K}}(s_{\mathrm{fin}})]\\
&= [(\mathrm{N}_{\mathrm{L/K}}(s^{-1}),\mathrm{K}^{\mathrm{ab}}/\mathrm{K})]_{\mathrm{K}}\cdot[\mathrm{N}_{\mathrm{L/K}}(s_{\mathrm{fin}})]\\
&= [(\mathrm{N}_{\mathrm{L/K}}(s_{\mathrm{fin}}^{-1}),\mathrm{K}^{\infty}/\mathrm{K})]_{\mathrm{K}}\cdot[\mathrm{N}_{\mathrm{L/K}}(s_{\mathrm{fin}})]\\
&= [\mathrm{N}_{\mathrm{L/K}}(s_{\mathrm{fin}}^{-1})]_{\mathrm{K}}\cdot[\mathrm{N}_{\mathrm{L/K}}(s_{\mathrm{fin}})]\\
&= 1.
\end{aligned}$$

Therefore, $\rho_{\mathrm{E/L}}(\mathrm{I_L})\subset \ker([-]:(\mathrm{A}\otimes_{\mathrm{O_K}}\mathrm{K})^{\times}\to \mathrm{CL}_{\mathrm{O_K},\infty})=\mathrm{K}^{\times}$.

2.5.12 Proposition. — *Let* L/K *be a finite Galois extension,* E/L *a* CM *elliptic curve, v be a non-archimedian place of* $\mathrm{K}^{\mathrm{sep}}$ *lying over the primes* $\mathfrak{P}$ *of* $\mathrm{O_L}$ *and* $\mathfrak{p}$ *of* $\mathrm{O_K}$*, and let* $\mathrm{I}_v\subset \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{L})$ *be the inertia group at* v*. Then* $\rho_{\mathrm{E/L}}(\mathrm{I}_v)\subset \mathrm{O}_{\mathrm{K}}^{\times}\cdot\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}^{\times}\subset \mathrm{A}_{\mathrm{O_K}}^{\times}$ *and* E/L *has good reduction at* $\mathfrak{P}$ *if and only if* $\rho_{\mathrm{E/L}}(\mathrm{I}_v)\subset \mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}^{\times}$.

Proof. — The homomorphisms $\rho_{\mathrm{E/L}}$ and $[-]_{\mathrm{L}}$ both factor through $\mathrm{G}(\mathrm{L}^{\mathrm{ab}}/\mathrm{L})$ and we will denote the resulting homomorphisms by the same symbol. The image $[\mathrm{I}_v]_{\mathrm{L}}$ of the inertia group at v is equal to $[(\mathrm{O}_{\mathrm{L}_{\mathfrak{P}}}^{\times},\mathrm{L}^{\mathrm{ab}}/\mathrm{L})]_{\mathrm{L}}$ where $(-,\mathrm{L}^{\mathrm{ab}}/\mathrm{L}):\mathrm{C_L}\to\mathrm{G}(\mathrm{L}^{\mathrm{ab}}/\mathrm{L})$ is the global reciprocity map (1.3.3) and where $\mathrm{O}_{\mathrm{L}_{\mathfrak{P}}}^{\times}\subset \mathrm{I_L}/\mathrm{L}^{\times}=\mathrm{C_L}$.

As $[-]_{\mathrm{L}}=[-]_{\mathrm{K}}|_{\mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{L})}$, the compatibility of the reciprocity maps with the norm (1.3.4) shows that

$$[(\mathrm{O}_{\mathrm{L}_{\mathfrak{P}}}^{\times},\mathrm{L}^{\mathrm{ab}}/\mathrm{L})]_{\mathrm{L}}=[(\mathrm{N}_{\mathrm{L/K}}(\mathrm{O}_{\mathrm{L}_{\mathfrak{P}}}^{\times}),\mathrm{K}^{\mathrm{ab}}/\mathrm{K})]_{\mathrm{K}}\subset[(\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}^{\times},\mathrm{K}^{\mathrm{ab}}/\mathrm{K})]_{\mathrm{K}}.$$

By (iii) of (2.5.9) we have

$$[(\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}^{\times},\mathrm{K}^{\mathrm{ab}}/\mathrm{K})]_{\mathrm{K}}=[(\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}^{\times},\mathrm{K}^{\infty}/\mathrm{K})]_{\mathrm{K}}=[\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}^{\times}]\subset \mathrm{CL}_{\mathrm{O_K},\infty}.$$

This combined with the relation $[\rho_{\mathrm{E/L}}^{-1}]=[-]_{\mathrm{L}}$ and the fact that

$$\ker([-]:\mathrm{A}_{\mathrm{O_K}}^{\times}\to\mathrm{CL}_{\mathrm{O_K},\infty})=\mathrm{O}_{\mathrm{K}}^{\times}\subset\mathrm{A}_{\mathrm{O_K}}^{\times}$$

shows that $\rho_{\mathrm{E/L}}(\mathrm{I}_v)\subset \mathrm{O}_{\mathrm{K}}^{\times}\cdot\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}^{\times}$.

Now let ℓ be a rational prime such that $\ell\cdot\mathrm{O_K}$ is prime to $\mathfrak{p}$. Then the action of I_v on $\mathrm{E}[\ell^{\infty}](\mathrm{Spec}(\mathrm{L}^{\mathrm{sep}}))$ factors through the image of $\rho_{\mathrm{E/L}}(\mathrm{I}_v)$ under the projection $\mathrm{A}_{\mathrm{O_K}}^{\times}\to(\mathrm{O_K}\otimes_{\mathbf{Z}}\mathbf{Z}_{\ell})^{\times}$ and is trivial if and only if this image is trivial. As $\rho_{\mathrm{E/L}}(\mathrm{I}_v)\subset \mathrm{O}_{\mathrm{K}}^{\times}\cdot\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}^{\times}$ the image of this homomorphism is equal to $\rho(\mathrm{I}_v)\cap\mathrm{O}_{\mathrm{K}}^{\times}\subset(\mathrm{O_K}\otimes_{\mathbf{Z}}\mathbf{Z}_{\ell})^{\times}$ which is trivial if and only if $\rho_{\mathrm{E/L}}(\mathrm{I}_v)\subset\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}^{\times}$. We may now apply (2.1.16) to see that E/L has good reduction at v if and only if $\rho_{\mathrm{E/L}}(\mathrm{I}_v)\subset\mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}^{\times}$. □

2.5.13 Proposition. — *Let* L *be a finite Galois extension of* K *and let* E/L *a* CM *elliptic curve. If* $\mathrm{E}[\mathfrak{f}]$ *is a constant scheme over* $\mathrm{Spec}(\mathrm{L})$ *for some* $\mathfrak{f}$ *which separates units then* E/L *has good reduction everywhere.*

Proof. — If $\mathrm{E}[\mathfrak{f}]$ is constant then the action of $\mathrm{G}(\mathrm{L}^{\mathrm{sep}}/\mathrm{L})$ on $\mathrm{E}[\mathfrak{f}](\mathrm{Spec}(\mathrm{L}^{\mathrm{sep}}))$ is trivial and therefore $\rho_{\mathrm{E/L}}$ takes values in $\mathrm{A}_{\mathrm{O_K}}^{\times,\mathfrak{f}} \subset \mathrm{A}_{\mathrm{O_K}}^{\times}$. By (2.5.12), for each finite place v of $\mathrm{L}^{\mathrm{sep}}$ lying over the prime $\mathfrak{p}$ of $\mathrm{O_K}$, we have $\rho_{\mathrm{E/L}}(\mathrm{I}_v) \subset \mathrm{O_K^{\times}} \cdot \mathrm{O}_{\mathrm{K}_{\mathfrak{p}}^{\times}} \subset \mathrm{A}_{\mathrm{O_K}}^{\times}$. Combining these, we have

$$\rho_{\mathrm{E/L}}(\mathrm{I}_v) \subset (\mathrm{O_K^{\times}} \cdot \mathrm{O}_{\mathrm{K}_{\mathfrak{p}}^{\times}}) \cap \mathrm{A}_{\mathrm{O_K}}^{\times,\mathfrak{f}} \subset \mathrm{O_K^{\times,\mathfrak{f}}} \cdot \mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}^{\times}.$$

As $\mathfrak{f}$ separates units $\mathrm{O_K^{\times,\mathfrak{f}}} = \{1\}$ and so $\rho_{\mathrm{E/L}}(\mathrm{I}_v) \subset \mathrm{O}_{\mathrm{K}_{\mathfrak{p}}}^{\times}$. It now follows from (2.5.12) that E/L has good reduction at v. □

2.5.14 Example. — Let $\mathfrak{p}$ be a prime of $\mathrm{O_K}$ and let $\mathbf{F}_{\mathfrak{p}^n}$ be the unique extension of $\mathbf{F}_{\mathfrak{p}}$ of degree n. As $\mathrm{G}(\mathbf{F}_{\mathfrak{p}}^{\mathrm{sep}}/\mathbf{F}_{\mathfrak{p}^n}) \xrightarrow{\sim} \widehat{\mathbf{Z}}$ is topologically generated by the $\mathrm{N}\mathfrak{p}^n$-power Frobenius map, we see from (i) of (2.5.9) to give a continuous homomorphism

$$\rho : \mathrm{G}(\mathbf{F}_{\mathfrak{p}}^{\mathrm{sep}}/\mathbf{F}_{\mathfrak{p}^n}) \to \lim_{(\mathfrak{p},\mathfrak{f})=\mathrm{O_K}} (\mathrm{O_K}/\mathfrak{f})^{\times}$$

such that $[-]_{\mathbf{F}_{\mathfrak{p}^n}} = [\rho^{-1}]$ is the same as giving a generator $\rho(\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}) = \pi_n \in \mathrm{O_K}$ of the ideal $\mathfrak{p}^n$. The corresponding isogeny class of CM elliptic curves $\mathrm{E}/\mathrm{Spec}(\mathbf{F}_{\mathfrak{p}^n})$ are those with the property that the endomorphism

$$\pi_n : \mathrm{E} \to \mathrm{E}$$

is equal to the $\mathrm{N}\mathfrak{p}^n$-power Frobenius.

2.5.15 Example. — Let $\mathfrak{f}$ be an ideal that separates units and recall the isomorphism (1.4.8.1):

$$\mathrm{A}_{\mathrm{O_K}}^{\times,\mathfrak{f}} \xrightarrow{\sim} \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K}(\mathfrak{f})).$$

Now define

$$\rho^{-1} : \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K}(\mathfrak{f})) \to \mathrm{A}_{\mathrm{O_K}}^{\times}$$

to be the composition

$$\mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K}(\mathfrak{f})) \to \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K}(\mathfrak{f})) \xrightarrow{\sim} \mathrm{A}_{\mathrm{O_K}}^{\times,\mathfrak{f}} \to \mathrm{A}_{\mathrm{O_K}}^{\times}.$$

Then $[\rho^{-1}(-)] = [-]_{\mathrm{K}(\mathfrak{f})}$ and ρ corresponds to an isogeny class of CM elliptic curves $\mathrm{E}/\mathrm{Spec}(\mathrm{K}(\mathfrak{f}))$. These curves are distinguished by the fact that their $\mathfrak{f}$-torsion $\mathrm{E}[\mathfrak{f}]$ is constant and their study is the topic of the next section.

2.6. Moduli and level structures

In this section we define level-$\mathfrak{f}$ structures for CM elliptic curves (for each integral ideal $\mathfrak{f}$) and we show that the corresponding moduli stack $\mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})}$ admits a natural action of $\mathscr{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}$ under which it becomes a torsor (2.6.6). This induces an action of $\mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})}$ on the coarse sheaf $\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})}$ of $\mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})}$ and using this we prove that $\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})}$ is isomorphic to $\mathrm{Spec}(\mathrm{O}_{\mathrm{K}(\mathfrak{f})}[\mathfrak{f}^{-1}])$ compatibly with the isomorphism

$$\theta_{\mathrm{K},\mathfrak{f}} : \mathrm{CL}_{\mathrm{O_K}}^{(\mathfrak{f})} \xrightarrow{\sim} \mathrm{G}(\mathrm{K}(\mathfrak{f})/\mathrm{K})$$

of (1.4.7.3).

Most of the results contained in this section are probably more or less known, however they do not seem to have appeared in the literature and so we are happy to present a detailed account.

2.6.1. Let E/S be a CM elliptic curve and let $\mathfrak{f}$ be an integral ideal of $\mathrm{O_K}$. A level-$\mathfrak{f}$ structure on E/S is an isomorphism of $\underline{\mathrm{O_K}}_{\mathrm{S}}$-modules $\beta : \mathrm{E}[\mathfrak{f}] \xrightarrow{\sim} \underline{\mathrm{O_K}/\mathfrak{f}}_{\mathrm{S}}$. An $\mathfrak{f}$-isomorphism $(\mathrm{E}/\mathrm{S}, \beta) \to (\mathrm{E}'/\mathrm{S}, \beta')$ between CM elliptic curves with level-$\mathfrak{f}$ structures is an isomorphism $f : \mathrm{E} \to \mathrm{E}'$ such that $\beta' \circ f|_{\mathrm{E}[\mathfrak{f}]} = \beta$. We write $\mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})}$ for the moduli stack over $\mathrm{Sh}_{\mathrm{O_K}}$ whose fibre over an sheaf S is the category of CM elliptic curves with level-$\mathfrak{f}$ structures together with their $\mathfrak{f}$-isomorphisms and if $\mathfrak{f} = \mathrm{O_K}$ we identify $\mathscr{M}_{\mathrm{CM}}$ with $\mathscr{M}_{\mathrm{CM}}^{(\mathrm{O_K})}$. If $(\mathrm{E}/\mathrm{S}, \beta)$ is a CM elliptic curve with level-$\mathfrak{f}$ structure we shall often just denote it by E/S when the level-$\mathfrak{f}$ structure is clear (or at least does not need to be explicitly mentioned). We list the following (usual) constructions and properties of CM elliptic curves equipped with level-$\mathfrak{f}$ structures.

2.6.2 Remark. — (i) If (E, β) and (E', β') are a pair of CM elliptic curves equipped with level-$\mathfrak{f}$ structures then we equip the rank one $\mathrm{O_K}$-local system $\underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}')$ with the level-$\mathfrak{f}$ structure

$$\underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}') \to \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}[\mathfrak{f}], \mathrm{E}'[\mathfrak{f}]) \xrightarrow{\sim} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\underline{\mathrm{O_K}/\mathfrak{f}}_{\mathrm{S}}, \underline{\mathrm{O_K}/\mathfrak{f}}_{\mathrm{S}}) = \underline{\mathrm{O_K}/\mathfrak{f}}_{\mathrm{S}}$$

where the central isomorphism is

$$f \mapsto \alpha \circ f \circ \alpha'^{-1}.$$

(ii) If (E, β) and $(\mathscr{L}, \alpha)$ are a CM elliptic curve and rank one $\mathrm{O_K}$-local system over S with level-$\mathfrak{f}$ structures then we equip $\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}$ with the level-$\mathfrak{f}$ structure $\beta \otimes_{\mathrm{O_K}} \alpha$.

(iii) The sheaf of $\mathfrak{f}$-automorphisms $\underline{\mathrm{Aut}}_{\mathrm{S}}^{(\mathfrak{f})}(\mathrm{E})$ of a CM elliptic curve with level-$\mathfrak{f}$ structure $(\mathrm{E}/\mathrm{S}, \beta)$ is equal to $\underline{\mathrm{O_K^{\times,\mathfrak{f}}}}$. In particular, it is trivial if $\mathfrak{f}$ separates units.

(iv) The sheaf of $\mathfrak{f}$-isomorphisms $\underline{\mathrm{Isom}}_{\mathrm{S}}^{(\mathfrak{f})}(\mathrm{E}, \mathrm{E}')$ between two CM elliptic curves over S equipped with level-$\mathfrak{f}$ structures is finite and étale over S and E and E' are locally isomorphic if and only if $\underline{\mathrm{Isom}}_{\mathrm{S}}^{(\mathfrak{f})}(\mathrm{E}, \mathrm{E}')$ is an $\underline{\mathrm{O_K^{\times,\mathfrak{f}}}}_{\mathrm{S}}$-torsor.

(v) Given a CM elliptic curve E/S with level-$\mathfrak{f}$ structure $(\mathrm{E}/\mathrm{S}, \beta) \in \mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})}(\mathrm{S})$ the existence of the isomorphism $\beta : \mathrm{E}[\mathfrak{f}] \xrightarrow{\sim} \underline{\mathrm{O_K}/\mathfrak{f}}_{\mathrm{S}}$ implies that $\mathrm{E}[\mathfrak{f}]$ is étale over S. It follows from (2.2.11) that $\mathfrak{f}$ is invertible on S and that morphism $\mathrm{S} \to \mathrm{Spec}(\mathrm{O_K})$ factors through $\mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])$. In other words, the structure map $\mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})} \to \mathrm{Spec}(\mathrm{O_K})$ factors through $\mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}]) \to \mathrm{Spec}(\mathrm{O_K})$.

(vi) Let $\mathscr{E} \to \mathrm{Spec}(\mathrm{O_{K^{sep}}})$ be a CM elliptic curve (such a curve exists by (2.3.3)). Then

$$\mathrm{E}[\mathfrak{f}] \times_{\mathrm{Spec}(\mathrm{O_{K^{sep}}})} \mathrm{Spec}(\mathrm{O_{K^{sep}}}[\mathfrak{f}^{-1}])$$

is étale and constant over $\mathrm{Spec}(\mathrm{O_{K^{sep}}}[\mathfrak{f}^{-1}])$ and so admits a level-$\mathfrak{f}$ structure. Choosing such a structure one obtains a map $\mathrm{Spec}(\mathrm{O_{K^{sep}}}[\mathfrak{f}^{-1}]) \to \mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})}$. As $\mathrm{Spec}(\mathrm{O_{K^{sep}}}[\mathfrak{f}^{-1}]) \to \mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])$ is a cover, this shows that the structure map from (the coarse sheaf of) $\mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})}$ to $\mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])$ is an epimorphism.

(vii) If $\mathfrak{a}$ is a fractional ideal prime to $\mathfrak{f}$ then $\mathfrak{a}$ has a natural level-$\mathfrak{f}$ structure, coming from $\mathfrak{a} \to \mathfrak{a} \otimes_{\mathrm{O_K}} \mathrm{O_K}/\mathfrak{f} = \mathrm{O_K}/\mathfrak{f}$, and we just write $- \otimes_{\mathrm{O_K}} \mathfrak{a}$ for the corresponding auto-equivalence of $\mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})}$.

2.6.3. Using (ii) of (2.6.2) we can define a functor

$$\mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})} \times \mathscr{C}\mathscr{L}_{\mathrm{O_K}}^{(\mathfrak{f})} \to \mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})} : (\mathrm{E}/\mathrm{S}, \mathscr{L}/\mathrm{S}) \to \mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}/\mathrm{S}$$

(the level-$\mathfrak{f}$ structures are understood).

2.6.4 Proposition. — *Let* E, E' *be a pair of* CM *elliptic curves with level-*$\mathfrak{f}$ *structures over* S. *Then the evaluation map*

$$\mathrm{E} \otimes_{\mathrm{O_K}} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O_K}}(\mathrm{E}, \mathrm{E}') \xrightarrow{\sim} \mathrm{E}'$$

is an $\mathfrak{f}$*-isomorphism.*

Proof. — This is immediate from the definitions. □

2.6.5 Proposition. — *For each prime ideal* $\mathfrak{p}$ *prime to* $\mathfrak{f}$ *and each* $n \geq 0$ *there is a unique isomorphism of* $\mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})} \times \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}})$ *auto-equivalences* $\nu_{\mathfrak{p}^n} : -\otimes_{\mathrm{O_K}} \mathfrak{p}^{-n} \xrightarrow{\sim} \mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n *}(-)$ *such that for all* CM *elliptic curves* E *over* $\mathrm{Spec}(\mathbf{F}_{\mathfrak{p}})$*-sheaves* S *the diagram*

$$\begin{array}{ccc} & \mathrm{E} & \\ {\scriptstyle i_{\mathfrak{p}^n}}\swarrow & & \searrow{\scriptstyle \mathrm{Fr}_{\mathrm{E/S}}^{\mathrm{N}\mathfrak{p}^n}} \\ \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1} & \xrightarrow[\sim]{\nu_{\mathfrak{p}^n}} & \mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n *}(\mathrm{E}) \end{array}$$

commutes.

Proof. — We need only verify that the isomorphism $\nu_{\mathfrak{p}^n}(\mathrm{E}/\mathrm{S}) : \mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{p}^{-n} \xrightarrow{\sim} \mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n *}(\mathrm{S})$ of (2.2.13) is an $\mathfrak{f}$-isomorphism. However, the morphisms $i_{\mathfrak{p}^n}$ and $\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}_{\mathrm{E}/\mathrm{S}}$ induce isomorphisms on the $\mathfrak{f}$-torsion which are compatible with the level-$\mathfrak{f}$ structures on E, $\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{p}^{-n}$ and $\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n *}(\mathrm{E})$ so that as $\mathrm{Fr}^{\mathrm{N}\mathfrak{p}^n}_{\mathrm{E}/\mathrm{S}} = \nu_{\mathfrak{p}^n}\circ i_{\mathfrak{p}^n}$ it follows that $\nu_{\mathfrak{p}^n}(\mathrm{E}/\mathrm{S})$ is an $\mathfrak{f}$-isomorphism. □

2.6.6 Proposition. — *The functor*

$$\mathscr{M}^{(\mathfrak{f})}_{\mathrm{CM}}\times\mathscr{C}\mathscr{L}^{(\mathfrak{f})}_{\mathrm{O_K}} \to \mathscr{M}^{(\mathfrak{f})}_{\mathrm{CM}}\times\mathscr{M}^{(\mathfrak{f})}_{\mathrm{CM}} : (\mathrm{E},\mathscr{L}) \mapsto (\mathrm{E},\mathrm{E}\otimes_{\mathrm{O_K}}\mathscr{L})$$

is an equivalence of stacks and $\mathscr{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ is locally equivalent to $\mathscr{C}\mathscr{L}^{(\mathfrak{f})}_{\mathrm{O_K}}\times\mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])$.

Proof. — By (2.6.4) this functor is essentially surjective. Moreover, for all S the morphism

$$\underline{\mathrm{Isom}}^{(\mathfrak{f})}_{\mathrm{S}}(\mathrm{E},\mathrm{E}')\times_{\mathrm{S}}\underline{\mathrm{Isom}}^{(\mathfrak{f})}_{\mathrm{S}}(\mathscr{L},\mathscr{L}') \to \underline{\mathrm{Isom}}^{(\mathfrak{f})}_{\mathrm{S}}(\mathrm{E},\mathrm{E}')\times_{\mathrm{S}}\underline{\mathrm{Isom}}^{(\mathfrak{f})}_{\mathrm{S}}(\mathrm{E}\otimes_{\mathrm{O_K}}\mathscr{L},\mathrm{E}'\otimes_{\mathrm{O_K}}\mathscr{L}')$$

is an isomorphism of sheaves over S, as this can be checked on S sections. Indeed, if $\underline{\mathrm{Isom}}^{(\mathfrak{f})}_{\mathrm{S}}(\mathrm{E},\mathrm{E}')(\mathrm{S}) = \emptyset$ then it is clear and if $\underline{\mathrm{Isom}}^{(\mathfrak{f})}_{\mathrm{S}}(\mathrm{E},\mathrm{E}')(\mathrm{S}) \neq \emptyset$, we may assume that $\mathrm{E} = \mathrm{E}'$ and show instead that the map

$$\mathrm{Isom}^{(\mathfrak{f})}_{\mathrm{S}}(\mathscr{L},\mathscr{L}') \to \mathrm{Isom}^{(\mathfrak{f})}_{\mathrm{S}}(\mathrm{E}\otimes_{\mathrm{O_K}}\mathscr{L},\mathrm{E}\otimes_{\mathrm{O_K}}\mathscr{L}') : h \mapsto \mathrm{id}_{\mathrm{E}}\otimes h \qquad (2.6.6.1)$$

is bijective. The bijectivity of this map follows from (2.2.6) combined with the fact that an isomorphism $h : \mathscr{L} \to \mathscr{L}'$ induces an $\mathfrak{f}$-isomorphism $\mathrm{id}_{\mathrm{E}}\otimes_{\mathrm{O_K}} h : \mathrm{E}\otimes_{\mathrm{O_K}}\mathscr{L} \xrightarrow{\sim} \mathrm{E}\otimes_{\mathrm{O_K}}\mathscr{L}'$ if and only if h is an $\mathfrak{f}$-isomorphism. □

2.6.7. We now wish to compute the coarse sheaves $\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}} := \mathrm{C}(\mathscr{M}^{(\mathfrak{f})}_{\mathrm{CM}})$ of the stacks $\mathscr{M}^{(\mathfrak{f})}_{\mathrm{CM}}$. First let us define an action of

$$\underline{\mathrm{CL}}^{(\mathfrak{f})}_{\mathrm{O_K}}[\mathfrak{f}^{-1}] = \underline{\mathrm{CL}}^{(\mathfrak{f})}_{\mathrm{O_K}}\times\mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])$$

on $\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$. As this group is constant it is enough to define an action of $\mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}$ and then, using the isomorphism

$$\mathrm{Id}^{(\mathfrak{f})}_{\mathrm{O_K}}/\mathrm{Prin}^{(\mathfrak{f})}_{1\bmod\mathfrak{f}} \xrightarrow{\sim} \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}} : \mathfrak{a} \mapsto [\mathfrak{a}]_{\mathfrak{f}}$$

it is enough to define an action of $\mathrm{Id}^{(\mathfrak{f})}_{\mathrm{O_K}}$ with the property that $\mathrm{Prin}^{(\mathfrak{f})}_{1\bmod\mathfrak{f}}$ acts trivially. Each ideal $\mathfrak{a} \in \mathrm{Id}^{(\mathfrak{f})}_{\mathrm{O_K}}$, equipped with its standard level-$\mathfrak{f}$ structure induces an auto-equivalence

$$-\otimes_{\mathrm{O_K}}\mathfrak{a} : \mathscr{M}^{(\mathfrak{f})}_{\mathrm{CM}} \to \mathscr{M}^{(\mathfrak{f})}_{\mathrm{CM}}$$

and by the universal property of the coarse sheaf an automorphism $[\mathfrak{a}]_{\mathfrak{f}} : \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}} \to \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$. For $\mathfrak{a},\mathfrak{b} \in \mathrm{Id}^{(\mathfrak{f})}_{\mathrm{O_K}}$, the natural $\mathfrak{f}$-isomorphisms

$$(-\otimes_{\mathrm{O_K}}\mathfrak{a})\otimes_{\mathrm{O_K}}\mathfrak{b} \xrightarrow{\sim} -\otimes_{\mathrm{O_K}}\mathfrak{a}\mathfrak{b}$$

show that $[\mathfrak{b}]_\mathfrak{f} \circ [\mathfrak{a}]_\mathfrak{f} = [\mathfrak{a}\mathfrak{b}]_\mathfrak{f}$. We have $[\mathfrak{a}]_\mathfrak{f} = [\mathfrak{b}]_\mathfrak{f} \in \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}$ if and only if there exists an $\mathfrak{f}$-isomorphism $\mathfrak{a} \xrightarrow{\sim} \mathfrak{b}$, which in turn induces an isomorphism auto-equivalences

$$- \otimes_{\mathrm{O_K}} \mathfrak{a} \xrightarrow{\sim} - \otimes_{\mathrm{O_K}} \mathfrak{b}$$

and gives $[\mathfrak{a}]_\mathfrak{f} = [\mathfrak{b}]_\mathfrak{f} : \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}} \to \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ so that we have defined our action.

Moreover, by (2.6.5) it follows that for each prime $\mathfrak{p} \in \mathrm{Id}^{(\mathfrak{f})}_{\mathrm{O_K}}$ the pull-back of the automorphism

$$[\mathfrak{p}^{-1}]_\mathfrak{f} : \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}} \xrightarrow{\sim} \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$$

along $\mathrm{Spec}(\mathbf{F}_\mathfrak{p}) \to \mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])$ is equal to the $\mathrm{N}\mathfrak{p}$-power Frobenius

$$[\mathfrak{p}^{-1}]_\mathfrak{f} \times \mathrm{Spec}(\mathbf{F}_\mathfrak{p}) = \mathrm{Fr}^{\mathrm{N}\mathfrak{p}} : \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}} \times \mathrm{Spec}(\mathbf{F}_\mathfrak{p}) \xrightarrow{\sim} \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}} \times \mathrm{Spec}(\mathbf{F}_\mathfrak{p}) \quad (2.6.7.1)$$

2.6.8. If $(\mathrm{E}/\mathrm{S}, \beta)$ is a CM elliptic curve with level-$\mathfrak{f}$ structure then we write

$$c_{\mathrm{E/S},\mathfrak{f}} : \mathrm{S} \to \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$$

for the composition

$$\mathrm{S} \xrightarrow{(\mathrm{E},\beta)} \mathscr{M}^{(\mathfrak{f})}_{\mathrm{CM}} \xrightarrow{c^{\mathscr{M}^{(\mathfrak{f})}_{\mathrm{CM}}}} \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$$

(when $\mathfrak{f} = \mathrm{O_K}$ we drop the $\mathfrak{f}$). It follows from the definition of $\sigma_\mathfrak{a}$ that

$$c_{\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{a}/\mathrm{S},\mathfrak{f}} = \sigma_\mathfrak{a} \circ c_{\mathrm{E/S},\mathfrak{f}}. \quad (2.6.8.1)$$

2.6.9 Corollary. — (i) *The action of* $\underline{\mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}}[\mathfrak{f}^{-1}]$ *on* $\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ *makes it a torsor over* $\mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])$.

(ii) $\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ *is finite and étale over* $\mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])$.

(iii) *The action of* $\mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$ *on* $\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}(\mathrm{Spec}(\mathrm{K}^{\mathrm{sep}}))$ *is through the homomorphism*

$$\mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K}) \to \mathrm{G}(\mathrm{K}(\mathfrak{f})/\mathrm{K}) \xrightarrow{\theta_{\mathrm{K},\mathfrak{f}}} \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}} \subset \mathrm{Aut}_{\mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])}(\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}})$$

hence

$$\mathrm{Spec}(\mathrm{O}_{\mathrm{K}(\mathfrak{f})}[\mathfrak{f}^{-1}]) \xrightarrow{\sim} \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}.$$

Proof. — (i) To show that the action of $\underline{\mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}}[\mathfrak{f}^{-1}]$ is free it is enough to show that for each $[\mathfrak{a}]_\mathfrak{f} \in \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}$ the automorphism $[\mathfrak{a}]_\mathfrak{f} : \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}} \xrightarrow{\sim} \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ fixes a section $\mathrm{S} \to \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ if and only if $[\mathfrak{a}]_\mathfrak{f} = [\mathrm{O_K}]_\mathfrak{f}$. So let $[\mathfrak{a}]_\mathfrak{f} \in \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}$ fix a section $\mathrm{S} \to \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$. By the definition of the coarse sheaf, there exists a cover $\mathrm{S}' \to \mathrm{S}$ and a CM elliptic curve E/S' such that the induced map $\mathrm{S}' \to \mathrm{S} \to \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ is equal to $c_{\mathrm{E/S}',\mathfrak{f}}$. This section $c_{\mathrm{E/S}',\mathfrak{f}}$ is also fixed by $[\mathfrak{a}]_\mathfrak{f}$ which is now the statement that the two CM elliptic curves with level-$\mathfrak{f}$ structure E and $\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{a}$ are locally $\mathfrak{f}$-isomorphic over S'. After refining S', we may assume that E and $\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{a}$ are actually $\mathfrak{f}$-isomorphic which by (2.6.6) implies the existence of an $\mathfrak{f}$-isomorphism $\underline{\mathrm{O_K}}_{\mathrm{S}'} \xrightarrow{\sim} \underline{\mathfrak{a}}_{\mathrm{S}'}$. After refining S' again such an isomorphism

is constant and of the form $\underline{h}$ where $h : \mathrm{O_K} \to \mathfrak{a}$ is an $\mathfrak{f}$-isomorphism and it follows that $[\mathfrak{a}]_\mathfrak{f} = [\mathrm{O_K}]_\mathfrak{f}$.

Similarly, to show that the action of $\underline{\mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}}[\mathfrak{f}^{-1}]$ is transitive, it is enough to show that for each pair of sections $c_1, c_2 : \mathrm{S} \to \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ there is a cover $(\mathrm{S}_i \to \mathrm{S})_{i\in\mathrm{I}}$ and elements $[\mathfrak{a}_i]_\mathfrak{f} \in \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}$ such that $[\mathfrak{a}_i]_\mathfrak{f} \circ c_1|_{\mathrm{S}_i} = c_2|_{\mathrm{S}_i}$. Again by the definition of the coarse sheaf there exists a cover $\mathrm{S}' \to \mathrm{S}$ and CM elliptic curves E_1, E_2 over S such that the compositions $\mathrm{S}' \to \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ of c_1 and c_2 with $\mathrm{S}' \to \mathrm{S}$ are equal to $c_{\mathrm{E}_1/\mathrm{S},\mathfrak{f}}$ and $c_{\mathrm{E}_2/\mathrm{S},\mathfrak{f}}$. By (2.6.6) there exists an $\mathrm{O_K}$-local system $(\mathscr{L}, \alpha)$ with level-$\mathfrak{f}$ structure and an $\mathfrak{f}$-isomorphism

$$\mathrm{E}_1 \xrightarrow{\sim} \mathrm{E}_2 \otimes_{\mathrm{O_K}} \mathscr{L}.$$

After base change to a cover $(\mathrm{S}_i \to \mathrm{S})_{i\in\mathrm{I}}$ (the corresponding class of $\mathscr{L}$ may not be constant which is why our cover may consist of multiple elements) we may assume that $(\mathscr{L}, \alpha) = (\underline{\mathfrak{a}}_{\mathrm{S}'}, \underline{f}_{\mathrm{S}'})$ and it follows from (2.6.8.1) that $c_{\mathrm{E}_2/\mathrm{S},\mathfrak{f}} = [\mathfrak{a}]_\mathfrak{f} \circ c_{\mathrm{E}_1/\mathrm{S},\mathfrak{f}}$ and this proves the claim.

(ii) The fact that $\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ is finite and étale over $\mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])$ follows by descent, as $\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ is locally (over $\mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])$) isomorphic to $\underline{\mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}}[\mathfrak{f}^{-1}]$ by (i) and $\underline{\mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}}[\mathfrak{f}^{-1}]$ is finite and étale over $\mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])$.

(iii) For each prime $\mathfrak{p}$ prime to $\mathfrak{f}$, the automorphism $[\mathfrak{p}^{-1}]_\mathfrak{f} : \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}} \to \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ lifts the $\mathrm{N}\mathfrak{p}$-power Frobenius automorphism modulo $\mathfrak{p}$ (2.6.7.1). For any such automorphism (of any finite étale $\mathrm{Spec}(\mathrm{O_K}[\mathfrak{f}^{-1}])$-scheme) there exists an element $\sigma \in \mathrm{G}(\mathrm{K^{sep}}/\mathrm{K})$ such that

$$\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}(\sigma) = [\mathfrak{p}^{-1}]_\mathfrak{f}(\mathrm{Spec}(\mathrm{K^{sep}})) : \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}(\mathrm{Spec}(\mathrm{K^{sep}})) \to \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}(\mathrm{Spec}(\mathrm{K^{sep}})).$$

However, the action of $\mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}$ on $\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}(\mathrm{Spec}(\mathrm{K^{sep}}))$ is transitive by (i), and $\mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}$ is generated by elements of the form $[\mathfrak{p}^{-1}]_\mathfrak{f}$ and so it follows that the action $\mathrm{G}(\mathrm{K^{sep}}/\mathrm{K})$ on $\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}(\mathrm{Spec}(\mathrm{K^{sep}}))$ is transitive. Therefore $\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ is connected and isomorphic to $\mathrm{Spec}(\mathrm{O_L}[\mathfrak{f}^{-1}])$ for some finite extension L/K which is unramified away from $\mathfrak{f}$. By construction, the isomorphism $\mathrm{G}(\mathrm{L}/\mathrm{K}) \to \mathrm{CL}^{(\mathfrak{f})}_{\mathrm{O_K}}$ sends the Frobenius element $\sigma_{\mathrm{L}/\mathrm{K},\mathfrak{p}}$ to $[\mathfrak{p}^{-1}]_\mathfrak{f}$ and it follows that $\mathrm{L} \xrightarrow{\sim} \mathrm{K}(\mathfrak{f})$ (cf. (1.4.7.3)). □

2.6.10 Remark. — We list the following consequences of (2.6.9).

(a) The coarse sheaf $\mathrm{M_{CM}}$ of $\mathscr{M}_{\mathrm{CM}}$ is isomorphic to $\mathrm{Spec}(\mathrm{O_H})$ where H is the Hilbert class field of K. This recovers the fact the j-invariants of CM elliptic curves defined over extensions of K lie in $\mathrm{H} \subset \mathrm{L}$.

(b) Let $\mathrm{E} \to \mathrm{S}$ be any CM elliptic curve and recall that

$$c_{\mathrm{E/S}} : \mathrm{S} \to \mathrm{M_{CM}}$$

denotes the morphism

$$\mathrm{S} \xrightarrow{\mathrm{E}} \mathscr{M}_{\mathrm{CM}} \xrightarrow{c_{\mathscr{M}_{\mathrm{CM}}}} \mathrm{M_{CM}}.$$

Then by definition, if E' is another CM elliptic curve over S then $c_{\mathrm{E}/\mathrm{S}}, c_{\mathrm{E}'/\mathrm{S}} : \mathrm{S} \to \mathrm{M}_{\mathrm{CM}}$ are equal if and only if E and E' are locally isomorphic. Combining this with (2.4.3) and (2.5.8), we find that if $\mathrm{S} = \mathrm{Spec}(\mathrm{F})$ for F a field then the map

$$\mathrm{E}/\mathrm{F} \mapsto (\rho_{\mathrm{E}/\mathrm{F}}, c_{\mathrm{E}/\mathrm{F}})$$

defines a bijection between the set of isomorphism classes of CM elliptic curves over $\mathrm{E}/\mathrm{Spec}(\mathrm{F})$ with the set of pairs (ρ, c) where:

(i) $\rho : \mathrm{G}(\mathrm{F}^{\mathrm{sep}}/\mathrm{F}) \to \lim_{\mathfrak{f}}(\mathrm{O}_{\mathrm{K}}/\mathfrak{f})^{\times}$ is a homomorphism such that $[\rho^{-1}] = [-]_{\mathrm{F}}$, and

(ii) $c : \mathrm{Spec}(\mathrm{L}) \to \mathrm{M}_{\mathrm{CM}}$ is any map.

(c) If $\mathfrak{f}$ separates units then $\mathscr{M}_{\mathrm{CM}}^{(\mathfrak{f})} \xrightarrow{\sim} \mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})} \xrightarrow{\sim} \mathrm{Spec}(\mathrm{O}_{\mathrm{K}(\mathfrak{f})}[\mathfrak{f}^{-1}])$. If $\mathrm{E}/\mathrm{Spec}(\mathrm{K}(\mathfrak{f}))$ denotes the generic fibre of the universal CM elliptic curve with level-$\mathfrak{f}$ structure the homomorphism

$$\rho_{\mathrm{E}/\mathrm{K}(\mathfrak{f})} : \mathrm{G}(\mathrm{K}(\mathfrak{f})^{\mathrm{sep}}/\mathrm{K}(\mathfrak{f})) \to \mathrm{A}_{\mathrm{O}_{\mathrm{K}}}^{\times}$$

is equal to (cf. (1.4.8.1))

$$\mathrm{G}(\mathrm{K}(\mathfrak{f})^{\mathrm{sep}}/\mathrm{K}(\mathfrak{f})) \xrightarrow{-|_{\mathrm{K}^{\infty}}} \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{K}(\mathfrak{f})) \xrightarrow{\sim} \mathrm{A}_{\mathrm{O}_{\mathrm{K}}}^{\times,\mathrm{f}} \xrightarrow{\mathrm{incl}} \mathrm{A}_{\mathrm{O}_{\mathrm{K}}}^{\times}.$$

CHAPTER 3

Λ-STRUCTURES, WITT VECTORS AND ARITHMETIC JETS

In this chapter we give a brief introduction to, and overview of, the theory Λ-structures, Witt vectors and arithmetic jet spaces following the approach of Borger [**4**], [**5**]. It is by nature a technical and notationally heavy theory, but its many applications make it a worthwhile subject. The two papers mentioned are both an excellent introduction and general reference and we encourage to the reader to consult them. We give here really only the minimal set up necessary for our applications in Chapter 4 and proofs are given only where they cannot be cited or where it would be perhaps enlightening.

In the final section we prove a small new result which shows that Λ-structures on relative abelian schemes are determined by their underlying Ψ-structures.

3.1. Plethories

3.1.1. Fix a pair of rings O and O′. An O-O′-biring Φ is an O-algebra together the structure of an O′-algebra on the set $\mathrm{Hom}_{\mathrm{O}}(\Phi, \mathrm{A})$ which is functorial in the O-algebra A. This is structure is determined by certain homomorphisms

(i) coaddition and comultiplication: $\Delta^{+}_{\Phi}, \Delta^{\times}_{\Phi} : \Phi \to \Phi \otimes_{\mathrm{O}} \Phi$
(ii) coadditive and comultiplicative units: $\epsilon^{+}_{\Phi}, \epsilon^{\times}_{\Phi} : \Phi \to \mathrm{O}$
(iii) O′ coaction: $\mathrm{O}' \to \mathrm{End}_{\mathrm{O}}(\Phi) : s \mapsto s_{\Phi}$

satisfying various identities (cocommutativity of the coaddition and comultiplication, coassociativity and so on).

We denote by $\mathrm{Biring}_{\mathrm{O},\mathrm{O}'}$ the category whose objects are O-O′-birings and whose morphisms are those O-homomorphisms $\Phi \to \Phi'$ inducing functorial homomorphisms of O′-algebras $\mathrm{Hom}_{\mathrm{O}}(\Phi', \mathrm{A}) \to \mathrm{Hom}_{\mathrm{O}}(\Phi', \mathrm{A})$. Of course, this is equivalent to the homomorphism $\Phi \to \Phi'$ being 'compatible' with the maps Δ^{+}_{Φ}, $\Delta^{+}_{\Phi'}$ and so on.

3.1.2. The functor corepresented by a biring Φ:

$$\mathrm{A} \mapsto \mathrm{Hom}_{\mathrm{O}}(\Phi, \mathrm{A}) : \mathrm{Alg}_{\mathrm{O}} \to \mathrm{Alg}_{\mathrm{O}'}$$

admits a left adjoint, which we denote by $\mathrm{B} \mapsto \Phi \odot_{\mathrm{O}'} \mathrm{B}$, which is defined as follows: $\Phi \odot_{\mathrm{O}'} \mathrm{B}$ is the quotient of the free O-polynomial algebra generated by the symbols $\phi \odot b$ for $\phi \in \Phi$ and $b \in \mathrm{B}$ subject to the relations

$$(\phi + \phi') \odot b = \phi \odot b + \phi' \odot b, \quad \phi\phi' \odot b = (\phi \odot b)(\phi' \odot b), \quad (r\phi) \odot b = r(\phi \odot b)$$

and

$$\phi \odot (b + b') = \Delta^{+}_{\Phi}(\phi)(b, b')^{(1)}, \quad \phi \odot bb' = \Delta^{\times}_{\Phi}(\phi)(b, b'), \quad \phi \odot sb = s_{\Phi}(\phi) \odot b$$

for all $\phi, \phi' \in \Phi$, $b, b' \in \mathrm{B}$, $r \in \mathrm{O}$ and $s \in \mathrm{O}'$. The O-algebra $\Phi \odot_{\mathrm{O}'} \mathrm{B}$ is called composition product of Φ with B.

3.1.3. If Φ is an O-O′-biring and $\mathrm{O} \to \mathrm{O}''$ is a homomorphism then $\Phi \otimes_{\mathrm{O}} \mathrm{O}''$ is an O″-O′-biring and $(\Phi \odot_{\mathrm{O}'} \mathrm{B}) \otimes_{\mathrm{O}} \mathrm{O}'' = (\Phi \otimes_{\mathrm{O}} \mathrm{O}'') \odot_{\mathrm{O}'} \mathrm{B}$. The functor $\mathrm{Biring}_{\mathrm{O},\mathrm{O}'} \times \mathrm{Alg}_{\mathrm{O}'} \to \mathrm{Alg}_{\mathrm{O}} : (\Phi, \mathrm{B}) \to \Phi \odot_{\mathrm{O}'} \mathrm{B}$ commutes with colimits in each variable. We give the two simplest examples when $\mathrm{O} = \mathrm{O}'$.

(i) The functor $\mathrm{A} \mapsto \mathrm{A}$ is represented by the O-O-biring $\mathrm{O}[e]$.
(ii) Even simpler is the functor $\mathrm{A} \mapsto 0$ represented by the O-O-biring O itself.

3.1.4. We now concentrate on the case $\mathrm{O} = \mathrm{O}'$ and just call an O-O-biring an O-biring and shall drop O from the notation when there is no risk of confusion. If Φ and Φ' are two O-birings then we may consider the composition product $\Phi \odot \Phi'$ which, using the standard properties of adjunctions, is again an O-biring. The composition product then defines a monoidal structure on the category of O-birings with identity $\mathrm{O}[e]$. The functor

$$\Phi \mapsto \Phi \odot -$$

from O-birings to endofunctors on $\mathrm{Alg}_{\mathrm{O}}$ is monoidal and fully faithful.

3.1.5. An O-plethory is an O-biring Φ together with the structure of a monad on the functor $\mathrm{A} \mapsto \Phi \odot \mathrm{A}$ or equivalently a comonad on the functor $\mathrm{A} \mapsto \mathrm{Hom}_{\mathrm{O}}(\Phi, \mathrm{A})$. The remarks in (3.1.4) then show that to give the functor $\mathrm{A} \mapsto \Phi \odot \mathrm{A}$ the structure of a monad is equivalent to giving

(i) a homomorphism of O-birings $i_{\Phi} : \mathrm{O}[e] \to \Phi$ and
(ii) a homomorphism of O-birings $h_{\Phi} : \Phi \odot \Phi \to \Phi$

such that

$$h_{\Phi} \circ (\Phi \odot i_{\Phi}) = h_{\Phi} \circ (i_{\Phi} \odot \Phi) = \mathrm{id}_{\Phi} \quad \text{and} \quad h_{\Phi} \circ (\Phi \odot h_{\Phi}) = h_{\Phi} \circ (h_{\Phi} \odot \Phi).$$

(1) This notation means that if $\Delta^{+}_{\Phi}(\phi) = \sum_i \phi_i \otimes \phi'_i$ then $\Delta^{+}_{\Phi}(\phi)(b, b') = \sum_i (\phi_i \odot b_i)(\phi'_i \odot b'_i)$ and similarly for $\Delta^{\times}_{\Phi}(b, b')$.

3.1.6. If Φ is an O-plethory we define a Φ-ring to be an O-algebra A equipped with an action of the monad $\Phi \odot -$. Given a Φ-ring A we denote by

$$h_{\mathrm{A}} : \Phi \odot \mathrm{A} \to \mathrm{A}$$

the map defining the Φ-ring structure on A. We denote the category of Φ-rings and compatible morphisms by $\mathrm{Alg}_{\mathrm{O}}^{\Phi}$. If A is an O-algebra then $\Phi \odot \mathrm{A}$ and $\mathrm{Hom}_{\mathrm{O}}(\Phi, \mathrm{A})$ are Φ-rings and these two functors are the left and right adjoints of the forgetful functor $\mathrm{Alg}_{\mathrm{O}}^{\Phi} \to \mathrm{Alg}$. We have the diagram of functors, each one left adjoint to the one below it:

$$\mathrm{Alg}_{\mathrm{O}}^{\Phi} \underset{\mathrm{Hom}_{\mathrm{O}}(\Phi,-)}{\overset{\Phi\odot_{\mathrm{O}}-}{\underset{\text{forget}}{\rightleftarrows}}} \mathrm{Alg}_{\mathrm{O}}.$$

3.2. Witt vectors and arithmetic jets I

3.2.1. During §§3.2–3.4 we fix a Dedekind domain O with finite residue fields and $\mathrm{P} \subset \mathrm{Id}_{\mathrm{O}}$ a sub-monoid generated by some set of prime ideals of O and we write K for the fraction field of O. Note that we allow Dedekind domains of finite characteristic, e.g. $\mathrm{O} = \mathbf{F}_p[\mathrm{T}]$.

3.2.2. Denote by Ψ the free polynomial O-algebra generated by the symbols $\psi^{\mathfrak{a}}$ for $\mathfrak{a} \in \mathrm{P}$. We make Ψ an O-biring by equipping the set

$$\mathrm{Hom}_{\mathrm{O}}(\Psi, \mathrm{A}) = \mathrm{Hom}_{\mathrm{O}}(\mathrm{O}[\psi^{\mathfrak{a}} : \mathfrak{a} \in \mathrm{P}], \mathrm{A}) \xrightarrow{\sim} \prod_{\mathfrak{a}\in\mathrm{P}} \mathrm{A} : f \mapsto (f(\psi^{\mathfrak{a}}))_{\mathfrak{a}\in\mathrm{P}}$$

with the product O-algebra structure. We then give Ψ the structure of an O-plethory by setting

$$i_{\Psi} : \mathrm{O}[e] \to \Psi : e \mapsto \psi^{(1)} \quad \text{and} \quad h_{\Psi} : \Psi \odot \Psi \to \Psi : \psi^{\mathfrak{a}} \odot \psi^{\mathfrak{b}} \mapsto \psi^{\mathfrak{a}\mathfrak{b}}.$$

3.2.3. For each ring A we write $\Gamma(\mathrm{A})$ for the ring

$$\Gamma(\mathrm{A}) := \mathrm{Hom}_{\mathrm{O}}(\Psi, \mathrm{A}) = \prod_{\mathfrak{a}\in\mathrm{P}} \mathrm{A}$$

and call it the ring of ghost vectors of A. We define the ghost jets of a ring A to be the ring

$$\Psi \odot_{\mathrm{O}} \mathrm{A}.$$

Let us examine a little more the ring of ghost jets $\Psi \odot_{\mathrm{O}} \mathrm{A}$ of a ring A and what it means for A to be a Ψ-ring.

Recall (3.1.2) that if A is an O-algebra then $\Psi \odot_{\mathrm{O}} \mathrm{A}$ is given by the quotient of the O-polynomial algebra

$$\mathrm{O}[\psi^{\mathfrak{a}} \odot a : \mathfrak{a} \in \mathrm{P}, a \in \mathrm{A}]$$

by the ideal generated by the elements of the following form

$$\psi^{\mathfrak{a}} \odot (a+b) - \psi^{\mathfrak{a}} \odot a - \psi^{\mathfrak{a}} \odot b$$
$$\psi^{\mathfrak{a}} \odot (ab) - (\psi^{\mathfrak{a}} \odot a)(\psi^{\mathfrak{a}} \odot b)$$
$$\psi^{\mathfrak{a}} \odot (ra) - r(\psi^{\mathfrak{a}} \odot a)$$

for $a, b \in \mathrm{A}$, $r \in \mathrm{O}$. Now to give A the structure of a Ψ-ring is the same as giving an O-homomorphism

$$h_{\mathrm{A}} : \Psi \odot_{\mathrm{O}} \mathrm{A} \to \mathrm{A}$$

satisfying certain properties. In this case, the properties which must be satisfied are equivalent to the following:

(i) for each $\mathfrak{a} \in \mathrm{P}$ the map $\psi^{\mathfrak{a}}_{\mathrm{A}} : \mathrm{A} \to \mathrm{A}$ defined by $a \mapsto h_{\mathrm{A}}(\psi^{\mathfrak{a}} \odot a)$ is an O-algebra homomorphism,
(ii) for each $\mathfrak{a}, \mathfrak{b} \in \mathrm{P}$ we have $\psi^{\mathfrak{a}}_{\mathrm{A}} \circ \psi^{\mathfrak{b}}_{\mathrm{A}} = \psi^{\mathfrak{b}}_{\mathrm{A}} \circ \psi^{\mathfrak{a}}_{\mathrm{A}} = \psi^{\mathfrak{a}\mathfrak{b}}_{\mathrm{A}}$, and
(iii) we have $\psi^{(1)}_{\mathrm{A}} = \mathrm{id}_{\mathrm{A}} : \mathrm{A} \to \mathrm{A}$.

We see that if A is a Ψ-ring then A has an action of the monoid P where $\mathfrak{a} \in \mathrm{P}$ acts by $\psi^{\mathfrak{a}}_{\mathrm{A}} : \mathrm{A} \to \mathrm{A}$. This sets up a bijection between Ψ-ring structures on A and actions of P on A. Given a Ψ-ring we will write $\psi^{\mathfrak{a}}_{\mathrm{A}} : \mathrm{A} \to \mathrm{A}$ for the corresponding P-action. In particular, the Ψ-ring Ψ itself has the P-action

$$\psi^{\mathfrak{a}}_{\Psi} : \psi^{\mathfrak{b}} \mapsto \psi^{\mathfrak{a}\mathfrak{b}}$$

for $\mathfrak{a}, \mathfrak{b} \in \mathrm{P}$. Note that the Ψ-ring structure on O is given by

$$\psi^{\mathfrak{a}}_{\mathrm{O}} = \mathrm{id}_{\mathrm{O}} : \mathrm{O} \to \mathrm{O}.$$

3.2.4. As we are dealing with rings equipped with endomorphisms, it will be useful here to say a little about semi-linear self maps versus twisted linear maps. The example to have in mind is the following: if A is a ring of characteristic p and $\mathrm{A} \to \mathrm{B}$ is an A-algebra then the p-power Frobenius

$$\mathrm{Fr}^p_{\mathrm{B}} : \mathrm{B} \to \mathrm{B} : b \mapsto b^p$$

is $\mathrm{Fr}^p_{\mathrm{A}}$-linear where $\mathrm{Fr}^p_{\mathrm{A}} : \mathrm{A} \to \mathrm{A} : a \mapsto a^p$ is the p-power Frobenius of A. This then induces an A-linear map, the relative p-power Frobenius, $\mathrm{Fr}^p_{\mathrm{B/A}} : \mathrm{Fr}^{p*}_{\mathrm{A}}(\mathrm{B}) \to \mathrm{B}$.

Now, a morphism of Ψ-rings $f : \mathrm{A} \to \mathrm{B}$ is just a homomorphism such that the diagram

$$\begin{array}{ccc} \mathrm{A} & \xrightarrow{\psi^{\mathfrak{a}}_{\mathrm{A}}} & \mathrm{A} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ \mathrm{B} & \xrightarrow{\psi^{\mathfrak{a}}_{\mathrm{B}}} & \mathrm{B} \end{array}$$

commutes for all $\mathfrak{a} \in \mathrm{P}$. Viewing B as an A-algebra via f, the homomorphism $\psi_{\mathrm{B}}^{\mathfrak{a}} : \mathrm{B} \to \mathrm{B}$ is $\psi_{\mathrm{A}}^{\mathfrak{a}}$-linear and induces an A-linear map

$$\psi_{\mathrm{B/A}}^{\mathfrak{a}} : \psi_{\mathrm{A}}^{\mathfrak{a}*}(\mathrm{B}) \to \mathrm{B}.$$

That the homomorphisms $\psi_{\mathrm{B}}^{\mathfrak{a}}$ for $\mathfrak{a} \in \mathrm{P}$ commute is now expressed by the condition that for all $\mathfrak{a}, \mathfrak{b} \in \mathrm{P}$ we have

$$\psi_{\mathrm{B/A}}^{\mathfrak{b}} \circ \psi_{\mathrm{A}}^{\mathfrak{a}*}(\psi_{\mathrm{B/A}}^{\mathfrak{b}}) = \psi_{\mathrm{B/A}}^{\mathfrak{a}} \circ \psi_{\mathrm{A}}^{\mathfrak{b}*}(\psi_{\mathrm{B/A}}^{\mathfrak{a}}) = \psi_{\mathrm{B/A}}^{\mathfrak{ab}} \tag{3.2.4.1}$$

or in a commutative diagram:

$$\begin{array}{ccc} \psi_{\mathrm{A}}^{\mathfrak{ab}*}(\mathrm{B}) & \xrightarrow{\psi_{\mathrm{A}}^{\mathfrak{b}*}(\psi_{\mathrm{B/A}}^{\mathfrak{a}})} & \psi_{\mathrm{A}}^{*\mathfrak{a}}(\mathrm{B}) \\ \Big\downarrow{\scriptstyle \psi_{\mathrm{A}}^{\mathfrak{a}*}(\psi_{\mathrm{B/A}}^{\mathfrak{b}})} & & \Big\downarrow{\scriptstyle \psi_{\mathrm{B/A}}^{\mathfrak{a}}} \\ \psi_{\mathrm{A}}^{*\mathfrak{b}}(\mathrm{B}) & \xrightarrow{\psi_{\mathrm{B/A}}^{\mathfrak{b}}} & \mathrm{B}. \end{array}$$

Moreover, if A is a Ψ-ring and $\mathrm{A} \to \mathrm{B}$ is an A-algebra then to give B the structure of Ψ-ring such that $\mathrm{A} \to \mathrm{B}$ is a Ψ-homomorphism is the same as giving maps $\psi_{\mathrm{B/A}}^{\mathfrak{a}} : \psi_{\mathrm{A}}^{\mathfrak{a}*}(\mathrm{B}) \to \mathrm{B}$ for each $\mathfrak{a} \in \mathrm{P}$ such that $\psi_{\mathrm{B/A}}^{(1)} = \mathrm{id}_{\mathrm{B}}$ and which satisfy the commutativity condition (3.2.4.1). The category of Ψ-rings over a Ψ-ring A is denoted $\mathrm{Alg}_{\Psi_{\mathrm{A}}}$ and its objects called Ψ_{A}-rings.

3.2.5. We now come to the matter of interest which is lifting the Frobenius. We wish to impose on a Ψ-ring A the condition that the homomorphisms $\psi_{\mathrm{A}}^{\mathfrak{p}} : \mathrm{A} \to \mathrm{A}$, for $\mathfrak{p} \in \mathrm{P}$ prime, be lifts of the $\mathrm{N}\mathfrak{p}$-power Frobenius endomorphism (recall that $\mathrm{N}\mathfrak{p} = \#\mathbf{F}_{\mathfrak{p}}$):

$$\psi_{\mathrm{A}}^{\mathfrak{p}}(a) = a^{\mathrm{N}\mathfrak{p}} \bmod \mathfrak{p}\mathrm{A} \tag{3.2.5.1}$$

This is done by enlarging the plethory Ψ in such a way that the endomorphisms corresponding to the elements $\psi_{\mathfrak{p}} \in \Psi$, for each prime $\mathfrak{p} \in \mathrm{P}$, will be forced to satisfy the relation (3.2.5.1).

So for each integer $n \geq 0$ define sub-O-algebras $\Lambda_n \subset \Psi \otimes_{\mathrm{O}} \mathrm{K}$ inductively by setting $\Lambda_0 = \Psi$, and for $n \geq 0$, setting Λ_{n+1} to be the sub-Λ_n-algebra of $\Psi \otimes_{\mathrm{O}} \mathrm{K}$ generated by the subsets

$$\mathfrak{p}^{-1}(f^{\mathrm{N}\mathfrak{p}} - \psi_{\Psi}^{\mathfrak{p}}(f)) \subset \Psi \otimes_{\mathrm{O}} \mathrm{K} \tag{3.2.5.2}$$

for $\mathfrak{p} \in \mathrm{P}$ a prime ideal and $f \in \Lambda_n$. Finally, we set

$$\Lambda = \cup_{n \geq 0} \Lambda_n \subset \Psi \otimes_{\mathrm{O}} \mathrm{K}.$$

Then $\Lambda_n \subset \Psi \otimes_{\mathrm{O}} \mathrm{K}$ is stabilised by the endomorphisms $\psi_{\Psi}^{\mathfrak{a}}$ of $\Psi \otimes_{\mathrm{O}} \mathrm{K}$ for each $\mathfrak{a} \in \mathrm{P}$, as is $\Lambda \subset \Psi \otimes_{\mathrm{R}} \mathrm{K}$. Thus Λ_n and Λ admit unique Ψ-ring structures such that $\Psi \subset \Lambda_n \subset \Lambda$ are Ψ-morphisms. Moreover, for each $n \geq 0$, and each $f \in \Lambda_n$ it follows from the definition (3.2.5.2) of Λ_{n+1} that

$$\psi_{\Lambda}^{\mathfrak{p}}(f) = f^{\mathrm{N}\mathfrak{p}} \bmod \mathfrak{p}\Lambda_{n+1}$$

and hence for all $f \in \cup_{n\geq 0}\Lambda_n = \Lambda$ we have

$$\psi^{\mathfrak{p}}_{\Lambda}(f) = f^{\mathrm{N}\mathfrak{p}} \bmod \mathfrak{p}\Lambda.$$

3.2.6 Proposition. — *There is a unique* O*-plethory structure on* Λ *such that the inclusion* $\Psi \to \Lambda$ *is a morphism of* O*-plethories.*

3.2.7 Remark. — Before we examine exactly what a Λ-ring is, the fact that $\Psi \to \Lambda$ is a morphism of O-plethories implies that every Λ-ring A inherits a Ψ-ring structure and hence a family of endomorphisms $\psi^{\mathfrak{a}}_{\mathrm{A}} : \mathrm{A} \to \mathrm{A}$ for each $\mathfrak{a} \in \mathrm{P}$ such that $\psi_{(1)} = \mathrm{id}_{\mathrm{A}}$ and $\psi^{\mathfrak{a}\mathfrak{b}}_{\mathrm{A}} = \psi^{\mathfrak{a}}_{\mathrm{A}} \circ \psi^{\mathfrak{b}}_{\mathrm{A}}$ for all $\mathfrak{a}, \mathfrak{b} \in \mathrm{P}$.

3.2.8 Proposition. — *Let* A *be an* O*-algebra. We have the following:*

(i) *If* A *is a* Λ*-ring the endomorphism* $\psi^{\mathfrak{p}}_{\mathrm{A}} : \mathrm{A} \to \mathrm{A}$ *satisfies*

$$\psi^{\mathfrak{p}}_{\mathrm{A}}(a) = a^{\mathrm{N}\mathfrak{p}} \bmod \mathfrak{p}\mathrm{A}$$

for each maximal ideal $\mathfrak{p} \in \mathrm{P}$.

(ii) *If* A *is a* Ψ*-ring and* $\mathfrak{p}$*-torsion free for each prime* $\mathfrak{p} \in \mathrm{P}$ *(i.e. flat at* $\mathfrak{p}$ *for each prime* $\mathfrak{p} \in \mathrm{P}$*) then the given* Ψ*-structure comes from a* Λ*-structure if and only if for each prime ideal* $\mathfrak{p} \in \mathrm{P}$ *the endomorphism* $\psi^{\mathfrak{p}}_{\mathrm{A}} : \mathrm{A} \to \mathrm{A}$ *lifts the* N$\mathfrak{p}$*-power Frobenius*

$$\psi^{\mathfrak{p}}_{\mathrm{A}}(a) = a^{\mathrm{N}\mathfrak{p}} \bmod \mathfrak{p}\mathrm{A}.$$

In this case the Λ*-structure inducing the* Ψ*-structure is unique.*

(iii) *If each* $\mathfrak{p} \in \mathrm{P}$ *is invertible in* A *then every* Ψ*-structure on* A *is induced by a unique* Λ*-structure.*

Proof. — (i) and (ii) are (essentially) the definition of Λ-ring given in [**4**]. In particular, see §§1.6–1.19 [**4**].

(iii) If each P in A is invertible any endomorphism $\psi^{\mathfrak{p}}_{\mathrm{A}} : \mathrm{A} \to \mathrm{A}$ lifts the N$\mathfrak{p}$-power Frobenius (trivially) and so this follows from (i) and (ii). □

3.2.9 Remark. — We point out that if $\mathrm{A} \to \mathrm{B}$ is a homomorphism of Λ-rings then $\psi^{\mathfrak{p}}_{\mathrm{A}} = \mathrm{Fr}^{\mathrm{N}\mathfrak{p}}_{\mathrm{A}_{\mathfrak{p}}} \bmod \mathfrak{p}\mathrm{A}$ and the relative morphisms $\psi^{\mathfrak{p}}_{\mathrm{B}/\mathrm{A}} : \psi^{\mathfrak{p}*}_{\mathrm{A}}(\mathrm{B}) \to \mathrm{B}$ are now lifts of the relative N$\mathfrak{p}$-power Frobenius:

$$\psi^{\mathfrak{p}}_{\mathrm{B}/\mathrm{A}} = \mathrm{Fr}^{\mathrm{N}\mathfrak{p}}_{\mathrm{B}_{\mathfrak{p}}/\mathrm{A}_{\mathfrak{p}}} : \mathrm{Fr}^{\mathrm{N}\mathfrak{p}*}_{\mathrm{A}_{\mathfrak{p}}}(\mathrm{B}_{\mathfrak{p}}) \to \mathrm{B}_{\mathfrak{p}}$$

where we write $\mathrm{A}_{\mathfrak{p}} = \mathrm{A} \otimes_{\mathrm{O}} \mathbf{F}_{\mathfrak{p}}$ and $\mathrm{B}_{\mathfrak{p}} = \mathrm{B} \otimes_{\mathrm{O}} \mathbf{F}_{\mathfrak{p}}$.

3.2.10 Example. — Using (3.2.8) we are now able to give the first examples of Λ-rings:

(i) Of course O is always a Λ-ring with $\psi^{\mathfrak{a}}_{\mathrm{O}} : \mathrm{O} \to \mathrm{O}$ equal to the identity. The fact that $\psi^{\mathfrak{p}}_{\mathrm{O}}$ lifts the N$\mathfrak{p}$-power Frobenius is then Fermat's little theorem:

$$\psi^{\mathfrak{p}}_{\mathrm{O}}(a) = a = a^{\mathrm{N}\mathfrak{p}} \bmod \mathfrak{p}$$

(recall that $\mathrm{O}/\mathfrak{p} = \mathbf{F}_{\mathfrak{p}}$ is a finite field with N$\mathfrak{p}$-elements).

(ii) The polynomial ring O[T] is a Λ-ring with $\psi^{\mathfrak{a}}_{\mathrm{O[T]}} : \mathrm{O[T]} \to \mathrm{O[T]}$ given by $\mathrm{T} \mapsto \mathrm{T}^{\mathrm{N}\mathfrak{a}}$.

(iii) If $\mathrm{O} = \mathrm{O_K}$ is the ring of integers in a number field, L/K is an abelian extension and $\mathrm{P} \subset \mathrm{Id}_{\mathrm{O_K}}$ is the sub-monoid generated by the primes which are unramified in L/K, then the ring of integers $\mathrm{O_L}$ of L is a Λ_{P}-ring with $\psi^{\mathfrak{p}}_{\mathrm{O_L}} = \sigma_{\mathrm{L/K},\mathfrak{p}} : \mathrm{O_L} \to \mathrm{O_L}$ given by the Frobenius element $\sigma_{\mathrm{L/K},\mathfrak{p}} \in \mathrm{G(L/K)}$ (cf. (1.3.1)). Examples of this form will be very important later give the first link between Λ-structures and class field theory.

3.2.11. We now give an explicit description of what it means for a non-flat ring to be have Λ-structure in the special case $\mathrm{P} = \{\mathfrak{p}, \mathfrak{p}^2, \ldots\} \subset \mathrm{Id_O}$ is generated by a single prime ideal of O and the prime ideal $\mathfrak{p} = (\pi)$ is principal. In this case, a Λ-structure on an O-algebra can described explicitly, and this notion was discovered independently by Buium [**10**] (for some of the many interesting arithmetic applications of δ-rings and δ-geometry see [**11**]).

So let us describe Λ in this situation. Define elements $\delta_n \in \Lambda$ for $n \geq 0$ inductively by $\delta_0 = \psi^{(1)}$ and

$$\delta_{n+1} = \pi^{-1}(\psi^{\mathfrak{p}}_{\Lambda}(\delta_n) - (\delta_n)^{\mathrm{N}\mathfrak{p}}) \in \Lambda.$$

Let $\Delta_\pi \subset \Lambda$ be the sub-O-algebra generated by the elements $\{\delta_n\}_{n\geq 0}$.

3.2.12 Proposition. — *The inclusion $\Delta_\pi \subset \Lambda$ is an equality and Δ_π is freely generated as an* O*-algebra by the elements $\{\delta_n\}_{n\geq 0}$.*

Proof. — See §1.19 of [**4**]. □

3.2.13 Corollary. — *With notation as in* (3.2.11) *to give an* O*-algebra* A *a* Λ*-structure is equivalent to defining a map*

$$\delta_\pi : \mathrm{A} \to \mathrm{A}$$

such that:

(i) *for $r \in \mathrm{O}$ we have*

$$\delta_\pi(r) = \frac{r^{\mathrm{N}\mathfrak{p}} - r}{\pi},$$

(ii) *for $a, b \in \mathrm{A}$ we have*

$$\delta_\pi(ab) = a^{\mathrm{N}\mathfrak{p}}\delta_\pi(b) + b^{\mathrm{N}\mathfrak{p}}\delta_\pi(a) + \pi\delta_\pi(a)\delta_\pi(b),$$

and

(iii) *for $a, b \in \mathrm{A}$ we have*

$$\delta_\pi(a+b) = \delta_\pi(a) + \delta_\pi(b) + \sum_{i=1}^{\mathrm{N}\mathfrak{p}-1} \frac{1}{\pi}\binom{\mathrm{N}\mathfrak{p}}{i} a^{\mathrm{N}\mathfrak{p}-i} b^i.$$

Proof. — Also see §1.19 of [**4**]. □

3.2.14 Remark. — Let us spell out the equivalence between Λ-rings and rings with an operator δ_π satisfying (3.2.12) explicitly, in the case A is flat.

If $\delta_\pi : \mathrm{A} \to \mathrm{A}$ is a map satisfying the conditions (i)–(iii) of (3.2.12) then it follows that the map

$$\psi^{\mathfrak{p}}_{\mathrm{A}} : \mathrm{A} \to \mathrm{A} : a \mapsto a^{\mathrm{N}\mathfrak{p}} + \pi\delta_\pi(a)$$

is a O-algebra homomorphism satisfying

$$\psi^{\mathrm{A}}_{\mathfrak{p}}(a) = a^{\mathrm{N}\mathfrak{p}} + \pi\delta_\pi(a) = a^{\mathrm{N}\mathfrak{p}} \bmod \mathfrak{p}\mathrm{A}.$$

Conversely, if A is a $\mathfrak{p}$-torsion free Λ-ring then the relation

$$\psi_{\mathrm{A}}(a) = a^{\mathrm{N}\mathfrak{p}} \bmod \mathfrak{p}\mathrm{A}$$

implies that there is a unique $\delta_\pi(a) \in \mathrm{A}$ such that

$$\psi_{\mathrm{A}}(a) = a^{\mathrm{N}\mathfrak{p}} + \pi\delta_\pi(a)$$

and the fact that $\psi^{\mathfrak{p}}_{\mathrm{A}}$ is an O-algebra homomorphism forces the map $a \mapsto \delta_\pi(a)$ to satisfy conditions (i)–(iii) of (3.2.12).

3.2.15 Remark. — We can now explain why the approach with plethories was taken. To define a Λ-ring as an O-algebra with a Frobenius lift $\psi^{\mathfrak{p}}_{\mathrm{A}} : \mathrm{A} \to \mathrm{A}$ is a perfectly reasonable thing to do, however, there is a hidden existential quantifier in this definition: that for all $a \in \mathrm{A}$ there exists an $a_{\mathfrak{p}} \in \mathfrak{p}\mathrm{A}$ such that $\psi^{\mathfrak{p}}_{\mathrm{A}}(a) = a^{\mathrm{N}\mathfrak{p}} + a_{\mathfrak{p}}$. This causes problems from the point of view of universal algebra and the effect of the plethystic approach is to remove this existential quantifier so that, rather than the Frobenius lift $\psi^{\mathfrak{p}}_{\mathrm{A}}$, is it the operator δ_π which determines the structure.

3.2.16 Corollary. — *If* A *is a* Λ*-ring then the kernel of the homomorphism* $\mathrm{O} \to \mathrm{A}$ *is either prime to all* $\mathfrak{p} \in \mathrm{P}$ *or* $\mathrm{A} = 0$ *is the zero ring.*

Proof. — We shall prove this in the situation of (3.2.12) remarking that it is possible to reduce to this case once more of the theory has been set-up. So let A be a Λ-ring and assume that $\pi^n \in \mathfrak{p}^n \subset \ker(\mathrm{O} \to \mathrm{A})$. As the homomorphism $\mathrm{O} \to \mathrm{A}$ is a Λ-homomorphism the kernel is stabilised by the endomorphism $\delta_\pi : \mathrm{O} \to \mathrm{O}$ which is given by

$$a \mapsto \frac{a^{\mathrm{N}\mathfrak{p}} - a}{\pi}.$$

In particular, we see that

$$\delta_\pi(\pi^n) = \frac{\pi^{\mathrm{N}\mathfrak{p}n} - \pi^n}{\pi} = \pi^{\mathrm{N}\mathfrak{p}n-1} - \pi^{n-1} = \pi^{n-1}(\pi^{\mathrm{N}\mathfrak{p}(n-1)} - 1) \in \mathfrak{p}^{n-1}.$$

Therefore, $\mathfrak{p}^{n-1} \subset \ker(\mathrm{O} \to \mathrm{A})$ and by induction we find that $\mathrm{O} \subset \ker(\mathrm{O} \to \mathrm{A})$ and so A is the zero ring. □

3.2.17. Let $\mathrm{P}' \subset \mathrm{P}$ be a sub-monoid generated by some set of prime ideals. Then the restriction of the map $h_{\Lambda_\mathrm{P}} : \Lambda_\mathrm{P} \odot \Lambda_\mathrm{P} \to \Lambda_\mathrm{P}$ along $\Lambda_{\mathrm{P}'} \odot \Lambda_\mathrm{P} \to \Lambda_\mathrm{P}$ makes Λ_P a $\Lambda_{\mathrm{P}'}$-ring. Similarly, for Ψ_P and $\Psi_{\mathrm{P}'}$.

Now denote by

$$\mathrm{P}'' = \{\mathfrak{a} \in \mathrm{P} : (\mathfrak{a}, \mathfrak{b}) = (1) \text{ for all } \mathfrak{b} \in \mathrm{P}'\} \subset \mathrm{P}$$

so that $\mathrm{P}' \cdot \mathrm{P}'' = \mathrm{P}$ and $\mathrm{P}' \cap \mathrm{P}'' = \{\mathrm{O}\}$. By the remark above the map $\Lambda_{\mathrm{P}''} \to \Lambda_\mathrm{P}$ extends by adjunction to a homomorphism of $\Lambda_{\mathrm{P}'}$-rings

$$\alpha_{\mathrm{P}',\mathrm{P}''} : \Lambda_{\mathrm{P}'} \odot \Lambda_{\mathrm{P}''} \to \Lambda_\mathrm{P}$$

which is also a homomorphism of Ψ_P-rings where $\mathrm{P}'' \subset \mathrm{P}$ acts on the left factor.

3.2.18 Proposition. — *The map $\alpha_{\mathrm{P}',\mathrm{P}''} : \Lambda_{\mathrm{P}'} \odot \Lambda_{\mathrm{P}''} \to \Lambda_\mathrm{P}$ defined above is a $\Lambda_{\mathrm{P}'}$-isomorphism.*

Proof. — This is Proposition 5.3 of [**4**]. □

3.2.19. We now define truncated versions of the birings Λ and Ψ as, when we come to geometrise the theory of Λ-rings, they will be more well behaved (cf. (3.2.22)).

We equip the O-algebra $\Psi \otimes_\mathrm{O} \mathrm{K}$ with an exhaustive filtration by sub-O-algebras, indexed by the elements of P ordered by division, by setting $(\Psi \otimes \mathrm{K})_\mathfrak{a}$ for $\mathfrak{a} \in \mathrm{P}$ to be the sub-K-algebra generated by the $\psi^\mathfrak{b}$ such that $\mathfrak{b} | \mathfrak{a}$. The intersection of this filtration with the sub-O-algebras Λ and Ψ induces exhaustive filtrations by sub-O-algebras $\Lambda_\mathfrak{a} \subset \Lambda$ and $\Psi_\mathfrak{a} \subset \Psi$ and we have $\Psi_\mathfrak{a} = \mathrm{O}[\psi_\mathfrak{b} : \mathfrak{b} | \mathfrak{a}]$.

3.2.20 Proposition. — *We have the following:*

(i) *for each $\mathfrak{a} \in \mathrm{P}$ there is a unique* O*-biring structure on $\Lambda_\mathfrak{a}$ making $\Psi_\mathfrak{a} \to \Lambda_\mathfrak{a}$ a biring homomorphism,*

(ii) *for each pair $\mathfrak{a}, \mathfrak{b} \in \mathrm{P}$ the homomorphism $h_\Lambda : \Lambda \odot \Lambda \to \Lambda$ induces a homomorphism $\Lambda_\mathfrak{a} \odot \Lambda_\mathfrak{b} \to \Lambda_{\mathfrak{a}\mathfrak{b}}$ and this map is an isomorphism if $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime.*

Proof. — (i) This is Proposition 2.3 of [**4**].
(ii) This is Propositions 2.3 and 5.3 of [**4**]. □

3.2.21. Let A be an O-algebra. We write

$$\mathrm{W}(\mathrm{A}) = \mathrm{Hom}_\mathrm{O}(\Lambda, \mathrm{A}) \quad \text{and} \quad \mathrm{W}_\mathfrak{a}(\mathrm{A}) = \mathrm{Hom}_\mathrm{O}(\Lambda_\mathfrak{a}, \mathrm{A})$$

and call these the rings of Witt vectors and Witt vectors of length $\mathfrak{a}$ of A. We also write

$$\Gamma(\mathrm{A}) = \mathrm{Hom}_\mathrm{O}(\Psi, \mathrm{A}) \xrightarrow{\sim} \prod_{\mathfrak{a} \in \mathrm{P}} \mathrm{A} \quad \text{and} \quad \Gamma_\mathfrak{a}(\mathrm{A}) = \mathrm{Hom}_\mathrm{O}(\Psi_\mathfrak{a}, \mathrm{A}) \xrightarrow{\sim} \prod_{\mathfrak{b} | \mathfrak{a}} \mathrm{A}$$

and call these the rings of ghost vectors and length-$\mathfrak{a}$ ghost vectors.

3.2.22 Proposition. — *Let* $\mathfrak{a} \in \mathrm{P}$ *and let* A *be an* O*-algebra. Then*

(i) *If* $(\mathrm{A} \to \mathrm{A}_i)_{i\in\mathrm{I}}$ *is an étale cover of* A *so is* $(\mathrm{W}_\mathfrak{a}(\mathrm{A}) \to \mathrm{W}_\mathfrak{a}(\mathrm{A}_i))$*, and*

(ii) *for all homomorphisms* $\mathrm{A} \to \mathrm{B}$ *and all étale homomorphisms* $\mathrm{A} \to \mathrm{A}'$ *the natural map*

$$\mathrm{W}_\mathfrak{a}(\mathrm{A}') \otimes_{\mathrm{W}_\mathfrak{a}(\mathrm{A})} \mathrm{W}_\mathfrak{a}(\mathrm{B}) \to \mathrm{W}_\mathfrak{a}(\mathrm{A}' \otimes_\mathrm{A} \mathrm{B})$$

is an isomorphism.

Proof. — This is Theorem 9.2 and Corollary 9.3 of [**4**]. □

3.3. Witt vectors and arithmetic jets II

The purpose of this section is to extend the definition of Λ-structures, Witt vectors and arithmetic jets to sheaves for the étale topology.

3.3.1. Recall that $\mathrm{Sh}^{\text{ét}}_\mathrm{O}$ denotes the category of sheaves for the étale topology over Spec(O), or ét-sheaves over Spec(O). We begin with the arithmetic jets and coghosts. Let X be an ét-sheaf and define the presheaves on Aff_O

$$\mathrm{W}_{\mathfrak{a}*}(\mathrm{X}) := \mathrm{X} \circ \mathrm{W}_\mathfrak{a} : \mathrm{Aff}^\circ_\mathrm{O} \to \mathrm{Set} \qquad \Gamma_{\mathfrak{a}*}(\mathrm{X}) := \mathrm{X} \circ \Gamma_\mathfrak{a} : \mathrm{Aff}^\circ_\mathrm{O} \to \mathrm{Set}.$$

3.3.2 Proposition. — *Let* $\mathfrak{a} \in \mathrm{P}$ *and let be* X *an* ét*-sheaf. Then*

$$\mathrm{W}_{\mathfrak{a}*}(\mathrm{X}) := \mathrm{X} \circ \mathrm{W}_\mathfrak{a} : \mathrm{Aff}^\circ_\mathrm{O} \to \mathrm{Set} \qquad \Gamma_{\mathfrak{a}*}(\mathrm{X})(\mathrm{X}) := \mathrm{X} \circ \Gamma_\mathfrak{a} : \mathrm{Aff}^\circ_\mathrm{O} \to \mathrm{Set}$$

are again ét*-sheaves. Moreover,*

(i) *if* $\mathrm{X} = \mathrm{Spec}(\mathrm{A})$ *is affine then*

$$\mathrm{W}_{\mathfrak{a}*}(\mathrm{X}) = \mathrm{Spec}(\Lambda_\mathfrak{a} \odot \mathrm{A}) \quad \textit{and} \quad \Gamma_{\mathfrak{a}*}(\mathrm{X}) = \mathrm{Spec}(\Psi_\mathfrak{a} \odot \mathrm{A}),$$

(ii) $\mathrm{W}_{\mathfrak{a}*}$ *and* $\Gamma_{\mathfrak{a}*}$ *commute with filtered colimits, and*

(iii) $\mathrm{W}_{\mathfrak{a}*}$ *sends smooth affine* $\mathrm{Spec}(\mathrm{O_K})$*-schemes to smooth affine* $\mathrm{Spec}(\mathrm{O_K})$*-schemes.*

Proof. — It is clear that $\Gamma_{\mathfrak{a}*}(\mathrm{X})$ of an ét-sheaf is again a sheaf, and for $\mathrm{W}_{\mathfrak{a}*}(\mathrm{X})$ it follows from (i) of (3.2.22).

(i) This is clear for $\Gamma_{\mathfrak{a}*}$ and Proposition 10.7 of [**5**] for $\mathrm{W}_{\mathfrak{a}*}$.

(ii) This is clear for $\Gamma_{\mathfrak{a}*}$ and Proposition 11.7 of [**5**] for $\mathrm{W}_{\mathfrak{a}*}$.

(iii) This is Proposition 13.3 of [**5**]. □

3.3.3. For an ét-sheaf X we have the following simple description of $\Gamma_\mathfrak{a}(\mathrm{X})$. The fact that $\Gamma_\mathfrak{a}(\mathrm{A}) = \Pi_{\mathfrak{b}\in\mathrm{P},\mathfrak{b}|\mathfrak{a}}\mathrm{A}$ for all O-algebras A (3.2.19) shows that

$$\Gamma_{\mathfrak{a}*}(\mathrm{X})(\mathrm{A}) = \mathrm{X}(\Gamma_\mathfrak{a}(\mathrm{A})) = \prod_{\mathfrak{b}\in\mathrm{P},\mathfrak{b}|\mathfrak{a}} \mathrm{X}(\mathrm{A}) = \prod_{\mathfrak{b}\in\mathrm{P},\mathfrak{b}|\mathfrak{a}} \mathrm{X}(\mathrm{A}),$$

that is

$$\Gamma_\mathfrak{a}(\mathrm{X}) \xrightarrow{\sim} \prod_{\mathfrak{b}\in\mathrm{P},\mathfrak{b}|\mathfrak{a}} \mathrm{X}.$$

3.3.4. For an ét-sheaf X we call $\mathrm{W}_{\mathfrak{a}*}(\mathrm{X})$ the (ét-sheaf of) length-$\mathfrak{a}$ arithmetic jets of X and $\Gamma_{\mathfrak{a}*}(\mathrm{X})$ the (ét-sheaf of) length-$\mathfrak{a}$ coghosts of X.

Standard sheaf theory supplies $\mathrm{W}_{\mathfrak{a}*}$ and $\Gamma_{\mathfrak{a}*}$ with left adjoints which we denote by $\mathrm{W}^*_{\mathfrak{a}}$ and $\Gamma^*_{\mathfrak{a}}$. For a sheaf X we call $\mathrm{W}^*_{\mathfrak{a}}(\mathrm{X})$ the length-$\mathfrak{a}$ Witt vectors of X and $\Gamma^*_{\mathfrak{a}}(\mathrm{X})$ the length $\mathfrak{a}$-ghost vectors of X.

3.3.5 Proposition. — *If* $\mathrm{X} = \mathrm{Spec}(\mathrm{A})$ *is an affine scheme then*

$$\mathrm{W}^*_{\mathfrak{a}}(\mathrm{Spec}(\mathrm{A})) = \mathrm{Spec}(\mathrm{W}_{\mathfrak{a}}(\mathrm{A})) \quad \textit{and} \quad \Gamma^*_{\mathfrak{a}}(\mathrm{Spec}(\mathrm{A})) = \mathrm{Spec}(\Gamma_{\mathfrak{a}}(\mathrm{A})).$$

Proof. — This is true for all left adjoints to push forwards along a morphism of sites. □

3.3.6. For a sheaf X we have the following simple description of $\Gamma_{\mathfrak{a}*}(\mathrm{X})$. The fact that $\Gamma_{\mathfrak{a}}(\mathrm{A}) = \Pi_{\mathfrak{b}\in\mathrm{P},\mathfrak{b}|\mathfrak{a}}\mathrm{A}$ for all O-algebras A (3.2.19) shows that:

$$\begin{aligned}\Gamma^*_{\mathfrak{a}}(\mathrm{X}) = \operatorname*{colim}_{\mathrm{Spec}(\mathrm{A})\to\mathrm{X}} \Gamma^*_{\mathfrak{a}}(\mathrm{Spec}(\mathrm{A})) &= \operatorname*{colim}_{\mathrm{Spec}(\mathrm{A})\to\mathrm{X}} \mathrm{Spec}(\Gamma_{\mathfrak{a}}(\mathrm{A})) \\ &= \operatorname*{colim}_{\mathrm{Spec}(\mathrm{A})\to\mathrm{X}} \coprod_{\mathfrak{b}\in\mathrm{P},\mathfrak{b}|\mathfrak{a}} \mathrm{Spec}(\mathrm{A}) \\ &= \coprod_{\mathfrak{b}\in\mathrm{P},\mathfrak{b}|\mathfrak{a}} \mathrm{X}\end{aligned}$$

3.3.7. For a sheaf X, the inclusions $\Lambda_{\mathfrak{a}} \to \Lambda_{\mathfrak{b}}$ and $\Psi_{\mathfrak{a}} \to \Psi_{\mathfrak{b}}$ (3.2.19), for $\mathfrak{a}, \mathfrak{b} \in \mathrm{P}$ with $\mathfrak{b}|\mathfrak{a}$, induce maps

$$\Gamma_{\mathfrak{a}*}(\mathrm{X}) \to \Gamma_{\mathfrak{b}*}(\mathrm{X}) \quad \text{and} \quad \mathrm{W}_{\mathfrak{a}*}(\mathrm{X}) \to \mathrm{W}_{\mathfrak{b}*}(\mathrm{X})$$

and taking the inverse limit in each case over the $\mathfrak{a} \in \mathrm{P}$ defines sheaves

$$\Gamma_*(\mathrm{X}) := \lim_{\mathfrak{a}} \Gamma_{\mathfrak{a}*}(\mathrm{X}) \quad \text{and} \quad \mathrm{W}_*(\mathrm{X}) := \lim_{\mathfrak{a}} \mathrm{W}_{\mathfrak{a}*}(\mathrm{X})$$

which we call the (ét-sheaf of) arithmetic jets of X and (ét-sheaf of) coghosts of X.

Adjointly, there are also induced maps

$$\mathrm{W}^*_{\mathfrak{b}}(\mathrm{X}) \to \mathrm{W}^*_{\mathfrak{a}}(\mathrm{X}) \quad \text{and} \quad \Gamma^*_{\mathfrak{b}}(\mathrm{X}) \to \Gamma^*_{\mathfrak{a}}(\mathrm{X})$$

and taking the colimit we obtain ét-sheaves

$$\mathrm{W}^*(\mathrm{X}) := \operatorname*{colim}_{\mathfrak{a}} \mathrm{W}^*_{\mathfrak{a}}(\mathrm{X}) \quad \text{and} \quad \Gamma^*(\mathrm{X}) := \operatorname*{colim}_{\mathfrak{a}} \Gamma^*_{\mathfrak{a}}(\mathrm{X})$$

which we call the (ét-sheaf of) ghost vectors of X and the (ét-sheaf of) Witt vectors of X. By construction the functor Γ^* is left adjoint to Γ_*, and W^* is left adjoint to W_*.

Generalising the descriptions of $\Gamma_{\mathfrak{a}*}(\mathrm{X})$ and $\Gamma^*_{\mathfrak{a}}(\mathrm{X})$ we have

$$\Gamma_*(\mathrm{X}) \xrightarrow{\sim} \prod_{\mathfrak{a}\in\mathrm{P}} \mathrm{X} \quad \text{and} \quad \Gamma^*(\mathrm{X}) \xrightarrow{\sim} \coprod_{\mathfrak{a}\in\mathrm{P}} \mathrm{X}.$$

3.3.8. The maps $\Lambda_{\mathfrak{a}} \odot \Lambda_{\mathfrak{b}} \to \Lambda_{\mathfrak{ab}}$ (3.2.20) induce maps

$$\mathrm{W}^*_{\mathfrak{b}}(\mathrm{W}^*_{\mathfrak{a}}(\mathrm{X})) \to \mathrm{W}^*_{\mathfrak{ab}}(\mathrm{X}) \quad \text{and} \quad \mathrm{W}_{\mathfrak{ab}*}(\mathrm{X}) \to \mathrm{W}_{\mathfrak{a}*}(\mathrm{W}_{\mathfrak{b}*}(\mathrm{X}))$$

and taking the colimit and limit respectively over all $\mathfrak{a}, \mathfrak{b} \in \mathrm{P}$ we obtain maps

$$\mu_{\mathrm{W}^*(\mathrm{X})} : \mathrm{W}^*(\mathrm{W}^*(\mathrm{X})) \to \mathrm{W}^*(\mathrm{X}) \quad \text{and} \quad h_{\mathrm{W}_*(\mathrm{X})} : \mathrm{W}_*(\mathrm{X}) \to \mathrm{W}_*(\mathrm{W}_*(\mathrm{X}))$$

which together with the natural maps

$$g_{(1)} : \mathrm{X} \to \mathrm{W}^*(\mathrm{X}) \quad \text{and} \quad \gamma_{(1)} : \mathrm{W}_*(\mathrm{X}) \to \mathrm{X}$$

induced by the compatible maps $\mathrm{O}[e] \to \Lambda_{\mathfrak{a}}$ for all $\mathfrak{a} \in \mathrm{P}$ equip W^* with the structure of a monad and W_* with the structure of a comonad on $\mathrm{Sh}^{\text{ét}}_{\mathrm{O}}$. We define the category of Λ-sheaves $\mathrm{Sh}^{\text{ét}}_{\Lambda}$ to be the category of ét-sheaves X equipped with an action of W^* or equivalently a coaction of W_*. The functors W^* and W_* now define functors $\mathrm{Sh}^{\text{ét}}_{\mathrm{O}} \to \mathrm{Sh}^{\text{ét}}_{\Lambda}$ which are left and right adjoint to the forgetful functor $\mathrm{Sh}^{\text{ét}}_{\Lambda} \to \mathrm{Sh}^{\text{ét}}_{\mathrm{O}}$. We have the following diagram of functors each one right adjoint to the one below:

$$\mathrm{Sh}^{\text{ét}}_{\Lambda} \underset{\mathrm{W}^*}{\overset{\mathrm{W}_*}{\rightleftarrows}} \mathrm{Sh}^{\text{ét}}_{\mathrm{O}}, \qquad \mathrm{Sh}^{\text{ét}}_{\Lambda} \xrightarrow{\text{forget}} \mathrm{Sh}^{\text{ét}}_{\mathrm{O}}.$$

In particular, the forgetful functor in the middle admits both a left and right adjoint and so commutes with both limits and colimits. That is, limits and colimits in $\mathrm{Sh}^{\text{ét}}_{\Lambda}$ may be computed in $\mathrm{Sh}^{\text{ét}}_{\mathrm{O}}$.

3.3.9. The same construction above applied to the maps $\Psi_{\mathfrak{a}} \odot \Psi_{\mathfrak{b}} \to \Psi_{\mathfrak{ab}}$ equips Γ^* with the structure of a monad and Γ_* with the structure of a comonad on $\mathrm{Sh}^{\text{ét}}_{\mathrm{O}}$. In this case, it is easy to see that the map obtained

$$\mu_{\Gamma^*(\mathrm{X})} : \Gamma^*(\Gamma^*(\mathrm{X})) \to \Gamma^*(\mathrm{X})$$

is identified with the map

$$\coprod_{\mathfrak{b}\in\mathrm{P}} \coprod_{\mathfrak{a}\in\mathrm{P}} \mathrm{X} = \coprod_{\mathfrak{a},\mathfrak{b}\in\mathrm{P}} \mathrm{X} \to \coprod_{\mathfrak{c}\in\mathrm{P}} \mathrm{X}$$

whose restriction to the summand at $\mathfrak{b}, \mathfrak{a} \in \mathrm{P}$ is the inclusion onto the summand at $\mathfrak{c} = \mathfrak{ab} \in \mathrm{P}$. Similarly, the map obtained

$$h_{\Gamma_*(\mathrm{X})} : \Gamma_*(\mathrm{X}) \to \Gamma_*(\Gamma_*(\mathrm{X}))$$

is identified with the map

$$\prod_{\mathfrak{c}\in\mathrm{P}} \mathrm{X} \to \prod_{\mathfrak{a}\in\mathrm{P}} \prod_{\mathfrak{b}\in\mathrm{P}} \mathrm{X}$$

whose composition with the projection onto the factor at $\mathfrak{a}, \mathfrak{b} \in \mathrm{P}$ is the projection onto the factor at $\mathfrak{c} = \mathfrak{ab}$.

We define the category of Ψ-sheaves $\mathrm{Sh}^{\text{ét}}_{\Psi}$ to be the category of sheaves X equipped with an action of Γ^* or equivalently with a coaction of Γ_*. Then Γ^* and Γ_* define functors $\mathrm{Sh}^{\text{ét}}_{\mathrm{O}} \to \mathrm{Sh}^{\text{ét}}_{\Psi}$ which are left and right adjoint to the forgetful functor $\mathrm{Sh}^{\text{ét}}_{\Psi} \to \mathrm{Sh}^{\text{ét}}_{\mathrm{O}}$. We have the following diagram of functors each one right adjoint to the one below:

$$\mathrm{Sh}^{\text{ét}}_{\Psi} \underset{\Gamma^*}{\overset{\text{forget}}{\underset{\Gamma_*}{\rightleftarrows}}} \mathrm{Sh}^{\text{ét}}_{\mathrm{O}}.$$

3.3.10. From the descriptions of the monadic and comonadic structures on Γ^* and Γ_* it is easy to see that to give a sheaf X the structure of Ψ sheaf is equivalent to equipping X with an action of the monoid P. Indeed, denoting the action of $\mathfrak{a} \in \mathrm{P}$ by $\psi^{\mathfrak{a}}_{\mathrm{X}} : \mathrm{X} \to \mathrm{X}$ the map $\Gamma^*(\mathrm{X}) \to \mathrm{X}$ defining the corresponding action of Γ^* is just

$$\coprod_{\mathfrak{a}\in\mathrm{P}} \psi^{\mathfrak{a}}_{\mathrm{X}} : \coprod_{\mathfrak{a}\in\mathrm{P}} \mathrm{X} = \Gamma^*(\mathrm{X}) \to \mathrm{X}.$$

As with Ψ-rings if $\mathrm{X} \to \mathrm{S}$ is a morphism of Ψ-sheaves the $\psi^{\mathfrak{a}}_{\mathrm{S}}$-linear endomorphisms $\psi^{\mathfrak{a}}_{\mathrm{X}} : \mathrm{X} \to \mathrm{X}$ for $\mathfrak{a} \in \mathrm{P}$ induce S-linear endomorphisms

$$\psi^{\mathfrak{a}}_{\mathrm{X/S}} : \mathrm{X} \to \psi^{\mathfrak{a}*}_{\mathrm{S}}(\mathrm{X})$$

satisfying the commutativity condition

$$\psi^{\mathfrak{b}*}_{\mathrm{S}}(\psi^{\mathfrak{a}}_{\mathrm{X/S}}) \circ \psi^{\mathfrak{b}}_{\mathrm{X/S}} = \psi^{\mathfrak{ab}}_{\mathrm{X/S}} = \psi^{\mathfrak{a}*}_{\mathrm{S}}(\psi^{\mathfrak{b}}_{\mathrm{X/S}}) \circ \psi^{\mathfrak{a}}_{\mathrm{X/S}} \tag{3.3.10.1}$$

for all $\mathfrak{a}, \mathfrak{b} \in \mathrm{P}$. Moreover, to give an ét-sheaf $\mathrm{X} \to \mathrm{S}$ over S a Ψ-structure such that the morphism $\mathrm{X} \to \mathrm{S}$ is a Ψ-morphism is the same as giving maps $\psi^{\mathfrak{a}}_{\mathrm{X/S}} : \mathrm{X} \to \psi^{\mathfrak{a}*}_{\mathrm{S}}(\mathrm{X})$ all $\mathfrak{a} \in \mathrm{P}$ with $\psi^{(1)}_{\mathrm{X/S}} = \mathrm{id}_{\mathrm{X}}$ and satisfying the commutativity condition (3.3.10.1).

3.3.11. The inclusions $\Lambda_{\mathfrak{a}} \to \Psi_{\mathfrak{a}}$ induce functorial maps for each sheaf X

$$g_{\leq\mathfrak{a}} : \Gamma^*_{\mathfrak{a}}(\mathrm{X}) \to \mathrm{W}^*_{\mathfrak{a}}(\mathrm{X}) \quad \text{and} \quad \gamma_{\leq\mathfrak{a}} : \mathrm{W}_{\mathfrak{a}*}(\mathrm{X}) \to \Gamma_{\mathfrak{a}*}(\mathrm{X})$$

which we call the length-$\mathfrak{a}$ ghost and coghost maps.

The inclusions

$$\mathrm{O}[\psi_{\mathfrak{a}}] \subset \mathrm{O}[\psi_{\mathfrak{b}} : \mathfrak{b} \in \mathrm{P}, \mathfrak{b}|\mathfrak{a}] = \Psi_{\mathfrak{a}}$$

induce for each $\mathfrak{a}$ the $\mathfrak{a}$-ghost component and $\mathfrak{a}$-coghost components

$$g_{\mathfrak{a}} : \mathrm{X} \to \Gamma^*(\mathrm{X}) \to \mathrm{W}^*(\mathrm{X}) \quad \gamma_{\mathfrak{a}} : \mathrm{W}_*(\mathrm{X}) \to \Gamma_*(\mathrm{X}) \to \mathrm{X}$$

which we denote by $g_{\mathfrak{a}}$ and $\gamma_{\mathfrak{a}}$ and view as maps from $\mathrm{X} \to \mathrm{W}^*(\mathrm{X})$ or $\mathrm{X} \to \Gamma^*(\mathrm{X})$ and similarly for the $\mathfrak{a}$-coghost maps. We then have

$$g_{\leq \mathfrak{a}} = \coprod_{\mathfrak{b}|\mathfrak{a}} g_{\mathfrak{b}} : \Gamma^*_{\mathfrak{a}}(\mathrm{X}) = \coprod_{\mathfrak{b}|\mathfrak{a}} \mathrm{X} \to \Gamma^*(\mathrm{X}).$$

Taking the colimit and limit along the length-$\mathfrak{a}$ ghost and coghost maps we obtain the full ghost and coghost maps

$$g : \Gamma^*(\mathrm{X}) \to \mathrm{W}^*(\mathrm{X}) \quad \text{and} \quad \gamma : \mathrm{W}_*(\mathrm{X}) \to \Gamma_*(\mathrm{X}).$$

Finally, the natural transformations given by the ghost and coghost maps $g : \Gamma^* \to \mathrm{W}^*$ and $\gamma : \mathrm{W}_* \to \Gamma_*$ are morphisms of monads and comonads respectively and every Λ-sheaf X inherits the structure of a Ψ-sheaf. That is every Λ-sheaf X admits a canonical action of the monoid P which, as for Ψ-sheaves, we denote by $\psi^{\mathfrak{a}}_{\mathrm{X}} : \mathrm{X} \to \mathrm{X}$ for $\mathfrak{a} \in \mathrm{P}$ (and similarly for the relative versions (cf. (3.3.10)).

3.3.12 Proposition. — *We have the following:*

(i) *For each* Λ*-sheaf* X *and each prime* $\mathfrak{p} \in \mathrm{P}$ *the map*

$$\psi^{\mathfrak{p}}_{\mathrm{X}} \times_{\mathrm{Spec}(\mathrm{O})} \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}}) : \mathrm{X} \times_{\mathrm{Spec}(\mathrm{O})} \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}}) \to \mathrm{X} \times_{\mathrm{Spec}(\mathrm{O})} \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}})$$

is equal to the $\mathrm{N}\mathfrak{p}$*-power Frobenius endomorphism of* $\mathrm{X} \times_{\mathrm{Spec}(\mathrm{O})} \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}})$.

(ii) *A* Ψ*-structure on a scheme* X*, flat over* O *at all primes* $\mathfrak{p} \in \mathrm{O}$*, is induced by a* Λ*-structure on* X *if and only if for each prime* $\mathfrak{p} \in \mathrm{P}$ *the map*

$$\psi^{\mathfrak{p}}_{\mathrm{X}} \times_{\mathrm{Spec}(\mathrm{O})} \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}}) : \mathrm{X} \times_{\mathrm{Spec}(\mathrm{O})} \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}}) \to \mathrm{X} \times_{\mathrm{Spec}(\mathrm{O})} \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}})$$

is the $\mathrm{N}\mathfrak{p}$*-power Frobenius endomorphism. Moreover, in this case such a* Λ*-structure on* X *is unique.*

(iii) *If each* $\mathfrak{p} \in \mathrm{P}$ *is invertible on* X *then every* Ψ*-structure on* X *is induced by a unique* Λ*-structure.*

Proof. — See [**6**] or it is an exercise using Theorem 17.3 of [**5**]. □

3.3.13 Proposition. — *We have the following:*

(i) *If* $f : \mathrm{X} \to \mathrm{Y}$ *an affine étale morphism of ind-affine-schemes then for each* $\mathfrak{a} \in \mathrm{P}$ *the morphism*

$$\mathrm{W}^*_{\mathfrak{a}}(f) : \mathrm{W}^*_{\mathfrak{a}}(\mathrm{X}) \to \mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y})$$

is affine and étale.

(ii) *If* $f : \mathrm{X} \to \mathrm{Y}$ *is a affine étale morphism of ind-affine-schemes then for any affine morphism* $\mathrm{Y}' \to \mathrm{Y}$ *of ind-schemes the natural map*

$$\mathrm{W}^*_{\mathfrak{a}}(\mathrm{X} \times_{\mathrm{Y}} \mathrm{Y}') \to \mathrm{W}^*_{\mathfrak{a}}(\mathrm{X}) \times_{\mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y})} \mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y}')$$

is an isomorphism.

Proof. — The case where X and Y are affine follows from (3.2.22) and we shall reduce to this case. So write $\mathrm{Y} = \mathrm{colim}_{i\in\mathrm{I}}\,\mathrm{Y}_i$ as a filtered colimit of affine schemes, and for $i \in \mathrm{I}$ write $\mathrm{X}_i = \mathrm{X} \times_{\mathrm{Y}} \mathrm{Y}_i$.

(i) Let $i, j \in \mathrm{I}$ with $\mathrm{Y}_i \to \mathrm{Y}_j \to \mathrm{Y}$. Then as Y_i and Y_j are affine and $\mathrm{X} \to \mathrm{Y}$ is affine we have a cartesian diagram

$$\begin{array}{ccc} \mathrm{W}^*_{\mathfrak{a}}(\mathrm{X}_j) & \longrightarrow & \mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y}_j) \\ \uparrow & & \uparrow \\ \mathrm{W}^*_{\mathfrak{a}}(\mathrm{X}_i) & \longrightarrow & \mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y}_i) \end{array}$$

where the bottom arrow is affine and étale. Now taking the colimit over j yields a cartesian diagram

$$\begin{array}{ccc} \mathrm{W}^*_{\mathfrak{a}}(\mathrm{X}) & \longrightarrow & \mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y}) \\ \uparrow & & \uparrow \\ \mathrm{W}^*_{\mathfrak{a}}(\mathrm{X}_i) & \longrightarrow & \mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y}_i) \end{array}$$

where the bottom arrow is affine, so that as $(\mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y}_i) \to \mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y}))_{i\in\mathrm{I}}$ is a cover we are done.

(ii) Writing $\mathrm{Y}'_i = \mathrm{Y}' \times_{\mathrm{Y}} \mathrm{Y}_i$ the morphism

$$\mathrm{W}^*_{\mathfrak{a}}(\mathrm{X} \times_{\mathrm{Y}} \mathrm{Y}') \to \mathrm{W}^*_{\mathfrak{a}}(\mathrm{X}) \times_{\mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y})} \mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y}')$$

is the colimit over $i \in \mathrm{I}$ of the morphisms

$$\mathrm{W}^*_{\mathfrak{a}}(\mathrm{X}_i \times_{\mathrm{Y}_i} \mathrm{Y}'_i) \to \mathrm{W}^*_{\mathfrak{a}}(\mathrm{X}_i) \times_{\mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y}_i)} \mathrm{W}^*_{\mathfrak{a}}(\mathrm{Y}'_i)$$

which is an isomorphism as $\mathrm{Y}_i, \mathrm{Y}'_i$ and X_i are all affine. □

3.4. Λ-structures

3.4.1. Let S be a Λ-sheaf so that S is equipped with an action of the monad W^* and equivalently a coaction of the monad W_*.

From the monadic point of view we write

$$\mu_{\mathrm{S}} : \mathrm{W}^*(\mathrm{S}) \to \mathrm{S}$$

for map defining the action of W^* on S and we call this the structure map. The fact that it defines an action of W^* on S is the expressed via the commutativity of the diagram

$$\begin{array}{ccc} & & \mathrm{W}^*(\mathrm{S}) \\ & \overset{g_{(1)}}{\nearrow} & \big\downarrow \mu_{\mathrm{S}} \\ \mathrm{S} & \xrightarrow{\mathrm{id}_{\mathrm{S}}} & \mathrm{S} \end{array}$$

and the property that the two compositions

$$\mathrm{W}^*(\mathrm{W}^*(\mathrm{S})) \underset{\mu_{\mathrm{W}^*(\mathrm{S})}}{\overset{\mathrm{W}^*(\mu_\mathrm{S})}{\rightrightarrows}} \mathrm{W}^*(\mathrm{S}) \xrightarrow{\mu_\mathrm{S}} \mathrm{S}$$

coincide.

From the comonadic point of view we write

$$h_\mathrm{S} : \mathrm{S} \to \mathrm{W}_*(\mathrm{S})$$

for the map defining the coaction of W_*, and the fact that it defines a coaction is expressed via the commutativity of the diagram

$$\begin{array}{ccc} \mathrm{S} & \xrightarrow{h_\mathrm{S}} & \mathrm{W}_*(\mathrm{S}) \\ & \searrow^{\mathrm{id}_\mathrm{S}} & \downarrow{\scriptstyle \gamma_{(1)}} \\ & & \mathrm{S} \end{array}$$

and the fact that the two compositions

$$\mathrm{S} \xrightarrow{h_\mathrm{S}} \mathrm{W}_*(\mathrm{S}) \underset{h_{\mathrm{W}_*(\mathrm{S})}}{\overset{\mathrm{W}_*(h_\mathrm{S})}{\rightrightarrows}} \mathrm{W}_*(\mathrm{W}_*(\mathrm{S}))$$

are equal.

3.4.2. We denote by $\mathrm{Sh}^{\text{ét}}_{\Lambda_\mathrm{S}}$ the category of Λ-sheaves equipped with a Λ-morphism $\mathrm{X} \to \mathrm{S}$. The functor

$$\mathrm{W}_{\mathrm{S}*} : \mathrm{Sh}^{\text{ét}}_\mathrm{S} \to \mathrm{Sh}^{\text{ét}}_{\Lambda_\mathrm{S}} : \mathrm{X} \mapsto \mathrm{W}_*(\mathrm{X}) \times_{\mathrm{W}_*(\mathrm{S})} \mathrm{S}$$

composed with the forgetful functor is a comonad on $\mathrm{Sh}^{\text{ét}}_\mathrm{S}$ and identifies the category of S-sheaves X with a coaction of $\mathrm{W}_{\mathrm{S}*}$ with the category of Λ-sheaves equipped with a Λ-morphism $\mathrm{X} \to \mathrm{S}$.

3.4.3 Proposition. — *Let* S *be a* Λ*-sheaf and let* X *and* Y *be a pair of* Λ_S*-sheaves. Then the functor*

$$\mathrm{Sh}^{\text{ét}}_{\Lambda_\mathrm{S}} \to \mathrm{Set} : \mathrm{S}' \mapsto \mathrm{Hom}_{\Lambda_{\mathrm{S}'}}(\mathrm{X}_{\mathrm{S}'}, \mathrm{Y}_{\mathrm{S}'})$$

is a sheaf for the canonical topology.

Proof. — Let $\mathrm{S}' \to \mathrm{S}$ be a cover of S in $\mathrm{Sh}_{\Lambda_\mathrm{S}}$. Then $\mathrm{S}' \to \mathrm{S}$ is also a cover when viewed in $\mathrm{Sh}^{\text{ét}}_\mathrm{S}$ and so any $\Lambda_{\mathrm{S}'}$-morphism $f' : \mathrm{X}_{\mathrm{S}'} \to \mathrm{Y}_{\mathrm{S}'}$ with the property that the two pull-backs of f along the two projections $\mathrm{S}' \times_\mathrm{S} \mathrm{S}' \to \mathrm{S}$ coincide descends

to a morphism $X \to Y$. It remains to verify that it is a Λ_S-morphism, which is the commutivity of the

$$\begin{array}{ccc} X & \xrightarrow{h_{X/S}} & W_*(X) \times_{W_*(S)} S \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle W_*(f)\times_{W_*(S)}S} \\ Y & \xrightarrow{h_{Y/S}} & W_*(Y) \times_{W_*(S)} S. \end{array} \tag{3.4.3.1}$$

However, using the identifications

$$\begin{aligned} W_*(X) \times_{W_*(S)} S \times_S S' &= W_*(X) \times_{W_*(S)} S' \\ &= W_*(X) \times_{W_*(S)} W_*(S') \times_{W_*(S')} S' \\ &= W_*(X \times_S S') \times_{W_*(S')} S' \end{aligned}$$

and similarly for Y, the diagram (3.4.3.1) pulls-back along $S' \to S$ to the diagram

$$\begin{array}{ccc} X_{S'} & \xrightarrow{h_{X_{S'}/S'}} & W_*(X) \times_{W_*(S')} S' \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle W_*(f')\times_{W_*(S')}S'} \\ Y_{S'} & \xrightarrow{h_{Y_{S'}/S'}} & W_*(Y) \times_{W_*(S')} S' \end{array}$$

which commutes by hypothesis. Therefore, as $S' \to S$ is an epimorphism, the diagram (3.4.3.1) commutes. □

3.4.4. Let S be a Λ-sheaf and let $X \to S$ be an S-ét-sheaf. Denote by $\Lambda_{X/S}$ the functor

$$\Lambda_{X/S} : \mathrm{Sh}^{\text{ét}}_{\Lambda_S} \to \mathrm{Set} : S'/S \mapsto \{\text{the set of } \Lambda_{S'}\text{-structures on } X \times_S S'\}.$$

3.4.5 Proposition. — *The functor $\Lambda_{X/S}$ is a sheaf for the canonical topology on $\mathrm{Sh}^{\text{ét}}_{\Lambda_S}$.*

Proof. — Let $S' \to S$ be an epimorphism and write $S'' = S \times_S S'$, $X' = X \times_S S'$ and $X'' = X \times_S S''$. By the definition of a Λ_S-structure (in terms of W^*) we have an equaliser (the Homs are of ét-sheaves not Λ-sheaves)

$$\Lambda_{X/S}(S) \longrightarrow \mathrm{Hom}_S(W^*(X), X) \rightrightarrows \mathrm{Hom}_S(X, X) \times \mathrm{Hom}_S(W^*(W^*(X)), X)$$

where the first map sends a Λ_S-structure on S to the map $\mu_X : W^*(X) \to X$ and the two parallel arrows send a map μ_X to

$$(\mu_X \circ g_{(1)}, \mu_{W^*(X)} \circ \mu_X) \quad \text{and} \quad (\mathrm{id}_X, W^*(\mu_X) \circ \mu_X).$$

Now consider corresponding commutative diagram:

$$\begin{array}{ccccc}
\Lambda_{X/S}(S) & \longrightarrow & \mathrm{Hom}_S(W^*(X), X) & \rightrightarrows & \mathrm{Hom}_S(X, X) \times \mathrm{Hom}_S(W^*(W^*(X)), X) \\
\downarrow & & \downarrow & & \downarrow \\
\Lambda_{X/S}(S') & \longrightarrow & \mathrm{Hom}_S(W^*(X'), X) & \rightrightarrows & \mathrm{Hom}_S(X', X) \times \mathrm{Hom}_S(W^*(W^*(X')), X) \\
\downarrow\downarrow & & \downarrow\downarrow & & \downarrow\downarrow \\
\Lambda_{X/S}(S'') & \longrightarrow & \mathrm{Hom}_S(W^*(X''), X) & \rightrightarrows & \mathrm{Hom}_S(X'', X) \times \mathrm{Hom}_S(W^*(W^*(X'')), X).
\end{array}$$

The two right columns are equalisers as $X' = X \times_S S' \to X$ is a cover and W^* preserves push-outs and all three rows are equalisers. Therefore it follows that the first column is an equaliser and we are done. □

3.4.6 Proposition. — *Let* O *be the ring of integers in a number field* K, $\mathfrak{f} \in \mathrm{Id}_O$ *an ideal and write* $P = \mathrm{Id}_O^{(\mathfrak{f})}$. *Then a finite étale* $S = \mathrm{Spec}(O[\mathfrak{f}^{-1}])$*-scheme* X *admits a* $\Lambda_{P,S}$*-structure if and only if* $X \times_S \mathrm{Spec}(K) = \amalg_{1 \le i \le n} \mathrm{Spec}(L_i)$ *where each* L_i *is a finite abelian extension of* K. *Moreover, in this case the* $\Lambda_{P,S}$*-structure is unique and any morphism of finite étale* $\Lambda_{P,S}$*-schemes is a* $\Lambda_{P,S}$*-morphism.*

Proof. — Let $X \to S$ be a finite étale morphism. Then $X \times_S \mathrm{Spec}(K) = \amalg_{i \in I} \mathrm{Spec}(L_i)$ with L_i/K a finite extension and $X \xrightarrow{\sim} \amalg_i X_i$ where $X_i = \mathrm{Spec}(O_{L_i}[\mathfrak{f}^{-1}])$. If $X \to S$ has a $\Lambda_{P,S}$-structure then for each prime $\mathfrak{p} \in P = \mathrm{Id}_{O_K}^{(\mathfrak{f})}$, the Frobenius lift $\psi_X^{\mathfrak{p}} : X \to X$ fixes the fibre of each X_i over $\mathrm{Spec}(\mathbf{F}_\mathfrak{p})$ so that $\psi_X^{\mathfrak{p}}$ maps each X_i to itself. It follows that the $\Lambda_{P,S}$-structure on X is induced by unique $\Lambda_{P,S}$-structures on each X_i and so we may assume that $X = X_i$ is connected. In this case, write $X = \mathrm{Spec}(O_L[\mathfrak{f}^{-1}])$ with L/K a finite extension. If $\mathfrak{P}$ is a prime of L laying over the prime $\mathfrak{p}$ then there is a unique automorphism

$$\sigma_{\mathfrak{P},L/K} : X \to X$$

whose restriction to fibre over $\mathrm{Spec}(O_L/\mathfrak{P})$ is equal to the $N\mathfrak{p}$-power Frobenius automorphism. But $\psi_X^{\mathfrak{p}}$ also has this property and so $\sigma_{\mathfrak{P},L/K} = \psi_X^{\mathfrak{p}}$. As the maps $\psi_X^{\mathfrak{p}} = \sigma_{\mathfrak{P},L/K}$ commute and generate the group G(L/K) it follows that G(L/K) is abelian. Moreover, the uniqueness of $\sigma_{\mathfrak{P},L/K} = \sigma_{\mathfrak{p},L/K} = \psi_X^{\mathfrak{p}}$ shows that the Λ_P-structure on X is unique, is also a $\Lambda_{P,S}$-structure and that any morphism of finite étale $\Lambda_{P,S}$-schemes is a $\Lambda_{P,S}$-morphism.

Conversely, if each L_i/K is abelian then there is a unique automorphism

$$\sigma_{\mathfrak{p},L_i/K} : X_i \to X_i$$

lifting the $N\mathfrak{p}$-power Frobenius automorphism of the fibre over $\mathrm{Spec}(\mathbf{F}_\mathfrak{p})$. It follows that setting $\psi_X^{\mathfrak{p}} = \amalg_{i \in I} \sigma_{L_i/K,\mathfrak{p}}$ defines a Frobenius lift on X. Moreover, as $G(L_i/K)$ is abelian these Frobenius lifts commute and so define a $\Lambda_{P,S}$-structure on X. □

3.4.7 Remark. — In the notation of (3.4.6) if $X \to S$ is a finite étale Λ_P-scheme then its Frobenius lifts $\psi^{\mathfrak{a}}_X$ for $\mathfrak{a} \in P$ will be denoted by $\sigma_{S,\mathfrak{a}}$, or just $\sigma_{\mathfrak{a}}$. This agrees with (or extends) the conventions set up in (1.3.1).

3.5. Ghosts and coghosts

3.5.1 Proposition. — *Let* X *be a sheaf. For each* $\mathfrak{a} \in P$ *the length-*$\mathfrak{a}$ *ghost map*

$$g_{\mathfrak{a}} : \Gamma^*_{\mathfrak{a}}(X) \to W^*_{\mathfrak{a}}(X)$$

is surjective on geometric points and so is the full ghost map

$$g : \Gamma^*(X) \to W^*(X).$$

Proof. — Writing $X = \operatorname{colim} \operatorname{Spec}(A)$ as a colimit of affine schemes, and $W^*(X) = \operatorname{colim}_{\mathfrak{a}} W^*_{\mathfrak{a}}(X)$ and $\Gamma^*(X) = \operatorname{colim}_{\mathfrak{a}} \Gamma^*_{\mathfrak{a}}(X)$ it is enough to show this for

$$\operatorname{Spec}(\Gamma_{\mathfrak{a}}(A)) = \Gamma^*_{\mathfrak{a}}(\operatorname{Spec}(A)) \to \operatorname{Spec}(W_{\mathfrak{a}}(A)) = W^*_{\mathfrak{a}}(\operatorname{Spec}(A)).$$

But the map $W_{\mathfrak{a}}(A) \to \Gamma_{\mathfrak{a}}(A)$ is integral with nilpotent kernel (Proposition 8.1 of [**4**]) and therefore

$$\operatorname{Spec}(\Gamma_{\mathfrak{a}}(A)) \to \operatorname{Spec}(W_{\mathfrak{a}}(A))$$

is surjective on geometric points. □

3.5.2 Proposition. — *If* S *is an ind-affine scheme, and* T *an affine étale* $W^*(S)$*-sheaf then the sequence*

$$T(W^*(S)) \xrightarrow{T(g)} T(\Gamma^*(S)) \rightrightarrows T(\Gamma^*(S) \times_{W^*(S)} \Gamma^*(S))$$

is an equaliser.

Proof. — As $W^*(S) = \operatorname{colim}_{\mathfrak{a}\in P} W^*_{\mathfrak{a}}(S)$ and $\Gamma^*(S) = \operatorname{colim}_{\mathfrak{a}\in P} \Gamma^*_{\mathfrak{a}}(S)$ and filtered colimits are exact, we may replace $W^*(S)$ and $\Gamma^*(S)$ and T with $W^*_{\mathfrak{a}}(S)$, $\Gamma^*_{\mathfrak{a}}(S)$ and $T \times_{W^*(S)} W^*_{\mathfrak{a}}(S)$ respectively. Now writing S as a filtered colimit of affine schemes we may assume that S is affine in which case the claim follows as $\Gamma^*_{\mathfrak{a}}(S) \to W^*_{\mathfrak{a}}(S)$ is integral and surjective, and therefore an effective descent map for the category of affine étale schemes. □

3.5.3 Remark. — In order for (3.5.2) to be useful in applications we should say something about the fibre product $W^*(S) \times_{\Gamma^*(S)} W^*(S)$. Let $\mathfrak{p}$ be a prime ideal, $\mathfrak{a}$ any ideal, $n \geq 1$ an integer and write $S_{\mathfrak{p}} = S \times_{\operatorname{Spec}(O)} \operatorname{Spec}(\mathbf{F}_{\mathfrak{p}})$ and consider the two maps (where the inclusions are the obvious ones)

$$r^{(1)}_{\mathfrak{a},\mathfrak{p}^n} : S_{\mathfrak{p}} \subset S \xrightarrow{g_{\mathfrak{a}\mathfrak{p}^n}} \Gamma^*(S) \quad \text{and} \quad r^{(2)}_{\mathfrak{a},\mathfrak{p}^n} : S_{\mathfrak{p}} \xrightarrow{\operatorname{Fr}^{N\mathfrak{p}^n}_{S_{\mathfrak{p}}}} S_{\mathfrak{p}} \subset S \xrightarrow{g_{\mathfrak{q}}} \Gamma^*(S).$$

Then for $i, j \in \{1, 2\}$ the two compositions

$$\mathrm{S}_{\mathfrak{p}} \xrightarrow{(r^{(i)}_{\mathfrak{a},\mathfrak{p}^n}, r^{(j)}_{\mathfrak{a},\mathfrak{p}^n})} \Gamma^*(\mathrm{S}) \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S}) \rightrightarrows \mathrm{W}^*(\mathrm{S})$$

are equal and the morphism

$$\coprod_{i\neq j\in\{1,2\}} \coprod_{\mathfrak{a},\mathfrak{p}^n} \mathrm{S}_{\mathfrak{p}} \xrightarrow{(r^{(i)}_{\mathfrak{a},\mathfrak{p}^n}, r^{(j)}_{\mathfrak{a},\mathfrak{p}^n})} \Gamma^*(\mathrm{S}) \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S})$$

defines a nilpotent immersion onto the complement of the diagonal in $\Gamma^*(\mathrm{S}) \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S})$ (this follows by an iterated application of 17.1 [**5**]). Therefore, in the notation of (3.5.2) an element of $\mathrm{T}(\Gamma^*(\mathrm{S}))$ is in the image of $\mathrm{T}(\mathrm{W}^*(\mathrm{S})) \to \mathrm{T}(\Gamma^*(\mathrm{S}))$ if and only if for all prime ideals $\mathfrak{p}$, ideals $\mathfrak{a}$, integers $n \geq 0$ and pairs $i \neq j \in \{1, 2\}$, it is equalised by the maps

$$\mathrm{T}(\Gamma^*(\mathrm{S})) \underset{\mathrm{T}(r^{(j)}_{\mathfrak{a},\mathfrak{p}^n})}{\overset{\mathrm{T}(r^{(i)}_{\mathfrak{a},\mathfrak{p}^n})}{\rightrightarrows}} \mathrm{T}(\mathrm{S}_{\mathfrak{p}}).$$

3.5.4 Lemma. — *If* X *is a scheme with the property that every finite set of points of* X *is contained in an open affine sub-scheme of* X *then for each* $\mathfrak{a} \in \mathrm{P}$ *the length-*$\mathfrak{a}$ *coghost map*

$$\gamma_{\leq \mathfrak{a}} : \mathrm{W}_{\mathfrak{a}*}(\mathrm{X}) \to \Gamma_{\mathfrak{a}*}(\mathrm{X})$$

is affine.

Proof. — The property satisfied by X implies that there is an open affine cover $(\mathrm{X}_i)_{i\in\mathrm{I}}$ of X such that $(\Gamma_{\mathfrak{a}*}(\mathrm{X}_i))_{i\in\mathrm{I}}$ is an open cover of $\Gamma_{\mathfrak{a}*}(\mathrm{X})$ (recall that $\Gamma_{\mathfrak{a}*}$ of a sheaf X is just a finite product of copies of X). However, the diagram

$$\begin{array}{ccc} \mathrm{W}_{\mathfrak{a}*}(\mathrm{X}_i) & \xrightarrow{\gamma_{\leq\mathfrak{a}}} & \Gamma_{\mathfrak{a}*}(\mathrm{X}_i) \\ \downarrow & & \downarrow \\ \mathrm{W}_{\mathfrak{a}*}(\mathrm{X}) & \xrightarrow{\gamma_{\leq\mathfrak{a}}} & \Gamma_{\mathfrak{a}*}(\mathrm{X}) \end{array} \tag{3.5.4.1}$$

is cartesian by Proposition 12.2 of [**5**] ([**5**] also assumes that the open immersions $\mathrm{X}_i \to \mathrm{X}$ are closed but the proof that the diagram (3.5.4.1) is cartesian does not use this assumption) and the top morphisms is affine. As $(\Gamma_{\mathfrak{a}*}(\mathrm{X}_i))_{i\in\mathrm{I}}$ is a cover of $\Gamma_{\mathfrak{a}*}(\mathrm{X})$ it follows that the bottom row of (3.5.4.1) is affine. □

3.5.5. Let S be a Λ-sheaf and X an S-group sheaf. Then to equip X with a Λ_{S}-structure making it a Λ_{S}-sheaf in groups over S is equivalent to equipping it with a Λ_{S}-structure such that the defining structure map

$$h_{\mathrm{X}/\mathrm{S}} : \mathrm{X} \to \mathrm{W}_*(\mathrm{X}) \times_{\mathrm{W}_*(\mathrm{S})} \mathrm{S}$$

is a homomorphism of S-groups (recall the W_* being a right adjoint preserves limits so that $\mathrm{W}_*(\mathrm{X})$ is a $\Lambda_{\mathrm{W}_*(\mathrm{S})}$-sheaf of groups over $\mathrm{W}_*(\mathrm{S})$).

3.5.6 Lemma. — *Let* $\mathrm{S} = \operatorname{colim}_{i\in\mathrm{I}} \mathrm{S}_i$ *be a* Λ*-ind-affine scheme,* $f : \mathrm{X} \to \mathrm{S}$ *be an* ét*-sheaf over* S *and* $\mathfrak{a} \in \mathrm{P}$*. If for each* $i \in \mathrm{I}$*, setting* $\mathrm{X}_i = \mathrm{X} \times_{\mathrm{S}} \mathrm{S}_i$*, the length-*$\mathfrak{a}$ *coghost map*

$$\gamma_{\leq\mathfrak{a}} : \mathrm{W}_{\mathfrak{a}*}(\mathrm{X}_i) \to \Gamma_{\mathfrak{a}*}(\mathrm{X}_i)$$

is affine then the length-$\mathfrak{a}$ *relative coghost map*

$$\gamma_{\mathrm{X}/\mathrm{S},\leq\mathfrak{a}} : \mathrm{W}_{\mathfrak{a}*}(\mathrm{X}) \times_{\mathrm{W}_{\mathfrak{a}*}(\mathrm{S})} \mathrm{S} \to \Gamma_{\mathfrak{a}*}(\mathrm{X}) \times_{\Gamma_{\mathfrak{a}*}(\mathrm{S})} \mathrm{S}$$

is affine.

Proof. — The morphism $\gamma_{\mathrm{X}/\mathrm{S},\leq\mathfrak{a}}$ if affine if and only if the morphisms

$$\gamma_{\mathrm{X}/\mathrm{S},\mathfrak{a}} \times_{\mathrm{S}} \mathrm{S}_i$$

are affine for each $i \in \mathrm{I}$. Fixing such an i, as S_i is affine (in particular, quasi-compact) and

$$\operatorname*{colim}_i \mathrm{W}^*_{\mathfrak{a}}(\mathrm{S}_i) = \mathrm{W}_{\mathfrak{a}*}(\operatorname*{colim}_i \mathrm{S}_i)$$

(by (iv) of (3.3.2)) there is some $j \in \mathrm{I}$ such that $\mathrm{S}_i \to \mathrm{W}_{\mathfrak{a}*}(\mathrm{S})$ factors through $\mathrm{W}_{\mathfrak{a}*}(\mathrm{S}_j) \to \mathrm{W}_{\mathfrak{a}*}(\mathrm{S})$. Therefore, we can factor $\gamma_{\mathrm{X}/\mathrm{S},\mathfrak{a}} \times_{\mathrm{S}} \mathrm{S}_i$ as the composition

$$\mathrm{W}_{\mathfrak{a}*}(\mathrm{X}_j) \times_{\mathrm{W}_{\mathfrak{a}*}(\mathrm{S}_j)} \mathrm{S}_i \to \mathrm{W}_{\mathfrak{a}*}(\mathrm{X}_j) \times_{\Gamma_{\mathfrak{a}*}(\mathrm{S}_j)} \mathrm{S}_i \to \Gamma_{\mathfrak{a}*}(\mathrm{X}_j) \times_{\Gamma_{\mathfrak{a}*}(\mathrm{S}_j)} \mathrm{S}_i$$

where the first map is induced by $\mathrm{W}_{\mathfrak{a}*}(\mathrm{S}_j) \to \Gamma_{\mathfrak{a}*}(\mathrm{S}_j)$, which is affine as $\mathrm{W}_{\mathfrak{a}*}(\mathrm{S}_j) \to \Gamma_{\mathfrak{a}*}(\mathrm{S}_j)$ is affine, and the second is $\gamma_{\leq\mathfrak{a}} \times_{\Gamma_{\mathfrak{a}*}(\mathrm{S}_j)} \mathrm{S}_i$ which is affine as $\gamma_{\mathrm{X}_j,\mathfrak{a}}$ is affine by hypothesis. Therefore, $\gamma_{\mathrm{X}/\mathrm{S},\mathfrak{a}} \times_{\mathrm{S}} \mathrm{S}_i$ is affine and we are done. □

3.5.7 Proposition. — *Let* S *be an* Λ*-ind-affine scheme, let* A *and* A' *be a pair of abelian schemes over* S *and let* $f : \mathrm{A} \to \mathrm{A}'$ *be an* S*-homomorphism. If* f *is a* Ψ_{S}*-morphism then it is a* Λ_{S}*-morphism.*

Proof. — Write $\mathrm{S} = \operatorname{colim}_{i\in\mathrm{I}} \mathrm{S}_i$ as a filtered colimit of affine schemes. By Theorem 1.9 of Chapter I of [**21**], for each $i \in \mathrm{I}$ and $\mathfrak{a} \in \mathrm{P}$, the S_i-scheme $\mathrm{A}' \times_{\mathrm{S}} \mathrm{S}_i$ satisfies the hypotheses of (3.5.4) so that we may apply (3.5.6) to deduce that the relative coghost homomorphism of length $\mathfrak{a}$

$$\gamma_{\mathrm{A}'/\mathrm{S},\mathfrak{a}} : \mathrm{W}_{\mathfrak{a}*}(\mathrm{A}') \times_{\mathrm{W}_{\mathfrak{a}*}(\mathrm{S})} \mathrm{S} \to \Gamma_{\mathfrak{a}*}(\mathrm{A}') \times_{\Gamma_{\mathfrak{a}*}(\mathrm{S})} \mathrm{S}$$

is affine. Taking the limit over $\mathfrak{a}$ we see that

$$\gamma_{\mathrm{A}'/\mathrm{S}} : \mathrm{W}_*(\mathrm{A}') \times_{\mathrm{W}_*(\mathrm{S})} \mathrm{S} \to \Gamma_*(\mathrm{A}') \times_{\Gamma_*(\mathrm{S})} \mathrm{S}$$

is affine. Now let the Λ_{S}-structures on A and A' be given by the S-homomorphisms

$$h_{\mathrm{A}/\mathrm{S}} : \mathrm{A} \to \mathrm{W}_*(\mathrm{A}) \times_{\mathrm{W}_*(\mathrm{S})} \mathrm{S} \quad \text{and} \quad h_{\mathrm{A}'/\mathrm{S}} : \mathrm{A}' \to \mathrm{W}_*(\mathrm{A}') \times_{\mathrm{W}_*(\mathrm{S})} \mathrm{S}$$

and let $f : \mathrm{A} \to \mathrm{A}'$ be a Ψ_{S}-homomorphism. By hypothesis, the difference

$$h_{\mathrm{A}'/\mathrm{S}} \circ f - (\mathrm{W}_*(f) \times_{\mathrm{W}_*(\mathrm{S})} \mathrm{S}) \circ h_{\mathrm{A}/\mathrm{S}} : \mathrm{A} \to \mathrm{W}_*(\mathrm{A}') \times_{\mathrm{W}_*(\mathrm{S})} \mathrm{S}$$

factors through the kernel of the relative coghost homomorphism $\gamma_{A/S}$. However, the kernel of $\gamma_{A/S}$ is affine over S and any homomorphism from an abelian S-scheme to an S-affine scheme is trivial. Therefore,

$$h_{A'/S} \circ f - (W_*(f) \times_{W_*(S)} S) \circ h_{A/S} = 0$$

and f is a Λ_S-homomorphism. □

3.5.8 Remark. — It follows from (3.5.7) above that if A is an abelian variety over an Λ-ind-affine scheme S then any two Λ_S-structures on A, compatible with the group law, coincide if and only if the underlying Ψ_S-structures coincide.

CHAPTER 4

CM ELLIPTIC CURVES AND Λ-STRUCTURES

In this chapter we explain the connection between CM elliptic curves and Λ-structures. The first and main result being, essentially, that the moduli stack of CM elliptic curves $\mathscr{M}_{\mathrm{CM}}$ admits a Λ-structure. The observant reader will have noticed that we have not defined what it means for a stack to have a Λ-structure and we do not propose to do so here (not because we cannot but only because to do so would involve various 2-categorical issues that would in this instance serve only to make matters more complicated than they need be). However, we shall explain what we mean to prove.

We continue with the set-up in (2.2.1). So that all sheaves considered are always over $\mathrm{Spec}(\mathrm{O_K})$ and we will use the theory of Chapter 3 with Λ-structures relative to the full monoid of ideals $\mathrm{Id}_{\mathrm{O_K}}$ (later we will also consider submonoids).

Recall that to give a ét-sheaf X a Λ-structure is to give for each ét-sheaf S, a map

$$h_{\mathrm{X}}(\mathrm{S}) : \mathrm{X}(\mathrm{S}) \to \mathrm{X}(\mathrm{W}^*(\mathrm{S}))$$

which is functorial in S and such that:

(i) the composition

$$\mathrm{X}(\mathrm{S}) \overset{h_{\mathrm{X}}(\mathrm{S})}{\to} \mathrm{X}(\mathrm{W}^*(\mathrm{S})) \overset{\mathrm{X}(g_{(1)})}{\to} \mathrm{X}(\mathrm{S})$$

is the identity and

(ii) the two compositions

$$\mathrm{X}(\mathrm{S}) \xrightarrow{h_{\mathrm{X}}(\mathrm{S})} \mathrm{X}(\mathrm{W}^*(\mathrm{S})) \underset{h_{\mathrm{X}}(\mathrm{W}^*(\mathrm{S}))}{\overset{\mathrm{X}(\mu_{\mathrm{W}^*(\mathrm{S})})}{\rightrightarrows}} \mathrm{X}(\mathrm{W}^*(\mathrm{W}^*(\mathrm{S})))$$

are equal.

To this end we show that given an ind-affine scheme S and an element of $\mathscr{M}_{\mathrm{CM}}(\mathrm{S})$, i.e. a CM elliptic curve E/S, there is a functorially associated element of $\mathscr{M}_{\mathrm{CM}}(\mathrm{W}^*(\mathrm{S}))$, i.e. a CM elliptic curve $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})/\mathrm{W}^*(\mathrm{S})$, satisfying the following properties:

(i) the pull-back of $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})$ along the ghost component at (1) is canonically isomorphic to E:

$$\mathrm{E} \xrightarrow{\sim} g^*_{(1)}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})) = \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{S},$$

(ii) the pull-back of $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})$ along $\mu_{\mathrm{S}} : \mathrm{W}^*(\mathrm{W}^*(\mathrm{S})) \to \mathrm{W}^*(\mathrm{S})$ is canonically isomorphic to $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}))$:

$$\mu^*_{\mathrm{S}}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})) = \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{W}^*(\mathrm{S})) \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})).$$

We call $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})/\mathrm{W}^*(\mathrm{S})$ the canonical lift of E/S. In addition to (i) and (ii) above, we also show that the CM elliptic curve $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})$ admits a canonical $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure. It is worth pointing out that these 'canonical lifts' are both global and big – the base is S is an arbitrary ind-affine scheme over $\mathrm{Spec}(\mathrm{O_K})$ and the Witt vectors over which we lift the CM elliptic curves have Frobenius lifts at all primes of $\mathrm{O_K}$.

We now give a brief overview of each of the sections. The construction of $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})/\mathrm{W}^*(\mathrm{S})$ and the verification of its properties is the content of §1. We also use this to define what it means for a CM elliptic curve over Λ-ind-affine scheme E/S to have a canonical Λ-structure (what we really do is define what it means for a morphism

$$\mathrm{S} \xrightarrow{\mathrm{E}} \mathscr{M}_{\mathrm{CM}}$$

corresponding to a CM elliptic curve E/S to be a Λ-morphism).

In §2 we consider a certain special class of CM elliptic curves (those of 'Shimura type') and show that they are exactly those admitting Λ-structures. These curves were first defined and studied by Shimura ([**33**]), and subsequently by several other authors with particular reference to their L-functions (see [**13**], [**17**] and [**30**]). We finish §2 by showing that many CM elliptic curves of Shimura type admit global minimal models. This gives a broad generalisation of a result of Gross [**22**]. The proof we give is quite different to that in [**22**] and relies ons a certain strengthening (A.4.8) of an old principal ideal theorem (valid for arbitrary number fields).

In §3 we show how to (intelligently) construct the quotient of the universal CM elliptic curve by its group of automorphisms and we show that this curve descends to a smooth projective curve $\mathrm{X} \to \mathrm{M_{CM}}$ over the coarse sheaf $\mathrm{M_{CM}}$. We also show that this descended curved admits a $\Lambda_{\mathrm{M_{CM}}}$-structure and that this $\Lambda_{\mathrm{M_{CM}}}$-structure can be used to construct the maximal abelian extension of K in a natural way. This gives a canonical, integral and Λ-theoretic version of the explicit generation of the ray class fields of K using Weber functions of CM elliptic curves over fields. We end this section by showing that the possibly mysterious curve X is non-other than $\mathbf{P}^1_{\mathrm{M_{CM}}}$.

In §4 we use the results of §1 and §2 to construct a flat affine formally smooth presentation $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}} \to \mathscr{M}_{\mathrm{CM}}$ of $\mathscr{M}_{\mathrm{CM}}$. The flat affine formally smooth scheme $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}$ has a natural moduli theoretic interpretation, and is also a torsor

under a certain affine flat affine group scheme $\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}$. Finally, we show that $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}$ admits a natural Λ-structure compatible with that on $\mathscr{M}_{\mathrm{CM}}$.

In §5 we exhibit a rather interesting relationship between a (variant of) the canonical lift of an CM elliptic curve (over an arbitrary base) and its Tate module. This gives an analogue for CM elliptic curves of a certain construction in p-adic Hodge theory involving Lubin–Tate O-modules and we end by sketching a certain analytic analogue.

4.1. Canonical lifts of CM elliptic curves

We continue with the set-up of Chapter 2, so that we work over the base scheme $\mathrm{Spec}(\mathrm{O_K})$ where $\mathrm{O_K}$ is the ring of integers of an imaginary quadratic field. In order to apply the theory of Chapter 3, we will no longer be working with arbitrary sheaves $\mathrm{S} \in \mathrm{Sh}_{\mathrm{O_K}}$ but only with ind-affine schemes $\mathrm{S} \in \mathrm{IndAff}_{\mathrm{O_K}} \subset \mathrm{Sh}_{\mathrm{O_K}}$.

By a Λ-structure is meant one relative to the Dedekind domain $\mathrm{O_K}$ and to the full set of ideals $\mathrm{P} = \mathrm{Id}_{\mathrm{O_K}}$.

We note that if S is an ind-affine scheme then $\mathrm{W}^*(\mathrm{S})$ is again an ind-affine scheme and therefore a sheaf for the fpqc topology. Moreover, $\mathrm{W}_*(\mathrm{S}) = \lim_{\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}} \mathrm{W}_{\mathfrak{a}*}(\mathrm{S})$ is an inverse limit of ind-affine schemes (as $\mathrm{W}_{\mathfrak{a}*}$ commutes with filtered colimits and sends affine schemes to affine schemes) and is also a sheaf for the fpqc topology.

For technical reasons we also work with the affine étale topology on $\mathrm{IndAff}_{\mathrm{O_K}}$ whose covers are given by families of affine étale morphisms $(\mathrm{S}_i \to \mathrm{S})_{i \in \mathrm{I}}$ which are covers when viewed in $\mathrm{Sh}_{\mathrm{O_K}}$ (or equivalently $\mathrm{Sh}^{\text{ét}}_{\mathrm{O_K}}$).

We shall also continue to work with the fibred category $\mathscr{M}_{\mathrm{CM}}$ but from here on view it as a fibred category over the category of ind-affine schemes $\mathrm{IndAff}_{\mathrm{O_K}} \subset \mathrm{Sh}_{\mathrm{O_K}}$, rather than all of $\mathrm{Sh}_{\mathrm{O_K}}$.

Unless otherwise noted S will denote an arbitrary ind-affine scheme.

4.1.1. Denote by $\mathscr{L}_{\mathrm{CM}}$ the rank one $\mathrm{O_K}$-local system over $\Gamma^*(\mathrm{Spec}(\mathrm{O_K}))$ whose fibre over the ghost component at $\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}$ is the constant sheaf $\underline{\mathfrak{a}}^{-1}$, i.e.

$$\mathscr{L}_{\mathrm{CM}} = \coprod_{\mathfrak{a} \in \mathrm{Id}_{\mathrm{O}}} \underline{\mathfrak{a}}^{-1} \to \coprod_{\mathfrak{a} \in \mathrm{Id}_{\mathrm{O}}} \mathrm{Spec}(\mathrm{O_K}) = \Gamma^*(\mathrm{Spec}(\mathrm{O_K})).$$

For an ind-affine scheme S we shall abuse notation and write $\mathscr{L}_{\mathrm{CM}}$ for the rank one $\mathrm{O_K}$-local system over $\Gamma^*(\mathrm{S})$ obtained by pulling back $\mathscr{L}_{\mathrm{CM}}$ along $\Gamma^*(\mathrm{S}) \to \Gamma^*(\mathrm{Spec}(\mathrm{O_K}))$.

4.1.2. Let $\mathrm{E} \to \mathrm{S}$ a CM elliptic curve . Writing $p_{\mathrm{S}} : \Gamma^*(\mathrm{S}) \to \mathrm{S}$ for the map

$$\coprod_{\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}} \mathrm{id}_{\mathrm{S}} : \Gamma^*(\mathrm{S}) = \coprod_{\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}} \mathrm{S} \to \mathrm{S},$$

we define a new CM elliptic curve over $\Gamma^*(S)$ by

$$\Gamma^*_{CM}(E) = p_S^*(E) \otimes_{O_K} \mathscr{L}_{CM}.$$

In other words, we have

$$\Gamma^*_{CM}(E) = \coprod_{\mathfrak{a} \in \mathrm{Id}_{O_K}} E \otimes_{O_K} \mathfrak{a}^{-1} \to \coprod_{\mathfrak{a} \in \mathrm{Id}_{O_K}} S = \Gamma^*(S).$$

If $f : E \to E'$ is a homomorphism of CM elliptic curves over S then we write

$$\Gamma^*_{CM}(f) = p_S^*(f) \otimes_{O_K} \mathscr{L}_{CM} : \Gamma^*_{CM}(E) \to \Gamma^*_{CM}(E')$$

so that Γ^*_{CM} defines a functor from the category of CM elliptic curves over S to the category of CM elliptic curves over $\Gamma^*(S)$.

By construction, the rank one O_K-local system $\mathscr{L}_{CM}$ over $\Gamma^*(S)$ satisfies $\mathscr{L}_{CM} \otimes_{O_K} \mathfrak{a}^{-1} = \psi^{\mathfrak{a}*}(\mathscr{L}_{CM})$ for each ideal $\mathfrak{a}$ and this induces isomorphisms

$$\Gamma^*_{CM}(E) \otimes_{O_K} \mathfrak{a}^{-1} \xrightarrow{\sim} \psi^{\mathfrak{a}*}(\Gamma^*_{CM}(E)).$$

We equip $\Gamma^*_{CM}(E)$ with the $\Psi_{\Gamma^*(S)}$-structure with the relative endomorphisms given for each ideal $\mathfrak{a}$ by the composition

$$\Gamma^*_{CM}(E) \xrightarrow{i_{\mathfrak{a}}} \Gamma^*_{CM}(E) \otimes_{O_K} \mathfrak{a}^{-1} \xrightarrow{\sim} \psi^{\mathfrak{a}*}(\Gamma^*_{CM}(E)).$$

In order to avoid overly cumbersome notation, we will denote this map by $\varphi^{\mathfrak{a}}_{E/S}$ (instead of by the usual by monstrous $\psi^{\mathfrak{a}*}_{\Gamma^*_{CM}(E)/\Gamma^*(S)}$). Note that $\ker(\varphi^{\mathfrak{a}}_{E/S}) = \Gamma^*_{CM}(E)[\mathfrak{a}]$.

The sheaf of rings $\underline{O_K}_{\Gamma^*(S)} = \Gamma^*(\underline{O_K}_S)$ is naturally a sheaf of $\Psi_{\Gamma^*(S)}$-rings and the $\underline{O_K}_{\Gamma^*(S)}$-module structure

$$\underline{O_K}_{\Gamma^*(S)} \times \Gamma^*_{CM}(E) \to \Gamma^*_{CM}(E)$$

is compatible with the $\Psi_{\Gamma^*(S)}$-structures.

If $S' \to S$ is a morphism there is a obvious isomorphism of CM elliptic curves over $\Gamma^*(S')$ equipped with $\Psi_{\Gamma^*(S')}$-structures

$$\Gamma^*_{CM}(E) \times_{\Gamma^*(S)} \Gamma^*(S') \xrightarrow{\sim} \Gamma^*_{CM}(E \times_S S').$$

4.1.3. Write $\Gamma_*(\mathscr{M}_{CM})_\Psi$ for the fibred category over IndAff_{O_K} whose fibre over S is the essential image of the functor $E/S \mapsto \Gamma^*_{CM}(E)/\Gamma^*(S)$ from CM elliptic curves over S to CM elliptic curves over $\Gamma^*(S)$ equipped with $\Psi_{\Gamma^*(S)}$-structures compatible with their $\underline{O_K}_{\Gamma^*(S)}$-module structure. The pull-back maps for $S' \to S$ are given by

$$E/\Gamma^*(S) \mapsto E \times_{\Gamma^*(S)} \Gamma^*(S')/\Gamma^*(S').$$

4.1.4 Remark. — The symbol $\Gamma_*(\mathscr{M}_{\mathrm{CM}})_\Psi$ is only notation but it supposed to inspire the following interpretation. Assuming $\mathscr{M}_{\mathrm{CM}}$ did admit a Λ-structure, and so a fortiori a Ψ-structure, then we should have equivalences

$$\mathscr{M}_{\mathrm{CM}}(\mathrm{S}) = \mathrm{Hom}(\mathrm{S}, \mathscr{M}_{\mathrm{CM}}) \xrightarrow{\sim} \mathrm{Hom}^{\Psi}_{\mathrm{Spec}(\mathrm{O_K})}(\Gamma^*(\mathrm{S}), \mathscr{M}_{\mathrm{CM}}) = \Gamma_*(\mathscr{M}_{\mathrm{CM}})_\Psi(\mathrm{S}).$$

Of course, we do not define a Ψ-structure on $\mathscr{M}_{\mathrm{CM}}$. Instead we opt to define which morphisms (equivalently CM elliptic curves $\mathrm{E}/\Gamma^*(\mathrm{S})$)

$$\Gamma^*(\mathrm{S}) \xrightarrow{\mathrm{E}} \mathscr{M}_{\mathrm{CM}}$$

should be though of as (coming from) Ψ-morphisms. The following gives some justification to this.

4.1.5 Lemma. — *The functor*

$$\mathscr{M}_{\mathrm{CM}} \to \Gamma_*(\mathscr{M}_{\mathrm{CM}})_\Psi : \mathrm{E}/\mathrm{S} \mapsto \Gamma^*_{\mathrm{CM}}(\mathrm{E})/\Gamma^*(\mathrm{S})$$

is an equivalence of stacks with quasi-inverse given by pull-back along the ghost component at (1)

$$\mathrm{E}/\Gamma^*(\mathrm{S}) \mapsto g^*_{(1)}(\mathrm{E})/\mathrm{S}.$$

Proof. — The functor in question is clearly essentially surjective and faithful as composing it with

$$\mathrm{E}/\Gamma^*(\mathrm{S}) \mapsto g^*_{(1)}(\mathrm{E})/\mathrm{S}$$

yields a functor isomorphic to the identity on $\mathscr{M}_{\mathrm{CM}}$. Now to see that it is an equivalence, and that $\mathrm{E}/\Gamma^*(\mathrm{S}) \mapsto g^*_{(1)}(\mathrm{E})/\mathrm{S}$ is a quasi-inverse, we need only show that it is full.

So let $f : \Gamma^*_{\mathrm{CM}}(\mathrm{E}) \to \Gamma^*_{\mathrm{CM}}(\mathrm{E}')$ be a $\Psi_{\Gamma^*(\mathrm{S})}$-isomorphism and write f as the sum of its ghost components

$$f = \coprod_{\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}} g^*_{\mathfrak{a}}(f).$$

As f is a $\Psi_{\Gamma^*(\mathrm{S})}$-homomorphism the diagram

$$\begin{array}{ccc} \mathrm{E} & \xrightarrow{g^*_{(1)}(f)} & \mathrm{E}' \\ {\scriptstyle i_{\mathfrak{a}}}\downarrow & & \downarrow{\scriptstyle i_{\mathfrak{a}}} \\ \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} & \xrightarrow{g^*_{\mathfrak{a}}(f)} & \mathrm{E}' \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \end{array}$$

commutes for each $\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}$ by the definition of $\Gamma^*_{\mathrm{CM}}(\mathrm{E})$ and $\Gamma^*_{\mathrm{CM}}(\mathrm{E}')$ and their $\Psi_{\Gamma^*(\mathrm{S})}$-structures. However, as $i_{\mathfrak{a}}$ is epimorphism the only map $g^*_{\mathfrak{a}}(f)$ for which this is possible is $g^*_{(1)}(f) \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}$. It follows that

$$f = \coprod_{\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}} g^*_{(1)}(f) \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} = \Gamma^*_{\mathrm{CM}}(g^*_{(1)}(f))$$

and we are done. □

4.1.6. Let $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ be a CM elliptic curve equipped with a $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure compatible with its $\underline{\mathrm{O}_\mathrm{K}}_{\mathrm{W}^*(\mathrm{S})} = \mathrm{W}^*(\underline{\mathrm{O}_\mathrm{K}}_\mathrm{S})$-module structure. We say that the $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure on $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ is canonical if there exists a $\Psi_{\Gamma^*(\mathrm{S})}$-isomorphism

$$\mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S}) \xrightarrow{\sim} \Gamma^*_{\mathrm{CM}}(g^*_{(1)}(\mathrm{E}))$$

inducing the identity on $g^*_{(1)}(\mathrm{E})$ after pull-back along $g_{(1)} : \mathrm{S} \to \Gamma^*(\mathrm{S})$. Such an isomorphism is unique by (4.1.5) and so, when it exists, we shall denote it by $\rho_{\mathrm{E}/\mathrm{W}^*(\mathrm{S})}$.

4.1.7 Lemma. — *Let* $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ *be a* CM *elliptic curve.*

(i) E *admits at most one canonical* $\Lambda_{\mathrm{W}^*(\mathrm{S})}$*-structure.*

(ii) *If* $\mathrm{S}' \to \mathrm{S}$ *is a morphism of ind-affine schemes then, writing* $\mathrm{E}' = \mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{S}')$*, the* $\Lambda_{\mathrm{W}^*(\mathrm{S}')}$*-structure on* E' *is canonical and*

$$\rho_{\mathrm{E}/\mathrm{W}^*(\mathrm{S})} \times_{\Gamma^*(\mathrm{S})} \Gamma^*(\mathrm{S}') = \rho_{\mathrm{E}'/\mathrm{W}^*(\mathrm{S}')}.$$

(iii) *Let* $(\mathrm{S}_i \to \mathrm{S})_{i\in\mathrm{I}}$ *be an affine étale cover in* $\mathrm{IndAff}_{\mathrm{O}_\mathrm{K}}$*. If* $\mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{S}_i)$ *admits a canonical* $\Lambda_{\mathrm{W}^*(\mathrm{S}_i)}$*-structure for each* $i \in \mathrm{I}$ *then* $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ *admits a canonical* $\Lambda_{\mathrm{W}^*(\mathrm{S})}$*-structure.*

Proof. — (i) Let $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ have a pair of canonical $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structures and write $\rho_{\mathrm{E}/\mathrm{W}^*(\mathrm{S}),1}$ and $\rho_{\mathrm{E}/\mathrm{W}^*(\mathrm{S}),2}$ for the corresponding unique isomorphisms

$$\mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S}) \xrightarrow{\sim} \Gamma^*_{\mathrm{CM}}(g^*_{(1)}(\mathrm{E}))$$

inducing the identity on $g^*_{(1)}(\mathrm{E})$ after pull-back along $g_{(1)} : \mathrm{S} \to \Gamma^*(\mathrm{S})$. The composition

$$\rho^{-1}_{\mathrm{E}/\mathrm{W}^*(\mathrm{S}),1} \circ \rho_{\mathrm{E}/\mathrm{W}^*(\mathrm{S}),2}$$

defines an $\Psi_{\Gamma^*(\mathrm{S})}$-automorphism of $\Gamma^*_{\mathrm{CM}}(g^*_{(1)}(\mathrm{E}))$ which is the identity on $g^*_{(1)}(\mathrm{E})$ after pull-back along $g_{(1)}$ and so is the identity itself by (4.1.5).

It follows that the two $\Psi_{\Gamma^*(\mathrm{S})}$-structures on each $\mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S})$, induced by the two $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structures on E and E', are equal. Writing

$$\psi^{\mathfrak{p}}_{\mathrm{E}/\mathrm{W}^*(\mathrm{S}),1}, \psi^{\mathfrak{p}}_{\mathrm{E}/\mathrm{W}^*(\mathrm{S}),2} : \mathrm{E} \to \psi^{\mathfrak{p}*}(\mathrm{E})$$

for the relative Frobenius lifts at $\mathfrak{p}$ corresponding to the two $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structures, we have shown that

$$\psi^{\mathfrak{p}}_{\mathrm{E}/\mathrm{W}^*(\mathrm{S}),1} \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S}) = \psi^{\mathfrak{p}}_{\mathrm{E}/\mathrm{W}^*(\mathrm{S}),2} \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S}).$$

As $\Gamma^*(\mathrm{S}) \to \mathrm{W}^*(\mathrm{S})$ is surjective on geometric points (3.5.1), it follows by rigidity that

$$\psi^{\mathfrak{p}}_{\mathrm{E}/\mathrm{W}^*(\mathrm{S}),1} = \psi^{\mathfrak{p}}_{\mathrm{E}/\mathrm{W}^*(\mathrm{S}),2}.$$

Therefore, the two $\Psi_{\mathrm{W}^*(\mathrm{S})}$-structures on $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ induced by the two $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structures are equal and by (3.5.8) it follows that the two $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structures themselves are equal.

(ii) The CM elliptic curve $\mathrm{E}' := \mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{S}')$ has a natural $\Lambda_{\mathrm{W}^*(\mathrm{S}')}$-structure and the pull-back of $\rho_{\mathrm{E}/\mathrm{W}^*(\mathrm{S})}$ along $\Gamma^*(\mathrm{S}') \to \Gamma^*(\mathrm{S})$ defines a $\Psi_{\Gamma^*(\mathrm{S}')}$-isomorphism

$$\mathrm{E}' \times_{\mathrm{W}^*(\mathrm{S}')} \Gamma^*(\mathrm{S}') = \mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S}') \overset{\rho_{\mathrm{E}/\mathrm{W}^*(\mathrm{S})} \times_{\Gamma^*(\mathrm{S})} \Gamma^*(\mathrm{S}')}{\longrightarrow} \Gamma^*_{\mathrm{CM}}(g^*_{(1)}(\mathrm{E})) \times_{\Gamma^*(\mathrm{S})} \Gamma^*(\mathrm{S}') = \Gamma^*_{\mathrm{CM}}(g^*_{(1)}(\mathrm{E}'))$$

inducing the identity after pull-back along $g_{(1)}$. It follows by uniqueness of such an isomorphism that

$$\rho_{\mathrm{E}/\mathrm{W}^*(\mathrm{S})} \times_{\Gamma^*(\mathrm{S})} \Gamma^*(\mathrm{S}') = \rho_{\mathrm{E}'/\mathrm{W}^*(\mathrm{S}')}.$$

(iii) We will first show that $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ admits a unique $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure inducing the canonical $\Lambda_{\mathrm{W}^*(\mathrm{S}_i)}$-structures on $\mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{S}_i)$ and then show that this $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure is canonical. The family $(\mathrm{W}^*(\mathrm{S}_i) \to \mathrm{W}^*(\mathrm{S}))_{i \in \mathrm{I}}$ is a cover in $\mathrm{Sh}^{\text{ét}}_{\Lambda}$ and we have

$$\mathrm{W}^*(\mathrm{S}_{ij}) := \mathrm{W}^*(\mathrm{S}_i \times_{\mathrm{S}} \mathrm{S}_j) \xrightarrow{\sim} \mathrm{W}^*(\mathrm{S}_i) \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{S}_j)$$

by (3.3.13). By (ii) above, the two $\Lambda_{\mathrm{W}^*(\mathrm{S}_{ij})}$-structures on

$$\mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{S}_{ij})$$

induced by pull-back are canonical and by (i) they are equal. By (3.4.4), this defines an element of the equaliser

$$\Lambda_{\mathrm{E}/\mathrm{W}^*(\mathrm{S})}(\mathrm{W}^*(\mathrm{S})) \longrightarrow \Lambda_{\mathrm{E}/\mathrm{W}^*(\mathrm{S})}(\mathrm{W}^*(\mathrm{S}_i)) \rightrightarrows \prod_{i,j \in \mathrm{I}} \Lambda_{\mathrm{E}/\mathrm{W}^*(\mathrm{S})}(\mathrm{W}^*(\mathrm{S}_{ij}))$$

or in other words, there is a unique $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure on $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ inducing the canonical $\Lambda_{\mathrm{W}^*(\mathrm{S}_i)}$-structures on each $\mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{S}_i)$. The uniqueness of the isomorphisms $\rho_{\mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{S}_i)/\mathrm{W}^*(\mathrm{S}_i)}$ and their compatibility with pull-backs (this is (ii) above) show that they descend to an $\Psi_{\Gamma^*(\mathrm{S})}$-isomorphism

$$\rho_{\mathrm{E}/\mathrm{W}^*(\mathrm{S})} : \mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S}) \xrightarrow{\sim} \Gamma^*_{\mathrm{CM}}(g^*_{(1)}(\mathrm{E}))$$

inducing the identity after pull-back along $g_{(1)}$ so that the $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure on $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ is canonical. □

4.1.8. Using (4.1.7) we may define a fibred category $\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_{\Lambda}$ over $\mathrm{IndAff}_{\mathrm{O_K}}$ by setting the fibre over S to be the category of CM elliptic curves $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ equipped with a canonical $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure and whose pull-back maps for $\mathrm{S}' \to \mathrm{S}$ are given by

$$\mathrm{E}/\mathrm{W}^*(\mathrm{S}) \mapsto \mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{S}').$$

4.1.9 Remark. — As with $\Gamma_*(\mathscr{M}_{\mathrm{CM}})_{\Psi}$ the symbol $\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_{\Lambda}$ is supposed to inspire in the reader the idea that $\mathscr{M}_{\mathrm{CM}}$ admits some Λ-structure and that we have

$$\mathscr{M}_{\mathrm{CM}}(\mathrm{S}) = \mathrm{Hom}_{\mathrm{Spec}(\mathrm{O_K})}(\mathrm{S}, \mathscr{M}_{\mathrm{CM}}) \xrightarrow{\sim} \mathrm{Hom}^{\Lambda}_{\mathrm{Spec}(\mathrm{O_K})}(\mathrm{W}^*(\mathrm{S}), \mathscr{M}_{\mathrm{CM}}) = \mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_{\Lambda}(\mathrm{S}).$$

4.1.10 Lemma. — *The fibred category* $\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_\Lambda$ *over* $\mathrm{IndAff}_{\mathrm{O_K}}$ *is a stack for the affine étale topology.*

Proof. — Let $(\mathrm{S}_i \to \mathrm{S})_{i\in\mathrm{I}}$ be an affine étale cover and let $(\mathrm{E}_i/\mathrm{W}^*(\mathrm{S}_i))_{i\in\mathrm{I}}$ be a collection of objects of $\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_\Lambda$ equipped with descent data relative to the cover $(\mathrm{S}_i \to \mathrm{S})_{i\in\mathrm{I}}$. By (ii) of (3.3.13) we have

$$\mathrm{W}^*(\mathrm{S}_{ij}) := \mathrm{W}^*(\mathrm{S}_i \times_{\mathrm{S}} \mathrm{S}_j) \xrightarrow{\sim} \mathrm{W}^*(\mathrm{S}_i) \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{S}_j)$$

an so we may view the objects $(\mathrm{E}_i/\mathrm{W}^*(\mathrm{S}_i))_{i\in\mathrm{I}}$ of $\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_\Lambda$ equipped with their descent data relative to the affine étale cover $(\mathrm{S}_i \to \mathrm{S})_{i\in\mathrm{I}}$ as objects of $\mathscr{M}_{\mathrm{CM}}$ equipped with descent data relative to the fpqc cover $(\mathrm{W}^*(\mathrm{S}_i) \to \mathrm{W}^*(\mathrm{S}))_{i\in\mathrm{I}}$. As $\mathscr{M}_{\mathrm{CM}}$ is a stack over $\mathrm{Sh}_{\mathrm{O_K}}$ (2.1.2), the family $(\mathrm{E}_i/\mathrm{W}^*(\mathrm{S}_i))_{i\in\mathrm{I}}$ descends to a CM elliptic curve $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ unique upto compatible isomorphisms $\mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{S}_i) \xrightarrow{\sim} \mathrm{E}_i$. It remains to see that $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ admits a canonical $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure and this follows from (iii) of (4.1.7).

In much the same way, using (3.3.13) and (3.4.3), Λ-isomorphisms of CM elliptic curves with canonical Λ-structures also satisfy descent for the affine étale topology and we find that $\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_\Lambda$ is a stack over $\mathrm{IndAff}_{\mathrm{O_K}}$. □

4.1.11 Theorem. — *The functor induced by base change along the ghost component at* (1)

$$\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_\Lambda \to \mathscr{M}_{\mathrm{CM}} : \mathrm{E}/\mathrm{W}^*(\mathrm{S}) \mapsto g_{(1)}^*(\mathrm{E})/\mathrm{S}$$

is an equivalence of stacks over $\mathrm{IndAff}_{\mathrm{O_K}}$ *for the affine étale topology.*

Proof. — The functor in question factors as

$$\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_\Lambda \to \Gamma_*(\mathscr{M}_{\mathrm{CM}})_\Psi \to \mathscr{M}_{\mathrm{CM}}$$

where the first functor is $\mathrm{E}/\mathrm{W}^*(\mathrm{S}) \mapsto \mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S})/\Gamma^*(\mathrm{S})$ and the second is pull-back along $g_{(1)} : \mathrm{S} \to \Gamma^*(\mathrm{S})$. By (4.1.5) the second functor is an equivalence and, as $\Gamma^*(\mathrm{S}) \to \mathrm{W}^*(\mathrm{S})$ is surjective on geometric points, the first functor is faithful by rigidity. Therefore,

$$\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_\Lambda \to \mathscr{M}_{\mathrm{CM}}$$

is faithful.

Now fix a pair $\mathrm{E}, \mathrm{E}'/\mathrm{W}^*(\mathrm{S})$ of CM elliptic curves equipped with canonical $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structures and let $f : \mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S}) \to \mathrm{E}' \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S})$ be a $\Psi_{\Gamma^*(\mathrm{S})}$-isomorphism. Let $\mathfrak{p}$ be a prime ideal, $\mathfrak{a}$ any ideal and $n \geq 0$ an integer.

Consider the diagram:

$$\begin{array}{ccc}
\overline{g_{\mathfrak{a}}^*(\mathrm{E})} & \xrightarrow{\overline{g_{\mathfrak{a}}^*(f)}} & \overline{g_{\mathfrak{a}}^*(\mathrm{E}')} \\
\downarrow{\scriptstyle \overline{g_{\mathfrak{a}}^*(\psi_{\mathrm{E}}^{\mathfrak{p}^n})}} & & \downarrow{\scriptstyle \overline{(g_{\mathfrak{a}}^*(\psi_{\mathrm{E}'}^{\mathfrak{p}^n})}} \\
\overline{g_{\mathfrak{a}\mathfrak{p}^n}^*(\mathrm{E})} & \xrightarrow{\overline{g_{\mathfrak{a}\mathfrak{p}^n}^*(f)}} & \overline{g_{\mathfrak{a}\mathfrak{p}^n}^*(\mathrm{E}')} \\
\wr\downarrow & & \downarrow\wr \\
\mathrm{Fr}_{\overline{\mathrm{S}}}^{\mathrm{N}\mathfrak{p}^n *}(\overline{g_{\mathfrak{a}}^*(\mathrm{E})}) & \xrightarrow{\mathrm{Fr}_{\overline{\mathrm{S}}}^{\mathrm{N}\mathfrak{p}^n *}(\overline{g_{\mathfrak{a}}^*(f)})} & \mathrm{Fr}_{\overline{\mathrm{S}}}^{\mathrm{N}\mathfrak{p}^n *}(\overline{g_{\mathfrak{a}}^*(\mathrm{E}')}),
\end{array} \tag{4.1.11.1}$$

where the bar denotes pull-back along $\overline{\mathrm{S}} = \mathrm{S} \times_{\mathrm{Spec}(\mathrm{O_K})} \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}}) \to \mathrm{S}$ and the bottom vertical isomorphisms are the unique such making the vertical compositions equal to the $\mathrm{N}\mathfrak{p}^n$-power relative Frobenius morphisms of $\overline{g_{\mathfrak{a}}^*(\mathrm{E})}$ and $\overline{g_{\mathfrak{a}}^*(\mathrm{E}')}$ respectively (such isomorphisms exist as $\psi_{\mathrm{E}}^{\mathfrak{p}^n} : \mathrm{E} \to \mathrm{E}$ and $\psi_{\mathrm{E}'}^{\mathfrak{p}^n} : \mathrm{E}' \to \mathrm{E}'$ lift the $\mathrm{N}\mathfrak{p}^n$-power Frobenius). As f is a $\Psi_{\Gamma^*(\mathrm{S})}$-morphism, the top square of (4.1.11.1) commutes and, by functoriality of the $\mathrm{N}\mathfrak{p}^n$-power relative Frobenius, the outer square commutes. As $\overline{g_{\mathfrak{a}}^*(\psi_{\mathrm{E}}^{\mathfrak{p}^n})}$ is an epimorphism, it follows that the bottom square of (4.1.11.1) also commutes. We will show that this implies that the functor

$$\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_\Lambda \to \mathscr{M}_{\mathrm{CM}}$$

is full.

For the functor to be full, it is enough to show that the (injective) map

$$\mathrm{Isom}_{\mathrm{W}^*(\mathrm{S})}^{\mathrm{O_K},\Lambda}(\mathrm{E},\mathrm{E}') \to \mathrm{Isom}_{\Gamma^*(\mathrm{S})}^{\mathrm{O_K},\Psi}(\mathrm{E}_{\Gamma^*(\mathrm{S})},\mathrm{E}'_{\Gamma^*(\mathrm{S})})$$

is surjective (where the super script Λ and Ψ denote Λ- and Ψ-morphisms). Now to show this, it is enough to show that each $\Psi_{\Gamma^*(\mathrm{S})}$-isomorphism

$$f : \mathrm{E}_{\Gamma^*(\mathrm{S})} \to \mathrm{E}'_{\Gamma^*(\mathrm{S})}$$

is obtained via pull-back from an isomorphism $\mathrm{E} \to \mathrm{E}'$ over $\mathrm{W}^*(\mathrm{S})$ as by (3.5.7) it will follow that any such isomorphism $\mathrm{E} \to \mathrm{E}'$ is also a $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-isomorphism.

Applying (3.5.2) and (3.5.3) to the finite étale $\mathrm{W}^*(\mathrm{S})$-sheaf

$$\underline{\mathrm{Isom}}_{\mathrm{W}^*(\mathrm{S})}^{\mathrm{O_K}}(\mathrm{E},\mathrm{E}'),$$

we see that f comes from a morphism $\mathrm{E} \to \mathrm{E}'$ over $\mathrm{W}^*(\mathrm{S})$ if and only if, for each prime $\mathfrak{p}$, each ideal $\mathfrak{a}$ and each $n \geq 0$, the two pull-backs of f to $\overline{\mathrm{S}} := \mathrm{S} \times_{\mathrm{Spec}(\mathrm{O_K})} \mathrm{Spec}(\mathbf{F}_{\mathfrak{p}})$ along the maps

$$\overline{\mathrm{S}} \subset \mathrm{S} \xrightarrow{g_{\mathfrak{a}\mathfrak{p}^n}} \Gamma^*(\mathrm{S}) \quad \text{and} \quad \overline{\mathrm{S}} \xrightarrow{\mathrm{Fr}_{\overline{\mathrm{S}}}^{\mathrm{N}\mathfrak{p}^n}} \overline{\mathrm{S}} \subset \mathrm{S} \xrightarrow{g_{\mathfrak{a}}} \Gamma^*(\mathrm{S})$$

of (3.5.3) are equal. This is precisely the commutativity of the bottom square of the diagram (4.1.11.1) and therefore

$$\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_\Lambda \to \mathscr{M}_{\mathrm{CM}}$$

is full.

Finally, for the functor in question to be an equivalence it is enough (as both categories are stacks and we have already shown that it is fully faithful) to show that for each ind-affine scheme S and each CM elliptic curve E/S there is an affine étale cover $(S_i \to S)_{i\in I}$ such that $E \times_S S_i$ is in the essential image of

$$W_*(\mathscr{M}_{CM})_\Lambda \to \mathscr{M}_{CM}.$$

By (2.2.12) the family of S-sheaves

$$(\underline{\mathrm{Isom}}_S^{O_K}(E[\mathfrak{f}], \underline{O_K/\mathfrak{f}}_S) \to S)_\mathfrak{f}$$

indexed by integral ideals $\mathfrak{f}$ which separate units forms an affine étale cover of S. We may then base change to any element of this cover and assume that E/S admits a level-$\mathfrak{f}$ structure for some integral ideal $\mathfrak{f}$ which separates units, and then we may assume that $E/S = E^{(\mathfrak{f})}/M_{CM}^{(\mathfrak{f})}$. This case is (4.1.12) below. □

4.1.12 Lemma. — *Let $\mathfrak{f} \in \mathrm{Id}_{O_K}$ separate units. The universal* CM *elliptic curve with level $\mathfrak{f}$-structure $E^{(\mathfrak{f})} \to M_{CM}^{(\mathfrak{f})}$ is in the essential image of the functor*

$$W_*(\mathscr{M}_{CM})_\Lambda \to \mathscr{M}_{CM}.$$

Proof. — Write $M = M_{CM}^{(\mathfrak{f})}$, $E = E^{(\mathfrak{f})}$ and $P = \mathrm{Id}_{O_K}^{(\mathfrak{f})}$ and let $P' \subset \mathrm{Id}_{O_K}$ be the sub-monoid generated by the prime ideals dividing $\mathfrak{f}$ so that $P \cap P' = \{O_K\}$ and $\mathrm{Id}_{O_K} = P \cdot P'$.

Then the finite étale $\mathrm{Spec}(O_K[\mathfrak{f}^{-1}])$-scheme M admits a unique Λ_P-structure by (3.4.6). By the definition of the automorphisms $\sigma_\mathfrak{p} = [\mathfrak{p}^{-1}]_\mathfrak{f} : M \to M$ there exists a unique $\mathfrak{f}$-isomorphism

$$E \otimes_{O_K} \mathfrak{p}^{-1} \xrightarrow{\sim} \sigma_\mathfrak{p}^*(E)$$

whose pull-back along $M \times \mathrm{Spec}(\mathbf{F}_\mathfrak{p}) \to M$ is the isomorphism $\nu_\mathfrak{p}$ of (2.6.5). It follows that setting $\psi_{E/M}^\mathfrak{p} : E \to \sigma_\mathfrak{p}^*(E)$ to be the composition

$$E \xrightarrow{i_\mathfrak{p}} E \otimes_{O_K} \mathfrak{p}^{-1} \xrightarrow{\sim} \sigma_\mathfrak{p}^*(E)$$

defines a lift of the relative $N\mathfrak{p}$-power Frobenius on $E \to M$. Note that $\ker(\psi_{E/M}^\mathfrak{p}) = E[\mathfrak{p}]$. Let $\mathfrak{l} \in P$ be another prime ideal and consider the diagram

$$\begin{array}{ccc} E & \xrightarrow{\psi_{E/M}^\mathfrak{p}} & \sigma_\mathfrak{p}^*(E) \\ {\scriptstyle \psi_{E/M}^\mathfrak{l}}\downarrow & & \downarrow{\scriptstyle \sigma_\mathfrak{p}^*(\psi_{E/M}^\mathfrak{l})} \\ \sigma_\mathfrak{l}^*(E) & \xrightarrow{\sigma_\mathfrak{l}^*(\psi_{E/M}^\mathfrak{p})} & \sigma_{\mathfrak{p}\mathfrak{l}}^*(E). \end{array} \tag{4.1.12.1}$$

The kernel of the compositions along the top and right, and left and bottom of (4.1.12.1) are both equal to $E[\mathfrak{p}\mathfrak{l}]$ so that, as M is connected, these compositions differ by scaling by some $\epsilon \in O_K^\times$. As the $\mathfrak{f}$-torsion $E[\mathfrak{f}]$ is constant over M, and $M \xrightarrow{\sim} \mathrm{Spec}(O_{K(\mathfrak{f})}[\mathfrak{f}^{-1}])$, it admits a unique $\Lambda_{P,M}$-structure by (3.4.6).

The uniqueness of the $\Lambda_{P,M}$-structure on $E[\mathfrak{f}]$ now implies that the diagram (4.1.12.1) commutes when restricted to the $\mathfrak{f}$-torsion and therefore $\epsilon \in O_K^{\times,\mathfrak{f}}$. However, $\mathfrak{f}$ separates units, so that $\epsilon \in O_K^{\times,\mathfrak{f}} = \{1\}$ and (4.1.12.1) commutes. As E is flat over $\mathrm{Spec}(O_K)$ this defines a $\Lambda_{P,M}$-structure on E by (3.3.12).

Pulling-back $E \to M$ along the map $\Gamma_P^*(M) \to M$ corresponding to the Ψ_P-structure on M, we obtain an isomorphism of CM elliptic curves

$$E \times_M \Gamma_P^*(M) = \coprod_{\mathfrak{a}\in P} \sigma_{\mathfrak{a}}^*(E) \xrightarrow{\sim} \coprod_{\mathfrak{a}\in P} E \otimes_{O_K} \mathfrak{a}^{-1} \xrightarrow{\sim} \Gamma_{CM}^*(E) \times_{\Gamma^*(M)} \Gamma_P^*(M)$$

compatible with the $\Psi_{P,\Gamma_P^*(M)}$-structures. We then get a $\Psi_{\Gamma^*(M)}$-isomorphism

$$\Gamma_{CM}^*(E) \xrightarrow{\sim} \coprod_{\mathfrak{b}\in P'} (E \times_M \Gamma_P^*(M)) \otimes_{O_K} \mathfrak{b}^{-1}$$

inducing the identity after pull-back along $g_{(1)}$ and where on the right hand side the relative Frobenius lifts for $\mathfrak{p} \in P'$ are defined in the obvious way.

Now set $\widetilde{E}_P := E \times_M W_{P,M}^*(M)$ where we have base changed along the map $\mu_M : W_P^*(M) \to M$ defining the Λ_P-structure on M. Then $\widetilde{E}_P$ has a $\Lambda_{P,W_P^*(S)}$-structure by virtue of the facts that E/M has a $\Lambda_{P,M}$-structure and $W_P^*(M) \to M$ is a Λ_P-morphism. We also have $\Psi_{\Gamma_P^*(S)}$-isomorphisms

$$\widetilde{E}_P \times_{W_P^*(S)} \Gamma_P^*(S) \xrightarrow{\sim} E \times_M \Gamma_P^*(S) \xrightarrow{\sim} \Gamma_{CM}^*(E) \times_{\Gamma^*(M)} \Gamma_P^*(M) \qquad (4.1.12.2)$$

inducing the identity after pull-back along the first ghost component.

Finally, setting

$$\widetilde{E} := \coprod_{\mathfrak{b}\in P'} \widetilde{E}_P \otimes_{O_K} \mathfrak{b}^{-1} \to \coprod_{\mathfrak{b}\in P'} W_P^*(M) = W^*(M)$$

and defining relative Frobenius lifts on $\widetilde{E}$ for the primes $\mathfrak{p} \in P'$ in the obvious way equips $\widetilde{E}$ with a $\Lambda_{W^*(S)}$-structure. Again by construction we have a $\Psi_{\Gamma^*(M)}$-isomorphism of CM elliptic curves

$$\widetilde{E} \times_{W^*(M)} \Gamma^*(M) \xrightarrow{\sim} \Gamma_{CM}^*(E)$$

inducing the identity after pull-back along the ghost component at (1). Therefore the $\Lambda_{W^*(M)}$-structure so defined on $\widetilde{E}/W^*(M)$ is canonical and $E \to M$ is in the essential image of the functor

$$W_*(\mathscr{M}_{CM})_\Lambda \to \mathscr{M}_{CM}.$$

□

4.1.13. We now fix for all time an inverse equivalence

$$\mathscr{M}_{CM} \to W_*(\mathscr{M}_{CM})_\Lambda : E/S \mapsto W_{CM}^*(E)/W^*(S)$$

to the functor $W_*(\mathscr{M}_{CM,\Lambda}) \to \mathscr{M}_{CM}$ and call $W_{CM}^*(E)/W^*(S)$, equipped with its canonical $\Lambda_{W^*(S)}$-structure, the canonical lift of E/S.

4.1.14 Remark. — We note for future reference that the proof of (4.1.12) shows that the CM elliptic curve $\mathrm{E}^{(\mathfrak{f})}/\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})}$ admits a $\Lambda_{\mathrm{P},\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})}}$-structure and that this $\Lambda_{\mathrm{P},\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})}}$-structure has the property that there exists a $\Lambda_{\mathrm{P},\mathrm{W}_{\mathrm{P}}^{*}(\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})})}$-isomorphism

$$\mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{E}^{(\mathfrak{f})}) \times_{\mathrm{W}^{*}(\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})})} \mathrm{W}_{\mathrm{P}}^{*}(\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})}) \xrightarrow{\sim} \mathrm{E}^{(\mathfrak{f})} \times_{\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})}} \mathrm{W}_{\mathrm{P}}^{*}(\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})}) = \mu_{\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})}}^{*}(\mathrm{E})$$

inducing the identity on E after pull-back to the ghost component at (1) (this is (4.1.12.2)).

4.1.15. By virtue of the definition of $\mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{E})/\mathrm{W}^{*}(\mathrm{S})$ we have a canonical isomorphism

$$\mathrm{E} \xrightarrow{\sim} g_{(1)}^{*}(\mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{E})).$$

That is, the composition

$$\mathscr{M}_{\mathrm{CM}}(\mathrm{S}) \overset{\mathrm{W}_{\mathrm{CM}}^{*}}{\to} \mathscr{M}_{\mathrm{CM}}(\mathrm{W}^{*}(\mathrm{S})) \overset{g_{(1)}^{*}}{\to} \mathscr{M}_{\mathrm{CM}}(\mathrm{S})$$

is canonically isomorphic to the identity. We will now show that the two compositions

$$\mathscr{M}_{\mathrm{CM}}(\mathrm{S}) \xrightarrow{\mathrm{W}_{\mathrm{CM}}^{*}} \mathscr{M}_{\mathrm{CM}}(\mathrm{W}^{*}(\mathrm{S})) \underset{\mu_{\mathrm{W}^{*}(\mathrm{S})}^{*}}{\overset{\mathrm{W}_{\mathrm{CM}}^{*}}{\rightrightarrows}} \mathscr{M}_{\mathrm{CM}}(\mathrm{W}^{*}(\mathrm{W}^{*}(\mathrm{S})))$$

are also canonically isomorphic.

4.1.16 Proposition. — *Let* S *be an ind-affine scheme and let* E/S *be a* CM *elliptic curve. Then there is a unique isomorphism, compatible with the* $\Lambda_{\mathrm{W}^{*}(\mathrm{W}^{*}(\mathrm{S}))}$*-structures,*

$$\mu_{\mathrm{W}^{*}(\mathrm{S})}^{*}(\mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{E})) \xrightarrow{\sim} \mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{E}))$$

inducing the identity after pull-back along $g_{(1)} : \mathrm{W}^{*}(\mathrm{S}) \to \mathrm{W}^{*}(\mathrm{W}^{*}(\mathrm{S}))$.

Proof. — Both $\mu^{*}\mathrm{W}^{*}(\mathrm{S})(\mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{E}))$ and $\mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{E}))$ are equipped with natural $\Lambda_{\mathrm{W}^{*}(\mathrm{W}^{*}(\mathrm{S}))}$-structures and the pull-backs of each along the ghost component at (1) are equal to $\mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{E})$. Therefore, it is enough by (4.1.12) to show that the $\Lambda_{\mathrm{W}^{*}(\mathrm{W}^{*}(\mathrm{S}))}$-structures on $\mu_{\mathrm{W}^{*}(\mathrm{S})}^{*}(\mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{E}))$ are $\mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{W}_{\mathrm{CM}}^{*}(\mathrm{E}))$ are canonical.

For $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}))$ this is true by definition. For $\mu^*_{\mathrm{W}^*(\mathrm{S})}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}))$ we have the sequence of $\Psi_{\Gamma^*(\mathrm{W}^*(\mathrm{S}))}$-isomorphisms

$$\begin{aligned}
\mu^*_{\mathrm{W}^*(\mathrm{S})}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})) \times_{\mathrm{W}^*(\mathrm{W}^*(\mathrm{S}))} \Gamma^*(\mathrm{W}^*(\mathrm{S})) &= (\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{W}^*(\mathrm{S}))) \times_{\mathrm{W}^*(\mathrm{W}^*(\mathrm{S}))} \Gamma^*(\mathrm{W}^*(\mathrm{S})) \\
&= \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{W}^*(\mathrm{S})) \\
&\xrightarrow{\sim} \coprod_{\mathfrak{a}} \psi^{\mathfrak{a}*}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})) \\
&\xrightarrow{\sim} \coprod_{\mathfrak{a}} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \\
&\xrightarrow{\sim} \Gamma^*_{\mathrm{CM}}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})) \\
&= \Gamma^*_{\mathrm{CM}}(g^*_{(1)}(\mu^*_{\mathrm{W}^*(\mathrm{S})}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})))).
\end{aligned}$$

The resulting $\Psi_{\Gamma^*(\mathrm{W}^*(\mathrm{S}))}$-isomorphism

$$\mu^*_{\mathrm{W}^*(\mathrm{S})}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})) \times_{\mathrm{W}^*(\mathrm{W}^*(\mathrm{S}))} \Gamma^*(\mathrm{W}^*(\mathrm{S})) \xrightarrow{\sim} \Gamma^*_{\mathrm{CM}}(g^*_{(1)}(\mu^*_{\mathrm{S}}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}))))$$

induces the identity after pull-back along the ghost component at (1) and this is precisely the definition of a canonical $\Lambda_{\mathrm{W}^*(\mathrm{W}^*(\mathrm{S}))}$-structure. □

4.1.17. We now define what it means for a CM elliptic curve over an arbitrary Λ-ind-affine scheme (not just those of the form $\mathrm{W}^*(\mathrm{S})$) to have a canonical Λ-structure.

It will be convenient later to allow ourselves the flexibility of working with Λ-structures relative to a sub-monoid $\mathrm{P} \subset \mathrm{Id}_{\mathrm{O_K}}$ generated by some set of prime ideals and so we fix such a P.

Let S be an Λ_{P}-ind-affine scheme and let E/S be a CM elliptic curve equipped with a $\Lambda_{\mathrm{P,S}}$-structure (again compatible with its $\underline{\mathrm{O_K}}_{\mathrm{S}}$-module structure). We say that the Λ_{P}-structure on E/S is canonical if there is a $\Lambda_{\mathrm{P},\mathrm{W}^*_{\mathrm{P}}(\mathrm{S})}$-isomorphism

$$\lambda_{\mathrm{E/S}} : \mathrm{E} \times_{\mathrm{S}} \mathrm{W}^*_{\mathrm{P}}(\mathrm{S}) \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*_{\mathrm{P}}(\mathrm{S})$$

inducing the identity on the ghost components at (1). There is at most one such isomorphism $\lambda_{\mathrm{E/S}}$ satisfying this condition and so we are safe to label it. Indeed, any two differ by a $\Lambda_{\mathrm{P},\mathrm{W}^*_{\mathrm{P}}(\mathrm{S})}$-automorphism of $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \times_{\mathrm{W}^*(\mathrm{E})} \mathrm{W}^*_{\mathrm{P}}(\mathrm{E})$ inducing the identity on the ghost component at (1) and all such automorphisms are the identity as this can be checked after pull-back along $\Gamma^*_{\mathrm{P}}(\mathrm{S}) \to \mathrm{W}^*_{\mathrm{P}}(\mathrm{S})$, and arguing as in the proof of (4.1.5) one sees that a $\Psi_{\mathrm{P},\Gamma^*_{\mathrm{P}}(\mathrm{S})}$-automorphism of $\Gamma^*_{\mathrm{CM}}(\mathrm{E}) \times_{\Gamma^*(\mathrm{S})} \Gamma^*_{\mathrm{P}}(\mathrm{S})$ is equal to the identity if and only if i t is after pull-back to the ghost component at (1).

4.1.18 Remark. — When $\mathrm{P} = \mathrm{Id}_{\mathrm{O_K}}$ and $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ is a CM elliptic curve equipped with a $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure then it follows from (4.1.16) that this $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure is canonical in the sense of (4.1.17) if and only if there exists a $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-isomorphism

$$f : \mathrm{E} \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(g^*_{(1)}(\mathrm{E}))$$

inducing the identity after pull-back to the ghost component at (1), i.e. $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ is canonical in the sense of (4.1.6).

Indeed, if there exists such an isomorphism $f : \mathrm{E} \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(g^*_{(1)}(\mathrm{E}))$ then (4.1.16) gives an isomorphism $\lambda_{\mathrm{E}/\mathrm{W}^*(\mathrm{S})}$ via the compositions

$$\begin{aligned} \mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{W}^*(\mathrm{S})) &\xrightarrow{f\times_{\mathrm{W}^*(\mathrm{S})}\mathrm{W}^*(\mathrm{W}^*(\mathrm{S}))} \mathrm{W}^*_{\mathrm{CM}}(g^*_{(1)}(\mathrm{E})) \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{W}^*(\mathrm{S})) \\ &\xrightarrow{(4.1.16)} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{W}^*_{\mathrm{CM}}(g^*_{(1)}(\mathrm{E}))) \\ &\xrightarrow{\mathrm{W}^*_{\mathrm{CM}}(f^{-1})} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}). \end{aligned}$$

Conversely, the pull-back of an isomorphism

$$\lambda_{\mathrm{E}/\mathrm{W}^*(\mathrm{S})} : \mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{W}^*(\mathrm{S})) \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})$$

along $\widetilde{g} = \mathrm{W}^*(g_{(1)}) : \mathrm{W}^*(\mathrm{S}) \to \mathrm{W}^*(\mathrm{W}^*(\mathrm{S}))$ yields a $\Lambda_{\mathrm{W}^*(\mathrm{W}^*(\mathrm{S}))}$-isomorphism $f : \mathrm{E} \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(g^*_{(1)}(\mathrm{E}))$ via

$$\mathrm{E} \xrightarrow{\sim} \widetilde{g}^*(\mathrm{E} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{W}^*(\mathrm{S}))) \xrightarrow{\widetilde{g}^*(\lambda_{\mathrm{E}/\mathrm{W}^*(\mathrm{S})})} \widetilde{g}^*(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})) \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(g^*_{(1)}(\mathrm{E})).$$

Hence the two notions of canonical $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure on a CM elliptic curve $\mathrm{E}/\mathrm{W}^*(\mathrm{S})$ defined in (4.1.6) and (4.1.17) coincide.

4.1.19 Proposition. — *Let* S *be an* Λ_{P}*-ind-affine-scheme and* E/S *a* CM *elliptic curve. Then:*

(i) E/S *admits at most one canonical* $\Lambda_{\mathrm{P},\mathrm{S}}$*-structure.*

(ii) *If* $\mathrm{S}' \to \mathrm{S}$ *is a morphism of* Λ_{P}*-ind-affine schemes, the* $\Lambda_{\mathrm{P},\mathrm{S}'}$*-structure on* $\mathrm{E} \times_{\mathrm{S}} \mathrm{S}'$ *is canonical and*

$$\lambda_{\mathrm{E}/\mathrm{S}} \times_{\mathrm{W}^*_{\mathrm{P}}(\mathrm{S})} \mathrm{W}^*_{\mathrm{P}}(\mathrm{S}') = \lambda_{\mathrm{E}\times_{\mathrm{S}}\mathrm{S}'/\mathrm{S}'}.$$

(iii) *Let* $(\mathrm{S}_i \to \mathrm{S})_{i\in\mathrm{I}}$ *be a* ét*-cover of* Λ_{P}*-ind-affine schemes. If* $\mathrm{E} \times_{\mathrm{S}} \mathrm{S}'$ *admits a canonical* $\Lambda_{\mathrm{P},\mathrm{S}_i}$*-structure for each* $i \in \mathrm{I}$ *then* E/S *admits a canonical* $\Lambda_{\mathrm{P},\mathrm{S}}$*-structure.*

Proof. — (i) Let E/S admit two canonical $\Lambda_{\mathrm{P},\mathrm{S}}$-structures with corresponding isomorphisms

$$\lambda_{\mathrm{E}/\mathrm{S}}, \lambda'_{\mathrm{E}/\mathrm{S}} : \mathrm{E} \times_{\mathrm{S}} \mathrm{W}^*_{\mathrm{P}}(\mathrm{S}) \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*_{\mathrm{P}}(\mathrm{S}).$$

The difference

$$\lambda'_{\mathrm{E}/\mathrm{S}} \circ \lambda^{-1}_{\mathrm{E}/\mathrm{S}} : \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*_{\mathrm{P}}(\mathrm{S}) \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*_{\mathrm{P}}(\mathrm{S})$$

defines $\Lambda_{\mathrm{P},\mathrm{W}^*_{\mathrm{P}}(\mathrm{S})}$-automorphism of $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*_{\mathrm{P}}(\mathrm{S})$ which is the identity on the first ghost component. Base changing along $\Gamma^*_{\mathrm{P}}(\mathrm{S}) \to \mathrm{W}^*_{\mathrm{P}}(\mathrm{S})$ and arguing again as in the proof of (4.1.5) we find that such an automorphism must be the identity itself and so $\lambda_{\mathrm{E}/\mathrm{S}} = \lambda'_{\mathrm{E}/\mathrm{S}}$.

It follows now that the two $\Lambda_{P,W_P^*(S)}$-structures on $E \times_S W_P^*(S)$ coincide so that as $W_P^*(S) \to S$ is an epimorphism and Λ_P-structures descend (3.4.5) the two $\Lambda_{P,S}$-structures on E/S coincide.

(ii) This follows from the uniqueness of the isomorphisms $\lambda_{E/S}$.

(iii) As canonical Λ_P-structures are unique and compatible with pull-back (this is (ii) above) if $E \times_S S_i$ admits a canonical Λ_{P,S_i}-structure for each $i \in I$ it follows that E admits a $\Lambda_{P,S}$-structure. As the isomorphisms making a Λ_P-structure canonical are unique and compatible with pull back (again this is (ii)) the isomorphisms $\lambda_{E\times_S S_i/S_i}$ descend to an isomorphism

$$\lambda_{E/S} : E \times_S W_P^*(S) \xrightarrow{\sim} W_{CM}^*(E) \times_{W^*(S)} W_P^*(S)$$

inducing the identity after base change long the ghost component at (1) and so the $\Lambda_{P,S}$-structure on E/S canonical. □

4.1.20 Proposition. — *Let* $\mathfrak{f} \in \mathrm{Id}_{O_K}$ *be an ideal which separates units. Then the unique* $\Lambda_{P,M_{CM}^{(\mathfrak{f})}}$*-structure on the universal* CM *elliptic curve with level-*$\mathfrak{f}$ *structure* $E^{(\mathfrak{f})} \to M_{CM}^{(\mathfrak{f})}$ *is canonical.*

Proof. — This is the content of (4.1.14). □

4.2. CM elliptic curves of Shimura type

The purpose of this section is to explain the relationship between Λ-structures and CM elliptic curves of Shimura type. A CM elliptic curve of Shimura type is a CM elliptic curve E/Spec(L) where L is an abelian extension of K with the property that the extension L(E[tors])/K is an abelian extension of K (it is always an abelian extension of L).

This class of CM elliptic curves was introduced by Shimura (see Theorem 7.44 of [**33**]). By virtue of their definition, CM elliptic curves of Shimura type have much simpler arithmetic than arbitrary CM elliptic curves (and of course elliptic curves in general). In the special case where K has class number one, every CM elliptic curve E/Spec(K) is of Shimura type, and the first (partial) verifications of the Birch-Swinnerton-Dyer conjecture made by Coates and Wiles ([**13**]) concerned these curves. Along these lines let us also mention the paper of Rubin ([**30**]) which considers the Birch-Swinnerton-Dyer conjecture for general CM elliptic curves of Shimura type.

Let us now give a brief outline of what follows. We first recall a result of Shimura (4.2.2) stating the existence of infinitely many CM elliptic curves of Shimura type over the Hilbert class field H of K. We then show that such CM elliptic curves cannot have good reduction everywhere (4.2.4) and answer the question raised in (2.4.5) regarding the triviality of the $\mathscr{CL}_{O_K}$-torsor $\mathscr{M}_{CM}$.

We then prove the main result (4.2.8) which is that a CM elliptic curve E/Spec(L) is of Shimura type if and only if it admits a canonical Λ-structure. There are some minor technicalities in that one must avoid the ramified primes

in L/K and the primes of bad reduction for E but we get around this naturally enough.

The second part of this section concerns itself with the tangent spaces of Néron models of CM elliptic curves of Shimura type. The Λ-structure on E/Spec(L) induces a rather rigid structure on Lie algebra of its Néron model. We then show (4.2.13) that if E/Spec(K(ƒ)) is a CM elliptic curve of Shimura type over the ray class field of conductor ƒ, and the ƒ-torsion of E is constant, then the Lie algebra of its Néron model is free away from ƒ, or in other words that E/Spec(K(ƒ)) admits global minimal model away from ƒ. In particular, if one takes $\mathfrak{f} = \mathrm{O_K}$ so that $\mathrm{K}(\mathfrak{f}) = \mathrm{H}$, this shows that every CM elliptic curve of Shimura type E/Spec(H) admits a global minimal model *everywhere*. This extends a result of Gross ([**22**]) and will be used crucially in (4.4) in our construction of a flat affine Λ-presentation of the stack $\mathscr{M}_{\mathrm{CM}}$.

4.2.1. Let L be an abelian extension of K and E/Spec(L) a CM elliptic curve. One says that E/Spec(L) is of Shimura type if the extension L(E[tors])/K is abelian.

***4.2.2 Proposition* (Shimura).** — *There exist infinitely many prime ideals* $\mathfrak{p}$ *of* K *for which there is a* CM *elliptic curve* E/Spec(H) *of Shimura type with good reduction away from* $\mathfrak{p}$.

Proof. — By Proposition 7, §5 of [**32**] there exists infinitely many primes $\mathfrak{p}$ of K with $\mathrm{N}\mathfrak{p} = p$ a rational prime, $\mathrm{N}\mathfrak{p} = 1 \bmod w$ and $(\mathrm{N}\mathfrak{p} - 1)/w$ prime to w, where $w = \#\mathrm{O_K^\times}$. Given such a prime $\mathfrak{p}$ it follows that the reduction map

$$\mathrm{O_K^\times} \to (\mathrm{O_K}/\mathfrak{p})^\times$$

is the inclusion of a direct factor. Therefore, we may define a map $\alpha : \mathrm{A_{O_K}^\times} \to \mathrm{O_K^\times}$ satisfying $\alpha|_{\mathrm{O_K^\times}} = \mathrm{id}_{\mathrm{O_K^\times}}$ by

$$\mathrm{A_{O_K}^\times} \to (\mathrm{O_K}/\mathfrak{p})^\times \to \mathrm{O_K^\times}$$

where the first map is the quotient map and the second is a retraction of $\mathrm{O_K^\times} \to (\mathrm{O_K}/\mathfrak{p})^\times$. Finally, setting

$$g : \mathrm{A_{O_K}^\times}/\mathrm{O_K^\times} \to \mathrm{A_{O_K}^\times} : s \bmod \mathrm{O_K^\times} \mapsto s\alpha(s)^{-1}$$

we define $\rho^{-1} : \mathrm{G}(\mathrm{H^{sep}}/\mathrm{H}) \to \mathrm{A_{O_K}^\times}$ by

$$\mathrm{G}(\mathrm{H^{sep}}/\mathrm{H}) \xrightarrow{-|_{\mathrm{K}^\infty}} \mathrm{G}(\mathrm{K^{ab}}/\mathrm{H}) \xrightarrow{\theta_{\mathrm{K}}^{-1}|_{\mathrm{G}(\mathrm{K}^\infty/\mathrm{H})}} \mathrm{A_{O_K}^\times}/\mathrm{O_K^\times} \xrightarrow{g} \mathrm{A_{O_K}^\times}.$$

We will now show that ρ satisfies the conditions of (2.5.8) to construct a CM elliptic curve E/Spec(H) with $\rho_{\mathrm{E/H}} = \rho$. For each $\sigma \in \mathrm{G}(\mathrm{H^{sep}}/\mathrm{H})$ there is an $s \in \mathrm{A_{O_K}^\times}/\mathrm{O_K^\times}$ such that $\sigma|_{\mathrm{K}^\infty} = \theta_{\mathrm{K}}(s) \in \mathrm{G}(\mathrm{K}^\infty/\mathrm{H})$. Unwinding the definition of ρ^{-1} we find

$$[\rho(\sigma)^{-1}] = [g(s \bmod \mathrm{O_K^\times})] = [s\alpha(s)^{-1}] = [s]$$

so that by (iii) of (2.5.9) we have

$$[\sigma]_{\mathrm{H}} = [\sigma|_{\mathrm{K}^{\mathrm{sep}}}]_{\mathrm{K}} = [s] = [\rho(\sigma)^{-1}].$$

Therefore, the diagram

$$\begin{array}{ccc} \mathrm{G}(\mathrm{H}^{\mathrm{sep}}/\mathrm{H}) & \xrightarrow{\rho^{-1}} & \mathrm{A}_{\mathrm{O_K}}^{\times} \\ & \searrow^{[-]_{\mathrm{H}}} & \downarrow{\scriptstyle [-]} \\ & & \mathrm{CL}_{\mathrm{O_K},\infty} \end{array}$$

commutes and by (2.5.8) there exists a CM elliptic curve E/Spec(H) with $\rho_{\mathrm{E/H}} = \rho$. As $\rho_{\mathrm{E/H}} : \mathrm{G}(\mathrm{H}^{\mathrm{sep}}/\mathrm{H}) \to \mathrm{A}_{\mathrm{O_K}}^{\times}$ factors through $\mathrm{G}(\mathrm{K}^{\mathrm{ab}}/\mathrm{H}) \to \mathrm{A}_{\mathrm{O_K}}^{\times}$, it follows that H(E[tors])/K is abelian over K and E/Spec(H) is of Shimura type. Moreover, E/Spec(H) has good reduction away from $\mathfrak{p}$ by (2.5.12) as by construction the composition

$$\mathrm{O}_{\mathrm{K}_{\mathfrak{l}}}^{\times} \to \mathrm{A}_{\mathrm{O_K}}^{\times}/\mathrm{O}_{\mathrm{K}}^{\times} \xrightarrow{\sim} \mathrm{G}(\mathrm{K}^{\mathrm{ab}}/\mathrm{H}) \to \mathrm{A}_{\mathrm{O_K}}^{\times}$$

is equal to the natural inclusion $\mathrm{O}_{\mathrm{K}_{\mathfrak{l}}}^{\times} \to \mathrm{A}_{\mathrm{O_K}}^{\times}$ for all primes $\mathfrak{l} \neq \mathfrak{p}$. □

4.2.3 Remark. — It follows from (4.2.2) above that the map $c_{\mathscr{E}/\mathscr{M}} : \mathscr{M}_{\mathrm{CM}} \to \mathrm{M}_{\mathrm{CM}}$ from $\mathscr{M}_{\mathrm{CM}}$ to its coarse sheaf admits sections Zariski locally over $\mathrm{Spec}(\mathrm{O_K})$. Indeed, by (4.2.2) there are infinitely many primes $\mathfrak{p}$ of $\mathrm{O_K}$ and CM elliptic curves $\mathrm{E}/\mathrm{M}_{\mathrm{CM}}[\mathfrak{p}^{-1}]$. Each map $c_{\mathrm{E}/\mathrm{M}_{\mathrm{CM}}[\mathfrak{p}^{-1}]} : \mathrm{M}_{\mathrm{CM}}[\mathfrak{p}^{-1}] \to \mathrm{M}_{\mathrm{CM}}$ is then equal to the inclusion $\mathrm{M}[\mathfrak{p}^{-1}] \to \mathrm{M}$ followed by some automorphism $\sigma_{\mathfrak{a}}$ of M_{CM}. By (2.6.8), replacing E with $\mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}$, we may assume that $c_{\mathrm{E}/\mathrm{M}_{\mathrm{CM}}[\mathfrak{p}^{-1}]} : \mathrm{M}_{\mathrm{CM}}[\mathfrak{p}^{-1}] \to \mathrm{M}_{\mathrm{CM}}$ is the inclusion.

We note for future reference that if $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are two such primes with $\mathrm{E}_1/\mathrm{M}_{\mathrm{CM}}[\mathfrak{p}_1^{-1}]$ and $\mathrm{E}_2/\mathrm{M}_{\mathrm{CM}}[\mathfrak{p}_2^{-1}]$ as above, then the fact that $c_{\mathrm{E}_1/\mathrm{M}_{\mathrm{CM}}[\mathfrak{p}_1^{-1}]}$ and $c_{\mathrm{E}_2/\mathrm{M}_{\mathrm{CM}}[\mathfrak{p}_2^{-1}]}$ are equal to the natural inclusions implies that E_1 and E_2 are locally isomorphic on the over lap $\mathrm{M}_{\mathrm{CM}}[\mathfrak{p}_1^{-1}] \cap \mathrm{M}_{\mathrm{CM}}[\mathfrak{p}_2^{-1}] = \mathrm{M}_{\mathrm{CM}}[(\mathfrak{p}_1\mathfrak{p}_2)^{-1}] \subset \mathrm{M}_{\mathrm{CM}}$.

4.2.4 Proposition. — *There does not exist a* CM *elliptic curve* E/H *of Shimura type with good reduction everywhere.*

Proof. — Let E/H be a CM elliptic curve and consider the character (2.5.3)

$$\rho_{\mathrm{E/H}} : \mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{H}) \to \mathrm{A}_{\mathrm{O_K}}^{\times}.$$

If H(E[tors])/K is abelian then $\rho_{\mathrm{E/H}}$ factors as

$$\rho_{\mathrm{E/H}} : \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{H}) = \mathrm{G}(\mathrm{K}^{\mathrm{ab}}/\mathrm{H}) \to \mathrm{A}_{\mathrm{O_K}}^{\times}$$

(note that $\mathrm{K}^{\mathrm{ab}} = \mathrm{K}^{\infty}$). Composing the reciprocal $\rho_{\mathrm{E/H}}^{-1}$ with the isomorphism $\theta_{\mathrm{K}} : \mathrm{A}_{\mathrm{O_K}}^{\times}/\mathrm{O}_{\mathrm{K}}^{\times} \xrightarrow{\sim} \mathrm{G}(\mathrm{K}^{\infty}/\mathrm{H}) = \mathrm{G}(\mathrm{K}^{\mathrm{ab}}/\mathrm{H})$ of (1.4.8.1) we obtain a homomorphism

$$f : \mathrm{A}_{\mathrm{O_K}}/\mathrm{O}_{\mathrm{K}}^{\times} \to \mathrm{A}_{\mathrm{O_K}}^{\times}.$$

The fundamental relation $[\rho_{E/H}^{-1}] = [-]_H$, the fact that $[-]_H = [-]_K|_{G(K^{sep}/H)}$, the fact that $\theta_K \circ [-]_K = |_{K^\infty}$ and the fact that the inertia group $I_\mathfrak{p}(K^\infty/H) \subset G(K^\infty/K)$ corresponds to $O_{K_\mathfrak{p}}^\times \subset A_{O_K}^\times/O_K^\times \subset (A_{O_K} \otimes_{O_K} K)^\times/O_K^\times$ under θ_K combined with (2.5.12) shows that for E/H to have good reduction at all places of H lying above a prime $\mathfrak{p}$ of O_K is equivalent to the composition

$$O_{K_\mathfrak{p}}^\times \subset A_{O_K}^\times/O_K^\times \xrightarrow{f} A_{O_K}^\times$$

being equal to the inclusion $O_{K_\mathfrak{p}}^\times \subset A_{O_K}^\times$. If this is true for all prime ideals $\mathfrak{p}$, the composition of f with the quotient map

$$A_{O_K}^\times \to A_{O_K}^\times/O_K^\times \xrightarrow{f} A_{O_K}^\times \tag{4.2.4.1}$$

is equal to the identity on the sub-group of $A_{O_K}^\times$ generated by the sub-groups $O_{K_\mathfrak{p}}^\times$ for all primes $\mathfrak{p}$ of O_K. But this sub-group is dense and so it follows that the composition (4.2.4.1) is equal to the identity and this is clearly impossible. □

4.2.5 Remark. — We can now answer the question raised in (2.4.5) asking for a trivialisation of the $\mathscr{CL}_{O_K}$-torsor $\mathscr{M}_{O_K}$. In light of the fact that the coarse sheaf M_{CM} of $\mathscr{M}_{CM}$ is isomorphic to $\mathrm{Spec}(O_H)$ it more natural to ask the following: does there exists a CM elliptic curve $\mathscr{E}/\mathrm{Spec}(O_H)$ inducing a trivialisation of the $\mathscr{CL}_{O_K}$-torsor $\mathscr{M}_{CM}$, i.e. an equivalence of stacks

$$\mathscr{CL}_{O_H} \times \mathrm{Spec}(O_H) \xrightarrow{\sim} \mathscr{M}_{CM} \times \mathrm{Spec}(O_H) : \mathscr{L}/S \mapsto E_S \otimes_{O_K} \mathscr{L} \ ?$$

While we have shown (4.2.4) that there do not exist CM elliptic curves E/H of Shimura type with good reduction everywhere, it is possible for there to exist CM elliptic curves $\mathscr{E}/\mathrm{Spec}(O_H)$ (of course they will not be of Shimura type). Indeed, Rohrlich [**29**] has shown that if the discriminant of K over **Q** is divisible by at least two primes congruent to 3 mod 4 then there does exist a CM elliptic curve $\mathscr{E}/\mathrm{Spec}(O_H)$. The answer in general to the question above is however negative. Indeed, if K has class number, so that K = H, then every CM elliptic curve E/Spec(K) is of Shimura type and so cannot have good reduction everywhere, i.e. there does not exist a CM elliptic curve $\mathscr{E}/\mathrm{Spec}(O_K)$.

4.2.6. We continue with the notation of (4.2.1) so that L/K is an abelian extension and E/Spec(L) is a CM elliptic curve. We also fix an integral ideal $\mathfrak{g} \in \mathrm{Id}_{O_K}$ such that $\mathrm{Spec}(O_L[\mathfrak{g}^{-1}])$ is unramified over $\mathrm{Spec}(O_K)$ and such that E has good reduction over $\mathrm{Spec}(O_L[\mathfrak{g}^{-1}])$. We then set $S = \mathrm{Spec}(O_L[\mathfrak{g}^{-1}])$ and $P = \mathrm{Id}_{O_K}^{(\mathfrak{g})}$ so that S admits a unique Λ_P-structure (3.4.6) whose Frobenius lifts we denote by $\sigma_\mathfrak{a} = \sigma_{\mathfrak{a},S} : S \to S$ for $\mathfrak{a} \in P$. We write $\mathscr{E} \to S$ for the Néron model of E relative to $\mathrm{Spec}(L) \to S$ so that $\mathscr{E} \to S$ is a CM elliptic curve. For $\mathfrak{p} \in P$ a prime ideal let us write $S_\mathfrak{p} = S \times_{\mathrm{Spec}(O_K)} \mathrm{Spec}(\mathbf{F}_\mathfrak{p})$ and $\mathscr{E}_\mathfrak{p} = S \times_S S_\mathfrak{p}$.

4.2.7 Lemma. — *For each* $\mathfrak{p} \in \mathrm{P}$*, there is at most one homomorphism*

$$\psi^{\mathfrak{p}}_{\mathscr{E}/\mathrm{S}} : \mathscr{E} \to \sigma_{\mathfrak{p}}^{*}(\mathscr{E})$$

lifting the $\mathrm{N}\mathfrak{p}$*-power relative Frobenius map of* $\mathscr{E}_{\mathfrak{p}}$*.*

Proof. — By rigidity the difference of two such homomorphisms is equal to the zero map on some open and closed sub-scheme of S, the only choices of which are S and $\emptyset$. Therefore, as any two such isomorphisms must agree on $\mathrm{S}_{\mathfrak{p}} \subset \mathrm{S}$ which is non-empty, they agree everywhere. □

4.2.8 Theorem. — *In the notation of* (4.2.6)*, the following are equivalent:*

(i) *The* CM *elliptic curve* $\mathscr{E} \to \mathrm{S}$ *admits a canonical* $\Lambda_{\mathrm{P,S}}$*-structure.*
(ii) *The* CM *elliptic curve* $\mathscr{E} \to \mathrm{S}$ *admits a* $\Lambda_{\mathrm{P,S}}$*-structure.*
(iii) *The extension* $\mathrm{L}(\mathrm{E}[\mathrm{tors}])/\mathrm{K}$ *is abelian, i.e.* $\mathrm{E}/\mathrm{Spec}(\mathrm{L})$ *is a* CM *elliptic curve of Shimura type.*
(iv) *The homomorphism* $\rho_{\mathrm{E/L}} : \mathrm{G}(\mathrm{L}^{\mathrm{sep}}/\mathrm{L}) \to \mathrm{A}_{\mathrm{O_K}}^{\times}$ *factors through* $\mathrm{G}(\mathrm{L}^{\mathrm{sep}}/\mathrm{L}) \to \mathrm{G}(\mathrm{K}^{\mathrm{ab}}/\mathrm{L})$*.*

Proof. — (i) implies (ii): This is clear.

(ii) implies (iii): For each ideal $\mathfrak{a}$ the sub-schemes $\mathscr{E}[\mathfrak{a}] = \ker(\psi^{\mathfrak{a}}_{\mathscr{E}/\mathrm{S}}) \subset \mathscr{E}$ are finite and locally free $\Lambda_{\mathrm{P,S}}$-schemes. After inverting $\mathfrak{a}$ and forgetting about the Frobenius lifts for primes dividing $\mathfrak{a}$, we may apply (3.4.6) to see that $\mathrm{K}(\mathrm{E}[\mathfrak{a}]) = \mathrm{L}(\mathrm{E}[\mathfrak{a}])$ is abelian over K.

(iii) is equivalent to (iv): This is immediate from the definition of $\rho_{\mathrm{E/L}}$ (2.5.3).

(iv) implies (i): If $\mathfrak{g} = \mathrm{O_K}$ then L/K is unramified and so $\mathrm{L} \subset \mathrm{H}$. However, $\mathrm{M_{CM}} \xrightarrow{\sim} \mathrm{Spec}(\mathrm{O_H})$ and so we must have $\mathrm{L} = \mathrm{H}$. However, if $\mathrm{L} = \mathrm{H}$ and $\mathfrak{g} = \mathrm{O_K}$ then $\mathrm{E}/\mathrm{Spec}(\mathrm{H})$ admits good reduction everywhere which, as $\mathrm{E}/\mathrm{Spec}(\mathrm{H})$ is of Shimura type by hypothesis, is impossible (4.2.4). Therefore, $\mathfrak{g} \neq \mathrm{O_K}$ and it follows that replacing $\mathfrak{g}$ with $\mathfrak{g}^n$ for some $n \geq 0$ we may assume that $\mathfrak{g}$ separates units (this changes neither $\mathrm{Spec}(\mathrm{O_L}[\mathfrak{g}^{-1}])$ nor $\mathrm{P} = \mathrm{Id}^{(\mathfrak{g})}_{\mathrm{O_K}}$).

Write $\mathrm{L}' = \mathrm{L}(\mathrm{E}[\mathfrak{g}])$ and $\mathrm{S}' = \mathrm{Spec}(\mathrm{O_{L'}}[\mathfrak{g}^{-1}])$. The extension L'/K is abelian (by hypothesis $\mathrm{L}(\mathrm{E}[\mathrm{tors}])$ is abelian) and unramified away from $\mathfrak{g}$ (as $\mathscr{E}[\mathfrak{g}]$ is étale over S) so that S' admits a unique Λ_{P}-structure. By construction, the CM elliptic curve $\mathscr{E} \times_{\mathrm{S}} \mathrm{S}'$ admits a level-$\mathfrak{g}$ structure and, choosing one, we obtain a map $\mathrm{S} \to \mathrm{M}^{(\mathfrak{g})}_{\mathrm{CM}}$ and an isomorphism $\mathscr{E} \times_{\mathrm{S}} \mathrm{S}' \xrightarrow{\sim} \mathrm{E}^{(\mathfrak{g})} \times_{\mathrm{M}^{(\mathfrak{g})}_{\mathrm{CM}}} \mathrm{S}'$. As the morphism $\mathrm{S}' \to \mathrm{M}^{(\mathfrak{g})}_{\mathrm{CM}}$ is a Λ_{P}-morphism and $\mathrm{E}^{(\mathfrak{g})} \to \mathrm{M}^{(\mathfrak{g})}_{\mathrm{CM}}$ admits a canonical $\Lambda_{\mathrm{P},\mathrm{M}^{(\mathfrak{g})}_{\mathrm{CM}}}$-structure it follows that

$$\mathscr{E} \times_{\mathrm{S}} \mathrm{S}' \xrightarrow{\sim} \mathrm{E}^{(\mathfrak{g})} \times_{\mathrm{M}^{(\mathfrak{g})}_{\mathrm{CM}}} \mathrm{S}'$$

admits a canonical $\Lambda_{\mathrm{P,S}'}$-structure and by (iii) of (4.1.19) that $\mathscr{E} \to \mathrm{S}$ admits a canonical $\Lambda_{\mathrm{P,S}}$-structure. □

4.2.9 Remark. — Now let $\mathscr{E}, \mathscr{E}'$ be a pair of CM elliptic curves of Shimura type over S (we keep $\mathfrak{g}$ the same). If $\mathscr{E}$ and $\mathscr{E}'$ are locally isomorphic (note that there is always some ideal $\mathfrak{a}$ such that $\mathscr{E} \otimes_{\mathrm{O_K}} \mathfrak{a}$ and $\mathscr{E}'$ are locally isomorphic) then they are actually $\Lambda_{\mathrm{P,S}}$-locally isomorphic. Indeed, generically, they become isomorphic over the extension L'/L corresponding to the character

$$\rho := \rho_{\mathrm{E/L}} \rho_{\mathrm{E}'/\mathrm{L}}^{-1} : \mathrm{G}(\mathrm{K}^{\mathrm{ab}}/\mathrm{L}) \to \mathrm{O_K^\times}.$$

It is clear that the extension L'/K is abelian and it also is unramified away from $\mathfrak{g}$ (the characters $\rho_{\mathrm{E/L}}$ and $\rho_{\mathrm{E}'/\mathrm{L}}$ agree on the inertia sub-groups for all $\mathfrak{p} \nmid \mathfrak{g}$ — this is the good reduction of $\mathscr{E}$ and $\mathscr{E}'$ away from $\mathfrak{g}$). Therefore, $\mathrm{S}' = \mathrm{Spec}(\mathrm{O_L}[\mathfrak{g}^{-1}])$ is finite and étale over S and admits a unique Λ_{P}-structure. Moreover, there exists an isomorphism

$$f : \mathscr{E} \times_{\mathrm{S}} \mathrm{S} \xrightarrow{\sim} \mathscr{E}' \times_{\mathrm{S}} \mathrm{S}'$$

and it remains to observe that all such isomorphisms are $\Lambda_{\mathrm{P,S}'}$-isomorphisms. Indeed, f is a $\Lambda_{\mathrm{P,S}'}$-isomorphism if and only if the $\Lambda_{\mathrm{P,S}'}$-structure on $\mathscr{E}$ induced by transport of structure along f is equal to the given $\Lambda_{\mathrm{P,S}'}$-structure on $\mathscr{E}'$ and this follows from (4.2.7).

4.2.10. We now wish to study the Lie algebras of the Néron models of CM elliptic curves of Shimura type. So we continue with the notation of (4.2.6) but will also assume that the CM elliptic curve $\mathscr{E} \to \mathrm{S}$ admits a canonical $\Lambda_{\mathrm{P,S}}$-structure, i.e. that $\mathrm{E}/\mathrm{Spec}(\mathrm{L})$ is a CM elliptic curve of Shimura type. The field L must contain the Hilbert class field $\mathrm{H} \subset \mathrm{L}$. The following well known property enjoyed by the Hilbert class field H will be crucial:

***4.2.11 Proposition* (Hauptidealsatz).** — *Every rank one* $\mathrm{O_K}$*-module becomes free after base change to* $\mathrm{O_H}$.

4.2.12. We shall abuse notation and write, for each prime ideal $\mathfrak{p} \in \mathrm{P}$,

$$\nu_{\mathfrak{p}} : \mathscr{E} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1} \xrightarrow{\sim} \sigma_{\mathfrak{p}}^*(\mathscr{E})$$

for the unique isomorphism lifting the isomorphism $\nu_{\mathfrak{p}}(\mathscr{E}_{\mathfrak{p}}/\mathrm{S}_{\mathfrak{p}})$ of (2.2.13) or equivalently the unique isomorphism such that the composition

$$\mathscr{E} \xrightarrow{i_{\mathfrak{p}}} \mathscr{E} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1} \xrightarrow{\nu_{\mathfrak{p}}} \sigma_{\mathfrak{p}}^*(\mathscr{E})$$

is equal to the relative Frobenius lift $\psi^{\mathfrak{p}}_{\mathscr{E}/\mathrm{S}}$.

For a pair of primes $\mathfrak{p}$, $\mathfrak{l}$ the commutativity of the (relative) Frobenius lifts on $\mathscr{E} \to \mathrm{S}$ amounts to the equalities

$$\sigma_{\mathfrak{l}}^*(\nu_{\mathfrak{p}}) \circ (\nu_{\mathfrak{l}} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1}) = \sigma_{\mathfrak{p}}^*(\nu_{\mathfrak{l}}) \circ (\nu_{\mathfrak{p}} \otimes_{\mathrm{O_K}} \mathfrak{l}^{-1}) \tag{4.2.12.1}$$

so that for any ideal $\mathfrak{a} \in \mathrm{P}$, choosing a prime factorisation of $\mathfrak{a}$, we may define isomorphisms

$$\nu_{\mathfrak{a}} : \mathscr{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \xrightarrow{\sim} \sigma_{\mathfrak{a}}^*(\mathscr{E})$$

by composing the various $\nu_{\mathfrak{p}}$ for $\mathfrak{p}|\mathfrak{a}$, with the resulting isomorphism being independent of any choices involved by virtue of (4.2.12.1). These isomorphisms now satisfy

$$\sigma_{\mathfrak{a}}^*(\nu_{\mathfrak{b}}) \circ (\nu_{\mathfrak{a}} \otimes_{\mathrm{O_K}} \mathfrak{b}^{-1}) = \sigma_{\mathfrak{b}}^*(\nu_{\mathfrak{a}}) \circ (\nu_{\mathfrak{b}} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1}) \tag{4.2.12.2}$$

for each $\mathfrak{a}, \mathfrak{b} \in \mathrm{P}$.

We can actually say more about the $\nu_{\mathfrak{a}}$ when $\sigma_{\mathfrak{a}} = \mathrm{id_L}$. In this case, we get an isomorphism $\nu_{\mathfrak{a}} : \mathscr{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \to \sigma_{\mathfrak{a}}^*(\mathscr{E}) = \mathscr{E}$ which must be of the form $1 \otimes l(\mathfrak{a})$ for some $l(\mathfrak{a}) \in \mathrm{O_K}$ which generates $\mathfrak{a}$. If, moreover, there is an ideal $\mathfrak{f}$ such that $\mathrm{E}[\mathfrak{f}]$, and hence $\mathscr{E}[\mathfrak{f}]$, are constant then composition

$$\mathscr{E}[\mathfrak{f}] \to \mathscr{E}[\mathfrak{f}] \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \overset{\nu_{\mathfrak{a}}[\mathfrak{f}]}{\to} \mathscr{E}[\mathfrak{f}]$$

is equal to the unique relative Frobenius lift

$$l(\mathfrak{a}) = \psi^{\mathfrak{a}}_{\mathscr{E}[\mathfrak{f}]/\mathrm{S}} = \mathrm{id}_{\mathscr{E}[\mathfrak{f}]} : \mathscr{E}[\mathfrak{f}] \to \mathscr{E}[\mathfrak{f}]$$

so that $l(\mathfrak{a}) = 1 \bmod \mathfrak{f}$.

By the Néron mapping property the isomorphisms $\nu_{\mathfrak{a}}$ extend to isomorphisms on the full Néron model

$$\nu_{\mathfrak{a}} : \mathrm{Nér}_{\mathrm{O_L}}(\mathrm{E}) \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \xrightarrow{\sim} \sigma_{\mathfrak{a}}^*(\mathrm{Nér}_{\mathrm{O_L}}(\mathrm{E}))$$

satisfying the same commutativity condition (note that $\mathrm{Nér}_{\mathrm{O_L}}(\mathrm{E})$ is a smooth group scheme of relative dimension one, not necessarily proper). Denoting by

$$\mathrm{T} = \underline{\mathrm{Lie}}_{\mathrm{Nér}_{\mathrm{O_L}}(\mathrm{E})/\mathrm{Spec}(\mathrm{O_L})}$$

the Lie algebra of the Néron model, which is a projective rank one $\mathrm{O_L}$-module, the isomorphisms $\nu_{\mathfrak{a}}$ induce $\mathrm{O_L}$-isomorphisms (which we denote by the same letter)

$$\nu_{\mathfrak{a}} : \mathrm{T} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \xrightarrow{\sim} \sigma_{\mathfrak{a}}^*(\mathrm{T})$$

for each $\mathfrak{a} \in \mathrm{P}$, satisfying the same commutativity condition (4.2.12.2) as the $\nu_{\mathfrak{a}}$ on $\mathrm{Nér}_{\mathrm{O_L}}(\mathrm{E})$.

4.2.13 Corollary. — *In the notation of* (4.2.12)*, if* $\mathrm{L} = \mathrm{K}(\mathfrak{f})$ *is a ray class field and* $\mathrm{E}[\mathfrak{f}]$ *is constant then the Lie algebra of the Néron model* $\mathrm{Nér}_{\mathrm{O_{K(f)}}}(\mathrm{E})$ *becomes free after inverting* $\mathfrak{f}$*. In other words,* $\mathrm{E}/\mathrm{Spec}(\mathrm{K}(\mathfrak{f}))$ *admits a global minimal model away from* $\mathfrak{f}$*.*

Proof. — We have the isomorphisms

$$\nu_{\mathfrak{a}} : \mathrm{T} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \xrightarrow{\sim} \sigma_{\mathfrak{a}}^*(\mathrm{T})$$

for each ideal $\mathfrak{a} \in \mathrm{P} = \mathrm{Id}^{(\mathfrak{g})}_{\mathrm{O_K}}$ and when $\sigma_{\mathfrak{a}} = \mathrm{id}_{\mathrm{O_{K(f)}}}$ (this is the case if and only if $\mathfrak{a} = (a)$ is principal with $a = 1 \bmod \mathfrak{f}$) the isomorphism

$$\nu_{\mathfrak{a}} : \mathrm{T} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \xrightarrow{\sim} \sigma_{\mathfrak{a}}^*(\mathrm{T}) = \mathrm{T}$$

takes the form $1 \otimes l(\mathfrak{a})$ where $l(\mathfrak{a}) \in \mathrm{O_K}$ is a generator of $\mathfrak{a}$ such that $l(\mathfrak{a}) = 1 \bmod \mathfrak{f}$. We now apply (A.4.1) to extend l to a map $l : \mathrm{Id}^{(\mathfrak{g})}_{\mathrm{O_K}} \to \mathrm{O_{K(\mathfrak{f})}}$ satisfying

$$l(\mathfrak{a}) \cdot \mathrm{O_{K(\mathfrak{f})}} = \mathfrak{a} \cdot \mathrm{O_{K(\mathfrak{f})}} \quad \text{and} \quad l(\mathfrak{ab}) = l(\mathfrak{a})\sigma_{\mathfrak{a}}(l(\mathfrak{b})) \tag{4.2.13.1}$$

for all $\mathfrak{a}, \mathfrak{b} \in \mathrm{Id}^{(\mathfrak{g})}_{\mathrm{O_K}}$. Define $t_{\mathfrak{a}} : \mathrm{T} \to \sigma^*_{\mathfrak{a}}(\mathrm{T})$ be the composition

$$\mathrm{T} \xrightarrow{1 \otimes l(\mathfrak{a})^{-1}} \mathrm{T} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} \xrightarrow{\nu_{\mathfrak{a}}} \sigma^*_a(\mathrm{T}).$$

Then $t_{\mathfrak{a}}$ is an isomorphism by (4.2.13.1), and if $\mathfrak{a} \in \mathrm{Prin}^{(\mathfrak{g})}_{1 \bmod \mathfrak{f}}$ then $t_{\mathfrak{a}} = l(\mathfrak{a}) \otimes l(\mathfrak{a})^{-1} = \mathrm{id_T}$ which, combined with the commutativity conditions (4.2.12.2) on the $\nu_{\mathfrak{a}}$ and (4.2.13.1) on the $l(\mathfrak{a})$, show that $t_{\mathfrak{a}}$ depends only on the class $\sigma_{\mathfrak{a}} \in \mathrm{G(K(\mathfrak{f})/K)}$, that $t_{\mathrm{id_{K(\mathfrak{f})}}} = \mathrm{id_T}$ and that $t_{\sigma\tau} = t_\sigma \circ \sigma^*(t_\tau)$ for $\sigma, \tau \in \mathrm{G(K(\mathfrak{f})/K)}$.

In other words, the isomorphisms t_σ (or perhaps what is more standard, their inverses) define Galois descent data on T relative to $\mathrm{O_K} \to \mathrm{O_{K(\mathfrak{f})}}$. As $\mathrm{O_K} \to \mathrm{O_{K(\mathfrak{f})}}$ becomes finite and étale after inverting $\mathfrak{f}$, there exists an $\mathrm{O_K}[\mathfrak{f}^{-1}]$-module T_0 such that

$$\mathrm{T}_0 \otimes_{\mathrm{O_K}[\mathfrak{f}^{-1}]} \mathrm{O_{K(\mathfrak{f})}}[\mathfrak{f}^{-1}] \xrightarrow{\sim} \mathrm{T} \otimes_{\mathrm{O_{K(\mathfrak{f})}}} \mathrm{O_{K(\mathfrak{f})}}[\mathfrak{f}^{-1}].$$

However, as $\mathrm{K}(\mathfrak{f})$ contains the Hilbert class field H, all rank one projective $\mathrm{O_K}[\mathfrak{f}^{-1}]$-modules become free after base change to $\mathrm{O_{K(\mathfrak{f})}}[\mathfrak{f}^{-1}]$ (all rank one projective $\mathrm{O_K}$-modules do by the Hauptidealsatz (4.2.11) and every rank one projective $\mathrm{O_K}[\mathfrak{f}^{-1}]$-module is a localisation of a rank one projective $\mathrm{O_K}$-module). It follows that

$$\mathrm{T}_0 \otimes_{\mathrm{O_K}[\mathfrak{f}^{-1}]} \mathrm{O_{K(\mathfrak{f})}}[\mathfrak{f}^{-1}] \xrightarrow{\sim} \mathrm{T} \otimes_{\mathrm{O_{K(\mathfrak{f})}}} \mathrm{O_{K(\mathfrak{f})}}[\mathfrak{f}^{-1}] = \underline{\mathrm{Lie}}_{\mathrm{Nér_{O_L}(E)/Spec(O_L)}} \otimes_{\mathrm{O_L}} \mathrm{O_L}[\mathfrak{f}^{-1}]$$

is free. □

4.2.14 Remark. — We note that when $\mathfrak{f} = \mathrm{O_K}$ (4.2.13) the condition on the $\mathfrak{f}$-torsion becomes trivial so that *any* CM elliptic E/H of Shimura type admits a *global* minimal model. This generalises the main result (see Corollary 4.4) of [**22**] where it is shown that a CM elliptic curve E/H admits a global minimal model whenever the conductor of K over **Q** is prime and the homomorphism $\rho_{\mathrm{E/H}}$ satisfies a certain invariance condition. One can show that these assumptions imply E/H is a CM elliptic curve of Shimura type so that (4.2.13) is indeed a generalisation of [**22**]. To say a little, the invariance condition on $\rho_{\mathrm{E/H}}$ is equivalent to E being isogenous to $\sigma^*(\mathrm{E})$ for each $\sigma \in \mathrm{G(H/K)}$ and the primality of the discriminant of K over **Q** implies that the order of G(H/K) is prime to the order of $\mathrm{O_K^\times}$ and together these properties allow one to show that E/H is a CM elliptic curve of Shimura type (for a result along these lines see Proposition 2 of [**28**]).

4.3. Weber functions

The purpose of this section is to define, for each CM elliptic curve E over an arbitrary base S, a certain quotient $\mathrm{E} \to \mathrm{X}_{\mathrm{E/S}}$ and then to study its resulting properties. Informally, $\mathrm{X}_{\mathrm{E/S}}$ will be the quotient of E by its group of automorphisms $\underline{\mathrm{O}_{\mathrm{K}}^{\times}}_{\mathrm{S}}$. However, $\underline{\mathrm{O}_{\mathrm{K}}^{\times}}_{\mathrm{S}}$ does not act freely on E and so the orbits of are not well behaved. This makes it difficult to construct a quotient (in the naive sense) with any useful properties. We get around this problem by using Cartier divisors to define intelligent orbits for the action of $\underline{\mathrm{O}_{\mathrm{K}}^{\times}}_{\mathrm{S}}$ under which it behaves as though it were free. Taking the quotient by the resulting equivalence relation, we get a smooth, proper curve $\mathrm{X}_{\mathrm{E/S}}$ together with a $\underline{\mathrm{O}_{\mathrm{K}}^{\times}}_{\mathrm{S}}$-invariant finite locally free map of degree $w = \#\mathrm{O}_{\mathrm{K}}^{\times}$

$$p_{\mathrm{E/S}} : \mathrm{E} \to \mathrm{X}_{\mathrm{E/S}}.$$

The construction we give is functorial in E/S and so we may run it for the universal CM elliptic curve $\mathscr{E} \to \mathscr{M}_{\mathrm{CM}}$ to obtain a smooth, proper curve $\mathrm{X}_{\mathscr{E}/\mathscr{M}_{\mathrm{CM}}} \to \mathscr{M}_{\mathrm{CM}}$. Almost by definition, this curve descends to a smooth proper curve $f : \mathrm{X} \to \mathrm{M}_{\mathrm{CM}}$ over the coarse sheaf.

The remainder of the section is devoted to the study of $\mathrm{X} \to \mathrm{M}_{\mathrm{CM}}$. We first show that it has the following properties:

(i) $f : \mathrm{X} \to \mathrm{M}_{\mathrm{CM}}$ admits a natural $\Lambda_{\mathrm{M}_{\mathrm{CM}}}$-structure and a $\Lambda_{\mathrm{M}_{\mathrm{CM}}}$-point $0_{\mathrm{X}} : \mathrm{M}_{\mathrm{CM}} \to \mathrm{X}$,

(ii) $f : \mathrm{X} \to \mathrm{M}_{\mathrm{CM}}$ has genus zero. Thus, if $\mathscr{I}_{\mathrm{X}} \subset \mathscr{O}_{\mathrm{X}}$ denotes the ideal sheaf defining the closed point $0_{\mathrm{X}} : \mathrm{M}_{\mathrm{CM}} \to \mathrm{X}$ and $\mathscr{W} = f_*(\mathscr{I}_{\mathrm{X}}^{-1})$ then $\mathscr{W}$ is locally free of rank two over $\mathscr{O}_{\mathrm{M}_{\mathrm{CM}}}$, the map $f^*(\mathscr{W}) \to \mathscr{I}_{\mathrm{X}}^{-1}$ is an epimorphism and the resulting map

$$\mathrm{X} \xrightarrow{\sim} \mathbf{P}_{\mathrm{M}_{\mathrm{CM}}}(\mathscr{W})$$

is an isomorphism,

(iii) setting $\mathrm{X}[\mathfrak{a}] = \psi^{\mathfrak{a}*}_{\mathrm{X}/\mathrm{M}_{\mathrm{CM}}}(0_{\mathrm{X}}) \subset \mathrm{X}$, the scheme $\mathrm{X}[\mathfrak{a}]$ is a finite locally free $\Lambda_{\mathrm{M}_{\mathrm{CM}}}$-scheme of degree $\mathrm{N}\mathfrak{a}$ and $\mathrm{K}(\mathrm{X}[\mathfrak{a}]) = \mathrm{K}(\mathfrak{a})$.

Thus the curve $\mathrm{X} \to \mathrm{M}_{\mathrm{CM}}$ together with its $\Lambda_{\mathrm{M}_{\mathrm{CM}}}$-structure and its $\Lambda_{\mathrm{M}_{\mathrm{CM}}}$-point $0_{\mathrm{X}} : \mathrm{M}_{\mathrm{CM}} \to \mathrm{X}$ allow one to construct the ray class fields of K in an integral and coherent, choice free manner. Of course, this is just a more streamlined and abstract approach to the classical construction of the ray class fields of K using Weber functions — this approach being to choose a CM elliptic curve E/H and to consider the image of $\mathrm{E}[\mathfrak{a}] \subset \mathrm{E}$ under a 'Weber map'

$$\mathrm{E} \to \mathbf{P}^1_{\mathrm{H}}$$

which is a certain $\mathrm{O}_{\mathrm{K}}^{\times}$-invariant map of degree w (see Theorem 5.6 of [**34**]).

The only defect of our approach is that the curve $\mathrm{X} \to \mathrm{M}_{\mathrm{CM}}$ is not particularly explicit. However, we end the section by showing (by the same method

we used to show that CM elliptic curves of Shimura type admit global minimal models) that there exists an isomorphism $\mathrm{X} \xrightarrow{\sim} \mathbf{P}^1_{\mathrm{M_{CM}}}$.

4.3.1. We begin by recalling some basic facts regarding Cartier divisors on curves (see §§1.1-1.2 Chapter I of [**24**]). Let S be a scheme and let $\mathrm{X} \to \mathrm{S}$ be a smooth proper S-curve, i.e. $\mathrm{X} \to \mathrm{S}$ is smooth of relative dimension one and proper. An S-relative Cartier divisor on X, or just a Cartier divisor, is a closed sub-scheme $\mathrm{D} \subset \mathrm{X}$ which is finite locally free over S. Equivalently, a closed sub-scheme $\mathrm{D} \subset \mathrm{X}$ is a Cartier divisor if and only if $\mathrm{D} \to \mathrm{S}$ is flat and the ideal sheaf $\mathscr{I}_{\mathrm{D}} \subset \mathscr{O}_{\mathrm{E}}$ defining D is a locally free rank one $\mathscr{O}_{\mathrm{X}}$-module. Given two Cartier divisors $\mathrm{D}, \mathrm{D}' \subset \mathrm{X}$, their sum $\mathrm{D} + \mathrm{D}' \subset \mathrm{X}$ is defined to be the closed sub-scheme corresponding to the ideal sheaf $\mathscr{I}_{\mathrm{D}+\mathrm{D}'} := \mathscr{I}_{\mathrm{D}} \otimes_{\mathscr{O}_{\mathrm{X}}} \mathscr{I}_{\mathrm{D}'} \subset \mathscr{O}_{\mathrm{X}}$, which is again a Cartier divisor.

The degree $\deg(\mathrm{D})$ of a Cartier divisor $\mathrm{D} \subset \mathrm{S}$ is defined to be the degree of the finite locally free S-scheme D. We have $\deg(\mathrm{D} + \mathrm{D}') = \deg(\mathrm{D}) + \deg(\mathrm{D})$. The structure map $\mathrm{D} \to \mathrm{S}$ of a Cartier divisor on X is an isomorphism if and only if $\deg(\mathrm{D}) = 1$ and the set of degree one Cartier divisors on E is equal to the set of S-points $\mathrm{S} \to \mathrm{X}$. If $s \in \mathrm{X}(\mathrm{S})$ is an S-point then we will denote the corresponding Cartier divisor by s.

If $f : \mathrm{X}' \to \mathrm{X}$ is a finite locally free map of smooth, proper S-curves and if $\mathrm{D} \subset \mathrm{X}$ is a Cartier divisor then $f^*(\mathrm{D}) \subset \mathrm{X}'$ is a Cartier divisor and $\deg(f^*(\mathrm{D})) = \deg(f)\deg(\mathrm{D})$.

Given a pair of Cartier divisors $\mathrm{D}, \mathrm{D}' \subset \mathrm{X}$ such that $\deg(\mathrm{D}) \leq \deg(\mathrm{D}')$ (resp. $\deg(\mathrm{D}) = \deg(\mathrm{D}')$) we can form the inclusion (resp. equality) S-sheaf of D and D′:

$$\mathrm{In}_{\mathrm{X/S}}(\mathrm{D}, \mathrm{D}') \subset \mathrm{S} \quad (\text{resp.} \quad \mathrm{Eq}_{\mathrm{X/S}}(\mathrm{D}, \mathrm{D}') \subset \mathrm{S})$$

defined by the property that $\mathrm{T} \to \mathrm{S}$ factors through $\mathrm{In}_{\mathrm{X/S}}(\mathrm{D}, \mathrm{D}') \to \mathrm{S}$ (resp. $\mathrm{Eq}_{\mathrm{X/S}}(\mathrm{D}, \mathrm{D}') \to \mathrm{S}$) if and only we have an inclusion (resp. equality) of Cartier divisors

$$\mathrm{D} \times_{\mathrm{S}} \mathrm{T} \subset \mathrm{D}' \times_{\mathrm{S}} \mathrm{T} \subset \mathrm{X} \times_{\mathrm{S}} \mathrm{T} \quad (\text{resp.} \quad \mathrm{D} \times_{\mathrm{S}} \mathrm{T} = \mathrm{D}' \times_{\mathrm{S}} \mathrm{T} \subset \mathrm{X} \times_{\mathrm{S}} \mathrm{T}).$$

By Key Lemma 1.3.4 and Corollary 1.3.5 of [**24**], the sub-sheaves $\mathrm{In}_{\mathrm{X/S}}(\mathrm{D}, \mathrm{D}')$ and $\mathrm{Eq}_{\mathrm{X/S}}(\mathrm{D}, \mathrm{D}')$ of S are finitely presented closed sub-schemes of S. Finally, if $\mathrm{S}' \to \mathrm{S}$ is a morphism then we have natural isomorphisms

$$\mathrm{In}_{\mathrm{X_{S'}/S'}}(\mathrm{D}_{\mathrm{S}'}, \mathrm{D}'_{\mathrm{S}'}) \xrightarrow{\sim} \mathrm{In}_{\mathrm{X/S}}(\mathrm{D}, \mathrm{D}')_{\mathrm{S}'} \quad \text{and} \quad \mathrm{Eq}_{\mathrm{X_{S'}/S'}}(\mathrm{D}_{\mathrm{S}'}, \mathrm{D}'_{\mathrm{S}'}) \xrightarrow{\sim} \mathrm{Eq}_{\mathrm{X/S}}(\mathrm{D}, \mathrm{D}')_{\mathrm{S}'}.$$

4.3.2. Now let E/S be a CM elliptic curve. We would like to take the quotient of E by the action of its group of automorphisms $\underline{\mathrm{O_K}}^{\times}_{\mathrm{S}}$ but, as noted in the introduction, this action is not free and in particular the map

$$\coprod_{\epsilon \in \mathrm{O_K^\times}} (\epsilon, \mathrm{id_E}) : \coprod_{\epsilon \in \mathrm{O_K^\times}} \mathrm{E} = \underline{\mathrm{O_K^\times}}_{\mathrm{S}} \times_{\mathrm{S}} \mathrm{E} \to \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$$

is not injective so that the orbits of points under this action are not well behaved. Of course, one could just take the image of this map and obtain an equivalence relation but then one would have little control over the quotient.

We get around this as follows. If $s : \mathrm{S} \to \mathrm{E}$ is an S-point, we define its 'orbit' $[\mathrm{O}_\mathrm{K}^\times](s) \subset \mathrm{E}$ to be the Cartier divisor

$$[\mathrm{O}_\mathrm{K}^\times](s) = \sum_{\epsilon \in \mathrm{O}_\mathrm{K}^\times} \epsilon^*(s)$$

(note the sum is of Cartier divisors and has nothing to do with the group law on E). Then $[\mathrm{O}_\mathrm{K}^\times](s) \subset \mathrm{E}$ contains the Cartier divisor s, is stable under the action of $\underline{\mathrm{O}_\mathrm{K}^\times}_\mathrm{S}$ and is finite locally free of degree w over S (as the usual orbit would be if the action of G were free). Equality of these 'orbits' defines an equivalence relation on E, which we denote by

$$\mathrm{Eq}_{\mathrm{E}/\mathrm{S}}^{\mathrm{O}_\mathrm{K}^\times} \subset \mathrm{E} \times_\mathrm{S} \mathrm{E},$$

so that an S-morphism $\mathrm{T} \to \mathrm{E} \times_\mathrm{S} \mathrm{E}$ factors through $\mathrm{Eq}_{\mathrm{E}/\mathrm{S}}^{\mathrm{O}_\mathrm{K}^\times}$ if and only if, writing $(t_1, t_2) : \mathrm{T} \to (\mathrm{E} \times_\mathrm{S} \mathrm{E}) \times_\mathrm{S} \mathrm{T} = \mathrm{E}_\mathrm{T} \times_\mathrm{T} \mathrm{E}_\mathrm{T}$ for the resulting map, we have an equality of Cartier divisors

$$[\mathrm{O}_\mathrm{K}^\times](t_1) = [\mathrm{O}_\mathrm{K}^\times](t_2) \subset \mathrm{E}_\mathrm{T} = \mathrm{E} \times_\mathrm{S} \mathrm{T}.$$

For this equivalence relation to behave as though it really does come from a group action, it should be the case that, given two points $s_1, s_2 : \mathrm{S} \to \mathrm{E}$ then having $s_1 \in [\mathrm{O}_\mathrm{K}^\times](s_2)$, i.e. $s_1 : \mathrm{S} \to \mathrm{E}$ factoring through $[\mathrm{O}_\mathrm{K}^\times](s_2)$, should imply the equality of 'orbits'

$$[\mathrm{O}_\mathrm{K}^\times](s_1) = [\mathrm{O}_\mathrm{K}^\times](s_2).$$

With this in mind, we define the sub-sheaf

$$\mathrm{In}_{\mathrm{E}/\mathrm{S}}^{\mathrm{O}_\mathrm{K}^\times} \subset \mathrm{E} \times_\mathrm{S} \mathrm{E}$$

by the property that an S-morphism $\mathrm{T} \to \mathrm{E} \times_\mathrm{S} \mathrm{E}$ factors through $\mathrm{In}_{\mathrm{E}/\mathrm{S}}^{\mathrm{O}_\mathrm{K}^\times} \subset \mathrm{E} \times_\mathrm{S} \mathrm{E}$ if and only if, writing $(t_1, t_2) : \mathrm{T} \to (\mathrm{E} \times_\mathrm{S} \mathrm{E}) \times_\mathrm{S} \mathrm{T} = \mathrm{E}_\mathrm{T} \times_\mathrm{T} \mathrm{E}_\mathrm{T}$ for the corresponding map, the Cartier divisor $t_1 : \mathrm{E} \to \mathrm{E}_\mathrm{T}$ factors through the Cartier divisor $[\mathrm{O}_\mathrm{K}^\times](t_2) \subset \mathrm{E}_\mathrm{T}$, i.e. $t_1 \in [\mathrm{O}_\mathrm{K}^\times](t_2)$. There is a natural inclusion

$$\mathrm{Eq}_{\mathrm{E}/\mathrm{S}}^{\mathrm{O}_\mathrm{K}^\times} \subset \mathrm{In}_{\mathrm{E}/\mathrm{S}}^{\mathrm{O}_\mathrm{K}^\times} \subset \mathrm{E} \times_\mathrm{S} \mathrm{E}$$

and our claim that the equivalence relation $\mathrm{Eq}_{\mathrm{E}/\mathrm{S}}^{\mathrm{O}_\mathrm{K}^\times}$ behaves as though it were coming from a free action of a group is that we have an equality

$$\mathrm{Eq}_{\mathrm{E}/\mathrm{S}}^{\mathrm{O}_\mathrm{K}^\times} = \mathrm{In}_{\mathrm{E}/\mathrm{S}}^{\mathrm{O}_\mathrm{K}^\times} \subset \mathrm{E} \times_\mathrm{S} \mathrm{E}.$$

Before we prove this, let us make two observations. First, the sub-sheaves $\mathrm{Eq}_{\mathrm{E}/\mathrm{S}}^{\mathrm{O}_\mathrm{K}^\times} \subset \mathrm{In}_{\mathrm{E}/\mathrm{S}}^{\mathrm{O}_\mathrm{K}^\times} \subset \mathrm{E} \times_\mathrm{S} \mathrm{E}$ are in fact closed sub-schemes. View $\mathrm{E} \times_\mathrm{S} (\mathrm{E} \times_\mathrm{S} \mathrm{E}) \to$

$\mathrm{E} \times_{\mathrm{S}} \mathrm{E}$ as a CM elliptic curve over $\mathrm{E} \times_{\mathrm{S}} \mathrm{E}$ via projection onto the second two factors and consider the Cartier divisors

$$u_{\mathrm{E/S},1} : \mathrm{E} \times_{\mathrm{S}} \mathrm{E} \to \mathrm{E} \times_{\mathrm{S}} (\mathrm{E} \times_{\mathrm{S}} \mathrm{E}) : (e_1, e_2) \mapsto (e_1, e_1, e_2)$$

and

$$u_{\mathrm{E/S},2} : \mathrm{E} \times_{\mathrm{S}} \mathrm{E} \to \mathrm{E} \times_{\mathrm{S}} (\mathrm{E} \times_{\mathrm{S}} \mathrm{E}) : (e_1, e_2) \mapsto (e_2, e_1, e_2).$$

Then it is an easy exercise to check that we have equalities of sub-sheaves of $\mathrm{E} \times_{\mathrm{S}} \mathrm{E}$

$$\mathrm{Eq}^{\mathrm{O_K^\times}}_{\mathrm{E/S}} = \mathrm{Eq}_{\mathrm{E}\times_{\mathrm{S}}(\mathrm{E}\times_{\mathrm{S}}\mathrm{E})/\mathrm{E}\times_{\mathrm{S}}\mathrm{E}}([\mathrm{O_K^\times}](u_{\mathrm{E/S},1}), [\mathrm{O_K^\times}](u_{\mathrm{E/S},2})) \subset \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$$

and

$$\mathrm{In}^{\mathrm{O_K^\times}}_{\mathrm{E/S}} = \mathrm{In}_{\mathrm{E}\times_{\mathrm{S}}(\mathrm{E}\times_{\mathrm{S}}\mathrm{E})/\mathrm{E}\times_{\mathrm{S}}\mathrm{E}}(u_{\mathrm{E/S},2}, [\mathrm{O_K^\times}](u_{\mathrm{E/S},2})) \subset \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$$

so that by the representability of equality and inclusion sub-sheaves of Cartier divisors we find that $\mathrm{Eq}^{\mathrm{O_K^\times}}_{\mathrm{E/S}}$ and $\mathrm{In}^{\mathrm{O_K^\times}}_{\mathrm{E/S}}$ are closed sub-schemes of $\mathrm{E} \times_{\mathrm{S}} \mathrm{E}$.

Our second observation is that, viewing $\mathrm{E} \times_{\mathrm{S}} \mathrm{E} \to \mathrm{E}$ as a CM elliptic curve over E via projection onto the second factor, we have an equality of sub-schemes

$$\mathrm{In}^{\mathrm{O_K^\times}}_{\mathrm{E/S}} = [\mathrm{O_K^\times}](\Delta_{\mathrm{E/S}}) \subset \mathrm{E} \times_{\mathrm{S}} \mathrm{E}.$$

Indeed, fixing an affine scheme T over S and a morphism $\mathrm{T} \to \mathrm{E}$, which we identify with a morphism $t_2 : \mathrm{T} \to \mathrm{E} \times_{\mathrm{S}} \mathrm{T} = \mathrm{E_T}$, the pull-back of the E-morphism $[\mathrm{O_K^\times}](\Delta_{\mathrm{E/S}}) \subset \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$ along $\mathrm{T} \to \mathrm{E}$ is given by

$$[\mathrm{O_K^\times}](t_2) \subset \mathrm{E_T} = \mathrm{E} \times_{\mathrm{S}} \mathrm{T}$$

(as the pull-back of $\Delta_{\mathrm{E/S}} : \mathrm{E} \to \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$ is given by $t_2 : \mathrm{T} \to \mathrm{E_T} = \mathrm{E} \times_{\mathrm{S}} \mathrm{T}$). Therefore, for a second S-morphism $\mathrm{T} \to \mathrm{E}$, which we identify with a morphism $t_1 : \mathrm{T} \to \mathrm{E_T} = \mathrm{E} \times_{\mathrm{S}} \mathrm{T}$, to have the property that the induced map $\mathrm{T} \to \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$ factors through $[\mathrm{O_K^\times}](\Delta_{\mathrm{E/S}})$, is equivalent to the morphism $t_1 : \mathrm{T} \to \mathrm{E_T}$ factoring through $[\mathrm{O_K^\times}](t_2) \subset \mathrm{E_T}$. All said and done, a morphism $\mathrm{T} \to \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$ factors through $[\mathrm{O_K^\times}](\Delta_{\mathrm{E/S}}) \subset \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$ if and only if, in the notation above, the morphism $t_1 : \mathrm{T} \to \mathrm{E_T}$ factors through $[\mathrm{O_K^\times}](t_2) \subset \mathrm{E_T}$ which is to say that $\mathrm{T} \to \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$ factors through $\mathrm{In}^{\mathrm{O_K^\times}}_{\mathrm{E/S}} \subset \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$. We are now ready to prove our claim.

4.3.3 Proposition. — *Let* $\mathrm{E/S}$ *be a* CM *elliptic curve. Then we have equalities of closed sub-schemes of* $\mathrm{E} \times_{\mathrm{S}} \mathrm{E}$

$$\mathrm{Eq}^{\mathrm{O_K^\times}}_{\mathrm{E/S}} = \mathrm{In}^{\mathrm{O_K^\times}}_{\mathrm{E/S}} = [\mathrm{O_K^\times}](\Delta_{\mathrm{E/S}}) \subset \mathrm{E} \times_{\mathrm{S}} \mathrm{E}.$$

In particular, $\mathrm{Eq}^{\mathrm{O_K^\times}}_{\mathrm{E/S}}$ *is a finite locally free equivalence relation of degree* w.

Proof. — The only thing we need to show is that the inclusion

$$\mathrm{Eq}_{\mathrm{E/S}}^{\mathrm{O_K^\times}} \subset \mathrm{In}_{\mathrm{E/S}}^{\mathrm{O_K^\times}}$$

is an equality. The first thing we note is that it is bijective on geometric points. That is, if $\mathrm{S} = \mathrm{Spec}(\mathrm{F})$ is the spectrum of an algebraically closed field F, and $(s_1, s_2) \in \mathrm{E}(\mathrm{S}) \times \mathrm{E}(\mathrm{S})$ satisfy $s_1 \in [\mathrm{O_K^\times}](s_2)$ then $[\mathrm{O_K^\times}](s_1) = [\mathrm{O_K^\times}](s_2)$. But this is clear, as E is then a Dedekind scheme and unique factorisation of Cartier divisors (i.e. of the corresponding ideals) shows that there exists an $\epsilon \in \mathrm{O_K^\times}$ (not necessarily unique!) such that $s_1 = \epsilon s_2$ which gives

$$[\mathrm{O_K^\times}](s_1) = [\mathrm{O_K^\times}](\epsilon s_1) = [\mathrm{O_K^\times}](s_2).$$

It follows that the inclusion

$$\mathrm{Eq}_{\mathrm{E/S}}^{\mathrm{O_K^\times}} \subset \mathrm{In}_{\mathrm{E/S}}^{\mathrm{O_K^\times}},$$

which is a closed immersion, is a nilpotent thickening.

Now, our claim is local on S and so we may assume that S admits a level-$\mathfrak{f}$ structure for some $\mathfrak{f}$ which separates units. It follows that way assume there exists a morphism $\mathrm{S} \to \mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})}$ and an isomorphism

$$\mathrm{E} \xrightarrow{\sim} \mathrm{E}^{(\mathfrak{f})} \times_{\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})}} \mathrm{S}$$

and again by the compatibility of inclusion and equality schemes of Cartier divisors with base change, we may assume that $\mathrm{E/S} = \mathrm{E}^{(\mathfrak{f})}/\mathrm{M}_{\mathrm{CM}}^{(\mathfrak{f})}$, or what is important, that S is integral.

We will now show that the nilpotent immersion

$$\mathrm{Eq}_{\mathrm{E/S}}^{\mathrm{O_K^\times}} \to \mathrm{In}_{\mathrm{E/S}}^{\mathrm{O_K^\times}}$$

is an isomorphism by showing that $\mathrm{In}_{\mathrm{E/S}}^{\mathrm{O_K^\times}}$ is reduced. Since S is an integral scheme, it follows that E is also an integral scheme. Therefore, the finite locally free E-scheme $\mathrm{In}_{\mathrm{E/S}}^{\mathrm{O_K^\times}} \subset \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$ is reduced if and only if for some non-empty open sub-scheme $\mathrm{U} \subset \mathrm{E}$ the pull-back $\mathrm{In}_{\mathrm{E/S}}^{\mathrm{O_K^\times}} \times_{\mathrm{E}} \mathrm{U}$ is reduced.

So let

$$\mathrm{U} = \bigcap_{1 \neq \epsilon \in \mathrm{O_K^\times}} (\mathrm{E} - \mathrm{E}[1 - \epsilon]).$$

Then over U, the Cartier divisors

$$\epsilon^*(\Delta_{\mathrm{E/S}} \times_{\mathrm{E}} \mathrm{U}) : \mathrm{U} \to \mathrm{E} \times_{\mathrm{S}} \mathrm{U}$$

for $\epsilon \in \mathrm{O_K^\times}$ are all disjoint so that

$$\mathrm{In}_{\mathrm{E/S}}^{\mathrm{O_K^\times}} \times_{\mathrm{E}} \mathrm{U} = [\mathrm{O_K^\times}](\Delta_{\mathrm{E/S}}) \times_{\mathrm{E}} \mathrm{U} = \coprod_{\epsilon \in \mathrm{O_K^\times}} \epsilon^*(\Delta_{\mathrm{E/S}} \times_{\mathrm{E}} \mathrm{U}) \xrightarrow{\sim} \coprod_{\mathrm{O_K^\times}} \mathrm{E} \times_{\mathrm{S}} \mathrm{U}.$$

It follows that $\mathrm{In}^{\mathrm{O_K^\times}}_{\mathrm{E/S}} \times_{\mathrm{E}} \mathrm{U}$ and therefore $\mathrm{In}^{\mathrm{O_K^\times}}_{\mathrm{E/S}}$ are reduced and the nilpotent immersion

$$\mathrm{Eq}^{\mathrm{O_K^\times}}_{\mathrm{E/S}} \subset \mathrm{In}^{\mathrm{O_K^\times}}_{\mathrm{E/S}}$$

is an isomorphism. □

4.3.4. We are now ready to construct our quotients. So let E/S be a CM elliptic curve. Then the Cartier divisor of degree w

$$\mathrm{Eq}^{\mathrm{O_K^\times}}_{\mathrm{E/S}} = [\mathrm{O_K^\times}](\Delta_{\mathrm{E/S}}) \subset \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$$

defines the equivalence relation on E/S where $s_1, s_2 \in \mathrm{E(S)}$ are equivalent if and only if

$$[\mathrm{O_K^\times}](s_1) = [\mathrm{O_K^\times}](s_2).$$

We write

$$p_{\mathrm{E/S}} : \mathrm{E} \to \mathrm{X}_{\mathrm{E/S}}$$

for the resulting quotient (in the category of fpqc sheaves). As our equivalence relation is finite locally free (and E is projective over S) it follows from Corollaire 7.1 Exposé VII of [**3**] that $\mathrm{X}_{\mathrm{E/S}}$ is representable by a scheme over S. We have thus constructed a finite locally free $\underline{\mathrm{O_K^\times}}_{\mathrm{S}}$-invariant map of degree w

$$p_{\mathrm{E/S}} : \mathrm{E} \to \mathrm{X}_{\mathrm{E/S}}.$$

4.3.5 Proposition. — *The* S*-scheme* $\mathrm{X}_{\mathrm{E/S}} \to \mathrm{S}$ *is smooth of relative dimension one, proper and geometrically connected.*

Proof. — As $\mathrm{E} \to \mathrm{S}$ is proper, flat, and geometrically connected and $p_{\mathrm{E/S}} : \mathrm{X} \to \mathrm{X}_{\mathrm{E/S}}$ is finite locally free of degree w (in particular, proper, flat and surjective), it follows that $\mathrm{X}_{\mathrm{E/S}} \to \mathrm{S}$ is proper, flat, and geometrically connected. As $\mathrm{X}_{\mathrm{E/S}} \to \mathrm{S}$ is flat, it is smooth if and only if its fibres are smooth, but when S is the spectrum of a field E is a regular scheme of dimension one and $\mathrm{E} \to \mathrm{X}_{\mathrm{E/S}}$ is finite locally free so that $\mathrm{X}_{\mathrm{E/S}}$ is also regular of dimension one and therefore smooth over S. □

4.3.6 Remark. — The method used above to construct the quotients $\mathrm{X}_{\mathrm{E/S}}$ applies more generally. Indeed, if $\mathrm{X} \to \mathrm{S}$ is a smooth (not necessarily proper) curve, S is an integral scheme and G is a finite group acting generically freely on X by S-automorphisms then there exists a smooth curve X/[G] and a finite locally free G-invariant map $p : \mathrm{X} \to \mathrm{X}/[\mathrm{G}]$ of degree #G, i.e. what might be called a 'quotient' of X by G. It would be interesting to know whether this method could be extended to construct 'quotients' of curves over more general bases S, or under more general (non-constant) group actions.

4.3.7. Let us now consider the functorial properties of the association $\mathrm{E}/\mathrm{S} \mapsto \mathrm{X}_{\mathrm{E}/\mathrm{S}}$. First, if $f : \mathrm{E} \to \mathrm{E}'$ is a morphism of CM elliptic curves over S, then $(f \times_{\mathrm{S}} f)|_{\mathrm{Eq}^{\mathrm{O}_{\mathrm{K}}^{\times}}_{\mathrm{E}/\mathrm{S}}} \subset \mathrm{Eq}^{\mathrm{O}_{\mathrm{K}}^{\times}}_{\mathrm{E}'/\mathrm{S}} \subset \mathrm{E} \times_{\mathrm{S}} \mathrm{E}$ and so there is an induced morphism $\mathrm{X}_f : \mathrm{X}_{\mathrm{E}/\mathrm{S}} \to \mathrm{X}_{\mathrm{E}'/\mathrm{S}}$ and a commutative diagram

$$\begin{array}{ccc} \mathrm{E} & \xrightarrow{f} & \mathrm{E}' \\ {\scriptstyle p_{\mathrm{E}/\mathrm{S}}}\downarrow & & \downarrow{\scriptstyle p_{\mathrm{E}'/\mathrm{S}}} \\ \mathrm{X}_{\mathrm{E}/\mathrm{S}} & \xrightarrow{\mathrm{X}_f} & \mathrm{X}_{\mathrm{E}'/\mathrm{S}}. \end{array}$$

The invariance of $p_{\mathrm{E}/\mathrm{S}}$ and $p_{\mathrm{E}'/\mathrm{S}}$ under $\underline{\mathrm{O}^{\times}_{\mathrm{K}}}_{\mathrm{S}}$ shows that $f \mapsto \mathrm{X}_f$ is also invariant under $\underline{\mathrm{O}^{\times}_{\mathrm{K}}}_{\mathrm{S}}$. In symbols, the map

$$\underline{\mathrm{Hom}}^{\mathrm{O}_{\mathrm{K}}}_{\mathrm{S}}(\mathrm{E}, \mathrm{E}') \to \underline{\mathrm{Hom}}_{\mathrm{S}}(\mathrm{X}_{\mathrm{E}/\mathrm{S}}, \mathrm{X}_{\mathrm{E}'/\mathrm{S}'}) : f \mapsto \mathrm{X}_f$$

factors through the quotient sheaf

$$\underline{\mathrm{Hom}}^{\mathrm{O}_{\mathrm{K}}}_{\mathrm{S}}(\mathrm{E}, \mathrm{E}')/\underline{\mathrm{O}^{\times}_{\mathrm{K}}}_{\mathrm{S}} \to \underline{\mathrm{Hom}}_{\mathrm{S}}(\mathrm{X}_{\mathrm{E}/\mathrm{S}}, \mathrm{X}_{\mathrm{E}'/\mathrm{S}'}).$$

In particular, if E and E′ are locally isomorphic then $\underline{\mathrm{Isom}}^{\mathrm{O}_{\mathrm{K}}}_{\mathrm{S}}(\mathrm{E}, \mathrm{E}')$ is an $\underline{\mathrm{O}^{\times}_{\mathrm{K}}}_{\mathrm{S}}$-torsor so that $\underline{\mathrm{Isom}}^{\mathrm{O}_{\mathrm{K}}}_{\mathrm{S}}(\mathrm{E}, \mathrm{E}')/\underline{\mathrm{O}^{\times}_{\mathrm{K}}}_{\mathrm{S}} \xrightarrow{\sim} \mathrm{S}$ and we obtain a canonical map $\mathrm{S} \to \underline{\mathrm{Isom}}_{\mathrm{S}}(\mathrm{X}_{\mathrm{E}/\mathrm{S}}, \mathrm{X}_{\mathrm{E}'/\mathrm{S}})$ or what is the same an isomorphism

$$\mathrm{X}_{\mathrm{E}/\mathrm{S}} \xrightarrow{\sim} \mathrm{X}_{\mathrm{E}'/\mathrm{S}}.$$

4.3.8. Now let S be an M_{CM}-sheaf, i.e. $\mathrm{S} \to \mathrm{M}_{\mathrm{CM}}$. By the definition of the coarse sheaf M_{CM}, this implies that there exists a cover $(\mathrm{S}_i \to \mathrm{S})_{i \in \mathrm{I}}$ of S and CM elliptic curves $(\mathrm{E}_i/\mathrm{S}_i)_{i \in \mathrm{I}}$, such that for $i, j \in \mathrm{I}$, writing $\mathrm{S}_{ij} = \mathrm{S}_i \times_{\mathrm{S}} \mathrm{S}_j$, the CM elliptic curves $\mathrm{E}_i \times_{\mathrm{S}_i} \mathrm{S}_{ij}$ and $\mathrm{E}_j \times_{\mathrm{S}_j} \mathrm{S}_{ij}$ are locally isomorphic. Therefore, writing $\mathrm{X}_i = \mathrm{X}_{\mathrm{E}_i/\mathrm{S}_i}$ for $i \in \mathrm{I}$ we have for all $i, j \in \mathrm{I}$ canonical isomorphisms

$$\mathrm{X}_i \times_{\mathrm{S}_i} \mathrm{S}_{ij} \xrightarrow{\sim} \mathrm{X}_j \times_{\mathrm{S}_j} \mathrm{S}_{ij}. \tag{4.3.8.1}$$

The independence of these isomorphisms from the choice of isomorphism $\mathrm{E}_i \times_{\mathrm{S}_i} \mathrm{S}_{ij} \xrightarrow{\sim} \mathrm{E}_j \times_{\mathrm{S}_j} \mathrm{S}_{ij}$ (and similarly on the triple products) show that the isomorphisms (4.3.8.1) equip the family of curves $(\mathrm{X}_i/\mathrm{S}_i)_{i \in \mathrm{I}}$ with descent data relative to the cover $(\mathrm{S}_i \to \mathrm{S})_{i \in \mathrm{I}}$, which furnishes us with (a priori) a sheaf $\mathrm{X}_{\mathrm{S}} \to \mathrm{S}$. Similar observations show that the sheaf $\mathrm{X}_{\mathrm{S}} \to \mathrm{S}$ is independent (upto canonical isomorphism) of the cover $(\mathrm{S}_i \to \mathrm{S})_{i \in \mathrm{I}}$ and the CM elliptic curves $(\mathrm{E}_i/\mathrm{S}_i)_{i \in \mathrm{I}}$ and that if $\mathrm{S}' \to \mathrm{S}$ is a morphism of M_{CM}-sheaves then we have a canonical isomorphism

$$\mathrm{X}_{\mathrm{S}'} \xrightarrow{\sim} \mathrm{X}_{\mathrm{S}} \times_{\mathrm{S}} \mathrm{S}'.$$

In particular, applying this to $\mathrm{id}_{\mathrm{M}_{\mathrm{CM}}} : \mathrm{M}_{\mathrm{CM}} \to \mathrm{M}_{\mathrm{CM}}$ we obtain a sheaf $\mathrm{X} \to \mathrm{M}_{\mathrm{CM}}$ and isomorphisms

$$\mathrm{X}_{\mathrm{S}} \xrightarrow{\sim} \mathrm{X} \times_{\mathrm{M}_{\mathrm{CM}}} \mathrm{S}.$$

4.3.9. Before we consider the geometric properties of the sheaf $\mathrm{X} \to \mathrm{M_{CM}}$, let us first make the following observations.

(i) There is a unique morphism $0_{\mathrm{X}} : \mathrm{M_{CM}} \to \mathrm{X}$ with the property that if $\mathrm{E/S}$ is a CM elliptic curve and $c_{\mathrm{E/S}} : \mathrm{S} \to \mathrm{M_{CM}}$ is the coarse map then $c^*_{\mathrm{E/S}}(0_{\mathrm{X}}) = 0_{\mathrm{E}} : \mathrm{S} \to \mathrm{X}_{\mathrm{E/S}} = c^*_{\mathrm{E/S}}(\mathrm{X})$.

(ii) For each $\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}$ there is a unique morphism

$$\psi^{\mathfrak{a}}_{\mathrm{X/M_{CM}}} : \mathrm{X} \to \sigma^*_{\mathfrak{a}}(\mathrm{X})$$

such that for all CM elliptic curves $\mathrm{E/S}$, using the identifications

$$c_{\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{a}^{-1}/\mathrm{S}} = \sigma_{\mathfrak{a}} \circ c_{\mathrm{E/S}} \quad \text{and then} \quad c^*_{\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{a}^{-1}/\mathrm{S}}(\mathrm{X}) = c^*_{\mathrm{E/S}}(\sigma^*_{\mathfrak{a}}(\mathrm{X}))$$

the diagram

$$\begin{array}{ccc} \mathrm{E} & \xrightarrow{\quad i_{\mathfrak{a}} \quad} & \mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{a}^{-1} \\ \downarrow & & \downarrow \\ c^*_{\mathrm{E/S}}(\mathrm{X}) & \xrightarrow{c^*_{\mathrm{E/S}}(\psi^{\mathfrak{a}}_{\mathrm{X/M_{CM}}})} & c^*_{\mathrm{E/S}}(\sigma^*_{\mathfrak{a}}(\mathrm{X})) \end{array} \tag{4.3.9.1}$$

commutes.

(iii) The morphisms $\psi^{\mathfrak{p}}_{\mathrm{X/M_{CM}}} : \mathrm{X} \to \sigma^*_{\mathfrak{p}}(\mathrm{X})$ for $\mathfrak{p}$ prime lift the $\mathrm{N}\mathfrak{p}$-power relative Frobeniuses and for $\mathfrak{a}, \mathfrak{b}$ any two ideals we have the commutativity condition

$$\psi^{\mathfrak{ab}}_{\mathrm{X/M_{CM}}} = \sigma^*_{\mathfrak{a}}(\psi^{\mathfrak{b}}_{\mathrm{X/M_{CM}}}) \circ \psi^{\mathfrak{a}}_{\mathrm{X/M_{CM}}}$$

which equips $\mathrm{X_{E/S}}$ with the structure of a $\Psi_{\mathrm{M_{CM}}}$-sheaf.

(iv) The morphism $0_{\mathrm{X}} : \mathrm{M_{CM}} \to \mathrm{X}$ is a $\Psi_{\mathrm{M_{CM}}}$-morphism.

4.3.10 Proposition. — *The sheaf $f : \mathrm{X} \to \mathrm{M_{CM}}$ is a smooth, projective curve of genus zero. In particular, if $\mathscr{I}_{\mathrm{X}} \subset \mathscr{O}_{\mathrm{X}}$ denotes the ideal sheaf defining the closed point $0_{\mathrm{X}} : \mathrm{M_{CM}} \to \mathrm{X}$ then $\mathscr{W} := f_{\mathrm{X}*}(\mathscr{I}_{\mathrm{X}}^{-1})$ is a locally free rank two $\mathscr{O}_{\mathrm{M_{CM}}}$-module, the morphism $f^*_{\mathrm{X}}(\mathscr{W}) \to \mathscr{I}_{\mathrm{X}}^{-1}$ is an epimorphism, and the induced map $\mathrm{X} \to \mathbf{P}_{\mathrm{M_{CM}}}(\mathscr{W})$ is an isomorphism.*

Proof. — The fact that $\mathrm{X} \to \mathrm{M_{CM}}$ is a curve is immediate from the fact that $\mathrm{M_{CM}}$ admits an open cover $(\mathrm{M}_i \to \mathrm{M_{CM}})_{i\in\mathrm{I}}$ with CM elliptic curves $\mathrm{E}_i/\mathrm{M}_i$. Indeed, the defining property of $\mathrm{X} \to \mathrm{M_{CM}}$ then gives

$$\mathrm{X} \times_{\mathrm{M_{CM}}} \mathrm{M}_i \xrightarrow{\sim} \mathrm{X}_{\mathrm{E}_i/\mathrm{M}_i}$$

and we know that $\mathrm{X}_{\mathrm{E}_i/\mathrm{M}_i}$ is a smooth of relative dimension one, proper and geometrically connected.

It remains to compute the genus. The genus is constant along the fibres of a smooth, proper geometrically connected curve, and so to compute it we may do so after base change along any morphism $\mathrm{Spec}(\mathrm{K}^{\mathrm{sep}}) \to \mathrm{M}$. Fixing a CM elliptic curve $\mathrm{E/Spec}(\mathrm{K}^{\mathrm{sep}})$ and considering the degree w finite locally

free morphism $p = p_{\mathrm{E}/\mathrm{Spec}(\mathrm{K}^{\mathrm{sep}})} : \mathrm{E} \to \mathrm{X} \times_{\mathrm{M}} \mathrm{Spec}(\mathrm{K}^{\mathrm{sep}})$ the Riemann-Hurwitz formula gives:

$$2 - 2g_{\mathrm{E}} = w(2 - 2g_{\mathrm{X}}) - \sum_{x \in \mathrm{E}(\mathrm{K}^{\mathrm{sep}})} (e_x - 1)$$

where g_{E} is the genus of E, g_{X} is the genus of $\mathrm{X} \times_{\mathrm{M}_{\mathrm{CM}}} \mathrm{Spec}(\mathrm{K}^{\mathrm{sep}})$ and where e_x is the ramification degree of p at x. We have $g_{\mathrm{E}} = 1$, and for each $x \in \mathrm{E}(\mathrm{K}^{\mathrm{sep}})$ the ramification degree e_x is equal to $\#\mathrm{Stab}(x) - 1$ where $\mathrm{Stab}(x) \subset \mathrm{O}_{\mathrm{K}}^{\times}$ is the stabiliser of x. It is now just a matter computation, depending on whether $\mathrm{O}_{\mathrm{K}}^{\times} = \mu_2$, μ_4 or μ_6, to verify that the equality

$$0 = (2 - 2g_{\mathrm{E}}) = w(2 - 2g_{\mathrm{X}}) - \sum_{x \in \mathrm{E}(\mathrm{K}^{\mathrm{sep}})} (e_x - 1)$$

implies $g_{\mathrm{X}} = 0$. We do it for $\mathrm{O}_{\mathrm{K}}^{\times} = \mu_6$. The only point with stabiliser μ_6 is $0 \in \mathrm{E}(\mathrm{K}^{\mathrm{sep}})$, the points with stabiliser $\mu_2 \subset \mu_6$ are the three points of $\mathrm{E}[2] - 0$ and the points with stabiliser $\mu_3 \subset \mu_6$ are the two points of $\mathrm{E}[1 - \zeta_3] - 0$ (for $\zeta_3 \in \mu_3$ a generator). Therefore, we find

$$0 = 6 \cdot (2 - 2g_{\mathrm{X}}) - 1 \cdot (6 - 1) - 3 \cdot (2 - 1) - 2 \cdot (3 - 1) = -12g_{\mathrm{X}}$$

and hence $g_{\mathrm{X}} = 0$.

The other claims now follow using standard arguments from the theory of curves. □

4.3.11 Corollary. — *For each* $\mathfrak{a} \in \mathrm{Id}_{\mathrm{O}_{\mathrm{K}}}$ *the morphism* $\psi^{\mathfrak{a}}_{\mathrm{X}/\mathrm{M}_{\mathrm{CM}}} : \mathrm{X} \to \sigma^*_{\mathfrak{a}}(\mathrm{X})$ *is finite locally free of degree* $\mathrm{N}\mathfrak{a}$ *and together they equip* X *with the structure of a* $\Lambda_{\mathrm{M}_{\mathrm{CM}}}$*-scheme and the morphism* $0_{\mathrm{X}} : \mathrm{M}_{\mathrm{CM}} \to \mathrm{X}$ *is a* $\Lambda_{\mathrm{M}_{\mathrm{CM}}}$*-morphism.*

Proof. — As X is flat over $\mathrm{Spec}(\mathrm{O}_{\mathrm{K}})$ it follows by (3.3.12) and (iv) of (4.3.9) that X admits a $\Lambda_{\mathrm{M}_{\mathrm{CM}}}$-structure and that the morphism $0_{\mathrm{X}} : \mathrm{M}_{\mathrm{CM}} \to \mathrm{X}$ is a $\Lambda_{\mathrm{M}_{\mathrm{CM}}}$-morphism. The only thing we need to verify is that $\psi^{\mathfrak{a}}_{\mathrm{X}/\mathrm{M}_{\mathrm{CM}}}$ is finite locally free of degree $\mathrm{N}\mathfrak{a}$ but this follows from the diagram (4.3.9.1) defining $\psi^{\mathfrak{a}}_{\mathrm{X}/\mathrm{M}_{\mathrm{CM}}}$ as both columns are finite locally free of degree w and the top map is finite locally free of degree $\mathrm{N}\mathfrak{a}$ and hence the bottom map must also be finite locally free of degree $\mathrm{N}\mathfrak{a}$. □

4.3.12. Write $\mathrm{X}[\mathrm{O}_{\mathrm{K}}] \subset \mathrm{X}$ for the (image of) the morphism $0_{\mathrm{X}} : \mathrm{M}_{\mathrm{CM}} \to \mathrm{X}$, and for each $\mathfrak{a} \in \mathrm{Id}_{\mathrm{O}_{\mathrm{K}}}$ define $\mathrm{X}[\mathfrak{a}] := \psi^{\mathfrak{a}*}_{\mathrm{X}}(\mathrm{X}[\mathrm{O}_{\mathrm{K}}]) \subset \mathrm{X}$. Then $\mathrm{X}[\mathfrak{a}] \subset \mathrm{X}$ is a finite locally free $\Lambda_{\mathrm{M}_{\mathrm{CM}}}$-scheme of degree $\mathrm{N}\mathfrak{a}$.

4.3.13 Proposition. — *For each ideal* $\mathfrak{a} \in \mathrm{Id}_{\mathrm{O}_{\mathrm{K}}}$ *the extension* $\mathrm{K}(\mathrm{X}[\mathfrak{a}])$ *of* K *generated by the coordinates of* $\mathrm{X}[\mathfrak{a}]$ *is equal to ray class field* $\mathrm{K}(\mathfrak{a})$*.*

Proof. — As $\mathrm{M}_{\mathrm{CM}} \xrightarrow{\sim} \mathrm{Spec}(\mathrm{O}_{\mathrm{H}})$ it is enough to show that the action of $\mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{H})$ on $\mathrm{X}[\mathfrak{a}](\mathrm{Spec}(\mathrm{K}^{\mathrm{sep}}))$ factors faithfully through the quotient $\mathrm{G}(\mathrm{K}^{\mathrm{sep}}/\mathrm{H}) \to$

$G(K(\mathfrak{a})/K)$. To do this we may choose a CM elliptic curve $E/\mathrm{Spec}(H)$ with character $\rho_{E/H} : G(K^{\mathrm{sep}}/H) \to A_{O_K}^{\times}$ and consider the map

$$p = p_{E/\mathrm{Spec}(H)} : E \to X_{E/\mathrm{Spec}(H)} = X \times_{M_{CM}} \mathrm{Spec}(H).$$

Then p induces a surjective map of $G(K^{\mathrm{sep}}/H)$-sets

$$E[\mathfrak{a}](\mathrm{Spec}(K^{\mathrm{sep}})) \to X[\mathfrak{a}](\mathrm{Spec}(K^{\mathrm{sep}}))$$

and moreover factors through an isomorphism

$$E[\mathfrak{a}](\mathrm{Spec}(K^{\mathrm{sep}})) \to E[\mathfrak{a}](\mathrm{Spec}(K^{\mathrm{sep}}))/O_K^{\times} \xrightarrow{\sim} X[\mathfrak{a}](\mathrm{Spec}(K^{\mathrm{sep}})).$$

Therefore, an element $\sigma \in G(K^{\mathrm{sep}}/H)$ acts trivially on $X[\mathfrak{a}](\mathrm{Spec}(K^{\mathrm{sep}}))$ if and only if $\rho_{E/H,\mathfrak{a}}(\sigma) \in (O_K/\mathfrak{a})^{\times}$ is contained in the image of $O_K^{\times} \to (O_K/\mathfrak{a})^{\times}$, i.e. in the notation of (2.5.1) if and only if $[\rho_{E/H,\mathfrak{a}}(\sigma)]_{\mathfrak{a}} = 1$. But

$$[\rho_{E/H,\mathfrak{a}}(\sigma)^{-1}]_{\mathfrak{a}} = [\sigma]_{H,\mathfrak{a}} = [\sigma]_{K,\mathfrak{a}}$$

and the kernel of $[-]_{K,\mathfrak{a}}$ is precisely $G(K^{\mathrm{sep}}/K(\mathfrak{a}))$ and so we are done. □

4.3.14. We now wish to study the Lie algebra $T := \underline{\mathrm{Lie}}_{X/M_{CM}}$ at the closed point $0_{M_{CM}} : M_{CM} \to X$.

4.3.15 Proposition. — *For each $\mathfrak{a} \in \mathrm{Id}_{O_K}$ the map*

$$D_{\mathfrak{a}} : T \to \sigma_{\mathfrak{a}}^*(T)$$

induced by $\psi^{\mathfrak{a}*}_{X/M_{CM}} : X \to \sigma_{\mathfrak{a}}^*(X)$ factors as

$$T \xrightarrow{\sim} \sigma_{\mathfrak{a}}^*(T) \otimes_{O_K} \mathfrak{a}^w \to \sigma_{\mathfrak{a}}^*(T)$$

where the second map is multiplication.

Proof. — It is enough to show that for each $\mathfrak{a}$, Zariski locally on M_{CM}, the image of

$$D_{\mathfrak{a}} : T \to \sigma_{\mathfrak{a}}^*(T)$$

is equal to $\mathfrak{a}^w \otimes_{\mathscr{O}_{M_{CM}}} \sigma_{\mathfrak{a}}^*(T)$.

So let $x \in M_{CM}$ be a point and let $S = \mathrm{Spec}(\mathscr{O}_{M_{CM},x}) \to M_{CM}$ be the inclusion of the local ring at x, and let E/S be a CM elliptic curve. The inverse image of $0 : S \to X_{E/S} = X \times_{M_{CM}} S$ along the map $p_{E/S} : E \to X_{E/S}$ is equal to $[O_K^{\times}](0_E)$ and as $0 : S \to E$ is invariant under $O_K^{\times}$ we have $[O_K^{\times}](0_E) = \mathrm{Inf}_{0_E}^{w-1}(E)$ is the $(w-1)$st infinitesimal neighbourhood of $0_E : S \to E$. It follows that, writing $\widehat{X} = \mathrm{Inf}_{0_X}(X)$ that $p_{E/S}^*(\widehat{X}_S) = \mathrm{Inf}_{0_E}(E) = \widehat{E}$ and that the map

$$\widehat{E} \to \widehat{X}$$

is finite locally free of degree w and $O_K^{\times}$ invariant.

It now follows from Proposition 7.5.2 that, choosing an isomorphism $\widehat{\mathrm{E}} \xrightarrow{\sim} \widehat{\mathbf{A}}^1_{\mathrm{S}}$ there is a unique isomorphism $\widehat{\mathrm{X}}_{\mathrm{S}} \xrightarrow{\sim} \widehat{\mathbf{A}}^1_{\mathrm{S}}$ such that the diagram

$$\begin{array}{ccc} \widehat{\mathrm{E}} & \longrightarrow & \widehat{\mathrm{X}}_{\mathrm{S}} \\ \wr\downarrow & & \downarrow\wr \\ \widehat{\mathbf{A}}^1_{\mathrm{S}} & \xrightarrow{\mathrm{N}_{\mathrm{O}_{\mathrm{K}}^\times}(\mathrm{T})} & \widehat{\mathbf{A}}^1_{\mathrm{S}} \end{array}$$

commutes where the bottom map is

$$a \mapsto \mathrm{N}_{\mathrm{O}_{\mathrm{K}}^\times}(a) = \prod_{\epsilon \in \mathrm{O}_{\mathrm{K}}^\times} [\epsilon](a)$$

and $[\epsilon](\mathrm{T})$ is the power series on $\widehat{\mathbf{A}}^1_{\mathrm{S}} \xrightarrow{\sim} \widehat{\mathrm{E}}$ representing the automorphism $\epsilon : \widehat{\mathrm{E}} \to \widehat{\mathrm{E}}$. But as the action of O_{K} is strict we known that $[\epsilon](\mathrm{T}) = \epsilon \mathrm{T} + \cdots$ and so $\mathrm{N}_{\mathrm{O}_{\mathrm{K}}^\times}(\mathrm{T}) = -\mathrm{T}^w + \cdots$. From this and the fact that the induced map on Lie algebras of $\psi^{\mathfrak{p}}_{\mathrm{E/S}} : \mathrm{E} \to \sigma^*_{\mathfrak{p}}(\mathrm{E})$ factors as

$$\underline{\mathrm{Lie}}_{\mathrm{E/S}} \xrightarrow{\sim} \mathfrak{p} \otimes_{\mathscr{O}_{\mathrm{M_{CM}}}} \sigma^*_{\mathfrak{p}}(\underline{\mathrm{Lie}}_{\mathrm{E/S}}) \to \sigma^*_{\mathfrak{p}}(\underline{\mathrm{Lie}}_{\mathrm{E/S}})$$

the claim follows. □

4.3.16 Corollary. — *The rank one $\mathscr{O}_{\mathrm{M_{CM}}}$-module* T *is free and there exists an isomorphism*

$$\mathrm{X} \xrightarrow{\sim} \mathbf{P}^1_{\mathrm{M_{CM}}}.$$

Proof. — We have

$$\mathrm{X} \xrightarrow{\sim} \mathbf{P}_{\mathrm{M_{CM}}}(\mathscr{W})$$

where $\mathscr{W} = f_*(\mathscr{I}_{\mathrm{X}}^{-1})$ where $\mathscr{I}_{\mathrm{X}} \subset \mathscr{O}_{\mathrm{X}}$ is the ideal sheaf defining the closed point $0_{\mathrm{X}} : \mathrm{M_{CM}} \to \mathrm{X}$. Moreover, we have an exact sequence

$$0 \to \mathscr{O}_{\mathrm{M_{CM}}} \to \mathscr{W} \to \mathrm{T} \to 0.$$

As T is projective this exact sequence splits. Then by the same method as in the proof of (4.2.13) one shows that the isomorphisms

$$\mathrm{D}_{\mathfrak{a}} : \mathrm{T} \xrightarrow{\sim} \mathfrak{a}^w \otimes_{\mathscr{O}_{\mathrm{M_{CM}}}} \sigma^*_{\mathfrak{a}}(\mathrm{T})$$

can be turned into descent data from $\mathrm{M_{CM}}$ to $\mathrm{Spec}(\mathrm{O_K})$ and so by the Hauptidealsatz T is free. Therefore, $\mathscr{W} \xrightarrow{\sim} \mathscr{O}^2_{\mathrm{M_{CM}}}$ and

$$\mathrm{X} \xrightarrow{\sim} \mathbf{P}_{\mathrm{M_{CM}}}(\mathscr{W}) \xrightarrow{\sim} \mathbf{P}_{\mathrm{M_{CM}}}(\mathscr{O}^2_{\mathrm{M_{CM}}}) = \mathbf{P}^1_{\mathrm{M_{CM}}}.$$

□

4.3.17 Remark. — We end this section with a remark regarding possible applications to monogeneity of rings of integers. Define Cartier divisors

$$\Theta_{\mathfrak{a}} \subset \mathrm{X}[\mathfrak{a}] \subset \mathrm{X}$$

inductively by setting $\Theta_{\mathrm{O_K}} = \mathrm{X}[\mathrm{O_K}]$ and, having defined $\Theta_{\mathfrak{a}} \subset \mathrm{X}[\mathfrak{a}]$, we define $\Theta_{\mathfrak{a}\mathfrak{p}}$ to be

$$\Theta_{\mathfrak{a}\mathfrak{p}} := \psi_{\mathfrak{p}}^{*}(\sigma_{\mathfrak{a}}^{*}(\Theta_{\mathfrak{a}})) - \Theta_{\mathfrak{a}}$$

if $\mathfrak{p} \nmid \mathfrak{a}$ (an analysis of the $\Lambda_{\mathrm{M_{CM}}}$-structure on $\mathrm{X}[\mathfrak{a}]$ shows that this is possible) or to be

$$\Theta_{\mathfrak{a}\mathfrak{p}} := \psi_{\mathrm{X}/\mathrm{M_{CM}}}^{\mathfrak{p}*}(\sigma_{\mathfrak{p}}^{*}(\Theta_{\mathfrak{a}}))$$

if $\mathfrak{p}|\mathfrak{a}$. Then one can show that $\Theta_{\mathfrak{a}} \subset \mathrm{X}$ is irreducible (but in general non-reduced), that $\mathrm{K}(\Theta_{\mathfrak{a}}) = \mathrm{K}(\mathfrak{a})$ and that

$$\mathrm{X}[\mathfrak{a}] = \sum_{\mathfrak{d}|\mathfrak{a}} \Theta_{\mathfrak{a}}.$$

The identity above should be viewed as analogous to the factorisation of the polynomials $\mathrm{X}^n - 1$ in terms of cyclotomic polynomials.

Moreover, when $\mathfrak{a}$ is composite $\Theta_{\mathfrak{a}}$ and $\mathrm{X}[\mathrm{O_K}] = \Theta_{\mathrm{O_K}}$ are disjoint so that one finds a closed immersion

$$\Theta_{\mathfrak{a}} \subset \mathrm{X} - \mathrm{X}[\mathrm{O_K}] = \mathbf{P}_{\mathrm{M_{CM}}} - \mathrm{X}[\mathrm{O_K}](\mathscr{W}) \xrightarrow{\sim} \mathbf{V}_{\mathrm{M_{CM}}}(\mathrm{T}) \xrightarrow{\sim} \mathbf{A}^1_{\mathrm{M_{CM}}}.$$

With a more detailed analysis of the $\Lambda_{\mathrm{M_{CM}}}$-structure on $\mathrm{X}_{\mathrm{M_{CM}}} \xrightarrow{\sim} \mathbf{P}^1_{\mathrm{O_H}}$ it may be possible to show that the divisors $(\Theta_{\mathfrak{a}})_{\mathrm{red}}$ are regular which would imply isomorphisms

$$(\Theta_{\mathfrak{a}})_{\mathrm{red}} \xrightarrow{\sim} \mathrm{Spec}(\mathrm{O}_{\mathrm{K}(\mathfrak{a})}).$$

This would then give closed immersion

$$\mathrm{Spec}(\mathrm{O}_{\mathrm{K}(\mathfrak{a})}) \to \mathbf{A}^1_{\mathrm{O_H}} \xrightarrow{\sim} \mathbf{A}^1_{\mathrm{M_{CM}}}$$

or in other words $\mathrm{O}_{\mathrm{K}(\mathfrak{a})}$ would be monogenic over the ring of integers in the Hilbert class field $\mathrm{O_H}$. It is worth noting that this method would only apply to conductors $\mathfrak{a}$ which are composite, and that when $\mathfrak{a}$ is not composite counterexamples to the monogeneity of $\mathrm{O}_{\mathrm{K}(\mathfrak{a})}$ over $\mathrm{O_H}$ are known to exist (see [**14**]).

4.4. A Λ-equivariant cover of $\mathscr{M}_{\mathrm{CM}}$

In this section we show how one can use the existence of canonical lifts of CM elliptic curves to define a flat, affine and formally smooth cover of $\mathscr{M}_{\mathrm{CM}}$ admitting a Λ-structure compatible with that on $\mathscr{M}_{\mathrm{CM}}$. Indeed, we rigidify $\mathscr{M}_{\mathrm{CM}}$ by equipping a CM elliptic curve E/S with a trivialisation of the Lie algebra of its canonical lift. The results of (4.2) allow us to show that this does indeed define a cover of $\mathscr{M}_{\mathrm{CM}}$ with the desired properties.

4.4.1. Let S be an ind-affine scheme. The category $\mathscr{CL}_{\mathrm{O_K}}(\mathrm{S})$ acts on the category $\mathscr{M}^*_{\mathrm{CM}}(\mathrm{S})$. However, we have shown that $\mathscr{M}_{\mathrm{CM}}(\mathrm{S})$ is equivalent to the category $\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_\Lambda(\mathrm{S})$ so that $\mathscr{CL}_{\mathrm{O_K}}$ should also act on $\mathrm{W}_*(\mathscr{M}_{\mathrm{CM}})_\Lambda$ and now explain how.

As W^* commutes with étale fibre products and $\underline{\mathrm{O_K}}_{\mathrm{S}}$ is étale over S, the sheaf $\mathrm{W}^*(\underline{\mathrm{O_K}}_{\mathrm{S}})$ is naturally a $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-sheaf of rings over $\mathrm{W}^*(\mathrm{S})$. Moreover, W^* also commutes with disjoint unions which gives an identification

$$\mathrm{W}^*(\underline{\mathrm{O_K}}_{\mathrm{S}}) \xrightarrow{\sim} \underline{\mathrm{O_K}}_{\mathrm{W}^*(\mathrm{S})}$$

compatible with the ring structures. In much the same way, if $\mathscr{L}$ is a rank one $\mathrm{O_K}$-local system over S, then $\mathrm{W}^*(\mathscr{L})$ is a rank one $\mathrm{O_K}$-local system over $\mathrm{W}^*(\mathrm{S})$ equipped with a $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure which is compatible with its $\underline{\mathrm{O_K}}_{\mathrm{W}^*(\mathrm{S})} = \mathrm{W}^*(\underline{\mathrm{O_K}}_{\mathrm{S}})$-module structure, i.e. the map

$$\underline{\mathrm{O_K}}_{\mathrm{W}^*(\mathrm{S})} \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(mc\mathrm{L}) \to \mathrm{W}^*(\mathscr{L})$$

defining the action of $\underline{\mathrm{O_K}}_{\mathrm{W}^*(\mathrm{S})}$ on $\mathrm{W}^*(\mathscr{L})$ is a $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-morphism.

Now if E/S is a CM elliptic curve then, as both $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})$ and $\mathrm{W}^*(\mathscr{L})$ have $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structures compatible with their $\underline{\mathrm{O_K}}_{\mathrm{S}}$-module structures, and as the forgetful functor $\mathrm{Sh}_{\Lambda_{\mathrm{W}^*(\mathrm{S})}} \to \mathrm{Sh}_{\mathrm{W}^*(\mathrm{S})}$ commutes with all limits and colimits (3.3.8), the CM elliptic curve

$$\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \otimes_{\mathrm{O_K}} \mathrm{W}^*(\mathscr{L})$$

is also equipped with a $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure compatible with its $\underline{\mathrm{O_K}}_{\mathrm{W}^*(\mathrm{S})}$-module structure.

4.4.2 Proposition. — *The $\Lambda_{\mathrm{W}^*(\mathrm{S})}$ structure on $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})\otimes_{\mathrm{O_K}}\mathrm{W}^*(\mathscr{L})$ is canonical and there is a unique $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-isomorphism*

$$\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}) \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \otimes_{\mathrm{O_K}} \mathrm{W}^*(\mathscr{L})$$

inducing the identity on the ghost components at (1).

Proof. — The $\Psi_{\Gamma^*(\mathrm{S})}$-structure on $\mathrm{W}^*(\mathscr{L})\times_{\mathrm{W}^*(\mathrm{S})}\Gamma^*(\mathrm{S})$ is compatible with the isomorphisms

$$\mathrm{W}^*(\mathscr{L}) \times_{\mathrm{W}^*(\mathrm{S})} \Gamma^*(\mathrm{S}) \xrightarrow{\sim} \Gamma^*(\mathscr{L}) \xrightarrow{\sim} \mathscr{L} \times_{\mathrm{S}} \Gamma^*(\mathrm{S})$$

where the last fibre product is over the sum of the identity maps

$$\Gamma^*(\mathrm{S}) = \coprod_{\mathfrak{a}\in \mathrm{Id}_{\mathrm{O_K}}} \mathrm{S} \to \mathrm{S}$$

and where the $\Psi_{\Gamma^*(\mathrm{S})}$-structure on $\mathscr{L} \times_{\mathrm{S}} \Gamma^*(\mathrm{S})$ is induced by the Ψ-structure on $\Gamma^*(\mathrm{S})$. Therefore, we obtain $\Psi_{\Gamma^*(\mathrm{S})}$-isomorphisms

$$(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})\otimes_{\mathrm{O_K}}\mathrm{W}^*(\mathscr{L}))\times_{\mathrm{W}^*(\mathrm{S})}\Gamma^*(\mathrm{S}) \xrightarrow{\sim} \Gamma^*_{\mathrm{CM}}(\mathrm{E})\otimes_{\mathrm{O_K}}\Gamma^*(\mathscr{L}) \xrightarrow{\sim} \Gamma^*_{\mathrm{CM}}(\mathrm{E}\otimes_{\mathrm{O_K}}\mathscr{L})$$

which induce the identity after pull-back to the ghost component at (1). This is precisely the definition of a canonical $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-structure and this proves the

first statement. As the ghost components at (1) of $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \otimes_{\mathrm{O_K}} \mathrm{W}^*(\mathscr{L})$ and $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L})$ are equal to $\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}$ we get a unique $\Lambda_{\mathrm{W}^*(\mathrm{S})}$-isomorphism

$$\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \otimes_{\mathrm{O_K}} \mathrm{W}^*(\mathscr{L}) \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L})$$

inducing the identity after pull-back along the ghost component at (1). □

4.4.3 Remark. — Consider the sheaf

$$\mathrm{W}_*(\mathbf{A}^1) = \mathrm{W}_*(\mathrm{Spec}(\mathrm{O_K}[\mathrm{T}])) = \mathrm{Spec}(\Lambda \odot \mathrm{O_K}[\mathrm{T}]) = \mathrm{Spec}(\Lambda)$$

of arithmetic jets of $\mathbf{A}^1$ over $\mathrm{Spec}(\mathrm{O_K})$. It is a ring scheme over $\mathrm{Spec}(\mathrm{O_K})$ and its sections over an affine scheme $\mathrm{S} = \mathrm{Spec}(\mathrm{A})$ are given by

$$\mathrm{W}_*(\mathbf{A}^1)(\mathrm{Spec}(\mathrm{A})) = \mathrm{W}(\mathrm{A}).$$

The structure map

$$\mathrm{O_K} \to \mathrm{W}(\mathrm{A}) = \mathrm{W}_*(\mathbf{A}^1)(\mathrm{S})$$

for varying affine schemes $\mathrm{S} = \mathrm{Spec}(\mathrm{A})$ is injective (3.2.16) and induces a *monomorphism* of sheaves of rings

$$i_{\mathrm{W}} : \underline{\mathrm{O_K}} \to \mathrm{W}_*(\mathbf{A}^1). \tag{4.4.3.1}$$

This fact will be crucial for what follows.

4.4.4. Let $\mathscr{L}/\mathrm{S}$ be a rank one $\mathrm{O_K}$-local system. A level-W structure on $\mathscr{L}$ is an isomorphism of $\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}$-modules

$$\lambda : \mathrm{W}^*(\mathscr{L}) \otimes_{\underline{\mathrm{O_K}}_{\mathrm{W}^*(\mathrm{S})}} \mathscr{O}_{\mathrm{W}^*(\mathrm{S})} \xrightarrow{\sim} \mathscr{O}_{\mathrm{W}^*(\mathrm{S})}.$$

A W-isomorphism $(\mathscr{L}/\mathrm{S}, \lambda) \xrightarrow{\sim} (\mathscr{L}'/\mathrm{S}, \lambda')$ of rank one $\mathrm{O_K}$-local systems with level-W structure is an $\underline{\mathrm{O_K}}_{\mathrm{S}}$-isomorphism $h : \mathscr{L} \xrightarrow{\sim} \mathscr{L}'$ such that

$$\lambda = \lambda' \circ \mathrm{W}^*(h).$$

The tensor product of two rank one $\mathrm{O_K}$-local systems with level-W structure $(\mathscr{L}, \lambda)$ and $(\mathscr{L}', \lambda')$ is defined to be

$$(\mathscr{L} \otimes_{\mathrm{O_K}} \mathscr{L}', \lambda \otimes_{\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}} \lambda')$$

where we view $\lambda \otimes_{\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}} \lambda'$ as a level-W structure on $\mathscr{L} \otimes_{\mathrm{O_K}} \mathscr{L}'$ using the identification

$$\mathrm{W}^*(\mathscr{L} \otimes_{\mathrm{O_K}} \mathscr{L}') \xrightarrow{\sim} \mathrm{W}^*(\mathscr{L}) \otimes_{\mathrm{O_K}} \mathrm{W}^*(\mathscr{L}').$$

We write $\mathscr{C}\mathscr{L}^{\mathrm{W}}_{\mathrm{O_K}}$ for the fibred category over $\mathrm{IndAff}_{\mathrm{O_K}}$ with fibre over S given by the category rank one $\mathrm{O_K}$-local systems over S equipped with a level-W structure $(\mathscr{L}/\mathrm{S}, \lambda)$ together with their W-isomorphisms.

4.4.5 Proposition. — *$\mathscr{C}\mathscr{L}^{\mathrm{W}}_{\mathrm{O_K}}$ is a stack over* $\mathrm{IndAff}_{\mathrm{O_K}}$ *for the étale topology and is equivalent to its coarse sheaf for the étale topology.*

Proof. — That $\mathscr{C}\mathscr{L}^{\mathrm{W}}_{\mathrm{O_K}}$ is a stack for the affine étale topology on $\mathrm{IndAff}_{\mathrm{O_K}}$ is easy to see using the fact that if $\mathscr{L}/\mathrm{S}$ is a rank one $\mathrm{O_K}$-local system and $\mathrm{S}' \to \mathrm{S}$ is any morphism then

$$\mathrm{W}^*(\mathscr{L}) \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{S}') \xrightarrow{\sim} \mathrm{W}^*(\mathscr{L} \times_{\mathrm{S}} \mathrm{S}')$$

and that for any étale morphism $\mathrm{T} \to \mathrm{S}$ we have

$$\mathrm{W}^*(\mathrm{S}' \times_{\mathrm{S}} \mathrm{T}) \xrightarrow{\sim} \mathrm{W}^*(\mathrm{S}') \times_{\mathrm{W}^*(\mathrm{S})} \mathrm{W}^*(\mathrm{T}).$$

For the second statement it is enough to show that if $(\mathscr{L}, \lambda)$ is a rank one $\mathrm{O_K}$-local system with level-W structure then every W-automorphism of $\mathscr{L}$ is trivial. But if $\epsilon \in \underline{\mathrm{O}^\times_{\mathrm{K}}}_{\mathrm{S}}(\mathrm{S})$ defines a W-automorphism of $\mathscr{L}$, we have an equality

$$\mathrm{id}_{\mathrm{W}^*(\mathscr{L})} \otimes_{\underline{\mathrm{O_K}}_{\mathrm{W}^*(\mathrm{S})}} i_{\mathrm{W}}(\epsilon) = \mathrm{W}^*(\epsilon) \otimes_{\underline{\mathrm{O_K}}_{\mathrm{W}^*(\mathrm{S})}} \mathrm{id}_{\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}} \tag{4.4.5.1}$$

of automorphisms of $\mathrm{W}^*(\mathscr{L}) \otimes_{\underline{\mathrm{O_K}}_{\mathrm{W}^*(\mathrm{S})}} \mathscr{O}_{\mathrm{W}^*(\mathrm{S})}$. As i_{W} is a monomorphism and the ρ is invariant under the automorphism (4.4.5.1) we must have $\epsilon = 1$. □

4.4.6. We write $\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}$ for the coarse sheaf of $\mathscr{C}\mathscr{L}^{\mathrm{W}}_{\mathrm{O_K}}$ with which we identify it by (4.4.5). The tensor product of rank one $\mathrm{O_K}$-local systems with level-W structure equips $\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}$ with the structure of a sheaf of groups over $\mathrm{Spec}(\mathrm{O_K})$.

We now describe a short exact sequence relating $\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}$ to the $\mathrm{Spec}(\mathrm{O_K})$-group scheme of arithmetic jets $\mathrm{W}_*(\mathbf{G}_{\mathrm{m}})$ of $\mathbf{G}_{\mathrm{m}}$.

Let $\mathrm{S} = \mathrm{Spec}(\mathrm{A})$ be an affine $\mathrm{Spec}(\mathrm{O_K})$-scheme. The sections of $\mathrm{W}_*(\mathbf{G}_{\mathrm{m}})$ over S are given by

$$\mathrm{W}_*(\mathbf{G}_{\mathrm{m}})(\mathrm{Spec}(\mathrm{A})) = \mathrm{W}(\mathrm{A})^\times$$

and the monomorphism (4.4.3.1) restricts to a monomorphism again denoted

$$i_{\mathrm{W}} : \underline{\mathrm{O}^\times_{\mathrm{K}}} \to \mathrm{W}_*(\mathbf{G}_{\mathrm{m}}).$$

For each

$$a \in \mathbf{G}_{\mathrm{m}}(\mathrm{W}^*(\mathrm{S})) = \mathrm{Aut}_{\mathrm{W}^*(\mathrm{S})}(\mathscr{O}_{\mathrm{W}^*(\mathrm{S})})$$

we define an element $[a]_{\mathrm{W}} \in \mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}(\mathrm{S})$ by $[a]_{\mathrm{W}} := (\underline{\mathrm{O_K}}_{\mathrm{S}}, a)$ where we view a as the level-W structure on $\underline{\mathrm{O_K}}_{\mathrm{S}}$:

$$\underline{\mathrm{O_K}}_{\mathrm{W}^*(\mathrm{S})} \otimes_{\underline{\mathrm{O_K}}_{\mathrm{W}^*(\mathrm{S})}} \mathscr{O}_{\mathrm{W}^*(\mathrm{S})} = \mathscr{O}_{\mathrm{W}^*(\mathrm{S})} \xrightarrow{a} \mathscr{O}_{\mathrm{W}^*(\mathrm{S})}.$$

This defines a homomorphism

$$[-]_{\mathrm{W}} : \mathrm{W}_*(\mathbf{G}_{\mathrm{m}}) \to \mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}$$

Finally, composing the forgetful map

$$\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}} \to \mathscr{C}\mathscr{L}_{\mathrm{O_K}} : (\mathscr{L}/\mathrm{S}, \lambda) \mapsto \mathscr{L}/\mathrm{S}$$

with the map $\mathscr{C}\mathscr{L}_{\mathrm{O_K}} \to \underline{\mathrm{CL}_{\mathrm{O_K}}}$ of (1.5.4) we obtain a homomorphism

$$f_{\mathrm{W}} : \mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}} \to \underline{\mathrm{CL}_{\mathrm{O_K}}}.$$

4.4.7 Proposition. — *The sequence of sheaves*

$$0 \to \underline{\mathrm{O}_\mathrm{K}^\times} \xrightarrow{i_\mathrm{W}} \mathrm{W}_*(\mathbf{G}_\mathrm{m}) \xrightarrow{[-]_\mathrm{W}} \mathrm{CL}^\mathrm{W}_{\mathrm{O}_\mathrm{K}} \xrightarrow{f_\mathrm{W}} \underline{\mathrm{CL}_{\mathrm{O}_\mathrm{K}}} \to 0$$

is exact for the étale topology and $\mathrm{CL}^\mathrm{W}_{\mathrm{O}_\mathrm{K}}$ *is representable by a flat, affine formally smooth group scheme over* $\mathrm{Spec}(\mathrm{O}_\mathrm{K})$.

Proof. — We first show that $f_\mathrm{W} : \mathrm{CL}^\mathrm{W}_{\mathrm{O}_\mathrm{K}} \to \underline{\mathrm{CL}_{\mathrm{O}_\mathrm{K}}}$ is an epimorphism for the étale topology. This is equivalent to showing that for each ideal $\mathfrak{a}$ (or at least one in each ideal class of $\mathrm{CL}_{\mathrm{O}_\mathrm{K}}$) there is an étale cover $\mathrm{S} \to \mathrm{Spec}(\mathrm{O}_\mathrm{K})$ with the property that the O_K-local system $\underline{\mathfrak{a}}_\mathrm{S}$ admits a level-W structure.

Let $\mathrm{S} = \mathrm{Spec}(\mathrm{O}_\mathrm{H}) \to \mathrm{Spec}(\mathrm{O}_\mathrm{K})$. Then we have an isomorphism of $\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}$-modules

$$\underline{\mathfrak{a}}_{\mathrm{W}^*(\mathrm{S})} \otimes_{\mathrm{O}_\mathrm{K}} \mathscr{O}_{\mathrm{W}^*(\mathrm{S})} \xrightarrow{\sim} \mathfrak{a} \cdot \mathscr{O}_{\mathrm{W}^*(\mathrm{S})}$$

where $\mathfrak{a}\cdot\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}$ is the ideal sheaf defining the closed immersion $\mathrm{W}^*(\mathrm{S}) \times_{\mathrm{Spec}(\mathrm{O}_\mathrm{K})} \mathrm{Spec}(\mathrm{O}_\mathrm{K}/\mathfrak{a}) \to \mathrm{W}^*(\mathrm{S})$. However, this map is obtained by pulling-back the map $\mathrm{S} \times_{\mathrm{Spec}(\mathrm{O}_\mathrm{K})} \mathrm{Spec}(\mathrm{O}_\mathrm{K}/\mathfrak{a}) \to \mathrm{S}$ along the morphism $\mu_\mathrm{S} : \mathrm{W}^*(\mathrm{S}) \to \mathrm{S}$ defining the Λ-structure on $\mathrm{S} = \mathrm{Spec}(\mathrm{O}_\mathrm{H})$. Therefore, it is enough to show that the ideal sheaf defining the closed immersion $\mathrm{S} \times_{\mathrm{Spec}(\mathrm{O}_\mathrm{K})} \mathrm{Spec}(\mathrm{O}_\mathrm{K}/\mathfrak{a}) \to \mathrm{S}$ is free, but this sheaf is $\mathfrak{a} \otimes_{\mathrm{O}_\mathrm{K}} \mathrm{O}_\mathrm{H}$ which is free by the Hauptidealsatz (4.2.11).

We now show that the map $[-]_\mathrm{W} : \mathrm{W}_*(\mathbf{G}_\mathrm{m}) \to \mathrm{CL}^\mathrm{W}_{\mathrm{O}_\mathrm{K}}$ defines an epimorphism onto the kernel of f_W. It is clear that $[-]_\mathrm{W}$ maps to $\ker(f_\mathrm{W})$ as the rank one O_K-local system underling $[-]_\mathrm{W}$ is the trivial one. Now let S be an affine scheme and let $(\mathscr{L}/\mathrm{S}, \lambda) \in \ker(f_\mathrm{W})$. We will show that there exists a cover $(\mathrm{S}_i \to \mathrm{S})_{i\in\mathrm{I}}$ and elements $a_i \in \mathrm{W}_*(\mathbf{G}_\mathrm{m})(\mathrm{S}_i)$ with $[a_i] = (\mathscr{L}_{\mathrm{S}_i}, \lambda_{\mathrm{S}_i})$.

Since $(\mathscr{L}, \lambda) \in \ker(f_\mathrm{W})$ it follows that $\mathscr{L}$ is étale locally isomorphic $\underline{\mathrm{O}_{\mathrm{K}\mathrm{S}}}$. Therefore, we may assume that $(\mathscr{L}, \lambda) = (\underline{\mathrm{O}_{\mathrm{K}\mathrm{S}}}, \lambda)$ but then the isomorphism

$$\lambda : \underline{\mathrm{O}_{\mathrm{K}\mathrm{S}}} \otimes_{\underline{\mathrm{O}_{\mathrm{K}\mathrm{S}}}} \mathscr{O}_{\mathrm{W}^*(\mathrm{S})} = \mathscr{O}_{\mathrm{W}^*(\mathrm{S})} \xrightarrow{\sim} \mathscr{O}_{\mathrm{W}^*(\mathrm{S})}$$

is given by some $a \in \mathrm{W}_*(\mathbf{G}_\mathrm{m})(\mathrm{S}) = \mathrm{Aut}_{\mathrm{W}^*(\mathrm{S})}(\mathscr{O}_{\mathrm{W}^*(\mathrm{S})})$ and we have

$$(\underline{\mathrm{O}_{\mathrm{K}\mathrm{S}}}, \lambda) = (\underline{\mathrm{O}_{\mathrm{K}\mathrm{S}}}, a) = [a]_\mathrm{W}.$$

Finally, we compute the kernel of $[-]_\mathrm{W}$. So let $a \in \mathrm{W}_*(\mathbf{G}_\mathrm{m})(\mathrm{S})$ and assume that $[a]_\mathrm{W} = (\underline{\mathrm{O}_{\mathrm{K}\mathrm{S}}}, a) = (\underline{\mathrm{O}_{\mathrm{K}\mathrm{S}}}, \mathrm{id}_{\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}})$. By definition, this implies the existence of an isomorphism

$$\epsilon \in \mathrm{Isom}^{\mathrm{O}_\mathrm{K}}_\mathrm{S}(\underline{\mathrm{O}_{\mathrm{K}\mathrm{S}}}, \underline{\mathrm{O}_{\mathrm{K}\mathrm{S}}}) = \underline{\mathrm{O}^\times_{\mathrm{K}\mathrm{S}}}(\mathrm{S})$$

such that $\mathrm{W}^*(\epsilon) = a$. But $\mathrm{W}^*(\epsilon)$ viewed as an element of

$$\underline{\mathrm{Aut}}_{\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}}(\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}) = \mathrm{W}_*(\mathbf{G}_\mathrm{m})(\mathrm{S}),$$

is precisely $i_\mathrm{W}(\epsilon)$. Therefore $a = i_\mathrm{W}(\epsilon)$ and $\ker([-]_\mathrm{W}) = \underline{\mathrm{O}_\mathrm{K}}^\times \subset \mathrm{W}_*(\mathbf{G}_\mathrm{m})$.

It follows from the above that the kernel of f_W is equal to the sheaf of groups

$$\mathrm{W}_*(\mathbf{G}_\mathrm{m})/\underline{\mathrm{O}^\times_\mathrm{K}}.$$

However, $\underline{\mathrm{O}_{\mathrm{K}}^{\times}}$ is finite étale and $\mathrm{W}_*(\mathbf{G}_{\mathrm{m}})$ is flat and affine and so it follows that the quotient sheaf

$$\mathrm{W}_*(\mathbf{G}_{\mathrm{m}})/\underline{\mathrm{O}_{\mathrm{K}}^{\times}}$$

is also flat and affine. As $\underline{\mathrm{CL}_{\mathrm{O_K}}}$ is affine, f_{W} is an epimorphism and

$$\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}} \times_{\underline{\mathrm{CL}_{\mathrm{O_K}}}} \mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}} \xrightarrow{\sim} \mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}} \times \mathrm{W}_*(\mathbf{G}_{\mathrm{m}})/\underline{\mathrm{O}_{\mathrm{K}}^{\times}}$$

is affine and flat it follows that $\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}$ is affine and flat over $\mathrm{Spec}(\mathrm{O_K})$. Similarly, as $\mathrm{W}_*(\mathbf{G}_{\mathrm{m}})$ is formally smooth (being an inverse limit of smooth affine schemes) and $\mathrm{W}_*(\mathbf{G}_{\mathrm{m}}) \to \mathrm{W}_*(\mathbf{G}_{\mathrm{m}})/\underline{\mathrm{O_K}^{\times}}$ is étale it follows that $\mathrm{W}_*(\mathbf{G}_{\mathrm{m}})/\underline{\mathrm{O_K}^{\times}}$ is formally smooth and by descent that $\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}$ is formally smooth. □

4.4.8. Let S be an affine scheme and let E/S be a CM elliptic curve. A level-W structure on E/S is an isomorphism of $\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}$-modules

$$\rho : \underline{\mathrm{Lie}}_{\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})/\mathrm{W}^*(\mathrm{S})} \xrightarrow{\sim} \mathscr{O}_{\mathrm{W}^*(\mathrm{S})}.$$

A W-isomorphism $(\mathrm{E}/\mathrm{S}, \rho) \xrightarrow{\sim} (\mathrm{E}'/\mathrm{S}, \rho')$ of CM elliptic curves with level-W structures is an isomorphism $f : \mathrm{E} \xrightarrow{\sim} \mathrm{E}'$ of CM elliptic curves such that

$$\rho = \rho' \circ \underline{\mathrm{Lie}}_{\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}')/\mathrm{W}^*(\mathrm{S})}(\mathrm{W}^*_{\mathrm{CM}}(f)).$$

We denote by $\mathscr{M}^{\mathrm{W}}_{\mathrm{CM}}$ the fibred category over $\mathrm{IndAff}_{\mathrm{O_K}}$ whose fibre over an ind-affine scheme S is given by the category of CM elliptic curves with level-W structures together with their W-isomorphisms.

Just as with $\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}$, the objects of $\mathscr{M}^{\mathrm{W}}_{\mathrm{CM}}$ admit no non-trivial automorphisms and so the stack $\mathscr{M}^{\mathrm{W}}_{\mathrm{CM}}$ is equivalent to its coarse sheaf which we denote by $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}$.

There is an action of $\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}$ on $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}$ given by

$$\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}} \times \mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}} \to \mathrm{M}^{\mathrm{W}}_{\mathrm{CM}} : ((\mathscr{L}/\mathrm{S}, \lambda), (\mathrm{E}/\mathrm{S}, \rho)) \mapsto (\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}, \rho \otimes_{\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}} \lambda)$$

where we use the identification (4.4.2)

$$\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}) \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \otimes_{\mathrm{O_K}} \mathrm{W}^*(\mathscr{L}).$$

4.4.9 Theorem. — *We have the following:*

(i) *The forgetful map*

$$\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}} \to \mathscr{M}_{\mathrm{CM}}$$

is affine, faithfully flat and formally smooth.

(ii) $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}$ *is an* $\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}$*-torsor over* $\mathrm{Spec}(\mathrm{O_K})$ *and is therefore flat, affine and formally smooth over* $\mathrm{Spec}(\mathrm{O_K})$.

(iii) *The map*

$$\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}} \times_{\mathrm{Spec}(\mathrm{O_K})} \mathrm{W}_*(\mathbf{G}_{\mathrm{m}}) \to \mathrm{M}^{\mathrm{W}}_{\mathrm{CM}} \times_{\mathscr{M}_{\mathrm{CM}}} \mathrm{M}^{\mathrm{W}}_{\mathrm{CM}} : ((\mathrm{E}/\mathrm{S}, \rho), a) \mapsto ((\mathrm{E}/\mathrm{S}, \rho), (\mathrm{E}/\mathrm{S}, a\rho))$$

is an isomorphism.

Proof. — (i) Let E/S be CM elliptic curve and write

$$\mathrm{T} = \underline{\mathrm{Lie}}_{\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})/\mathrm{W}^*(\mathrm{S})}.$$

Then the fibre of the map $\mathscr{M}^{\mathrm{W}}_{\mathrm{CM}} \to \mathscr{M}_{\mathrm{CM}}$ along $\mathrm{S} \xrightarrow{\mathrm{E}} \mathscr{M}_{\mathrm{CM}}$ is given by

$$t_{\mathrm{E/S}} : \mathrm{W}_*(\underline{\mathrm{Isom}}_{\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}}(\mathrm{T}, \mathscr{O}_{\mathrm{W}^*(\mathrm{S})})) \times_{\mathrm{W}_*(\mathrm{W}^*(\mathrm{S}))} \mathrm{S} \to \mathrm{S}$$

and so to the prove the claim we need only show that $t_{\mathrm{E/S}}$ is affine, faithfully flat and formally smooth.

We now show that $t_{\mathrm{E/S}}$ is affine, faithfully flat and formally smooth whenever E/S admits a level-W structure. Indeed, if $(\mathrm{E/S}, \rho)$ is a level-W structure on E/S then we obtain an isomorphism

$$\mathbf{G}_{\mathrm{m}} \times \mathrm{W}^*(\mathrm{S}) \xrightarrow{\sim} \underline{\mathrm{Isom}}_{\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}}(\mathrm{T}, \mathscr{O}_{\mathrm{W}^*(\mathrm{S})}) : a \mapsto a \cdot \rho$$

and so an isomorphism

$$\mathrm{W}_*(\mathbf{G}_{\mathrm{m}} \times \mathrm{W}^*(\mathrm{S})) \times_{\mathrm{W}_*(\mathrm{W}^*(\mathrm{S}))} \mathrm{S} \xrightarrow{\sim} \mathrm{W}_*(\underline{\mathrm{Isom}}_{\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}}(\mathrm{T}, \mathscr{O}_{\mathrm{W}^*(\mathrm{S})})) \times_{\mathrm{W}_*(\mathrm{W}^*(\mathrm{S}))} \mathrm{S}.$$

But

$$\mathrm{W}_*(\mathbf{G}_{\mathrm{m}} \times \mathrm{W}^*(\mathrm{S})) \times_{\mathrm{W}_*(\mathrm{W}^*(\mathrm{S}))} \mathrm{S} = \mathrm{W}_*(\mathbf{G}_{\mathrm{m}}) \times \mathrm{S} \to \mathrm{S}$$

is faithfully flat, affine and formally smooth as

$$\mathrm{W}_*(\mathbf{G}_{\mathrm{m}}) = \lim_{\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}} \mathrm{W}_{\mathfrak{a}*}(\mathbf{G}_{\mathrm{m}})$$

is an inverse limit of faithfully flat, affine and smooth $\mathrm{Spec}(\mathrm{O_K})$-schemes.

As the morphism $t_{\mathrm{E/S}}$ is compatible with base change in order to finish the proof of our claim, we may localise S and in particular assume that E admits a level-$\mathfrak{f}$ structure for some $\mathfrak{f}$ which separates units. We may now assume that $\mathrm{S} = \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ and that $\mathrm{E} = \mathrm{E}^{(\mathfrak{f})}$ and, by the previous arguments, to show that $t_{\mathrm{E}^{(\mathfrak{f})}/\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}}$ is faithfully flat, affine and formally smooth it is enough to show that $\mathrm{E}^{(\mathfrak{f})}/\mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$ admits a level-W structure. To ease notation, let us write $\mathrm{M} = \mathrm{M}^{(\mathfrak{f})}_{\mathrm{CM}}$, $\mathrm{E} = \mathrm{E}^{(\mathfrak{f})}$, $\mathrm{P} = \mathrm{Id}^{(\mathfrak{f})}_{\mathrm{O_K}}$ and $\mathrm{P}' \subset \mathrm{Id}_{\mathrm{O_K}}$ for the sub-monoid generated by the prime divisors of $\mathfrak{f}$ (so that $\mathrm{P} \cap \mathrm{P}' = \{\mathrm{O_K}\}$ and $\mathrm{P} \cdot \mathrm{P}' = \mathrm{Id}_{\mathrm{O_K}}$).

Then $\mathrm{W}^*(\mathrm{M}) = \mathrm{W}^*_{\mathrm{P}}(\mathrm{W}^*_{\mathrm{P}'}(\mathrm{M}))$ and as $\mathfrak{f}$ is invertible on M we have $\Gamma^*_{\mathrm{P}'}(\mathrm{M}) = \mathrm{W}^*_{\mathrm{P}'}(\mathrm{M})$ so that

$$\mathrm{W}^*(\mathrm{M}) = \coprod_{\mathfrak{a} \in \mathrm{P}'} \mathrm{W}^*_{\mathrm{P}}(\mathrm{M}).$$

Using this and the fact that the $\Lambda_{\mathrm{P,M}}$-structure on E is canonical (4.1.20) we find

$$\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \xrightarrow{\sim} \coprod_{\mathfrak{a} \in \mathrm{P}'} \mu^*_{\mathrm{M}}(\mathrm{E}) \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} = \coprod_{\mathfrak{a}} \mu^*_{\mathrm{M}}(\mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1})$$

where

$$\mu_{\mathrm{M}} : \mathrm{W}^*_{\mathrm{P}}(\mathrm{M}) \to \mathrm{M}$$

defines the (unique) Λ_{P}-structure on M.

Now to show that E/M admits level-W structure it is enough to show that

$$\underline{\mathrm{Lie}}_{\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{a}^{-1}/\mathrm{M}} = \underline{\mathrm{Lie}}_{\mathrm{E/M}} \otimes_{\mathrm{O_K}} \mathfrak{a}^{-1} = \underline{\mathrm{Lie}}_{\mathrm{E/M}}$$

(the last equality is because $\mathfrak{a} \in \mathrm{P}'$ is invertible on M) is free for each $\mathfrak{a} \in \mathrm{P}'$ but this is (4.2.13).

(ii) Let $(\mathrm{E/S}, \rho)$ and $(\mathrm{E}'/\mathrm{S}, \rho')$ be a pair of CM elliptic curves with level-W structures. Then $\mathrm{E}' \xrightarrow{\sim} \mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}$ for some $\mathscr{L} \in \mathscr{C}\mathscr{L}_{\mathrm{O_K}}(\mathrm{S})$ and therefore

$$\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \otimes_{\mathrm{O_K}} \mathrm{W}^*(\mathscr{L}) \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}) = \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}').$$

We then have

$$\begin{aligned} \underline{\mathrm{Lie}}_{\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}')/\mathrm{W}^*(\mathrm{S})} &= \underline{\mathrm{Lie}}_{\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}\otimes_{\mathrm{O_K}}\mathscr{L})/\mathrm{W}^*(\mathrm{S})} \\ &= \underline{\mathrm{Lie}}_{\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})\otimes_{\mathrm{O_K}}\mathrm{W}^*(\mathscr{L})/\mathrm{W}^*(\mathrm{S})} \\ &= \underline{\mathrm{Lie}}_{\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})/\mathrm{W}^*(\mathrm{S})} \otimes_{\mathrm{O_K}} \mathrm{W}^*(\mathscr{L}) \end{aligned}$$

so that the isomorphism

$$\rho' : \underline{\mathrm{Lie}}_{\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}')/\mathrm{W}^*(\mathrm{S})} = \underline{\mathrm{Lie}}_{\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})/\mathrm{W}^*(\mathrm{S})} \otimes_{\mathrm{O_K}} \mathrm{W}^*(\mathscr{L}) \xrightarrow{\sim} \mathscr{O}_{\mathrm{W}^*(\mathrm{S})}$$

must be of the form $\rho \otimes_{\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}} \lambda$ where $\lambda : \mathrm{W}^*(\mathscr{L}) \otimes_{\mathrm{O_K}} \mathscr{O}_{\mathrm{W}^*(\mathrm{S})} \to \mathscr{O}_{\mathrm{W}^*(\mathrm{S})}$ is a level-W structure on $\mathscr{L}$. Therefore

$$(\mathrm{E}'/\mathrm{S}, \rho') = (\mathscr{L}/\mathrm{S}, \lambda) \cdot (\mathrm{E/S}, \rho) = (\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}, \rho \otimes_{\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}} \lambda)$$

and the action of $\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}$ on $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}$ is transitive.

Let us now see that it is free which is equivalent to the claim that if $(\mathrm{E/S}, \rho)$ and $(\mathscr{L}/\mathrm{S}, \lambda)$ are a CM elliptic curve and rank one $\mathrm{O_K}$-local system with level-W structure then there exists an W-isomorphism

$$f : (\mathrm{E/S}, \rho) \xrightarrow{\sim} (\mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}, \rho \otimes \lambda)$$

only if there exists a W-isomorphism $(\underline{\mathrm{O_K}}_{\mathrm{S}}, 1) \xrightarrow{\sim} (\mathscr{L}, \lambda)$.

So let f be such an isomorphism. Then $f : \mathrm{E} \xrightarrow{\sim} \mathrm{E} \otimes_{\mathrm{O_K}} \mathscr{L}$ is of the form $\mathrm{id}_{\mathrm{E}} \otimes_{\mathrm{O_K}} h$ for a unique isomorphism $h : \underline{\mathrm{O_K}}_{\mathrm{S}} \xrightarrow{\sim} \mathscr{L}$ (2.4.4) and as f is compatible with the level-W structures ρ and $\lambda \otimes \rho$, the isomorphism h defines a W-isomorphism

$$(\underline{\mathrm{O_K}}_{\mathrm{S}}, \mathrm{id}_{\mathscr{O}_{\mathrm{W}^*(\mathrm{S})}}) \xrightarrow{\sim} (\mathscr{L}, \lambda)$$

and our claim follows.

Therefore, the action of $\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}}$ on $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}$ is free and transitive so that to show $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}$ is a torsor it is enough to show that the structure map $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}} \to \mathrm{Spec}(\mathrm{O_K})$ is an epimorphism, but this follows from the work done in (ii) showing that any CM elliptic curve E/S étale locally admits a level-W structure.

(iii) It is clear that any pair of level-W structures on a CM elliptic curve E/S differ by scaling by an element of $\mathrm{W}_*(\mathbf{G}_{\mathrm{m}})(\mathrm{S})$ which is the claim. □

4.4.10. We now equip $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}$ with a Λ-structure. As $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}$ is flat and affine to give $\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}$ a Λ-structure it is enough to define a commuting family of Frobenius lifts $\psi^{\mathfrak{p}}_{\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}}$ for each prime ideal $\mathfrak{p}$. We now set $\psi^{\mathfrak{p}}_{\mathrm{M}^{\mathrm{W}}_{\mathrm{CM}}}$ to be the map defined on S-sections

$$(\mathrm{E}/\mathrm{S}, \rho) \mapsto (\mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1}/\mathrm{S}, \psi^{\mathfrak{p}*}(\rho))$$

where $\psi^{\mathfrak{p}*}(\rho)$ can be viewed as a level-W structure on $\mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1}$ via the identifications

$$\psi^{\mathfrak{p}*}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})) \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}) \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1} \xrightarrow{\sim} \mathrm{W}^*_{\mathrm{CM}}(\mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{p}^{-1}).$$

It is clear that these maps commute and that they lift the $\mathrm{N}\mathfrak{p}$-power Frobenius endomorphisms modulo $\mathfrak{p}$. Finally, this equips the stack $\mathscr{M}_{\mathrm{CM}}$ with a flat affine presentation

$$\mathrm{CL}^{\mathrm{W}}_{\mathrm{O_K}} \times \mathrm{M}^{\mathrm{W}}_{\mathrm{CM}} \rightrightarrows \mathrm{M}^{\mathrm{W}}_{\mathrm{CM}} \longrightarrow \mathscr{M}_{\mathrm{CM}}$$

and where the two parallel arrows are morphisms of Λ-schemes, again expressing the 'fact' that $\mathscr{M}_{\mathrm{CM}}$ is a Λ-stack.

4.5. Perfect Λ-schemes and Tate modules

In this final section we exhibit a rather interesting relationship the Tate module of a canonical CM elliptic curve over an Λ-ind-affine-scheme and a certain deformation of it to the perfection of S, which is the universal Λ-ind-affine-scheme under S on which the Frobenius lifts are isomorphisms. We then show that the canonical lift E/S can be deformed to a canonical CM elliptic curve $\mathrm{E}_{\mathrm{per}}/\mathrm{S}^{\mathrm{per}}$. We end the section by making some remarks about the relationship of this exact sequence with periods, both p-adic and analytic.

4.5.1. We first define the Tate module of an arbitrary CM elliptic curve. So let S be an ind-affine scheme E/S a CM elliptic curve. The Tate module of E/S is defined to be the pro-finite locally free S-group scheme

$$\mathrm{T}(\mathrm{E}) := \lim_{\mathfrak{a}} \mathrm{E}[\mathfrak{a}] \otimes_{\mathrm{O_K}} \mathfrak{a}$$

where the transition maps are induced multiplication

$$\mathrm{E}[\mathfrak{a}\mathfrak{b}] \otimes_{\mathrm{O_K}} \mathfrak{a}\mathfrak{b} \to \mathrm{E}[\mathfrak{a}] \otimes_{\mathrm{O_K}} \mathfrak{a}.$$

We also define the universal cover of E/S to be the sheaf

$$\widetilde{\mathrm{E}} := \lim_{\mathfrak{a}} \mathrm{E} \otimes_{\mathrm{O_K}} \mathfrak{a}$$

where again the transition maps are induced by multiplication. The inclusion $\mathrm{T}(\mathrm{E}) \to \widetilde{\mathrm{E}}$ identifies $\mathrm{T}(\mathrm{E})$ with the kernel of the projection $\widetilde{\mathrm{E}} \to \mathrm{E}$ so that we have an exact sequence of sheaves (for the fpqc topology)

$$0 \to \mathrm{T}(\mathrm{E}) \to \widetilde{\mathrm{E}} \to \mathrm{E} \to 0. \tag{4.5.1.1}$$

4.5.2. Now let S be a Λ-ind-affine scheme. The perfection S^{per} of S is the Λ-sheaf defined by

$$S^{per} = \operatorname*{colim}_{\mathfrak{a}\in \mathrm{Id}_{O_K}, \psi^{\mathfrak{a}}} S$$

where the transition maps are the Frobenius lifts. The action of the monoid of ideals Id_{O_K} on S^{per} is now by automorphisms so that it extends to an action of the group of fractional ideals Id_K. For $\mathfrak{a} \in \mathrm{Id}_K$ (now a fractional ideal) we write $\psi^{\mathfrak{a}}_{S_{per}} : S^{per} \to S^{per}$ for the corresponding automorphism. It follows immediately from the definition that S^{per} is universal among Λ-sheaves lying under S on which the Frobenius lifts are isomorphisms. When $S = W^*(T)$ is the Witt vectors of an ind-affine scheme we write

$$\widehat{W}^*(T) = W^*(T)^{per}.$$

Viewing S as a $\Lambda_{S^{per}}$-ind-affine scheme via the element of the colimit (4.5.2) corresponding to $O_K \in \mathrm{Id}_{O_K}$ we see that the structure map of the element of the colimit (4.5.2) corresponding $\mathfrak{a}$ is

$$S \to S^{per} \overset{\psi^{\mathfrak{a}^{-1}}_{S^{per}}}{\to} S^{per}$$

and the colimit (4.5.2) can be rewritten as the colimit of S^{per}-sheaves

$$S^{per} = \operatorname*{colim}_{\mathfrak{a}\in \mathrm{Id}_{O_K}, \psi_{\mathfrak{a}}} \psi^{\mathfrak{a}^{-1}}_{S^{per}!}(S). \tag{4.5.2.1}$$

4.5.3. If E/S is a CM elliptic curve equipped with a canonical Λ-structure then we have a natural identification $E \otimes_{O_K} \mathfrak{a}^{-1} \xrightarrow{\sim} \psi^{\mathfrak{a}*}_S(E)$. Hence for $\mathfrak{a}, \mathfrak{b} \in \mathrm{Id}_{O_K}$ we have isomorphisms

$$E \otimes \mathfrak{b} \xrightarrow{\sim} \psi^{\mathfrak{a}*}_S(E \otimes \mathfrak{a}\mathfrak{b})$$

and this gives for all $\mathfrak{a}$ and $\mathfrak{b}$ a Cartesian diagram

$$\begin{array}{ccc} E \otimes_{O_K} \mathfrak{b} & \longrightarrow & E \otimes_{O_K} \mathfrak{a}\mathfrak{b} \\ \downarrow & & \downarrow \\ \psi^{\mathfrak{b}^{-1}}_{S^{per}!}(S) & \xrightarrow{\psi^{\mathfrak{a}}} & \psi^{(\mathfrak{a}\mathfrak{b})^{-1}}_{S^{per}!}(S). \end{array} \tag{4.5.3.1}$$

We then define a Λ-sheaf over S^{per} by

$$E_{per} = \operatorname*{colim}_{\mathfrak{a}\in \mathrm{Id}_{O_K}} E \otimes_{O_K} \mathfrak{a} \to S^{per} = \operatorname*{colim}_{\mathfrak{a}\in \mathrm{Id}_{O_K}} \psi^{\mathfrak{a}^{-1}}_{S^{per}!}(S) = S^{per}.$$

4.5.4 Proposition. — E_{per} *is a* CM *elliptic curve over* S^{per} *equipped with a canonical* $\Lambda_{S^{per}}$*-structure.*

Proof. — First, E_{per} admits a $\Lambda_{S^{per}}$-structure as it is a colimit of $\Lambda_{S^{per}}$-sheaves. Secondly, as the colimit is filtered and the diagrams (4.5.3.1) are all cartesian it follows that for all $\mathfrak{a} \in \mathrm{Id}_{O_K}$ we have $\Lambda_{S^{per}}$-isomorphisms

$$E_{per} \times_{S^{per}} \psi^{\mathfrak{a}^{-1}}_{S^{per}!}(S) \xrightarrow{\sim} E \otimes_{O_K} \mathfrak{a}.$$

This shows that $\mathrm{E}_{\mathrm{per}}$ is a CM elliptic curve. It now also follows from (iii) of (4.1.19) that its $\Lambda_{\mathrm{S}^{\mathrm{per}}}$-structure is canonical, as the Λ_{S}-structures of $\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{a}$ are canonical and $(\psi^{\mathfrak{a}^{-1}}_{\mathrm{S}^{\mathrm{per}}!}(\mathrm{S})\to\mathrm{S}_{\mathrm{per}})_{\mathfrak{a}\in\mathrm{Id}_{\mathrm{O_K}}}$ is a cover. □

4.5.5. We now relate $\mathrm{E}_{\mathrm{per}}/\mathrm{S}^{\mathrm{per}}$ to $\widetilde{\mathrm{E}}/\mathrm{S}$. This is nothing more than an application of certain adjunctions and the definitions. Indeed, for each ind-affine scheme $\mathrm{T}\to\mathrm{S}$, the morphism $\mathrm{T}\to\mathrm{S}^{\mathrm{per}}$ induces a morphism $\widehat{\mathrm{W}}^*(\mathrm{T})\to\mathrm{S}_{\mathrm{per}}$ and viewing $\widehat{\mathrm{W}}^*(\mathrm{T})$ as a $\Lambda_{\mathrm{S}^{\mathrm{per}}}$-ind-affine scheme we have

$$\begin{aligned}
\mathrm{Hom}^{\Lambda}_{\mathrm{S}^{\mathrm{per}}}(\widehat{\mathrm{W}}^*(\mathrm{T}),\mathrm{E}_{\mathrm{per}}) &= \varinjlim_{\mathfrak{a}}\mathrm{Hom}^{\Lambda}_{\mathrm{S}^{\mathrm{per}}}(\psi^{\mathfrak{a}^{-1}}_{\mathrm{S}^{\mathrm{per}}!}(\mathrm{W}^*(\mathrm{T})),\mathrm{E}_{\mathrm{per}})\\
&= \varinjlim_{\mathfrak{a}}\mathrm{Hom}^{\Lambda}_{\mathrm{S}^{\mathrm{per}}}(\mathrm{W}^*(\mathrm{T}),\psi^{\mathfrak{a}^{-1}*}_{\mathrm{S}^{\mathrm{per}}}(\mathrm{E}_{\mathrm{per}}))\\
&= \varinjlim_{\mathfrak{a}}\mathrm{Hom}^{\Lambda}_{\mathrm{S}^{\mathrm{per}}}(\mathrm{W}^*(\mathrm{T}),\mathrm{E}_{\mathrm{per}}\otimes_{\mathrm{O_K}}\mathfrak{a}))\\
&= \varinjlim_{\mathfrak{a}}\mathrm{Hom}^{\Lambda}_{\mathrm{S}}(\mathrm{W}^*(\mathrm{T}),\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{a})\\
&= \varinjlim_{\mathfrak{a}}\mathrm{Hom}_{\mathrm{S}}(\mathrm{T},\mathrm{E}\otimes_{\mathrm{O_K}}\mathfrak{a})\\
&= \mathrm{Hom}_{\mathrm{S}}(\mathrm{T},\widetilde{\mathrm{E}}).
\end{aligned}$$

Therefore, we have a natural isomorphism of functors on ind-affine S-schemes

$$\mathrm{Hom}^{\Lambda}_{\mathrm{S}^{\mathrm{per}}}(\widehat{\mathrm{W}}^*(-),\mathrm{E}_{\mathrm{per}})\xrightarrow{\sim}\mathrm{Hom}_{\mathrm{S}}(-,\widetilde{\mathrm{E}}).$$

If we denote the left hand side by

$$\widehat{\mathrm{W}}_*(\mathrm{E}_{\mathrm{per}})_{\Lambda}:\mathrm{T}/\mathrm{S}\mapsto\mathrm{Hom}^{\Lambda}_{\mathrm{S}^{\mathrm{per}}}(\widehat{\mathrm{W}}^*(\mathrm{T}),\mathrm{E}_{\mathrm{per}})$$

then we may then rewrite the exact sequence of (4.5.1.1) to obtain the following:

4.5.6 Theorem. — *The is an exact sequence of* fpqc *sheaves*

$$0\to\mathrm{T}(\mathrm{E})\to\widehat{\mathrm{W}}_*(\mathrm{E}_{\mathrm{per}})_{\Lambda}\to\mathrm{E}\to 0.$$

4.5.7. If now S is an ind-affine scheme (not a Λ-scheme) and E/S is any CM elliptic curve then we may perform the above construction for $\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})/\mathrm{W}^*(\mathrm{S})$ to obtain a CM elliptic curve

$$\widehat{\mathrm{W}}^*_{\mathrm{CM}}(\mathrm{E}):=\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E})_{\mathrm{per}}\to\widehat{\mathrm{W}}^*(\mathrm{S})=\mathrm{W}^*(\mathrm{S})_{\mathrm{per}}$$

and an exact sequence of sheaves for the fpqc topology over $\mathrm{W}^*(\mathrm{S})$:

$$0\to\mathrm{T}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}))\to\widehat{\mathrm{W}}_*(\widehat{\mathrm{W}}^*_{\mathrm{CM}}(\mathrm{E}))_{\Lambda}\to\widehat{\mathrm{W}}^*_{\mathrm{CM}}(\mathrm{E})\to 0. \tag{4.5.7.1}$$

If we pull-back this exact sequence along the first ghost component $g_{(1)}:\mathrm{S}\to\mathrm{W}^*(\mathrm{S})$, and just write

$$\widehat{\mathrm{W}}_*(\widehat{\mathrm{W}}^*_{\mathrm{CM}}(\mathrm{E}))_{\Lambda}|_{\mathrm{S}}=g^*_{(1)}(\widehat{\mathrm{W}}_*(\widehat{\mathrm{W}}^*_{\mathrm{CM}}(\mathrm{E}))_{\Lambda})$$

then (4.5.7.1) becomes the exact sequence over S:

$$0\to\mathrm{T}(\mathrm{E})\to\widehat{\mathrm{W}}_*(\widehat{\mathrm{W}}^*_{\mathrm{CM}}(\mathrm{E}))_{\Lambda}|_{\mathrm{S}}\to\mathrm{E}\to 0$$

(where we use the fact that $g^*_{(1)}(\mathrm{W}^*_{\mathrm{CM}}(\mathrm{E}))) = \mathrm{E}$).

4.5.8 Corollary. — *For any ind-affine scheme* S *and any* CM *elliptic curve* E/S *there exists an exact sequence of* fpqc *sheaves over* S

$$0 \to \mathrm{T}(\mathrm{E}) \to \widehat{\mathrm{W}}_*(\widehat{\mathrm{W}}^*_{\mathrm{CM}}(\mathrm{E}))_\Lambda|_{\mathrm{S}} \to \mathrm{E} \to 0.$$

4.5.9 Remark. — Although we have not discussed it, there is a completely analogous theory of canonical lifts for Lubin–Tate O-modules for which the above constructions can also be made. For $\mathrm{O} = \mathbf{Z}_p$ and $\mathrm{F} = \mu_{p^\infty}$, the analogue of the exact sequence (4.5.8) evaluated on $\mathrm{Spf}(\overline{\mathbf{Z}}_p)$ gives

$$0 \to \mathrm{T}(\mu_{p^\infty})(\overline{\mathbf{Z}}_p) \to \mu_{p^\infty}(\mathrm{A}_{\mathrm{inf}})^{\varphi_p = p} \to \mu_{p^\infty}(\overline{\mathbf{Z}}_p) \to 0$$

where $\mathrm{A}^{\mathrm{inf}}$ with its Frobenius lift φ_p is Fontaine's ring, and we have used the (non-obvious) fact that

$$\mathrm{Spf}(\mathrm{A}^{\mathrm{inf}}) \xrightarrow{\sim} \widehat{\mathrm{W}}^*(\mathrm{Spf}(\overline{\mathbf{Z}}_p)).$$

The image in $\mu_{p^\infty}(\mathrm{A}^{\mathrm{inf}})$ of a generator $\epsilon \in \mathrm{T}(\mu_{p^\infty})(\overline{\mathbf{Z}}_p)$ is Fontaine's element $[\epsilon]$, the logarithm of which is the p-adic period t.

4.5.10 Remark. — While there is (as yet) no theory of analytic Λ-structures one can fudge a theory of analytic canonical lifts. Here let us sketch the construction of an analytic analogue of the short exact sequence (4.5.8) relating the period lattice of $\mathrm{E}^{\mathrm{an}}/\mathrm{S}^{\mathrm{an}}$ to a certain analytic canonical lift of E/S.

So let $\mathrm{S} \to \mathrm{Spec}(\mathbf{C})$ be a complex scheme of finite type. We note that as $\mathrm{K} \subset \mathbf{C}$, we have

$$\mathrm{W}^*(\mathrm{S}) = \Gamma^*(\mathrm{S}) = \coprod_{\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}} \mathrm{S} = \underline{\mathrm{Id}_{\mathrm{O_K}}} \times \mathrm{S}$$

and

$$\widehat{\mathrm{W}}^*(\mathrm{S}) = \underline{\mathrm{Id}_{\mathrm{K}}} \times \mathrm{S}.$$

There is a natural analytic analogue of Id_{K} which we call $\mathrm{Id}_{\mathbf{C}}$ and is given by $(\mathrm{Id}_{\mathrm{K}} \times \mathbf{C}^\times)/\mathrm{K}^\times$ where $a \in \mathrm{K}^\times$ acts on $\mathrm{Id}_{\mathrm{K}} \times \mathbf{C}$ by $(\mathfrak{a}, s) \mapsto ((a)\mathfrak{a}, as)$. Note there is a short exact sequence

$$0 \to \mathrm{O}_{\mathrm{K}}^\times \to \mathbf{C}^\times \to \mathrm{Id}_{\mathbf{C}} \to \mathrm{CL}_{\mathrm{O_K}} \to 0.$$

It is natural, in light of the above, to define the analytic Witt vectors of the analytification S^{an} of S to be the analytic space

$$\mathrm{W}^{\mathrm{an}*}(\mathrm{S}) := \mathrm{Id}_{\mathbf{C}} \times \mathrm{S}^{\mathrm{an}}$$

together with its action of $\mathrm{Id}_{\mathbf{C}}$.

We can now analytically mimic our construction of $\mathrm{W}^*_{\mathrm{CM}}$ over $\mathrm{W}^{\mathrm{an}*}(\mathrm{S})$. So define the rank one $\mathrm{O_K}$-local system $\mathscr{L}_{\mathrm{an}}$ to have fibre over $(\mathfrak{a}, s) \times \mathrm{S}^{\mathrm{an}} \subset \mathrm{S}^{\mathrm{an}} \times \mathrm{Id}_{\mathbf{C}} = \mathrm{W}^{\mathrm{an}*}(\mathrm{S})$ the constant $\mathrm{O_K}$-local system associated to the rank one $\mathrm{O_K}$-module $s \cdot \mathfrak{a}^{-1} \subset s \cdot \mathrm{K} \subset \mathbf{C}$ (note this depends only on the class of

$(\mathfrak{a}, s) \in (\mathrm{Id}_K \times \mathbf{C}^\times)/K^\times = \mathrm{Id}_{\mathbf{C}})$. If E/S is a CM elliptic curve then we define $W^{an*}_{CM}(E)$ to be

$$p_S^*(E^{an}) \otimes_{O_K} \mathscr{L}_{an}$$

where $p_S : W^{an*}(S) = \mathrm{Id}_{\mathbf{C}} \times S^{an} \to S^{an}$ is the projection (cf. (4.1.2)).

The CM elliptic curve $W^{an*}_{CM}(E) \to W^{an*}(S)$ inherits a natural action of Id_{O_K} (not $\mathrm{Id}_{\mathbf{C}}$!) which is compatible with that on $W^{an*}(S)$. Finally, setting $W^{an*}(X) = \mathrm{Id}_{\mathbf{C}} \times X$ with its $\mathrm{Id}_{\mathbf{C}}$ action for any analytic space, we define a sheaf on the big analytic site of S by

$$W^{an}_*(W^{an*}_{CM}(E))_\Lambda|_S : X/S \mapsto \mathrm{Hom}^{\mathrm{Id}_{O_K}}_{W^{an*}(S)}(W^{an*}(X), W^{an*}_{CM}(E)).$$

Let us spell out here that the right hand side here denotes the Id_{O_K}-equivariant *analytic* $W^{an*}(S)$-maps

$$W^{an*}(X) \to W^{an*}_{CM}(E).$$

With this definition one can show (almost as formally as in the algebraic situation) that there exists an isomorphism of sheaves on the big analytic site of S^{an}

$$W^{an}_*(W^{an*}_{CM}(E))_\Lambda|_S \xrightarrow{\sim} \underline{\mathrm{Lie}}_{E^{an}/S^{an}}$$

and so the exponential sequence

$$0 \to T_{O_K}(E^{an}) \to \underline{\mathrm{Lie}}_{E^{an}/S^{an}} \to E^{an} \to 0$$

of E^{an}/S^{an} can be rewritten as

$$0 \to T_{O_K}(E^{an}) \to W^{an}_*(W^{an*}_{CM}(E))_\Lambda|_S \to E^{an} \to 0.$$

APPENDIX A

ODD AND ENDS

A.1. Formal groups

The purpose of this section is to give an intrinsic definition of a (smooth) formal group. We do this using Messing's definition of infinitesimal neighbourhoods given in [**27**], and the general theory of tangent spaces given in [**2**].

A.1.1. First let us recall the construction of infinitesimal neighbourhoods from Chapter II of [**27**] and some its properties. So fix a monomorphism of sheaves $\mathrm{Z} \to \mathrm{X}$. The kth infinitesimal neighbourhood of Z in X, denoted $\mathrm{Inf}_{\mathrm{Z}}^{(k)}(\mathrm{X})$, is the sub-sheaf of X defined by the property that an affine scheme T mapping to X factors through $\mathrm{Inf}_{\mathrm{Z}}^{(k)}(\mathrm{X}) \to \mathrm{X}$ if and only if there exists an fpqc cover $(\mathrm{T}_i \to \mathrm{T})_{i\in\mathrm{I}}$ and closed sub-schemes $(\overline{\mathrm{T}}_i \to \mathrm{T}_i)_{i\in\mathrm{I}}$ defined by ideals whose $(k+1)$st power is (0), such that the composition $\overline{\mathrm{T}}_i \to \mathrm{T} \to \mathrm{X}$ factors through $\mathrm{Z} \to \mathrm{X}$. Diagrammatically, we have

$$\begin{array}{ccccc} \mathrm{Z} & \hookrightarrow & \mathrm{Inf}_{\mathrm{Z}}^{(k)}(\mathrm{X}) & \hookrightarrow & \mathrm{X} \\ \uparrow & & \uparrow & \nearrow & \uparrow \\ \overline{\mathrm{T}}_i & \hookrightarrow & \mathrm{T}_i & \longrightarrow & \mathrm{T}. \end{array}$$

If $\mathrm{Z} \to \mathrm{X}$ is a closed immersion of *schemes* defined by a quasi-coherent ideal $\mathscr{I} \subset \mathscr{O}_{\mathrm{X}}$ then $\mathrm{Inf}_{\mathrm{Z}}^{(k)}(\mathrm{X}) \to \mathrm{X}$ is the closed sub-scheme defined by the ideal $\mathscr{I}^{(k+1)} \subset \mathscr{O}_{\mathrm{X}}$.

These constructions satisfy the following:

(a) For $k \leq k'$ there is an inclusion $\mathrm{Inf}_{\mathrm{Z}}^{(k)}(\mathrm{X}) \subset \mathrm{Inf}_{\mathrm{Z}}^{k+1}(\mathrm{X})$. We write $\mathrm{Inf}_{\mathrm{Z}}(\mathrm{X}) = \mathrm{colim}_k \mathrm{Inf}_{\mathrm{Z}}^{(k)}(\mathrm{X})$ and call this completion of X along Z.

(b) If $\mathrm{X}' \to \mathrm{X}$ is any morphism then we have

$$\mathrm{Inf}_{\mathrm{Z}}^{(k)}(\mathrm{X}) \times_{\mathrm{X}} \mathrm{X}' = \mathrm{Inf}_{\mathrm{Z}\times_{\mathrm{X}}\mathrm{X}'}^{(k)}(\mathrm{X}').$$

(c) If $\mathrm{Z} \to \mathrm{X}$ is an monomorphism of S-sheaves for some sheaf S and Y is another S-sheaf equipped with an S-monomorphism $\mathrm{Z} \to \mathrm{Y}$ then, as

sub-sheaves of $\mathrm{X} \times_{\mathrm{S}} \mathrm{Y}$, there are inclusions:

$$\mathrm{Inf}_{\mathrm{Z}}^{(k)}(\mathrm{Y} \times_{\mathrm{S}} \mathrm{X}) \subset \mathrm{Inf}_{\mathrm{Z}}^{(k)}(\mathrm{X}) \times_{\mathrm{S}} \mathrm{Inf}_{\mathrm{Z}}^{(k)}(\mathrm{Y}) \subset \mathrm{Inf}_{\mathrm{Z}}^{(2k)}(\mathrm{X} \times_{\mathrm{S}} \mathrm{Y})$$

and taking colimits we have

$$\mathrm{Inf}_{\mathrm{Z}}(\mathrm{X} \times_{\mathrm{S}} \mathrm{Y}) = \mathrm{Inf}_{\mathrm{Z}}(\mathrm{Y}) \times_{\mathrm{S}} \mathrm{Inf}_{\mathrm{Z}}(\mathrm{X}).$$

A.1.2. Write $\mathrm{Sh}_{\mathrm{S}}^{\bullet}$ for the category of S-pointed S-sheaves. If X is a pointed S-sheaf we write $\widehat{\mathrm{X}} = \mathrm{colim}_k \mathrm{Inf}_{\mathrm{S}}^{(k)}(\mathrm{X})$ for the formal neighbourhood of the point $\mathrm{S} \to \mathrm{X}$. The functor $\mathrm{X} \mapsto \widehat{\mathrm{X}}$ preserves finite products of pointed S-sheaves so that if G is an S-group, viewed as a pointed S-sheaf via the identity $\mathrm{S} \to \mathrm{G}$, then $\widehat{\mathrm{G}}$ is again a sheaf of groups over S which we call the formal group of G.

A.1.3. Here we recall part of the rather general construction of Lie algebras given in Exposé II of [**2**]. Let S be a sheaf and $\mathscr{V}$ a vector bundle. Make $\mathscr{O}_{\mathrm{S}} \oplus \mathscr{V}$ a sheaf of quasi-coherent $\mathscr{O}_{\mathrm{S}}$-algebras by declaring that $\mathscr{V}$ be a square zero ideal, and write $\mathrm{D}_{\mathrm{S}}(\mathscr{V})$ for the S-sheaf whose sections over an ind-affine scheme $\mathrm{T} \to \mathrm{S}$ are given

$$\mathrm{D}_{\mathrm{S}}(\mathscr{V})(\mathrm{T}) = \mathrm{Hom}_{\mathscr{O}_{\mathrm{T}}}(\mathscr{O}_{\mathrm{T}} \oplus \mathscr{V}_{\mathrm{T}}, \mathscr{O}_{\mathrm{T}}).$$

This defines a contravariant functor $\mathrm{QCoh}(\mathscr{O}_{\mathrm{S}}) \to \mathrm{Sh}_{\mathrm{S}}^{\bullet}$. If $\mathscr{V}_1$ and $\mathscr{V}_2$ are two quasi-coherent $\mathscr{O}_{\mathrm{S}}$-modules then the two projections $\mathscr{V}_1 \oplus \mathscr{V}_2 \to \mathscr{V}_i$ for $i = 1, 2$ induce for each pointed S-sheaf X a morphism

$$\underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}(\mathscr{V}_1 \oplus \mathscr{V}_2), \mathrm{X}) \to \underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}(\mathscr{V}_1), \mathrm{X}) \times_{\mathrm{S}} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}(\mathscr{V}_2), \mathrm{X}) \quad \text{(A.1.3.1)}$$

and a pointed S-sheaf X is said to satisfy condition (E) if for all vector bundles $\mathscr{V}_1$, $\mathscr{V}_2$ the morphism (A.1.3.1) is an isomorphism.

A.1.4 Proposition. — *With notation as above:*

(i) *if* X *satisfies condition* (E) *over* S *and* $\mathrm{S}' \to \mathrm{S}$ *is a morphism then* $\mathrm{X}_{\mathrm{S}'}$ *satisfies condition* (E) *over* S'*,*

(ii) X *satisfies condition* E *for* S *if and only if there is a cover* $(\mathrm{S}_i \to \mathrm{S})_{i \in \mathrm{I}}$ *such that for each* $i \in \mathrm{I}$ *the sheaf* $\mathrm{X}_{\mathrm{S}_i}$ *satisfies condition* (E) *over* S_i*,*

(iii) *if* S *is a scheme and* X *is an* S*-pointed ind-scheme then* X *satisfies condition* (E)*.*

Proof. — (i) and (ii) follow immediately from the definition. For (iii) we may assume that X is a scheme as filtered colimits preserve fibre products. In which case the claim follows from the fact that

$$\underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}(\mathscr{M}), \mathrm{X}) = \mathscr{M} \otimes_{\mathscr{O}_{\mathrm{S}}} \underline{\mathrm{Hom}}_{\mathscr{O}_{\mathrm{S}}}(\Omega_{\mathrm{X}/\mathrm{S},\bullet}, \mathscr{O}_{\mathrm{S}}).$$

□

A.1.5. If X is a pointed S sheaf satisfying condition (E) over S then, writing $\mathrm{D}_{\mathrm{S}}^{(n)} = \mathrm{D}_{\mathrm{S}}(\mathscr{O}^n)$, the inverse of the isomorphism

$$\underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}^{(2)}, \mathrm{X}) \to \underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}^{(1)}, \mathrm{X}) \times_{\mathrm{S}} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}^{(1)}, \mathrm{X})$$

composed with the map

$$\underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}^{(2)}, \mathrm{X}) \to \underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}^{(1)}, \mathrm{X})$$

induced by the sum $\mathscr{O}_{\mathrm{S}}^2 \to \mathscr{O}_{\mathrm{S}}$ defines a map

$$\underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}^{(1)}, \mathrm{X}) \times \underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}^{(1)}, \mathrm{X}) \to \underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}^{(1)}, \mathrm{X}).$$

This equips

$$\underline{\mathrm{Lie}}_{\mathrm{X/S}} := \underline{\mathrm{Hom}}_{\mathrm{S}}^{\bullet}(\mathrm{D}_{\mathrm{S}}^{(1)}, \mathrm{X})$$

with the structure of an abelian group over S. Moreover, the S-pointed sheaf $\mathrm{D}_{\mathrm{S}}^{(1)}$ admits an action of the sheaf of monoids $\mathscr{O}_{\mathrm{S}}$ induced by the action of $\mathscr{O}_{\mathrm{S}}$ on itself and this equips $\underline{\mathrm{Lie}}_{\mathrm{X/S}}$ with the structure of an $\mathscr{O}_{\mathrm{S}}$-module. We call $\underline{\mathrm{Lie}}_{\mathrm{X/S}}$ the Lie algebra of the pointed S-sheaf X.

A.1.6. Let S be a sheaf and let X be a pointed S-sheaf. We say that X is a formal variety over S if the following conditions hold:

(i) the inclusion $\widehat{\mathrm{X}} \to \mathrm{X}$ is an isomorphism,
(ii) for each $k \geq 0$ the morphism $\mathrm{Inf}_{\mathrm{S}}^{(k)}(\mathrm{X}) \to \mathrm{S}$ affine,
(iii) X is formally smooth and locally finitely presented over S, and
(iv) $\underline{\mathrm{Lie}}_{\mathrm{X/S}}$ is a vector bundle.[(1)]

A.1.7 Proposition. — *Let* S *be a sheaf and* X *a pointed* S*-sheaf. Then the following are equivalent:*

(i) X *is a formal variety over* S*,*
(ii) *there exists a cover* $(\mathrm{S}_i \to \mathrm{S})_{i\in\mathrm{I}}$*, integers* $n_i \geq 0$ *for* $i \in \mathrm{I}$ *and pointed* S_i*-isomorphisms*

$$\widehat{\mathbf{A}}_{\mathrm{S}_i}^{n_i} = \mathrm{Inf}_{\mathrm{S}_i}(\mathbf{A}_{\mathrm{S}_i}^{n_i}) \xrightarrow{\sim} \mathrm{X}_{\mathrm{S}_i}.$$

Proof. — This follows from Proposition 3.1.1 of [**27**]. □

A.1.8. The dimension $\dim_{\mathrm{S}}(\mathrm{X})$ of a formal variety X/S is defined to be the map $\mathrm{S} \to \underline{\mathbf{N}}_{\mathrm{S}}$ giving the rank of the locally free $\mathscr{O}_{\mathrm{S}}$-module $\underline{\mathrm{Lie}}_{\mathrm{X/S}}$.

If S is a scheme and X/S is a smooth scheme over S equipped with a closed S-point $\mathrm{S} \to \mathrm{X}$ then $\widehat{\mathrm{X}}$ is a formal variety over S. A formal group F over S is a formal variety F/S which is also a sheaf of groups over S (with identity the given point). As the functor $\mathrm{X} \mapsto \widehat{\mathrm{X}}$ commutes with products, it follows that if S is a scheme and G/S is a smooth separated group scheme over S then $\widehat{\mathrm{G}}$/S is a formal group over S.

(1) (i) and (ii) combined show that X satisfies condition (E) over S so that this makes sense.

A.2. Serre's tensor product

Here we give a (very broad) generalisation of a basic construction due to Serre (Chapter XIII §2 of [**1**]). The idea that this construction of Serre could and should be generalised, at least in the study of CM elliptic curves, is not an idea wholly original to the author (see §1.7.4 of [**12**]) however it was arrived at independently.

A.2.1. Let S be a sheaf and let $\mathscr{A}$ be a sheaf of rings over S. We say that an $\mathscr{A}$-module $\mathscr{V}$ satisfies condition (P) if, locally on S, $\mathscr{V}$ is a direct factor of a free $\mathscr{A}$-module of finite rank. The class of $\mathscr{A}$-modules satisfying condition (P) is clearly closed under the operations of taking $\mathscr{A}$-linear Hom, tensor product, direct factors and direct sums.

A.2.2 Proposition. — *Let $\mathscr{V}$ satisfy condition* (P)*. Then the functor*

$$\mathrm{Mod}(\mathscr{A}) \to \mathrm{Mod}(\mathscr{A}) : \mathrm{G} \mapsto \mathrm{G} \otimes_{\mathscr{A}} \mathscr{V}$$

is exact.

Proof. — We need only show that this functor preserves monomorphisms. This is local on S and so we may assume that $\mathscr{V}$ is a direct factor of a free $\mathscr{A}$-module in which case it is clear as $\mathrm{G} \otimes_{\mathscr{A}} \mathscr{V} \subset \mathrm{G} \otimes_{\mathscr{A}} \mathscr{A}^n = \mathrm{G}^n$ for some $n \geq 0$ and $\mathrm{G} \mapsto \mathrm{G}^n$ is exact. □

A.2.3 Proposition. — *We have the following*

(i) *For each pair of $\mathscr{A}$-modules $\mathscr{V}, \mathscr{W}$ satisfying condition* (P) *and each pair of $\mathscr{A}$-modules $\mathrm{G}, \mathrm{F} \in \mathrm{Mod}(\mathscr{A})$ the morphism*

$$\underline{\mathrm{Hom}}^{\mathscr{A}}_{\mathrm{S}}(\mathrm{F}, \mathrm{G}) \otimes_{\mathscr{A}} \underline{\mathrm{Hom}}^{\mathscr{A}}_{\mathrm{S}}(\mathscr{V}, \mathscr{W}) \to \underline{\mathrm{Hom}}^{\mathscr{A}}_{\mathrm{S}}(\mathrm{F} \otimes_{\mathscr{A}} \mathscr{V}, \mathrm{G} \otimes_{\mathscr{A}} \mathscr{W})$$

is an isomorphism.

(ii) *If* G *is an $\mathscr{A}$-module satisfying condition* (E) *and $\mathscr{V}$ is an $\mathscr{A}$-module satisfying condition* (P) *then the natural morphism $\underline{\mathrm{Lie}}_{\mathrm{G/S}} \otimes_{\mathscr{A}} \mathscr{V} \to \underline{\mathrm{Lie}}_{\mathrm{G} \otimes_{\mathscr{A}} \mathscr{V}/\mathrm{S}}$ is an isomorphism.*

Proof. — (i) The map defined is functorial and so we may, by adjunction, assume that $\mathscr{V} = \mathscr{A}$ so that we are reduced to showing that the map

$$i_{\mathscr{W}} : \underline{\mathrm{Hom}}^{\mathscr{A}}_{\mathrm{S}}(\mathrm{F}, \mathrm{G}) \otimes_{\mathscr{A}} \mathscr{W} \to \underline{\mathrm{Hom}}^{\mathscr{A}}_{\mathrm{S}}(\mathrm{F}, \mathrm{G} \otimes_{\mathscr{A}} \mathscr{W})$$

is an isomorphism. The claim is clearly local on S so we may assume that $\mathscr{A}^n = \mathscr{W} \oplus \mathscr{W}'$. We then have $i_{\mathscr{A}^n} = i_{\mathscr{W}} \oplus i_{\mathscr{W}'}$ so that it is enough to show the claim for $\mathscr{A}^n$ which is clear.

(ii) This is proved in much the same way as (i). □

A.2.4. A formal $\mathscr{A}$-module over S is a formal group F/S equipped with an action of $\mathscr{A}$. If we are given a homomorphism $\mathscr{A} \to \mathscr{O}_S$ then we say the action is strict, or that F is a strict formal $\mathscr{A}$-module, if the two actions of $\mathscr{A}$ on the $\mathscr{O}_S$-module $\underline{\mathrm{Lie}}_{F/S}$ coming from the action of $\mathscr{A}$ on F and the homomorphism $\mathscr{A} \to \mathscr{O}_S$ coincide. In this case, if $\mathscr{V}$ is an $\mathscr{A}$-module satisfying condition (P) then $\mathscr{V} \otimes_{\mathscr{A}} \mathscr{O}_S$ is a locally free $\mathscr{O}_S$-module and we write $\mathrm{rk}(\mathscr{V}) : S \to \underline{\mathbf{N}}_S$ for the rank of this $\mathscr{O}_S$-module.

A.2.5 Corollary. — *If* F *is a strict formal $\mathscr{A}$-module over* S *and $\mathscr{V}$ is an $\mathscr{A}$-module over* S *satisfying condition* (P) *then* $F \otimes_{\mathscr{A}} \mathscr{V}$ *is a strict formal $\mathscr{A}$-module. Moreover, we have* $\dim(F \otimes_{\mathscr{A}} \mathscr{V}) = \dim(F) \cdot \mathrm{rk}(\mathscr{V})$

Proof. — As the claim is local on S we may assume that $\mathscr{V}$ is the kernel of some idempotent endomorphism $\mathscr{A}^n \to \mathscr{A}^n$ for some n. The diagram of S-pointed sheaves

$$\begin{array}{ccc} F^n & \longrightarrow & F^n \\ \uparrow & & \uparrow \\ F \otimes_{\mathscr{A}} \mathscr{V} & \longrightarrow & S \end{array}$$

remains cartesian after applying $\mathrm{Inf}_S^{(k)}$ for each $k \geq 1$. This shows that $F \otimes_{\mathscr{A}} \mathscr{V}$ satisfies conditions (i) and (ii) of (A.1.6) and by (A.2.6) we see that $F \otimes_{\mathscr{A}} \mathscr{V}$ also satisfies (iii). Therefore $F \otimes_{\mathscr{A}} \mathscr{V}$ satisfies condition (E) over S and by (A.2.3) it satisfies condition (iv) of (A.1.6) so that F/S is a formal $\mathscr{A}$-module over S. That the action of $\mathscr{A}$ on $F \otimes_{\mathscr{A}} \mathscr{V}$ is strict and $\dim(F \otimes_{\mathscr{A}} \mathscr{V}) = \dim(F) \cdot \mathrm{rk}(\mathscr{V})$ follows from (A.2.3). □

A.2.6 Proposition. — *Let $f : G \to F$ be a homomorphism of $\mathscr{A}$-modules and let $\mathscr{V}$ satisfy condition* (P)*. If f satisfies one of the following properties then so does $f \otimes_{\mathscr{A}} \mathscr{V} : G \otimes_{\mathscr{A}} \mathscr{V} \to F \otimes_{\mathscr{A}} \mathscr{V}$:*

(i) *formally unramified, formally smooth or formally étale,*
(ii) *formally universally closed, formally separated, formally proper*[(2)]
(iii) *locally finitely presented, quasi-compact or quasi-separated,*
(iv) *has connected geometric fibres,*
(v) *affine, or affine and flat,*
(vi) *finite locally free.*

Proof. — All properties of morphisms of sheaves descend under covers of S so we may assume that $\mathscr{V} \oplus \mathscr{V}' = \mathscr{A}^n$ and hence

$$(f \otimes_{\mathscr{A}} \mathscr{V}) \oplus (f \otimes_{\mathscr{A}} \mathscr{V}') = f \otimes_{\mathscr{A}} \mathscr{A}^n = f^n.$$

(2) Here we mean that G/S satisfies the local existence, resp. uniqueness (resp. local existence and uniqueness) of the valuative criterion.

Moreover, these properties are all preserved by $f \mapsto f^n$ and base change. From the cartesian diagram

$$\begin{array}{ccc} \mathrm{G}^n & \xrightarrow{\quad f^n \quad} & \mathrm{F}^n \\ \uparrow & & \uparrow \\ (\mathrm{G} \otimes_{\mathscr{A}} \mathscr{V}) \oplus \ker(f \otimes_{\mathscr{A}} \mathscr{V}') & \xrightarrow{(f\otimes_{\mathscr{A}}\mathscr{V})\oplus 0} & \mathrm{F} \otimes_{\mathscr{A}} \mathscr{V} \end{array}$$

we see that

$$(f \otimes_{\mathscr{A}} \mathscr{V}) \oplus 0 = (f \otimes_{\mathscr{A}} \mathscr{V}) \times_{\mathrm{S}} \ker(f \otimes_{\mathscr{A}} \mathscr{V}')$$

satisfies the given property. But $\ker(f \otimes_{\mathscr{A}} \mathscr{V}') \to \mathrm{S}$ is an epimorphism hence, $f \otimes_{\mathscr{A}} \mathscr{V}$ satisfies the given property. □

A.3. Strict finite O-modules

A.3.1. Here we give a short overview of faltings' generalisation of Cartier duality to strict finite O-modules [**20**]. We will then use it to prove (1.2.12) and (1.2.13) as claimed (see (A.3.7)).

Let O be a complete local Dedekind domain with maximal ideal $\mathfrak{p}$, residue field $\mathbf{F}$ of cardinality $\mathrm{N}\mathfrak{p}$ and fix an affine scheme $\mathrm{S} \to \mathrm{Spf}(\mathrm{O})$. In [**20**] faltings' defines the notion of a strict finite O-module G over S and the notion of a strict homomorphism between strict finite O-modules. We will not recall the definition but only say the following. A strict finite O-module is a finite locally free group scheme G over S, equipped with an action of O satisfying a certain strictness condition. The strictness condition on the O-action means that for each $a \in \mathrm{O}$, the endomorphism $a : \mathrm{G} \to \mathrm{G}$, can be lifted along a certain nilpotent thickening $\mathrm{G} \to \mathrm{G}^\flat$ in such a way that this lift acts by multiplication by a on the fibre of the cotangent complex of G/S at the origin. A homomorphism $f : \mathrm{G} \to \mathrm{G}'$ of strict finite O-modules is strict if it can be lifted to a map $\mathrm{G}^\flat \to \mathrm{G}'^\flat$ compatible with the lift of the O-action. We refer the reader to §2 of [**20**] for the precise definitions.

In any case, one obtains the category of strict finite O-modules and it is a sub-category of the category of finite locally free groups schemes over S equipped with an action of O. Moreover, if $\mathrm{S}' \to \mathrm{S}$ is a morphism and G/S is a strict finite O-module so is $\mathrm{G} \times_{\mathrm{S}} \mathrm{S}'$.

A.3.2 Example. — Every finite locally free étale group scheme over S equipped with an action of O is strict and every O-linear homomorphism either to or from an étale strict finite O-module is strict. This is explained by the fact that the cotangent complex of such a scheme is trivial.

For each $\mathfrak{p}$-adic affine scheme S and each Lubin–Tate module $\mathrm{F} \to \mathrm{Spf}(\mathrm{O})$, writing $\mathrm{F}_{\mathrm{S}} = \mathrm{F} \times_{\mathrm{Spf}(\mathrm{O})} \mathrm{S}$, the finite locally free group schemes $\mathrm{F}_{\mathrm{S}}[\mathfrak{p}^n]$ equipped with their O-action are naturally strict finite O-modules over S.

A.3.3. We now explain faltings' version of Cartier duality for strict finite O-modules. Let $\mathrm{F} = \mathrm{F}_\pi$ be the Lubin–Tate module over $\mathrm{Spf}(\mathrm{O})$ associated to the uniformiser $\pi \in \mathrm{O}$, so that

$$\pi : \mathrm{F} \to \mathrm{F}$$

lifts the $\mathrm{N}\mathfrak{p}$-power Frobenius map over $\mathrm{Spec}(\mathbf{F}) \to \mathrm{Spf}(\mathrm{O})$. Given a strict finite O-module G/S we define the sheaf of O-modules over S

$$\mathrm{D}_\pi(\mathrm{G}) = \operatorname*{colim}_r \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O},\mathrm{str}}(\mathrm{G}, \mathrm{F}_{\mathrm{S}}[\mathfrak{p}^r]).$$

Faltings then proves the following (see Theorem 8 of [**20**]):

A.3.4 Theorem. — *The functor*

$$\mathrm{G} \mapsto \mathrm{D}_\pi(\mathrm{G}) := \operatorname*{colim}_r \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O},\mathrm{str}}(\mathrm{G}, \mathrm{F}_{\pi/\mathrm{S}}[\mathfrak{p}^r])$$

defines a duality on the category strict finite O*-modules over* S *and is compatible with base change in* S*. Moreover, the degree of* $\mathrm{D}_\pi(\mathrm{G})$ *is equal to the degree of* G *and if* $f : \mathrm{G} \to \mathrm{G}'$ *is a strict homomorphism of strict finite* O*-modules over* S *then* $\mathrm{D}_\pi(f)$ *is a closed immersion (resp. faithfully flat) if and only if* f *is faithfully flat (resp. a closed immersion).*

A.3.5. Given a strict finite O-module G we call $\mathrm{D}_\pi(\mathrm{G})$ the dual of G.

If S has characteristic $\mathfrak{p}$ then for each strict finite O-module G the $\mathrm{N}\mathfrak{p}$-power relative Frobenius map

$$\mathrm{Fr}_{\mathrm{G/S}}^{\mathrm{N}\mathfrak{p}} : \mathrm{G} \to \mathrm{Fr}^{\mathrm{N}\mathfrak{p}*}(\mathrm{G})$$

is strict so that taking the dual of the $\mathrm{N}\mathfrak{p}$-power relative Frobenius map of the dual of G one obtains a map

$$\mathrm{V}_{\mathrm{G/S}} : \mathrm{Fr}^{\mathrm{N}\mathfrak{p}*}(\mathrm{G}) \to \mathrm{G}$$

and Faltings shows that the composition

$$\mathrm{G} \xrightarrow{\mathrm{Fr}_{\mathrm{G/S}}^{\mathrm{N}\mathfrak{p}}} \mathrm{Fr}^{\mathrm{N}\mathfrak{p}*}(\mathrm{G}) \xrightarrow{\mathrm{V}_{\mathrm{G/S}}} \mathrm{G}$$

is equal to the endomorphism $\pi : \mathrm{G} \to \mathrm{G}$ (see the paragraph of §7 [**20**]).

It is a formality to extend the duality $\mathrm{G} \mapsto \mathrm{D}_\pi(\mathrm{G})$ to a pair of functors defining inverse anti-equivalences between the categories of ind-strict finite O-modules and pro-strict finite O-modules.

The final observation we need to make is that if F/S is a Lubin–Tate O-module then the inclusions

$$\mathrm{F}[\mathfrak{p}^n] \to \mathrm{F}[\mathfrak{p}^{n+1}]$$

are strict so that we may view $\mathrm{F} = \mathrm{colim}_n \mathrm{F}[\mathfrak{p}^n]$ as an ind-strict O-module over S. Moreover, with this definition every homomorphism of Lubin–Tate O-modules over S is a morphism of ind-strict finite O-modules (this is a consequence of the formal smoothness of F).

A.3.6 Corollary. — *The functor from ind-strict finite* O*-modules to pro-strict finite* O*-modules*

$$\mathrm{F/S} \mapsto \lim_n \mathrm{D}_\pi(\mathrm{F}[\mathfrak{p}^n])$$

defines an anti-equivalence of categories between Lubin–Tate O*-modules over* S *and rank one* O*-local systems over* S *with quasi-inverse*

$$\mathscr{L} \mapsto \mathrm{F}_{\pi/\mathrm{S}} \otimes_{\mathrm{O}} \mathscr{L}^\vee.$$

Proof. — It is enough to show that given an ind-strict finite O-module G, the pro-strict finite O-module $\mathrm{D}_\pi(\mathrm{G})$ is a rank one O-local system if and only if G is a Lubin–Tate O-module. If $\mathrm{D}_\pi(\mathrm{G})$ is a rank one O-local system, as the functor D_π is compatible with base change and being a Lubin–Tate O-module is local on S we may assume that $\mathrm{D}_\pi(\mathrm{F}) \xrightarrow{\sim} \widehat{\mathrm{O}}_\mathrm{S}$. We then get $\mathrm{G} \xrightarrow{\sim} \mathrm{D}_\pi(\mathrm{D}_\pi(\mathrm{G})) \xrightarrow{\sim} \mathrm{D}_\pi(\widehat{\mathrm{O}}_\mathrm{S}) = \mathrm{F}_{\pi/\mathrm{S}}$ so that G is a Lubin–Tate O-module.

Conversely, let G be a Lubin–Tate O-module. We claim that $\mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^n])$ is étale for all $n \geq 0$. As $\mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^n])$ is finite locally free and S is $\mathfrak{p}$-adic, to show this we may assume that S has characteristic $\mathfrak{p}$. In this case, the composition

$$\mathrm{G} \overset{\mathrm{Fr}^{\mathrm{N}\mathfrak{p}}_{\mathrm{G/S}}}{\to} \mathrm{Fr}^{\mathrm{N}\mathfrak{p}*}(\mathrm{G}) = \mathrm{G} \otimes_{\mathrm{O}} \mathfrak{p}^{-1} \xrightarrow{1\otimes\pi} \mathrm{G}$$

is equal to π from which it follows that $\mathrm{V}_{\mathrm{G/S}}$ is an isomorphism. This implies that $\mathrm{V}_{\mathrm{G}[\mathfrak{p}^n]/\mathrm{S}}$ is an isomorphism for all $n \geq 0$, so that $\mathrm{D}(\mathrm{V}_{\mathrm{G}[\mathfrak{p}^n]/\mathrm{S}}) = \mathrm{Fr}^{\mathrm{N}\mathfrak{p}}_{\mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^n])/\mathrm{S}}$ is an isomorphism. Therefore $\mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^n])$ is étale and it follows that $\mathrm{D}_\pi(\mathrm{G}) = \lim_n \mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^n])$ is a pro-finite étale strict O-module scheme.

The exact sequences

$$0 \to \mathrm{G}[\mathfrak{p}^n] \to \mathrm{G}[\mathfrak{p}^{n+1}] \xrightarrow{\pi} \mathrm{G}[\mathfrak{p}^{n+1}]$$

now give exact sequences

$$\mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^{n+1}]) \xrightarrow{\pi} \mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^{n+1}]) \to \mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^n]) \to 0. \tag{A.3.6.1}$$

Localising, we may assume that $\mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^n])$ is a strict finite constant O-module for all $n \geq 0$. Then the short exact sequences (A.3.6.1) combined with the fact that $\deg(\mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^n])) = \mathrm{N}\mathfrak{p}^n$ for all $n \geq 0$, show inductively that there exists an isomorphism $\mathrm{D}_\pi(\mathrm{F}[\mathfrak{p}^n]) \xrightarrow{\sim} \underline{\mathrm{O}/\mathfrak{p}^n}_\mathrm{S}$ such that the maps

$$\mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^{n+1}]) \to \mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^n])$$

correspond to the reduction maps

$$\underline{\mathrm{O}/\mathfrak{p}^{n+1}}_\mathrm{S} \to \underline{\mathrm{O}/\mathfrak{p}^n}_\mathrm{S}.$$

Therefore,

$$\mathrm{D}_\pi(\mathrm{G}) = \lim_n \mathrm{D}_\pi(\mathrm{G}[\mathfrak{p}^n]) \xrightarrow{\sim} \lim_n \underline{\mathrm{O}/\mathfrak{p}^n} = \widehat{\mathrm{O}}_\mathrm{S}$$

is a rank one O-local system on S and this shows that D_π defines a contravariant equivalence between the category of Lubin-Tate O-modules and rank one O-local systems over S.

For the statement regarding the quasi-inverse, we have

$$\begin{aligned}
\mathrm{D}_\pi(\mathscr{L}) &= \operatorname*{colim}_n \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O},\mathrm{str}}(\mathscr{L}, \mathrm{F}_{\mathrm{S}}[\mathfrak{p}^n]) \\
&= \operatorname*{colim}_n \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O}}(\mathscr{L}, \mathrm{F}_{\mathrm{S}}[\mathfrak{p}^n]) \\
&= \operatorname*{colim}_n \underline{\mathrm{Hom}}_{\mathrm{S}}(\widehat{\mathrm{O}}_{\mathrm{S}}, \mathrm{F}_{\mathrm{S}}[\mathfrak{p}^n] \otimes_{\mathrm{O}} \mathscr{L}^\vee) \\
&= \operatorname*{colim}_n \mathrm{F}_{\mathrm{S}}[\mathfrak{p}^n] \otimes_{\mathrm{O}} \mathscr{L}^\vee \\
&= \mathrm{F}_{\mathrm{S}} \otimes_{\mathrm{O}} \mathscr{L}^\vee.
\end{aligned}$$

□

A.3.7 Corollary. — *Let* S *be a* $\mathfrak{p}$*-adic sheaf.*

(i) *If* F/S *is a Lubin–Tate* O*-module the natural homomorphism*

$$\widehat{\mathrm{O}}_{\mathrm{S}} \to \underline{\mathrm{End}}_{\mathrm{S}}^{\mathrm{O}}(\mathrm{F})$$

is an isomorphism.

(ii) *If* $\mathrm{F}, \mathrm{F}'/\mathrm{S}$ *are a pair of Lubin–Tate* O*-modules over* S *then* $\underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O}}(\mathrm{F}, \mathrm{F}')$ *is an* O*-local system over* S *and the evaluation homomorphism*

$$\mathrm{F} \otimes_{\mathrm{O}} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O}}(\mathrm{F}, \mathrm{F}') \to \mathrm{F}'$$

is an isomorphism.

(iii) *The functor*

$$\mathscr{M}_{\mathrm{LT}} \times \mathscr{C}\mathscr{L}_{\mathrm{O}} \to \mathscr{M}_{\mathrm{LT}} \times \mathscr{M}_{\mathrm{LT}} : (\mathrm{F}, \mathscr{L}) \mapsto (\mathrm{F}, \mathrm{F} \otimes_{\mathrm{O}} \mathscr{L})$$

is an equivalence of stacks.

Proof. — (i) For any rank one O-local system we have $\widehat{\mathrm{O}}_{\mathrm{S}} \xrightarrow{\sim} \underline{\mathrm{End}}_{\mathrm{S}}^{\mathrm{O}}(\mathscr{L})$ so that the composition

$$\widehat{\mathrm{O}}_{\mathrm{S}} \to \underline{\mathrm{End}}_{\mathrm{S}}^{\mathrm{O}}(\mathrm{F}) \xrightarrow{\sim} \underline{\mathrm{End}}_{\mathrm{S}}^{\mathrm{O}}(\mathrm{D}_\pi(\mathrm{F}))$$

is an isomorphism and therefore $\widehat{\mathrm{O}}_{\mathrm{S}} \to \underline{\mathrm{End}}_{\mathrm{S}}^{\mathrm{O}}(\mathrm{F})$ is an isomorphism.

(ii) We may assume that $\mathrm{F}' = \mathrm{F} \otimes_{\mathrm{O}} \mathscr{L}$. Then (i) combined with (1.2.8) gives

$$\mathscr{L} \xrightarrow{\sim} \underline{\mathrm{Hom}}_{\mathrm{S}}(\mathrm{F}, \mathrm{F} \otimes_{\mathrm{O}} \mathscr{L}).$$

Moreover, using this identification the evaluation homomorphism

$$\mathrm{F} \otimes_{\mathrm{O}} \mathscr{L} = \mathrm{F} \otimes_{\mathrm{O}} \underline{\mathrm{Hom}}_{\mathrm{S}}^{\mathrm{O}}(\mathrm{F}, \mathrm{F} \otimes_{\mathrm{O}} \mathscr{L}) \to \mathrm{F}' = \mathrm{F} \otimes_{\mathrm{O}} \mathscr{L}$$

becomes the identity.

(iii) The functor in question is the product of the equivalences $\mathrm{id}_{\mathscr{M}_{\mathrm{LT}}}$ and $\mathscr{L} \mapsto \mathrm{D}_\pi(\mathscr{L}^\vee)$ and is therefore an equivalence. □

A.4. A principal ideal theorem

In this section we would like to prove a strengthening of an old principal ideal theorem (see Tannaka [**35**]). We first state a special case for imaginary quadratic fields (A.4.1) as it is possible to do so without having to make any new definitions and it is the only case we need in main the text. We shall then prove the general result (A.4.8) for arbitrary number fields K and explain how it strengthens the result in [**35**].

The author would like to point out that while the result is new, our proof is really just a refinement of Tannaka's, essentially a combination of his proof, some very old results in class field theory, and a result of one of his contemporaries (see Terada [**36**]). It is also interesting to point out that Tannaka was motivated to prove his result by Deuring who had conjectured it, presumably inspired during his work on CM elliptic curves.

A.4.1 Proposition. — *Let* K *be an imaginary quadratic field, let* $\mathrm{K}(\mathfrak{f})/\mathrm{K}$ *be the ray class field of conductor* $\mathfrak{f}$*, let* $\mathfrak{g}$ *be an ideal divisible by* $\mathfrak{f}$ *and let*

$$l : \mathrm{Prin}^{(\mathfrak{g})}_{1 \bmod \mathfrak{f}} \to \mathrm{K}^\times : \mathfrak{a} \mapsto l(\mathfrak{a})$$

be a homomorphism such that $l(\mathfrak{a}) \cdot \mathrm{O}_\mathrm{K} = \mathfrak{a} \subset \mathrm{K}$ *and such that* $l(\mathfrak{a}) = 1 \bmod \mathfrak{f}$*. Then* l *can be extended to a map*

$$l : \mathrm{Id}^{(\mathfrak{g})}_{\mathrm{O}_\mathrm{K}} \to \mathrm{K}(\mathfrak{f})^\times : \mathfrak{a} \mapsto l(\mathfrak{a})$$

such that $l(\mathfrak{a}) \cdot \mathrm{O}_{\mathrm{K}(\mathfrak{f})} = \mathfrak{a} \cdot \mathrm{O}_{\mathrm{K}(\mathfrak{f})}$ *and such that for all* $\mathfrak{a}, \mathfrak{b} \in \mathrm{Id}^{(\mathfrak{g})}_{\mathrm{O}_\mathrm{K}}$ *we have*

$$l(\mathfrak{a}\mathfrak{b}) = l(\mathfrak{a})\sigma_\mathfrak{a}(l(\mathfrak{b})).$$

A.4.2. Let K be a number field with ring of integers O_K. Recall by a modulus of K is meant a finite formal sum

$$\mathfrak{f} = \sum_v \mathfrak{f}_v v$$

over the places v of K such that $\mathfrak{f}_v \in \mathbf{N}$ for all v and such that $\mathfrak{f}_v \in \{0, 1\}$ for v infinite and real and $\mathfrak{f}_v = 0$ for v infinite and complex. If $\mathfrak{f}$ and $\mathfrak{f}'$ are moduli of K then their product $\mathfrak{f}\mathfrak{f}'$ is defined by $(\mathfrak{f}\mathfrak{f}')_v = \mathfrak{f}_v + \mathfrak{f}_{v'}$ for all finite places v and $(\mathfrak{f}\mathfrak{f}')_v = \max(\mathfrak{f}_v, \mathfrak{f}'_v)$ for all infinite primes v. We say $\mathfrak{f}$ divides $\mathfrak{f}'$ if $\mathfrak{f}_v \leq \mathfrak{f}'_v$ for all places v. If $\mathfrak{f}_v = 0$ for all infinite v then we identify $\mathfrak{f}$ with an ideal of O_K in the usual way.

If $a \in \mathrm{K}^\times$ we write $a = 1 \bmod \mathfrak{f}$ to mean that $v(a-1) \geq \mathfrak{f}_v$ for all finite places v and such that $a > 0$ for all infinite real places v of K with $\mathfrak{f}_v \neq 0$. For a pair of fractional ideals $\mathfrak{a}, \mathfrak{b}$ of K we write $\mathfrak{a} = \mathfrak{b} \bmod \mathfrak{f}$ to mean that $\mathfrak{a}\mathfrak{b}^{-1} = (a)$ with $a = 1 \bmod \mathfrak{f}$.

For each modulus $\mathfrak{f}$ there is a certain extension $\mathrm{K}(\mathfrak{f})/\mathrm{K}$ called the ray class field of conductor $\mathfrak{f}$ which is unramified at all finite places v of K with $\mathfrak{f}_v = 0$. This extension is characterised by the property that if $\mathfrak{g}$ is any ideal of K

divisible by (the finite part of) $\mathfrak{f}$ and $\mathrm{Id}_{\mathrm{K}}^{(\mathfrak{g})}$ denotes the group of fractional ideals prime to $\mathfrak{g}$ then the map

$$\mathrm{Id}_{\mathrm{K}}^{(\mathfrak{g})} \to \mathrm{G}(\mathrm{K}(\mathfrak{f})/\mathrm{K}) : \mathfrak{a} \mapsto \sigma_{\mathfrak{a}} \tag{A.4.2.1}$$

is surjective and its kernel is equal to $\mathrm{Prin}_{1 \bmod \mathfrak{f}}^{(\mathfrak{g})} \subset \mathrm{Id}_{\mathrm{K}}^{(\mathfrak{g})}$, the sub-group generated by ideals $\mathfrak{a}$ prime to (the finite part of) $\mathfrak{g}$ with $\mathfrak{a} = \mathrm{O}_{\mathrm{K}} \bmod \mathfrak{f}$.

We now recall certain moduli defined for a finite abelian extension of number fields L/K (see §1 of [**36**] for precise details). We write $\mathfrak{f}_{\mathrm{L/K}}$, $\mathfrak{D}_{\mathrm{L/K}}$ and $\mathfrak{G}_{\mathrm{L/K}}$ for conductor, different and genus ideal ('Geschlechtermodul') of the extension L/K which are moduli for K, L and K respectively and we have

$$\mathfrak{f}_{\mathrm{L/K}} = \mathfrak{D}_{\mathrm{L/K}}\mathfrak{G}_{\mathrm{L/K}}.$$

The moduli $\mathfrak{f}_{\mathrm{L/K}}$, $\mathfrak{D}_{\mathrm{L/K}}$ are not necessarily ideals however $\mathfrak{G}_{\mathrm{L/K}}$ is always an ideal of O_{L}. Finally, if L/K′/K is an intermediate extension we define $\mathfrak{f}_{\mathrm{L/K'/K}} = \mathfrak{D}_{\mathrm{L/K'}}\mathfrak{G}_{\mathrm{L/K}}$ which is an integral ideal of K′. We note that $\mathfrak{f}_{\mathrm{L/K}}$, $\mathfrak{G}_{\mathrm{L/K}}$, and $\mathfrak{f}_{\mathrm{L/K'/K}}$ are all invariant under G(L/K).

Finally, for what follows we will use exponential notation for the action of Galois groups on elements or fractional ideals of the respective fields.

A.4.3 Theorem **(Hasse's Norm Theorem)**. — *Let* L/K *be a finite cyclic extension. Then* $\mathrm{N}_{\mathrm{L/K}}(\mathrm{I}_{\mathrm{L}}) \cap \mathrm{K}^{\times} = \mathrm{N}_{\mathrm{L/K}}(\mathrm{L}^{\times})$.

A.4.4 Theorem **(Principal Genus Theorem)**. — *Let* L/K *be a finite cyclic extension with generator* $\sigma \in \mathrm{G}(\mathrm{L/K})$ *and let* $\mathfrak{a}$ *be a fractional ideal of* L. *Then* $\mathrm{N}_{\mathrm{L/K}}(\mathfrak{a}) = \mathrm{O}_{\mathrm{K}}$ *if and only if* $\mathfrak{a} = \mathfrak{b}^{1-\sigma}$ *for some fractional ideal* $\mathfrak{b}$ *of* L.

Proof. — As G(L/K) is cyclic and generated by σ we have

$$\frac{\{\mathfrak{a} \in \mathrm{Id}_{\mathrm{L}} : \mathfrak{a}\mathfrak{a}^{\sigma} \cdots \mathfrak{a}^{\sigma^{n-1}} = \mathrm{O}_{\mathrm{L}}\}}{\mathrm{Id}_{\mathrm{L}}^{1-\sigma}} \xrightarrow{\sim} \mathrm{H}^1(\mathrm{G}(\mathrm{L/K}), \mathrm{Id}_{\mathrm{L}}) : \mathfrak{a} \mapsto (\sigma^i \mapsto \mathfrak{a}\mathfrak{a}^{\sigma} \cdots \mathfrak{a}^{\sigma^{i-1}})$$

and by Proposition 6, §13, Chapter V of [**25**] the group $\mathrm{H}^1(\mathrm{G}(\mathrm{L/K}), \mathrm{Id}_{\mathrm{L}})$ vanishes which is precisely the claim. □

A.4.5 Theorem **(Terada's Norm Theorem)**. — *Let* L/K *be a finite cyclic extension with generator* $\sigma \in \mathrm{G}(\mathrm{L/K})$, *let* $a \in \mathrm{K}$ *and let* $\mathfrak{m}$ *be an ideal of* O_{L}. *Then the following are equivalent:*

(i) $\mathrm{N}_{\mathrm{L/K}}(a) = 1 \bmod \mathfrak{f}_{\mathrm{L/K}}\mathfrak{m}$.
(ii) $a = b^{1-\sigma} \bmod \mathfrak{G}_{\mathrm{L/K}}\mathfrak{m}$ *for some* $b \in \mathrm{L}$.

Proof. — This is Theorem 2 of [**36**]. □

A.4.6. Now let L/K be the ray class field of conductor $\mathfrak{f}_{\mathrm{L/K}}$ and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be prime ideals of K, unramified in L/K and such that

$$\mathrm{G(L/K)} = \bigoplus_{i=1}^{r} \langle \sigma_i \rangle$$

where σ_i is the Frobenius element corresponding to $\mathfrak{p}_i$ (we can do this by (A.4.2.1)). Also, for $1 \leq i \leq n$ let n_i be the order of σ_i and let $\mathrm{K}_i \subset \mathrm{L}$ be the sub-extension fixed by the sub-group of G(L/K) generated by $\{\sigma_j\}_{j \neq i}$. We note that $\mathrm{G(K}_i\mathrm{/K}) \xrightarrow{\sim} \langle \sigma_i \rangle$.

***A.4.7 Theorem* (Tannaka).** — *For $1 \leq i \leq r$ let $\mathfrak{a}_i$ be a fractional ideal of K_i such that $\mathfrak{p}_i = \mathfrak{a}_i^{1-\sigma_i} \bmod \mathfrak{f}_{\mathrm{L/K}_i/\mathrm{K}}$. Then $\mathfrak{a}_1 \cdots \mathfrak{a}_r = \mathrm{O_L} \bmod \mathfrak{G}_{\mathrm{L/K}}$.*

Proof. — This is Theorem 3 of [**35**]. □

A.4.8 Theorem. — *Let* K *be a number field, let* L/K *be the ray class field of conductor $\mathfrak{f}_{\mathrm{L/K}}$, let $\mathfrak{g}$ be an ideal divisible by (the finite part of) $\mathfrak{f}_{\mathrm{L/K}}$ and let*

$$l : \mathrm{Prin}^{(\mathfrak{g})}_{1 \bmod \mathfrak{f}_{\mathrm{L/K}}} \to \mathrm{K}^\times : \mathfrak{a} \mapsto l(\mathfrak{a})$$

be a homomorphism such that $l(\mathfrak{a}) \cdot \mathrm{O_K} = \mathfrak{a} \subset \mathrm{K}$ and such that $l(\mathfrak{a}) = 1 \bmod \mathfrak{f}_{\mathrm{L/K}}$. Then l can be extended to a map

$$l : \mathrm{Id}^{(\mathfrak{g})}_{\mathrm{O_K}} \to \mathrm{L}^\times : \mathfrak{a} \mapsto l(\mathfrak{a})$$

such that:

(i) $l(\mathfrak{a}) \cdot \mathrm{O_L} = \mathfrak{a} \cdot \mathrm{O_L}$,
(ii) $l(\mathfrak{a}) = 1 \bmod \mathfrak{G}_{\mathrm{L/K}}$, *and*
(iii) *for all $\mathfrak{a}, \mathfrak{b} \in \mathrm{Id}^{(\mathfrak{g})}_{\mathrm{O_K}}$ we have*

$$l(\mathfrak{ab}) = l(\mathfrak{a})\sigma_{\mathfrak{a}}(l(\mathfrak{b})).$$

Proof. — For each $1 \leq i \leq r$ let us make the following constructions. As $\mathfrak{p}_i^{n_i} \in \mathrm{Prin}^{(\mathfrak{g})}_{1 \bmod \mathfrak{f}_{\mathrm{L/K}}}$ we have $l(\mathfrak{p}_i^{n_i}) = 1 \bmod \mathfrak{f}_{\mathrm{L/K}}$ and a fortiori $l(\mathfrak{p}_i^{n_i}) = 1 \bmod \mathfrak{f}_{\mathrm{K}_i/\mathrm{K}}$ so that $l(\mathfrak{p}_i^{n_i}) \in \mathrm{N}_{\mathrm{K}_i/\mathrm{K}}(\mathrm{I}_{\mathrm{K}_i})$. By Hasse's Norm Theorem, there is some $\pi_i \in \mathrm{K}_i$ with $\mathrm{N}_{\mathrm{K}_i/\mathrm{K}}(\pi_i) = l(\mathfrak{p}_i^{n_i})$. By construction we have

$$\mathrm{N}_{\mathrm{K}_i/\mathrm{K}}(\mathfrak{p}_i(\pi_i)^{-1}) = \mathfrak{p}_i^{n_i}\mathfrak{p}_i^{-n_i} = \mathrm{O_K}$$

so that, by the Principal Genus Theorem, we can find an ideal $\mathfrak{b}_i$ of K_i with

$$\mathfrak{p}_i(\pi_i)^{-1} = \mathfrak{b}_i^{1-\sigma_i}.$$

We note that

$$\mathfrak{f}_{\mathrm{L/K}_i/\mathrm{K}} = \mathfrak{G}_{\mathrm{K}_i/\mathrm{K}}(\mathfrak{f}_{\mathrm{L/K}}\mathfrak{f}^{-1}_{\mathrm{K}_i/\mathrm{K}})$$

so that

$$\mathrm{N}_{\mathrm{K}_i/\mathrm{K}}(\pi_i) = l(\mathfrak{p}_i^{f_i}) = 1 \bmod \mathfrak{f}_{\mathrm{L/K}} = 1 \bmod \mathfrak{f}_{\mathrm{K}_i/\mathrm{K}}(\mathfrak{f}_{\mathrm{L/K}}\mathfrak{f}^{-1}_{\mathrm{K}_i/\mathrm{K}}).$$

We now apply Terada's Norm Theorem (with $\mathfrak{m} = \mathfrak{f}_{\mathrm{L/K}}\mathfrak{f}_{\mathrm{K}_i/\mathrm{K}}^{-1}$) to find $\alpha_i \in \mathrm{K}_i$ with $\alpha_i = 1 \bmod \mathfrak{f}_{\mathrm{L/K}_i/\mathrm{K}}$ and $\pi_i = \alpha_i\beta_i^{1-\sigma_i}$ and

$$\mathrm{N}_{\mathrm{K}_i/\mathrm{K}}(\pi_i) = \mathrm{N}_{\mathrm{K}_i/\mathrm{K}}(\alpha_i\beta_i^{1-\sigma_i}) = \mathrm{N}_{\mathrm{K}_i/\mathrm{K}}(\alpha_i) = l(\mathfrak{p}_i^{n_i}). \tag{A.4.8.1}$$

Finally, we set $\mathfrak{a}_i = (\beta_i)\mathfrak{b}_i$ to get

$$\mathfrak{p}_i = (\alpha_i)\mathfrak{a}_i^{1-\sigma_i} \quad \text{and so} \quad \mathfrak{p}_i = \mathfrak{a}_i^{1-\sigma_i} \bmod \mathfrak{f}_{\mathrm{L/K}_i/\mathrm{K}}.$$

The ideals $\mathfrak{a}_i$ for $1 \leq i \leq r$ satisfy the conditions of Tannaka's Theorem and so we find an $\mathrm{A} \in \mathrm{L}$ with $\mathrm{A} = 1 \bmod \mathfrak{G}_{\mathrm{L/K}}$ with

$$\prod_{1\leq i\leq m} \mathfrak{a}_i = (\mathrm{A}).$$

Finally, we set

$$\Theta_i = \alpha_i \mathrm{A}^{1-\sigma_i}$$

and note that $\Theta_i \cdot \mathrm{O_L} = \mathfrak{p}_i$.

We now go about extending the map l, following rather closely the method of §1 of [**35**]. Each $\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}^{(\mathfrak{g})}$ can be written uniquely as a product of ideals

$$\mathfrak{a} = \gamma(\mathfrak{a}) \cdot \prod_{i=1}^{r} \mathfrak{p}_i^{x_i} \tag{A.4.8.2}$$

with $\gamma(\mathfrak{a}) \in \mathrm{Prin}_{1 \bmod \mathfrak{f}_{\mathrm{L/K}}}^{(\mathfrak{g})}$ and $0 \leq x_i < n_i$. Before we continue let us note the following multiplicative relations for the ideals $\gamma(\mathfrak{a})$:

(i) If $\mathfrak{b} \in \mathrm{Prin}_{1 \bmod \mathfrak{f}_{\mathrm{L/K}}}^{(\mathfrak{g})}$ then

$$\gamma(\mathfrak{a}\mathfrak{b}) = \gamma(\mathfrak{a})\gamma(\mathfrak{b}). \tag{A.4.8.3}$$

(ii) If $\mathfrak{b} = \mathfrak{p}_j$ and $x_j \neq n_j - 1$ then

$$\gamma(\mathfrak{p}_j) = \mathrm{O_K} \quad \text{and} \quad \gamma(\mathfrak{a}\mathfrak{p}_j) = \gamma(\mathfrak{a}). \tag{A.4.8.4}$$

(iii) If $\mathfrak{b} = \mathfrak{p}_j$ and $x_j = n_j - 1$ then

$$\gamma(\mathfrak{a}\mathfrak{p}_j) = \gamma(\mathfrak{a})\gamma(\mathfrak{p}_j^{n_j}). \tag{A.4.8.5}$$

Still following §1 of [**35**] we now define $l(\mathfrak{a})$ by

$$l(\mathfrak{a}) = l(\gamma(\mathfrak{a})) \prod_{i=1}^{n} \Theta_i^{w_i(x_i)} = l(\gamma(\mathfrak{a}))\mathrm{A}^{\sigma_{\mathfrak{a}}-1} \prod_{i=1}^{r} \alpha_i^{1+\sigma_i+\cdots+\sigma_i^{x_i-1}}$$

where

$$w_i(x_i) = \left(\sum_{j=1}^{x_i} \sigma_{\mathfrak{p}_i}^j\right) \cdot \prod_{k=1}^{i-1} \sigma_{\mathfrak{p}_k}^{x_k}.$$

It is clear that $l(\mathfrak{a}) \cdot \mathrm{O_L} = \mathfrak{a} \cdot \mathrm{O}_{\mathrm{K}(\mathfrak{a})}$ and that this map does indeed extend the given map l. Moreover, by construction we have the relations

$$\mathrm{A} = 1 \bmod \mathfrak{G}_{\mathrm{L/K}} \qquad l(\mathfrak{a}) = 1 \bmod \mathfrak{f}_{\mathrm{L/K}} \qquad \alpha_i = 1 \bmod \mathfrak{f}_{\mathrm{L/K}_i/\mathrm{K}},$$

so that as $\mathfrak{G}_{\mathrm{L/K}}$ divides both $\mathfrak{f}_{\mathrm{L/K}}$ and $\mathfrak{f}_{\mathrm{L/K}_i/\mathrm{K}}$, and as $\mathfrak{G}_{\mathrm{L/K}}$, $\mathfrak{f}_{\mathrm{L/K}}$ and $\mathfrak{f}_{\mathrm{L/K}_i/\mathrm{K}}$ are invariant under the action of $\mathrm{G(L/K)}$, we get the relation

$$l(\mathfrak{a}) = 1 \bmod \mathfrak{G}_{\mathrm{L/K}}.$$

All that remains to be shown is that $l(\mathfrak{ab}) = l(\mathfrak{a})\sigma_{\mathfrak{a}}(l(\mathfrak{b}))$ for $\mathfrak{a}, \mathfrak{b} \in \mathrm{Id}_{\mathrm{O_K}}^{(\mathfrak{g})}$.

So let $\mathfrak{b} \in \mathrm{Id}_{\mathrm{O_K}}^{(\mathfrak{g})}$ be another fractional ideal, and also write

$$\mathfrak{b} = \gamma(\mathfrak{b}) \cdot \prod_{i=1}^{r} \mathfrak{p}_i^{y_i} \quad \text{and} \quad \mathfrak{ab} = \gamma(\mathfrak{ab}) \cdot \prod_{i=1}^{r} \mathfrak{p}_i^{z_i}$$

where $\gamma(\mathfrak{b}), \gamma(\mathfrak{ab}) \in \mathrm{Prin}_{1 \bmod \mathfrak{f}_{\mathrm{L/K}}}^{(\mathfrak{g})}$ and $0 \leq y_i, z_i < n_i$. Define $\delta_i \in \{0, 1\}$ for $1 \leq i \leq r$ by the equality

$$z_i = x_i + y_i - \delta_i n_i.$$

Then one finds (see equation (9) of [**35**])

$$\frac{l(\mathfrak{a})\sigma_{\mathfrak{a}}(l(\mathfrak{b}))}{l(\mathfrak{ab})} = \frac{l(\gamma(\mathfrak{a}))l(\gamma(\mathfrak{b}))}{l(\gamma(\mathfrak{ab}))} \cdot \prod_{i=1}^{r} \mathrm{N}_{\mathrm{K}_i/\mathrm{K}}(\alpha_i)^{\delta_i}. \tag{A.4.8.6}$$

It remains to check that the right hand side of (A.4.8.6) is equal to one for all ideals $\mathfrak{b}$. The group $\mathrm{Id}_{\mathrm{O_K}}^{(\mathfrak{g})}$ is generated (as a monoid!) by $\mathrm{Prin}_{1 \bmod \mathfrak{f}_{\mathrm{L/K}}}^{(\mathfrak{g})}$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ so that by induction, it is enough to check that $l(\mathfrak{ab}) = l(\mathfrak{a})\sigma_{\mathfrak{a}}(l(\mathfrak{b}))$ when $\mathfrak{b} \in \mathrm{Prin}_{1 \bmod \mathfrak{f}_{\mathrm{L/K}}}^{(\mathfrak{g})}$ or when $\mathfrak{b} = \mathfrak{p}_j$ for $1 \leq j \leq r$. If $\mathfrak{b} \in \mathrm{Prin}_{1 \bmod \mathfrak{f}_{\mathrm{L/K}}}^{(\mathfrak{g})}$ then $\delta_i = 0$ for $1 \leq i \leq r$ and by (A.4.8.3) we have $\gamma(\mathfrak{a})\gamma(\mathfrak{b}) = \gamma(\mathfrak{ab})$ so that

$$\frac{l(\gamma(\mathfrak{a}))l(\gamma(\mathfrak{b}))}{l(\gamma(\mathfrak{ab}))} \prod_{i=1}^{r} \mathrm{N}_{\mathrm{K}_i/\mathrm{K}}(\alpha_i)^{\delta_i} = 1.$$

If $\mathfrak{b} = \mathfrak{p}_j$ and $x_j \neq n_j - 1$ then $\delta_i = 0$ for $1 \leq i \leq r$ and by (A.4.8.4) we have $\gamma(\mathfrak{p}_j) = \mathrm{O_K}$ and $\gamma(\mathfrak{ap}_j) = \gamma(\mathfrak{a})$ so that

$$\frac{l(\gamma(\mathfrak{a}))l(\gamma(\mathfrak{b}))}{l(\gamma(\mathfrak{ab}))} \prod_{i=1}^{r} \mathrm{N}_{\mathrm{K}_i/\mathrm{K}}(\alpha_i)^{\delta_i} = 1.$$

Finally, if $\mathfrak{b} = \mathfrak{p}_j$ and $x_j = n_j - 1$ then $\delta_i = 0$, unless $i = j$ in which case $\delta_j = 1$, so that

$$\prod_{i=1}^{r} \mathrm{N}_{\mathrm{K}_i/\mathrm{K}}(\alpha_i)^{\delta_i} = \mathrm{N}_{\mathrm{K}_j/\mathrm{K}}(\alpha_j) = l(\gamma(\mathfrak{p}_j^{n_j}))$$

by (A.4.8.1). By (A.4.8.5) we have $\gamma(\mathfrak{ap}_j) = \gamma(\mathfrak{a})\gamma(\mathfrak{p}_j^{n_j})$ so that

$$\frac{l(\gamma(\mathfrak{a}))l(\gamma(\mathfrak{b}))}{l(\gamma(\mathfrak{ab}))} \prod_{i=1}^{r} \mathrm{N}_{\mathrm{K}_i/\mathrm{K}}(\alpha_i)^{\delta_i} = l(\gamma(\mathfrak{p}_j^{n_j}))^{-1} l(\gamma(\mathfrak{p}_j^{n_j})) = 1.$$

Therefore, for all $\mathfrak{a}, \mathfrak{b} \in \mathrm{Id}_{\mathrm{O_K}}^{(\mathfrak{g})}$ we have $l(\mathfrak{ab}) = l(\mathfrak{a})\sigma_{\mathfrak{a}}(l(\mathfrak{b}))$. □

A.4.9 Remark. — Let us now explain how (A.4.8) strengthens the main result of [**35**]. The result in question is Theorem 1 of [**35**] and it states (we continue to use the notation of (A.4.8))

***Theorem* (Tannaka's Principal Ideal Theorem)**. — *There exist numbers* $\Theta(\mathfrak{a}) \in \mathrm{L}$, *indexed by ideals* $\mathfrak{a} \in \mathrm{Id}_{\mathrm{O_K}}$, *such that the following hold:*

(i) $\Theta(\mathfrak{a}) \cdot \mathrm{O_L} = \mathfrak{a} \cdot \mathrm{O_L}$,
(ii) $\Theta(\mathfrak{a}) = 1 \bmod \mathfrak{G}_{\mathrm{L/K}}$, *and*
(iii)

$$\frac{\Theta(\mathfrak{a})\sigma_{\mathfrak{a}}(\Theta(\mathfrak{b}))}{\Theta(\mathfrak{ab})} \in \mathrm{O_K^\times}.$$

It is now an easy to replace (iii) of Tannaka's Principal Ideal Theorem with

$$\frac{\Theta(\mathfrak{a})\sigma_{\mathfrak{a}}(\Theta(\mathfrak{b}))}{\Theta(\mathfrak{ab})} = 1.$$

Consider the sub-group

$$\mathrm{Prin}^{(\mathfrak{f}_{\mathrm{L/K}})}_{1 \bmod \mathfrak{f}_{\mathrm{L/K}}} \subset \mathrm{Id}^{(\mathfrak{f}_{\mathrm{L/K}})}_{\mathrm{K}}.$$

As $\mathrm{Id}^{(\mathfrak{f}_{\mathrm{L/K}})}_{\mathrm{K}}$ is free abelian (generated by the prime ideals prime to $\mathfrak{f}_{\mathrm{L/K}}$) and every sub-group of a free abelian group is itself free abelian, one can define a multiplicative map

$$\mathrm{Prin}^{(\mathfrak{f}_{\mathrm{L/K}})}_{1 \bmod \mathfrak{f}_{\mathrm{L/K}}} \to \mathrm{K}^\times : \mathfrak{a} \mapsto l(\mathfrak{a})$$

such that $l(\mathfrak{a}) \cdot \mathrm{O_K} = \mathfrak{a}$ and such that $l(\mathfrak{a}) = 1 \bmod \mathfrak{f}_{\mathrm{L/K}}$. Applying (A.4.8) to the map l we find a map

$$l : \mathrm{Id}^{(\mathfrak{f}_{\mathrm{L/K}})}_{\mathrm{O_K}} \to \mathrm{L}^\times : \mathfrak{a} \mapsto l(\mathfrak{a})$$

such that $l(\mathfrak{a}) \cdot \mathrm{O_L} = \mathfrak{a} \cdot \mathrm{O_L}$, $l(\mathfrak{a}) = 1 \bmod \mathfrak{G}_{\mathrm{L/K}}$ and such that

$$\frac{l(\mathfrak{a})\sigma_{\mathfrak{a}}(l(\mathfrak{b}))}{l(\mathfrak{ab})} = 1.$$

Therefore, putting $l(\mathfrak{a}) = \Theta(\mathfrak{a})$ we can replace (iii) of Tannaka's Principal Ideal Theorem with

$$\frac{\Theta(\mathfrak{a})\sigma_{\mathfrak{a}}(\Theta(\mathfrak{b}))}{\Theta(\mathfrak{ab})} = 1.$$

BIBLIOGRAPHY

[1] *Algebraic number theory* – Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich, Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967.

[2] *Schémas en groupes. I: Propriétés générales des schémas en groupes* – Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 151, Springer-Verlag, Berlin-New York, 1970.

[3] *Revêtements étales et groupe fondamental* – Springer-Verlag, Berlin-New York, 1971, Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1), Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud, Lecture Notes in Mathematics, Vol. 224.

[4] J. Borger – "The basic geometry of Witt vectors, I: The affine case", *Algebra Number Theory* **5** (2011), no. 2, p. 231–285.

[5] ———, "The basic geometry of Witt vectors. II: Spaces", *Math. Ann.* **351** (2011), no. 4, p. 877–933.

[6] ———, "Sheaves in lambda-algebraic geometry", preprint, 2012.

[7] J. Borger & B. de Smit – "Lambda actions of rings of integers", preprint, arXiv:1105.4662.

[8] ———, "Galois theory and integral models of Λ-rings", *Bull. Lond. Math. Soc.* **40** (2008), no. 3, p. 439–446.

[9] S. Bosch, W. Lütkebohmert & M. Raynaud – *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990.

[10] A. Buium – "Differential characters of abelian varieties over p-adic fields", *Invent. Math.* **122** (1995), no. 2, p. 309–340.

[11] ———, *Arithmetic differential equations*, Mathematical Surveys and Monographs, vol. 118, American Mathematical Society, Providence, RI, 2005.

[12] C.-L. Chai, B. Conrad & F. Oort – *Complex multiplication and lifting problems*, Mathematical Surveys and Monographs, vol. 195, American Mathematical Society, Providence, RI, 2014.

[13] J. Coates & A. Wiles – "On the conjecture of Birch and Swinnerton-Dyer", *Invent. Math.* **39** (1977), no. 3, p. 223–251.

[14] J. Cougnard & V. Fleckinger – "Sur la monogénéité de l'anneau des entiers de certains corps de rayon", *Manuscripta Math.* **63** (1989), no. 3, p. 365–376.

[15] P. Deligne – "Courbes elliptiques: formulaire d'après J. Tate", Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, p. 53–73. Lecture Notes in Math., Vol. 476.

[16] P. Deligne – "Formes modulaires et représentations l-adiques", Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Math., vol. 175, Springer, Berlin, 1971, p. Exp. No. 355, 139–172.

[17] C. Deninger – "Higher regulators and Hecke L-series of imaginary quadratic fields. I", *Invent. Math.* **96** (1989), no. 1, p. 1–69.

[18] V. G. Drinfel′d – "Elliptic modules", *Mat. Sb. (N.S.)* **94(136)** (1974), p. 594–627, 656.

[19] ———, "Coverings of p-adic symmetric domains", *Funkcional. Anal. i Priložen.* **10** (1976), no. 2, p. 29–40.

[20] G. Faltings – "Group schemes with strict o-action", *Mosc. Math. J.* **2** (2002), no. 2, p. 249–279, Dedicated to Yuri I. Manin on the occasion of his 65th birthday.

[21] G. Faltings & C.-L. Chai – *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 22, Springer-Verlag, Berlin, 1990, With an appendix by David Mumford.

[22] B. H. Gross – "Minimal models for elliptic curves with complex multiplication", *Compositio Math.* **45** (1982), no. 2, p. 155–164.

[23] A. Grothendieck – "Géométrie formelle et géométrie algébrique", Séminaire Bourbaki, Vol. 5, Soc. Math. France, Paris, 1995, p. Exp. No. 182, 193–220, errata p. 390.

[24] N. M. Katz & B. Mazur – *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.

[25] F. Lemmermeyer – "The development of the principal genus theorem", The shaping of arithmetic after C. F. Gauss's *D*isquisitiones arithmeticae, Springer, Berlin, 2007, p. 529–561.

[26] J. Lubin – "One-parameter formal Lie groups over $\mathfrak{p}$-adic integer rings", *Ann. of Math. (2)* **80** (1964), p. 464–484.

[27] W. Messing – *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, Lecture Notes in Mathematics, Vol. 264, Springer-Verlag, Berlin-New York, 1972.

[28] G. Robert – "Sur le corps de définition de certaines courbes elliptiques à multiplications complexes", Séminaire de théorie des nombres, Paris 1983–84, Progr. Math., vol. 59, Birkhäuser Boston, Boston, MA, 1985, p. 235–253.

[29] D. E. Rohrlich – "Elliptic curves with good reduction everywhere", *J. London Math. Soc. (2)* **25** (1982), no. 2, p. 216–222.

[30] K. Rubin – "Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer", *Invent. Math.* **64** (1981), no. 3, p. 455–470.

[31] J.-P. Serre & J. Tate – "Good reduction of abelian varieties", *Ann. of Math. (2)* **88** (1968), p. 492–517.

[32] G. Shimura – "On the zeta-function of an abelian variety with complex multiplication.", *Ann. of Math. (2)* **94** (1971), p. 504–533.

[33] ———, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[34] J. H. Silverman – *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[35] T. Tannaka – "A generalized principal ideal theorem and a proof of a conjecture of Deuring", *Ann. of Math. (2)* **67** (1958), p. 574–589.

[36] F. Terada – "On the principal genus theorem concerning the abelian extensions", *Tôhoku Math. J. (2)* **4** (1952), p. 141–152.

[37] W. C. Waterhouse – "Basically bounded functors and flat sheaves", *Pacific J. Math.* **57** (1975), no. 2, p. 597–610.