REND. SEM. MAT. UNIV. PADOVA, Vol. 127 (2012)

The Arithmetic Theory of Local Constants for Abelian Varieties

MARCO ADAMO SEVESO

ABSTRACT - We present a generalization of the theory of local constants developed by B. Mazur and K. Rubin in order to cover the case of abelian varieties, with emphasis to abelian varieties with real multiplication. Let l be an odd rational prime and let L/K be an abelian l-power extension. Assume that we are given a quadratic extension K/k such that L/k is a dihedral extension and the abelian variety A/k is defined over k and polarizable. This theory can be used to relate the rank of the l-Selmer group of A over K to the rank of the l-Selmer group of A over L.

1. Introduction

In the paper [7] Mazur and Rubin provide an arithmetic theory of local constants to study the parity of the Selmer groups. We briefly sketch their ideas and present a generalization of the main result, which applies to abelian varieties with real multiplication. This is needed in [14], where the result is applied in order to relate the growth of the Selmer group to the rationality of Stark-Heegner points.

Let K/k be a quadratic extension of a number field k and let L/K be a finite abelian l-power extension, with Galois group Γ, such that L/k is dihedral, where $l \neq 2$ is a rational prime. Let $(A, \mathcal{O}, \mathfrak{l}) = (A, \mathcal{O}, \mathfrak{l})_k$ be triple where $(A, \mathcal{O})_k$ is an abelian variety with multiplication by an order $\mathcal{O}$ in a number field F (the data being defined over k) and $\mathfrak{l} \subset \mathcal{O}$ is a prime ideal of residue characteristic l. Since $\mathcal{O}$ is commutative the dual abelian variety A^t is canonically endowed with multiplication by $\mathcal{O}$ by letting $\alpha : A \to A$ acts on A^t through $\alpha^t : A^t \to A^t$. We make the following assumptions on the

(*) Indirizzo dell'A.: Università degli studi di Milano, Dipartimento di Matematica Federigo Enriques, via Saldini 50, 20133 Milano, Italy.

E-mail: seveso.marco@gmail.com

triple $(A, \mathcal{O}, \mathfrak{l})$:

- it is polarizable, meaning that there exists an $\mathcal{O}$-linear and symmetric isogeny
$$\lambda : A \to A^t$$
of degree prime to l;
- $(\mathcal{O}, \mathfrak{l})$ is regular, meaning that l is prime to the conductor of $\mathcal{O}$ in $\mathcal{O}_F$, the ring of integers of F;
- $(\mathcal{O}, \mathfrak{l})$ is unramified, meaning that the discriminant of $F/\mathbb{Q}$ is prime to l.

The present paper is organized as follows. Section 2 quickly reviews the theory of twisting abelian varieties and introduces some preliminary material. Section 3 is devoted to review the Mazur-Rubin argument in the more general setting of abelian varieties with multiplication by an order $\mathcal{O}$. The main result is Theorem 3.2, which applies to triples $(A, \mathcal{O}, \mathfrak{l})$ as above and notably under the assumption $[F : \mathbb{Q}] = \dim A$. We note that it is remarked in [7] that their theory generalizes to abelian varieties; Section 3 is understood to provide a suitable reference where unspoken assumptions that are always satisfied in the case of elliptic curves are made explicit. In particular, when $[F : \mathbb{Q}] = \dim A$ and one considers a prime $\mathfrak{l}$ as above, the $\mathfrak{l}$-torsion and the $\mathfrak{l}$-adic Tate module look essentially like those of an elliptic curve. Finally, the appendix "$\mathcal{O}$-polarizations on abelian varieties with real multiplication" is devoted to eliminate the above polarizability assumption when $(A, \mathcal{O})$ has real multiplication, i.e. F is a totally real field and $[F : \mathbb{Q}] = \dim A$.

Let $\mathcal{O}_\mathfrak{l}$ be the completion of $\mathcal{O}$ at the prime ideal $\mathfrak{l}$, which is a discrete valuation ring since $(\mathcal{O}, \mathfrak{l})$ is regular. Then we have

$$\mathcal{O}_l = \bigoplus_{\mathfrak{l}' | l} \mathcal{O}_{\mathfrak{l}'},$$

thus inducing a decomposition

$$Sel_{l^\infty}(A/L) = \bigoplus_{\mathfrak{l}' | l} Sel_{\mathfrak{l}'^\infty}(A/L).$$

We will be interested in the Selmer group $Sel_{\mathfrak{l}^\infty}(A/L)$ attached to the prime $\mathfrak{l} \mid l$. Note that it is a cofinitely generated module over the discrete valuation ring $\mathcal{O}_\mathfrak{l}$, so that it makes sense to talk about its corank over $\mathcal{O}_\mathfrak{l}$. Let $\mathrm{Irr}(\Gamma)$ be the set of all the rational irreducible representations of Γ and note that $Sel_\mathfrak{l}(A/L)$ and $Sel_{\mathfrak{l}^\infty}(A/L)$ are $\mathcal{O}_\mathfrak{l}[\Gamma]$-modules in a natural way. There is a

canonical isogeny (map with finite kernel and cokernel)

$$\bigoplus_{\rho} Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K) \overset{isog}{\to} Sel_{\mathfrak{l}^\infty}(A/L), \tag{1}$$

where $Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K)$ is the Selmer group of a twist A_ρ of A by ρ in the sense of [8] and $\mathfrak{l}_\rho$ is the unique prime ideal of $\mathcal{O}_\mathfrak{l}[\Gamma]$ corresponding to the irreducible representation ρ and dividing $\mathfrak{l}$ (see the preliminary discussion in Section 2). The action of $\mathcal{O}[\Gamma]$ on ρ factors through a quotient $\mathcal{O}_\rho$, whose completion $\mathcal{O}_{\rho,\mathfrak{l}} = \mathcal{O}_{\rho,\mathfrak{l}_\rho}$ at $\mathfrak{l}_\rho$ is again a discrete valuation ring. Denote by $\mathbb{F}$ the residue field of $\mathcal{O}_\mathfrak{l}$, which is also the residue field of $\mathcal{O}_{\rho,\mathfrak{l}}$ for every ρ (again we refer to Section 2).

The isogeny decomposition (1) yields

$$\operatorname{corank}_{\mathcal{O}_\mathfrak{l}}(Sel_{\mathfrak{l}^\infty}(A/L)) = \sum_{\rho} r_\rho \operatorname{corank}_{\mathcal{O}_{\mathfrak{l},\rho}}\left(Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K)\right), \tag{2}$$

where we set $r_\rho := \operatorname{rank}_{\mathcal{O}_\mathfrak{l}}(\mathcal{O}_{\mathfrak{l},\rho}) \geq 1$.

Hence, in order to get information on $\operatorname{corank}_{\mathcal{O}_\mathfrak{l}}(Sel_{\mathfrak{l}^\infty}(A/L))$ from the knowledge of $\operatorname{corank}_{\mathcal{O}_\mathfrak{l}}(Sel_{\mathfrak{l}^\infty}(A/K))$ we are led to compare $\operatorname{corank}_{\mathcal{O}_\mathfrak{l}}(Sel_{\mathfrak{l}^\infty}(A/K))$ with $\operatorname{corank}_{\mathcal{O}_{\mathfrak{l},\rho}}\left(Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K)\right)$.

It turns out that, assuming that $(A,\mathcal{O})$ has real multiplication, every regular and unramified triple $(A,\mathcal{O},\mathfrak{l})$ is polarizable (see Theorem A.11), so that the following generalization of [7, Theorem 7.1, case (a)] is deduced from Theorem 3.2. Let $ram(L/K/k)$ be the set of primes v of K that ramify in L and are inert or ramified over k, i.e. v is unramified in L and $v^c = v$ for the non-trivial automorphism c of K over k. Denote by $Bad(A/K)$ the set of primes of K that are of bad reduction for A/K.

THEOREM 1.1. *Assume that $(A,\mathcal{O},\mathfrak{l})_k$ is a regular and unramified triple with real multiplication. If $ram(L/K/k) \cap Bad(A/K) = \phi$ and $ram(L/K/k) \cap \{v \mid l\} = \phi$, for every ρ*

$$\dim_{\mathbb{F}}\left(Sel_{\mathfrak{l}_\rho}(A_\rho/K)\right) \equiv \dim_{\mathbb{F}}(Sel_\mathfrak{l}(A/K)) \bmod 2$$

and

$$\operatorname{corank}_{\mathcal{O}_{\mathfrak{l},\rho}}\left(Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K)\right) \equiv \operatorname{corank}_{\mathcal{O}_\mathfrak{l}}(Sel_{\mathfrak{l}^\infty}(A/K)) \bmod 2.$$

The main application of Theorem 1.1 is the following. Define

$$\operatorname{parity}_{\mathfrak{l}^\infty}(A/K) := \operatorname{corank}_{\mathcal{O}_\mathfrak{l}}(Sel_{\mathfrak{l}^\infty}(A/K)) \bmod 2.$$

COROLLARY 1.2. *Assume that* $(A, \mathcal{O}, \mathfrak{l})_k$ *is a regular and unramified triple with real multiplication. If* $ram(L/K/k) \cap Bad(A/K) = \phi$, $ram(L/K/k) \cap \{v \mid l\} = \phi$ *and* $\text{parity}_{\mathfrak{l}^\infty}(A/K) = 1$ *then*

$$\text{corank}_{\mathcal{O}_\mathfrak{l}}(Sel_{\mathfrak{l}^\infty}(A/K)) \geq [L : K].$$

PROOF. This is a consequence of Theorem 1.1, together with (2) and the equality $\sum_\rho r_\rho = \#\Gamma$ (see following (5) for this last equality). □

Note also that, whenever $A[\mathfrak{l}](K) = 0$, it follows from the subsequent (7), together with the congruence relation appearing in the subsequent Theorem 2.2, that we have:

$$\text{parity}_\mathfrak{l}(A/K) := \dim_{\mathbb{F}}(Sel_\mathfrak{l}(A/K)) \equiv \text{corank}_{\mathcal{O}_\mathfrak{l}}(Sel_{\mathfrak{l}^\infty}(A/K)) \bmod 2.$$

Another useful application is the following Corollary, that we state without proof.

COROLLARY 1.3. *Under the assumption of the above Corollary, further suppose*

$$A[\mathfrak{l}](K) = 0.$$

Then, for every $n \in \mathbb{N}$, $Sel_{\mathfrak{l}^n}(A/L)$ *contains an* $\frac{\mathcal{O}}{\mathfrak{l}^n}[\Gamma]$*-module which is* $\frac{\mathcal{O}}{\mathfrak{l}^n}$*-free of rank at least* $[L : K]$ *and, in particular,*

$$\dim_{\mathbb{F}}(Sel_\mathfrak{l}(A/L)) \geq [L : K].$$

The paper [7] deals with the theory of local constants for elliptic curves. As remarked in [7], an extension of the theory of local constants to abelian varieties is expected. The aim of the present work is to provide such a generalization. The results of Section 3 work for arbitrary polarized, regular and unramified triples $(A, \mathcal{O}, \mathfrak{l}) = (A, \mathcal{O}, \mathfrak{l})_k$. In the setting of elliptic curves the existence of a principal polarization makes the polarizability assumption supefluous. As explained, the appendix "$\mathcal{O}$-polarizations on abelian varieties with real multiplication" removes this assumption when A has real multiplication by an order $\mathcal{O}$ in a (totally real) number field F. We do not prove the existence of a principal polarization, which is false when the class number of F is not one, but rather show the existence of a polarization of degree prime to l. Of course Theorem 3.2 is applicable to other scenarios: for example when $(A, \mathcal{O}, \mathfrak{l}) = (A, \mathbb{Z}, l)$ and A is an abelian surface with quaternionic multiplication it is well known that a principal polarization exists. The above corollaries are true for an arbitrary polar-

ized, regular and unramified triple $(A, \mathcal{O}, \mathfrak{l}) = (A, \mathcal{O}, \mathfrak{l})_k$, but we have choosen to state them without the polarizability assumption when we have real multiplication since this is the statement needed in [14].

2. Twisting abelian varieties

Let $\mathcal{O} = \mathcal{O}_F$ be the ring of integers of a number field F and let Γ be a finite abelian l-torsion group. We explain how to get a canonical isogeny decomposition of the group algebra $\mathcal{O}[\Gamma]$. This will be regarded like an algebra with involution using the inversion in Γ.

Let $\mathrm{Irr}_F(\Gamma)$ be the set of isomorphism classes of distinct irreducible representations of Γ over F. Since $F[\Gamma]$ is semisimple there is a canonical decomposition

$$F[\Gamma] = \bigoplus_{\rho \in \mathrm{Irr}_F(\Gamma)} F_\rho,$$

where F_ρ/F are field extensions. The projection of $F[\Gamma]$ onto F_ρ gives the action of $F[\Gamma]$ on the representation ρ.

DEFINITION 2.1. An ideal $\mathcal{I} \subset \mathcal{O}[\Gamma]$ is said to be saturated whenever the quotient $\dfrac{\mathcal{O}[\Gamma]}{\mathcal{I}}$ is $\mathcal{O}$-flat.

Tensoring a saturated module $\mathcal{I} \subset \mathcal{O}[\Gamma]$ over $\mathcal{O}$ with F and conversely intersecting an ideal in $F[\Gamma]$ with $\mathcal{O}[\Gamma]$ establishes a bijection between the set of the saturated ideals of $\mathcal{O}[\Gamma]$ and the ideals of $F[\Gamma]$. We will denote by $\mathcal{I}_\rho := F_\rho \cap \mathcal{O}[\Gamma]$ the saturated ideal corresponding to the field F_ρ.

Since $\oplus_{\rho \in \mathrm{Irr}_F(\Gamma)} \mathcal{I}_\rho$ is an $\mathcal{O}[\Gamma]$-submodule contained in $\mathcal{O}[\Gamma]$ with finite index we get an $\mathcal{O}[\Gamma]$-linear isogeny:

$$\bigoplus_{\rho \in \mathrm{Irr}_F(\Gamma)} \mathcal{I}_\rho \overset{isog}{\hookrightarrow} \mathcal{O}[\Gamma]. \tag{3}$$

The aim of the following discussion is to study the $\mathcal{O}[\Gamma]$-module structure of the modules $\mathcal{I}_\rho$, which factors through a certainly quotient $\mathcal{O}_\rho$ contained in the field F_ρ. From now on we will assume that F is unramified over $l \neq 2$. The effect of this assumption is that the study of $\mathcal{O}_\rho$ is essentially reduced to the case $\mathcal{O} = \mathbb{Z}$. The following facts can be directly proved or can be deduced from the case $\mathcal{O} = \mathbb{Z}$ and [8, in particular Lemma 5.4]. The set $\mathrm{Irr}_F(\Gamma)$ is in bijection with the subgroups $\Gamma' \subset \Gamma$ such that Γ/Γ' is cyclic, i.e. with

$\mathrm{Irr}_{\mathbb{Q}}(\Gamma)$. If $\rho \in \mathrm{Irr}_F(\Gamma)$ corresponds to a cyclic quotient Γ/Γ' of order l^r we have $F_\rho \simeq F(\zeta)$, where ζ a primitive l^r-root of unity. Denote by l_ρ the unique prime of $\mathbb{Z}[\zeta]$ dividing l, so that $\mathbb{Z}[\zeta]l = l_\rho^e$. The ring $\mathcal{O}[\Gamma]$ acts on $\mathcal{I}_\rho$ through the quotient $\mathcal{O}_\rho \simeq \mathcal{O}[\zeta]$ and for every prime $\mathfrak{l}' \mid l$ of $\mathcal{O}$ there is one only prime $\mathfrak{l}'_\rho$ of $\mathcal{O}_\rho \simeq \mathcal{O}[\zeta]$ over $\mathfrak{l}'$ and $\mathfrak{l}_\rho'^e = \mathcal{O}_\rho \mathfrak{l}'$, where $e = \varphi(l^r)$. We have

$$l\mathcal{O} = \prod_{\mathfrak{l}' \mid l} \mathfrak{l}' \text{ and } l_\rho \mathcal{O}_\rho = \prod_{\mathfrak{l}' \mid l} \mathfrak{l}'_\rho. \tag{4}$$

In particular the localization $\mathcal{O}_{\rho,\mathfrak{l}}$ of $\mathcal{O}_\rho$ at $\mathfrak{l}$ is a discrete valuation ring with uniformizers $\zeta - 1$ or $\pi := \zeta - \zeta^{-1}$ and we have $\mathcal{O}_{\rho,\mathfrak{l}}\mathfrak{l}_\rho = \mathcal{O}_{\rho,\mathfrak{l}}\pi$. Indeed $F_{\rho,\mathfrak{l}}/F_{\mathfrak{l}}$ is totally ramified of degree $\varphi(l^r)$ and $\mathcal{O}_{\rho,\mathfrak{l}} \simeq \mathcal{O}_{\mathfrak{l}}[\zeta]$. Under the isomorphism $\mathcal{O}_\rho \simeq \mathcal{O}[\zeta]$ we have $\mathcal{I}_\rho \simeq (\zeta_l - 1)\mathcal{O}_\rho$, where ζ_l is a primitive l-root of unity and in particular $\mathcal{O}_{\rho,\mathfrak{l}}\mathcal{I}_\rho \simeq \pi^{l^{r-1}}\mathcal{O}_\rho$. Furthermore sending ζ to ζ^{-1} induces a well defined involution ι on $\mathcal{O}_\rho \simeq \mathcal{O}[\zeta]$ such that the projection of $\mathcal{O}[\Gamma]$ onto $\mathcal{O}_\rho \simeq \mathcal{O}[\zeta]$ is a morphism of rings with involution. Then the formula

$$[-,-]_\rho \colon \mathcal{O}_{\rho,\mathfrak{l}}\mathcal{I}_\rho \times \mathcal{O}_{\rho,\mathfrak{l}}\mathcal{I}_\rho \to \mathcal{O}_\rho$$

$$[\alpha,\beta]_\rho := \pi^{-2l^{r-1}}\alpha\iota(\beta)$$

gives on $\mathcal{O}_{\rho,\mathfrak{l}}\mathcal{I}_\rho$ a perfect and $(\mathcal{O}_\rho, \iota)$-Hermetian $\mathcal{O}_\rho$ -valued pairing. We also note that, if we write $\mathcal{I}_{\rho,\mathbb{Z}}$ (resp. $\mathcal{I}_{\rho,\mathcal{O}}$) for the saturated ideal corresponding to the same irreducible $\mathbb{Q}$-representation (resp. F-representation) it holds the equality $\mathcal{I}_{\rho,\mathcal{O}} = \mathcal{O} \otimes_{\mathbb{Z}} \mathcal{I}_{\rho,\mathbb{Z}}$. In particular, setting $r_\rho := \mathrm{rank}_{\mathcal{O}_{\mathfrak{l}}}(\mathcal{O}_{\mathfrak{l},\rho})$ as in the introduction, we have

$$\sum_\rho r_\rho = \#\Gamma. \tag{5}$$

Recall the extensions $L/K/k$ that was considered in the introduction, as well as the polarizable, regular and unramified triple $(A,\mathcal{O},\mathfrak{l}) = (A,\mathcal{O},\mathfrak{l})_k$. The above discussion applies to $\Gamma := G_{L/K}$. We denote by $\mathbb{F}$ the common residue field of $\mathcal{O}$ (resp. $\mathcal{O}_{\mathfrak{l}}$) and $\mathcal{O}_\rho$ (resp. $\mathcal{O}_{\mathfrak{l},\rho}$) at $\mathfrak{l}$ (resp. $\mathcal{O}_{\mathfrak{l}}\mathfrak{l}$) and at $\mathfrak{l}_\rho$ (resp. $\mathcal{O}_\rho\mathfrak{l}_\rho$). The above discussion implies that the twists

$$A_\rho := \mathcal{I}_{\rho,\mathcal{O}} \otimes_{\mathcal{O}} A = \mathcal{I}_{\rho,\mathbb{Z}} \otimes_{\mathbb{Z}} \mathcal{O} \otimes_{\mathcal{O}} A = \mathcal{I}_{\rho,\mathbb{Z}} \otimes_{\mathbb{Z}} A$$

do not depend on the ring $\mathcal{O}$ over which we are twisting. These twists have been already considered in the literature and we refer to [8] for details. A_ρ is again an abelian variety and for every K -algebra X there is a canonical identification (see [8, Theorem 1.4])

$$\big(\mathcal{I}_{\rho,\mathcal{O}} \otimes_{\mathcal{O}} A\big)(X) = \big(\mathcal{I}_{\rho,\mathcal{O}} \otimes_{\mathcal{O}} A(X \otimes_K L)\big)^{G_{L/K}}.$$

As it follows from [8, Prop. 4.1], $\mathcal{O}[\Gamma] \otimes_{\mathcal{O}} A$ is identified with the restriction of scalars from K to L of A/K. It then follows that we have (see [7, Prop. 3.1]):

$$Sel_{\mathfrak{l}}(A/L) \simeq Sel_{\mathfrak{l}}(\mathcal{O}[\Gamma] \otimes_{\mathcal{O}} A/K)$$

and hence the isogeny (3) yields the $\mathcal{O}[\Gamma]$-linear isogeny decomposition (1).

The abelian varieties A_ρ/K are endowed with multiplication by $\mathcal{O}_\rho$ acting on $\mathcal{I}_{\rho,\mathcal{O}}$ and we can consider the triple $(A_\rho, \mathcal{O}_\rho, \mathfrak{l}_\rho)$. Note that $(A_\rho, \mathcal{O}_\rho, \mathfrak{l}_\rho)$ is again regular and unramified, as it follows from the above discussion, but may fail to be polarizable. The decomposition (4) yields canonical $\mathcal{O}/\mathcal{O}l^n$-module decompositions (see also [6] for a direct definition of the $\mathfrak{l}_\rho$-adic Selmer groups):

$$\begin{aligned} &A_\rho\left[l_\rho^n\right] = \bigoplus_{\mathfrak{l}'|l} A_\rho\left[\mathfrak{l}_\rho'^n\right] \text{ for } n \in \mathbb{N}, \\ &Sel_{l_\rho^\infty}(A/K) = \bigoplus_{\mathfrak{l}'|l} Sel_{\mathfrak{l}_\rho'^\infty}(A/K). \end{aligned} \tag{6}$$

As in the setting of classical Selmer groups one can prove that there is an exact sequence:

$$0 \to \frac{\mathfrak{l}_\rho^{-1}}{\mathcal{O}_\rho} \otimes_{\mathcal{R}} A_\rho\left[\mathfrak{l}_\rho^\infty\right](K) \to Sel_{\mathfrak{l}_\rho}(A_\rho/K) \to Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K)\left[\mathfrak{l}_\rho\right] \to 0 \tag{7}$$

and furthermore

$$\dim_{\mathbb{F}}\left(\frac{\mathfrak{l}_\rho^{-1}}{\mathcal{O}_\rho} \otimes_{\mathcal{R}} A_\rho\left[\mathfrak{l}_\rho^\infty\right](K)\right) = \dim_{\mathbb{F}}\left(A_\rho\left[\mathfrak{l}_\rho\right](K)\right). \tag{8}$$

Let $T_{\mathfrak{l}}(A)$ be the Tate module attached to the $\mathfrak{l}$-adic representation of the abelian variety A/k over the field k. We recall the following fact (see [8, Theorem 2.2]): there is a G_K-equivariant isomorphism

$$T_{\mathfrak{l}}(A_\rho) = \mathcal{I}_{\rho,\mathcal{O}} \otimes_{\mathcal{O}} T_{\mathfrak{l}}(A),$$

where G_K-acts on the right hand side via $g^{-1} \otimes g$. The polarizability assumption on $(A, \mathcal{O}, \mathfrak{l})$ implies that the $\mathcal{O}_{\mathfrak{l}}(1)$-valued Weil pairing on $T_{\mathfrak{l}}(A)$ is perfect.

We only sketch the proof of the following Theorem, which is a straightforward generalization of [7, Theorem A.12 and Prop. A.11], which in turn is an application of the techniques developed in [4] (see also [13, Prop. B.27] for further details).

THEOREM 2.2. *The pairing* $\langle -,-\rangle_\rho$ *induces on* $Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K)$ *a* $G_{K/k}$*-equivariant and skew-*$(\mathcal{O}_{\mathfrak{l},\rho},\imath)$*-Hermetian pairing with kernel* $Sel_{\mathfrak{l}_\rho^\infty}(A/K)_{div}$*:*

$$Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K)\times Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K)\to\frac{F_{\mathfrak{l},\rho}}{\mathcal{O}_{\mathfrak{l},\rho}}$$

In particular

$$\operatorname{corank}_{\mathcal{O}_{\mathfrak{l},\rho}}\left(Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K)\right)\equiv\dim_{\mathbb{F}}\left(Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K)[\mathfrak{l}_\rho]\right)\bmod 2.$$

PROOF. The first step in the proof of the Theorem is to provide a "model" of A_ρ over k. This can be done as in [7, Prop. A.9]: choose a lift $\boldsymbol{c}$ of the non-trivial automorphism of the extension K/k to the algebraic closure $\overline{k}/k$. For every $\rho\in\operatorname{Irr}_F(\Gamma)$ define $\mathcal{J}_{\mathcal{O},\rho}:=(1+\boldsymbol{c})\mathcal{I}_{\mathcal{O},\rho}$, which is a right ideal in $\mathcal{O}[G_{L/k}]$. The left multiplication by $1+\boldsymbol{c}$ gives a right $\mathcal{O}[\Gamma]$-module isomorphism $\mathcal{I}_\rho\xrightarrow{\simeq}\mathcal{J}_\rho$, thus inducing an isomorphism over K: $A_\rho:=\mathcal{I}_{\rho,\mathcal{O}}\otimes_{\mathcal{O}}A\simeq\mathcal{J}_{\mathcal{O},\rho}\otimes_{\mathcal{O}}A=:A'_\rho$. The second step is in producing $\mathcal{O}_{\mathfrak{l},\rho}(1)$-valued perfect, skew-$(\mathcal{O}_{\mathfrak{l},\rho},\imath)$-Hermetian and G_K-equivariant pairings on $T_{\mathfrak{l}}(A_\rho)$, that are G_k-equivariant when making the identification $T_{\mathfrak{l}}(A_\rho)\xrightarrow{\simeq}T_{\mathfrak{l}}(A'_\rho)$. They are obtained setting $\langle -,-\rangle_\rho:=[-,-]_\rho\otimes e$ where e is the $\mathcal{O}_{\mathfrak{l}}(1)$-valued Weil pairing on $T_{\mathfrak{l}}(A_\rho)$, which is perfect in light of the polarizability assumption on $(A,\mathcal{O},\mathfrak{l})$. Finally one applies the Flach construction as explained in [7, Theorem A.12].

3. The arithmetic theory of local constants

Recall our polarized, regular and unramified triple $(A,\mathcal{O},\mathfrak{l})=(A,\mathcal{O},\mathfrak{l})_k$ from the introduction. Since the claim of Theorem 3.2 is invariant under isogenies of degree prime to l we can suppose that $\mathcal{O}=\mathcal{O}_F$ (see Lemma A.10).

LEMMA 3.1. *There are canonical identifications of* $\mathbb{F}[G_K]$*-modules:*

$$A_\rho[\mathfrak{l}_\rho]=A[\mathfrak{l}].$$

PROOF. By [7, Prop. 4.1] there is a canonical identification of $\mathbb{F}_l[G_K]$-modules $A_\rho[l_\rho]=A[l]$, which is an identification of $\mathcal{O}/l\mathcal{O}$-modules (by the canonicity). The claim follows from the $\mathcal{O}/\mathcal{O}l$-modules decompositions (6). □

The first of the subsequent congruences follows from Theorem 2.2, while the second follows from Lemma 3.1 together with the exact sequence (7):

$$\begin{aligned} &\operatorname{corank}_{\mathcal{O}_{\mathfrak{l},\rho}}\left(Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K)\right) - \operatorname{corank}_{\mathcal{O}_\mathfrak{l}}(Sel_{\mathfrak{l}^\infty}(A/K)) \quad &\equiv \\ (9)\qquad &\dim_{\mathbb{F}}\left(Sel_{\mathfrak{l}_\rho^\infty}(A_\rho/K)[\mathfrak{l}_\rho]\right) - \dim_{\mathbb{F}}(Sel_{\mathfrak{l}^\infty}(A/K)[\mathfrak{l}]) \quad &\equiv \\ &\dim_{\mathbb{F}}\left(Sel_{\mathfrak{l}_\rho}(A_\rho/K)\right) - \dim_{\mathbb{F}}(Sel_{\mathfrak{l}}(A/K)) \quad &\mod 2. \end{aligned}$$

The $\mathbb{F}[G_K]$-module identification $A_\rho[\mathfrak{l}_\rho] = A[\mathfrak{l}]$ allow us to view $Sel_{\mathfrak{l}_\rho}(A_\rho/K)$ as the sub-$\mathbb{F}$ -module of $H^1(K, A[\mathfrak{l}])$ defined by the set of local conditions $\mathcal{S}_\rho$,

$$\mathcal{S}_{\rho,v} := \operatorname{Im}\left(\frac{A_\rho(K_v)}{\mathfrak{l}_\rho A_\rho(K_v)} \overset{\delta_v}{\hookrightarrow} H^1(K_v, A_\rho[\mathfrak{l}_\rho]) = H^1(K_v, A[\mathfrak{l}])\right)$$

for the local Kummer map δ_v at v. Recall that, as explained in the proof of Theorem 2.2, the $\mathcal{O}$-polarization on A induces on $T_\mathfrak{l}(A_\rho) = T_{\mathfrak{l}_\rho}(A_\rho)$ perfect twisted pairings and, up to the canonical identification $A_\rho[\mathfrak{l}_\rho] = A[\mathfrak{l}]$, they induce the same pairing on $A[\mathfrak{l}]$. It follows that, for every ρ, the Selmer structure $\mathcal{S}_\rho$ is selfdual (for the Weil pairing on $A[\mathfrak{l}]$) by the Bloch-Kato generalization of Tate's local duality applied to $T_\mathfrak{l}(A_\rho)$ (see [2, Prop. 3.8] and [7, Prop. A.7]). We can now apply [7, Theorem 1.4], whose proof relies on a clever argument of Howard, which implies:

$$(10)\quad \dim_{\mathbb{F}}\left(Sel_{\mathfrak{l}_\rho}(A_\rho/K)\right) - \dim_{\mathbb{F}}(Sel_{\mathfrak{l}}(A/K)) \equiv \sum_{v\in\Sigma} \dim_{\mathbb{F}}\left(\frac{\mathcal{S}_v}{\mathcal{S}_v \cap \mathcal{S}_{\rho,v}}\right) \mod 2,$$

where Σ denotes the set of primes out of which the Selmer structures $\mathcal{S}$ and $\mathcal{S}_\rho$ coincides, which is finite. The local constants are defined as being

$$\delta_v = \delta_v(A, \mathcal{O}, \mathfrak{l}, L/K, \rho) := \dim_{\mathbb{F}}\left(\frac{\mathcal{S}_v}{\mathcal{S}_v \cap \mathcal{S}_{\rho,v}}\right) \text{ in } \mathbb{Z}/2\mathbb{Z}.$$

We are going to recover, from the results of [7], an explicit description of the spaces $\dfrac{\mathcal{S}_v}{\mathcal{S}_v \cap \mathcal{S}_{\rho,v}}$. In order to connect these spaces with those defined in [7] when working over $\mathbb{Z}$, we will write $\mathcal{S}_v = \mathcal{S}_{v,\mathfrak{l}}$ (resp. $\mathcal{S}_{\rho,v} = \mathcal{S}_{\rho,v,\mathfrak{l}_\rho}$) to emphasize the dependence on the chosen prime $\mathfrak{l} \mid l$. Then it is clear that we have

$$\frac{\mathcal{S}_{v,l}}{\mathcal{S}_{v,l} \cap \mathcal{S}_{\rho,v,l_\rho}} = \bigoplus_{\mathfrak{l}'\mid l} \frac{\mathcal{S}_{v,\mathfrak{l}'}}{\mathcal{S}_{v,\mathfrak{l}'} \cap \mathcal{S}_{\rho,v,\mathfrak{l}'_\rho}}.$$

The space $\dfrac{\mathcal{S}_{v,l}}{\mathcal{S}_{v,l} \cap \mathcal{S}_{\rho,v,l_\rho}}$ can be explicitly described as follows. For every ρ let L_ρ/K be the cyclic subextension of L/K corresponding to the irreducible representation ρ, choose a prime w of L_ρ dividing v and set:

$$L'_{\rho,w} := \begin{cases} \text{unique subfield such that } \left[L_{\rho,w} : L'_{\rho,w}\right] = l & \text{if } K_v \neq L_{\rho,w} \\ L_{\rho,w} & \text{if } K_v = L_{\rho,w} \end{cases}$$

The proof of [7, Corollary 5.3] readily generalizes to our setting and gives a canonical identification

$$\frac{\mathcal{S}_{v,l}}{\mathcal{S}_{v,l} \cap \mathcal{S}_{\rho,v,l_\rho}} = \frac{A(K_v)}{A(K_v) \cap N_{L_{\rho,w}/L'_{\rho,w}} A\left(L_{\rho,w}\right)}.$$

THEOREM 3.2. *Let $ram(L/K/k)$ be the set of primes of K which ramify in L/K and such that $v^c = v$ (if c is the non-trivial automorphism of K/k) and let $Good_l(A/K)$ be the set of primes of K of good reduction for A/K which do not divide l. Then, for every ρ,*

$$\begin{aligned} &\operatorname{corank}_{\mathcal{O}_{l,\rho}}\left(Sel_{l_\rho^\infty}\left(A_\rho/K\right)\right) - \operatorname{corank}_{\mathcal{O}_l}(Sel_{l^\infty}(A/K)) \equiv \\ &\equiv \sum_{v \in ram(L/K/k)} \delta_v(A, \mathcal{O}, l, L/K, \rho). \end{aligned}$$

and when $[F : \mathbb{Q}] = \dim A$

$$\begin{aligned} &\operatorname{corank}_{\mathcal{O}_{l,\rho}}\left(Sel_{l_\rho^\infty}\left(A_\rho/K\right)\right) - \operatorname{corank}_{\mathcal{O}_l}(Sel_{l^\infty}(A/K)) \equiv \\ &\equiv \sum_{v \in ram(L/K/k) - Good_l(A/K)} \delta_v(A, \mathcal{O}, l, L/K, \rho). \end{aligned}$$

PROOF. According to (9) and (10) we have to show that $\delta_v = 0$ whenever $v \notin ram(L/K/k)$ (resp. $v \notin ram(L/K/k) - Good_l(A/K)$ when $[F : \mathbb{Q}] = \dim A$).

If $v \notin ram(L/K/k)$ there are two possibilities: $v^c \neq v$ or $v^c = v$ and $v \notin ram(L/K)$. In the first case it is clear that [7, Lemma 5.1] generalizes: since the entire triples $(A, \mathcal{O}, l)$ and $\left(A_\rho, \mathcal{O}_\rho, l_\rho\right)$ are defined over k (see the proof of Theorem 2.2) the automorphism of K/k induces isomorphisms

$$\begin{aligned} (A, \mathcal{O}, l)_{K_v} &\xrightarrow{\simeq} (A, \mathcal{O}, l)_{K_{v^c}}, \\ \left(A_\rho, \mathcal{O}_\rho, l_\rho\right)_{K_v} &\xrightarrow{\simeq} \left(A_\rho, \mathcal{O}_\rho, l_\rho\right)_{K_{v^c}}. \end{aligned}$$

Therefore, under the isomorphism $H^1(K_v, A[\mathfrak{l}]) \xrightarrow{\simeq} H^1(K_{v^c}, A[\mathfrak{l}])$ induced by conjugation, $\mathcal{S}_v$ (resp. $\mathcal{S}_{\rho,v}$) corresponds to $\mathcal{S}_{v^c}$ (resp. $\mathcal{S}_{\rho,v^c}$) and hence $\delta_{v^c} = \delta_v$ (thus, assuming $v^c \neq v$, we have $\delta_{v^c} + \delta_v = 0$). In the second case, since $v^c = v$, by [7, Lemma 6.5 (i)], for every prime w of L_ρ the extension $L_{\rho,w}/K_v$ is (non-trivial) totally ramified or v splits completely. Since the first possibility has to be excluded (otherwise L/K should be ramified too), the module $\dfrac{\mathcal{S}_{v,l}}{\mathcal{S}_{v,l} \cap \mathcal{S}_{\rho,v,l_\rho}}$ is trivial by the previous description and hence the direct addend $\dfrac{\mathcal{S}_{v,\mathfrak{l}}}{\mathcal{S}_{v,\mathfrak{l}} \cap \mathcal{S}_{\rho,v,\mathfrak{l}_\rho}}$ is trivial too (so that $\delta_v = 0$). It follows the first formula.

Now assume $[F : \mathbb{Q}] = \dim A$ and let $v \in ram(L/K/k)$ be a prime such that $v \nmid l$ and A/K has good reduction at v (more generally assume $v^c = v$, $v \nmid l$ and A/K to have good reduction at v). Since $v^c = v$, by [7, Lemma 6.5 (i)] there are two possibilities: $L_{\rho,w}/K_v$ is (non-trivial) totally ramified for (every) w dividing v or v splits completely in L_ρ, but in this latter case we have seen that $\dfrac{\mathcal{S}_{v,\mathfrak{l}}}{\mathcal{S}_{v,\mathfrak{l}} \cap \mathcal{S}_{\rho,v,\mathfrak{l}_\rho}}$ is trivial. Thus we may assume $L_{\rho,w}/K_v$ to be totally ramified (non-trivial) and since $v \nmid l$ and A/K has good reduction at v the proof of [7, Theorem 5.6] generalizes. More precisely [7, Lemma 5.4] readily generalizes to the case of an abelian variety $A/\mathcal{K}$ with multiplication, giving the identification

$$\frac{\mathfrak{l}^{-1}}{\mathcal{O}} \otimes_{\mathcal{O}} A(\mathcal{K}) = \frac{\mathfrak{l}^{-1}}{\mathcal{O}} \otimes_{\mathcal{O}} A[\mathfrak{l}^\infty](\mathcal{K}),$$

for every local field $\mathcal{K}$ of residue characteristic coprime with l. It is also true that [7, Lemma 5.5] generalizes to abelian varieties $A/\mathcal{K}$, showing that, whenever in this case $\mathcal{L}/\mathcal{K}$ is a (non-trivial) totally ramified extension and $A/\mathcal{K}$ has good reduction, there are equalities:

$$N_{\mathcal{L}/\mathcal{K}} A(\mathcal{L}) = lA(\mathcal{K}) \text{ if } [\mathcal{L} : \mathcal{K}] = l,$$

$$A(\mathcal{K}) \cap lA(\mathcal{L}) = lA(\mathcal{K}).$$

These last two equalities applies first to $L_{\rho,w}/L'_{\rho,w}$ and then to $L'_{\rho,w}/K_v$, giving:

$$\frac{\mathcal{S}_{v,l}}{\mathcal{S}_{v,l} \cap \mathcal{S}_{\rho,v,l_\rho}} = \frac{A(K_v)}{A(K_v) \cap N_{L_{\rho,w}/L'_{\rho,w}} A\big(L_{\rho,w}\big)} = \frac{A(K_v)}{A(K_v) \cap lA\big(L'_{\rho,w}\big)} = \frac{A(K_v)}{lA(K_v)}.$$

From the canonical decomposition of $\dfrac{A(K_v)}{lA(K_v)}$ as a module over $\mathcal{O}/l\mathcal{O} = \bigoplus_{\mathfrak{l}'|l} \mathbb{F}_{\mathfrak{l}'}$ and then using the generalization of [7, Lemma 5.4], we find

$$\frac{\mathcal{S}_{v,\mathfrak{l}}}{\mathcal{S}_{v,\mathfrak{l}} \cap \mathcal{S}_{\rho,v,\mathfrak{l}_\rho}} = \frac{\mathfrak{l}^{-1}}{\mathcal{O}} \otimes_{\mathcal{O}} A(K_v) = \frac{\mathfrak{l}^{-1}}{\mathcal{O}} \otimes_{\mathcal{O}} A[\mathfrak{l}^\infty](K_v).$$

By (8) the $\mathbb{F}$-dimension of $\dfrac{\mathfrak{l}^{-1}}{\mathcal{O}} \otimes_{\mathcal{O}} A[\mathfrak{l}^\infty](K_v)$ is the same as the $\mathbb{F}$-dimension of $A[\mathfrak{l}](K_v)$. Thus we find

$$\delta_v \equiv \dim_{\mathbb{F}} A[\mathfrak{l}](K_v),$$

which is the claimed generalization of [7, Theorem 5.6]. Hence to get the second formula it is enough to show that the $\mathbb{F}$-dimension of $A[\mathfrak{l}](K_v)$ is even and this is where the assumption $[F : \mathbb{Q}] = \dim A$ plays its role. Indeed this last fact follows exactly as in [7, Lemma 6.6], using the $\mathbb{F}[G_k]$-vector space $A[\mathfrak{l}]$ (which is 2-dimensional over $\mathbb{F}$ since $[F : \mathbb{Q}] = \dim A$, by Proposition A.11) and the $\mathbb{F}(1)$-valued Weil pairing on $A[\mathfrak{l}]$ in a place of the $\mathbb{F}_l[G_k]$-vector space $E[l]$ and the $\mathbb{F}_l$ (1)-valued Weil pairing, which is used in the case of an elliptic curve. □

A $\mathcal{O}$-polarizations on abelian varieties with real multiplication

Let A be an abelian S-scheme with multiplication by an order $\mathcal{O}$ in a totally real number field F such that $\dim_S A = [F : \mathbb{Q}]$ is constant. The dual abelian S-scheme A^t/S, that we assume to exists (for example suppose that A/S is projective), is canonically endowed with multiplication by $\mathcal{O}$.

Let

$$Hom_{\mathcal{O}}^{Sym}(A, A^t) := \{\lambda : A \to A^t : \lambda = \lambda^t \text{ and } \lambda \text{ is } \mathcal{O}\text{ −linear}\}$$

be the set of all symmetric $\mathcal{O}$-linear morphisms (over S) from A/S to the dual abelian scheme A^t/S (here $\lambda = \lambda^t$ up to the canonical identification $A = A^{tt}$). Let us be given a prime $\mathfrak{l} \subset \mathcal{O}$ of residue characteristic l invertible in S. For a torsion free finitely generated $\mathcal{O}_\mathfrak{l}$ -module T, $T = T^{**}$ canonically where we write $T^* = Hom_{\mathcal{O}_\mathfrak{l}}(T, \mathcal{O}_\mathfrak{l})$ to denote the $\mathcal{O}_\mathfrak{l}$-dual. Using this identification we may define

$$Hom_{\mathcal{O}_\mathfrak{l}}^{Alt}(T, T^*) := \{\lambda : T \to T^* : \lambda = -\lambda^* \text{ and } \lambda \text{ is } \mathcal{O}_\mathfrak{l}\text{−linear}\},$$

called the $\mathcal{O}_\mathfrak{l}$-module of alternating homomorphisms from T to T^*. Then $T_\mathfrak{l}(A^t) = T_\mathfrak{l}(A)^*$ and we can consider the following commutative diagram (see [3, 1.5]):

$$\begin{array}{ccc} Hom_{\mathcal{O}}^{Sym}(A,A^t)_\mathfrak{l} & \hookrightarrow & Hom_{\mathcal{O}_\mathfrak{l}}^{Alt}(T,T^*) \\ \cap & & \cap \\ Hom_{\mathcal{O}}(A,A^t)_\mathfrak{l} & \hookrightarrow & Hom_{\mathcal{O}_\mathfrak{l}}(T,T^*) \end{array} \tag{11}$$

where we set $T := T_\mathfrak{l}(A)$. Here $M_\mathfrak{l} = M \otimes_{\mathcal{O}} \mathcal{O}_\mathfrak{l}$ is the $\mathfrak{l}$-adic completion of M, since the modules involved are finitely generated.

If M is an $\mathcal{O}$-module we write M to denote the constant presheaf $M(T/S) := M$ on the big étale site and we let $\underline{M}$ be the associated sheaf $\underline{M}(T/S) = M^{\pi_0(T)}$, where $\pi_0(T)$ denotes the set of connected components of T and $M^{\pi_0(T)}$ is the $\mathcal{O}$-module of maps from $\pi_0(T)$ to M. We also write M and $\underline{M}$ to denote their restrictions to the étale site.

If M is a projective $\mathcal{O}$-module of finite rank r_M, the functor $M \otimes_{\mathcal{O}} A$ defined by the rule

$$(M \otimes_{\mathcal{O}} A)(T/S) := M \otimes_{\mathcal{O}} A(T/S),\ T/S \text{ arbitrary}$$

is representable by an abelian S-scheme with multiplication by $\mathcal{O}$ and dimension $\dim_S M \otimes_{\mathcal{O}} A = r_M \dim_S A$. Indeed this is clear when $M = \mathcal{O}^n$; in general we may write $\mathcal{O}^n \simeq M \oplus N$, so that $(M \otimes_{\mathcal{O}} A) \oplus (N \otimes_{\mathcal{O}} A) \simeq A^n$ holds as functors and then we may apply Yoneda's Lemma to deduce the existence of an idemponent $e_M \in End_S(A^n)$ such that $e_M A^n \simeq M \otimes_{\mathcal{O}} A$. In particular $M \otimes_{\mathcal{O}} A$ is a sheaf on the big étale site and its restriction to the étale site is a sheaf.

On the other hand we may consider the presheaf $\underline{M} \otimes^p_{\mathcal{O}} A$ defined by the rule

$$\big(\underline{M} \otimes^p_{\mathcal{O}} A\big)(T/S) := \underline{M}(T/S) \otimes_{\mathcal{O}} A(T/S) = M^{\pi_0(T)} \otimes_{\mathcal{O}} A(T/S),$$

where T/S may be an arbitrary S-scheme or an étale S-scheme if we work with the étale site. We write $\underline{M} \otimes^p_{\mathcal{O}} A \to \underline{M} \otimes_{\mathcal{O}} A$ to denote the associated presheaf with the canonical sheafication morphism. We may therefore consider the canonical morphism

$$\Delta : M \otimes_{\mathcal{O}} A \xrightarrow{\Delta^p} \underline{M} \otimes^p_{\mathcal{O}} A \to \underline{M} \otimes_{\mathcal{O}} A$$

where Δ^p is given by the sheafication morphism $M \to \underline{M}$, i.e. the diagonal morphism $M(T/S) = M \to \underline{M}(T/S) = M^{\pi_0(T)}$. More generally, for an arbitrary sheaf $\mathfrak{F}$, we write $\mathfrak{F} \otimes_{\mathcal{O}} A$ for the sheaf associated to the presheaf $\mathfrak{F} \otimes^p_{\mathcal{O}} A$ defined by the rule $\big(\mathfrak{F} \otimes^p_{\mathcal{O}} A\big)(T/S) := \mathfrak{F}(T) \otimes^p_{\mathcal{O}} A(T)$.

LEMMA A.1. *The canonical morphism $M \otimes_{\mathcal{O}} A \to \underline{M} \otimes_{\mathcal{O}} A$ is an isomorphism as sheaves on the big étale site or the étale site.*

PROOF. After a base change to an arbitrary S-scheme T, i.e. after restricting the values of our functors to étale T-schemes T'/T we may work with the étale site. Suffices to check that the canonical morphism is an isomorphism on the stalks (see [9, II Theorem 2.15] or [15, II Theorem (5.6) *iii*)]). Let $\overline{s} \to S$ be a geometric point and let $\mathcal{O}_{S,\overline{s}} = \varinjlim \mathcal{O}_U$ be the strict henselization of $\mathcal{O}_{S,s}$, where the limit runs over all étale neightbourhoods of $\overline{s}$. Set $S_{\overline{s}} := \mathfrak{Spec}\big(\mathcal{O}_{S,\overline{s}}\big) = \varprojlim U$. If $\mathfrak{F}$ is a presheaf on the étale site, $\mathfrak{F}_{\overline{s}} = \big(\mathfrak{F}^{\#}\big)_{\overline{s}}$ where $\mathfrak{F}^{\#}$ is the associated sheaf (see [9, II Remark 2.14 (*c*)]); in particular $(\underline{M} \otimes_{\mathcal{O}} A)_{\overline{s}} = \big(\underline{M} \otimes^p_{\mathcal{O}} A\big)_{\overline{s}}$. There is a canonical morphism

$$\mathfrak{F}_{\overline{s}} = \varinjlim \mathfrak{F}(U) \to \mathfrak{F}\Big(\varprojlim U\Big) = \mathfrak{F}(S_{\overline{s}}).$$

Since $\mathfrak{F} = M \otimes_{\mathcal{O}} A$ is an S-scheme of finite type, $\varinjlim (M \otimes_{\mathcal{O}} A)(U) = (M \otimes_{\mathcal{O}} A)\Big(\varprojlim U\Big)$ (see [9, II Remarks 2.9 (*d*)]). Similarly, since we may assume that the Us appearing in $\varinjlim \mathcal{O}_U$ are connected, A is an S -scheme of finite type, the formation of direct limits commutes with tensor products and $S_{\overline{s}}$ is connected,

$$\begin{aligned}\varinjlim \big(\underline{M} \otimes^p_{\mathcal{O}} A\big)(U) &= \varinjlim (M \otimes_{\mathcal{O}} A(U)) = M \otimes_{\mathcal{O}} \varinjlim A(U) \\ &= M \otimes_{\mathcal{O}} A\Big(\varprojlim U\Big) = \big(\underline{M} \otimes^p_{\mathcal{O}} A\big)(S_{\overline{s}}).\end{aligned}$$

Summarizing we have canonical identifications $(M \otimes_{\mathcal{O}} A)_{\overline{s}} = (M \otimes_{\mathcal{O}} A)(S_{\overline{s}})$, $(\underline{M} \otimes_{\mathcal{O}} A)_{\overline{s}} = \big(\underline{M} \otimes^p_{\mathcal{O}} A\big)(S_{\overline{s}})$ and the canonical morphism Δ induces on the stalks the morphism $\Delta^p(S_{\overline{s}})$, which is the identity since $S_{\overline{s}}$ is connected. □

We sketch a proof of the following well known fact.

PROPOSITION A.2. *Let A be an abelian S-scheme (with $\mathcal{O}$-multiplication) and let $0 \neq \lambda \in \mathfrak{Q}$ be an element of an invertible $\mathcal{O}$-module $\mathfrak{Q}$. Then $\mathfrak{Q} \otimes_{\mathcal{O}} A$ is an abelian S-scheme of the same dimension as A,*

$$\begin{aligned}\lambda : A &\to \mathfrak{Q} \otimes_{\mathcal{O}} A \\ \lambda(a) &:= \lambda \otimes_{\mathcal{O}} a\end{aligned}$$

is a faithful flat morphism, $A[\lambda] := \ker \lambda$ is finite and flat over S and

$$\#A[\lambda] = \#\frac{\mathfrak{Q}^2}{\lambda\mathcal{O}},$$

where $\#A[\lambda]$ is the order of the finite S-scheme $A[\lambda]$. Furthermore, if $\#\dfrac{\mathfrak{L}}{\lambda\mathcal{O}}$ is invertible on S, λ is étale (and hence $A[\lambda]$ is S-étale).

PROOF. Consider the exact sequence

$$0 \to \mathcal{O} \xrightarrow{\lambda} \mathfrak{L} \to \frac{\mathfrak{L}}{\lambda\mathcal{O}} \to 0.$$

We view A as a sheaf for the fppf topology and apply $- \otimes_{\mathcal{O}} A$. Since $\mathfrak{L}$ is $\mathcal{O}$-flat, $Tor^1_{\mathcal{O}}(\mathfrak{L}, A) = 0$, and, since A is divisible and $\dfrac{\mathfrak{L}}{\lambda\mathcal{O}}$ finite, $\dfrac{\mathfrak{L}}{\lambda\mathcal{O}} \otimes_{\mathcal{O}} A = 0$. It follows that we have

$$0 \to Tor^1_{\mathcal{O}}\left(\frac{\mathfrak{L}}{\lambda\mathcal{O}}, A\right) \to A \xrightarrow{\lambda} \mathfrak{L} \otimes_{\mathcal{O}} A \to 0.$$

In particular, since $Tor^1_{\mathcal{O}}\left(\dfrac{\mathfrak{L}}{\lambda\mathcal{O}}, A\right) = A[\lambda]$ is finite, $\mathfrak{L} \otimes_{\mathcal{O}} A$ is an abelian S-scheme of the same dimension as A. We also see that λ is an isogeny, hence a faithful flat morphism and an étale morphism when $\#A[\lambda]$ is divisible on S. In order to compute the degree $\#A[\lambda]$ of the finite S-group scheme $A[\lambda]$, we first assume that $(\lambda, \mathfrak{L}) = (\lambda, \mathcal{O})$, so that $\lambda \in \mathcal{O} \subset End_S(A)$ is just the multiplication by λ map. Since $A[\lambda]$ is S-flat, working with each connected component of S, we may first assume that S is connected and then compute the degree of $A[\lambda]$ over S after a base change to the residue field $k(s)$ at any $s \in S$. Hence we may assume that $S = \mathfrak{Spec}(K)$ for a field K. Setting $N(\lambda) := \#A[\lambda]$, we see that N is a norm form on $F/\mathbb{Q}$ homogeneus of degree $2\dim_S A$ (by [10, III §19 Theorem 2]). It follows from [10, III § 19 Lemma] and our assumption $\dim_S(A) = [F : \mathbb{Q}]$ that we have $N = N^2_{F/\mathbb{Q}}$, so that $\#A[\lambda] = N^2_{F/\mathbb{Q}}(\lambda)$ for $\lambda \in \mathcal{O}$. The claim when $\mathfrak{L} = \mathcal{O}$ follows from the fact that $N_{F/\mathbb{Q}}(\lambda) = \#\dfrac{\mathcal{O}}{\lambda\mathcal{O}}$ because $\mathcal{O}$ is a lattice in F. We now remark that, if we have given $(\lambda_i, \mathfrak{L}_i)$ with $\lambda \in \mathfrak{L}_i$ an invertible $\mathcal{O}$-module, $i = 1, 2$ and if we assume that $\#\dfrac{\mathfrak{L}_1}{\lambda_1\mathcal{O}}$ is prime to $\#\dfrac{\mathfrak{L}_2}{\lambda_2\mathcal{O}}$, the morphism

$$\mu_{\lambda_1,\lambda_2} : \mathfrak{L}_1 \oplus \mathfrak{L}_2 \to \mathfrak{L}_1 \otimes_{\mathcal{O}} \mathfrak{L}_2$$
$$\mu_{\lambda_1,\lambda_2}(l_1, l_2) := l_1 \otimes \lambda_2 + \lambda_1 \otimes l_2$$

induces an isomorphism $\dfrac{\mathfrak{L}_1}{\lambda_1\mathcal{O}} \oplus \dfrac{\mathfrak{L}_2}{\lambda_2\mathcal{O}} \simeq \dfrac{\mathfrak{L}_1 \otimes_{\mathcal{O}} \mathfrak{L}_2}{\lambda_1 \otimes_{\mathcal{O}} \lambda_2\mathcal{O}}$. We apply this remark

as follows. We take $(\lambda_1, \mathfrak{L}_1) = (\lambda, \mathfrak{L})$ and $(\lambda_2, \mathfrak{L}_2) = (\lambda', \mathfrak{L}^{-1})$, where $\lambda' \in \mathfrak{L}^{-1}$ is choosen so that $\#\frac{\mathfrak{L}}{\lambda\mathcal{O}}$ is prime to $\#\frac{\mathfrak{L}^{-1}}{\lambda'\mathcal{O}}$. We deduce that $\#\frac{\mathcal{O}}{\lambda\lambda'\mathcal{O}} = \#\frac{\mathfrak{L}}{\lambda\mathcal{O}} \cdot \frac{\mathfrak{L}^{-1}}{\lambda'\mathcal{O}}$. On the other hand, we may consider the composition

$$\lambda'\lambda : A \xrightarrow{\lambda} \mathfrak{L} \otimes_{\mathcal{O}} A \xrightarrow{\lambda'} \mathfrak{L}^{-1} \otimes_{\mathcal{O}} \mathfrak{L} \otimes_{\mathcal{O}} A = A$$

and deduce $\#A[\lambda\lambda'] = \#A[\lambda] \cdot \#(\mathfrak{L} \otimes_{\mathcal{O}} A)[\lambda']$. By the case $\mathfrak{L} = \mathcal{O}$ we get

$$\#\frac{\mathfrak{L}}{\lambda\mathcal{O}} \cdot \#\frac{\mathfrak{L}^{-1}}{\lambda'\mathcal{O}} = \#A[\lambda] \cdot \#(\mathfrak{L} \otimes_{\mathcal{O}} A)[\lambda'].$$

Since $Tor^1_{\mathcal{O}}\left(\frac{\mathfrak{L}}{\lambda\mathcal{O}}, A\right) = A[\lambda]$ and $Tor^1_{\mathcal{O}}\left(\frac{\mathfrak{L}^{-1}}{\lambda'\mathcal{O}}, \mathfrak{L} \otimes_{\mathcal{O}} A\right) = (\mathfrak{L} \otimes_{\mathcal{O}} A)[\lambda']$, our choice of λ' so that $\#\frac{\mathfrak{L}}{\lambda\mathcal{O}}$ is prime to $\#\frac{\mathfrak{L}^{-1}}{\lambda'\mathcal{O}}$ implies that $\#A[\lambda]$ is prime to $(\mathfrak{L} \otimes_{\mathcal{O}} A)[\lambda']$ too. We deduce $\#\frac{\mathfrak{L}}{\lambda\mathcal{O}} = \#A[\lambda]$.

PROPOSITION A.3. *If $\mathcal{O}_\mathfrak{l}$ is a discrete valuation ring, the horizontal inclusions appearing in* (11) *have torsion free cokernel.*

PROOF. It suffices to show that the lower horizontal inclusion and the left vertical inclusion in (11) have torsion free cokernel, since then the torsion freeness of the upper horizontal inclusion follows from the commutativity of (11). Furthermore, to see that the left vertical inclusion has torsion free cokernel it suffices to show that the inclusion of $Hom^{Sym}_{\mathcal{O}}(A, A^t)$ in $Hom_{\mathcal{O}}(A, A^t)$ has torsion free cokernel. Suppose that $\lambda \in Hom_{\mathcal{O}}(A, A^t)$ is such that there exists $0 \neq n \in \mathbb{Z}$ such that $n\lambda \in Hom^{Sym}_{\mathcal{O}}(A, A^t)$. Then $n\lambda = (n\lambda)^t$ and the right hand side is $\lambda^t n^t = \lambda^t n$, while the left hand side is λn. Hence $\lambda n = \lambda^t n$ and, since n is an isogeny, it is an epimorphism in the category of sheaves for the fppf topology on S and the equality $\lambda = \lambda^t$ can be checked at the level of points. That the lower horizontal inclusion has torsion free cokernel follows as in [5, Theorem (12.10), Chapter 12], thanks to our assumption that $\mathcal{O}_\mathfrak{l}$ is a discrete valuation ring. □

Let $\mathfrak{L}$ be an invertible $\mathcal{O}$-module. For every $\sigma : F \hookrightarrow \mathbb{R}$ we may consider $i_\sigma : \mathfrak{L} \hookrightarrow \mathfrak{L} \otimes_\sigma \mathbb{R}$ and define $\mathfrak{L}^{\pm}_\sigma := i_\sigma^{-1}(\mathfrak{L} \otimes_\sigma \mathbb{R}^\times_\pm)$. An oriented invertible $\mathcal{O}$-module is an invertible $\mathcal{O}$-module $\mathfrak{L}$ together with the choice of a vector of

signs $\varepsilon = (\varepsilon_\sigma)$ such that $\varepsilon_\sigma \in \{\pm\}$. An homomorphism $f : (\mathfrak{L}_1, \varepsilon_1) \to (\mathfrak{L}_2, \varepsilon_2)$ of oriented invertibles $\mathcal{O}$-modules is an homomorphism f of $\mathcal{O}$-modules such that $f\left(\mathfrak{L}_{1,\sigma}^{\varepsilon_{1,\sigma}}\right) \subset \mathfrak{L}_{2,\sigma}^{\varepsilon_{2,\sigma}}$. To an orientation ε on $\mathfrak{L}$ we can associate the set of totally positive elements

$$\mathfrak{L}^+ := \bigcap_\sigma \mathfrak{L}_\sigma^{\varepsilon_\sigma} \subset \mathfrak{L}$$

and indeed, the isomorphism class of the oriented $\mathcal{O}$-module $\mathfrak{L}$, is uniquely determined by the couple $\left(\mathfrak{L}^+, \mathfrak{L}\right)$. Furthermore, since $Aut\left(\mathfrak{L}^+, \mathfrak{L}\right) = \mathcal{O}_+^\times$, the set of totally positive units of $\mathcal{O}$, we see that, to give an oriented $\mathcal{O}$ - module $\left(\mathfrak{L}^+, \mathfrak{L}\right)$ (up to isomorphism), is the same as to give an element in the narrow class group associated to the order $\mathcal{O}$.

Consider the functor of symmetric $\mathcal{O}$-linear morphisms:

$$\underline{\mathfrak{L}}(A)(T/S) := Hom_{\mathcal{O}}^{Sym}\left(A_T, A_T^t\right)$$

and the subfunctor $\underline{\mathfrak{L}}^+(A)$ of polarizations (where A_T and A_T^t are the base changes to T). They are in fact sheaves for the étale topology and in [12, Prop. 1.17], when $\mathcal{O} = \mathcal{O}_F$ is the maximal order in a totally real field F, it is proven that $\underline{\mathfrak{L}}(A)$ is locally constant with values in invertible $\mathcal{O}$-modules and generated by $\underline{\mathfrak{L}}^+(A)$. When S is connected and normal, by [12, Variante 1.18] $\underline{\mathfrak{L}}(A)$ is already constant, i.e. $\underline{\mathfrak{L}}(A) = \underline{\mathfrak{L}(A)}$ for the invertible $\mathcal{O}$-module $\mathfrak{L}(A) := \underline{\mathfrak{L}}(A)(T/S) = \underline{\mathfrak{L}}(A)(S)$ where T/S is connected. In general there exists T/S étale such that $\underline{\mathfrak{L}}(A) = \underline{\mathfrak{L}(A_T)}$ restricted to étale T'/T.

Let $\mu^p : \underline{\mathfrak{L}}(A) \otimes_{\mathcal{O}}^p A \to A^t$ be the morphism given by the rule $\mu^p(\lambda \otimes a) := \lambda(a)$, where $\lambda \in Hom_{\mathcal{O}}^{Sym}\left(A_T, A_T^t\right)$ and $a \in A_T(T) = A(T/S)$. Since A^t is a sheaf, it induces a unique

$$\mu : \underline{\mathfrak{L}}(A) \otimes_{\mathcal{O}} A \to A^t. \tag{12}$$

Note that, when $\underline{\mathfrak{L}}(A) = \underline{\mathfrak{L}(A)}$ is constant, μ is identified, via the isomorphism Δ of Lemma A.1 , with the morphism

$$\begin{aligned} &\mu : \mathfrak{L}(A) \otimes_{\mathcal{O}} A \to A^t \\ &\mu(\lambda \otimes a) := \lambda(a) \in A^t(T/S),\ a \in A(T/S) \end{aligned} \tag{13}$$

which is an isogeny being a non-zero map between abelian S-schemes of the same dimension (see also [1, proof of (3)⇒(1) of Proposition 3.1]).

The following proposition is a variant of [1, Proposition 3.1].

PROPOSITION A.4. *The following are equivalent, when $\mathcal{O} = \mathcal{O}_F$:*

(1) $\ker \mu$ *is n-torsion étale sheaf, where μ is* (12);
(2) *for every integer t prime to n there exists T/S étale and $\lambda \in \underline{\mathfrak{L}}^+(A)(T/S)$ of degree prime to t.*

PROOF. In [1, proof of (1) $\Rightarrow$(2) of Proposition 3.1] simply replace [1, (3.6)] with the assertion that $\Phi : (A \otimes_{\mathcal{O}_L} M_A)[t] \hookrightarrow A^\vee[t]$ is an inclusion (notations as in loc. cit.) and note that it is an isomorphism by a comparison of degrees. Hence one recovers [1, (3.6)] and the proof of the implication is the same. [1, proof of (2) $\Rightarrow$ (3) of Proposition 3.1] (with the obvius modification in the statement) is trivial. The analogous of [1, proof of (3) $\Rightarrow$ (1) of Proposition 3.1] is the same but we conclude that K has order prime to l for every prime l prime to n.

COROLLARY A.5. *Suppose that S is connected and normal or, more generally, that $\underline{\mathfrak{L}}(A) = \underline{\mathfrak{L}(A)}$ is a constant sheaf and that $\mathcal{O} = \mathcal{O}_F$. The following are equivalent:*

(1) $\ker \mu$ *is n-torsion étale sheaf, where μ is* (13);
(2) *for every integer t prime to n there exists $\lambda \in \mathfrak{L}^+(A)$ of degree prime to t.*

PROOF. We need to prove that, if there exists $\lambda' \in \underline{\mathfrak{L}}^+(A)(T/S)$ of degree prime to t, there exists $\lambda \in \mathfrak{L}^+(A)$ of the same degree. Since $\underline{\mathfrak{L}}(A) = \underline{\mathfrak{L}(A)}$, $\underline{\mathfrak{L}}(A)(T/S) = \mathfrak{L}(A)^{\pi_0(T)}$. We take any connected component $T_0 \subset T$ of T and we note that the image λ of λ' in $\underline{\mathfrak{L}}(A)(T_0/S) = \mathfrak{L}(A)$, which is simply the T_0-component of $\lambda' \in \mathfrak{L}(A)^{\pi_0(T)}$ (that we may assume to be non-zero), is the required polarization. □

We are now going to show that, under the assumptions of Corollary A.5, condition (1) is always satisfied if we take n to be the product of the primes that are invertible in S. Indeed we will prove a slightly more general statement without assuming that $\mathcal{O} = \mathcal{O}_F$. We first record the following corollary of Propositions A.2 and A.3.

COROLLARY A.6. *If $Hom_{\mathcal{O}}^{Sym}(A, A^t) \neq 0$ and $\mathcal{O}_\mathfrak{l} = \mathcal{O}_{F,\mathfrak{l}}$ coincides with the completion at $\mathfrak{l}$ of the maximal order $\mathcal{O}_F$, the upper horizontal inclusion appearing in* (11) *is an isomorphism*

$$Hom_{\mathcal{O}}^{Sym}\big(A, A^t\big)_\mathfrak{l} = Hom_{\mathcal{O}_\mathfrak{l}}^{Alt}(T, T^*) \simeq \mathcal{O}_\mathfrak{l}.$$

PROOF. For every $\mathcal{O}_\mathfrak{l}$-module T let us denote by $Hom_{\mathcal{O}_\mathfrak{l}}\left(\wedge^2_{\mathcal{O}_\mathfrak{l}} T, \mathcal{O}_\mathfrak{l}\right)$ the $\mathcal{O}_\mathfrak{l}$-module of bilinear forms $b : T \times T \to \mathcal{O}_\mathfrak{l}$ such that $b(x,y) = -b(y,x)$. Under the canonical identification $Hom_{\mathcal{O}_\mathfrak{l}}\left(\otimes^2_{\mathcal{O}_\mathfrak{l}} T, \mathcal{O}_\mathfrak{l}\right) = Hom_{\mathcal{O}_\mathfrak{l}}(T, T^*)$ the submodule $Hom_{\mathcal{O}_\mathfrak{l}}\left(\wedge^2_{\mathcal{O}_\mathfrak{l}} T, \mathcal{O}_\mathfrak{l}\right)$ corresponds to $Hom^{Alt}_{\mathcal{O}_\mathfrak{l}}(T, T^*)$. Proposition A.2 implies that $T_\mathfrak{l}(A)$ is a free rank two module over $\mathcal{O}_\mathfrak{l}$. It follows that $Hom_{\mathcal{O}_\mathfrak{l}}\left(\wedge^2_{\mathcal{O}_\mathfrak{l}} T, \mathcal{O}_\mathfrak{l}\right)$ is free of rank one over $\mathcal{O}_\mathfrak{l}$. Since $Hom^{Sym}_{\mathcal{O}}(A, A^t)$ is torsion free, the inclusion (11) shows that the free $\mathcal{O}_\mathfrak{l}$-module $Hom^{Sym}_{\mathcal{O}}(A, A^t)_\mathfrak{l}$ may have rank 0 or rank 1 (over $\mathcal{O}_\mathfrak{l}$). Under the assumption $Hom^{Sym}_{\mathcal{O}}(A, A^t) \neq 0$ we find that it holds the second possibility and the inclusion is an isomorphism, since it has torsion free cokernel by Proposition A.3. □

LEMMA A.7. *Suppose that S is connected and normal or, more generally, that $\underline{\mathfrak{Q}}(A) = \underline{\mathfrak{Q}(A)}$ is a constant sheaf. Let $n_{S,\mathcal{O}} \in \mathbb{N}$ be the product of those primes $l \in \mathbb{N}$ that are invertible in S or such that $\mathcal{O}_l = \mathcal{O}_{F,l}$ (i.e. l is coprime with the conductor of $\mathcal{O}$ in the maximal order $\mathcal{O}_F$). Then the primes dividing $\#\ker\mu$ divides $n_{S,\mathcal{O}}$ and, in particular,* $\ker\mu$ *is an $n_{S,\mathcal{O}}$-torsion étale sheaf.*

PROOF. As we already remarked μ in (13) is an isogeny. Let l be a prime that is invertible on S: for every such prime, to prove that μ is an isogeny of degree coprime with l, it is sufficient to show that $T_l(\mu)$ is an isomorphism. Whenever $\mathcal{O}_l = \mathcal{O}_{F,l}$ this is equivalent to checking that $T_\mathfrak{l}(\mu)$ is an isomorphism for every prime $\mathfrak{l} \mid l$. The formation of the $\mathfrak{l}$-adic Tate module, commutes with taking tensor product with flat $\mathcal{O}$-modules, so that:

$$T_\mathfrak{l}(\mathfrak{Q}(A) \otimes_{\mathcal{O}} A) = \mathfrak{Q}(A) \otimes_{\mathcal{O}} T_\mathfrak{l}(A) = \mathfrak{Q}(A)_\mathfrak{l} \otimes_{\mathcal{O}_\mathfrak{l}} T_\mathfrak{l}(A).$$

For every $\mathcal{O}_\mathfrak{l}$-module write $\mathfrak{Q}^{Alt}(T) := Hom^{Alt}_{\mathcal{O}_\mathfrak{l}}(T, T^*)$ for shortness. Consider the canonical morphism:

$$\mu = \mu_T : \mathfrak{Q}(A)_\mathfrak{l} \otimes_{\mathcal{O}_\mathfrak{l}} T_\mathfrak{l}(A) \to T^*$$
$$\lambda \otimes t \mapsto \lambda(t).$$

The canonical inclusion $\mathfrak{Q}(A)_\mathfrak{l} \subset \mathfrak{Q}^{Alt}(T_\mathfrak{l}(A))$ gives the following commutative diagram:

$$\begin{array}{ccc} \mathfrak{Q}(A)_\mathfrak{l} \otimes_{\mathcal{O}_\mathfrak{l}} T_\mathfrak{l}(A) & \overset{T_\mathfrak{l}(\mu_A)}{\to} & T_\mathfrak{l}(A)^* \\ \cap & & \| \\ \mathfrak{Q}^{Alt}(T_\mathfrak{l}(A)) \otimes_{\mathcal{O}_\mathfrak{l}} T_\mathfrak{l}(A) & \overset{\mu_{T_\mathfrak{l}(A)}}{\to} & T_\mathfrak{l}(A)^* \end{array}$$

Since $\mathfrak{L}(A) \neq 0$ and $\mathcal{O}_{\mathfrak{l}} = \mathcal{O}_{F,\mathfrak{l}}$, by Corollary A.6 the left vertical inclusion is an isomorphism. In other words the problem is reduced to the analogous problem in the category of $\mathcal{O}_{\mathfrak{l}}$-modules, i.e. we must show that, for every free rank 2 $\mathcal{O}_{\mathfrak{l}}$-module T, the canonical morphism μ_T is an isomorphism. This is a consequence of the subsequent algebraic Lemma A.8 □

LEMMA A.8. *Let T be a finitely generated free module over a commutative ring R. The canonical morphism*

$$\mu_T : Hom_R^{Alt}(T, T^*) \otimes T \to T^*$$
$$f \otimes t \mapsto f(t)$$

is surjective if $\operatorname{rank}(T) \neq 1$ *with projective kernel. Furthermore we have (with the convention that* $\operatorname{rank} \leq 0$ *means* $\operatorname{rank} = 0$*):*

$$\operatorname{rank}(T^*) = \operatorname{rank}(T),$$
$$\operatorname{rank}\big(Hom\big(\wedge^2 T, R\big) \otimes T\big) = \frac{\operatorname{rank}(T)^2(\operatorname{rank}(T) - 1)}{2},$$
$$\operatorname{rank}(\ker \mu_T) = \frac{\operatorname{rank}(T)(\operatorname{rank}(T) - 2)(\operatorname{rank}(T) + 1)}{2}.$$

In particular μ_T is an isomorphism if and only if $\operatorname{rank}(T) = 2$ *or* 0.

PROOF. Up to the canonical identification $Hom_R^{Alt}(T, T^*) = Hom_R\big(\wedge_R^2 T, R\big)$ the morphism μ_T corresponds to the canonical morphism:

$$\mu_T : Hom_R\big(\wedge_R^2 T, R\big) \otimes T \to T^*$$
$$b \otimes t \mapsto b(t, -).$$

Choose a basis $\{e_i : i = 1, \dots, n\}$ of T and let $\{\delta_i\}$ be the dual basis of $\{e_i\}$, defined by the rule $\delta_i(e_j) = \delta_{ij}$. By viewing the elements of T like column vectors with respect to the basis $\{e_i\}$, the element e_i corresponds to the column 1_i which is zero at all its entries with the only exception of the i-entry, which is equal to 1, and similarly δ_i corresponds to the row vector 1_i^t which is equal to zero at all its entries with the only exception of the i-entry, which is equal to 1. Furthermore any element of $b \in Hom\big(\wedge^2 T, R\big)$ corresponds to a matrix $\boldsymbol{b} = \big(b_{ij}\big)$ which has zeros on the diagonal and such that $b_{ij} = -\,b_{ij}$ for $i \neq j$. In particular a basis of $Hom\big(\wedge^2 T, R\big)$ is obtained from the elements $b_{i_0 j_0} \in Hom\big(\wedge^2 T, R\big)$ with $i_0 > j_0$ that corresponds to the

matrices $\boldsymbol{b}_{i_0j_0}$ with $b_{ij}=0$ whenever $(i,j)\neq(i_0,j_0)$ or (j_0,i_0) and $b_{i_0j_0}=1$. The assertion on the rank of $Hom\big(\wedge^2 T,R\big)\otimes T$ follows. We have

$$b_{i_0j_0}(e_k,-)=1_k^t\cdot\boldsymbol{b}_{i_0j_0}\cdot-=\begin{cases}0 & \text{if } k\neq i_0,j_0\\ 1_{j_0}^t=\delta_{j_0} & \text{if } k=i_0\\ -1_{i_0}^t=-\delta_{i_0} & \text{if } k=j_0.\end{cases}$$

Now suppose $\operatorname{rank}(T)\geq 2$, the other cases being trivial, and that we have given δ_h with $h\in\{1,\dots,n-1\}$: then we have $b_{nh}(e_n,-)=\delta_h$. Similarly suppose that we have given δ_h with $h\in\{2,\dots,n\}$: then we have $b_{h1}(e_1,-)=-\delta_h$. The surjectiveness of μ_T follows and, since T^* is a free R-module, there is a section of μ_T. Hence $\ker\mu_T$ appears like a direct addendum of the free module $Hom\big(\wedge^2 T,R\big)\otimes T$ and it has to be a projective R-module. Having computed the rank of $Hom\big(\wedge^2 T,R\big)\otimes T$, the assertion on the rank of $\ker\mu_T$ follows. □

LEMMA A.9. *The property of having an $\mathcal{O}$-polarization (over S) of degree coprime with a fixed integer $t\in\mathbb{N}$ is invariant under $\mathcal{O}$-isogenies (over S) of degree prime to t.*

PROOF. Let $\lambda:A\to B$ be an $\mathcal{O}$-isogeny of degree prime to t between two S-schemes and let $B\to B^t$ be the polarization $\varphi_{\mathcal{L}}$ induced by the ample line bundle $\mathcal{L}$, of degree prime to t. By definition one easily check the equality $\varphi_{\lambda^*\mathcal{L}}=\lambda^t\varphi_{\mathcal{L}}\lambda$: the left hand side shows that we get a polarization on A, since the pull-back of an ample line bundle by a finite morphism is an ample line bundle; the right hand side shows that, this polarization, is of degree coprime with t. □

LEMMA A.10. *Let A be an abelian S -scheme with multiplication by an order $\mathcal{O}$ in a field F and fix an integer $t\in\mathbb{N}$. There is an $\mathcal{O}$-linear isogeny of degree coprime with t (over S) $\lambda:A\to B$ of A into an abelian S-scheme B with multiplication by the maximal order $\mathcal{O}_F$.*

PROOF. Choose an invertible ideal $\mathfrak{I}\subset\mathcal{O}$ such that $\#\dfrac{\mathcal{O}}{\mathfrak{I}}$ is prime to t and the conductor $\mathfrak{f}(\mathcal{O})$ of the order $\mathcal{O}$ (in the maximal order). Then $\mathfrak{I}$ is an invertible $\mathcal{O}$-ideal and it is $\mathcal{O}_F$-stable. The inclusion $\mathcal{O}\subset\mathfrak{I}^{-1}=Hom_{\mathcal{O}}(\mathfrak{I},\mathcal{O})$ yields an $\mathcal{O}$-linear isogeny (see [6, 2.4]):

$$\lambda_{A,\mathfrak{I}}:A\to\mathfrak{I}^{-1}\otimes_{\mathcal{O}}A$$

which is of degree a power of $\#\dfrac{\mathcal{O}}{\mathfrak{I}}$, hence prime to t, and moreover $\mathfrak{I}^{-1}\otimes_{\mathcal{O}} A$ has a canonical structure of $\mathcal{O}_F$-module, since $\mathfrak{I}^{-1}$ is an $\mathcal{O}_F$-module. □

We are now ready to prove the main result of the appendix.

THEOREM A.11. *Let A/S be an abelian S-scheme over a conneced and normal scheme S, with real multiplication by an order $\mathcal{O}$ in a totally real number field F such that* $\dim_S A = [F:\mathbb{Q}]$ *and further assume that A^t/S exists. For every integer $t\in\mathbb{N}$ which is invertible in S there is an $\mathcal{O}$-linear polarization of degree prime to t.*

In particular, if $S=\mathfrak{Spec}(K)$ for a field K, we may find an $\mathcal{O}$-linear polarization of degree prime to t for every t prime to the characteristic of K.

PROOF. Let $n_{S,\mathcal{O}}$ be as in Lemma A.7 and let n_S be the product of those primes that are invertible in S. Thanks to Lemmas A.9 and A.10 we may assume $\mathcal{O}=\mathcal{O}_F$, so that $n_{S,\mathcal{O}}=n_S$. By Lemma A.7 $\ker\mu$ is an $n_{S,\mathcal{O}}=n_S$-torsion étale sheaf. Corollary A.5 gives the claim. □

Acknowledgments. The author would like to thank Professor Massimo Bertolini for his many advices. It is also a pleasure to thank the anonymous referee for its suggestions, that led to a substantial improvement of the earlier version of the paper. The reference [1], provided by the referee, has been particularly useful for clarifying the results of the appendix.

REFERENCES

[1] F. ANDREATTA - E. Z. GOREN, *Geometry of Hilbert modular varieties over totally ramified primes*, Internat. Math. Res. Notices, **33** (2003), pp. 1785–1835.

[2] S. BLOCH - K. KATO, *L-functions and Tamagawa numbers of motives, in: The Grothendieck Festschrift*, Vol. I, Prog. in Math. 86, Birkhauser, Boston (1990), P. Cartier, et al., eds., pp. 333–400.

[3] P. DELIGNE - G. PAPPAS, *Singularités des espaces de modules de Hilbert, en les caractérisque divisant le discriminant*, Compos. Math., **90**, No. 1 (1994), pp. 59–79.

[4] M. FLACH, *A generalisation of the Cassels-Tate pairing*, J. Reine Angew. Math., **412** (1990), pp. 113–127.

[5] G. VAN DER GEER, *Abelian varieties*. Manuscript available at http://staff.science.uva.nl/~bmoonen/boek/BookAV.html.

[6] B. H. GROSS - J. PARSON, *On the local divisibility of Heegner points*. Lang Memorial Volume.

[7] B. MAZUR - K. RUBIN, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2), **166**, No. 2 (2007), pp. 579–612.
[8] B. MAZUR - K. RUBIN - A. SILVERBERG, *Twisting commutative algebraic groups*, J. Algebra, **314**, No. 1 (2007), pp. 419–438.
[9] J. S. MILNE, *Etale cohomology*, Princeton University Press (1980).
[10] D. MUMFORD, *Abelian varieties*, Oxford University Press (1970).
[11] JAN NEKOVÁR, *Selmer complexes*, Astérisque, **310** (2006).
[12] M. RAPOPORT, *Compactifications de l'Espace de Modules de Hilbert-Blumenthal, Compos.* Math., **36** (1978), pp. 255–335.
[13] M. A. SEVESO, *Stark-Heegner points and Selmer groups of abelian varieties*, PhD Thesis, University of Milan, Federigo Enriques Department of Mathematics.
[14] M. A. SEVESO, *Congruences and rationality of Stark-Heegner points*, to appear in the Journal of Number Theory, doi: 10.1016/j.jnt.2011.10.001.
[15] G. TAMME, *Introduction to étale cohomology*, Springer-Verlag (1994).

Manoscritto pervenuto in redazione il 6 agosto 2010.