Root numbers, Selmer groups, and non-commutative Iwasawa theory

John Coates, Takako Fukaya, Kazuya Kato, Ramdorai Sujatha

November 4, 2008

1 Introduction

Global root numbers have played an important role in the study of rational points on abelian varieties since the discovery of the conjecture of Birch and Swinnerton-Dyer. The aim of this paper is to throw some new light on this intriguing and still largely conjectural relationship. The simplest avatar of this phenomenon is the parity conjecture which asserts that for an abelian variety A over a number field F, and for each prime number p, the $\mathbb{Z}_p$-corank of the Selmer group of A over F should have the same parity as the root number of the complex L-function of A. Many affirmative results in this direction have been established when A is an elliptic curve, notably by B. Birch and N. Stephens [4], T. and V. Dokchitser [17], [18], R. Greenberg and L. Guo [24], B-D. Kim [28], P. Monsky [33], and J. Nekovář [34], [35]. In §1, we use ideas due to Cassels, Fisher [15, Appendix], Shuter [43], and T.Dokchitser and V. Dokchitser [17] to prove with some technical restrictions, the parity conjecture for the prime p and and an abelian variety A of dimension g over a number field F having an isogeny of degree p^g. In the rest of the paper, we give some fragmentary evidence that there is a close connexion between root numbers and the Selmer group of an elliptic curve E over certain non-commutative p-adic Lie extensions of the base field F. The non-commutativity of the Galois group of these p-adic Lie extensions is important for us, because we are interested in cases in which there are infinite families of irreducible self-dual Artin representations of this group. In fact, for two non-commutative p-adic Lie extensions, we prove analogues of the parity conjecture for twists of both the Selmer group and the complex L-function by all irreducible, orthogonal Artin representations of the Galois group. Our results have some overlap with the recent work of Mazur and Rubin [30], [31], and T. and V. Dokchitser [19] although our viewpoint is rather different in that our proofs use methods and invariants arising from Iwasawa theory. Because of our use of Iwasawa theory, our results at present require much stronger hypotheses than these authors. However one advantage of our approach is that it provides both upper and lower bounds for the $\mathbb{Z}_p$-corank of the Selmer group, and surprisingly in some cases the two bounds coincide (see also [16, Appendix]).

One advantage of our approach is that it provides both upper and lower bounds for the $\mathbb{Z}_p$-corank of the Selmer group, and surprisingly in some cases the two bounds coincide (see also [16, Appendix]). We also believe that our methods are rather general, and can be used to establish analogous results for a wide class of p-adic Lie extensions, which contain the cyclotomic $\mathbb{Z}_p$-extension of the base field F. Another suprising aspect of our work is that it provides some evidence that there may be rather strong uniform upper bounds for the order of zero at s=1 of the twists of the complex L-function of E by the infinite family of all irreducible Artin representations of any fixed p-adic Lie extension of F of infinite degree.

We are extremely grateful to the generous help we have received from many colleagues while preparing this paper. In particular, we wish to thank T. Dokchitser, V. Dokchitser and D. Rohrlich for providing us with illuminating computations related to global root numbers, which play a vital role in §4 and §6. We would also like to thank R. Greenberg for informing us of the beautiful generalisation of his earlier theorem with L. Guo (see Theorem 3.8), which is crucial in our work. The second author gratefully acknowledges support from a JSPS Postdoctoral Fellowship held at DPMMS, Cambridge University, and the first, second and fourth authors gratefully acknowledge support from RIMS and Kyoto University.

2 On the parity of the $\mathbb{Z}_p$-corank of Selmer

Let A be an abelian variety of dimension g defined over a finite extension F of $\mathbb{Q}$, and let p be a prime number. As F will be fixed throughout this section, we shall often omit it from the notation. We recall that the p-primary part $S(A)$ of the Selmer group of A is defined by

$$S(A) = \mathrm{Ker}\,(H^1(F, A_{p^\infty}) \to \prod_v H^1(F_v, A(\bar{F}_v))),$$

where A_{p^∞} denotes the Galois module of all p-power division points on A, and v runs over all places of F. It is a basic elementary result that $S(A)$ is a cofinitely generated $\mathbb{Z}_p$-module, and we write $s(A)$ for its $\mathbb{Z}_p$-corank. Let $w(A) = \pm 1$ be the root number occurring in the conjectural functional equation of the complex L-function of A. The parity conjecture asserts that we should have

$$w(A) = (-1)^{s(A)} \tag{1}$$

for all prime numbers p. The aim of this section is to prove the parity conjecture for the prime p when A admits an isogeny of degree p^g, subject to some technical restrictions on p.

Let A^* denote the dual abelian variety. We write $A[p]$ for the Galois module of p-division points on A, and let

$$\langle\ ,\ \rangle_{A,p} : A[p] \times A^*[p] \to \mu_p$$

be the Weil pairing, where μ_p denotes the Galois module of p-th roots of unity.

Theorem 2.1. *The parity conjecture* (1) *holds for A and p when the following conditions are satisfied:-*

(i) *There is a subgroup C of $A[p]$ of order p^g, stable under* $\mathrm{Gal}(\bar{F}/F)$*, and an isogeny $\psi : A \to A^*$ of degree prime to p, such that the dual isogeny $\psi^* : A = (A^*)^* \xrightarrow{\psi^*} A^*$ coincides with ψ, and also such that the Weil pairing $\langle\ ,\ \rangle_{A,p}$ annihilates $C \times \psi(C)$;*

(ii) *Either $p \geq 2g+2$, or $p \geq g+2$ and A has semistable reduction at each finite place v of F;*

(iii) *For each place v of F dividing p, either A is potentially ordinary at v, or A achieves semistable reduction over a finite abelian extension of F_v.*

By potentially ordinary at v, we mean that there is a finite extension L of F_v such that A has semistable reduction over L, and in addition, the connected component of the special fiber of the Néron model of $A \otimes_F L$ is an extension of an ordinary abelian variety by a torus. In particular, A is potentially ordinary at v if A has potentially good ordinary reduction at v. If A is an elliptic curve, A is potentially ordinary at v if and only if either A has potentially good ordinary reduction at v, or potentially multiplicative reduction at v.

Corollary 2.2. *Assume p is an odd prime number, and that E/F is an elliptic curve admitting an F-isogeny of degree p. If $p = 3$, assume that E has semistable reduction at each finite place of F. If $p > 3$, suppose that for each prime v of F dividing p, either E has potentially good ordinary reduction at v, or E has potentially multiplicative reduction at v, or E achieves good supersingular reduction over a finite abelian extension of F_v. Then the parity conjecture* (1) *holds for E and p.*

Our proof of Theorem 2.1 has been inspired by the work of [15], Appendix by T. Fisher, [17], [43], and has its origin in the work of Cassels. A slightly weaker version of Corollary 2.2 is already proven in [17]. We also note that [18] proves that the parity conjecture (1) holds for all elliptic curves E over $\mathbb{Q}$, and for all primes p, generalizing the works in [34], [35], [28].

We first show how the ideas going back to Cassels lead to a parity statement for $s(A)$ when A is an abelian variety of any dimension over F which satisfies (i) of Theorem 2.1. For a slightly different approach, which includes the case $p = 2$, see also [18], especially Theorem 4.3 there and its proof. If $g : M_1 \to M_2$ is any homomorphism of abelian groups whose kernel and cokernel are both finite, we define

$$\chi(g) = \sharp(\mathrm{Coker}\,(g))/\sharp(\mathrm{Ker}\,(g)). \tag{2}$$

We assume A satisfies (i) of Theorem 2.1. Let $A' = A/C$, and let $\phi : A \to A'$ be the associated isogeny. For each place v of F, we define

$$h(v) = \mathrm{ord}_p \chi(\phi_v), \tag{3}$$

where $\phi_v : A(F_v) \to A'(F_v)$ is the homomorphism induced by ϕ (of course, ϕ_v has finite kernel and cokernel). By an elementary argument, one can check that $h(v) = 0$ for almost all places v of F.

Theorem 2.3. *Let A/F be an abelian variety satisfying* (i) *of Theorem 2.1, with p an odd prime number. Then*

$$s(A) \equiv \sum_{v} h(v) \mod 2, \tag{4}$$

where the sum is taken over all finite and infinite places of F.

Proof. If M is any cofinitely generated $\mathbb{Z}_p$-module, we define M_{div} to be the maximal divisible subgroup of M, and put

$$M_{\mathrm{nd}} = M/M_{\mathrm{div}}, \quad T_p(M) = \varprojlim_{n} (M)_{p^n}, \tag{5}$$

where $(M)_{p^n}$ denotes the kernel of multiplication by p^n on M. For an abelian group M, $M(p)$ will denote the p-primary torsion subgroup of M. For any compact or discrete $\mathbb{Z}_p$-module M, $M^{\vee}$ will denote its Pontrjagin dual $\mathrm{Hom}_{\mathrm{cont}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$.

Let $\phi^* : (A')^* \to A^*$ be the dual isogeny of ϕ. We write

$$\phi_S : S(A) \to S(A'), \quad \phi_S^* : S((A')^*) \to S(A^*)$$

for the homomorphisms induced by ϕ and ϕ^*. Let Σ denote any finite set of places of F, which contains all places lying over p, all archimdean places, and all finite places where A has bad reduction. The first step in the proof is to use Cassels' variant of the Poitou-Tate sequence (see [32], Chap. 1) to prove that

$$\frac{\chi(\phi_S)}{\chi(\phi_S^*)} \cdot \prod_{v \in \Sigma} \chi(\phi_v) = \frac{\sharp(S(A')_{\mathrm{nd}})}{\sharp(S(A)_{\mathrm{nd}})} \cdot \frac{\sharp(A^*(F)(p))}{\sharp(A(F)(p))} \cdot \frac{\sharp(A'(F)(p))}{\sharp((A')^*(F)(p))}. \tag{6}$$

To establish this formula, we need three preparatory lemmas. Put

$$G_\Sigma = \mathrm{Gal}(F_\Sigma/F)$$

where F_Σ is the maximal Galois extension of F in which all places of F outside Σ are unramified. Since p is assumed to be odd, G_Σ has p-cohomological dimension equal to 2. If M is any finite G_Σ-module, we write

$$\chi(G_\Sigma, M) = \prod_{i=0}^{2} \sharp(H^i(G_\Sigma, M))^{(-1)^i}.$$

As $C = \mathrm{Ker}\,(\phi)$, it follows from the Weil pairing that $\mathrm{Ker}\,(\phi^*) = C^{\vee}(1)$. Hence ϕ^* gives rise to an exact sequence of Galois modules

$$0 \to C^{\vee}(1) \to (A')^*_{p^\infty} \to A^*_{p^\infty} \to 0. \tag{7}$$

For $m = 0, 1, 2$, write

$$\alpha_m : H^m(G_\Sigma, (A')^*_{p^\infty}) \to H^m(G_\Sigma, A^*_{p^\infty}) \tag{8}$$

for the homomorphisms induced by ϕ^*.

Lemma 2.4.

$$\frac{\chi(\alpha_1)}{\chi(\alpha_0)\chi(\alpha_2)} = \prod_{v|\infty} \chi(\phi_v),$$

where the product is taken over all archimedean places of F.

Proof. By the long exact sequence of cohomology arising from (7), we have

$$\frac{\chi(\alpha_1)}{\chi(\alpha_0)\chi(\alpha_2)} = \chi(G_\Sigma, C^\vee(1)).$$

On the other hand, since p is odd, Tate's Euler characteristic formula [32, Theorem 5.1], asserts that

$$\chi(G_\Sigma, C^\vee(1)) = \prod_{v|\infty} \sharp(H^0(F_v, C))^{-1}.$$

Again, since p is odd, it is clear that the right hand side of this last formula is equal to $\prod_{v|\infty} \chi(\phi_v)$, as required. □

We next define

$$P(A) = \varprojlim_n \; S_{p^n}(A),$$

where

$$S_{p^n}(A) = \mathrm{Ker}\,(H^1(F, A_{p^n}) \to \prod_v H^1(F_v, A(\bar{F}_v))).$$

It is easily seen that we have an exact sequence

$$0 \to A(F)(p) \to P(A) \to T_p(S(A)) \to 0. \tag{9}$$

Note also that $T_p(S(A)) = T_p(S(A)_{\mathrm{div}})$. Now the isogeny $\phi : A \to A'$ induces homomorphisms

$$\beta_1 : P(A) \to P(A'), \quad \beta_2 : S(A)_{\mathrm{div}} \to S(A')_{\mathrm{div}}.$$

Lemma 2.5.

$$\chi(\beta_1) = \frac{\sharp A'(F)(p)}{\sharp A(F)(p)} \cdot \frac{1}{\chi(\beta_2)}.$$

Proof. Let $\gamma : T_p(S(A)_{\mathrm{div}}) \to T_p(S(A')_{\mathrm{div}})$ be the map induced by β_2. As $S(A)$ and $S(A')$ have the same $\mathbb{Z}_p$-corank and the kernel of β_2 is finite, it follows that β_2 is surjective, γ is injective, and $\mathrm{Coker}\,(\gamma) \xrightarrow{\sim} \mathrm{Ker}\,(\beta_2)$. The assertion of the lemma now follows on using (9) for both A and A'. □

Finally, let

$$\delta \; : \; \oplus_{v\in\Sigma} H^1(F_v, (A')^*(\bar{F}_v))(p) \to \oplus_{v\in\Sigma} H^1(F_v, A^*(\bar{F}_v))(p) \tag{10}$$

be the homomorphism induced by the isogeny ϕ^*. We write Σ_f for the set of non-archimedean places contained in Σ.

Lemma 2.6.

$$\chi(\delta) = \prod_{v \in \Sigma_f} \chi(\phi_v)^{-1}.$$

Proof. Since p is odd, the v-component of (10) is 0 when v is archimedean. If M is an abelian group, we write $M^\wedge = \varprojlim_n M/p^n M$ for its p-adic completion, and we use a similar notation for homomorphisms. If v is in Σ_f, Tate local duality shows that the v-component of (10) is dual to the homomorphism

$$\phi_v^\wedge : A(F_v)^\wedge \to A'(F_v)^\wedge.$$

But Ker (ϕ_v) and Coker (ϕ_v) are p-primary, and so $\chi(\phi_v^\wedge) = \chi(\phi_v)$, completing the proof of the lemma. □

We can now complete the proof of (6). Cassels' variant of the Poitou-Tate sequence asserts that we have an exact sequence

$$0 \to S((A')^*) \to H^1(G_\Sigma, (A')^*_{p^\infty}) \to \oplus_{v\in\Sigma} H^1(F_v, (A')^*(\bar{F}_v))(p) \to P(A')^\vee \to H^2(G_\Sigma, (A')^*_{p^\infty}) \to 0,$$

and similarly an exact sequence

$$0 \to S(A^*) \to H^1(G_\Sigma, A^*_{p^\infty}) \to \oplus_{v\in\Sigma} H^1(F_v, A^*(\bar{F}_v))(p) \to P(A)^\vee \to H^2(G_\Sigma, A^*_{p^\infty}) \to 0.$$

The two sequences are related by the maps discussed in Lemmas 2.4, 2.5, and 2.6, making a large commutative diagram whose vertical columns are given by ϕ_S^*, α_1, δ, $\beta_1^\vee$, and α_2, respectively. But the existence of this commutative diagram shows that

$$\chi(\phi_S^*)\chi(\alpha_1)^{-1}\chi(\delta)\chi(\beta_1)\chi(\alpha_2) = 1. \tag{11}$$

Using Lemmas 2.4, 2.5 and 2.6, we see that (6) is equivalent to (11), and the proof of (6) is now complete.

We now consider the isogeny ψ. Let $\phi' : A' \to A$ be the unique isogeny such that $\phi'\phi = p$ and $\phi\phi' = p$. By the general theory of the duality of abelian varieties, the kernel of $(\phi')^* : A^* \to (A')^*$ coincides with the annihilator of C in $A^*[p]$ with respect to the Weil pairing $A[p] \times A^*[p] \to \mu_p$. Since the annihilator of C is $\psi(C)$, the isogeny $\psi : A \to A^*$ induces an isogeny $\psi' : A' = A/C \to A^*/\psi(C) \xrightarrow{\sim} (A')^*$ which satisfies

$$\psi'\phi = (\phi')^*\psi. \tag{12}$$

By composing ϕ' from the right to (12), we obtain $p\psi' = (\phi')^*\psi\phi'$. Since $(\psi)^* = \psi$, this shows that $p(\psi')^* = p\psi'$, and hence

$$(\psi')^* = \psi'. \tag{13}$$

By composing ϕ^* from the left to (12), we obtain also

$$\phi^*\psi'\phi = p\psi. \tag{14}$$

By (14), the composition

$$S(A) \overset{\phi_S}{\to} S(A') \overset{\psi'_S}{\to} S((A')^*) \xrightarrow{\phi^*_S} S(A^*)$$

coincides with the map induced by $p\psi$. Since the degrees of ψ and ψ' are prime to p, $\psi_S : S(A) \to S(A^*)$ and $\psi'_S : S(A') \to S((A')^*)$ are isomorphisms, and hence we have

$$\chi(\phi_S) \cdot \chi(\phi^*_S) = \chi(S(A) \overset{p}{\to} S(A)) = p^{-s(A)}. \tag{15}$$

We consider the right hand side of (6). There is a perfect pairing

$$S(A)_{\mathrm{nd}} \times S(A^*)_{\mathrm{nd}} \to \mathbb{Q}_p/\mathbb{Z}_p$$

([32], Chap. 1, §6), and since $\psi^* = \psi$, the composition

$$S(A)_{\mathrm{nd}} \times S(A)_{\mathrm{nd}} \xrightarrow{1\times\psi_S} S(A)_{\mathrm{nd}} \times S(A^*)_{\mathrm{nd}} \to \mathbb{Q}_p/\mathbb{Z}_p$$

is non-degenerate and alternating [20], and there is a similar pairing for A'. Hence

$$\sharp(S(A)_{\mathrm{nd}}) \text{ and } \sharp(S(A')_{\mathrm{nd}}) \text{ are squares.} \tag{16}$$

Since the degrees of ψ and ψ' are prime to p, they induce isomorphisms

$$A(F)(p) \simeq A^*(F)(p), \quad A'(F)(p) \simeq (A')^*(F)(p). \tag{17}$$

By (15), (16), (17), we immediately deduce Theorem 2.3 from (6). □

We now turn to root numbers, and we recall that for any abelian variety A over a number field F, we have

$$w(A) = \prod_v w_v(A)$$

where v ranges over all finite and infinite places of F and $w_v(A) = +1$ or -1 is the local root number of A at v which is $+1$ for all but a finite number of v. In order to compare $w_v(A)$ and $(-1)^{h(v)}$, we let

$$\alpha_C : \mathrm{Gal}(\bar{F}/F) \to \mathrm{Aut}(C) \simeq GL_g(\mathbb{Z}/p\mathbb{Z})$$

be the homomorphism giving the action of $\mathrm{Gal}(\bar{F}/F)$ on C, and for each place v of F, let

$$\alpha_{C,v} : \mathrm{Gal}(\bar{F}_v/F_v) \to \mathrm{Aut}(C)$$

be the homomorphism induced by α_C. The determinant of $\alpha_{C,v}$ is a 1-dimensional character of $\mathrm{Gal}(\bar{F}_v/F_v)$, and hence by class field theory can be viewed as a homomorphism

$$\chi_{C,v} : F_v^\times \to (\mathbb{Z}/p\mathbb{Z})^\times.$$

By the reciprocity law of global class field theory, we have

$$\prod_v \chi_{C,v}(-1) = 1.$$

Hence it is clear that Theorem 2.1 follows immediately from Theorem 2.3 and the following local result.

Theorem 2.7. *Assume that A satisfies the hypotheses of Theorem 2.1. Then for any place v of F, we have*

$$(-1)^{h(v)} = w_v(A)\chi_{C,v}(-1).$$

In fact, Theorem 2.7 follows directly from the following explicit and separate computation of $w_v(A)$ and $(-1)^{h(v)}$. For each finite place v of F, let $t(v)$ be the dimension of the largest split torus in the special fiber of the Néron model of A at v. For example, when A is an elliptic curve, then $t(v) = 1$ if A has split multiplicative reduction at v, and $t(v) = 0$ otherwise. For abelian varieties in general, we have

$$t(v) = \dim_{\mathbb{Q}_\ell}\mathrm{Hom}_{\,\mathrm{Gal}(\bar{F}_v/F_v)}(T_\ell(A)\otimes\mathbb{Q}_\ell, \mathbb{Q}_\ell)$$

for any prime number ℓ, where $T_\ell(A)$ is the l-adic Tate module of A. Also $t(v) = 0$ if A has potential good reduction at v. For each place v of F lying over p, with residue field k_v, we will later define a homomorphism

$$\chi_{C,v,\mathrm{crys}} : O_{F_v}^\times \to k_v^\times$$

which is a crystalline version of the Galois theoretic homomorphism $\chi_{C,v}$.

Proposition 2.8. *Let A/F be an abelian variety of dimension g.*

(1) *Assume* (i) *in the hypotheses of Theorem 2.1. Let v be an archimedean place of F. Then*

$$w_v(A) = (-1)^g, \quad (-1)^{h(v)} = (-1)^g\chi_{C,v}(-1).$$

(2) *Assume* (i) *and* (ii) *in the hypotheses of Theorem 2.1. If v is a finite place of F which does not divide p, we have*

$$w_v(A) = (-1)^{t(v)}\chi_{C,v}(-1), \quad (-1)^{h(v)} = (-1)^{t(v)}.$$

(3) *Assume* (i), (ii), (iii) *in the hypotheses of Theorem 2.1. If v is a place of F which divides p, we have*

$$w_v(A) = (-1)^{t(v)}\chi_{C,v,\mathrm{crys}}(-1), \quad (-1)^{h(v)} = (-1)^{t(v)}\chi_{C,v}(-1)\chi_{C,v,\mathrm{crys}}(-1).$$

The most difficult part in the above proposition is to prove the formula for $(-1)^{h(v)}$ in (3), which compares the Galois object $\chi_{C,v}$ and the crystalline object $\chi_{C,v,\mathrm{crys}}$. A part of the proof of this formula is given in the Appendix, and uses the Dieudonné theory of finite flat commutative group schemes over discrete valuation rings of mixed characteristic as developed by Breuil [3].

The remainder of this section is organised as follows. In 2.9 and 2.10, we review the definition of the local root numbers $w_v(A)$ via the theory of local ϵ-factors of representations of Weil-Deligne groups. We then prove Proposition 2.8, remarking that for the proof of the formula for $(-1)^{h(v)}$ in Proposition 2.8 (3), we need Lemma 2.20 (6) which is established in the Appendix.

2.9. We assume from now on that K is either $\mathbb{C}$, $\mathbb{R}$, or a complete discrete valuation field with finite residue field k. Let W_K denote the Weil group of K (see [13]). By local class field theory, the local reciprocity map gives an isomorphism

$$W_K^{\mathrm{ab}} \simeq K^\times, \tag{18}$$

where W_K^{ab} is the quotient of W_K by the closure of the commutator subgroup of W_K. We follow the convention of Deligne [13] in normalising (18), so that under the isomorphism (18), prime elements of K map to the geometric Frobenius φ_k in $\mathrm{Gal}(\bar{k}/k)$. Suppose V is a finite dimensional representation of W_K over $\mathbb{C}$. Then the local ϵ-factor $\epsilon(W_K, V, \psi, dx)$, which is a non-zero element of $\mathbb{C}$, is defined for each non-trivial continuous group homomorphism $\psi : K \to \{z \in \mathbb{C}^\times \mid |z| = 1\}$ and for every choice of a Haar measure dx of the additive group K [13]. We have

$$\epsilon(W_K, V, a\psi, cdx) = \chi_V(a)(c \cdot ||a||^{-1})^{\dim(V)}\epsilon(W_K, V, \psi, dx) \tag{19}$$

for $a \in K^\times$ and $c > 0$, where we set $(a\psi)(x) = \psi(ax)$, $||\ ||$ is the normalized absolute value of K, and χ_V denotes the homomorphism $K^\times \simeq W_K^{\mathrm{ab}} \to \mathbb{C}^\times$, arising from the determinant map on V. Another basic property of these ϵ-factors is

$$\epsilon(W_K, V, \psi, dx) = \epsilon(W_K, V', \psi, dx)\,\epsilon(W_K, V'', \psi, dx) \tag{20}$$

whenever we have an exact sequence

$$0 \to V' \to V \to V'' \to 0$$

of representations of W_K.

Let W_K' denote the Weil-Deligne group. We now recall some of the basic properties of finite dimensional representations of W_K' over $\mathbb{C}$. When K is archimedean, such a representation is simply a representation of W_K over $\mathbb{C}$ and the ϵ-factors are the same. When K is non-archimedean, a representation of W_K' over $\mathbb{C}$ is a pair (V, N) where V is a representation of W_K over $\mathbb{C}$ and $N : V \to V(-1)$ is a homomorphism of W_K representations. Here for a representation V of W_K, we set $V(n) = V \otimes \omega^n$ with the character

$$\omega : W_K \to W_K^{\mathrm{ab}} \simeq K^\times \xrightarrow{\|\ \|} \mathbb{R}^\times.$$

For such a representation (V, N), we define

$$\epsilon(W_K', V, \psi, dx) = \epsilon(W_K, V, \psi, dx)\det(-\varphi_k^{-1} : (V/\mathrm{Ker}\,(N))^{I_K}), \tag{21}$$

where φ_k is any geometric Frobenius in $\mathrm{Gal}(\bar{K}/K)$.

We recall that the pair (ψ, dx) is *self-dual* if, for the Fourier transform $\mathcal{F}_{\psi,dx}$ defined by

$$(\mathcal{F}_{\psi,dx})(f)(x) = \int_K f(y)\psi(xy)dy,$$

we have $(\mathcal{F}^2_{\psi,dx}(f))(x) = f(-x)$ where f is any $\mathbb{C}$-valued function on K which belongs to the Schwartz class. The following pairs (ψ, dx) are self-dual: (a) $K = \mathbb{R}$, $\psi(x) = \exp(2\pi i x)$, dx is the Lebesgue measure; (b) $K = \mathbb{C}$, $\psi(z) = \exp(2\pi i \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(z))$, $dx = dz \wedge d\bar{z}$ and (c) K is non-archimedean, the largest O_K-submodule of K contained in the kernel of ψ is O_K, and the volume of O_K with respect to dx is 1. Moreover, any self-dual pair is obtained as $(a\psi, ||a||^{-1/2}dx)$ from (ψ, dx) as in (a), (b), (c) for some $a \in K^\times$. If (ψ, dx) is self-dual, then for any representation V of W'_K over $\mathbb{C}$, we have

$$\epsilon(W'_K, V, \psi, dx)\epsilon(W'_K, V^*(1), \psi, dx) = \chi_V(-1), \tag{22}$$

where V^* is the dual of V viewed as a representation of W_K, and $N : V^*(1) \to V^*$ is defined to be $-\,{}^tN$ with ${}^tN$ the transpose of the given $N : V \to V(-1)$.

Suppose now that V is a representation of W'_K over $\mathbb{C}$ satisfying

$$V \simeq V^*(1), \tag{23}$$

$$\dim(V) \text{ is even, and } \det(V) \simeq \mathbb{C}(\dim(V)/2), \tag{24}$$

where $\det(V)$ denotes the determinant of V. It follows from (22), (23) and (24) that for (ψ, dx) self-dual, we have

$$\epsilon(W'_K, V, \psi, dx) = \pm 1. \tag{25}$$

Moreover by (19) and (24), $\epsilon(W'_K, V, \psi, dx)$ is independent of the choice of the self-dual pair (ψ, dx).

2.10. Let A be an abelian variety over our local field K. We now recall the definition of the fundamental representation $\mathcal{V}(A)$ of W'_K over $\mathbb{C}$ attached to A. This representation $\mathcal{V}(A)$ of W'_K always satisfies (23) and (24), and the local root number $w_K(A)$ is then defined by

$$w_K(A) = \epsilon(W'_K, \mathcal{V}(A), \psi, dx) \text{ with } (\psi, dx) \text{ self-dual.} \tag{26}$$

Suppose first that $K = \mathbb{C}$ or $\mathbb{R}$. Then $\mathcal{V}(A) = H_1(A(\mathbb{C}), \mathbb{C})$ on which W_K acts in the following manner. Recall that $W_\mathbb{C} = \mathbb{C}^\times$, $W_\mathbb{R}$ contains $W_\mathbb{C}$ as a subgroup of index 2, and $W_\mathbb{R}$ is generated by $W_\mathbb{C}$ and an element ι satisfying $\iota^2 = -1 \in \mathbb{C}^\times = W_\mathbb{C}$ and $\iota z \iota^{-1} = \bar{z}$ for $z \in \mathbb{C}^\times = W_\mathbb{C}$. We have a surjective homomorphism

$$H_1(A(\mathbb{C}), \mathbb{C}) \to \mathrm{Hom}_\mathbb{C}(H^0(A, \Omega^1_{A/\mathbb{C}}), \mathbb{C}) \; ; \; \gamma \mapsto (\omega \mapsto \int_\gamma \omega),$$

where $H^0(A, \Omega^1_{A/\mathbb{C}})$ is the vector space of holomorphic differentials on A. Let $\mathcal{V}^{-1,0}(A)$ be the kernel of this homomorphism. Then $\mathcal{V}(A)$ is the direct sum of $\mathcal{V}^{-1,0}(A)$ and the complex conjugate $\mathcal{V}^{0,-1}(A)$ of $\mathcal{V}^{-1,0}(A)$ with respect to the $\mathbb{R}$-structure $H_1(A(\mathbb{C}), \mathbb{R})$ of $H_1(A(\mathbb{C}), \mathbb{C})$. Consider the action of $\mathbb{C}^\times$ on $\mathcal{V}(A)$ where $z \in \mathbb{C}^\times$ acts by z^{-1} on $\mathcal{V}^{-1,0}(A)$

and by $\bar{z}^{-1}$ on $\mathcal{V}^{0,-1}(A)$. When $K = \mathbb{C}$, this is the action of W_K on $\mathcal{V}_{\mathbb{C}}(A)$. When $K = \mathbb{R}$, we extend this to the action of $W_{\mathbb{R}}$ for which ι acts as i^{-1} times the $\mathbb{C}$-linear map on $\mathcal{V}(A)$ induced by the complex conjugation $A(\mathbb{C}) \to A(\mathbb{C})$.

Now assume K is a complete discrete valuation field. The representation $\mathcal{V}(A)$ of W'_K associated to A is obtained from the representation $V_p(A) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(A)$ of $\mathrm{Gal}(\bar{K}/K)$, where p is any prime number which is different from $\mathrm{char}(k)$ and $T_p(A)$ is the p-adic Tate module of A, as in §8 of [13]. We introduce here a description of $\mathcal{V}(A)$ by using the theory of Raynaud [36] (see also [42, Chap. IX]), which we use for the proof of Proposition 2.8. We write O_K for the ring of integers of K, $\mathfrak{m}_K$ for its maximal ideal, k_K for its residue class field, and use similar notation for all finite extensions of K. Take a finite Galois extension L of K such that $A_L = A \otimes_K L$ has split semistable reduction. Let A_{O_L} be the Néron model of A_L over O_L. The work of Raynaud shows that there is a smooth commutative group scheme $\mathfrak{A}$ over O_L, which is characterized up to unique isomorphism, by the following two properties:- (i) There is an exact sequence

$$0 \to T \to \mathfrak{A} \to B \to 0 \tag{27}$$

with T a split torus over O_L and B an abelian scheme over O_L.

(ii) For $i \geq 1$, $\mathfrak{A} \otimes_{O_L} (O_L/\mathfrak{m}_L^i)$ is the connected component of $A_{O_L} \otimes_{O_L} (O_L/\mathfrak{m}_L^i)$ containing the origin.

We then have a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & T(O_L) \arrow[r] \arrow[d] & \mathfrak{A}(O_L) \arrow[r] \arrow[d] & B(O_L) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & T(L) \arrow[r] & \mathfrak{A}(L) \arrow[r] & B(L) \arrow[r] & 0.
\end{tikzcd}$$

Here $B(O_L) = B(L)$ since B is proper over O_L. Hence we have

$$\mathfrak{A}(L)/\mathfrak{A}(O_L) \simeq T(L)/T(O_L) = \mathrm{Hom}\,(X(T), L^\times)/\mathrm{Hom}\,(X(T), O_L^\times) \simeq \mathrm{Hom}\,(X(T), \mathbb{Z}),$$

where $X(T)$ denotes the character group of the split torus T.

The dual abelian variety A^* of A also has split semistable reduction over L, and we have the corresponding objects $\mathfrak{A}^*, T^*, B^*$ attached to A^*. In fact, B^* coincides with the dual abelian scheme of B. Raynaud constructed a canonical injective homomorphism

$$X(T^*) \to \mathfrak{A}(L) \tag{28}$$

such that if

$$N : X(T^*) \to \mathrm{Hom}\,(X(T), \mathbb{Z}) \tag{29}$$

denotes the composition of (28) and $\mathfrak{A}(L) \to \mathfrak{A}(L)/\mathfrak{A}(O_L) \simeq \mathrm{Hom}\,(X(T), \mathbb{Z})$, then N is injective and has finite cokernel (we shall see later that this N is very closely related to the one occurring in the definition of $\mathcal{V}(A)$). He also constructed a canonical isomorphism

$$A(\bar{K}) \simeq \mathfrak{A}(\bar{K})/X(T^*) \tag{30}$$

which is compatible with the action of $\mathrm{Gal}(\bar{K}/K)$, and which induces an isomorphism

$$A(L) \simeq \mathfrak{A}(L)/X(T^*). \tag{31}$$

For example, if A is an elliptic curve with split multiplicative reduction over L, then $\mathfrak{A} = T = \mathbb{G}_m$, $B = 0$, $X(T^*) \simeq \mathbb{Z}$, and the presentation (31) of $A(L)$ is none other than the Tate parametrization.

Naïvely, it is only $\mathrm{Gal}(\bar{K}/L)$ which acts on $\mathfrak{A}(\bar{K})$ since $\mathfrak{A}$ is a scheme over O_L. But in fact, $\mathrm{Gal}(\bar{K}/K)$ acts on it for the following reason. By the uniqueness of $\mathfrak{A}$ (up to unique isomorphism), we have an action of $\mathrm{Gal}(L/K)$ on the scheme $\mathfrak{A}$ which is compatible with the action of $\mathrm{Gal}(L/K)$ on $\mathrm{Spec}(O_L)$ via the canonical morphism $\mathfrak{A} \to \mathrm{Spec}(O_L)$, and which is compatible with the group structure of $\mathfrak{A}$. Here for $\sigma \in \Delta$, the action $\sigma : \mathrm{Spec}(O_L) \to \mathrm{Spec}(O_L)$ is the morphism corresponding to $\sigma^{-1} : O_L \to O_L$. For $\sigma \in \mathrm{Gal}(\bar{K}/K)$, the action of σ on $\mathfrak{A}(\bar{K})$ is defined to be $x \mapsto \sigma \circ x \circ \sigma^{-1}$ for $x \in \mathfrak{A}(\bar{K})$ which we regard as a morphism $\mathrm{Spec}(\bar{K}) \to \mathfrak{A}$. (The last σ^{-1} acts $\mathrm{Spec}(\bar{K})$ as the morphism corresponding to $\sigma : \bar{K} \to \bar{K}$.) Similarly, $\mathrm{Gal}(\bar{K}/K)$ acts on $T(\bar{K})$ and on $B(\bar{K})$.

Let $\mathfrak{A}_L = \mathfrak{A} \otimes_{O_L} L$, $T_L = T \otimes_{O_L} L$, $B_L = B \otimes_{O_L} L$. Let p be a prime number which is different from the characteristic of K. By (27), (30), we obtain exact sequences of $\mathrm{Gal}(\bar{K}/K)$-modules

$$0 \to T_p(\mathfrak{A}_L) \to T_p(A) \to X(T^*) \otimes \mathbb{Z}_p \to 0,$$

$$0 \to T_p(T_L) \to T_p(\mathfrak{A}_L) \to T_p(B_L) \to 0.$$

Define the $\mathrm{Gal}(\bar{K}/K)$-stable increasing filtration $\mathrm{Fil}_i(T_p(A))$ on $T_p(A)$ by

$$\mathrm{Fil}_{-3} = 0 \subset \mathrm{Fil}_{-2}T_p(A) = T_p(T_L) \subset \mathrm{Fil}_{-1}T_p(A) = T_p(\mathfrak{A}_L) \subset \mathrm{Fil}_0T_p(A) = T_p(A).$$

Then for $i = 0, -1, -2$, $\mathrm{gr}_iT_p(A) = \mathrm{Fil}_iT_p(A)/\mathrm{Fil}_{i-1}T_p(A)$ is described as

$$\mathrm{gr}_0T_p(A) = X(T^*) \otimes \mathbb{Z}_p, \quad \mathrm{gr}_{-1}T_p(A) = T_p(B_L), \quad \mathrm{gr}_{-2}T_p(A) = \mathrm{Hom}\,(X(T), \mathbb{Z}_p(1)).$$

For a group Γ, a semisimple representation V of Γ over a field M of characteristic 0, and a semisimple representation V' of Γ over a field M' of characteristic 0, we say V and V' are isomorphic as representations of Γ if $\mathrm{Trace}(\sigma; V) = \mathrm{Trace}(\sigma; V') \in \mathbb{Q}$ for any $\sigma \in \Gamma$. This condition is equivalent to the following condition: For any field M'' and any homomorphisms $M \to M''$ and $M' \to M''$ of fields, $M'' \otimes_M V$ and $M'' \otimes_{M'} V'$ are isomorphic as representations of Γ over M''. It is known that in the case $p \neq \mathrm{char}(k_K)$, $V_p(B_L)$ is semisimple as a representation of W_K over $\mathbb{Q}_p$, and the isomorphism class of this representation is independent of $p \neq \mathrm{char}(k_K)$ in the above sense.

The representation $\mathcal{V}(A)$ of W'_K over $\mathbb{C}$ is described as follows. As a representation of W_K,

$$\mathcal{V}(A) = \mathrm{gr}_0\mathcal{V}(A) \oplus \mathrm{gr}_{-1}\mathcal{V}(A) \oplus \mathrm{gr}_{-2}\mathcal{V}(A),$$

where

$$\mathrm{gr}_0\mathcal{V}(A) := X(T^*) \otimes \mathbb{C}, \quad \mathrm{gr}_{-2}\mathcal{V}(A) := \mathrm{Hom}\,(X(T), \mathbb{C})(1),$$

and $\mathrm{gr}_{-1}\mathcal{V}(A)$ is any representation of W_K over $\mathbb{C}$ which is isomorphic to the representation $V_p(B_L)$ of W_K over $\mathbb{Q}_p$ with $p \neq \mathrm{char}(k_K)$ (so $\mathcal{V}(A)$ is determined only up to isomorphism). We define the map $N : \mathcal{V}(A) \to \mathcal{V}(A)(-1)$ to be the composite

$$\mathcal{V}(A) \to \mathrm{gr}_0\mathcal{V}(A) \xrightarrow{N} \mathrm{gr}_{-2}\mathcal{V}(A)(-1) \to \mathcal{V}(A)(-1)$$

where the first arrow is the projection, the third arrow is the inclusion map, and the middle map is induced from (29). In view of this definition, for any $p \neq \mathrm{char}(k_K)$ and for $i = 0, -1, -2$, the representation $\mathrm{gr}_i\mathcal{V}(A)$ of W_K over $\mathbb{C}$ is isomorphic to the representation $\mathrm{gr}_i(T_p(A) \otimes \mathbb{Q}_p)$ of W_K over $\mathbb{Q}_p$. It is known that $\mathcal{V}(A)$ is semi-simple as a representation of W_K.

The following lemma is well known (see [42]).

Lemma 2.11. *The abelian variety A over K has semistable reduction if and only if the inertia subgroup of W_K acts trivially on $\mathcal{V}(A)$. It has split semistable reduction if and only if it has semistable reduction and the action of W_K on $\mathrm{gr}_0\mathcal{V}(A)$ and $(\mathrm{gr}_{-2}\mathcal{V}(A))(-1)$ is trivial.*

Taking now $p = \mathrm{char}(k_K)$, the representation $\mathcal{V}(A)$ can be explained in terms of Dieudonné theory as follows. Let $\mathfrak{A}_{p^\infty}$ (resp. T_{p^∞}, resp. B_{p^∞}) be the p-divisible group over O_L associated to $\mathfrak{A}$ (resp. T, resp. B), which is the inductive limit of the commutative finite flat group scheme $\mathfrak{A}[p^n]$ (resp. $T[p^n]$, resp. $B[p^n]$) over O_L. Let k_L be the residue field of L, and let $D = D(\mathfrak{A}_{p^\infty} \otimes_{O_L} k_L)$ (resp. $D(T_{p^\infty} \otimes_{O_L} k_L)$, resp. $D(B_{p^\infty} \otimes_{O_L} k_L)$) be the covariant Dieudonné module of the special fibre of this p-divisible group. Then D is a free module of finite rank over the ring $W(k_L)$ of Witt vectors, and D is endowed with a semi-linear action of $\mathrm{Gal}(L/K)$ and with a frobenius operator $\varphi_p : D \to D$. The operator φ_p is an injection with finite cokernel, $\varphi_p(ax) = \varphi_p(a)\varphi_p(x)$ for $a \in W(k_L)$ and $x \in D$, where $\varphi_p : W(k_L) \to W(k_L)$ is the ring homomorphism induced by the endomorphism of k_L given by $x \mapsto x^p$, and φ_p commutes with the action of $\mathrm{Gal}(L/K)$. Let $\mathrm{Frac}(W(k_L))$ be the field of fractions of $W(k_L)$, and define the linear action of W_K on $D \otimes_{W(k_L)} \mathrm{Frac}(W(k_L))$ over $\mathrm{Frac}(W(k_L))$ as follows. Let $\sigma \in W_K$ and let φ_k^n ($n \in \mathbb{Z}$) be the image of σ in $\mathrm{Gal}(\bar{k}/k)$. Define the linear action of σ on D as $\varphi_p^{nf}\bar{\sigma}$ where $f = [k_K : \mathbb{F}_p]$ and $\bar{\sigma}$ is the image of σ in $\mathrm{Gal}(L/K)$. The following result is well-known for $p = \mathrm{char}(k_K)$.

Lemma 2.12. *For $p = \mathrm{char}(k_K)$ we have:*

(1) *The representation $\mathrm{gr}_{-1}\mathcal{V}(A) \oplus \mathrm{gr}_{-2}\mathcal{V}(A)$ of W_K over $\mathbb{C}$ is isomorphic to the representation $D(\mathfrak{A}_{p^\infty} \otimes k_L) \otimes_{W(k_L)} \mathrm{Frac}(W(k_L))$ of W_K over $\mathrm{Frac}(W(k_L))$ defined above.*

(2) *The representation $\mathrm{gr}_{-1}\mathcal{V}(A)$ of W_K over $\mathbb{C}$ is isomorphic to the representation $D(B_{p^\infty} \otimes_{O_L} k_L) \otimes_{W(k_L)} \mathrm{Frac}(W(k_L))$ of W_K over $\mathrm{Frac}(W(k_L))$.*

(3) *The representation $\mathrm{gr}_{-2}\mathcal{V}(A)$ of W_K over $\mathbb{C}$ is isomorphic to the representation $D(T_{p^\infty} \otimes_{O_L} k_L) \otimes_{W(k_L)} \mathrm{Frac}(W(k_L))$ of W_K over $\mathrm{Frac}(W(k_L))$.*

Finally, assuming always that K is non-archimedean, since

$$(-1)^{t(K,A)} = \det(-\varphi_k^{-1}\ ;\ (\mathcal{V}(A)/\mathrm{Ker}\,(N))^{I_K}),$$

we have

$$w_K(A) = \epsilon(W_K, \mathcal{V}(A), \psi, dx) \cdot (-1)^{t(K,A)} \tag{32}$$

with (ψ, dx) self-dual, and where $t(K, A)$ denotes the multiplicity of the trivial representation in the representation $\mathrm{gr}_0\mathcal{V}(A)$ of W_K. By [42, Chap. IX], $t(K, A)$ coincides with the dimension of the split torus part of the reduction of the Néron model of A over O_K.

2.13. Let the assumptions be as in Theorem 2.1. We now make some remarks on $C = \mathrm{Ker}\,(A \to A')$ and discuss commutative finite flat group schemes over p-adic discrete valuation rings related to C. Let

$$C' = A[p]/C = \mathrm{Ker}\,(\phi' : A' \to A).$$

Since ψ induces an isomorphism $C \xrightarrow{\sim} \mathrm{Ker}\,((\phi')^* : A^* \to (A')^*)$, Cartier duality between $\mathrm{Ker}\,(\phi' : A' \to A)$ and $\mathrm{Ker}\,((\phi')^* : A^* \to (A')^*)$ induces a Cartier duality

$$C \simeq \mathcal{H}om\,(C', \mu_p) \tag{33}$$

of finite commutative group schemes over F. Here we have identified a finite commutative group scheme P over F with the corresponding representation $P(\bar{F})$ of $\mathrm{Gal}(\bar{F}/F)$.

We can apply the results of 2.10 with $K = F_v$, for a finite place v of F. Regarding C as a subgroup of $T_p(A)/pT_p(A) \simeq A[p]$, define $\mathrm{Gal}(\bar{F}_v/F_v)$-submodules C_{f,F_v} and C_{t,F_v} of C as

$$C_{t,F_v} = C \cap (T_p(T_L)/pT_p(T_L)) \subset C_{f,F_v} = C \cap (T_p(\mathfrak{A}_L)/pT_p(\mathfrak{A}_L)) \subset T_p(A)/pT_p(A).$$

By regarding C' as a subgroup of $T_p(A')/pT_p(A')$, define $C'_{t,F_v} \subset C'_{f,F_v} \subset C'$ similarly. Since A' and $(A')^*$ also have split semistable reduction over L, we can define analogous schemes to T, $\mathfrak{A}$, and B for both A' and $(A')^*$, and we denote these schemes in the evident analogous fashion. We then have

$$C/C_{f,F_v} \simeq \mathrm{Ker}\,(X(T^*)/pX(T^*) \to X((T')^*)/pX((T')^*)) \simeq X((T')^*)/X(T^*) \tag{34}$$

where the arrow and the embedding $X(T^*) \to X((T')^*)$ on the right are induced from $\phi : T \to T'$,

$$C'/C'_{f,F_v} \simeq \mathrm{Ker}\,(X((T')^*)/pX((T')^*) \to X(T^*)/pX(T^*)) \simeq X(T^*)/X((T')^*) \tag{35}$$

where the arrow and the embedding $X((T')^*) \to X(T^*)$ on the right are induced from $\phi' : T' \to T$. In the isomorphism (33), C_{f,F_v} and C'_{t,F_v} annihilate each other, C_{t,F_v}

and C'_{f,F_v} kill each other, and (33) induces Cartier dualities of finite commutative group schemes over F_v:-

$$C_{f,F_v}/C_{t,F_v} \simeq \mathcal{H}om\,(C'_{f,F_v}/C'_{t,F_v}, \mu_p). \tag{36}$$

$$C_{t,F_v} \simeq \mathcal{H}om\,(C'/C'_{f,F_v}, \mu_p) \tag{37}$$

$$C/C_{f,F_v} \simeq \mathcal{H}om\,(C'_{t,F_v}, \mu_p) \tag{38}$$

Now assume v divides p, and let the finite extension L/F_v be as in 2.10 (we take F_v as K in 2.10). Define finite flat commutative group schemes C_{f,O_L} and C_{t,O_L} over O_L by

$$C_{t,O_L} = \mathrm{Ker}\,(T \to T') \subset C_{f,O_L} = \mathrm{Ker}\,(\mathfrak{A} \to \mathfrak{A}').$$

We then have isomorphisms

$$C_{f,O_L}/C_{t,O_L} \simeq \mathrm{Ker}\,(B \to B'),\ C_{f,O_L} \otimes_{O_L} L = C_{f,F_v} \otimes_{F_v} L,\ C_{t,O_L} \otimes_{O_L} L = C_{t,F_v} \otimes_{F_v} L.$$

Similarly, define $C'_{t,O_L} = \mathrm{Ker}\,(T' \to T) \subset C'_{f,O_L} = \mathrm{Ker}\,(\mathfrak{A}' \to \mathfrak{A})$, where $\mathfrak{A}' \to \mathfrak{A}$ and $T' \to T$ are the homomorphisms induced by ϕ'. Since ψ induces an isomorphism $C_{f,O_L}/C_{t,O_L} \xrightarrow{\sim} \mathrm{Ker}\,((\phi')^* : B^* \to (B')^*)$, Cartier duality between $\mathrm{Ker}\,(\psi : B' \to B)$ and $\mathrm{Ker}\,((\phi')^* : B^* \to (B')^*)$ induces the following Cartier duality of finite flat commutative group schemes over O_L:-

$$C_{f,O_L}/C_{t,O_L} \simeq \mathcal{H}om\,(C'_{f,O_L}/C'_{t,O_L}, \mu_p). \tag{39}$$

We have also the following Cartier duality (40) and (41) of commutative finite flat group schemes over O_L. Denote by $(C/C_{f,F_v})_{O_L}$ the group $C/C_{f,F_v}$ regarded as a constant commutative group scheme over O_L, and define $(C'/C'_{f,F_v})_{O_L}$ similarly. Then, ψ' induces $X((T')^*)/X(T^*) \simeq X(T')/X(T)$ where $X(T) \to X(T')$ is induced by ϕ', and ψ induces $X(T^*)/X((T')^*) \simeq X(T)/X(T')$ where $X(T') \to X(T)$ is induced by ϕ. By (34) and (35), these induce

$$C_{t,O_L} \simeq \mathcal{H}om\,((C'/C'_{f,F_v})_{O_L}, \mu_p), \tag{40}$$

$$(C/C_{f,F_v})_{O_L} \simeq \mathcal{H}om\,(C'_{t,O_L}, \mu_p). \tag{41}$$

Lemma 2.14. *Let the assumptions be as in Theorem 2.1 and let v be a finite place of F. Then:-*

(1) *There is a finite Galois extension L/F_v such that the ramification index of L/F_v is prime to p and A has split semistable reduction over L.*

(2) *The image of $W_{F_v} \to \mathrm{Aut}(\mathrm{gr}_0\mathcal{V}(A))$ and the image of $W_{F_v} \to \mathrm{Aut}((\mathrm{gr}_{-2}\mathcal{V}(A))(-1))$ are finite groups whose orders are prime to p.*

(3) *The image of the inertial subgroup I_{F_v} of W_{F_v} in* $\mathrm{Aut}(\mathcal{V}(A))$ *is a finite group whose order is prime to p.*

(4) *Assume v does not divide p. Then there is a free $\mathbb{Z}_p$-module U of rank g endowed with a continuous action of W_{F_v} having the following properties: The inertial subgroup I_{F_v} of W_{F_v} acts on U through a finite quotient of order prime to p, the semi-simplifications of the representations $U \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ and C of W_{F_v} over $\mathbb{F}_p$ are isomorphic, and the semi-simplifications of the representations $(U \oplus U^*(1)) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ and $A[p]$ over $\mathbb{F}_p$ are isomorphic.*

(5) *Assume v divides p. Then there is a representation U of W_{F_v} over $\mathbb{C}$ of dimension g such that as representations of W_{F_v}, $\mathcal{V}(A)$ is isomorphic to $U \oplus U^*(1)$.*

(6) *Assume v divides p, let L/F_v be as in paragraph 2.10. Then for $\sigma \in I_{F_v}$, the characteristic polynomial giving the action of σ on the k_L-vector space $D(C_{f,O_L} \otimes_{O_L} k_L)$ has coefficients in the residue field k_v of F_v; here $D(C_{f,O_L} \otimes_{O_L} k_L)$ is the covariant Dieudonné module of the commutative finite flat group scheme $C_{f,O_L} \otimes_{O_L} k_L$ over k_L (2.13).*

Proof. By Lemma 2.11, (1) follows from (2) and (3). Since the representation of W_{F_v} on $\mathrm{gr}_0\mathcal{V}(A)$ and on $(\mathrm{gr}_{-2}\mathcal{V}(A))(-1)$ are $\mathbb{Q}$-rational and of dimension $\leq g$, (2) follows from the fact that $GL_g(\mathbb{Q})$ has no element of order p if $p \geq g+2$ (the last fact is deduced from $[\mathbb{Q}(\mu_p) : \mathbb{Q}] = p-1 > g$).

We prove (3). By (2), it is sufficient to consider $\mathrm{gr}_{-1}\mathcal{V}(A)$. If v does not divide p (resp. if v divides p), the representation of I_{F_v} on $\mathrm{gr}_{-1}\mathcal{V}(A)$ is realized over $\mathbb{Q}_p$ (resp. $\mathrm{Frac}(W(k_L))$) and is of dimension $\leq 2g$. Then (3) follows from the fact that $GL_{2g}(\mathbb{Q}_p)$ (resp. $GL_{2g}(\mathrm{Frac}(W(k_L)))$ has no element of order p if $p \geq 2g+2$ (the last fact is deduced from $[\mathbb{Q}_p(\mu_p) : \mathbb{Q}_p]$ (resp. $[\mathrm{Frac}(W(k_L))(\mu_p) : \mathrm{Frac}(W(k_L))]) = p-1 > 2g$).

We prove (4). Let $I' = \mathrm{Ker}\,(I_{F_v} \to \mathrm{Aut}(\mathcal{V}(A)))$ and let $H = I_{F_v}/I'$. Then W_{F_v}/I' acts on the semi-simplification C_{ss} of C. Since the order of H is prime to p by (3), C_{ss} can be regarded as a projective $\mathbb{F}_p[H]$-module. Take any finitely generated projective $\mathbb{Z}_p[H]$-module U such that $U \otimes_{\mathbb{Z}_p} \mathbb{F}_p = C_{\mathrm{ss}}$. We show that the action of H on U extends to an action of W_{F_v}/I' on U. Fix an element σ of W_{F_v} whose image in $\mathrm{Gal}(\bar{k}_v/k_v)$ is φ_{k_v}. For a $\mathbb{Z}_p[H]$-module M, let $M_{(\sigma)}$ be the $\mathbb{Z}_p[H]$-module whose underlying $\mathbb{Z}_p$-module is M but $a \in H$ acts on $M_{(\sigma)}$ by the original action of $\sigma a \sigma^{-1}$ on M. The action $\sigma : C_{\mathrm{ss}} \to C_{\mathrm{ss}}$ is regarded as an isomorphism of $\mathbb{Z}_p[H]$-modules $C_{\mathrm{ss}} \xrightarrow{\sim} (C_{\mathrm{ss}})_{(\sigma)}$. Hence $U \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ and $U_{(\sigma)} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ are isomorphic as $\mathbb{F}_p[H]$-modules. From this we conclude that U and $U_{(\sigma)}$ are isomorphic as $\mathbb{Z}_p[H]$-modules by Nakayama's lemma. We therefore fix a $\mathbb{Z}_p$-endomorphism of U, which gives rise to an isomorphism $U \to U_{(\sigma)}$ of $\mathbb{Z}_p[H]$-modules. For simplicity, we again denote this endomorphism of U by σ. Then this action of σ on U along with the original action of H on U, defines an action of W_{F_v} on U. As a representation of W_{F_v}, we have

$$(U \oplus U^*(1)) \otimes_{\mathbb{Z}_p} \mathbb{F}_p \simeq C_{\mathrm{ss}} \oplus C^*_{\mathrm{ss}}(1) \simeq C_{\mathrm{ss}} \oplus C'_{\mathrm{ss}} \simeq A[p]_{\mathrm{ss}}$$

where the second isomorphism is by 2.13.

We prove (5) and (6). Assume first that A is potentially ordinary at v. Since B is ordinary, $T_p(B_L)$ has a $\mathrm{Gal}(\bar{F}_v/F_v)$-stable $\mathbb{Z}_p$-submodule S of rank g such that $T_p(B_L)/S$ is torsion free and such that the actions of $\mathrm{Gal}(\bar{F}_v/L)$ on $T_p(B_L)/S$ and on $S^*(1)$ are unramified. The perfect duality $T_p(B_L) \times T_p(B_L^*) \to \mathbb{Z}_p(1)$ annihilates $S \times \psi(S)$, and hence induces an isomorphism $T_p(B_L)/S \simeq S^*(1)$ of representations of $\mathrm{Gal}(\bar{F}_v/F_v)$. Let $U_1 = T_p(B_L)/S \otimes_{\mathbb{Z}_p} \mathrm{Frac}(W(k_L))$. We have an exact sequence of representation of W_{F_v} over $\mathrm{Frac}(W(k_L))$

$$0 \to U_1^*(1) \to D(B_{p^\infty} \otimes_{O_L} k_L) \otimes_{W(k_L)} \mathrm{Frac}(W(k_L)) \to U_1 \to 0,$$

where, as always, $U_1^*(1)$ is the Tate twist of U_1^* as a representation of W_{F_v}. Let $U = U_1 \oplus X(T^*) \otimes \mathrm{Frac}(W(k_L))$. Then the representation $\mathcal{V}(A)$ of W_{F_v} is isomorphic to the representation $U \oplus U^*(1)$ over $\mathrm{Frac}(W(k_L))$. This proves (5) in this case. Since B is ordinary, we have an exact sequence of finite commutative group schemes

$$0 \to P \to C_{f,O_L}/C_{t,O_L} \otimes_{\mathbb{F}_p} k_L \to Q \to 0$$

over k_L endowed with actions of I_v, where P is multiplicative and Q is étale. Let P' be the Cartier dual of P which is an étale finite group scheme over k_L. We can view P' and Q as $\mathbb{F}_p$-vector spaces endowed with actions of $\mathrm{Gal}(\bar{k}_v/k_v)$. We have an exact sequence

$$0 \to \mathrm{Hom}_{\,\mathbb{F}_p}(P', k_L) \to D(C_{f,O_L}/C_{t,O_L} \otimes_{O_L} k_L) \to (Q \otimes_{\mathbb{F}_p} k_L) \to 0$$

of representations of I_v over k_L. Let Z be the dual representation of the representation $\mathrm{Hom}\,(C_{t,F_v}, \mu_p)$ of I_{F_v} over $\mathbb{F}_p$. Consider the representation Y of I_{F_v} over $\mathbb{F}_p$ defined as $Y = \mathrm{Hom}\,(P', \mathbb{F}_p) \oplus Q \oplus Z$. Then $Y \otimes_{\mathbb{F}_p} k_L \simeq D(C_{f,O_L} \otimes_{O_L} k_L)$ as representations of I_{F_v} over k_L. Hence the characteristic polynomial of the action of an element σ on the k_L-vector space $D(C_{f,O_L} \otimes_{O_L} k_L)$ coincides with the characteristic polynomial of the action of σ on the $\mathbb{F}_p$-vector space Y, and hence is a polynomial over $\mathbb{F}_p$. This proves (6) in this case.

Next assume that A achieves semistable reduction over a finite abelian extension L of F_v. We show first that the action of W_{F_v} on $\mathcal{V}(A)$ factors through the abelian quotient $F_v^\times$ of W_{F_v}. By Lemma 2.11, the action of I_{F_v} in the representation of W_{F_v} factors through the canonical map $I_{F_v} \to \mathrm{Gal}(L/F_v)$. Since L/F_v is abelian, the last map factors through the canonical surjection $I_{F_v} \to O_{F_v}^\times$ in local class field theory. But the quotient of W_{F_v} by the kernel of $I_{F_v} \to O_{F_v}^\times$ is $W_{F_v}^{\mathrm{ab}} \simeq F_v^\times$. Write the action of W_{F_v} on $\mathcal{V}(A)$ as the direct sum of characters of $F_v^\times$. By $\mathcal{V}(A) \simeq \mathcal{V}(A)^*(1)$ and by the fact $\dim(\mathcal{V}(A))$ is even, we can choose χ_i $(1 \leq i \leq g)$ among these characters such that $\mathcal{V}(A)$ is the direct sum $(\oplus_{i=1}^g \chi_i) \oplus (\oplus_{i=1}^g \chi_i^{-1}(1))$. This proves (5) in this case. By (3), the action of $O_{F_v}^\times$ on $\mathcal{V}(A)$ is trivial on the pro-p part of $O_{F_v}^\times$ and hence the action factors through the canonical projection $O_{F_v}^\times \to k_v^\times$. Thus for any $\sigma \in I_{F_v}$, $\sigma^{N(v)-1}$ acts on $\mathcal{V}(A)$ trivially, and therefore acts trivially on $D(\mathfrak{A}_{p^\infty}) \otimes_{O_L} k_L$, and also trivially on $D(C_{f,O_L} \otimes_{O_L} k_L)$. Thus the characteristic polynomial giving the action of $\sigma \in I_{F_v}$ on $D(C_{f,O_L} \otimes_{O_L} k_L)$ has coefficients over k_v. This proves (6) in this case.

□

2.15. Let the assumptions be as in Theorem 2.1 and suppose that v divides p. We now explain the definition of the homomorphism $\chi_{C,v,\mathrm{crys}} : O_{F_v}^\times \to k_v^\times$.

Let $I_{F_v} \to k_L^\times$ be the determinant of the action of I_{F_v} on the k_L-vector space $D(C_{f,O_L} \otimes_{O_L} k_L)$. By Lemma 2.14 (6), the image of this homomorphism is contained in $k_v^\times \subset k_L^\times$. Hence it factors through the unique cyclic quotient of I_{F_v} of order $N(v)-1$, and therefore through the homomorphism $I_{F_v} \to O_{F_v}^\times$ given by local class field theory. We denote the induced homomorphism $O_{F_v}^\times \to k_v^\times$ by $\chi_{C,v,f,\mathrm{crys}}$. On the other hand, let

$$\chi_{C,v,f} \text{ (resp. } \chi_{C,v,/f}) \ : \ \mathrm{Gal}(\bar{F}_v/F_v) \to \mathbb{F}_p^\times$$

be the determinant of the action of $\mathrm{Gal}(\bar{F}_v/F_v)$ on the $\mathbb{F}_p$-vector space C_{f,F_v} (resp. $C/C_{f,F_v}$). We again denote the homomorphism $F_v^\times \to \mathbb{F}_p^\times$ induced by $\chi_{C,v,f}$ (resp. $\chi_{C,v,/f}$) via local class field theory, by the same letter $\chi_{C,v,f}$ (resp. $\chi_{C,v,/f}$). Clearly $\chi_{C,v}$ is then the product of the two characters

$$\chi_{C,v} = \chi_{C,v,f}\chi_{C,v,/f}.$$

Thus we finally define the crystalline version $\chi_{C,v,\mathrm{crys}}$ of $\chi_{C,v}$ as the product of two characters

$$\chi_{C,v,\mathrm{crys}} = \chi_{C,v,f,\mathrm{crys}}\chi_{C,v,/f} : O_{F_v}^\times \to k_v^\times.$$

2.16. We prove Proposition 2.8 (1).

For $K = \mathbb{R}$ or $\mathbb{C}$, $\epsilon(W_K, V, \psi, dx)$ for an irreducible representation V of W_K is given as follows ([13]). Take (ψ, dx) as in (a), (b) in 2.9. Let $K = \mathbb{C}$. Then V is a 1-dimensional representation $z \mapsto z^{-N}||z||^s$ ($N \in \mathbb{Z}$, $s \in \mathbb{C}$, $z \in W_\mathbb{C} = \mathbb{C}^\times$), and $\epsilon(W_K, V, \psi, dx) = i^{|N|}$. Let $K = \mathbb{R}$. Then V is a 1-dimensional representation $x \mapsto ||x||^s$ ($s \in \mathbb{C}$, $x \in W_\mathbb{R}^{\mathrm{ab}} = \mathbb{R}^\times$) and $\epsilon(W_K, V, \psi, dx) = 1$, or V is a 1-dimensional representation $x \mapsto x^{-1}||x||^s$ ($s \in \mathbb{C}, x \in W_\mathbb{R}^{\mathrm{ab}} = \mathbb{R}^\times$) and $\epsilon(W_K, V, \psi, dx) = i$, or V is a 2-dimensional representation induced from the 1-dimensional representation $z \mapsto z^{-N}||z||^s$ ($N \in \mathbb{Z}$, $N \geq 1$, $s \in \mathbb{C}$, $z \in W_\mathbb{C} = \mathbb{C}^\times$) of $W_\mathbb{C} \subset W_\mathbb{R}$ and $\epsilon(W_K, V, \psi, dx) = i^{N+1}$.

We have $w_K(A) = (-1)^g$ where $g = \dim(A)$. In fact, if $K = \mathbb{C}$, $V(A)$ is the direct sum of g copies of $z \mapsto z^{-1} \oplus z||z||^{-1}$ and hence $\epsilon(W_K, \mathcal{V}(A), \psi, dx) = (i \cdot i)^g = (-1)^g$. If $K = \mathbb{R}$, $V(A)$ is the direct sum of g copies of the 2-dimensional irreducible representation induced from the 1-dimensional representation $z \mapsto z^{-1}$ of $W_\mathbb{C} = \mathbb{C}^\times$, and hence $\epsilon(W_K, V(A), \psi, dx) = (i^{1+1})^g = (-1)^g$.

We prove the statement on $(-1)^{h(v)}$ in Proposition 2.8 (1). First let v be a complex place of F. Then we have an exact sequence

$$0 \to C \to A(\mathbb{C}) \to A'(\mathbb{C}) \to 0.$$

Hence $\chi(A(\mathbb{C}) \to A'(\mathbb{C})) = \sharp(C)^{-1} = p^{-g}$ and hence $h(v) = -g$. Since $\chi_{C,v}$ is trivial, this proves $(-1)^{h(v)} = (-1)^g = (-1)^g\chi_{C,v}(-1)$. Next assume v is a real place of F. Let C^+ (resp. C^-) be the part of C on which the complex conjugation acts by 1 (resp. -1). Let $n(\pm) = \mathrm{ord}_p\sharp(C^\pm)$. Then $n(+) + n(-) = g$. We have an exact sequence

$$0 \to C^+ \to A(\mathbb{R}) \to A'(\mathbb{R}) \to J \to 0$$

where J is killed by 2. Hence $h(v) = \mathrm{ord}_p\chi(A(\mathbb{R}) \to A'(\mathbb{R})) = -n(+)$. On the other hand, $\chi_{C,v}(-1) = (-1)^{n(-)}$. Therefore $(-1)^g\chi_{C,v}(-1) = (-1)^{g-n(-)} = (-1)^{n(+)} = (-1)^{h(v)}$.

2.17. We prove the formula for $w_v(A)$ in Proposition 2.8 (2).

By (32), it is sufficient to prove $\epsilon(W_{F_v}, \mathcal{V}(A), \psi, dx) = \chi_{C,v}(-1)$ for (ψ, dx) self-dual. Let (ψ, dx) be as in (c) in 2.9. Let U be as in Lemma 2.14 (4). Fix an isomorphism $\mathbb{C} \simeq \bar{\mathbb{Q}}_p$. Since $(U \oplus U^*(1)) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ and $A[p]$ have isomorphic semi-simplifications as representations over $\mathbb{F}_p$, the theory of the "modified ϵ- factor" ϵ_0 of Deligne in [13, §6] shows that

$$\epsilon(W_{F_v}, \mathcal{V}(A), \psi, dx) \cdot \det(-\varphi_{k_v}\ ;\ \mathcal{V}(A)^{I_{F_v}})$$
$$\equiv \epsilon(W_{F_v}, U \oplus U^*(1), \psi, dx) \cdot \det(-\varphi_{k_v}\ ;\ ((U \oplus U^*(1)) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p)^{I_{F_v}}) \mod \mathfrak{m}$$

where $\mathfrak{m}$ is the maximal ideal of $\bar{\mathbb{Q}}_p$ (these ϵ and det are units in $\bar{\mathbb{Q}}_p$). Since the actions of I_{F_v} on $\mathcal{V}(A)$ and on $U \oplus U^*(1)$ factor through finite quotients of I_{F_v} whose orders are prime to p,

$$\det(-\varphi_{k_v}\ ;\ \mathcal{V}(A)^{I_{F_v}}) \mod \mathfrak{m} = \det(-\varphi_{k_v}\ ;\ (A[p]_{\mathrm{ss}})^{I_{F_v}})$$
$$\det(-\varphi_{k_v}\ ;\ ((U \oplus U^*(1)) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p)^{I_{F_v}}) \mod \mathfrak{m} = \det(-\varphi_{k_v}\ ;\ ((U \oplus U^*(1)) \otimes_{\mathbb{Z}_p} \mathbb{F}_p)^{I_{F_v}})$$

and hence these are equal. Hence

$$\epsilon(W_{F_v}, \mathcal{V}(A), \psi, dx) \equiv \epsilon(W_{F_v}, U \oplus U^*(1), \psi, dx) \mod \mathfrak{m}.$$

By (22), we have

$$\epsilon(W_{F_v}, U \oplus U^*(1), \psi, dx) = \chi_U(-1), \quad \chi_U(-1) \mod \mathfrak{m} = \chi_{C,v}(-1).$$

Since $\epsilon(W_{F_v}, \mathcal{V}(A), \psi, dx)$ and $\chi_{C,v}(-1)$ belong to $\{\pm 1\}$, these congruences $\mod \mathfrak{m}$ show that $\epsilon(W_{F_v}, \mathcal{V}(A), \psi, dx) = \chi_{C,v}(-1)$, as required.

2.18. We prove the formula for $w_v(A)$ in Proposition 2.8 (3). By (32), it is enough to prove $\epsilon(W_{F_v}, \mathcal{V}(A), \psi, dx) = \chi_{C,v,\mathrm{crys}}(-1)$ for (ψ, dx) self-dual. Let U be as in Lemma 2.14 (5). By (22), we have $\epsilon(W_{F_v}, \mathcal{V}(A), \psi, dx) = \chi_U(-1)$. This shows that for any representation Y of I_{F_v} of dimension g over k_L such that

$$Y \oplus Y^* \simeq D(T[p] \otimes_{O_L} k_L) \oplus D(B[p] \otimes_{O_L} k_L) \oplus X(T^*) \otimes_{\mathbb{Z}} k_L$$

as representations of I_{F_v}, we have $\epsilon(W_{F_v}, \mathcal{V}(A), \psi, dx) = \chi_Y(-1)$. By the duality described in 2.13, we can take $Y = D(C_{f,O_L} \otimes_{O_L} k_L) \oplus C/C_{f,L} \otimes_{\mathbb{F}_p} k_L$. For this Y, $\chi_Y(-1) = \chi_{C,v,\mathrm{crys}}(-1)$ by definition.

The next two lemmas will be used in the proof of the formulae for $(-1)^{h(v)}$ in Proposition 2.8 (2) (3).

Lemma 2.19. *Let the assumption be as in Theorem 2.1, and let v be a finite place of F, with $h(v)$ as in (3). In the notation of 2.10, take F_v as K, and let L be a finite Galois extension of K such that A has split semistable reduction over L and such that the order of the inertial subgroup of $\Delta := \mathrm{Gal}(L/K)$ is prime to p (cf. Lemma 2.14 (1)). Then:-*

(1) *We have $h(v) = a - b + c$, where*

$$a = \mathrm{ord}_p\, \chi(\mathfrak{A}(O_L)^{\Delta} \xrightarrow{\phi} \mathfrak{A}'(O_L)^{\Delta}),$$

$$b = \operatorname{ord}_p \chi(X(T^*)^\Delta \to X((T')^*)^\Delta), \quad c = \operatorname{ord}_p \chi(X(T')^\Delta \to X(T)^\Delta).$$

Here the arrows in the definitions of b and c are induced by ϕ^* and ϕ, respectively.

(2) $b + c = t(v)$.

(3) $\operatorname{ord}_p(\mathfrak{A}(k_L)^\Delta) = \operatorname{ord}_p(\mathfrak{A}'(k_L)^\Delta)$.

Proof. From the exact sequence of Δ-modules

$$0 \to X(T^*) \to \mathfrak{A}(L) \to A(L) \to 0,$$

we obtain the exact sequence

$$0 \to X(T^*)^\Delta \to \mathfrak{A}(L)^\Delta \to A(K) \to H^1(\Delta, X(T^*)). \tag{42}$$

We also have the exact sequence of Δ-modules

$$0 \to \mathfrak{A}(O_L) \to \mathfrak{A}(L) \to \operatorname{Hom}(X(T), \mathbb{Z}) \to 0,$$

which gives rise to a further exact sequence

$$0 \to \mathfrak{A}(O_L)^\Delta \to \mathfrak{A}(L)^\Delta \to \operatorname{Hom}(X(T), \mathbb{Z})^\Delta \to H^1(\Delta, \mathfrak{A}(O_L)). \tag{43}$$

It is then easy to see that assertion (1) of the lemma follows on applying (42), (43), and the following claims (i), (ii), and (iii), for both the abelian varieties A and A':-

(i). $H^1(\Delta, X(T^*))$ is a finite group whose order is prime to p.

(ii). $H^1(\Delta, \mathfrak{A}(O_L))$ is a finite group whose order is prime to p.

(iii). The canonical map $\operatorname{Hom}(X(T), \mathbb{Z})^\Delta \to \operatorname{Hom}(X(T)^\Delta, \mathbb{Z})$ is injective with finite cokernel of order prime to p.

We now prove these three claims, beginning with (i). Let $\Delta_1 \subset \Delta$ denote the kernel of the map $\Delta \to \operatorname{Aut}(X(T^*))$. Then the order of Δ/Δ_1 is prime to p by Lemma 2.14 (2). We have the exact sequence

$$0 \to H^1(\Delta/\Delta_1, X(T^*)) \to H^1(\Delta, X(T^*)) \to H^1(\Delta_1, X(T^*)).$$

But $H^1(\Delta_1, X(T^*)) = \operatorname{Hom}(\Delta_1, X(T^*)) = 0$, and $H^1(\Delta/\Delta_1, X(T^*))$ is finite and of order prime to p, and so (i) follows. It is also clear that (iii) follows from the fact that the order of the image of Δ in $\operatorname{Aut}(X(T))$ is prime to p. Hence we are left to establish the more delicate claim (ii). We first prove that

(iv). $H^1(\Delta, \mathfrak{A}(k_L))$ is a finite group of order prime to p.

Let $\Delta_0 \subset \Delta$ be the inertial subgroup, so that the order of Δ_0 is prime to p. In view of the exact sequence

$$0 \to H^1(\operatorname{Gal}(k_L/k_K), \mathfrak{A}(k_L)^{\Delta_0}) \to H^1(\Delta, \mathfrak{A}(k_L)) \to H^1(\Delta_0, \mathfrak{A}(k_L)),$$

in which $H^1(\Delta_0, \mathfrak{A}(k_L))$ is of order prime to p, it is suffices to prove that the left hand group in this sequence also has order prime to p. Now we have an injection

$$H^1(\mathrm{Gal}(k_L/k_K), \mathfrak{A}(k_L)^{\Delta_0}) \to H^1(\mathrm{Gal}(\bar{k}_K/k_K), \mathfrak{A}(\bar{k}_K)^{\Delta_0}) = \mathrm{Coker}\,(1 - \varphi_{k_K}; \mathfrak{A}(\bar{k}_K)^{\Delta_0}).$$

Since $\mathfrak{A}(\bar{k}_K)$ is p-divisible and the order of Δ_0 is prime to p, $\mathfrak{A}(\bar{k}_K)^{\Delta_0}$ is also p-divisible. Now $\mathrm{Ker}\,(1-\varphi_{k_K}; \mathfrak{A}(\bar{k}_K)^{\Delta_0})$ is a subgroup of $\mathfrak{A}(k_L)^{\Delta_0}$ and hence is finite. This shows that the map $1 - \varphi_{k_K} : \mathfrak{A}(\bar{k}_K)^{\Delta_0} \to \mathfrak{A}(\bar{k}_K)^{\Delta_0}$ is surjective, proving (iv). Next we establish the following assertion:-

(v). Assuming $p = \mathrm{char}(k_K)$, we have $H^1(\Delta, \mathfrak{A}(\mathfrak{m}_L^i)/\mathfrak{A}(\mathfrak{m}_L^{i+1})) = 0$ for all $i \geq 1$, where $\mathfrak{A}(\mathfrak{m}_L^i) = \mathrm{Ker}\,(\mathfrak{A}(O_L) \to \mathfrak{A}(O_L/\mathfrak{m}_L^i))$.

We have a canonical isomorphism of Δ-modules

$$(44) \qquad \mathfrak{A}(m_L^i)/\mathfrak{A}(m_L^{i+1}) \simeq \mathfrak{m}_L^i \mathrm{Lie}(\mathfrak{A})/\mathfrak{m}_L^{i+1}\mathrm{Lie}(\mathfrak{A}) \quad (i \geq 1).$$

Hence it is sufficient to prove that

$$(45) \qquad H^1(\Delta, \mathfrak{m}_L^i \mathrm{Lie}(\mathfrak{A})/\mathfrak{m}_L^{i+1}\mathrm{Lie}(\mathfrak{A})) = 0.$$

Let V be the Δ_0-fixed subgroup of $\mathfrak{m}_L^i \mathrm{Lie}(\mathfrak{A})/\mathfrak{m}_L^{i+1}\mathrm{Lie}(\mathfrak{A})$. Then

$$H^1(\Delta, \mathfrak{m}_L^i \mathrm{Lie}(\mathfrak{A})/\mathfrak{m}_L^{i+1}\mathrm{Lie}(\mathfrak{A})) \simeq H^1(\mathrm{Gal}(k_L/k_K), V).$$

But any k_L-vector space of finite dimension n endowed with a semi-linear action of $\mathrm{Gal}(k_L/k_K)$ is isomorphic to k_L^n because of the well known fact that $H^1(\mathrm{Gal}(k_L/k_K), GL_n(k_L)) = \{1\}$. By applying this to V, and noting again that $H^1(\mathrm{Gal}(k_L/k_K), k_L) = 0$, we conclude that $H^1(\mathrm{Gal}(k_L/k_K), V) = 0$. This completes the proof of (v). Finally, to deduce (ii), we observe that, when $p = \mathrm{char}(k_K)$, (ii) follows from immediately from (iv) and (v). When $\ell = \mathrm{char}(k_K)$ is distinct from p, (ii) is a consequence of (iv) and the fact that $\mathrm{Ker}\,(\mathfrak{A}(O_L) \to \mathfrak{A}(k_L))$ is a pro-ℓ group. This completes the proof of (ii), and so also of (1).

We now turn to assertion (2). In the commutative diagram

$$\begin{tikzcd}
T' \arrow[r, "\phi'"] \arrow[d, "\psi'"'] & T \arrow[d, "\psi"] \\
(T')^* \arrow[r, "\phi^*"] & T^*,
\end{tikzcd}$$

as the degrees of ψ, ψ' are prime to p, the vertical arrows induce an isomorphism from the kernel of the upper horizontal arrow to the kernel of the lower horizontal arrow. This proves that

$$\mathrm{Coker}\,(X(T^*)^{\Delta} \xrightarrow{\phi^*} X((T')^*)^{\Delta}) \simeq \mathrm{Coker}\,(X(T)^{\Delta} \xrightarrow{\phi'} X(T')^{\Delta}).$$

Hence

$$b + c = \mathrm{ord}_p \chi(X(T')^{\Delta} \xrightarrow{\phi} X(T)^{\Delta}) + \mathrm{ord}_p \chi(X(T)^{\Delta} \xrightarrow{\phi'} X(T')^{\Delta})$$

$$= \mathrm{ord}_p\chi(p : X(T)^\Delta \to X(T)^\Delta) = t(v).$$

For the proof of (3), let $\Delta_0 \subset \Delta$ be the inertia subgroup as above, and let W be the p-primary subgroup of $\mathfrak{A}(\bar{k}_K)^{\Delta_0}$. Then W is a divisible $\mathbb{Z}_p$-module of cofinite type, the map $1 - \varphi_{k_v}$ is surjective, and the p-primary subgroup of $\mathfrak{A}(k_L)^\Delta$ is the kernel of $1 - \varphi_{k_K} : W \to W$. Let $T_p(W)$ be the Tate module of W and let $V_p(W) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(W)$. Then the usual snake lemma argument shows that

$$\mathrm{ord}_p \, \sharp(\mathfrak{A}(k_L)^\Delta) = \mathrm{ord}_p \, \det(1 - \varphi_{k_K} \,:\, V_p(W) \to V_p(W)).$$

But the right hand side does not change if we replace A by A', because we have an isogeny from $\mathfrak{A}$ to $\mathfrak{A}'$. This completes the proof. □

Lemma 2.20. *Let the assumption and the notation be as in Lemma 2.19, and assume that v divides p. Then:-*

(1)
$$\mathrm{ord}_p\sharp((\mathrm{Lie}(\mathfrak{A}) \otimes_{O_L} k_L)^\Delta) \equiv \mathrm{ord}_p\sharp((\mathrm{Lie}(\mathfrak{A}') \otimes_{O_L} k_L)^\Delta) \mod 2.$$

(2) *Define $\chi(\exp_A)$ as follows. Take a Δ-stable subgroup U of* Lie($\mathfrak{A}$) *of finite index such that the exponential map $U \to \mathfrak{A}(O_L)$ is defined, and let*

$$\chi(\exp_A) := \chi(U^\Delta \overset{\exp}{\to} \mathfrak{A}(O_L)^\Delta) \cdot [\mathrm{Lie}(\mathfrak{A})^\Delta : U^\Delta]^{-1} \tag{46}$$

noting that $\chi(\exp_A)$ is independent of the choice of U. We have

$$\chi(\exp_A) = \sharp(\mathfrak{A}(k_L)^\Delta) \cdot \sharp((\mathrm{Lie}(\mathfrak{A}) \otimes_{O_L} k_L)^\Delta)^{-1},$$

and similarly for A'.

(3) $\mathrm{ord}_p\chi(\exp_A) \equiv \mathrm{ord}_p\chi(\exp_{A'}) \mod 2$.

(4) $\mathrm{ord}_p\chi(\mathfrak{A}(O_L)^\Delta \xrightarrow{\phi} \mathfrak{A}'(O_L)^\Delta) \equiv \mathrm{ord}_p\chi(\mathrm{Lie}(\mathfrak{A})^\Delta \xrightarrow{\phi} \mathrm{Lie}(\mathfrak{A}')^\Delta) \mod 2$.

(5) $\chi(\mathrm{Lie}(\mathfrak{A})^\Delta \xrightarrow{\phi} \mathrm{Lie}(\mathfrak{A}')^\Delta) = \sharp(\mathrm{Lie}(C_{f,O_L})^\Delta)$.

(6) *Let $n = \mathrm{ord}_p\sharp(\mathrm{Lie}(C_{f,O_L})^\Delta)$. Then $(-1)^n = \chi_{C,v}(-1)\chi_{C,v,\mathrm{crys}}(-1)$.*

Here, in connexion with (5), we recall that $\mathrm{Lie}(C_{f,O_L})$ is defined as follows. For a finite flat commutative scheme P over a commutative ring R such that $p : P \to P$ is the zero map, let

$$\mathrm{Lie}(P) = \mathrm{Ker}\,(P((R/pR)[x]/(x^2)) \to P(R/pR))$$

where x is an indeterminate.

Proof. We prove Lemma 2.20 except for part (6), whose proof will be given in the Appendix. To establish (1), let D be the covariant Dieudonné module of $\mathfrak{A}_{p^\infty} \otimes_{O_L} k_L$. Then

$$\mathrm{Lie}(\mathfrak{A}) \otimes_{O_L} k_L \simeq D/VD,$$

where $V : D \to D$ is the usual V-operator of the Dieudonné module. We have $H^1(\Delta, D) = 0$ by the method in the proof of (45). Thus

$$(\mathrm{Lie}(\mathfrak{A}) \otimes_{O_L} k_L)^\Delta \simeq (D/VD)^\Delta \simeq D^\Delta/VD^\Delta,$$

whence it follows easily that

$$\mathrm{ord}_p \sharp((\mathrm{Lie}(\mathfrak{A}) \otimes_{O_L} k_L)^\Delta) = \mathrm{ord}_p \det(V : \mathbb{Q}_p \otimes_{\mathbb{Z}_p} D \to \mathbb{Q}_p \otimes_{\mathbb{Z}_p} D).$$

The right hand side does not change when A is replaced by A' because we have an isogeny from $\mathfrak{A}$ to $\mathfrak{A}'$. Assertion (2) follows from the fact that for a sufficiently large i, $\exp_A$ induces an isomorphism from $\mathfrak{m}_L^i\mathrm{Lie}(\mathfrak{A})$ onto the kernel of the surjective homomorphism $\mathfrak{A}(O_L) \to \mathfrak{A}(O_L/\mathfrak{m}_L^i)$, and from (44). Part (3) follows from (1), (2), and Lemma 2.19, (3). Assertion (4) follows from (3) and the equality

$$\chi(\exp_A) \cdot \chi(\mathfrak{A}(O_L)^\Delta \to \mathfrak{A}'(O_L)^\Delta) = \chi(\exp_{A'}) \cdot \chi(\mathrm{Lie}(\mathfrak{A})^\Delta \to \mathrm{Lie}(\mathfrak{A}')^\Delta).$$

Finally, (5) follows from the exact sequence

$$0 \to \mathrm{Lie}(\mathfrak{A}) \to \mathrm{Lie}(\mathfrak{A}') \to \mathrm{Lie}(C_{f,O_L}) \to 0$$

which, in turn, arises from the exact sequence

$$0 \to C_{f,O_L} \to \mathfrak{A} \to \mathfrak{A}' \to 0.$$

□

2.21. We can at last prove the formulae for $(-1)^{h(v)}$ given in Proposition 2.8 (2),(3), where v is any finite place of F. By (1) and (2) of Lemma 2.19, we have $h(v) \equiv t(v) + a \mod 2$ with a as in Lemma 2.19 (1). Thus it is sufficient to prove that $a \equiv 0 \mod 2$ when v does not divide p, and $(-1)^a = \chi_{C,v}(1)\chi_{C,\mathrm{crys}}(-1)$ when v divides p. Suppose first that v does not divide p. Since the surjections $\mathfrak{A}(O_L) \to \mathfrak{A}(k_L)$ and $\mathfrak{A}'(O_L) \to \mathfrak{A}'(k_L)$ induce isomorphisms on the pro-p components, we have $a = \mathrm{ord}_p \chi(\mathfrak{A}(k_L) \xrightarrow{\phi} \mathfrak{A}'(k_L))$, and this is zero by Lemma 2.19 (3). Suppose next that v divides p. Then $a \equiv \mathrm{ord}_p \sharp(\mathrm{Lie}(C_{f,O_L})^\Delta) \mod 2$ by Lemma 2.20 (4) (5), whence

$$(-1)^a = \chi_{C,v}(-1)\chi_{C,v,\mathrm{crys}}(-1)$$

by Lemma 2.20 (6). This completes the proof.

3 Background from Iwasawa theory

The aim of this section is to collect together a number of results, all of which are essentially well known. However, as they will be used repeatedly later, we wish to set them out clearly in the form in which they will be needed.

We begin with an elementary result from K-theory. Quite generally, assume that H is any compact p-adic Lie group satisfying:- (i) H has no element of order p, (ii) H has a pro-p open normal subgroup H' such that $\Delta = H/H'$ is a finite abelian group of exponent $p-1$. Since H' is pro-p, and Δ has order prime to p, a well-known result from group theory shows that H is in fact the semi-direct product of its normal subgroup H' with a subgroup D isomorphic to Δ. Further, as H has no element of order p and Δ is finite of order prime to p, the rings $\Lambda(H)$ and $\mathbb{Z}_p[\Delta]$ both have finite global dimension. We can therefore identify in both cases, the K_0 of these rings with the Grothendieck group of the category of finitely generated modules. As H' is pro-p, it is well known that the map

$$K_0(\Lambda(H)) \to K_0(\mathbb{Z}_p[\Delta]) \tag{47}$$

which is given, for any finitely generated $\Lambda(H)$-module M, by

$$[M] \mapsto \sum_{i \geq 0} (-1)^i \, [H_i(H', M)]$$

is an isomorphism (see [8, Lemma 4.1]). Put

$$\hat{\Delta} = \mathrm{Hom}(\Delta, \mathbb{Z}_p^\times).$$

Each χ in $\hat{\Delta}$ gives rise to a ring homomorphism from $\mathbb{Z}_p[\Delta]$ to $\mathbb{Z}_p$, whence we obtain an isomorphism of rings

$$\mathbb{Z}_p[\Delta] \simeq \prod_{\chi \in \hat{\Delta}} \mathbb{Z}_p, \tag{48}$$

which, in turn, gives an isomorphism

$$K_0(\mathbb{Z}_p[\Delta]) \simeq \bigoplus_{\chi \in \hat{\Delta}} \mathbb{Z}. \tag{49}$$

Composing (47) and (49), we obtain an isomorphism

$$l_\Delta : K_0(\Lambda(H)) \simeq \bigoplus_{\chi \in \hat{\Delta}} \mathbb{Z}. \tag{50}$$

On the other hand, since H' is pro-p and has no elements of order p, the ring $\Lambda(H')$ is a Noetherian integral domain, and hence it has a skew field of quotients which we denote by $Q(\Lambda')$. If M is a finitely generated $\Lambda(H)$-module, we recall that

$$\mathrm{rank}_{\Lambda(H')}(M) = \dim_{Q(\Lambda')}(Q(\Lambda') \otimes_{\Lambda(H')} M).$$

Lemma 3.1. *Let M be a finitely generated $\Lambda(H)$-module and write $l_\Delta([M]) = (n_\chi(M))$, where l_Δ is the isomorphism* (50). *Then*

$$\mathrm{rank}_{\Lambda(H')}(M) = \sum_{\chi \in \hat{\Delta}} n_\chi(M). \tag{51}$$

Proof. Since H' is pro-p, and has no element of order p, it is well known that

$$\operatorname{rank}_{\Lambda(H')}(M) = \textstyle\sum_{i\geq 0} (-1)^i \operatorname{rank}_{\mathbb{Z}_p} H_i(H', M).$$

For each χ in $\hat{\Delta}$ and each $\mathbb{Z}_p[\Delta]$-module R, write $R^{(\chi)}$ for the χ-component of R. Plainly,

$$n_\chi(M) = \textstyle\sum_{i\geq 0} (-1)^i \operatorname{rank}_{\mathbb{Z}_p} H_i(H', M)^{(\chi)},$$

and the assertion (51) follows immediately. □

We continue to assume that H satisfies the conditions (i) and (ii) given at the beginning of this section. Suppose now that we are given an arbitrary Artin representation

$$\rho : H \to GL_{d_\rho}(\mathcal{O}),$$

where $\mathcal{O}$ is the ring of integers of some finite extension of $\mathbb{Q}_p$. We often write W_ρ for $\mathcal{O}^{d_\rho}$, endowed with the left action of H given by ρ. We define the Akashi homomorphism

$$h_\rho : K_0(\Lambda(H)) \to \mathbb{Z}$$

by

$$h_\rho([N]) = \sum_{i\geq 0} (-1)^i \operatorname{rank}_{\mathcal{O}} \left(H_i(H, \operatorname{tw}_\rho(N))\right), \tag{52}$$

where $\operatorname{tw}_\rho(N) = W_\rho \otimes N$ with the diagonal action of H. On the other hand, we have the isomorphism l_Δ given by (50), and for each χ in $\hat{\Delta}$, let P_χ be a projective $\Lambda(H)$-module such that $l_\Delta([P_\chi])$ is the vector with 1 in the χ-th component and 0 elsewhere. For example, we could take $P_\chi = \Lambda(H)e_\chi$, where e_χ is the idempotent of χ in $\mathbb{Z}_p[D]$. We define $m_\chi(\rho) = h_\rho([P_\chi])$ for each Artin representation ρ of G. Plainly, we then have

$$h_\rho([N]) = \sum_{\chi\in\hat{\Delta}} m_\chi(\rho)\, n_\chi, \tag{53}$$

where $l_\Delta([N]) = (n_\chi)$. The following lemma gives a useful alternative expression for these integers $m_\chi(\rho)$. Let k denote the residue field of $\mathcal{O}$ and

$$\tilde{\rho} : H \to GL_{d_\rho}(k)$$

be the reduction of ρ modulo the maximal ideal. We write $\tilde{\rho}^{\mathrm{ss}}$ for the semisimplification of $\tilde{\rho}$.

Lemma 3.2. *The representation $\tilde{\rho}^{\mathrm{ss}}$ of H is trivial on H' and so gives a representation of Δ. Further, we have $\tilde{\rho}^{\mathrm{ss}} = \bigoplus_{\chi\in\hat{\Delta}} m_{\chi^{-1}}(\rho)\tilde{\chi}$, where $\tilde{\chi}$ denotes the reduction of χ modulo p.*

Proof. To prove the first assertion, let θ be any irreducible representation of H in a finite dimensional $\bar{\mathbb{F}}_p$ vector space V_θ over $\bar{\mathbb{F}}_p$. Thus V_θ is a simple $\bar{\mathbb{F}}_p[[H]]$-module, and hence it is annihilated by the Jacobson radical of this ring. In particular, V_θ is annihilated by the kernel of the natural surjection from $\bar{\mathbb{F}}_p[[H]]$ to $\bar{\mathbb{F}}_p[\Delta]$ because H' is pro-p. Thus V_θ is an irreducible $\bar{\mathbb{F}}_p[\Delta]$-module, and hence $\theta = \tilde{\chi}$ for some $\chi \in \hat{\Delta}$. Thus $\tilde{\rho}^{\mathrm{ss}}$ must factor through Δ, proving the first assertion.

Next, noting that p lies in the Jacobson radical of $\Lambda(H)$ and again using that H' is pro-p, we have the isomorphism

$$\eta : K_0(\Lambda(H)) \simeq K_0(\mathbb{F}_p[\Delta]),$$

given explicitly by mapping the class $[P]$ of a projective module P to $[(P/pP)_{H'}]$. Given any representation $\phi : \Delta \to \mathrm{Aut}(V_\phi)$, where V_ϕ is a finite dimensional $\mathbb{F}_p$-vector space V_ϕ, we can also define a map

$$r_\phi : K_0(\mathbb{F}_p[\Delta]) \to \mathbb{Z}$$

by

$$r_\phi([W]) = \dim_{\mathbb{F}_p}(V_\phi \otimes W)^\Delta.$$

For each χ in Δ, let W_χ denote the $\mathbb{F}_p$ -vector space of dimension 1 on which Δ acts via χ. Plainly, we have

$$r_{\chi_1}([W_{\chi_2}]) = 1 \text{ if } \chi_1\chi_2 = \mathbf{1} \text{ and } = 0 \text{ if } \chi_1\chi_2 \neq \mathbf{1}.$$

Writing $\tilde{\rho}^{\mathrm{ss}} = \sum_{\chi \in \hat{\Delta}} a_\chi(\rho)\tilde{\chi}$, it follows that

$$r_{\tilde{\rho}^{\mathrm{ss}}}([W_\chi]) = a_{\chi^{-1}}(\rho).$$

On the other hand, it is readily verified that

$$r_{\tilde{\rho}^{\mathrm{ss}}} = h_\rho \circ \eta^{-1}.$$

But clearly $(h_\rho \circ \eta^{-1})([W_\chi]) = m_\chi(\rho)$ and the proof of the lemma is complete. □

We now discuss some important results about Selmer groups of elliptic curves and their Artin twists. Suppose now that F is a finite extension of $\mathbb{Q}$, and write F^{cyc} for the cyclotomic $\mathbb{Z}_p$-extension of F. Define a Galois extension F_∞ of F to be an *admissible p-adic Lie extension* if the following conditions are satisfied:- (i) $G = \mathrm{Gal}(F_\infty/F)$ is a p-adic Lie group having no element of order p, (ii) only finitely many primes of F ramify in F_∞, and (iii) F_∞ contains the cyclotomic $\mathbb{Z}_p$-extension F^{cyc} of F. Suppose now that we are given an admissible p-adic Lie extension F_∞ of F. We define

$$H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}}), \tag{54}$$

but we drop the additional assumptions on H made earlier in this section. Since H has no elements of order p by hypothesis, a wellknown theorem of Lazard-Serre [41] asserts that, for all finitely generated $\Lambda(H)$-modules M, we have $H_i(H, M) = 0$ when i is strictly greater than the dimension of G. As in [8], $\mathfrak{M}_H(G)$ will denote the category of all finitely generated $\Lambda(G)$-modules M such that $M/M(p)$ is finitely generated over $\Lambda(H)$. Throughout the remainder of this paper, E will denote an elliptic curve defined over F.

We suppose that we are given an Artin representation

$$\rho : \ G \to GL_{d_\rho}(\mathcal{O}),$$

where $\mathcal{O}$ is the ring of integers of some finite extension of $\mathbb{Q}_p$. Let

$$h_\rho : \ K_0(\Lambda(H)) \to \mathbb{Z}$$

be the homomorphism defined by (52). If $\mathcal{L}$ is any algebraic extension of F, we write $S(E/\mathcal{L})$ for the Selmer group of E over $\mathcal{L}$, and $X(E/\mathcal{L}) = \mathrm{Hom}\,(S(E/\mathcal{L}), \mathbb{Q}_p/\mathbb{Z}_p)$ for its Pontryagin dual. Moreover, we write

$$Y(E/\mathcal{L}) = X(E/\mathcal{L})/X(E/\mathcal{L})(p). \tag{55}$$

Assume now that E has potential good ordinary reduction at all primes v of F dividing p. Then it is conjectured [8] that we always have

$$X(E/F_\infty) \in \mathfrak{M}_H(G). \tag{56}$$

Assuming this conjecture, we now explain how to compute $h_\rho([Y(E/F_\infty)])$ in terms of invariants attached to E and ρ over F^{cyc}. To this end, let T denote any fixed finite set of primes of F which is so large that it contains (i) all primes dividing p, (ii) all primes where E has bad reduction, and (iii) all primes which ramify in F_∞. We write F_T for the maximal extension of F which is unramified outside T and the archimedean primes of F. We now recall the definition of Greenberg's twisted Selmer group $S(\mathrm{tw}_\rho(E)/\mathcal{L})$ for each extension $\mathcal{L}$ of F contained in F_∞ (see [22]). When ρ is the trivial representation of dimension 1, it is well known that (i) the classical Selmer group as defined in §2 is a subgroup of Greenberg's Selmer group of finite index when $\mathcal{L} = F$, and (ii) the two Selmer groups coincide whenever $\mathcal{L}$ contains F^{cyc}. As always, Greenberg's Selmer group will be a subgroup of $H^1(\mathrm{Gal}(F_T/\mathcal{L}), W_\rho \otimes_{\mathbb{Z}_p} E_{p^\infty})$, specified by local conditions at the primes of $\mathcal{L}$ above T; here W_ρ denotes a free $\mathcal{O}$-module of rank d_ρ realizing ρ. We now describe these local conditions. If w is a place of $\mathcal{L}$, we write $\mathcal{L}_w$ for the union of the completions at w of all finite extensions of F contained in $\mathcal{L}$. If w does not divide p, let

$$\lambda(w) : H^1(\mathrm{Gal}(F_T/\mathcal{L}), W_\rho \otimes_{\mathbb{Z}_p} E_{p^\infty}) \to H^1(\mathcal{L}_w, W_\rho \otimes_{\mathbb{Z}_p} E_{p^\infty})$$

denote the usual restriction map. Suppose next that v is a place of F dividing p, and let I_v be the inertial subgroup of $\mathrm{Gal}(\bar{F}_v/F_v)$. Since E has potential good ordinary reduction at v, it is well-known [9, p. 15] that there exists a canonical exact sequence of divisible $\mathrm{Gal}(\bar{F}_v/F_v)$-modules

$$0 \to C_v \to E_{p^\infty} \to D_v \to 0, \tag{57}$$

which is characterized by the fact that (i) C_v has $\mathbb{Z}_p$-corank equal to 1, and (ii) I_v acts on D_v via a finite quotient; here I_v is the inertia group at v. Tensoring (57) over $\mathbb{Z}_p$ with W_ρ, we obtain the exact sequence of $\mathrm{Gal}(\bar{F}_v/F_v)$-modules

$$0 \to W_\rho \otimes_{\mathbb{Z}_p} C_v \to W_\rho \otimes_{\mathbb{Z}_p} E_{p^\infty} \to W_\rho \otimes_{\mathbb{Z}_p} D_v \to 0. \tag{58}$$

Since ρ factors through a finite quotient of G, it is plain that again I_v will act on $W_\rho \otimes_{\mathbb{Z}_p} D_v$ via a finite quotient. If w is a place of $\mathcal{L}$ dividing p, we define

$$\lambda_w : H^1(\mathrm{Gal}(F_T/\mathcal{L}), W_\rho \otimes_{\mathbb{Z}_p} E_{p^\infty}) \to H^1(\mathcal{L}_w, W_\rho \otimes_{\mathbb{Z}_p} D_v)$$

to be the composition of the restriction map followed by the map from $H^1(\mathcal{L}_w, W_\rho \otimes_{\mathbb{Z}_p} E_{p^\infty})$ to $H^1(\mathcal{L}_w, W_\rho \otimes_{\mathbb{Z}_p} D_v)$ induced by (57). We can now define

$$S(\mathrm{tw}_\rho(E)/\mathcal{L}) = \bigcap_{w|T} \mathrm{Ker}\ \lambda_w, \tag{59}$$

where w runs over all places of $\mathcal{L}$ lying above T. We note that $S(\mathrm{tw}_\rho(E)/\mathcal{L})$ has a natural structure as an $\mathcal{O}$-module, and we define

$$X(\mathrm{tw}_\rho(E)/\mathcal{L}) = \mathrm{Hom}_{\mathcal{O}}(S(\mathrm{tw}_\rho(E)/\mathcal{L}), \mathcal{P}/\mathcal{O}), \tag{60}$$

where $\mathcal{P}$ denotes the quotient field of $\mathcal{O}$. We also put

$$Y(\mathrm{tw}_\rho(E)/\mathcal{L}) = X(\mathrm{tw}_\rho(E)/\mathcal{L})/X(\mathrm{tw}_\rho(E)/\mathcal{L})(p).$$

Assume now that ρ is irreducible, and write $\mathcal{F}$ for any finite Galois extension of F such that ρ factors through $\mathrm{Gal}(\mathcal{F}/F)$.

Definition 3.3. We define $s_{E,\rho}$ to be the number of copies of the representation $W_\rho \otimes_{\mathcal{O}} \bar{\mathbb{Q}}_p$ occurring in the finite dimensional $\bar{\mathbb{Q}}_p$-representation of $\mathrm{Gal}(\mathcal{F}/F)$ given by $X(E/\mathcal{F}) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$.

Lemma 3.4. *For each Artin representation ρ of G, we have*

$$\mathrm{tw}_\rho(X(E/F_\infty)) = X(\mathrm{tw}_{\hat{\rho}}(E)/F_\infty), \tag{61}$$

where $\hat{\rho}$ is the contragredient representation. Moreover, if ρ is irreducible, we have

$$s_{E,\rho} = \mathrm{rank}_{\mathcal{O}}(Y(\mathrm{tw}_\rho(E)/F)). \tag{62}$$

Proof. If M is any $\mathbb{Z}_p$-module, write $M_{\mathcal{O}} = M \otimes_{\mathbb{Z}_p} \mathcal{O}$. Since ρ factors through a finite quotient of G, we have

$$S(\mathrm{tw}_{\hat{\rho}}(E)/F_\infty) = S(E/F_\infty)_{\mathcal{O}} \otimes_{\mathcal{O}} W_{\hat{\rho}}.$$

Hence

$$X(\mathrm{tw}_{\hat{\rho}}(E)/F_\infty) = \mathrm{Hom}_{\mathcal{O}}(W_{\hat{\rho}}, X(E/F_\infty)_{\mathcal{O}}) = \mathrm{Hom}_{\mathcal{O}}(\mathrm{Hom}_{\mathcal{O}}(W_\rho, \mathcal{O}), X(E/F_\infty)_{\mathcal{O}}).$$

But as W_ρ is a free $\mathcal{O}$-module, by [5, Proposition 5.2], the module on the right above can be identified with

$$\mathrm{Hom}_{\mathcal{O}}(\mathcal{O}, X(E/F_\infty)_{\mathcal{O}}) \otimes_{\mathcal{O}} W_\rho = \mathrm{tw}_\rho(X(E/F_\infty)),$$

thereby proving (61).

Suppose next that ρ is irreducible and factors through a finite Galois extension $\mathcal{F}$ of F, and put

$$\Delta = \mathrm{Gal}(\mathcal{F}/F),\ W'_\rho = W_\rho \otimes_{\mathcal{O}} \bar{\mathbb{Q}}_p,\ A = Y(\mathrm{tw}_\rho(E)/\mathcal{F}) \otimes_{\mathcal{O}} \bar{\mathbb{Q}}_p.$$

An entirely similar argument to the one given above shows that

$$A = \mathrm{Hom}_{\bar{\mathbb{Q}}_p}(W'_\rho, Y(E/\mathcal{F}) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p).$$

On the other hand, the restriction map on cohomology gives rise to an isomorphism of $\bar{\mathbb{Q}}_p$-vector spaces

$$Y(\mathrm{tw}_\rho(E)/F) \otimes_{\mathcal{O}} \bar{\mathbb{Q}}_p \ \simeq\ A_\Delta = A^\Delta$$

where the last displayed equality is true by the semi-simplicity of the Δ-action. Hence

$$Y(\mathrm{tw}_\rho(E)/F) \otimes_{\mathcal{O}} \bar{\mathbb{Q}}_p \ \simeq\ \mathrm{Hom}_{\bar{\mathbb{Q}}_p[\Delta]}(W'_\rho, A),$$

and the last assertion (62) now follows from Schur's lemma. Indeed, since ρ is irreducible, Schur's lemma shows that $\mathrm{Hom}_{\bar{\mathbb{Q}}_p[\Delta]}(W'_\rho, W'_\rho)$ is $\bar{\mathbb{Q}}_p$. □

To proceed further, we must impose the following additional assumptions on our admissible p-adic Lie extension F_∞ of F, which are well known to be true for the extensions considered later in the paper. For each finite prime v of F^{cyc}, we write $H_v = \mathrm{Gal}(F_{\infty,v}/F_v^{\mathrm{cyc}})$ for the decomposition group of some fixed prime of F_∞ above v.

Hypothesis H1. For every open subgroup H' of H, $H^i(H', E_{p^\infty}(F_\infty))$ is finite for all $i \geq 1$.

Hypothesis H2. For each prime v of F^{cyc} dividing p, and each open subgroup H'_v of H_v, $H^i(H'_v, D_v(F_{\infty,v}))$ is finite for all $i \geq 1$, where D_v is given by the exact sequence (57).

We remark that, since E has potential good reduction at primes of F above p, Imai's theorem shows that the group $H^0(H', E_{p^\infty}(F_\infty))$ is finite. Write $P(F^{\mathrm{cyc}})$ for the set of primes of F^{cyc} which do not divide p, and whose inertial subgroups in $\mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$ are infinite.

Theorem 3.5. *Let F_∞/F be an admissible p-adic Lie extension, with p an odd prime. Assume that E has potential good ordinary reduction at all primes v of F dividing p and that Hypotheses H1 and H2 are valid. Further assume that $X(E/F_\infty) \in \mathfrak{M}_H(G)$. Then for all Artin representations ρ of G, we have that $H_i(H, \mathrm{tw}_\rho(Y(E/F_\infty)))$ is finite for all $i \geq 1$, and*

$$h_\rho([Y(E/F_\infty)]) = \mathrm{rank}_{\mathcal{O}}(Y(\mathrm{tw}_{\hat{\rho}}(E)/F^{\mathrm{cyc}})) + \sum_v \mathrm{corank}_{\mathcal{O}}(H^1(H_v, E_{p^\infty}(F_{\infty,v}) \otimes W_{\hat{\rho}})),$$

where the sum on the right is taken over all places of F^{cyc} lying in $P(F^{\mathrm{cyc}})$.

Proof. The proof is very similar to the arguments given in [10] and hence we omit the details. □

Lemma 3.6. *Assume v in $P(F^{\text{cyc}})$, and write J_v for the absolute Galois group of F_v^{cyc}. Then*

$$H^1(H_v, E_{p^\infty}(F_{\infty,v}) \otimes W_{\hat{\rho}}) = H^1(J_v, E_{p^\infty} \otimes W_{\hat{\rho}})$$

and its Pontryagin dual is $H^0(J_v, T_p(E) \otimes W_\rho)$.

Proof. The first assertion is true since the hypothesis that v is infinitely ramified in F_∞ shows that $\mathrm{Gal}(\bar{F}_v/F_{\infty,v})$ has no quotient of order divisible by p because $F_{\infty,v}$ contains the maximal tamely ramified p-extension of F_v. For the second assertion, we use the well known fact that, for any finite J_v-module M of order prime to the residue characteristic of v, $H^1(J_v, M)$ is dual to $H^0(J_v, M^D)$, where $M^D = \mathrm{Hom}\,(M, \mu_m)$ with $m = \#\,M$. Taking $M = E_{p^n} \otimes W_\rho$, $(n = 1, 2, \cdots)$, the result follows on passing to the limit over all n. □

Let v be a place of F^{cyc} such that $\mathrm{ord}_v(j_E) < 0$. If E does not have split multiplicative reduction at v, then it achieves split multiplicative reduction over a uniquely determined quadratic extension of F_v^{cyc}, which we denote by L_v. We then define χ_v to be either the trivial character of J_v, or the quadratic character of J_v defining the extension L_v, according as E does or does not have split multiplicative reduction at v. Let $\omega_v : J_v \to \mathbb{Z}_p^\times$ be the character giving the action of J_v on the group of all p-power roots of unity.

Lemma 3.7. *Let v be any finite place of F^{cyc} such that $ord_v(j_E) < 0$. Then*

$$\mathrm{rank}_{\mathcal{O}}(H^0(J_v, T_p(E) \otimes W_\rho)) = \mathrm{corank}_{\mathcal{O}}(H^1(J_v, E_{p^\infty} \otimes W_{\hat{\rho}})) = \langle \chi_v \omega_v^{-1}, \rho_v \rangle,$$

where $\langle \chi_v \omega_v^{-1}, \rho_v \rangle$ denotes the multiplicity of $\chi_v \omega_v^{-1}$ occurring in the restriction ρ_v of ρ to J_v.

Proof. By the theory of the Tate curve, we have the exact sequence of J_v-modules

$$0 \to W_{\chi_v}(1) \to T_p(E) \to W_{\chi_v} \to 0,$$

where W_{χ_v} denotes the free $\mathbb{Z}_p$-module of rank 1, on which J_v acts via χ_v. Let $\mathcal{L}_v$ denote a fixed finite Galois extension of F_v^{cyc} such that both χ_v and ρ_v factor through $\mathrm{Gal}(\mathcal{L}_v/F_v^{\text{cyc}})$, and write $\mathcal{J}_v$ for the absolute Galois group of $\mathcal{L}_v$. Then, since E has split multiplicative reduction over $\mathcal{L}_v$, it follows from the theory of the Tate curve (cf. [12], p. 138) that we have an isomorphism of J_v-modules

$$H^0(\mathcal{J}_v, W_{\chi_v}(1)) = H^0(\mathcal{J}_v, T_p(E)),$$

whence, on tensoring both sides with W_ρ and taking invariants under J_v, we obtain an isomorphism of $\mathcal{O}$-modules

$$H^0(J_v, W_{\chi_v}(1) \otimes W_\rho) = H^0(J_v, T_p(E) \otimes W_\rho).$$

The assertion of the lemma is now clear because J_v acts on $W_{\chi_v}(1) \otimes W_\rho$ via a finite quotient, and hence by semisimplicity its $\mathcal{O}$-rank is equal to $\langle \chi_v \omega_v^{-1}, \rho_v \rangle$. □

We next state an important result of Greenberg, which is proven in [23, Prop. 11.8], and which generalizes earlier work of Greenberg and Guo [21]. We shall use this result repeatedly in our subsequent arguments. If ρ is an irreducible Artin representation of G, we recall that ρ is said to be *orthogonal* if W_ρ admits a non-degenerate G-invariant symmetric bilinear form. An irreducible orthogonal Artin representation of G is automatically self-dual.

Theorem 3.8. *Assume that ρ is an irreducible orthogonal Artin representation of G such that $X(\mathrm{tw}_\rho(E)/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma_F)$-torsion, where $\Gamma_F = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$. Then*

$$s_{E,\rho} \equiv \lambda_\rho(E/F^{\mathrm{cyc}}) \mod 2, \tag{63}$$

where $\lambda_\rho(E/F^{\mathrm{cyc}}) = \mathrm{rank}_{\mathcal{O}}(Y(\mathrm{tw}_\rho(E)/F^{\mathrm{cyc}}))$.

We end this section by stating the standard hypotheses for an elliptic curve E and our admissible p-adic Lie extension F_∞/F, which we will need to impose in much of the remainder of the paper.

Hypothesis A1. E has potential good ordinary reduction at each place of F dividing p.

Hypothesis A2. $X(E/F_\infty)$ belongs to the category $\mathfrak{M}_H(G)$.

We believe that Hypothesis A2 should always be a consequence of Hypothesis A1. This is indeed true if there exists a finite extension F' of F contained in F_∞ such that the Galois group $\mathrm{Gal}(F_\infty/F')$ is pro-p and $X(E/F'^{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module. We also note that Hypothesis A2 implies that $X(\mathrm{tw}_\rho(E)/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma_F)$-torsion for each Artin representation ρ of G. Indeed, it is easily seen (cf. the proof of Lemma 5.3 of [8]) that Hypothesis A2 implies that $X(E/L^{\mathrm{cyc}})$ is $\Lambda(\Gamma_L)$-torsion for each finite extension L of F contained in F_∞. If ρ is an Artin representation of G, we now take L to be a finite Galois extension of F contained in F_∞ such that ρ factors through $\mathrm{Gal}(L/F)$. We then have

$$S(\mathrm{tw}_\rho(E)/L^{\mathrm{cyc}}) = S(E/L^{\mathrm{cyc}}) \otimes_{\mathcal{O}} W_\rho,$$

where, as earlier, W_ρ denotes a free $\mathcal{O}$-module of finite rank realizing ρ. As $X(E/L^{\mathrm{cyc}})$ is $\Lambda(\Gamma_L)$-torsion, it follows that the same is true for $X(\mathrm{tw}_\rho(E)/L^{\mathrm{cyc}})$. In particular, we see that $X(\mathrm{tw}_\rho(E)/F^{\mathrm{cyc}})$ must be $\Lambda(\Gamma_F)$-torsion, as claimed.

4 False Tate extension

Let E be an elliptic curve defined over a finite extension F of $\mathbb{Q}$, and assume throughout this section that p is an odd prime. Our goal is to strengthen the results of the Appendix of [16], using a more K-theoretic approach, combined with Theorem 3.8. Unlike the arguments in much of the remainder of the paper, we do not have to assume that our elliptic curve E admits a p-isogeny over the base field F.

To define our false Tate extension, we fix an element α of $F^\times$ and *assume for the rest of this section* that it satisfies the following conditions:-

Hypotheses on α. (i) There exists a finite place v of F such that $\mathrm{ord}_v(\alpha) \neq 0$, and (ii) $\mathrm{ord}_v(\alpha)$ is not divisible by p for all finite places v of F where $\mathrm{ord}_v(\alpha) \neq 0$, (iii) E does not have additive reduction at any place v of F with $\mathrm{ord}_v(\alpha) \neq 0$.

Define

$$F_n = F(\mu_{p^n}, \alpha^{1/p^n}), \qquad F_\infty = \underset{n \geq 1}{\cup} F_n.$$

Let F^{cyc} denote the cyclotomic $\mathbb{Z}_p$-extension of F, and write

$$G = \mathrm{Gal}(F_\infty/F), \qquad H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}}).$$

We also define

$$K = F(\mu_p), \qquad K^{\mathrm{cyc}} = F(\mu_{p^\infty}), \qquad H_K = \mathrm{Gal}(F_\infty/K^{\mathrm{cyc}}).$$

Note that H_K is isomorphic to $\mathbb{Z}_p$, and is the maximal pro-p subgroup of H. We shall also need to consider the extensions of F defined by

$$L_n = F(x_n), \qquad L_\infty = \underset{n \geq 1}{\cup} L_n$$

where $x_n := \alpha^{1/p^n}$ denotes some fixed p^n-th root of α such that $x_{n+1}^p = x_n$ for all $n \geq 1$. It is also covenient to put $L_0 = F$. Our hypotheses on α above imply that the degree $[L_n : F] = p^n$ for all $n \geq 0$. Put

$$\Delta = \mathrm{Gal}(K/F), \qquad e = \#(\Delta).$$

Since e is prime to p, we have the identifications

$$\Delta = \mathrm{Gal}(K^{\mathrm{cyc}}/F^{\mathrm{cyc}}) = \mathrm{Gal}(F_\infty/L_\infty^{\mathrm{cyc}})$$

under the restriction maps. As in §3, we write $X(E/\mathcal{L})$ for the Pontryagin dual of Greenberg's Selmer group, and put $Y(E/\mathcal{L}) := X(E/\mathcal{L})/X(E/\mathcal{L})(p)$.

Put $H_{L_m} = \mathrm{Gal}(F_\infty/L_m^{\mathrm{cyc}})$. We then have the homomorphism

$$h_{L_m} : K_0(\Lambda(H)) \to \mathbb{Z}$$

defined by

$$h_{L_m}([M]) = \sum_{i \geq 0} (-1)^i \, \mathrm{rank}_{\mathbb{Z}_p} H_i(H_{L_m}, M).$$

Proposition 4.1. *Assume M is a finitely generated $\Lambda(H)$-module, and let $(n_\chi(M))$ be the image of the class $[M]$ under the isomorphism* (47). *Then, for all $m \geq 1$, we have*

$$h_{L_m}([M]) = n_{\mathbf{1}}(M) + (p^m - 1)e^{-1} \sum_{\chi \in \hat{\Delta}} n_\chi(M), \tag{64}$$

where $e = \#(\Delta)$.

Proof. We recall that we identify Δ with the subgroup $\mathrm{Gal}(F_\infty/L_\infty^{\mathrm{cyc}})$ of H. We put $R = \mathbb{Z}_p[\Delta]$, and can in this way view R as a subring of $\Lambda(H)$. For each $\chi \in \hat{\Delta}$, let $\mathbb{Z}_p(\chi)$ denote $\mathbb{Z}_p$ with the action of Δ given by χ. Then $\Lambda(H) \otimes_R \mathbb{Z}_p(\chi)$ maps under the isomorphism (50) to the vector with component 1 at χ and 0 elsewhere (in other words, in terms of the discussion after (52), we can take $P_\chi = \Lambda(H)\otimes_R\mathbb{Z}_p(\chi)$). Since $\Lambda(H)\otimes_R\mathbb{Z}_p(\chi)$ is a projective $\Lambda(H_{L_m})$-module, we have $H_i(H_{L_m}, \Lambda(H)\otimes_R\mathbb{Z}_p(\chi)) = 0$ for all $i \geq 1$. Hence, to prove the proposition, it suffices to show that $H_0(H_{L_m}, \Lambda(H) \otimes_R \mathbb{Z}_p(\chi))$ has $\mathbb{Z}_p$-rank equal to $(p^m - 1)e^{-1}$ or $1 + (p^m - 1)e^{-1}$, according as $\chi \neq \mathbf{1}$ or $\chi = \mathbf{1}$ (cf. (53)).

We first observe that, by the associativity of the tensor product, we have

$$H_0(H_{L_m}, \Lambda(H) \otimes_R \mathbb{Z}_p(\chi)) = U_m \otimes_R \mathbb{Z}_p(\chi),$$

where U_m is the induced module $\mathbb{Z}_p \otimes_{\Lambda(H_{L_m})} \Lambda(H)$. But U_m is the free $\mathbb{Z}_p$-module on the set of right cosets $H_{L_m} \setminus H$ endowed with the natural right action of $\Delta = \mathrm{Gal}(F_\infty/L_\infty^{\mathrm{cyc}})$. There is a bijection from $H_{L_m} \setminus H$ to μ_{p^m} defined by mapping $H_{L_m}\sigma$ to $\sigma(x_m)/x_m$, where $x_m = \alpha^{1/p^m}$. Moreover, this is a bijection of sets with a right Δ-action provided we let Δ act on μ_{p^m} via the inverse of its usual action. It is therefore plain that every orbit of Δ acting on $H_{L_m} \setminus H$, apart from the singleton $\{H_{L_m}\}$, has $(p-1)e^{-1}$ elements. For each orbit Z of Δ acting on $H_{L_m} \setminus H$, define

$$\Phi_Z = (\bigoplus_{\sigma\in Z} \mathbb{Z}_p\sigma) \otimes_R \mathbb{Z}_p(\chi)$$

so that $U_m \otimes_R \mathbb{Z}_p(\chi)$ is the direct sum of the Φ_Z for Z varying over all the orbits. If Z has one element, it is clear that $\Phi_Z = \mathbb{Z}_p$ if $\chi = 1$ and $\Phi_Z = 0$ otherwise. If Z has more than one element, then the above remarks show that $\Phi_Z = W \otimes_R \mathbb{Z}_p(\chi)$, where W is a free R-module of rank 1, and so it is plain that Φ_Z is a free $\mathbb{Z}_p$-module of rank 1. This completes the proof. □

We remark that F_∞/F is an admissible p-adic Lie extension as defined in the previous section, and it is well-known that it satisfies Hypotheses H1 and H2 (see [26]). We suppose for the rest of this section that Hypotheses A1 and A2 are valid for E over F_∞. It is easy to see (cf. [8, Lemma 5.3]) that Hypotheses A1 and A2 imply that, for each finite extension J of F contained in F_∞, $X(E/J^{\mathrm{cyc}})$ is a $\Lambda(\mathrm{Gal}(J^{\mathrm{cyc}}/J))$-torsion module.

We define

$$\tau = \mathrm{rank}_{\Lambda(H_K)}\, Y(E/F_\infty), \qquad \lambda_m = \mathrm{rank}_{\mathbb{Z}_p}\, Y(E/L_m^{\mathrm{cyc}}). \tag{65}$$

We also recall that $s_{E/L_m} = \mathrm{rank}_{\mathbb{Z}_p} X(E/L_m)$.

Theorem 4.2. *Assume Hypotheses A1 and A2. Then for all integers $m \geq 1$, we have (i) $\lambda_m - \lambda_{m-1} = p^{m-1}(p-1)e^{-1}\tau$; (ii) if $(p-1)e^{-1}$ is odd, then $s_{E/L_m} \equiv s_{E/L_{m-1}} + \tau \mod 2$; (iii) If $(p-1)e^{-1}$ is even, then $s_{E/L_m} \equiv s_{E/L_{m-1}} \mod 2$.*

Proof. We first establish (i). We write Σ for the set of all places v of F^{cyc} which do not divide p and for which $\mathrm{ord}_v(\alpha) \neq 0$. Since $\mathrm{ord}_v(\alpha) \not\equiv 0 \mod p$ by hypothesis, each v in Σ

is totally ramified in $L_m^{\rm cyc}$ for all $m \geq 1$. We write $v(m)$ for the unique prime of $L_m^{\rm cyc}$ lying above v, and $J_{v(m)}$ for the absolute Galois group of $L_m^{\rm cyc}$. We claim that

$$\text{(66)} \qquad \mathrm{rank}_{\mathbb{Z}_p}(T_p(E)^{J_{v(m)}}) \text{ is constant for all } m \geq 1.$$

Note that assuming (66) and applying Lemma 3.1 and Proposition 4.1 to $M = Y(E/F_\infty)$, we conclude from Theorem 3.5 that

$$\text{(67)} \qquad \lambda_m - \lambda_{m-1} = (p^m - p^{m-1})e^{-1}\tau,$$

which is the assertion (i). We now prove (66). Suppose first that E has good reduction at v. Then the action of J_v on $T_p(E)$ is unramified, and hence the image of $J_{v(m)}$ in $\mathrm{Aut}(T_p(E))$ is independent of m, since $v(m)/v$ is totally ramified. Next assume that E has multiplicative reduction at v. Then, writing $I_{v(m)}$ for the inertial subgroup of $J_{v(m)}$, we know that $T_p(E)^{I_{v(m)}}$ has $\mathbb{Z}_p$ rank 1 and is independent of m. As the action of $J_{v(m)}$ is unramified, and $v(m)/v$ is totally ramified, it follows again that $T_p(E)^{J_{v(m)}}$ is independent of m. The proof of the theorem is now complete since assertions (ii) and (iii) follow by combining assertion (i) with Theorem 3.8 for the trivial Artin representation of G. □

Corollary 4.3. *Assume Hypotheses A1 and A2, and that both $(p-1)e^{-1}$ and τ are odd. Then, for all $m = 1, 2, \cdots$, we have*

$$\text{(68)} \qquad s_{E/L_m} \geq m + s_{E/F}, \qquad s_{E/F_m} \geq p^m - 1 + s_{E/K}.$$

The proof relies on the following delicate group theoretic lemma.

Lemma 4.4. *For all $n \geq 1$, the group $\mathrm{Gal}(F_n/F)$ has precisely one $\mathbb{Q}_p$-irreducible representation, which does not factor through $\mathrm{Gal}(F_{n-1}(\mu_{p^n})/F)$, where $F_0 = F$. The degree of this representation is $\phi(p^n)$.*

Proof. Put $K_n = F(\mu_{p^n})$, and let $A_n = \mathrm{Gal}(F_n/K_n)$. Since $H^1(\mathrm{Gal}(K_n/F), \mu_{p^n}) = 0$, Kummer theory and our hypotheses on α show that A_n is cyclic of order p^n, and that the natural action of $\mathrm{Gal}(K_n/F)$ on A_n via inner automorphisms is given by the character giving the action of $\mathrm{Gal}(K_n/F)$ on μ_{p^n}. It follows that $L_n \cap K_n = F$, and that $\mathrm{Gal}(F_n/F)$ is a semi-direct product of $\mathrm{Gal}(F_n/L_n)$ and A_n. Using the arguments of [40, §8.2]. one can then easily deduce the following explicit description of the set of all $\bar{\mathbb{Q}}_p$-irreducible representations of $\mathrm{Gal}(F_n/F)$, which do not factor through $\mathrm{Gal}(F'_{n-1}/F)$, where $F'_{n-1} = F_{n-1}(\mu_{p^n})$. Let $\mathcal{X}_n$ be the subset of $\mathrm{Hom}\,(A_n, \mu_{p^n})$ consisting of all characters of exact order p^n, and write $\mathcal{M}_n$ for the set of $\bar{\mathbb{Q}}_p$-representations of $\mathrm{Gal}(F_n/F)$ obtained from $\mathcal{X}_n$ by induction. It is shown in [40, Proposition 2.5] that (i) the $\phi(p^n)$ representations in $\mathcal{M}_n$ are all irreducible, (ii) there are precisely $\phi(p^n)/[K_n : F]$ non-isomorphic representations amongst them, and (iii) every irreducible $\bar{\mathbb{Q}}_p$-representation of $\mathrm{Gal}(F_n/F)$, which does not factor through $\mathrm{Gal}(F'_{n-1}/F)$, is in $\mathcal{M}_n$. Put $\Delta_n = \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)$, which we can identify with $\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$. Let D_n be the subgroup of Δ_n corresponding to $\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}(\mu_{p^n}) \cap F)$, and let Φ_n be the fixed field of D_n. Now the representations in

$\mathcal{X}_n$ can be realized over $\mathbb{Q}_p(\mu_{p^n})$, and so the same is true for the representations in $\mathcal{M}_n$. In fact, since Kummer theory shows that the conjugation action of $\mathrm{Gal}(F_n/L_n)$ on A_n is given by the cyclotomic character, it follows from the proof of Proposition 25 of [40] that each representation in $\mathcal{M}_n$ can be realized over the field Φ_n. Also, Δ_n acts transitively on $\mathcal{M}_n$ because it does on $\mathcal{X}_n$. As $\mathcal{M}_n$ contains precisely $\phi(p^n)/[K_n : F]$ non-isomorphic irreducible $\bar{\mathbb{Q}}_p$-representations, and $[\Phi_n : \mathbb{Q}_p] = \phi(p^n)/[K_n : F]$, we conclude that, on taking the direct sum of one representation from each isomorphism class in $\mathcal{M}_n$, we obtain an irreducible $\mathbb{Q}_p$-representation of $\mathrm{Gal}(F_n/F)$ of degree $\phi(p^n)$, which we denote by V_n in the rest of this section. Moreover, our arguments show that there is no other irreducible $\mathbb{Q}_p$-representation which does not factor through $\mathrm{Gal}(F_{n-1}(\mu_{p^n})/F)$. This completes the proof. □

We now prove the corollary. The first assertion of the corollary is an immediate consequence of Theorem 4.2 (ii). To prove the second assertion, we define

$$U = X(E/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, \qquad W_n = X(E/F_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Thus U and W_n are finite dimensional $\mathbb{Q}_p$-representations of $\mathrm{Gal}(F_n/F)$. As above, let V_n be the $\mathbb{Q}_p$-irreducible representation of $\mathrm{Gal}(F_n/F)$, whose existence is proven in Lemma 4.4. We shall prove by induction on n, that

$$W_n \supset U \oplus V_1 \oplus \cdots \oplus V_n \qquad (n \geq 1) \tag{69}$$

as $\mathrm{Gal}(F_n/F)$-representations. Since V_n has dimension $p^{n-1}(p-1)$, this will clearly prove the second assertion of the corollary.

We shall use the following general observation. Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be finite extensions of F such that $\mathcal{L}_2$ is Galois over $\mathcal{L}_1$ with Galois group Θ. Then, as $\mathbb{Q}_p$-representations of Δ, we have isomorphisms

$$(X(E/\mathcal{L}_2) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{\Theta} = (X(E/\mathcal{L}_2) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)_{\Theta} = X(E/\mathcal{L}_1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p. \tag{70}$$

The first equality is clear because the action of Θ on the finite dimensional $\mathbb{Q}_p$-vector space $X(E/\mathcal{L}_2) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is semisimple. The second equality is induced by the dual of the restriction map on cohomology. We first establish (69) for $n = 1$. We cannot have

$$W_1^{\mathrm{Gal}(F_1/K)} = W_1,$$

as $\mathbb{Q}_p$-representations of $\mathrm{Gal}(F_1/F)$. Indeed, if this were the case, then on taking invariants under $\mathrm{Gal}(F_1/L_1) \simeq \mathrm{Gal}(K/F)$, it would follow that

$$X(E/L_1) \otimes \mathbb{Q}_p = X(E/F) \otimes \mathbb{Q}_p.$$

This contradicts the first assertion of (68) for $n = 1$. Thus V_1 must occur in W_1 and also, by semisimplicity U is a direct summand of W_1 as a $\mathrm{Gal}(F_1/F)$-representation. This proves (69) for $n = 1$. Suppose now by induction that it is true for $n - 1$ with $n \geq 2$, and put $F'_{n-1} = F_{n-1}(\mu_{p^n})$. Then we cannot have

$$W_n^{\mathrm{Gal}(F_n/F'_{n-1})} = W_n$$

as $\mathbb{Q}_p$-representations of $\mathrm{Gal}(F_n/F)$. Indeed, if this were the case, then, on taking invariants under $\mathrm{Gal}(F_n/L_n) \simeq \mathrm{Gal}(F'_{n-1}/L_{n-1})$, it would follow that

$$X(E/L_n) \otimes \mathbb{Q}_p = X(E/L_{n-1}) \otimes \mathbb{Q}_p.$$

This again contradicts the first assertion of (68). Hence V_n must occur in W_n, and the inductive proof of the corollary is complete. □

We remark that T. Dokchitser and V. Dokchitser [18, Proposition 4.13] have established Corollary 4.3 in much greater generality than we have here. In particular, their method also applies when E has potential supersingular reduction at primes above p.

Proposition 4.5. *Assume Hypotheses A1 and A2. Then the parity of $\tau = \Lambda(H_K)$-rank of $Y(E/F_\infty)$ is given by*

$$\tau \equiv s_{E/K} + \mathfrak{s}_{E/K} \mod 2,$$

where $\mathfrak{s}_{E/K}$ is the number of primes v of K such that $\mathrm{ord}_v(\alpha) > 0$ and E has split multiplicative reduction at v.

Proof. Since $H_1(H_K, Y(E/F_\infty))$ is finite (see [8, Lemma 5.3]), we have

$$\tau = \mathrm{rank}_{\mathbb{Z}_p}(Y(E/F_\infty))_{H_K}.$$

By Theorem 3.5, we conclude that

$$\tau = \mathrm{rank}_{\mathbb{Z}_p}(Y(E/K^{\mathrm{cyc}})) + \sum_v \mathrm{rank}_{\mathbb{Z}_p} T_p(E)^{J_v},$$

where v runs over all places of K^{cyc}, which do not divide p, and for which $\mathrm{ord}_v(\alpha) \neq 0$. Again, J_v denotes the absolute Galois group of K_v^{cyc}. First, note that the number of places of K^{cyc} above any finite prime of K must be odd because K^{cyc}/K is a pro-p extension. Similarly, if u is any prime of K where E has multiplicative reduction, then E has split multiplicative reduction at each prime of K^{cyc} above u, if and only if it has split multiplicative reduction at u. We now proceed to show that $\mathrm{rank}_{\mathbb{Z}_p} T_p(E)^{J_v}$ is odd if and only if E has split multiplicative reduction at v.

Since K contains μ_p, the action of J_v on $\mathbb{Z}_p(1)$ is trivial. Suppose first that $\mathrm{ord}_v(j(E)) < 0$. By Lemma 3.7, we conclude that the $\mathbb{Z}_p$-rank of $H^0(J_v, T_p(E))$ is the multiplicity of χ_v occurring in the trivial representation of J_v, i.e. this $\mathbb{Z}_p$-rank is 0 or 1 according as E does or does not have split multiplicative reduction at v. Next assume that $\mathrm{ord}_v(j(E)) \geq 0$. Then the image of J_v in $\mathrm{Aut}(V_p(E))$ is finite. Hence the restriction of the Weil pairing

$$H^0(J_v, V_p(E)) \times H^0(J_v, V_p(E)) \longrightarrow \mathbb{Q}_p(1)$$

gives a non-degenerate pairing. This shows that $H^0(J_v, V_p(E))$ is endowed with a non-degenerate alternating bilinear form, and hence has even dimension.

Finally, we note that Theorem 3.8 shows that

$$\mathrm{rank}_{\mathbb{Z}_p}(Y(E/K^{\mathrm{cyc}})) \equiv s_{E/K} \mod 2.$$

This completes the proof of the proposition. □

We next establish an analogue of Theorem A.32 of the Appendix of [16]. For each character χ of $\mathrm{Gal}(F_n/L_n)$ of exact order p^n, write $\rho_{n,\chi}$ for the $\bar{\mathbb{Q}}_p$-representation obtained by inducing χ to $\mathrm{Gal}(F_n/F)$. When $e = [F : K]$ is odd, $\mathrm{Gal}(F_n/L_n)$ has no non-trivial irreducible self-dual representation. When $e = [F : K]$ is even, the irreducible self-dual representations of $\mathrm{Gal}(F_n/F)$ of dimension > 1 are given by the $\rho_{k,\chi}$ for $1 \leq k \leq n$, and all possible χ. Moreover, by the formula of V. Dokchitser given in the proof of the following theorem, the value of $w(E, \rho_{n,\chi})$ is independent of n and χ.

Theorem 4.6. *Assume Hypotheses A1 and A2, and that (i) $(p-1)/e$ is odd, and (ii) $w(E/K) = (-1)^{s_{E/K}}$. Then $Y(E/F_\infty)$ has odd $\Lambda(H_K)$-rank if and only if the root numbers $w(E, \rho_{n,\chi}) = -1$ for all $n \geq 1$ and all characters χ.*

Proof. Since $(p-1)/e$ is odd, the extension K/F is cyclic of even degree, and hence contains a unique quadratic extension J of F. Let v be any prime of F which does not divide p, and write R_v for the fixed field of the decomposition group of v for K/F. Thus the number n_v of primes of K above v is even if and only if $J \subset R_v$. In other words, n_v is even if and only if v splits in J. Let S be the set of primes v of F with $\mathrm{ord}_v(\alpha) > 0$ and E having multiplicative reduction at v (note that Hypothesis A1 shows that S does not contain any prime above p). Let S_1 be the subset of S consisting of all primes v in S such that E has split multiplicative reduction at all places of K above v. Thus, recalling that E does not have additive reduction at any prime which divides α, we have $\mathfrak{s}_{E/K} = \sum_{v \in S_1} n_v$. If v lies in S and is inert in J, then E certainly has split multiplicative reduction at all primes of K above v. Thus, writing S_2 for the set of all v in S, which are inert in J, we have $S_2 \subset S_1$. Moreover, n_v is even for for $v \in S \setminus S_2$. Hence we have

$$\mathfrak{s}_{E/K} \equiv \sum_{v \in S_2} 1 \mod 2,$$

and so by Proposition 4.5,

$$\tau \equiv s_{E/K} + \sum_{v \in S_2} 1 \mod 2. \tag{71}$$

On the other hand, we have the following explicit formula for the root numbers $w(E, \rho_{n,\chi})$, which is valid under our assumption that $(p-1)/e$ is odd (we are grateful to V. Dokchitser for kindly informing us of this result). For each place v of F, let q_v denote the cardinality of the residue field of v. Also, write $\left(\frac{-}{p}\right)$ for the Legendre symbol of p. Then

$$w(E, \rho_{n,\chi}) = w(E/K)\prod_{v\in S}\left(\frac{q_v}{p}\right). \tag{72}$$

Let J' denote the unique quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\mu_p)$. Since $(p-1)/e$ is odd, we have that $J = FJ'$, and the restriction map gives an isomorphism from $\mathrm{Gal}(J/F)$ onto $\mathrm{Gal}(J'/\mathbb{Q})$. For v in S, let $(v, J/F)$ be its Artin symbol for the quadratic extension J/F and note that the restriction of $(v, J/F)$ to J' is the Artin symbol of the norm $N_{F/\mathbb{Q}}(v)$ for the extension $J'/\mathbb{Q}$. Hence $(v, J/F)$ is the non-trivial element of $\mathrm{Gal}(J/F)$ if and only if $\left(\frac{q_v}{p}\right) = -1$. Comparing (71) and (72), and recalling our hypothesis that $w(E/K) = (-1)^{s_{E/K}}$, the proof of the theorem is complete. □

We next discuss the case when $Y(E/F_\infty)$ has $\Lambda(H_K)$-rank 1. The results in this case are striking because Iwasawa theory enables us to prove that the lower bounds given in Corollary 4.3 are exact for all $n \geq 1$. If v is a prime of F where E has good reduction, let $\tilde{E}_v$ denote the reduction of E modulo v. We also write l_v for the residue field of any prime of K above v. Consider the following sets of primes v of F:-

$$P_1 = \{v \mid v \nmid p \text{ such that } E \text{ has good reduction at } v \text{ and } \tilde{E}_v(l_v)(p) \neq 0.\}$$

$$P_2 = \{v \mid E \text{ has split multiplicative reduction at all primes } w \text{ of } K \text{ above } v.\}$$

Proposition 4.7. *Assume Hypotheses A1 and A2. A necessary condition that $Y(E/F_\infty)$ has $\Lambda(H_K)$-rank 1 is that $\mathrm{ord}_v(\alpha) = 0$ for all v in P_1. This condition is also sufficient if, in addition, we assume that either (i) $Y(E/K^{\mathrm{cyc}})$ has $\mathbb{Z}_p$-rank zero and $\mathrm{ord}_v(\alpha) > 0$ for precisely one prime v in P_2 which is inert in K^{cyc} or, (ii) $Y(E/K^{\mathrm{cyc}})$ has $\mathbb{Z}_p$-rank 1 and $\mathrm{ord}_v(\alpha) = 0$ for all primes v in P_2.*

Proof. The proof, which we omit, is entirely parallel to that of Proposition A.38 in [16, Appendix]. □

Theorem 4.8. *Assume Hypotheses A1, A2 and that $(p-1)/e$ is odd. Further assume that $Y(E/F_\infty)$ has $\Lambda(H_K)$-rank 1. Then for all $n \geq 1$, we have*

$$s_{E/L_n} = n + s_{E/F}, \quad s_{E/F_n} = p^n - 1 + s_{E/K}. \tag{73}$$

Proof. We first establish the theorem for the Galois extensions F_n of F. Put $M = X(E/F_\infty)$ and $H_n = \mathrm{Gal}(F_\infty/F_n^{\mathrm{cyc}})$. Since $H_1(H_n, M) = 0$ and $Y(E/F_\infty)$ has $\Lambda(H_K)$-rank 1, it follows easily that

$$\mathrm{rank}_{\mathbb{Z}_p} H_0(H_n, M) = p^n.$$

On the other hand, a standard analysis of the fundamental diagram (see [26]) shows that

$$\mathrm{rank}_{\mathbb{Z}_p} X(E/F_n^{\mathrm{cyc}}) = \mathrm{rank}_{\mathbb{Z}_p} H_0(H_n, M) - \delta_n$$

where δ_n denotes the number of primes v of F_n^{cyc} dividing α and such that E has split multiplicative reduction at v. It is clear from Proposition 4.7 that $\delta_n = 0$ or 1, according as $X(E/K^{\mathrm{cyc}})$ has $\mathbb{Z}_p$-rank 1 or 0. Hence $\delta_n = 1 - s_{E/K}$ for all $n \geq 1$, and thus

$$\mathrm{rank}_{\mathbb{Z}_p} X(E/F_n^{\mathrm{cyc}}) = p^n - 1 + s_{E/K} \quad (n \geq 1). \tag{74}$$

But the restriction map from $S(E/F_n)$ to $S(E/F_n^{\mathrm{cyc}})$ has finite kernel, whence it follows on combining (68) and (74) that

$$s_{E/F_n} = p^n - 1 + s_{E/K} \quad (n \geq 1), \tag{75}$$

as required.

We now consider the non-Galois extensions L_n of $\mathbb{Q}$. Combining (69) with (75), we conclude that

$$X(E/F_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = U \oplus V_1 \oplus \cdots \oplus V_n \tag{76}$$

as $\mathbb{Q}_p$-representations of $\mathrm{Gal}(F_n/F)$. Hence

$$X(E/L_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = (U \oplus V_1 \oplus \cdots \oplus V_n)^{\mathrm{Gal}(F_n/L_n)}.$$

On the other hand, the following results from group theory are readily verified by induction on $n = 0, 1, \cdots$. Put

$$R_n = \mathbb{Q}_p[\mathrm{Gal}(F_n/F)] \otimes_{\mathbb{Q}_p[\mathrm{Gal}(F_n/L_n)]} \mathbb{Q}_p,$$

where it is understood that $\mathrm{Gal}(F_n/L_n)$ acts trivially on $\mathbb{Q}_p$ on the right hand side of this tensor product. Then

$$R_n = \mathbb{Q}_p \oplus V_1 \oplus \cdots V_n,$$

and, by Frobenius reciprocity,

$$\dim_{\mathbb{Q}_p}(R_n^{\mathrm{Gal}(F_n/L_n)}) = n + 1.$$

It follows that

$$\dim_{\mathbb{Q}_p} V_i^{\mathrm{Gal}(F_n/L_n)} = 1 \quad (1 \leq 1 \leq n). \tag{77}$$

Since

$$U^{\mathrm{Gal}(F_n/L_n)} = X(E/F) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

we conclude from (76) and (77) that

$$s_{E/L_n} = n + s_{E/F} \quad (n \geq 1).$$

This completes the proof of (73). □

Remark 4.9. Under the same hypotheses of Theorem 4.8, the proof given above shows that for all $n \geq 1$, a characteristic power series for $X(E/F_n^{\mathrm{cyc}})$ is

$$p^{a_n} T^{p^n - 1 + s_{E/K}} \qquad (n \geq 1),$$

for some integer $a_n \geq 0$. Hence this module is semisimple at $T = 0$, in the sense that the $\mathbb{Z}_p$-rank of $H_0(\mathrm{Gal}(F_n^{\mathrm{cyc}}/F_n), X(E/F_n^{\mathrm{cyc}}))$ is also equal to $p^n - 1 + s_{E/K}$, which is the multiplicity of the zero at $T = 0$ of this characteristic power series. Here, as usual, we have identified $\Lambda(\mathrm{Gal}(F_n^{\mathrm{cyc}}/F_n))$ with $\mathbb{Z}_p[[T]]$ by mapping a topological generator to $1 + T$. In particular, this semisimplicity implies that the canonical p-adic height pairing on $X(E/F_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is non-degenerate for all $n \geq 1$.

Since the extension $F_\infty/K^{\mathrm{cyc}}$ is pro-p, the hypothesis that $X(E/K^{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module automatically implies that $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$.

Proposition 4.10. *Assume (i) Hypothesis A1, (ii) $X(E/K^{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module, (iii) $(p-1)/e$ is odd, (iv) $E(K)(p) = 0$, and (v) $X(E/F_\infty)$ has $\Lambda(H_K)$-rank 1. Then, for all $n \geq 1$, $S(E/F_n)$ is divisible.*

Proof. Let j_n denote the restriction map from $S(E/F_n)$ to $S(E/F_n^{cyc})$. Now the proof of Theorem 4.8 shows that j_n maps the divisible subgroup $S(E/F_n)$ onto the divisible subgroup of $S(E/F_n^{cyc})$. By the theorem of Hachimori and Matsuno [25], our hypothesis that $X(E/K^{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module implies that the same is true for $X(E/F_n^{\mathrm{cyc}})$ for all $n \geq 1$. Moreover, Matsuno's theorem [29] shows that $X(E/F_n^{\mathrm{cyc}})$ is in fact a free $\mathbb{Z}_p$-module, or equivalently that $S(E/F_n^{\mathrm{cyc}})$ is divisible, for all $n \geq 1$. . But $E(F_n)(p) = 0$ since $E(K)(p) = 0$ and F_n/K is a p-extension, whence it follows that j_n is injective. Combining these assertions, it follows easily that $S(E/F_n)$ is divisible for all $n \geq 1$, completing the proof. □

We next show that our arguments yield a simple proof of the ρ-parity conjecture for all absolutely irreducible self-dual Artin representations ρ of G having dimension > 1. Recall from 3.3 that, for any irreducible Artin representation ρ of G, $s_{E,\rho}$ denotes the number of copies of ρ occurring in $X(E/\mathcal{L}) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$, where $\mathcal{L}$ is any finite Galois extension of $\mathbb{Q}$ such that ρ factors through $\mathrm{Gal}(\mathcal{L}/\mathbb{Q})$.

Theorem 4.11. *Assume that (i) Hypotheses A1 and A2 are valid, (ii) $(p-1)e^{-1}$ is odd, and (iii) $w(E/K) = (-1)^{s_{E/K}}$. Then, for all absolutely irreducible self-dual Artin representations ρ of G with dimension > 1, we have $w(E, \rho) = (-1)^{s_{E,\rho}}$.*

Proof. As remarked earlier, ρ must be equal to one of the representations $\rho_{n,\chi}$, where n is some positive integer, and χ is some character of $\mathrm{Gal}(F_n/L_n)$ of exact order p^n. Let V_n be the $\mathbb{Q}_p$-irreducible representation of $\mathrm{Gal}(F_n/F)$ whose existence is proven in Lemma 4.4. Since $V_n \otimes_{\mathbb{Q}_p} \bar{\mathbb{Q}}_p$ is the direct sum of all conjugates of $\rho_{n,\chi}$ over $\mathbb{Q}_p$, it is clear that $s_{E,\rho_{n,\chi}}$ is equal to the number of copies of V_n occurring in $X(E/F_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, and we denote this number by a_n. In view of Lemma 4.4, we must have

$$X(E/F_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = (X(E/F'_{n-1}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \oplus V_n^{a_n},$$

where, as before, $F'_{n-1} = F_{n-1}(\mu_{p^n})$. Now take the subspaces fixed by $\mathrm{Gal}(F_n/L_n)$ on both sides of this equality. Recalling that the restriction of $\mathrm{Gal}(F_n/L_n)$ to F'_{n-1} is equal to $\mathrm{Gal}(F'_{n-1}/L_{n-1})$, we conclude that

$$X(E/L_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = (X(E/L_{n-1}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \oplus Z_n^{a_n},$$

where Z_n is the subspace of all elements of V_n which are fixed by $\mathrm{Gal}(F_n/L_n)$. But, as was shown in the proof of Theorem 4.8, Z_n has $\mathbb{Q}_p$-dimension equal to 1. Thus we deduce that

$$s_{E/L_n} = s_{E/L_{n-1}} + a_n,$$

whence, by (ii) of Theorem 4.2, we conclude that $\tau \equiv a_n$ modulo 2, where, as before, τ denotes the $\Lambda(H_K)$-rank of $Y(E/F_\infty)$. Thus the assertion of the theorem is now clear from Theorem 4.6. This completes the proof. □

In the next theorem, we assume for simplicity that the base field F is equal to $\mathbb{Q}$. We write Ψ for the group of all 1- dimensional characters of $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$.

Theorem 4.12. *Assume that $F = \mathbb{Q}$ and that Hypotheses A1 and A2 are valid. Let $\tau = \Lambda(H_K)$-rank of $Y(E/F_\infty)$. Then for all absolutely irreducible Artin representations ρ of G, we have*

$$\sum_{\psi \in \Psi} s_{E,\rho\psi} \leq \tau\, p/(p-1).$$

Before giving the proof of the theorem, we make the following remark. For each absolutely irreducible Artin representation ρ of G, let $L(E, \rho, s)$ be the complex L-function of E twisted by ρ. Since $E/\mathbb{Q}$ is now known to be modular, it follows from automorphic base change that $L(E, \rho, s)$ is entire. A refinement of the conjecture of Birch and Swinnerton-Dyer then asserts that $s_{E,\rho}$ should be the order of the zero of $L(E, \rho, s)$ at $s = 1$. Hence our theorem suggests that, for every absolutely irreducible Artin representation ρ of G, we have

$$\sum_{\psi \in \Psi} \mathrm{ord}_{s=1} L(E, \rho\psi, s) \leq \tau\, p/(p-1).$$

This uniform upper bound, which is independent of ρ, seems surprising from the point of view of complex L-functions.

We now prove Theorem 4.12. Since $F = \mathbb{Q}$, write ρ_n $(n \geq 1)$, for the representation of $\mathrm{Gal}(F_n/\mathbb{Q})$ which is induced by any character of exact order p^n of $\mathrm{Gal}(F_n/K_n)$ (these representations do not depend on the choice of such a character). Let ρ_0 denote the trivial one dimensional representation of G and put $F_0 = \mathbb{Q}(\mu_p)$. Since $F = \mathbb{Q}$, all absolutely irreducible characters of G are of the form $\rho_n\psi$ for some ψ in Ψ and some integer $n \geq 0$. Moreover, the dimension of $\rho_n\psi$ is equal to $\phi(p^n)$. Recall that $\lambda_n = \mathrm{rank}_{\mathbb{Z}_p}(Y(E/F_n^{\mathrm{cyc}}))$. Since all the representations $\rho_n\psi$ factor through some finite layer of the $\mathbb{Z}_p$-extension F_n^{cyc}/F_n, we have

$$\sum_{\psi \in \Psi} \phi(p^n) s_{E,\rho_n\psi} \;\leq\; \lambda_n \;\; (n \geq 0). \tag{78}$$

On the other hand, let $H_n = \mathrm{Gal}(F_\infty/F_n^{\mathrm{cyc}})$. By Theorem 3.5, we have

$$\lambda_n \;\leq\; \mathrm{rank}_{\mathbb{Z}_p} H_0(H_n, Y(E/F_\infty)) \;=\; \mathrm{rank}_{\Lambda(H_n)}(Y(E/F_\infty)),$$

the last equation being true because $H_1(H_n, Y(E/F_\infty))$ is finite. But since H_n has index p^n in H, it follows that

$$\mathrm{rank}_{\Lambda(H_n)}(Y(E/F_\infty)) \;=\; p^n\,\tau.$$

Thus $\lambda_n \leq p^n\,\tau$ and the assertion of the theorem now follows from the inequality (78). This completes the proof of the theorem. □

We now illustrate the results of this section by the elliptic curve

$$E = X_1(11):\; y^2 + y = x^3 - x^2$$

with $F = \mathbb{Q}$. Assume that p is a prime $\neq 2$, 11, and that α is a p-power free integer > 1. Then $w(E/K) = \left(\frac{p}{11}\right)$, and Dokchitser's formula (72) shows that $w(E, \rho_n) = -1$ for $n \geq 1$ if and only if either

$$(79) \qquad 11 \mid \alpha \text{ and } p \equiv 3 \mod 4, \text{ or } (11, \alpha) = 1 \text{ and } \left(\frac{p}{11}\right) = -1.$$

Suppose now that p is an odd prime of good ordinary reduction for $E = X_1(11)$ satisfying (79). Then, by Corollary 4.3 and Theorem 4.6,

$$s_{E/L_n} \geq n, \;\; s_{E/F_n} \geq p^n - 1 + s_{E/K} \;\; (n \geq 1),$$

provided $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$. The work of [27] shows that $X(E/K^{\mathrm{cyc}})$ is a torsion $\Lambda(\mathrm{Gal}(K^{\mathrm{cyc}}/K))$-module for all good ordinary primes $p \neq 2$, and it is very probable that $X(E/K^{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module for all such p. Whenever this last assertion is true, $X(E/F_\infty)$ does indeed belong to $\mathfrak{M}_H(G)$. However, in our present state of knowledge, we can only verify this numerically for small primes p. For example, if $p = 3$, then $X(E/K^{\mathrm{cyc}}) = 0$ by the calculations of [16]. Taking $\alpha = 11$, it follows from Proposition 4.7 that $X(E/F_\infty)$ has $\Lambda(H_K)$-rank 1, and thus Theorem 4.8 shows that in this case

$$s_{E/L_n} = n, \;\; s_{E/F_n} = 3^n - 1 \;\; (n \geq 1).$$

Now take $p = 7$. We are grateful to C. Wuthrich for the numerical computations in this case which show that $X(E/K^{\mathrm{cyc}})$ is a free $\mathbb{Z}_7$-module of rank 1. It may be of interest to record here that Wuthrich found the following point P of infinite order in $E(K)$, where $K = \mathbb{Q}(\mu_7)$ and ζ denotes a primitive 7-th root of unity:-

$$P = (1 + \zeta + \zeta^2 + \zeta^4, -\zeta - \zeta^2 - \zeta^4).$$

It follows that $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$ for all 7-power free $\alpha > 1$, and hence for all such α, we have

$$s_{E/L_n} \geq n, \;\; s_{E/F_n} \geq 7^n \;\; (n \geq 1).$$

By Proposition 4.7, $X(E/F_\infty)$ has $\Lambda(H_K)$-rank 1 if and only if $(\alpha, 11) = 1$ and no prime divisor of α lies in the set P_1, which is defined just before Proposition 4.7. In particular, one verifies easily that 2 and 3 do not belong to P_1, but 5 does. For example, there are two primes v_1 and v_2 of $\mathbb{Q}(\mu_7)$ lying above 2 and the reduction of E modulo 2 has five points in the residue fields of these primes. Hence if we choose the prime divisors of α to be any non-empty subset of $\{2, 3, 7\}$, we conclude that $X(E/F_\infty)$ has $\Lambda(H_K)$-rank 1, and so Theorem 4.8 shows that

$$s_{E/L_n} = n, \;\; s_{E/F_n} = 7^n \;\; (n \geq 1).$$

We remark that it does not seem easy numerically to find a point of infinite order in the field L_1 for any of these choices of α. Note finally that when $p = 5$, $X(E/K^{\mathrm{cyc}}) = 0$ so that $X(E/F_\infty)$ lies in $\mathfrak{M}_H(G)$ for all choices of α. However, Theorem 4.6 shows that $X(E/F_\infty)$ always has even $\Lambda(H_K)$-rank. If $\alpha = 5$, it is known [26] that $X(E/F_\infty) = 0$, and

$$s_{E/L_n} = s_{E/F_n} = 0 \;\; (n \geq 1).$$

If $\alpha = 11$, $X(E/F_\infty)$ has $\Lambda(H_K)$-rank 4, and it is known that $s_{E/L_1} = s_{E/F_1} = 0$, but it is unknown whether $s_{E/F_n} \geq 1$ for some $n \geq 1$.

We end this section by remarking that our methods prove nothing about the rank of the Mordell-Weil groups $E(L_n)$ and $E(F_n)$, since we cannot show that the p-primary part of the Tate-Shafarevich groups of E/L_n and E/F_n are finite. However, in a remarkable piece of work, Darmon and Tian have proven strong results in this direction [14] for the case when $F = \mathbb{Q}$, $X(E/K^{\mathrm{cyc}}) = 0$, and $X(E/F_\infty)$ has $\Lambda(H_K)$-rank 1.

5 Rank calculations in the p-power division case

We now study the arithmetic of E over the p-adic Lie extension of F given by $F_\infty = F(E_{p^\infty})$. Thus $G = \mathrm{Gal}(F_\infty/F)$ is a closed subgroup of $\mathrm{Aut}(T_p(E)) = GL_2(\mathbb{Z}_p)$. For simplicity, we shall assume that $p \geq 5$.

Let Ω denote the intersection of G with the torsion subgroup of the centre $\mathbb{Z}_p^\times$ of $GL_2(\mathbb{Z}_p)$. Fix any pro-p, open normal subgroup G' of G, and define $\mathcal{G}$ to be the subgroup of G generated by Ω and G'. Let F' be the fixed field of G' and $\mathcal{L}$ be the fixed field of $\mathcal{G}$. In addition, let $H' = H \cap G'$. Note that H' is pro-p and has no element of order p, so that $\Lambda(H')$ has a skew-field of fractions and hence one can define the $\Lambda(H')$-rank of any finitely generated $\Lambda(H')$-module. Also, we write $\hat{\Omega} = \mathrm{Hom}\,(\Omega, \mathbb{Z}_p^\times)$. If M is any finitely generated $\Lambda(G)$-module, then we have the decomposition

$$M = \underset{\alpha \in \hat{\Omega}}{\oplus} M^{(\alpha)},$$

where $M^{(\alpha)}$ is the $\Lambda(G)$-submodule consisting of all m in M such that $\sigma m = \alpha(\sigma) m$ for all σ in Ω.

We recall that $X(E/F_\infty)$ denotes the dual of the Selmer group of E over F_∞ and that

$$Y(E/F_\infty) = X(E/F_\infty)/X(E/F_\infty)(p).$$

By Hypothesis A2, $Y(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module. For each α in $\hat{\Omega}$, we define $\tau(\alpha)$ to be the $\Lambda(H')$-rank of $Y(E/F_\infty)^{(\alpha)}$. Since p is odd, the parity of $\tau(\alpha)$ does not depend on the choice of G'. For each extension K of F, we write $P_s(K)$ for the set of primes of K where E/K has split multiplicative reduction. Finally, as before $w(E/K)$ denotes the sign in the functional equation of $L(E/K,s)$, and we recall that

$$w(E/K) = \prod_v w_v(E/K)$$

where $w_v(E/K)$ is the local root number of E/K_v.

Theorem 5.1. *Assume that $p \geq 5$ and that Hypotheses A1 and A2 are valid. Then $\tau(\alpha) = \tau(\alpha^{-1})$ for all α in $\hat{\Omega}$. Moreover, if $\alpha = \alpha^{-1}$, we have*

$$\tau(\alpha) \equiv r(E/\mathcal{L}) + \#(P_s(\mathcal{L})) \mod 2, \tag{80}$$

where $\mathcal{L}$, as above, is the fixed field of $\mathcal{G}$, and $r(E/\mathcal{L})$ mod 2 is defined by $w(E/\mathcal{L}) = (-1)^{r(E/\mathcal{L})}$.

We now give a series of preparatory lemmas needed for the proof of Theorem 5.1. Let $H_{\mathcal{L}} = \mathrm{Gal}(F_\infty/\mathcal{L}^{\mathrm{cyc}})$. Viewing each α in $\hat{\Omega}$ as an Artin character of $\mathrm{Gal}(F_\infty/\mathcal{L})$, we recall that

$$h_\alpha : K_0(\Lambda(H_{\mathcal{L}})) \to \mathbb{Z},$$

is the homomorphism defined by (52).

Lemma 5.2. *For each $\alpha \in \hat{\Omega}$, we have $\tau(\alpha^{-1}) = h_\alpha([Y(E/F_\infty)])$.*

Proof. If N is any finitely generated $\Lambda(H_{\mathcal{L}})$-module, recalling that the order of Ω is prime to p, we see easily that for all $i \geq 0$,

$$H_i(H_{\mathcal{L}}, \mathrm{tw}_\alpha(N)) = H_i(H', N)^{(\alpha^{-1})} = H_i(H', N^{(\alpha^{-1})})$$

where we have identified Ω with $\mathrm{Gal}(F'^{\mathrm{cyc}}/\mathcal{L}^{\mathrm{cyc}})$. The assertion of the lemma is now clear since H' is pro-p, using the usual homological formula for ranks. □

For each α in $\hat{\Omega}$, let W_α be a free $\mathbb{Z}_p$-module of rank 1 on which Ω acts via α. We also note that a finite place v of F which does not divide p is infinitely ramified in F_∞ if and only if $\mathrm{ord}_v(j_E) < 0$, where j_E denotes the j-invariant of E. Hence, writing now $P(\mathcal{L}^{\mathrm{cyc}})$ for the set of primes w of $\mathcal{L}^{\mathrm{cyc}}$ with $\mathrm{ord}_w(j_E) < 0$, and defining

$$\lambda_\alpha(E/\mathcal{L}^{\mathrm{cyc}}) = \mathrm{rank}_{\mathbb{Z}_p}(Y(\mathrm{tw}_\alpha(E)/\mathcal{L}^{\mathrm{cyc}})), \tag{81}$$

it follows from Theorem 3.5 and Lemma 3.6 that

$$h_{\alpha^{-1}}(Y(E/F_\infty)) = \lambda_\alpha(E/\mathcal{L}^{\mathrm{cyc}}) + \sum_{u \in P(\mathcal{L}^{\mathrm{cyc}})} \mathrm{rank}_{\mathbb{Z}_p}(T_p(E) \otimes_{\mathbb{Z}_p} W_\alpha)^{H_{\mathcal{L},u}}; \tag{82}$$

here we have fixed an extension of the prime u to F_∞, and put $H_{\mathcal{L},u} = \mathrm{Gal}(F_{\infty,u}/\mathcal{L}_u^{\mathrm{cyc}})$.

For each place u of $\mathcal{L}^{\mathrm{cyc}}$, define

$$b_{\alpha,u} = \mathrm{rank}_{\mathbb{Z}_p}(T_p(E) \otimes W_\alpha)^{H_{\mathcal{L},u}}. \tag{83}$$

Lemma 5.3. *Let u be any place of $\mathcal{L}^{\mathrm{cyc}}$ with $\mathrm{ord}_u(j_E) < 0$ and let α be any element of $\hat{\Omega}$. If $E/\mathcal{L}^{\mathrm{cyc}}$ has split multiplicative reduction at u, then u splits completely in F'^{cyc} and $b_{\alpha,u} = 1$. Suppose next that $E/\mathcal{L}^{\mathrm{cyc}}$ does not have split multiplicative reduction at u. Then Ω has even order and writing θ for the unique element of order 2 in Ω, we have $b_{\alpha,u} = 1$ or $b_{\alpha,u} = 0$, according as $\alpha(\theta) = -1$ or $\alpha(\theta) = 1$.*

Proof. Note first that since G' is pro-p, we must have $\mu_p \subset F'$, and so $F'^{\mathrm{cyc}} = F'(\mu_{p^\infty})$. Also, it is clear that we can identify Ω with the Galois group $\mathrm{Gal}(F'^{\mathrm{cyc}}/\mathcal{L}^{\mathrm{cyc}})$. We write Ω_u for the decomposition group of u in the extension $F'^{\mathrm{cyc}}/\mathcal{L}^{\mathrm{cyc}}$.

Suppose first that E has split multiplicative reduction at u. We claim that we then have $\Omega_u = \{1\}$, or equivalently that u splits completely in F'^{cyc}. Indeed, by the theory of the Tate curve, we have an exact sequence of $H_{\mathcal{L},u}$-modules

$$0 \to \mathbb{Z}_p(1) \to T_p(E) \to \mathbb{Z}_p \to 0.$$

Hence any homothety σ in Ω_u must act trivially on the quotient $\mathbb{Z}_p$ of $T_p(E)$, and so we must have $\sigma = 1$, as claimed. We now apply Lemma 3.7 to compute $b_{\alpha,u}$. Since $\Omega_u = 1$, we conclude immediately that $b_{\alpha,u} = 1$.

Assume next that E does not have split multiplicative reduction at u. Then it is well-known that E achieves split multiplicative reduction over a quadratic extension $\mathcal{K}_u$ of $\mathcal{L}_u$, which must be contained in $F_{\infty,u}$. Therefore $\mathcal{K}_u^{\mathrm{cyc}}$ is a quadratic extension of $\mathcal{L}_u^{\mathrm{cyc}}$, which is contained in $F_u'^{\mathrm{cyc}}$. It follows that Ω_u must have even order, whence the same is also true for Ω. Moreover, by the argument of the previous paragraph, Ω_u then has order 2, and we write $\Omega_u = \{1, \theta\}$. But then, since Ω_u acts on μ_p via the determinant character, Ω_u must fix μ_p. Thus we must have $\mu_p \subset \mathcal{L}_u^{\mathrm{cyc}}$, and so $H_{\mathcal{L},u}$ acts trivially on $\mathbb{Z}_p(1)$. Hence, by Lemma 3.7, we have

$$b_{\alpha,u} = \langle \chi_u, \alpha_u \rangle,$$

which is 1 if $\chi_u = \alpha_u$, or equivalently if $\alpha_u(\theta) = -1$, and is 0 otherwise. This completes the proof of the lemma. □

Lemma 5.4. *There exists an isogeny of degree p for E defined over $\mathcal{L}$. Moreover, $\mathcal{L}$ is totally imaginary.*

Proof. Since G' is pro-p, there exists a 1-dimensional subspace U of E_p on which G' acts trivially. But then it is clear that $\mathcal{G}$ must leave U stable, and so there exists an isogeny defined over $\mathcal{L}$ with kernel precisely U. This proves the first assertion. If there was a real place u of $\mathcal{L}$, the complex conjugation attached to some infinite place of F_∞ lying above u, would have to have determinant -1, because the determinant map on $\mathcal{G}$ coincides with the cyclotomic character, where $\mathcal{G} = \mathrm{Gal}(F_\infty/\mathcal{L})$. But $\mathcal{G}$ has no element of order 2 whose determinant is -1. This completes the proof. □

If J is any quadratic extension of $\mathcal{L}$ and v is any prime of $\mathcal{L}$, we define

$$\delta_v(E/J) = \prod_{v'|v} w_{v'}(E/J), \tag{84}$$

where $w_{v'}(E/J)$ denotes the local root number of E/J at v' (see §2).

Lemma 5.5. *Suppose that there exists a character α of Ω of exact order 2, and let $\mathcal{L}'$ be the quadratic extension of $\mathcal{L}$ defined by α. Then $\delta_v(E/\mathcal{L}') = 1$ for all places v of $\mathcal{L}$, excepting those primes v of $\mathcal{L}$ with $\mathrm{ord}_v(j_E) < 0$ such that $E/\mathcal{L}$ does not have split multiplicative reduction at v, but achieves split multiplicative reduction at a place v' of $\mathcal{L}'$ above v. In this latter case , $\delta_v(E/\mathcal{L}') = -1$.*

Proof. Since E has an isogeny of degree p defined over $\mathcal{L}$, we can use the explicit formulae for the local root numbers given in Proposition 2.8. As these local root numbers are all ± 1, it is clear that $\delta_v(E/\mathcal{L}') = 1$ whenever v splits in $\mathcal{L}'$; in particular, since $\mathcal{L}$ is totally imaginary, this proves the lemma for all archimedean primes of $\mathcal{L}$. Suppose therefore that v does not split in $\mathcal{L}'$, so that the norm of -1 from $\mathcal{L}'$ to $\mathcal{L}$ is 1. It follows by class field theory that $\chi_{C,v'}(-1) = 1$ or $\chi_{C,v',crys}(-1) = 1$, according as v does not or does divide p. Hence it only remains to consider the term $(-1)^{t(v')}$. By Lemma 5.3,E cannot have split multiplicative reduction at v, since otherwise v would split in $\mathcal{L}'$. Hence $(-1)^{t(v')} = -1$ if and only if E achieves split multiplicative reduction over $\mathcal{L}'_{v'}$. This completes the proof of the lemma. □

We now prove Theorem 5.1. The theorem of Greenberg (see [22]), shows that for each $\alpha \in \hat{\Omega}$, the characteristic ideals in $\Lambda(\mathrm{Gal}(\mathcal{L}^{\mathrm{cyc}}/\mathcal{L}))$ of $X(\mathrm{tw}_\alpha(E)/\mathcal{L}^{\mathrm{cyc}})$ and $X(\mathrm{tw}_{\alpha^{-1}}(E)/\mathcal{L}^{\mathrm{cyc}})^\bullet$ are equal. Here, for a finitely generated $\Lambda(\mathrm{Gal}(\mathcal{L}^{\mathrm{cyc}}/\mathcal{L}))$-module M, $M^\bullet$ denotes the same underlying module but with the $\mathrm{Gal}(\mathcal{L}^{\mathrm{cyc}}/\mathcal{L})$ action inverted. In particular, it follows that

$$\lambda_\alpha(E/\mathcal{L}^{\mathrm{cyc}}) = \lambda_{\alpha^{-1}}(E/\mathcal{L}^{\mathrm{cyc}}). \tag{85}$$

Moreover, it is plain from Lemma 5.3 that, for each α in $\hat{\Omega}$, we have $b_{\alpha,u} = b_{\alpha^{-1},u}$. Hence by Lemma 5.2 and (82), it follows that $r(\alpha) = r(\alpha^{-1})$ for all α in $\hat{\Omega}$. Since E has an isogeny of degree p defined over $\mathcal{L}$, the results of §2 prove that $w(E/L) = (-1)^{s_{E/L}}$ for every finite extension L of $\mathcal{L}$. Applying Theorem 3.8 with $\rho = \mathbf{1}$, we obtain

$$s_{E/\mathcal{L}} \equiv \lambda_{\mathbf{1}}(E/\mathcal{L}^{\mathrm{cyc}}) \mod 2. \tag{86}$$

Thus the assertion (80) for $\alpha = \mathbf{1}$ is an immediate consequence of (82),(86) and Lemmas 5.2 and 5.3, noting that $\#(P_s(L))$ is congruent to $\#P_s(L^{\mathrm{cyc}})$ modulo 2. Now assume that α is a character of Ω of exact order 2, and let $\mathcal{L}'$ be the quadratic extension of $\mathcal{L}$ defined by α. Then

$$(87) \qquad \lambda(E/\mathcal{L}'^{\mathrm{cyc}}) = \lambda_{\mathbf{1}}(E/\mathcal{L}^{\mathrm{cyc}}) + \lambda_\alpha(E/\mathcal{L}^{\mathrm{cyc}}),$$

where $\lambda(E/\mathcal{L}'^{\mathrm{cyc}})$ denotes the $\mathbb{Q}_p$-dimension of $X(E/\mathcal{L}'^{\mathrm{cyc}}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. On the other hand, Lemma 5.5 shows that

$$(88) \qquad w(E/\mathcal{L}') = (-1)^{\#(P_{ns}(\mathcal{L}^{\mathrm{cyc}}))},$$

where $P_{ns}(\mathcal{L}^{\mathrm{cyc}})$ denotes the set of places v of $\mathcal{L}^{\mathrm{cyc}}$ satisfying (i) $E/\mathcal{L}^{\mathrm{cyc}}$ does not have split multiplicative reduction at v, and (ii) $E/\mathcal{L}'^{\mathrm{cyc}}$ does have split multiplicative reduction at a prime v' (necessarily unique) of $\mathcal{L}'^{\mathrm{cyc}}$ above v. Further, Theorem 3.8 also shows that

$$s_{E/\mathcal{L}'} \equiv \lambda(E/\mathcal{L}'^{\mathrm{cyc}}) \mod 2.$$

Noting finally that, for this choice of α, we have

$$\#P_{ns}(\mathcal{L}^{\mathrm{cyc}}) + \#(P_s(\mathcal{L}^{\mathrm{cyc}})) = \sum_{u \in P(\mathcal{L}^{\mathrm{cyc}})} b_{\alpha,u},$$

we conclude from Lemma 5.2 and (82) that

$$\tau(\alpha) \equiv \tau(\mathbf{1}) \mod 2.$$

This completes the proof of the theorem. □

Corollary 5.6. *Under the same hypotheses as Theorem 6.1, the $\Lambda(H')$-rank of $Y(E/F_\infty)$ is even when Ω has even order.*

Proof. Let τ denote the $\Lambda(H')$-rank of $Y(E/F_\infty)$, so that $\tau = \sum_{\alpha \in \hat{\Omega}} \tau(\alpha)$. But Theorem 5.1 shows that $\tau(\alpha) = \tau(\alpha^{-1})$, and also that $\tau(\mathbf{1}) \equiv \tau(\alpha)$ mod 2, when $\alpha^2 = \mathbf{1}$, from which the assertion follows. □

It is not always true that $Y(E/F_\infty)$ has even $\Lambda(H')$-rank, as is shown by the following numerical example. Take $F = \mathbb{Q}$, $p = 7$, and E to be the elliptic curve

$$(89) \qquad y^2 + xy = x^3 - x - 1$$

of conductor $N_E = 2.3.7^2$ [11, Chap. 4, §4.3]. Then E achieves good ordinary reduction over $\mathbb{Q}(\mu_7)$ at the unique prime above 7. Moreover, $\mu_7 \subset E_7$, so that $F_\infty = \mathbb{Q}(E_{7^\infty})$ is pro-7 over $\mathbb{Q}(\mu_7)$. Finally, the Selmer group of E over $\mathbb{Q}(\mu_{7^\infty})$ is equal to 0. Moreover, E has split multiplicative reduction at the unique prime of $\mathbb{Q}(\mu_7)$ above 3, and the two primes of $\mathbb{Q}(\mu_7)$ above 2. Taking $F' = \mathbb{Q}(\mu_7)$, we have $H' = \mathrm{Gal}(F_\infty/\mathbb{Q}(\mu_{7^\infty}))$, and it follows easily from the above facts that $X(E/F_\infty)$ is finitely generated over $\Lambda(H')$ and has $\Lambda(H')$-rank equal to 3. We remark that in this example we also have $X(E/F_\infty)(7) = 0$. The corollary of course does not apply in this case because one sees easily that $\Omega = \{1\}$.

Corollary 5.7. *Under the same hypotheses as Theorem 5.1, suppose in addition that $[\mathcal{L}:F]$ is even. Then for each α in $\hat{\Omega}$ with $\alpha = \alpha^{-1}$, we have*

$$\tau(\alpha) \equiv [\mathcal{L}:\mathbb{Q}]/2 \mod 2.$$

Proof. We will show that, under the hypothesis that $[\mathcal{L}:F]$ is even, we have

$$r(E/\mathcal{L}) \equiv [\mathcal{L}:\mathbb{Q}]/2 + \#(P_s(\mathcal{L})) \mod 2, \tag{90}$$

from which the corollary is clear in view of (80). Now

$$(-1)^{r(E/\mathcal{L})} \;=\; w(E/\mathcal{L}) \;=\; \prod_{v|\infty} w_v(E/\mathcal{L}) \prod_{v<\infty} w_v(E/\mathcal{L})$$

where the latter product is taken over all finite places v of $\mathcal{L}$. Since $\mathcal{L}$ is totally imaginary by Lemma 5.4, we have

$$\prod_{v|\infty} w_v(E/\mathcal{L}) = (-1)^{[\mathcal{L}:\mathbb{Q}]/2}.$$

Hence it remains to show that

$$\prod_{v<\infty} w_v(E/\mathcal{L}) \;=\; (-1)^{\#(P_s(\mathcal{L}))}. \tag{91}$$

By Proposition 2.8 (2), (3), it is enough to prove that for each finite place v of F, the product

$$\prod_{v'|v} \chi_{C,v'}(-1) \;=\; 1, \text{ when } v \text{ does not divide } p$$

and

$$\prod_{v'|v} \chi_{C,v',\mathrm{crys}}(-1) \;=\; 1, \text{ when } v \text{ divides } p;$$

here, in both cases, v' runs over all places of $\mathcal{L}$ lying over v. By local class field theory, if v does not divide p, the product

$$\prod_{v'|v} \chi_{C,v'}(-1) \;=\; \chi_{C,v}(-1)^{[\mathcal{L}:F]} \;=\; 1.$$

Similarly, if v divides p, we have

$$\prod_{v'|v} \chi_{C,v',\mathrm{crys}}(-1) \;=\; \chi_{C,v,\mathrm{crys}}(-1)^{[\mathcal{L}:F]} \;=\; 1.$$

This completes the proof. □

6 Parity results for Artin twists

Throughout this section, we assume that $F_\infty = F(E_{p^\infty})$, where E/F is an elliptic curve without complex multiplication. This last assumption on E is imposed because we shall use results of Rohrlich [38] on root numbers, which he only establishes in the more difficult case of elliptic curves without complex multiplication. Moreover, we suppose always that $p \geq 5$ and that E admits an isogeny of degree p, which is defined over F. As always $G = \mathrm{Gal}(F_\infty/F)$ and $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$.

Definition 6.1. The integer u_G is defined to be the order of the image of G under the natural surjection from $GL_2(\mathbb{Z}_p)$ to $PGL_2(\mathbb{F}_p)$.

Rohrlich [38] has shown that there exist irreducible self-dual Artin representations of G of dimension > 1 if and only if u_G is even. Hence we shall assume for the rest of this section that u_G is indeed even. Let $\rho : G \to GL(V_\rho)$ be an irreducible self-dual Artin representation of G, which is realized by the vector space V_ρ over some finite extension of $\mathbb{Q}_p$. Since ρ is self-dual, we can regard its character as being real valued, and by the theory of finite group representations, precisely one of the following two possibilities occurs:- (a) V_ρ admits a non-degenerate symmetric bilinear form which is invariant under the action of $\rho(G)$, or (b) V_ρ admits a non-degenerate symplectic bilinear form, which is invariant under the action of $\rho(G)$. If case (a) occurs, ρ is said to be *orthogonal* and if case (b) occurs, ρ is said to be *symplectic*. Our principal goal in this section is to prove the following parity result, in which we recall that $s_{E,\rho}$ is the number of copies of ρ occurring in $X(E/K) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$, where ρ factors through the finite Galois extension K of F. As earlier, $w(E, \rho)$ denotes the root number occurring in the conjectural functional equation of $L(E, \rho, s)$.

Theorem 6.2. *Assume that (i) E does not admit complex multiplication, (ii) $p \geq 5$, (iii) E admits an isogeny of degree p defined over F, (iv) u_G is even and (v) Hypotheses A1 and A2 are valid. Then, for each irreducible orthogonal representations ρ of G of dimension > 1, we have*

$$w(E, \rho) = (-1)^{s_{E,\rho}}. \tag{92}$$

See [19] for much stronger results in this direction, which are proven by quite different methods, when E is defined over Q and is semistable at 2 and 3. We note that the hypotheses of Theorem 6.2 imply that, for each v of F dividing p, E achieves good ordinary reduction over a finite abelian extension of F_v. Indeed, since p is at least 5, all the hypotheses of Lemma 2.14 are valid for E/F_v. Hence by (5) of Lemma 2.14, and the fact that U now has dimension 1, it follows that the image of the Weil group of F_v in the automorphism group of $\mathcal{V}(E)$ must be a finite abelian group. Hence, for some finite abelian extension of F_v, the image of the inertial subgroup of the Weil group becomes trivial. But Lemma 2.11 shows that E achieves good ordinary reduction over the fixed field of the kernel of the homomorphism of the inertial subgroup into $\mathrm{Aut}(\mathcal{V}(E))$, justifying our claim. Hence Theorem 6.2 follows immediately by combining Rohrlich's formula for $w(E,\rho)$ given in [38, Proposition 5] with the following Theorem 6.3, whose proof by Iwasawa theoretic methods will take up the rest of this section.

For each finite place v of F with $\mathrm{ord}_v(j_E) < 0$, let χ_v be the character of the absolute Galois group of F_v, with $\chi_v^2 = 1$, defined as follows:- (i) If E has split multiplicative reduction at v, then $\chi_v = 1$, (ii) if E does not have split multiplicative reduction at v, then χ_v defines the unique quadratic extension of F_v over which E achieves split multiplicative reduction. In fact, χ_v is a character of the decomposition group of any prime of F_∞ above v. Finally, ρ_v will denote the restriction of ρ to the decomposition group of some fixed prime of F_∞ above v.

Theorem 6.3. *Assume the same hypotheses as in Theorem 6.2. For all irreducible orthogonal representations ρ of G of dimension > 1, we have*

$$s_{E,\rho} \equiv u_G[F:\mathbb{Q}]/2 + \sum_v \langle \chi_v, \rho_v \rangle \mod 2, \tag{93}$$

where the sum is taken over all places v of F with $\mathrm{ord}_v(j_E) < 0$, *and $\langle \chi_v, \rho_v \rangle$ denotes the multiplicity of χ_v occurring in the representation ρ_v.*

We now establish several lemmas prior to the proof of Theorem 6.3. Assume from now on that we have fixed a $\mathbb{Z}_p$-basis of $T_p(E)$ such that the image of G in $GL_2(\mathbb{F}_p)$ is contained in the Borel subgroup

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,\, b,\, c \in \mathbb{F}_p,\ ac \neq 0 \right\},$$

where the character in the top left hand corner gives the action of G on Ker ϕ. Let

$$F' = F(\mathrm{Ker}\ \phi, \mu_p), \quad G' = \mathrm{Gal}(F_\infty/F'), \quad H' = \mathrm{Gal}(F_\infty/F(\mu_{p^\infty}, \mathrm{Ker}\ \phi)).$$

Let κ be the homomorphism

$$B \longrightarrow \mathbb{F}_p^\times \times \mathbb{F}_p^\times$$

which sends an element $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ to (a,c). Then G' is the kernel of the composite map

$$G \to B \xrightarrow{\kappa} \mathbb{F}_p^\times \times \mathbb{F}_p^\times$$

and is the unique p-Sylow subgroup of G. Putting

$$\Delta = G/G',$$

we clearly have an isomorphism $H/H' \simeq G/G'$. As earlier, let Ω denote the intersection of G with the torsion subgroup of the centre $\mathbb{Z}_p^\times$ of $GL_2(\mathbb{Z}_p)$. Plainly Ω is a cyclic group whose order divides $p-1$, and hence it injects into the quotient G/G'.

Lemma 6.4. *(i) The image of the canonical injection $\Omega \to \Delta$ coincides with the inverse image of the diagonal of $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ under the injection $\Delta \to \mathbb{F}_p^\times \times \mathbb{F}_p^\times$.*
(ii) The quotient group Δ/Ω is a cyclic group whose order d divides $p-1$. Moreover, either $u_G = d$, or $u_G = pd$.

Proof. Assertion (ii) follows from (i) because the quotient of $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ by its diagonal is cyclic. Hence it suffices to prove (i). Let σ be an element of G which maps to a diagonal element x of $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$. Let α be the unique $(p-1)$-th root of unity in $\mathbb{Z}_p^\times$ with $\alpha \equiv x \mod p$, and let

$$z_\alpha = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}.$$

We then have $\sigma = z_\alpha y$, where

$$y \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod p.$$

Clearly $\sigma^{p-1} = y^{p-1}$. This shows that y^{p-1} belongs to G, whence the same must be true for y itself, since y^{p-1} is also a topological generator of the subgroup $y^{\mathbb{Z}_p}$. Hence y is in G, and thus z_α is in G, completing the proof of the lemma. □

Before beginning the proof of Theorem 6.3, we note a further connection between our work and that of Rohrlich [38]. Define

$$\vartheta_n^- = \sum_\rho \dim V_\rho$$

where the summation is taken over all irreducible self-dual representations ρ of $\mathrm{Gal}(F_n/F)$, where $F_n = F(E_{p^n})$, with $w(E,\rho) = -1$. Rohrlich [37] has shown that all ρ occurring in the sum for ϑ_n^- are necessarily orthogonal. Hence Theorem 6.2 shows that we have

$$s_{E/F_n} \geq \vartheta_n^-, \quad (n \geq 1). \tag{94}$$

On the other hand, Rohrlich has shown in [38] that

$$\vartheta_n^- \geq a.p^{2n} \quad (n \geq 1) \tag{95}$$

for some $a > 0$ if and only if $p \equiv 3 \mod 4$ and $[F:\mathbb{Q}]$ is odd. In fact, Rohrlich proves the stronger result that, as n tends to infinity, ϑ_n^- is asymptotic to a positive constant times p^{2n} when $p \equiv 3 \mod 4$ and $[F:\mathbb{Q}]$ is odd, and is at most a constant times p^n otherwise. Let $\mathcal{L}$ be the fixed field of the subgroup of G generated by G' and Ω. It is proven in [38] (see formula 1.10 of the proof of Proposition 5), that we have

$$[\mathcal{L}:\mathbb{Q}] = u_G[F:\mathbb{Q}] \equiv (p-1)[F:\mathbb{Q}] \mod 4.$$

Hence, it follows from Corollary 5.7 that (95) holds if and only if the $\Lambda(H')$-rank of $Y(E/F_\infty)^{(\alpha)}$ is odd for each character α of Ω with $\alpha^2 = \mathbf{1}$. In particular, we have proven the following result.

Corollary 6.5. *In addition to the hypotheses of Theorem 6.2, assume that* $p \equiv 3 \bmod 4$ *and* $[F : \mathbb{Q}]$ *is odd. Then there exists* $a > 0$ *such that*

$$s_{E/F_n} \geq a \cdot p^{2n} \ \ (n \geq 1), \tag{96}$$

where $F_n = F(E_{p^n})$.

A numerical example for which both Theorem 6.2 and Corollary 6.5 hold is given by the elliptic curve E of conductor 294 whose equation is (89), with $F = \mathbb{Q}$ and $p = 7$. We remark that for this example, Rohrlich [38] has proven that the cases $w(E, \rho) = +1$ and $w(E, \rho) = -1$ both occur for infinitely many self-dual irreducible Artin representations ρ of G.

The following remark shows that, at least conjecturally, this lower bound may be essentially the best possible. Let C' denote the intersection of G' with the centre of $GL_2(\mathbb{Z}_p)$, and put $\mathfrak{G} = G'/C'$. Let $\mathfrak{F}_\infty$ be the fixed field of C', and define $\mathfrak{F}_n = \mathfrak{F}_\infty \cap F_n$. Since p is odd, any irreducible self-dual representation of $\mathrm{Gal}(F_n/F)$ factors through $\mathrm{Gal}(\mathfrak{F}_n/F)$. Hence, under the same hypotheses as Corollary 6.5, our arguments prove the stronger result that

$$s_{E/\mathfrak{F}_n} \geq a.p^{2n} \ \ (n \geq 1).$$

On the other hand, when E satisfies Hypothesis A1, it has long been conjectured that $X(E/\mathfrak{F}_\infty)$ is a torsion module over the Iwasawa algebra of $\mathfrak{G}$, but unfortunately this conjecture has still not been proven for a single numerical example. Nevertheless, assuming the conjecture to be true, it follows easily that there exists a constant $b > 0$ such that

$$s_{E/\mathfrak{F}_n} \leq b.p^{2n} \ \ (n \geq 1).$$

Naturally this leads one to speculate that perhaps, analogously to Theorem 4.12, $s_{E,\rho}$ has a uniform upper bound, independent of ρ, when ρ runs over all irreducible Artin representations of $\mathfrak{G}$.

We now begin the proof of Theorem 6.3. Let $\rho : G \to GL(V_\rho)$ be any irreducible, self-dual, orthogonal Artin representation of G. Fixing a lattice in V_ρ stable under the action of $\rho(G)$, we can view ρ as a representation

$$\rho : G \to \mathrm{Aut}(W_\rho)$$

where W_ρ is a free module of rank d_ρ over the ring of integers $\mathcal{O}$ of some finite extension of $\mathbb{Q}_p$. Following the strategy of our earlier arguments, we establish Theorem 6.2 by computing $h_\rho[Y(E/F_\infty)]$ where h_ρ is the Akashi homomorphism from $K_0(\Lambda(H))$ to $\mathbb{Z}$ defined by (52). Let $P(F^{\mathrm{cyc}})$ denote the set of all places u of F^{cyc} with $\mathrm{ord}_u(j_E) < 0$ (note that this is precisely the set of places of F^{cyc} which are infinitely ramified in F_∞). For each u in $P(F^{\mathrm{cyc}})$, we write H_u for the decomposition group of some fixed prime of F_∞ above u. Then Theorem 3.5 asserts that

$$h_\rho([Y(E/F_\infty)]) = \lambda_\rho(E/F^{\mathrm{cyc}}) \ + \sum_{u \in P(F^{\mathrm{cyc}})} b_{\rho,u}, \tag{97}$$

where

$$\lambda_\rho(E/F^{\mathrm{cyc}}) = \mathrm{rank}_{\mathcal{O}}\, X(\mathrm{tw}_\rho(E)/F^{\mathrm{cyc}})), \;\; b_{\rho,u} = \mathrm{rank}_{\mathcal{O}}(T_p(E)\otimes_{\mathbb{Z}_p} W_\rho)^{H_u}. \tag{98}$$

Moreover, since ρ is assumed to be orthogonal, Theorem 3.8 gives

$$s_{E,\rho} \equiv \lambda_\rho(E/F^{\mathrm{cyc}}) \mod 2. \tag{99}$$

Combining (97) and (99), we conclude that

$$s_{E,\rho} \equiv h_\rho([Y(E/F_\infty)]) \;-\; \sum_{u\in P(F^{\mathrm{cyc}})} b_{\rho,u} \mod 2. \tag{100}$$

Since $\Delta = H/H'$ is a finite abelian group of exponent $p-1$, the K-theoretic arguments explained at the beginning of §4 apply in this situation. Recalling that $\hat{\Delta} = \mathrm{Hom}\,(\Delta, \mathbb{Z}_p^\times)$, we have

$$l_\Delta([Y(E/F_\infty)]) = (n_\chi)_{\chi\in\hat{\Delta}},$$

where l_Δ is the isomorphism given by (50). We then obtain from (53) that

$$h_\rho([Y(E/F_\infty]) = \sum_{\chi\in\hat{\Delta}} m_\chi(\rho) n_\chi,$$

with integers $m_\chi(\rho)$ defined immediately before (53). Since ρ is irreducible, and Ω is contained in the centre of G, the restriction of ρ to Ω is d_ρ copies of a single character of Ω, which we denote by α. Hence, viewed as representations of Ω, we have

$$W_\rho = Z_\alpha^{d_\rho}, \tag{101}$$

where Z_α denotes a free $\mathcal{O}$-module of rank 1 on which Ω acts via α. Note that $\alpha^2 = \mathbf{1}$ since ρ is self-dual.

Lemma 6.6. *Let $\chi \in \hat{\Delta}$. Then $m_\chi(\rho) = 0$ unless $\chi_{|\Omega} = \alpha$, where α is as in* (101).

Proof. By definition,

$$m_\chi(\rho) = h_\rho(P_\chi) = \mathrm{rank}_{\mathcal{O}}(W_\rho \otimes_{\mathbb{Z}_p} \Lambda(H)e_\chi)_H.$$

But the $\mathcal{O}$-module on the right hand side is a quotient of $(W_\rho \otimes \Lambda(H)e_\chi)_\Omega$ and this latter group is clearly zero unless $\chi_{|\Omega} = \alpha$. □

We recall that we can write G as a semi-direct product of its normal pro-p subgroup G' and a subgroup D isomorphic to Δ. We identify the character groups of D and Δ. Let $\mathcal{K}$ be the quotient field of $\mathcal{O}$ and we write U_χ for the $\mathcal{K}$-vector space of dimension 1 on which D acts via the character χ of Δ.

Lemma 6.7. *Viewed as a representation of D via restriction, we have*

$$V_\rho = \underset{\chi\in\hat{\Delta}}{\oplus} U_\chi^{m_{\chi^{-1}}(\rho)}$$

Proof. The restriction of ρ to D is semisimple and hence is of the form $\oplus U_\chi^{a_\chi}$ for integers $a_\chi \geq 0$ and χ running over $\hat{\Delta}$. Taking the evident $\mathcal{O}$-lattice in this representation, it is clear that the reduction of this D-representation modulo the maximal ideal of $\mathcal{O}$ is the semisimple representation $\oplus a_\chi \tilde{\chi}$, where $\tilde{\chi}$ denotes the reduction of χ modulo the maximal ideal of $\mathcal{O}$. The assertion of the lemma now follows from Lemma 3.2 and the Brauer-Nesbitt theorem. □

Proposition 6.8. *Let $\mathcal{G}$ be the subgroup of G generated by G' and Ω. Then every self-dual irreducible Artin representation ρ of G of dimension > 1 is induced from an irreducible representation of $\mathcal{G}$.*

Corollary 6.9. *Let α be the character of Ω arising from the restriction of ρ to Ω as in* (101)*. Then $m_\chi(\rho)$ is the same for all χ in $\hat{\Delta}$ such that $\chi_{|\Omega} = \alpha$.*

Proof. Assuming Proposition 6.8, it follows that $V_\rho = \mathrm{Ind}_{\mathcal{G}}^{G}(V'_\rho)$, where V'_ρ is some irreducible representation of $\mathcal{G}$. Now G is the semi-direct product of its Sylow p-subgroup G' and D. Since Ω lies in the centre of G, and has order dividing $p-1$, it follows easily that Ω must be a subgroup of D. Moreover, we have $G/\mathcal{G} \simeq D/\Omega$. Hence, restricting ρ to D, we see that

$$V_{\rho|_D} \simeq \mathrm{Ind}_{\Omega}^{D}(V''_\rho), \tag{102}$$

where V''_ρ denotes the restriction of V'_ρ to Ω. But, since V'_ρ is an irreducible $\mathcal{G}$-representation and Ω lies in the centre of $\mathcal{G}$, we see that V''_ρ must consist of d'_ρ copies of α, where d'_ρ is the dimension of V'_ρ. Hence, as D is abelian, we conclude from (102) that the restriction of ρ to D is given by

$$V_{\rho|_D} \simeq \bigoplus_{\substack{\chi \in \hat{\Delta} \\ \chi_{|\Omega} = \alpha}} U_\chi^{d'_\rho}. \tag{103}$$

Therefore, by Lemma 6.7, we must have $m_{\chi^{-1}}(\rho) = d'_\rho$ for every χ in $\hat{\Delta}$ such that $\chi_{|\Omega} = \alpha$. This completes the proof of the corollary. □

Before giving the proof of Proposition 6.8, we need to establish two group theoretic lemmas. Put $R_0 = GL_2(\mathbb{Z}_p)$, and for $n \geq 1$, define R_n to be the subgroup of all matrices in R_0 which are congruent to the identity matrix modulo p^n. Let $G_n = G \cap R_n$ for all $n \geq 0$. For each $n \geq 0$, we define a chain of subgroups

$$G_n \supset B_n \supset A_n \supset G_{n+1}$$

where, writing

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{104}$$

we have

$$A_n = \{\sigma \in G_n : a \equiv d \equiv 1 \mod p^{n+1},\ c \equiv 0 \mod p^{n+1}\},\ B_n = \{\sigma \in G_n : c \equiv 0 \mod p^{n+1}\}.$$

If K, K' are any two subgroups of G, $[K, K']$ will denote the subgroup of G generated by all commutators $kk'k^{-1}k'^{-1}$, with k in K and k' in K'. We omit the proof of the following lemma, as it is straightforward.

Lemma 6.10. *For all $n \geq 0$, we have (i) $[G', G_n] \subset B_n$, (ii) $[G, B_n] \subset A_n$, and (iii) $[G', A_n] \subset G_{n+1}$.* □

It follows from (ii) that both A_n and B_n are normal subgroups of G for all $n \geq 0$. Let us define

$$i_n : G \to \mathrm{Aut}(A_n/G_{n+1}),\ \ j_n : G \to \mathrm{Aut}(G_n/B_n)$$

to be the homomorphisms defined by conjugation by elements of G.

Lemma 6.11. *For all $n \geq 0$, both A_n/G_{n+1} and G_n/B_n are cyclic groups of order dividing p. Moreover, if A_n/G_{n+1} (resp. G_n/B_n) has order p, then the kernel of i_n (resp. j_n) is precisely $\mathcal{G}$.*

Proof. One verifies immediately that the maps

$$f_n : A_n/G_{n+1} \to \mathbb{Z}/p\mathbb{Z},\ \ g_n : G_n/B_n \to \mathbb{Z}/p\mathbb{Z}$$

given by

$$f_n(\tau G_{n+1}) = p^{-n}v \mod p\mathbb{Z},\ g_n(\tau B_n) = p^{-n}w \mod p\mathbb{Z},$$

where

$$\tau = \begin{pmatrix} u & v \\ w & z \end{pmatrix},$$

yield injective group homomorphisms. This proves the first assertion of the lemma. Moreover, it is clear that $\mathcal{G}$ is contained in the kernel of both i_n and j_n. Further, if σ given by (104) above denotes any element of G, a straightforward calculation with matrices shows that

(105)
$$f_n(\sigma\tau\sigma^{-1}G_{n+1}) = ad^{-1}f_n(\tau G_{n+1}) \mod p\mathbb{Z},\ \ g_n(\sigma\tau\sigma^{-1}B_n) = a^{-1}dg_n(\tau B_n) \mod p\mathbb{Z}.$$

The assertion of the lemma is now clear since Lemma 6.4 shows that the maps

$$G/\mathcal{G} \to \mathbb{F}_p^\times$$

given by $\sigma \mapsto ad^{-1} \mod p$ (respectively $a^{-1}d \mod p$) are injective. □

We now prove Proposition 6.8. Fix an element ξ of G such that $\xi \mod \mathcal{G}$ is a generator of $G/\mathcal{G} = \Delta/\Omega$, and put $r = \#(\Delta/\Omega)$. Suppose that V'_ρ is an irreducible component of V_ρ restricted to $\mathcal{G}$. Since V_ρ is irreducible, we must have

$$V_\rho = \sum_{i=0}^{r-1} \xi^i V'_\rho, \tag{106}$$

as the right hand side of (106) is a non-zero subspace, which is stable under the action of G. We must show that the subspaces $\xi^i V'_\rho$ $(i = 0, \cdots, r-1)$ are linearly independent to establish the proposition.

Define n_0 to be the smallest integer ≥ 1 such that Ker $\rho \supset G_{n_0}$. We first prove that either Proposition 6.8 is valid or

$$\text{Ker } \rho \supset A_{n_{0-1}}. \tag{107}$$

Assume therefore that (107) does not hold. In particular, we then have that $A_{n_0-1} \neq G_{n_0}$, and so A_{n_0-1}/G_{n_0} is a cyclic group of order p, by Lemma 6.11. Pick a generator τ of A_{n_0-1}/G_{n_0}. By (iii) of Lemma 6.10, the image of A_{n_0-1} lies in the centre of G'/G_{n_0}. Since V'_ρ is an irreducible representation of $(G'/G_{n_0}) \times \Omega$, we conclude from Schur's lemma that τ must act on V'_ρ by a scalar t in μ_p. By the second assertion of Lemma 6.11, τ acts on $\chi^i V'_\rho$ by t^{k^i}, where k is an element of $\mathbb{F}_p^\times$ of order r. We can assume that $t \neq 1$, since otherwise (107) would be valid. Thus the subspaces $\xi^i V'_\rho$ $(i = 0, \cdots, r-1)$ are linearly independent since the t^{k^i} $(i = 0, \cdots, r-1)$ are all distinct, proving Proposition 6.8

Thus we can assume that (107) is valid. Also, since G/A_0 is abelian, we can suppose that $n_0 \geq 2$. It follows from (ii) of Lemma 6.10 that the image of B_{n_0-1} in G/A_{n_0-1} lies in the centre of G/A_{n_0-1}. But it is easily seen that B_{n_0-1}/A_{n_0-1} has exponent p. In view of (107) and the irreducibility of V_ρ, we conclude from Schur's lemma that B_{n_0-1} acts on V_ρ by scalars in μ_p. As $p \neq 2$ and ρ is self-dual, we deduce that B_{n_0-1} must act trivially on V_ρ, whence

$$\text{Ker } \rho \supset B_{n_0-1}. \tag{108}$$

If $G_{n_0-1} = B_{n_0-1}$, we have a contradiction by virtue of the minimality of n_0. Thus we may assume that $G_{n_0-1} \neq B_{n_0-1}$, and we choose τ to be a generator of G_{n_0-1}/B_{n_0-1}, which is cyclic of order p. By (i) of Lemma 6.10, the image of G_{n_0-1} in G'/B_{n_0-1} lies in the centre of this group. Thus, by Schur's lemma, τ must act on V'_ρ by a p-th root of unity t. By the second assertion of Lemma 6.11, τ acts on $\xi^i V'_\rho$ by t^{h^i}, where h is an element of $\mathbb{F}_p^\times$ of order r. If $t = 1$, we would then have G_{n_0-1} acting trivially on V_ρ, which contradicts the minimality of n_0. Hence we must have $t \neq 1$, and it is again clear that the subspaces $\xi^i V$ $(i = 0, \cdots, r-1)$, must be linearly independent. This completes the proof of Proposition 6.8. □

Remark 6.12. David Rohrlich kindly pointed out to us a somewhat different proof of Proposition 6.8.

Definition 6.13. We write $m(\rho) = m_\chi(\rho)$ for all χ in $\hat{\Delta}$ with $\chi_{|\Omega} = \alpha$.

The next result does not require the hypothesis that ρ be orthogonal.

Proposition 6.14. *Assume that hypotheses (i)-(v) of Theorem 6.2 are valid. Then for every irreducible, self-dual Artin representation ρ of G of dimension > 1, we have*

$$h_\rho([Y(E/F_\infty)]) \equiv u_G[F:\mathbb{Q}]/2 \mod 2. \tag{109}$$

Proof. In view of (53), Lemma 6.6 and Corollary 6.9, we have

$$h_\rho([Y(E/F_\infty)]) = m(\rho) \sum_{\substack{\chi \in \hat{\Delta} \\ \chi_{|\Omega} = \alpha}} n_\chi.$$

On the other hand, we have (cf. Lemmas 3.1 and 5.2),

$$\tau(\alpha) = \sum_{\substack{\chi \in \hat{\Delta} \\ \chi_{|\Omega} = \alpha}} n_\chi. \tag{110}$$

Now our hypothesis that u_G is even implies that $[\mathcal{L} : F] = \#(\Delta/\Omega)$ is even (see Lemma 6.4). Hence, by Corollary 5.7, we have

$$\tau(\alpha) \equiv [\mathcal{L} : \mathbb{Q}]/2 \mod 2.$$

Also, since p is odd, and u_G is even, we clearly have

$$[\mathcal{L} : \mathbb{Q}]/2 \equiv u_G[F : \mathbb{Q}]/2 \mod 2.$$

Thus to complete the proof, we must show that

$$m(\rho)u_G[F : \mathbb{Q}]/2 \equiv u_G[F : \mathbb{Q}]/2 \mod 2. \tag{111}$$

If F is totally imaginary, then $[F : \mathbb{Q}]$ is even, and so (111) clearly holds because both sides are even. Assume therefore that F has a real place v, and write $i_v \in G$ for the complex conjugation attached to some fixed place of F_∞ above v. Writing $\det(\rho)$ for the determinant of ρ, we then have

$$(\det(\rho))(i_v) = \left(\prod_{\substack{\chi \in \hat{\Delta} \\ \chi_{|\Omega} = \alpha}} \chi(i_v) \right)^{m(\rho)}. \tag{112}$$

Indeed, since both sides of (112) are roots of unity of order prime to p, it suffices to prove that (112) holds modulo the maximal ideal of $\mathcal{O}$. But this last assertion is clear from Lemmas 3.2 and 6.6, and Corollary 6.9. Also, since ρ has dimension greater than 1, Rohrlich [38] has shown that

$$(\det(\rho))(i_v) = (-1)^{u_G/2}. \tag{113}$$

If $m(\rho)$ is odd, (111) is clearly true. If $m(\rho)$ is even, $(\det(\rho))(i_v) = 1$ by (112), and this shows that $u_G/2$ is even by (113), whence again (111) holds. This completes the proof of the proposition. □

In view of (100) and Proposition 6.14, it suffices to establish the following purely local result to complete the proof of Theorem 6.3. For the rest of this section, v will denote any prime of F with $\mathrm{ord}_v(j_E) < 0$, and we fix some place u of F_∞ above v. For simplicity, we shall also write u for the restriction of u to F^{cyc}. We write G_v for the decomposition group of u over v, and let H_u be the intersection of H and G_v. If ρ is an Artin representation of G, ρ_v (resp. ρ_u) will denote the restriction of ρ to G_v (resp. H_u). Let χ_v be the character of order dividing 2 of G_v which is defined immediately before Theorem 6.3.

Proposition 6.15. *For each prime v of F with $\mathrm{ord}_v(j_E) < 0$, we have*

$$\langle \chi_v, \rho_v \rangle \equiv \mathrm{rank}_{\mathcal{O}}(T_p(E) \otimes_{\mathbb{Z}_p} W_\rho)^{H_u} \mod 2.$$

By Lemma 3.7, the assertion of Proposition 6.15 is equivalent to the congruence

$$\langle \chi_v, \rho_v \rangle \equiv \langle \chi_u \omega_u^{-1}, \rho_u \rangle \mod 2, \tag{114}$$

where, as before, ω_u is the character giving the action of H_u on the group of all p-power roots of unity. Hence to prove (114), it suffices to establish the following two equations

$$\langle \chi_v, \rho_v \rangle \equiv \langle \chi_u, \rho_u \rangle \mod 2, \tag{115}$$

$$\langle \chi_u, \rho_u \rangle = \langle \chi_u \omega_u^{-1}, \rho_u \rangle. \tag{116}$$

We first deal with (115). Noting that $\chi_v^{-1}\rho_v$ is also self dual because χ_v has order dividing 2, we see that (115) is an immediate consequence of the following lemma.

Lemma 6.16. *Let θ be any self-dual Artin representation of G_v, and let θ_u denote its restriction to H_u. Then*

$$\langle \mathbf{1}, \theta \rangle \equiv \langle \mathbf{1}, \theta_u \rangle \mod 2.$$

Proof. It suffices to consider the cases when either (i) θ is the direct sum of a representation τ of G_v and its contragredient representation, or (ii) θ is an irreducible self-dual representation of G_v. In the first case, we have

$$\langle \mathbf{1}, \theta \rangle = 2\langle \mathbf{1}, \tau \rangle, \;\; \langle \mathbf{1}, \theta_u \rangle = 2\langle \mathbf{1}, \tau_u \rangle,$$

and the assertion of the lemma is clearly true. Assume next that we are in case (ii), and let V be a finite dimensional vector space realizing θ. It is clear that if $\langle \mathbf{1}, \theta_u \rangle = 0$, then $\langle \mathbf{1}, \theta \rangle = 0$. If $\langle \mathbf{1}, \theta_u \rangle$ is non-zero, the subspace of V fixed by H_u is non-zero and stable under G_v, whence it must be the whole of V since θ is irreducible. Thus θ is in fact an irreducible self-dual Artin representation of G_v/H_u which is isomorphic to the additive group of p-adic integers. As p is odd, we must clearly have $\theta = \mathbf{1}$, and the assertion of the lemma is again clear. □

We now turn to the proof of (116). We recall that $\mathcal{G}$ is the subgroup of G generated by G' and Ω, and that $\mathcal{L}$ is the fixed field of $\mathcal{G}$. As always, u will denote our fixed prime of F_∞ lying above our place v of F with $\mathrm{ord}_v(j_E) < 0$. We have the tower of fields

$$F_{\infty,u} \supset F'^{\mathrm{cyc}}_u \supset \mathcal{L}^{\mathrm{cyc}}_u \supset F^{\mathrm{cyc}}_u.$$

We recall that $G_v = \mathrm{Gal}(F_{\infty,u}/F_v)$, and

$$H_u = H \cap G_v,\ D_u = D \cap H_u,\ \Omega_u = \Omega \cap H_u.$$

We also write $\Delta_u = \mathrm{Gal}(F'^{\mathrm{cyc}}_u/F^{\mathrm{cyc}}_u)$. It is easily seen that H_u is the semi-direct product of D_u and $\mathrm{Gal}(F_{\infty,u}/F'^{\mathrm{cyc}}_u)$. Moreover, we can identify Ω_u with $\mathrm{Gal}(F'^{\mathrm{cyc}}_u/\mathcal{L}^{\mathrm{cyc}}_u)$. As is explained in the proof of Lemma 5.3, Ω_u always acts trivially on μ_{p^∞}, and hence the characters χ_u and $\chi_u\omega_u^{-1}$ of Δ_u have the same restriction to Ω_u. Also, as p is odd, there is always an odd number of places of F^{cyc} lying above our given place v of F. Following our earlier notation, if θ is any representation of D_u, and ν is a 1-dimensional character of D_u, we write $\langle \nu, \theta \rangle$ for the multiplicity of ν occurring in θ. Thus the proof of (116), and so also the proof of Proposition 6.15 and Theorem 6.2, will be complete once we have established the following result.

Lemma 6.17. *Let ρ be any irreducible self-dual Artin representation of G of dimension > 1, and put $\rho_u = \rho_{|H_u}$. Then, as ν runs over all 1-dimensional characters of Δ_u with $\nu_{|\Omega_u}$ a fixed character of Ω_u, $\langle \nu, \rho_u \rangle$ is constant.*

Proof. We can regard Δ_u as a subgroup of Δ, and we write $\xi_u = \xi_{|\Delta_u}$ when ξ belongs to $\hat{\Delta}$. Let α be the character of Ω given by (101). We shall assume from now on that $\nu_{|\Omega_u} = \alpha_{|\Omega_u}$, since otherwise $\langle \nu, \rho_u \rangle = 0$. When it is convenient, we shall identify characters of Δ_u with characters of D_u.

We now use the fact that ρ is a global representation to conclude that

$$\langle \nu, \rho_{|D_u} \rangle \text{ is constant} \tag{117}$$

for all characters ν of Δ_u with $\nu_{|\Omega_u} = \alpha_{|\Omega_u}$. Indeed, given any such ν, it is easy to see that there are precisely $\#(D/\Omega D_u)$ distinct characters ψ of D such that $\psi_u = \nu$ and $\psi_{|\Omega} = \alpha$. The assertion (117) is then plain from Lemma 6.7 and Corollary 6.9.

Now ρ_u will factor through some finite Galois extension L of F^{cyc}_u with $L \supset F'^{\mathrm{cyc}}_u$. We put

$$A = \mathrm{Gal}(L/F'^{\mathrm{cyc}}_u),\ B = \mathrm{Gal}(L/F^{\mathrm{cyc}}_u),$$

so that A is a cyclic normal subgroup of p-power order of B. Moreover, as $\mathrm{Gal}(F_{\infty,u}/L)$ is pro-p, we can identify D_u with its image in B, and B will then be the semi-direct product of A and D_u.

Let $\mathcal{R}(B)$ denote the set of all irreducible representations of the finite group B, which do not factor through the abelian quotient Δ_u of B, and whose restriction to Ω_u is a finite number of copies of $\alpha_{|\Omega_u}$. Identifying ρ_u with a representation of B, it is then clear that we have

$$\langle \nu, \rho_u \rangle = \langle \nu, \rho_{|D_u} \rangle - \sum_{\mu \in \mathcal{R}(B)} \langle \mu, \rho_u \rangle \langle \nu, \mu_{|D_u} \rangle.$$

Thus, in view of (117), the proof of the lemma will be complete provided we can show that

$$\langle \nu, \mu_{|D_u} \rangle = 1 \text{ for all } \mu \text{ in } \mathcal{R}(B). \tag{118}$$

Let A' be the subgroup of B generated by A and Ω_u, so that $A' = \Omega_u \times A$. Put $C = B/A' \simeq \Delta_u/\Omega_u$, and let $r_u = \#C$. If C is trivial, then $\Delta_u = \Omega_u$, and $\mathcal{R}(B)$ is empty, and so (118) holds vacuously. Hence we may assume that C is a non-trivial cyclic group. The essential point then is that the centraliser of A in B is precisely A'. Indeed, if ξ is any element of B whose image in C is a generator, then the theory of the Tate curve shows that

$$\xi\gamma\xi^{-1} \;=\; \gamma^{\omega_u(\xi)}, \tag{119}$$

where γ is a generator of A. By an entirely similar argument to that given in the proof of Corollary 6.9, we see that (118) is implied by the fact that

$$\mu = \mathrm{Ind}_{A'}^{B}(W'_\mu), \tag{120}$$

where W'_μ is a 1-dimensional vector space on which A acts via a character θ of p-power order (of course, Ω_u acts on W'_μ via $\alpha_{|\Omega_u}$). Thus to complete the proof of Lemma 6.17, we must establish (120). Write W_μ for the vector space realizing the representation μ, and let W'_μ be a non-zero irreducible subspace for the action of A'. Since A' is abelian, W'_μ must have dimension 1, and A will act on it via a character θ of p-power order. Moreover, $\theta \neq \mathbf{1}$, because μ does not factor through the quotient Δ_u of B. Since W_μ is irreducible, we must have

$$W_\mu = \sum_{i=0}^{r_u-1} \xi^i W'_\mu,$$

and, as in the proof of Proposition 6.8, we must show that the subspaces $\xi^i W'_\mu$ ($i = 0, \cdots, r_u - 1$) are linearly independent. Put $\theta(\gamma) = \zeta$, so that ζ is a non-trivial p-power root of unity. But, by (119), γ acts on $\xi^i W'_\mu$ by $\zeta^{\omega_u(\xi)^{-i}}$ ($i = 0, \cdots, r_u - 1$). But, as ω_u has exact order r_u, all of these roots of unity are distinct. This proves that the subspaces $\xi^i W'_\mu$ ($i = 0, \cdots, r_u - 1$) are linearly independent and the proof is now complete.

□

7 Appendix. Some results on finite flat commutative group schemes

In this Appendix, by using the work [3] of Breuil, we prove a result (Proposition 7.3) on finite flat commutative group schemes defined over a finite tame Galois extension of a discrete valuation ring of mixed characteristic. From this Proposition, we will deduce Lemma 2.20 (6) in §2.

7.1. In this Appendix, p denotes an odd prime number, and K denotes a complete discrete valuation field of characteristic 0 with algebraically closed residue field k of characteristic p. Fix an algebraic closure $\bar{K}$ of K, let $L \subset \bar{K}$ be a finite tame Galois extension of K, and let $\Delta = \mathrm{Gal}(L/K)$. By our assumption, the order of Δ is prime to p.

Let $\mathcal{C}(L/K)$ be the following category. An object of $\mathcal{C}(L/K)$ is a finite flat commutative group scheme P over O_L, which is killed by p, and which is endowed with an action of Δ, for which the diagram

$$\begin{tikzcd} P \arrow[r, "\sigma"] \arrow[d] & P \arrow[d] \\ \mathrm{Spec}(O_L) \arrow[r, "\sigma"] & \mathrm{Spec}(O_L) \end{tikzcd}$$

is commutative for any $\sigma \in \Delta$, and which is compatible with the group scheme structure of P. Here for $\sigma \in \Delta$, the action $\sigma : \mathrm{Spec}(O_L) \to \mathrm{Spec}(O_L)$ is the morphism corresponding to $\sigma^{-1} : O_L \to O_L$.

If Q is a finite flat commutative group scheme over O_K killed by p, we obtain an object P of $\mathcal{C}(L/K)$ as $P = Q \otimes_{O_K} O_L$ on which Δ acts in the natural way. In this case, $Q = \mathrm{Spec}(\mathcal{O}(Q))$ is recovered from P by $\mathcal{O}(Q) = \mathcal{O}(P)^{\Delta}$. However, if $L \neq K$, there are objects of $\mathcal{C}(L/K)$ which are not obtained in this way. For example;

(7.1.1) Let L be the unique quadratic extension of K, let $P = \mu_{p,O_L} = \mathrm{Spec}(O_L[t]/(t^p - 1))$ and define the action of the non-trivial element σ of $\Delta = \mathrm{Gal}(L/K)$ on P by

$$O_L[t]/(t^p-1) \to O_L[t]/(t^p-1)\ ;\ \sum_i a_i t^i \mapsto \sum_i \sigma(a_i) t^{-i} \quad (a_i \in O_L).$$

Then $O_L \otimes_{O_K} \mathcal{O}(P)^{\Delta} \to \mathcal{O}(P)$ is not an isomorphism and hence P does not come from Q as above.

7.2. Let

$$R = \mathbb{Z}[\mathbb{Q}/\mathbb{Z}[1/p]],$$

that is, R is the group ring over $\mathbb{Z}$ of the group $\mathbb{Q}/\mathbb{Z}[1/p]$. For $a \in \mathbb{Q}/\mathbb{Z}[1/p]$, we denote by $\gamma(a)$ the corresponding group element of R.

We identify R with the Grothendieck group of the category of all finite dimensional continuous representations of $\mathrm{Gal}(\bar{K}/K)$ over k in the following way, and for such representation M, we denote by $[M]$ the class of M in R. For $a \in \mathbb{Q}$, we identify $\gamma(a \bmod \mathbb{Z}[1/p])$ with the class of the 1-dimensional representation $\pi_K^a O_{\bar{K}} / \sum_{b \in \mathbb{Q}, b > a} \pi_K^b O_{\bar{K}}$ of $\mathrm{Gal}(\bar{K}/K)$ over k. Here π_K denotes a prime element of K. The product structure of R corresponds to the tensor product of representations over k. The Grothendieck group of representations of Δ over k is identified with the subring of R consisting of $\mathbb{Z}$-linear combinations of $\gamma(a)$ with $a \in [L : K]^{-1}\mathbb{Z}/\mathbb{Z}$.

Define maps

$$\varphi : R \to R, \quad \alpha : R \to \mathbb{Q}/\mathbb{Z}[1/p], \quad \tilde{\alpha} : R \to \mathbb{Q}, \quad \delta_0 : R \to \mathbb{Z}, \quad \deg : R \to \mathbb{Z}$$

as follows.

Let $\varphi : R \to R$ be the automorphism of the ring R which sends $\gamma(a)$ to $\gamma(pa)$.

Let $\alpha : R \to \mathbb{Q}/\mathbb{Z}[1/p]$ be the $\mathbb{Z}$-linear map which sends $\gamma(a)$ to a.

Define the $\mathbb{Z}$-linear map $\tilde{\alpha} : R \to \mathbb{Q}$ as follows. For $a \in \mathbb{Q}/\mathbb{Z}[1/p]$, $\tilde{\alpha}$ sends $\gamma(a)$ ($a \in \mathbb{Q}/\mathbb{Z}[1/p]$) to the unique element b of $\mathbb{Z}_{(p)}$ such that $0 < b \leq 1$ and such that $b \bmod \mathbb{Z}[1/p] = a$. Then $\alpha = (\tilde{\alpha} \mod \mathbb{Z}[1/p])$.

Let $\delta_0 : R \to \mathbb{Z}$ be the $\mathbb{Z}$-linear map which sends $\gamma(a)$ to 1 if $a = 0$, and to 0 if $a \neq 0$.

Let $\deg : R \to \mathbb{Z}$ be the $\mathbb{Z}$-linear map which sends $\gamma(a)$ to 1 for any a.

The following proposition is the main result of this Appendix.

Proposition 7.3. *Let P be an object of $\mathcal{C}(L/K)$, and let $D(P \otimes_{O_L} k)$ be the covariant Dieudonné module of $P \otimes_{O_K} k$. Regard* $\mathrm{Lie}(P)$ *as a k-vector space via the Teichmuller lifting $k \to O_K/pO_K$. Regard $D(P \otimes_{O_L} k)$ and* $\mathrm{Lie}(P)$ *as representations of Δ over k, and regard $P(\bar{K})$ as a representation of* $\mathrm{Gal}(\bar{K}/K)$ *over $\mathbb{F}_p$.*

(1) $\tilde{\alpha}(\varphi^{-1}([D(P \otimes_{O_L} k])) - \tilde{\alpha}([D(P \otimes_{O_L} k]) = \deg([\mathrm{Lie}(P)])[L:K]^{-1} - \delta_0([\mathrm{Lie}(P)])$ *in* $\mathbb{Q}$.

(2) Assume $p \geq r+2$ where $r = \dim_{\mathbb{F}_p} P(\bar{K})$. Then

$$\alpha([P(\bar{K}) \otimes_{\mathbb{F}_p} k]) - \alpha([D(P \otimes_{O_L} k)]) = \deg([\mathrm{Lie}(P)])p(p-1)^{-1}[L:K]^{-1} \quad \textit{in } \mathbb{Q}/\mathbb{Z}[1/p].$$

Note that $\deg([\mathrm{Lie}(P)])$ coincides with the length of the O_L-module $\mathrm{Lie}(P)$, and $\delta_0([\mathrm{Lie}(P)]$ coincides with the O_L-length of the fixed part of $\mathrm{Lie}(P)$ by Δ.

The assumption $p \geq r+2$ in (2) may be unnecessary, but our method of the proof has to use it.

(7.3.1) Example. Let $P = \mu_{p,O_L}$ with the natural action of Δ. Then $[D(P \otimes_{O_L} k)] = \gamma(0)$, $[P(\bar{K}) \otimes_{\mathbb{F}_p} k] = \gamma(e(K)(p-1)^{-1})$, and $[\mathrm{Lie}(P)] = e(K)\sum_a \gamma(a)$ where a ranges over all elements of $[L:K]^{-1}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}[1/p]$. In this example, the above (1) has the shape $0 - 0 = e(K) - e(K)$, and (2) has the shape $e(K)(p-1)^{-1} - 0 = e(L)p(p-1)^{-1}[L:K]^{-1}$ in $\mathbb{Q}/\mathbb{Z}[1/p]$.

(7.3.2) Example. Let L be the unique quadratic extension of K and let P be the object of $\mathcal{C}(L/K)$ considered in (7.1.1). Then $[D(P \otimes_{O_L} k)] = \gamma(2^{-1})$, $[P(\bar{K}) \otimes_{\mathbb{F}_p} k] = \gamma(e(K)(p-1)^{-1} + 2^{-1})$, $[\mathrm{Lie}(P)] = e(K)\gamma(0) + e(K)\gamma(2^{-1})$, and the above (1) has the shape $2^{-1} - 2^{-1} = 2e(K) \cdot 2^{-1} - e(K)$, and (2) has the shape $(e(K)(p-1)^{-1} + 2^{-1}) - 2^{-1} = 2e(K)p(p-1)^{-1} \cdot 2^{-1}$ in $\mathbb{Q}/\mathbb{Z}[1/p]$.

7.4. We define a category $\mathcal{C}'(L/K)$ following the method of Breuil [3].

Note that L is generated over K as a field by an $[L:K]$-th root of a prime element of K. Fix a prime element π_L of L such that $\pi_K := \pi_L^{[L:K]}$ is a prime element of K. Consider the ring

$$\mathcal{S} = k[u]/(u^{e(L)p})$$

where u is an indeterminate and $e(L)$ is the absolute ramification index of L. We have an isomorphism over k

$$\theta : \mathcal{S}/(u^{e(L)}) \xrightarrow{\sim} O_L/pO_L \ \ ; \ \ u \mapsto \pi_L$$

where k is embedded in O_L/pO_L via the Teichmuller lifting. Consider the following action of Δ on the ring $\mathcal{S}$: For $\sigma \in \Delta$, the action of σ on $\mathcal{S}$ is the automorphism of the ring $\mathcal{S}$ over k characterized by $\sigma(u) = au$, where $a = \sigma(\pi_L)/\pi_L$ which is an $[L : K]$-th root of 1 regarded as an element of k. Then the action of Δ on $\mathcal{S}$ and that on O_L are compatible via the isomorphism θ.

Define $\mathcal{C}'(L/K)$ to be the category of triples $(\mathcal{M}, F^1\mathcal{M}, \varphi_1)$, where $\mathcal{M}$ is a free $\mathcal{S}$-module of finite rank endowed with an action of Δ satisfying $\sigma(x+y) = \sigma(x) + \sigma(y)$ and $\sigma(ax) = \sigma(a)\sigma(x)$ ($\sigma \in \Delta$, $x, y \in \mathcal{M}$, $a \in \mathcal{S}$), $F^1\mathcal{M}$ is a Δ-stable $\mathcal{S}$-submodule of $\mathcal{M}$ such that $u^{e(L)}\mathcal{M} \subset F^1\mathcal{M}$, and φ_1 is a map $F^1\mathcal{M} \to \mathcal{M}$ satisfying the following (i) - (iii).

(i) $\varphi_1(x+y) = \varphi_1(x) + \varphi_1(y)$ for any $x, y \in F^1\mathcal{M}$, and $\varphi_1(ax) = a^p\varphi_1(x)$ for any $a \in \mathcal{S}$ and $x \in F^1\mathcal{M}$.

(ii) $\sigma \circ \varphi_1 = \varphi_1 \circ \sigma$ for any $\sigma \in \Delta$.

(iii) $\varphi_1(F^1\mathcal{M})$ generates the $\mathcal{S}$-module $\mathcal{M}$.

By [3], the following (7.4.1) and (7.4.2) hold for any object $(\mathcal{M}, F^1\mathcal{M}, \varphi_1)$ of $\mathcal{C}'(L/K)$.

(7.4.1) We have an isomorphism

$$\mathcal{S} \otimes_{\varphi, \mathcal{S}/(u^{e(L)})} F^1\mathcal{M}/u^{e(L)}F^1\mathcal{M} \xrightarrow{\sim} \mathcal{M} \quad ; \quad b \otimes x \mapsto b^p\varphi_1(x).$$

Here $\otimes_{\varphi, \mathcal{S}/(u^{e(L)})}$ means the tensor product over $\mathcal{S}/(u^{e(L)})$ with respect to the p-th power map $\varphi : \mathcal{S}/(u^{e(L)}) \to \mathcal{S}$.

(7.4.2) There are an $\mathcal{S}$-basis $(v_i)_{1 \leq i \leq r}$ of $\mathcal{M}$ and integers ℓ_i $(1 \leq i \leq r)$ such that $0 \leq \ell_i \leq e(L)$ for any i and such that the $\mathcal{S}$-module $F^1\mathcal{M}$ is generated by $u^{\ell_i}v_i$ $(1 \leq i \leq r)$.

If there is no possibility of confusion, we will sometimes denote an object $(\mathcal{M}, F^1\mathcal{M}, \varphi_1)$ of $\mathcal{C}'(L/K)$ simply by $\mathcal{M}$.

By Breuil [3], we have an equivalence of categories

$$\mathcal{C}(L/K) \simeq \mathcal{C}'(L/K).$$

In fact, what is constructed in [3] is an equivalence $\mathcal{C}(L/L) \simeq \mathcal{C}'(L/L)$, but it is seen easily that his equivalence can carry the action of Δ.

This equivalence has the following properties. Let P be an object of $\mathcal{C}(L/K)$ and let $(\mathcal{M}, F^1\mathcal{M}, \varphi_1)$ be the corresponding object of $\mathcal{C}'(L/K)$.

(a) The Dieudonné module of the special fiber. Let $D(P \otimes_{O_L} k)$ be the covariant Dieudonné module of the special fiber $P \otimes_{O_L} k$ of P. Then

$$D(P \otimes_{O_L} k) \simeq \mathcal{M}/u\mathcal{M}$$

as representations of Δ over k.

(b) The tangent space. As an $O_L[\Delta]$-module, we have

$$\mathrm{Lie}(P) \simeq \mathcal{M}/F^1\mathcal{M}.$$

Here O_L acts on $\mathcal{M}/F^1\mathcal{M}$ via $\theta^{-1} : O_L/pO_L \simeq \mathcal{S}/(u^{e(L)})$.

(c) Cartier duality. Define an object $(\mathcal{M}', F^1\mathcal{M}', \varphi_1')$ of $\mathcal{C}'(L/K)$ as follows: $\mathcal{M}'$ is the dual $\mathcal{S}$-module $\mathrm{Hom}_{\mathcal{S}}(\mathcal{M}, \mathcal{S})$ of $\mathcal{M}$. $F^1\mathcal{M}' \subset \mathcal{M}'$ is the inverse image under $\mathcal{M}' \to \mathcal{M}'/u^{e(L)}\mathcal{M}'$ of the annihilator of $F^1M/u^{e(L)}\mathcal{M}$ in the perfect duality

$$\mathcal{M}/u^{e(L)}\mathcal{M} \times \mathcal{M}'/u^{e(L)}\mathcal{M}' \to \mathcal{S}/u^{e(L)}\mathcal{S}$$

of $\mathcal{S}/u^{e(L)}\mathcal{S}$-modules. For $y \in F^1\mathcal{M}$, $\varphi_1'(y) : \mathcal{M} \to \mathcal{S}$ is the composition

$$\mathcal{M} \xrightarrow{\sim} \mathcal{S} \otimes_{\varphi, \mathcal{S}/(u^{e(L)})} F^1\mathcal{M}/u^{e(L)}F^1\mathcal{M} \to \mathcal{S}$$

where the first isomorphism is the inverse of the isomorphism in (7.4.1), and the next arrow is the unique additive map which sends $b \otimes x$ to bc^p where c is an element of $\mathcal{S}$ such that y sends x to $cu^{e(L)}$. Then the object of $\mathcal{C}(L/K)$ corresponding to $\mathcal{M}'$ is isomorphic to the Cartier dual of P.

(d) The relation with the Galois representation $P(\bar{K})$. Fix a p-th root $\pi_L^{1/p} \in \bar{K}$ of π_L. Let

$$\tilde{\theta} : \mathcal{S} \to O_{\bar{K}}/pO_{\bar{K}} \;\; ; \;\; u \mapsto \pi_L^{1/p}$$

be the ring homomorphism which sends any element a of k to the Teichmuller lifting of $a^{1/p}$. Note that for any $a \in \mathcal{S}$, we have $\theta(a \mod u^{e(L)}) = \tilde{\theta}(a)^p$ in $O_{\bar{K}}/pO_{\bar{K}}$. Let $\pi_K^{1/p} := (\pi_L^{1/p})^{[L:K]}$. Then via $\tilde{\theta}$, for $\sigma \in \mathrm{Gal}(\bar{K}/K(\pi_K^{1/p}))$, the action of σ on $O_{\bar{K}}/pO_{\bar{K}}$ commutes with the action of σ on $\mathcal{S}$ via the canonical projection $\mathrm{Gal}(\bar{K}/K(\pi_K^{1/p})) \to \Delta$.

Let

$$T(\mathcal{M}) = \mathrm{Ker}\,(O_{\bar{K}}/pO_{\bar{K}} \otimes_{\tilde{\theta},\mathcal{S}} F^1\mathcal{M} \to O_{\bar{K}}/pO_{\bar{K}} \otimes_{\tilde{\theta},\mathcal{S}} \mathcal{M} \; ; \; a \otimes x \mapsto a \otimes x - a^p\varphi_1(x)),$$

where $\otimes_{\tilde{\theta},\mathcal{S}}$ means the tensor product over $\mathcal{S}$ with respect to $\tilde{\theta} : \mathcal{S} \to O_{\bar{K}}/pO_{\bar{K}}$, and endow $T(\mathcal{M})$ with the action of $\mathrm{Gal}(\bar{K}/K(\pi_K^{1/p}))$ defined by $\sigma \otimes \sigma$ ($\sigma \in \mathrm{Gal}(\bar{K}/K(\pi_K^{1/p}))$). Then as a representation of $\mathrm{Gal}(\bar{K}/K(\pi_K^{1/p}))$, we have

$$P(\bar{K}) \simeq T(\mathcal{M}).$$

We have $\mathrm{rank}_{\mathcal{S}}(\mathcal{M}) = \dim_{\mathbb{F}_p}(P(\bar{K}))$.

(7.4.3) Example. The object of $\mathcal{C}'(L/K)$ corresponding to the standard object $\mathbb{Z}/p\mathbb{Z}$ of $\mathcal{C}(L/K)$ is described as follows. $\mathcal{M} = F^1\mathcal{M} = \mathcal{S}$. $\varphi_1(a) = a^p$ for $a \in \mathcal{S}$. The action of Δ is the natural one.

(7.4.4) Example. Let $\mathcal{L}$ be the object of $\mathcal{C}'(L/K)$ defined as follows. $\mathcal{L} = \mathcal{S}$. $F^1\mathcal{L} = (u^{e(L)})$. $\varphi_1(au^{e(L)}) = a^p$ for $a \in \mathcal{S}$. The action of Δ on $\mathcal{L}$ is the natural one. Then the object of $\mathcal{C}(L/K)$ corresponding to $\mathcal{L}$ is isomorphic to μ_{p,O_L} with the natural action of Δ.

Lemma 7.5. *Let $\mathcal{M}$ be an object of $\mathcal{C}'(L/K)$. Define an increasing filtration on $\mathcal{M}/u\mathcal{M}$ and a decreasing filtration on $F^1\mathcal{M}/uF^1\mathcal{M}$ as follows. For $i \geq 0$, let $(\mathcal{M}/u\mathcal{M})_i$ be the image of $\{x \in \mathcal{M} \mid u^i x \in F^1\mathcal{M}\}$ in $\mathcal{M}/u\mathcal{M}$, and let $(\mathcal{M}/u\mathcal{M})_i = 0$ for $i < 0$.*

For $i \geq 0$, let $(F^1\mathcal{M}/uF^1\mathcal{M})^i$ be the image of $F^1\mathcal{M} \cap u^i\mathcal{M}$ in $F^1\mathcal{M}/uF^1\mathcal{M}$, and let $(F^1\mathcal{M}/u\mathcal{M})^i = F^1\mathcal{M}/uF^1\mathcal{M}$ for $i < 0$. Note that $(\mathcal{M}/u\mathcal{M})_i = \mathcal{M}/u\mathcal{M}$ if $i \geq e(L)$, and $(F^1\mathcal{M}/F^1\mathcal{M})^i = 0$ if $i > e(L)$.

(1) *For $0 \leq i \leq e(L)$, u^i induces an isomorphism $\mathrm{gr}_i(\mathcal{M}/u\mathcal{M}) \xrightarrow{\sim} \mathrm{gr}^i(F^1\mathcal{M}/uF^1\mathcal{M})$.*

(2) *For $0 \leq i \leq e(L)$, we have an exact sequence*

$$0 \to (\mathcal{M}/u\mathcal{M})_i \to \mathcal{M}/u\mathcal{M} \xrightarrow{u^i} (u^i\mathcal{M} + F^1\mathcal{M})/(u^{i+1}\mathcal{M} + F^1\mathcal{M}) \to 0.$$

Proof. (1) The surjectivity is clear. We prove the injectivity: The point is that the kernel of $u : \mathcal{M} \to \mathcal{M}$ is contained in $F^1\mathcal{M}$. Assume $x \in \mathcal{M}$, $u^ix \in F^1\mathcal{M}$, and assume that the class of u^ix in $\mathrm{gr}^i(F^1\mathcal{M}/uF^1\mathcal{M})$ is 0. We can write $u^ix = u^{i+1}y + uz$ with $y \in \mathcal{M}$, $z \in F^1\mathcal{M}$. The element $u^{i-1}x - u^iy - z$ is killed by u and hence is contained in $F^1\mathcal{M}$. Hence $u^{i-1}x - u^iy \in F^1\mathcal{M}$. Since $u^{i-1}(x - uy) \in F^1\mathcal{M}$, $x \mod u\mathcal{M}$ is contained in $(\mathcal{M}/u\mathcal{M})_{i-1}$.

(2) is clear. □

Lemma 7.6. *Let $\mathcal{M}$ be an object of $\mathcal{C}'(L/K)$. For $0 \leq i \leq e(L)$, write $[\mathrm{gr}_i(\mathcal{M}/u\mathcal{M})] = \sum_a d(i,a)\gamma(a)$ where a ranges over all elements of $[L : K]^{-1}\mathbb{Z}/\mathbb{Z}$ and $d(i,a) \in \mathbb{Z}$. Let I be the set of all pairs (i,a) such that i is an integer satisfying $0 \leq i \leq e(L)$ and a is an element of $[L : K]^{-1}\mathbb{Z}/\mathbb{Z}$. We have*

(1) $[\mathcal{M}/u\mathcal{M}] = \sum_{(i,a)\in I} d(i,a)\gamma(a)$.

(2) $[F^1\mathcal{M}/uF^1\mathcal{M}] = \sum_{(i,a)\in I} d(i,a)\gamma(a + i[L : K]^{-1})$.

(3) $[\mathcal{M}/F^1\mathcal{M}] = \sum_{(i,a)\in I} d(i,a) \sum_{j=0}^{i-1} \gamma(a + j[L : K]^{-1})$.

(4) $[F^1\mathcal{M}/uF^1\mathcal{M}]) = \varphi^{-1}([\mathcal{M}/u\mathcal{M}])$.

Proof. (1) is clear. (2) follows from Lemma 7.5 (1).

We prove (3). We have $[\mathcal{M}/F^1\mathcal{M}] = \sum_{j=0}^{e(L)-1}[(u^j\mathcal{M} + F^1\mathcal{M})/(u^{j+1}\mathcal{M} + F^1\mathcal{M})]$. By Lemma 7.5 (2), this element is equal to $\sum_{j=0}^{e(L)-1} \gamma(j/[L : K]) \sum_{j<i\leq e(L)}[\mathrm{gr}_i(\mathcal{M}/u\mathcal{M})]$ and hence is equal to $\sum_{(i,a)\in I} d(i,a) \sum_{j=0}^{i-1} \gamma(a + j[L : K]^{-1})$.

(4) follows from the isomorphism

$$k \otimes_{\varphi,k} F^1\mathcal{M}/uF^1\mathcal{M} \xrightarrow{\sim} \mathcal{M}/u\mathcal{M} \ ; \ b \otimes x \mapsto b^p\varphi_1(x)$$

($\varphi : k \to k$ is $a \mapsto a^p$) which is obtained from the isomorphism (7.4.1). □

7.7. We prove Proposition 7.3 (1). Let $\mathcal{M}$ be the object of $\mathcal{C}'(L/K)$ corresponding to P. By (a)-(c) in 7.4, it is sufficient to prove

$$\tilde{\alpha}(\varphi^{-1}([\mathcal{M}/u\mathcal{M}])) - \tilde{\alpha}([\mathcal{M}/u\mathcal{M}]) = \deg([\mathcal{M}/F^1\mathcal{M}])[L : K]^{-1} - \delta_0([\mathcal{M}/F^1\mathcal{M}]).$$

Let the notation be as in 7.6. By 7.6 (2) and (4), we have

$$\tilde{\alpha}(\varphi^{-1}([\mathcal{M}/u\mathcal{M}])) = \hat{\alpha}([F^1\mathcal{M}/uF^1\mathcal{M}]) = \sum_{(i,a)\in I} d(i,a)\tilde{\alpha}(\gamma(a + i[L : K]^{-1})).$$

By 7.6 (3),

$$\deg([\mathcal{M}/F^1\mathcal{M}]) = \sum_{(i,a)\in I} d(i,a)i.$$

By these and by 7.6 (1), we have

$$\begin{aligned}
&\deg([\mathcal{M}/F^1\mathcal{M}])[L:K]^{-1} + \tilde{\alpha}([\mathcal{M}/u\mathcal{M}]) - \tilde{\alpha}(\varphi^{-1}[\mathcal{M}/u\mathcal{M}])) \\
&= \sum_{(i,a)\in I} d(i,a)\{i[L:K]^{-1} + \tilde{\alpha}(\gamma(a)) - \tilde{\alpha}(\gamma(a+i[L:K]^{-1}))\}.
\end{aligned}$$

On the other hand, for each $(i,a) \in I$, $i[L:K]^{-1} + \tilde{\alpha}(\gamma(a)) - \tilde{\alpha}(\gamma(a+i[L:K]^{-1}))$ is 1 or 0, and if it is 1 (resp. 0), 0 appears exactly once (resp. 0 does not appear) in $a + j[L:K]^{-1}$ $(0 \le j \le i-1)$. Hence

$$\sum_{j=0}^{i-1} \delta_0(\gamma(a+j[L:K]^{-1})) = i[L:K]^{-1} + \tilde{\alpha}(\gamma(a)) - \tilde{\alpha}(a+i[L:K]^{-1})).$$

By 7.6 (3), this shows

$$\delta_0([\mathcal{M}/F^1\mathcal{M}]) = \sum_{(i,a)\in I} d(i,a)\{(i[L:K]^{-1} + \tilde{\alpha}(\gamma(a)) - \tilde{\alpha}(\gamma(a+i[L:K]^{-1}))\}.$$

7.8. We give some preparations for the proof of Proposition 7.3 (2).

Let $\mathcal{M}$ be an object of $\mathcal{C}'(L/K)$, let r be the rank of $\mathcal{M}$ over $\mathcal{S}$, and let $\wedge^r\mathcal{M}$ be the r-th exterior power of $\mathcal{M}$ over $\mathcal{S}$. We define a representation $T(\wedge^r\mathcal{M})$ of $\mathrm{Gal}(\bar{K}/K(\pi_K^{1/p}))$ over $\mathbb{F}_p$ in the following way. Let $\ell = \dim_k(\mathcal{M}/F^1\mathcal{M})$. Then by (7.4.2), $u^\ell \wedge^r \mathcal{M}$ coincides with $\mathcal{S}$-submodule of $\mathcal{M}$ generated by all elements of the form $x_1 \wedge \cdots \wedge x_r$ with $x_1, \cdots, x_r \in F^1\mathcal{M}$. If $r \le p-1$, there is a unique additive map $\varphi_r : u^\ell \wedge^r \mathcal{M} \to \wedge^r\mathcal{M}$ such that $\varphi_r(x_1 \wedge \cdots \wedge x_r) = \varphi_1(x_1) \wedge \cdots \wedge \varphi_1(x_r)$ for any $x_1, \cdots, x_r \in F^1\mathcal{M}$. In fact, if we fix an $\mathcal{S}$-basis $(v_i)_{1\le i\le r}$ of $\mathcal{M}$ for which there are integers ℓ_i $(1 \le i \le r)$ such that $1 \le \ell_i \le e(L)$ for any i and such that $u^{\ell_i}v_i$ $(1 \le i \le r)$ generate the $\mathcal{S}$-module $F^1\mathcal{M}$ as in (7.4.2), then $\ell = \sum_{i=1}^r \ell_i$ and φ_r is defined as

$$au^\ell v_1 \wedge \cdots \wedge v_r \mapsto a^p\varphi_1(u^{\ell_1}v_1) \wedge \cdots \wedge \varphi_1(u^{\ell_r}v_r) \quad (a \in \mathcal{S}).$$

This map is well defined since

$$\ell \le e(L)r \le e(L)p - e(L).$$

We have $\varphi_r(ax) = a^p\varphi_r(x)$ for any $a \in \mathcal{S}$ and $x \in u^\ell \wedge^r \mathcal{M}$.

Define

$$\begin{aligned}
T(\wedge^r\mathcal{M}) = \mathrm{Ker}\,(O_{\bar{K}}/pO_{\bar{K}} \otimes_{\tilde{\theta},\mathcal{S}} u^\ell \wedge^r \mathcal{M} \to O_{\bar{K}}/pO_{\bar{K}} \otimes_{\tilde{\theta},\mathcal{S}} \wedge^r\mathcal{M} \\
;\ a \otimes x \mapsto a \otimes x - a^p\varphi_r(x)),
\end{aligned}$$

and endow $T(\wedge^r\mathcal{M})$ with the action of $\mathrm{Gal}(\bar{K}/K(\pi_K^{1/p}))$ given by $\sigma\otimes\sigma$ $(\sigma \in \mathrm{Gal}(\bar{K}/K(\pi_K^{1/p})))$.

Lemma 7.9. *Let $\mathcal{M}$ be an object of $\mathcal{C}'(L/K)$ of $\mathcal{S}$-rank r with $r \leq p-2$.*

(1) $T(\wedge^r \mathcal{M})$ is 1*-dimensional over $\mathbb{F}_p$.*

(2) Let $a = \ell(p-1)^{-1}[L:K]^{-1}$ where $\ell = \dim_k(\mathcal{M}/F^1\mathcal{M})$. Then there is an isomorphism of representations of $\mathrm{Gal}(\bar{K}/K(\pi_K^{1/p}))$ over k

$$T(\wedge^r \mathcal{M}) \otimes_{\mathbb{F}_p} k \simeq (\pi_K^a O_{\bar{K}} / \cup_{b \in \mathbb{Q}, b > a} \pi_K^b O_{\bar{K}}) \otimes_{\varphi^{-1},k} \wedge_k^r (\mathcal{M}/u\mathcal{M})$$

where $\otimes_{\varphi^{-1},k}$ means that k acts on the left factor of the tensor product via $a \mapsto a^{1/p}$.

(3) The canonical map $\wedge^r_{\mathbb{F}_p} T(\mathcal{M}) \to T(\wedge^r \mathcal{M})$ is an isomorphism.

Proof. We prove (1) and (2). Let v be an R-basis of $\wedge^r \mathcal{M}$. Then $\varphi_r(u^\ell v) = cv$ for some $c \in \mathcal{S}^\times$. As a subset of $O_{\bar{K}}/pO_{\bar{K}} \otimes_{\tilde{\theta},\mathcal{S}} \wedge^r \mathcal{M}$, $O_{\bar{K}}/pO_{\bar{K}} \otimes_{\tilde{\theta},\mathcal{S}} u^\ell \wedge^r \mathcal{M}$ coincides with $(\pi_L^{1/p})^\ell O_{\bar{K}}/pO_{\bar{K}} \otimes_{\tilde{\theta},\mathcal{S}} \wedge^r \mathcal{M}$. Hence $T(\wedge^r \mathcal{M})$ is identified with the kernel of

(7.9.1) $(\pi_L^{1/p})^\ell O_{\bar{K}}/pO_{\bar{K}} \otimes_{\tilde{\theta},\mathcal{S}} \wedge^r \mathcal{M} \to O_{\bar{K}}/pO_{\bar{K}} \otimes_{\tilde{\theta},\mathcal{S}} \wedge^r \mathcal{M}$; $a(\pi_L^{1/p})^\ell \otimes v \mapsto (a(\pi_L^{1/p})^\ell - a^p c) \otimes v \quad (a \in O_{\bar{K}}/pO_{\bar{K}})$.

Let $\tilde{c} \in (O_{\bar{K}})^\times$ be a lifting of $\tilde{\theta}(c) \in O_{\bar{K}}/pO_{\bar{K}}$, and let $b \in O_{\bar{K}}$ be a $(p-1)$-th root of $(\pi_L^{1/p})^\ell \tilde{c}^{-1}$. Then as is easily seen, the kernel of (7.9.1) coincides with the kernel of

(7.9.2) $b(\pi_L^{1/p})^\ell O_{\bar{K}}/pO_{\bar{K}} \otimes_{\tilde{\theta},\mathcal{S}} \wedge^r \mathcal{M} \to b(\pi_L^{1/p})^\ell O_{\bar{K}}/pO_{\bar{K}} \otimes_{\tilde{\theta},\mathcal{S}} \wedge^r \mathcal{M}$; $xb(\pi_L^{1/p})^\ell \otimes v \mapsto (x - x^p) b (\pi_L^{1/p})^\ell \otimes v \quad (x \in O_{\bar{K}}/pO_{\bar{K}})$.

Hence this kernel is a 1-dimensional $\mathbb{F}_p$ vector space generated by $b(\pi_L^{1/p})^\ell \otimes v$. This proves (1) and (2).

Next we prove (3) in the special case where $\mathcal{M} = \mathcal{L}^{\oplus r}$ with $\mathcal{L}$ as in (7.4.4). Denote $T(\wedge^r(\mathcal{L}^{\oplus r}))$ by $T(\mathcal{L}^{\otimes r})$. By definition, $T(\mathcal{L}^{\otimes r})$ is identified with the kernel of the map

$$p^{r/p} O_{\bar{K}}/pO_{\bar{K}} \to O_{\bar{K}}/pO_{\bar{K}} \ ; \ a(\pi_L^{1/p})^{e(L)r} \mapsto a(\pi_L^{1/p})^{e(L)r} - a^p \quad (a \in O_{\bar{K}}/pO_{\bar{K}}).$$

By a similar computation as in the above proofs of (1) (2), we see that $T(\mathcal{L}^{\otimes r})$ is the 1-dimensional $\mathbb{F}_p$-vector space generated by $\pi_L^{e(L)r/(p-1)} \mod pO_{\bar{K}}$. In particular, $T(\mathcal{L})$ is the 1-dimensional $\mathbb{F}_p$-vector space generated by $\pi_L^{e(L)/(p-1)} \mod pO_{\bar{K}}$. This shows the bijectivity of $T(\mathcal{L})^{\otimes r} \to T(\mathcal{L}^{\otimes r})$.

Finally we prove (3) in general.

Let $\mathcal{M}'$ be the dual of $\mathcal{M}$ defined in (c) in 7.4, and let P, P', Q be the objects of $\mathcal{C}(L/K)$ corresponding to $\mathcal{M}$, $\mathcal{M}'$, $\mathcal{L}$, respectively. We have $Q \simeq \mu_{p,O_L}$. We have a commutative diagram where the upper row and the middle row are induced from the canonical pairings $\mathcal{M} \times \mathcal{M}' \to \mathcal{L}$ and $P \times P' \to Q$, respectively.

$$\begin{tikzcd}
\wedge^r_{\mathbb{F}_p} P(\bar{K}) \otimes \wedge^r_{\mathbb{F}_p} P'(\bar{K}) \arrow[r] \arrow[d, equal] & Q(\bar{K})^{\otimes r} \arrow[d, equal] \\
\wedge^r_{\mathbb{F}_p} T(\mathcal{M}) \otimes \wedge^r_{\mathbb{F}_p} T(\mathcal{M}') \arrow[r] \arrow[d] & T(\mathcal{L})^{\otimes r} \arrow[d] \\
T(\wedge^r \mathcal{M}) \otimes T(\wedge^r \mathcal{M}') \arrow[r] & T(\mathcal{L}^{\otimes r})
\end{tikzcd}$$

The right vertical arrow is an isomorphism as we have just shown, and the upper horizontal arrow is an isomorphism by Cartier duality. This proves that the canonical map $\wedge^r_{\mathbb{F}_p} T(\mathcal{M}) \to T(\wedge^r M)$ is injective. Since both $\wedge^r_{\mathbb{F}_p} T(\mathcal{M})$ and $T(\wedge^r M)$ are 1-dimensional over $\mathbb{F}_p$, this canonical map is bijective. □

7.10. Proof of Proposition 7.3 (2). Note that the natural map from the Grothendieck group R of all finite dimensional continuous representations of $\mathrm{Gal}(\bar{K}/K)$ over k to that of $\mathrm{Gal}(\bar{K}/K(\pi_K^{1/p}))$ induced by the restriction of the representation is bijective. This follows from the fact that all semi-simple representations factor through the tame quotient of the Galois group, and the canonical map from the tame quotient of $\mathrm{Gal}(\bar{K}/K(\pi_K^{1/p}))$ to the tame quotient of $\mathrm{Gal}(\bar{K}/K)$ is an isomorphism. We regard R as the Grothendieck group of all finite dimensional continuous representations of $\mathrm{Gal}(\bar{K}/K(\pi_K^{1/p}))$ over k.

Let $\alpha : R \to \mathbb{Q}/\mathbb{Z}[1/p]$ be as before. The following (7.10.1) and (7.10.2) are proved easily.

(7.10.1) For any finite dimensional continuous representation M of $\mathrm{Gal}(\bar{K}/K(\pi_K^{1/p}))$ over k, if r denotes the dimension of M, then $\alpha([M]) = \alpha([\wedge^r M])$.

(7.10.2) If M and M' are 1-dimensional continuous representations of $\mathrm{Gal}(\bar{K}/K(\pi_K^{1/p}))$ over k, then $\alpha([M \otimes_k M']) = \alpha([M]) + \alpha([M'])$.

Let $\mathcal{M}$ be the object of $\mathcal{C}'(L/K)$ corresponding to P and let $r = \dim_{\mathbb{F}_p}(P(\bar{K})) = \mathrm{rank}_{\mathcal{S}}(\mathcal{M})$. Then $\alpha([P(\bar{K}) \otimes_{\mathbb{F}_p} k)]) = \alpha([T(\mathcal{M}) \otimes_{\mathbb{F}_p} k])$ by (d) in 7.4, and this is equal to $\alpha([(\wedge^r T(M)) \otimes_{\mathbb{F}_p} k]) = \alpha([T(\wedge^r \mathcal{M}) \otimes_{\mathbb{F}_p} k])$ by (7.10.1) and by Lemma 7.9 (3). By Lemma 7.9 (2) and by (7.10.1) (7.10.2), the last element is equal to

$$\deg([\mathcal{M}/F^1\mathcal{M}])(p-1)^{-1}[L:K]^{-1} + \alpha(\varphi^{-1}([\mathcal{M}/u\mathcal{M}])).$$

Hence

$$\alpha([P(\bar{K}) \otimes_{\mathbb{F}_p} k)]) = \deg([\mathrm{Lie}(P)])(p-1)^{-1}[L:K]^{-1} + \alpha(\varphi^{-1}([D(P \otimes_{O_K} k)])).$$

By $\alpha \circ \varphi^{\pm 1} = p^{\pm 1}\alpha$ and by $\varphi([P(\bar{K}) \otimes_{\mathbb{F}_p} k]) = [P(\bar{K}) \otimes_{\mathbb{F}_p} k]$ (since the representation $P(\bar{K})$ is over $\mathbb{F}_p$), we obtain the formula in Proposition 7.3 (2). □

We give a preliminary lemma for the proof of Lemma 2.20 (6) in §2.

Lemma 7.11. *Let $\iota : R \to R$ be the automorphism of R which sends $\gamma(a)$ to $\gamma(-a)$. Let $x \in R$, and let $f \geq 1$ be an integer.*

Assume the following (i) and (ii).

(i) $\varphi^f(x) = x$.

(ii) $\varphi(x + \iota(x)) = x + \iota(x)$.

Then we have:

(1) Assume f is odd. Then

$$\tilde{\alpha}(x) - \tilde{\alpha}(\varphi(x)) \in 2\mathbb{Z}_{(2)}.$$

(2) Assume f is even. Then

$$\frac{p^f-1}{2}\alpha(x)=0.$$

Proof. By a p-orbit in $\mathbb{Q}/\mathbb{Z}[1/p]$, we mean a subset of $\mathbb{Q}/\mathbb{Z}[1/p]$ which has the form $\{p^i a \mid i \in \mathbb{Z}\}$ for some element $a \in \mathbb{Q}/\mathbb{Z}[1/p]$. An orbit is a finite set. If I is a p-orbit in $\mathbb{Q}/\mathbb{Z}[1/p]$, $-I = \{-a \mid a \in I\}$ is also a p-orbit in $\mathbb{Q}/\mathbb{Z}[1/p]$. For $x \in R$ and for a p-orbit I in $\mathbb{Q}/\mathbb{Z}[1/p]$, let x_I be the I-component of x (that is, for $x = \sum_{a\in\mathbb{Q}/\mathbb{Z}[1/p]} n_a\gamma(a)$ $(n_a \in \mathbb{Z})$, x_I denotes $\sum_{a\in I} n_a\gamma(a)$).

Let x be an element of R satisfying (i), (ii). If I is a p-orbit in $\mathbb{Q}/\mathbb{Z}[1/p]$ and if $I = -I$, then x_I also satisfies (i) and (ii). If I is a p-orbit in $\mathbb{Q}/\mathbb{Z}[1/p]$ and if $I \neq -I$, then $x_I + x_{-I}$ also satisfies (i) and (ii). Hence to prove the lemma, we may assume that either x belongs to $\oplus_{a\in I}\mathbb{Z}\gamma(a)$ for some p-orbit I such that $I = -I$ or x belongs to $\oplus_{a\in I\cup(-I)}\mathbb{Z}\gamma(a)$ for some p-orbit I such that $I \neq -I$.

The subset $\{0\}$ of $\mathbb{Q}/\mathbb{Z}[1/p]$ is a p-orbit. If $x \in \mathbb{Z}\gamma(0)$, then (1) and (2) for x are true clearly. Hence we may assume $I \neq \{0\}$.

Assume first f is odd, $I = -I$, and x is an element of $\oplus_{a\in I}\mathbb{Z}\gamma(a)$ satisfying the conditions (i) (ii). We prove $\varphi(x) = x$. Let $a \in I$ and take an integer s such that $-a = p^s a$. Then $\varphi^{2s}(x) = x$. Since $\varphi^f(x) = x$ and $s \in \mathbb{Z}2s + \mathbb{Z}f$ by the assumption f is odd, this shows $\varphi^s(x) = x$. Since φ^s and ι coincides on $\oplus_{a\in I}\mathbb{Z}\gamma(a)$, we have $\iota(x) = x$. Hence from $\varphi(x + \iota(x)) = x + \iota(x)$, we obtain $2\varphi(x) = 2x$. This proves $\varphi(x) = x$.

Next assume f is odd, $I \neq -I$, and x is an element of $\oplus_{a\in I\cup(-I)}\mathbb{Z}\gamma(a)$ satisfying (i) and (ii).

Claim 1. $\tilde{\alpha}(x) - \tilde{\alpha}(\varphi(x)) = 2(\tilde{\alpha}(x_I) - \tilde{\alpha}(\varphi(x_I)))$.

We prove Claim 1. We have

$$\tilde{\alpha}(x) - \tilde{\alpha}(\varphi(x)) - 2(\tilde{\alpha}(x_I) - \tilde{\alpha}(\varphi(x_I))) = -\tilde{\alpha}(x_I) + \tilde{\alpha}(x_{-I}) + \tilde{\alpha}(\varphi(x_I)) - \hat{\alpha}(\varphi(x_{-I})).$$

Since $\tilde{\alpha}(\gamma(a)) + \tilde{\alpha}(\gamma(-a)) = 1$ for any $a \in \mathbb{Q}/\mathbb{Z}[1/p] \setminus \{0\}$, this element is equal to $-\tilde{\alpha}(x_I) - \tilde{\alpha}(\iota(x_{-I})) + \tilde{\alpha}(\varphi(x_I)) + \tilde{\alpha}(\varphi(\iota(x_{-I})))$. The last element is zero because $x_I + \iota(x_{-I}) = (x + \iota(x))_I$ is invariant under φ by the assumption $\varphi(x + \iota(x)) = x + \iota(x)$.

By Claim 1, it is sufficient to prove $\tilde{\alpha}(x_I) - \tilde{\alpha}(\varphi(x_I)) \in \mathbb{Z}_{(2)}$. The image of $\tilde{\alpha}(x_I) - \tilde{\alpha}(\varphi(x_I))$ in $\mathbb{Q}/\mathbb{Z}_{(2)}$ is the image of $\alpha(x_I) - p\alpha(x_I) \in \mathbb{Q}/\mathbb{Z}[1/p]$. Note that $\alpha(x_I) = \alpha(\varphi^f(x_I)) = p^f\alpha(x_I)$. Since the order of the automorphism of the abelian group $2^{-m}\mathbb{Z}_{(2)}/\mathbb{Z}_{(2)}$ for $m \geq 0$ is a power of 2, and since f is odd, the fact $\alpha(x_I) \equiv p^f\alpha(x_I) \mod \mathbb{Z}_{(2)}$ shows that $\alpha(x_I) \equiv p\alpha(x_I) \mod \mathbb{Z}_{(2)}$.

Assume next f is even, $I = -I$, $I \neq \{0\}$, and x is an element of $\oplus_{a\in I}\mathbb{Z}\gamma(a)$ satisfying (i) (ii). Let $a \in I$ and take the smallest integer $s > 0$ such that $-a = p^s a$. Then the order of I is $2s$. Let $g = \mathrm{GCD}(2s, f)$. Then $\varphi^g(x) = x$. This shows that x is a $\mathbb{Z}$-linear combination of elements of the form $\sum_{i=0}^{2sg^{-1}-1}\gamma(p^{gi}b)$ with $b \in I$. We have

$$\frac{p^f-1}{2}\alpha(\sum_{i=0}^{2sg^{-1}-1}\gamma(p^{gi}b)) = \frac{p^f-1}{2}\cdot\frac{p^{2s}-1}{p^g-1}\cdot b = \frac{p^f-1}{p^g-1}\cdot\frac{p^s-1}{2}\cdot(p^s+1)b = 0.$$

Finally assume f is even, $I \neq -I$, and x is an element of $\oplus_{a \in I \cup (-I)} \mathbb{Z}\gamma(a)$ satisfying (i) (ii). Then

$$\alpha(x) = \alpha(x_I) + \alpha(x_{-I}) = \alpha(x_I) - \alpha(\iota(x_{-I})) = 2\alpha(x_I) - \alpha(x_I + \iota(x_{-I})).$$

Since $\varphi^f(x_I) = x_I$,

$$\frac{p^f - 1}{2} \cdot 2\alpha(x_I) = (p^f - 1)\alpha(x_I) = 0.$$

On the other hand, $x_I + \iota(x_{-I})$ is fixed by φ, and hence

$$\frac{p^f - 1}{2} \cdot \alpha(x_I + \iota(x_{-I})) = \frac{p^f - 1}{2(p-1)} \cdot (p-1)\alpha(x_I + \iota(x_{-I})) = 0$$

(note that $(p^f - 1)/(2(p-1))$ is an integer since f is even). □

7.12. Finally we prove Lemma 2.20 (6).

As K of this Appendix, take the completion of the maximal unramified extension $\hat{F}_v^{\mathrm{ur}}$ of F_v in Lemma 2.20. As L of this Appendix (we denote this field by L'), take the composite field of $\hat{F}_v^{\mathrm{ur}}$ and L in Lemma 2.20. In the following, L is the L of Lemma 2.20. We apply Proposition 7.3 by taking $P = C_{f,O_L} \otimes_{O_L} O_{L'}$, and Lemma 7.11 by taking $x = [D(C_{f,O_L} \otimes_{O_L} \bar{\mathbb{F}}_p)]$, $f = [k_v : \mathbb{F}_p]$.

We show that this element x of R satisfies the assumption of Lemma 7.11. By Lemma 2.14 (6), $\varphi^f(x) = x$. Hence it is sufficient to prove $\varphi(x + \iota(x)) = x + \iota(x)$. We denote $C_{f,O_L} \otimes_{O_L} \bar{\mathbb{F}}_p$ by $C_{f,\bar{\mathbb{F}}_p}$. We have $x = y + z$ with $y = [D(C_{f,\bar{\mathbb{F}}_p}/C_{t,\bar{\mathbb{F}}_p})]$, $z = [D(C_{t,\bar{\mathbb{F}}_p})]$. Since the representation of I_{F_v} on $D(C_{t,\bar{\mathbb{F}}_p})$ is $\mathbb{F}_p$-rational, we have $\varphi(z) = z$ and hence $\varphi(z + \iota(z)) = z + \iota(z)$. We have $\iota(y) = [D(C'_{f,\bar{\mathbb{F}}_p}/C'_{t,\bar{\mathbb{F}}_p})]$ and hence $y + \iota(y) = [D(B_{p^\infty} \otimes_{O_L} \bar{\mathbb{F}}_p)]$. For any $\sigma \in I_{F_v}$, from the fact the operator φ_p on $D(B_{p^\infty}) \otimes_{W(k_L)} \mathrm{Frac}(W(k_L))$ commutes with the action of σ, we can deduce that the characteristic polynomial of the action of σ on the vector space $D(B_{p^\infty}) \otimes_{W(k_L)} \mathrm{frac}(W(k_L))$ over $\mathrm{frac}(W(k_L))$ is a polynomial over $\mathbb{Q}_p$. Hence the characteristic polynomial of the action of σ on the $W(k_L)$-module $D(B_{p^\infty})$ is a polynomial over $\mathbb{Z}_p$, and this shows that the characteristic polynomial of the action of σ on the k_L-module $D(B_{p^\infty} \otimes_{O_L} \bar{\mathbb{F}}_p)$ is a polynomial over $\mathbb{F}_p$. Hence $\varphi(y + \iota(y)) = y + \iota(y)$.

We can write

$$\alpha([C_{f,O_L}(\bar{K}) \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p]) = i(p-1)^{-1}, \quad \alpha([D(C_{f,O_L} \otimes_{O_L} \bar{\mathbb{F}}_p]) = j(p^f - 1)^{-1} \quad \text{with } i, j \in \mathbb{Z}.$$

(the latter is due to Lemma 2.14 (6)), and we have

$$\chi_{C,v,f}(-1) = (-1)^{(p^f-1)i/(p-1)} = (-1)^{fi}, \quad \chi_{C,v,f,\mathrm{crys}}(-1) = (-1)^j.$$

Assume first f is even. Then $\mathrm{ord}_p\sharp(\mathrm{Lie}(C_{f,O_L})^\Delta)$ is even because $\mathrm{Lie}(C_{f,O_L})^\Delta$ is a module over O_{F_v} and $[\mathbb{F}_v : \mathbb{F}_p]$ is even. We have $\chi_{C,v}(-1) = (-1)^{fi} = 1$, and $\chi_{C,v,\mathrm{crys}}(-1) = (-1)^j = 1$ by Lemma 7.11 (2).

Next assume $f = [k_v : \mathbb{F}_p]$ is odd. By Proposition 7.3 (2), we have

$$i(p-1)^{-1} + j(p^f - 1)^{-1} = \ell(p-1)^{-1}[L' : K]^{-1} \text{ in } \mathbb{Q}/\mathbb{Z}[1/p]$$

where ℓ is the length of the O_L-module $\mathrm{Lie}(C_{f,O_L})$. Multiply this by p^f-1. Then using the fact f is odd, we obtain

$$i+j \equiv \ell[L':K]^{-1} \mod 2\mathbb{Z}_{(2)}.$$

By Proposition 7.3 (1) and Lemma 7.11 (1), $\ell[L':K]^{-1} \equiv \delta_0 \mod 2\mathbb{Z}_{(2)}$ where δ_0 is the length of $\mathrm{Lie}(C_{f,O_L})^{\Delta}$ as an O_{F_v}-module. Since $\chi_{C,v}(-1)\chi_{C,v,\mathrm{crys}}(-1)=(-1)^{i+j}$, this proves Lemma 2.20 (6). □

References

[1] Bass, H., Algebraic K-theory, Benjamin, NewYork (1966).

[2] Bourbaki, N., Elements of Mathematics, Commutative Algebra, Chapters 1–7, Springer (1989).

[3] Breuil, C., *Groupes p-divisibles, groupes finis et modules filtrés*, Ann. of Math. **152** (2000) 489–547.

[4] Birch, B., J., Stephens, N., *The parity of the rank of the Mordell-Weil group*, Topology **5** (1966), 295–299.

[5] Cartan, H., Eilenberg, S., Homological Algebra, Princeton University Press (1956).

[6] Curtis. C.W., Methods of representation theory, vol. I, John Wiley & Sons, (1981).

[7] Coates, J., Howson, S., *Euler characteristics and elliptic curves II*, J. Math. Soc. Japan **53** (2001), 175–235.

[8] Coates, J., Fukaya, T., Kato, K., Sujatha, R., Venjakob, O., *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES **101** (2005), 163-208.

[9] Coates, J., Greenberg, R., *Kummer theory for abelian varieties over local fields*, Invent. Math. **124** (1996), 129-174.

[10] Coates, J., Schneider, P., Sujatha, R., *Links between GL_2 and cyclotomic Iwasawa theory*, Documenta Math. (Extra Volume: Kazuya Kato's fiftieth birthday) (2003), 187–215.

[11] Coates, J., Sujatha, R., Galois cohomology of elliptic curves, Tata Institute of Fundamental Research Lectures on Mathematics 88, Narosa Publishing House, New Delhi (2000).

[12] Coates, J., Sujatha,R., Wintenberger, J.-P, *On the Euler-Poincaré characteristics of finite dimensional p-adic Galois representations.* Publ. Math. IHES **93** (2001), 107-143.

[13] Deligne, P., *Les constantes des équations fonctionnelles des fonctions L*, Modular functions of one variable, II, Lecture Notes in Math. **349** Springer (1973), 501–597.

[14] Darmon, H., Tian, Y., *Heegner points over false Tate curve extensions*, Preprint.

[15] Dokchitser, V., *Root numbers of non-abelian twists of elliptic curves*, with Appendix by Fisher, T., Proc. London Math. Soc. **91** (2005), 300-324.

[16] Dokchitser, T., Dokchitser, V., *Numerical computations in non-commutative Iwasawa theory*, with Appendix by Coates, J., and Sujatha, R., Proc. London Math. Soc. **94** (2006), 211-272

[17] Dokchitser, T., Dokchitser, V., *Ranks of elliptic curves with a cyclic isogeny*, Journal of Number Theory, (To appear).

[18] Dokchitser, T., Dokchitser, V., *On the Birch Swinnerton-Dyer quotients modulo squares*, arXiv:math/0610290v2 [math.NT].

[19] Dokchitser, T., Dokchitser, V., *Regulator constants and the parity conjecture*, preprint (2007).

[20] Flach, M. *A generalisation of the Cassels-Tate pairing*, J. Reine Angew Math. **512** (1990), 113–127.

[21] Greenberg, R., *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves, Lecture Notes in Math.**1716** Springer (1999), 51–144.

[22] Greenberg, R., *Iwasawa theory of p-adic representations*, in "Algebraic Number Theory - in honor of K. Iwasawa", Advanced Studies in Pure Math. **17**, Kinokuniya (1989), 97–137.

[23] Greenberg,R., *Iwasawa theory, projective modules, and modular representations*, Preprint (2007).

[24] Guo, L., *General Selmer groups and critical values of Hecke L-functions*, Math. Ann. 297 (1993), 221–233.

[25] Hachimori, Y., Matsuno, K., *An analogue of Kida's formula for the Selmer groups of elliptic curves*, J. Algebraic Geom. 8 (1999), no. 3, 581–601.

[26] Hachimori, Y., Venjakob, O., *Completely faithful Selmer groups over Kummer extensions*, Documenta Math. (Extra Volume: Kazuya Kato's fiftieth birthday) (2003), 443–478.

[27] Kato, K., *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et applications arithmétiques III, Astérisque **295** (2004), 117–290.

[28] Kim, B.-D., *The parity conjecture and algebraic functional equations for elliptic curves at supersingular reduction primes*, Ph.D Thesis, Stanford University (2005).

[29] Matsuno, K., *Finite Λ-submodules of Selmer groups of abelian varieties over cyclotomic $\mathbb{Z}_p$-extensions*, J. Number Theory 99 (2003), no. 2, 415–443.

[30] Mazur, M., Rubin, K., *Finding large Selmer ranks via an arithmetic theory of local constants*, Ann. of Math. (To appear).

[31] Mazur, M., Rubin, K., *Growth of Selmer ranks in nonabelian extensions of number fields*, (Preprint) (2006).

[32] Milne, J.S. Arithmetic Duality theorems, Progress. in Math. 1 (1986), Birkhäuser.

[33] Monsky, P., *Generalizing the Birch-Stephens theorem*, Math. Z., 221 (1996), 415–420.

[34] Nekovář, J., *Selmer complexes*, Astérisque, (To appear).

[35] Nekovář, J., *On the parity of ranks of Selmer groups. II*, C.R. Acad. Sci. Paris, 332 (2001), 99–104.

[36] Raynaud, M., *Variétés abéliennes et géométrie rigid*, Actes du Congrès International des Mathématiciens (Nice 1970), Tome 1, 473–477.

[37] Rohrlich, D.E., *Galois theory, elliptic curves, and root numbers*, Compositio Math. **100** (1996), 311–349.

[38] Rohrlich, D. E., *Scarcity and abundance of trivial zeros in division towers*, Journal of Algebraic Geometry, (To appear).

[39] Serre, J.-P., *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[40] Serre, J.-P., Linear representations of finite groups, GTM 42, Springer.

[41] Serre, J.-P., *Sur la dimension cohomologique des groupes profinis*, Topology **3** (1965), 413–420.

[42] Grothendieck, A. et al., Groupes de monodromie en géométrie algébrique (SGA 7, Vol 1), Lecture Notes in Math. **288** (1972).

[43] Shuter, M., *Descent on division fields of elliptic curves*, Cambridge Ph.D Thesis (2006).

[44] Swan, R., *The Grothendieck ring of a finite group*, Topology **2** (1963), 85–110.

[45] Swan, R., K-theory of finite groups and orders, LNM 149, Springer (1970).

J. C.
DPMMS, University of Cambridge,
Centre for Mathematical Sciences,
Wilberforce Road, Cambridge CB3 0WB, England.
J.H.Coates@dpmms.cam.ac.uk

T. F.
Keio University,
Hiyoshi, Kohoku-ku, Yokohama, 223-8521, Japan.
takakof@hc.cc.keio.ac.jp

K. K.
Department of Mathematics, Kyoto University,
Kyoto, 606-8502, Japan.
kzkt@math.kyoto-u.ac.jp

R. S.
School of Mathematics, Tata Institute of Fundamental Research,
Homi Bhabha Road, Mumbai 400 005, India.
sujatha@math.tifr.res.in