Invent. math. 124, 129–174 (1996)

Inventiones mathematicae

Kummer theory for abelian varieties over local fields

J. Coates[1], R. Greenberg[2,★]

[1] Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, 16 Mill Lane, Cambridge CB2 1SB, UK
[2] Department of Mathematics, University of Washington, Box 354350, Seattle, WA 98195, USA

Oblatum 29-III-1995 & 12-IV-1995

to Reinhold Remmert

1 Introduction

This paper attempts to throw new light on two classical questions about the arithmetic of abelian varieties over local fields. Let p be any prime number, $\mathbb{Q}_p$ the field of p-adic numbers, and $\overline{\mathbb{Q}}_p$ a fixed algebraic closure of $\mathbb{Q}_p$. Let A be an abelian variety, which is defined over a finite extension F of $\mathbb{Q}_p$ lying inside of $\overline{\mathbb{Q}}_p$. As usual, we let $A[p^\infty]$ denote the p-primary subgroup of $A(\overline{\mathbb{Q}}_p)$. It is endowed with a natural action of the Galois group $G_F = G(\overline{\mathbb{Q}}_p/F)$. Now let K be any extension of F contained in $\overline{\mathbb{Q}}_p$. We recall that the classical Kummer homomorphism

$$\kappa_{A,K} : A(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(K, A[p^\infty]) \tag{1.1}$$

is defined by mapping $P \otimes (p^{-n} \bmod \mathbb{Z}_p)$ (where $P \in A(K)$, $n \geqq 0$) to the class of the 1-cocycle φ defined by $\varphi(\sigma) = \sigma(Q) - Q$ for all $\sigma \in G_K$; here Q is any point in $A(\overline{\mathbb{Q}}_p)$ such that $p^n Q = P$. The first and main problem we shall be concerned with in this paper is:

(I) To find a description of the image of $\kappa_{A,K}$ solely in terms of the G_F-module $A[p^\infty]$.

The main earlier work on (I) is due to Bloch and Kato ([1], Sect. 3), who provided an answer to it for all finite extensions K of F, by using Fontaine's mysterious ring B_{DR}. This is a highly important result. In this article, we shall be primarily concerned with infinite extensions of F. Our approach has been partly motivated by the earlier celebrated paper of Tate [18]. By generalizing the arguments of Sect. 3 of [18], we have been led to introduce a new class of infinite algebraic extensions K of $\mathbb{Q}_p$, which we call *deeply ramified*. The

★ Supported partially by a National Science Foundation grant

simplest example of a deeply ramified extension is a ramified $\mathbb{Z}_p$-extension of a finite extension of $\mathbb{Q}_p$. More generally, a theorem of Sen [15] shows that if K is any p-adic Lie extension, with infinite inertial subgroup, of a finite extension of $\mathbb{Q}_p$, then K is deeply ramified (see Theorem 2.13). In Sect. 3, we explain how Tate's arguments for the formal additive group over a ramified $\mathbb{Z}_p$-extension generalize beautifully to arbitrary commutative formal groups over any deeply ramified extension of the base field. This gives us an analogue of Hilbert's Theorem 90 for commutative formal groups, which then enables us to give a remarkably simple answer to problem (I) when K is deeply ramified (see Proposition 4.3). We will also show that the same result is valid if we make the weaker assumption that K is infinitely wildly ramified, but impose an additional condition on the nature of the reduction of A (for example, that A has good, ordinary reduction over F; see Proposition 4.7).

To describe the second question, which we consider in Sect. 5, we use the following notation. If X is a torsion abelian group, we write $X(p)$ for its p-primary subgroup, and if X is a profinite abelian group, we let X_p denote its maximal pro-p subgroup. Let

$$r_{K/F} : H^1(F, A(\overline{\mathbb{Q}}_p))(p) \to H^1(K, A(\overline{\mathbb{Q}}_p))(p) \tag{1.2}$$

be the restriction homomorphism. We recall that Tate duality gives an alternative description of the image and kernel of $r_{K/F}$ in terms of universal norms. Let A^t be the dual abelian variety of A. Put

$$N_{K/F}(A^t) = \bigcap_{F'} N_{F'/F}(A^t(F')) , \tag{1.3}$$

where F' runs over all finite extensions of F contained in K, and $N_{F'/F}$ denotes the norm map from F' to F on A^t. Then Tate duality asserts that $A^t(F)_p$ is canonically dual to $H^1(F, A(\overline{\mathbb{Q}}_p))(p)$. Moreover, $N_{K/F}(A^t)_p$ is the exact orthogonal complement of $\mathrm{Ker}(r_{K/F})$ in this duality. Thus, $\mathrm{Im}(r_{K/F})$ is canonically dual to $N_{K/F}(A^t)_p$. The second problem is:

(II) To find a description of $\mathrm{Ker}(r_{K/F})$ in terms of the G_F-module $A[p^\infty]$.

Such a description would give the structure of $\mathrm{Im}(r_{K/F})$, and hence its dual $N_{K/F}(A^t)_p$. In Sect. 5, we will exploit a certain simple connection between problems (I) and (II). This allows us to give a solution to problem (II) for those fields K for which our answer to problem (I) is valid (see Theorem 5.2). For such fields K, we then obtain quite precise results about the subgroup $N_{K/F}(A^t)$ of universal norms. We also discuss in Sect. 5 several applications of Theorem 5.2 to special cases. In particular, we show how all earlier results concerning universal norms on abelian varieties can be derived and generalized in a rather simple fashion.

The original motivation for this paper was our realization many years ago that, for an elliptic curve defined over a number field which has good reduction at all primes above p, the p-Selmer group for E over the cyclotomic $\mathbb{Z}_p$-extension of the base field could be described in a simple way just in terms

of the Galois module $E[p^\infty]$. This description came from the fact that the images of the local Kummer homomorphisms which intervene in the definition of this Selmer group could be described quite simply. At the primes over p, the description depended on whether E has ordinary or supersingular reduction. It then seemed quite natural to ask for such a description for arbitrary abelian varieties over more general classes of extensions.

One application of these results, which the second author will describe in a subsequent article concerns the Galois theoretic behaviour of the p-Selmer group for abelian varieties with good ordinary reduction at all primes over p in certain infinite extensions of number fields. Results in this direction have been found by Mazur in [12] (Mazur's control theorem) and by Harris in [7]. However, by using the quite simple descriptions of the images of local Kummer homomorphisms given in Sect. 4, one can approach such questions in a simpler way, obtaining more general and sometimes more precise results.

The results of Sect. 4 suggest a rather natural and interesting question concerning p-adic representations V_p of G_F, where again F is a finite extension of $\mathbb{Q}_p$ (for example, V_p could be the p-adic realization of some motive). Then, as in [1], one defines

$$H^1_f(F', V_p) = \mathrm{Ker}(H^1(F', V_p)) \to H^1(F', V_p \otimes B_{\mathrm{cris}})$$

for any finite extension F' of F. Let T_p be a G_F-invariant $\mathbb{Z}_p$-lattice in V_p, and put $\mathscr{A} = V_p/T_p$. We then define

$$H^1_f(F', \mathscr{A}) = \phi_{F'}(H^1_f(F', V_p))\,,$$

where $\phi_{F'} : H^1(F', V_p) \to H^1(F', \mathscr{A})$ is the map induced by the canonical surjection of V_p onto $\mathscr{A}$. For an arbitrary algebraic extension K of F, one can define a certain subgroup of $H^1(K, \mathscr{A})$ by

$$H^1_f(K, \mathscr{A}) = \varinjlim_{F'} H^1_f(F', \mathscr{A})\,,$$

where F' runs over all finite extensions of F contained in K. One can then ask if there is an analogue of Proposition 4.3 which would describe $H^1_f(K, \mathscr{A})$ for some class of infinite extensions K of F. Similarly, one can define $H^1_e(K, \mathscr{A})$ and $H^1_g(K, \mathscr{A})$ following [1], and pose an analogous question for these subgroups of $H^1(K, \mathscr{A})$. We note that, if $V_p = T_p(A) \otimes \mathbb{Q}_p$ and $T_p = T_p(A)$, where A is an abelian variety over F with good reduction, then $\mathscr{A} = A[p^\infty]$ and $H^1_*(K, \mathscr{A})$, where $* = e, f, g$, is the image of the Kummer homomorphism $\kappa_{K,A}$.

Notation. All fields considered in this paper will be algebraic extensions of $\mathbb{Q}_p$ lying inside our fixed algebraic closure $\overline{\mathbb{Q}}_p$ (except for one minor digression in the proof of Theorem 2.13). We write ord for the order function on $\overline{\mathbb{Q}}_p^\times$, normalized so that $\mathrm{ord}(p) = 1$. When K is a finite extension of $\mathbb{Q}_p$, we put $e(K)$ for the ramification index of K over $\mathbb{Q}_p$, and it will also sometimes be convenient to use the order function $\mathrm{ord}_K = e(K)\mathrm{ord}$. For any algebraic

extension K of $\mathbb{Q}_p$, we write O_K for its ring of integers, $\mathfrak{m}_K$ for the maximal ideal of O_K, and $k_K = O_K/\mathfrak{m}_K$ for its residue field. For simplicity, we write $\overline{\mathfrak{m}}$ for the maximal ideal of the ring of integers of $\overline{\mathbb{Q}}_p$. We denote by G_K the Galois group of $\overline{\mathbb{Q}}_p$ over K. If M is a topological G_K-module, $H^i(K,M)$ will denote the G_K-cohomology groups of M, which are defined using continuous cochains.

2 Deeply ramified extensions

The aim of this section is to study a class of fields lying inside $\overline{\mathbb{Q}}_p$, which are of infinite degree over $\mathbb{Q}_p$, and which turn out to have a number of remarkable properties. Our original interest in these fields was motivated by cohomological arguments (see Sect. 3–Sect. 5), but we have decided to call them *deeply ramified* because of their connection with higher ramification theory. The whole of this section is devoted to proving the equivalence of various definitions of this class of fields, and many of our arguments have been inspired by Sect. 3 of Tate's celebrated paper [18].

Throughout, F will denote a finite extension of $\mathbb{Q}_p$, and we write G_F for the Galois group of $\overline{\mathbb{Q}}_p$ over F. For each $w \in [-1,\infty)$, we write $G_F^{(w)}$ for the w-th ramification subgroup of G_F in the upper numbering (recall that it is only the upper numbering which can be defined for infinite extensions – see Serre [17], Chap. 4, Sect. 3). We write $F^{(w)}$ for the fixed field of $G_F^{(w)}$. Let L be an arbitrary finite extension of F, and let $\delta(L/F)$ denote the different of L over F. We also write $e(L/F)$ for the ramification index of L over F. The following lemma will play a crucial role in the arguments of this section. It is well known in the Galois case, but we have been unable to find it in the literature in the non-Galois case.

Lemma 2.1 *Let L be an arbitrary finite extension of F. Then $\delta(L/F) = \mathfrak{m}_L^{a(L/F)}$, where*

$$a(L/F) = e(L/F)\int_{-1}^{\infty}\left(1 - \frac{1}{[L : L \cap F^{(w)}]}\right) \mathrm{d}w\,. \tag{2.1}$$

Remark. Since L is a finite extension of F, we must have $L \subset F^{(w)}$ for all sufficiently large w. Hence the integrand in the above formula is zero for all sufficiently large w.

Proof. We shall deduce (2.1) from the classical formula for the different of a finite Galois extension of F, in terms of the ramification groups for this extension in the lower numbering (see [17], Chap. IV, Prop. 4). Specifically, take M to be any finite Galois extension of F containing L. By the multiplicativity of the different, we have $\delta(M/L)\cdot\delta(L/F) = \delta(M/F)$, and thus

$$\mathrm{ord}_M(\delta(L/F)) = \mathrm{ord}_M(\delta(M/F)) - \mathrm{ord}_M(\delta(M/L))\,. \tag{2.2}$$

Put $G = G(M/F)$, and let H be the subgroup of G which fixes L. For $w \in [-1, \infty)$, let $G^{(w)}$ (resp. $G_{(w)}$) be the w-th ramification subgroup of G in the upper (resp. lower) numbering, and similarly for H. By the classical formula cited above, we have

$$\mathrm{ord}_M(\delta(M/F)) = \int_{-1}^{\infty} (\#(G_{(t)}) - 1)\,\mathrm{d}t, \quad \mathrm{ord}_M(\delta(M/L)) = \int_{-1}^{\infty} (\#(H_{(t)}) - 1)\,\mathrm{d}t$$

whence, by (2.2),

$$\mathrm{ord}_L(\delta(L/F)) = \frac{1}{e(M/L)} \int_{-1}^{\infty} (\#(G_{(t)}) - \#(H_{(t)}))\,\mathrm{d}t\,. \tag{2.3}$$

Thus we must show that the right hand side of (2.1) is equal to this last expression. For each $w \in [-1, \infty)$, $L \cap F^{(w)}$ is the fixed field of $G^{(w)}H = HG^{(w)}$, and thus

$$[L : L \cap F^{(w)}] = \#(G^{(w)}H)/\#(H) = \#(G^{(w)}/G^{(w)} \cap H)\,. \tag{2.4}$$

This last expression suggests that we pass from the upper numbering to the lower numbering for G. Thus let $\varphi_{M/F} : [-1, \infty) \to [-1, \infty)$ be the Herbrand function for M over F (see [17], Chap. IV, Sect. 3). Thus, if $w = \varphi_{M/F}(t)$, we have $G^{(w)} = G_{(t)}$ by the definition of the upper numbering. Moreover, for all $t \in [-1, \infty)$ with $t \notin \mathbb{Z}$, we have

$$\varphi'_{M/F}(t) = \#(G_{(t)})/\#(G_{(0)})\,.$$

Hence, making the change of variable $w = \varphi_{M/F}(t)$ in the integral on the right of (2.1), and recalling that

$$G_{(t)} \cap H = H_{(t)}$$

by a fundamental property of the lower numbering, we deduce from (2.4) that the right hand side of (2.1) is equal to

$$e(L/F) \int_{-1}^{\infty} \left(1 - \frac{\#(H_{(t)})}{\#(G_{(t)})}\right) \frac{\#(G_{(t)})}{\#(G_{(0)})}\,\mathrm{d}t\,.$$

This is clearly equal to the right hand side of (2.3), since

$$\#(G_{(0)}) = e(M/F) = e(M/L) \cdot e(L/F)\,.$$

If L is any finite extension of F, we recall that the conductor $f(L/F)$ is defined to the infimum of all $w \in [0, \infty)$ such that $L \subset F^{(w-1)}$.

Corollary 2.2 *If L is an arbitrary finite extension of F, we have*

$$e(L/F)f(L/F)/2 \leqq \mathrm{ord}_L(\delta(L/F)) \leqq e(L/F)f(L/F)\,,$$

where $f(L/F)$ is the conductor of L over F.

Proof. Consider the integrand in (2.1). It is clearly 0 when $w > f(L/F) - 1$, since in this case, we have $F^{(w)} \cap L = L$. On the other hand, the integrand is $\geqq \frac{1}{2}$ for $w < f(L/F) - 1$ because $F^{(w)} \cap L \neq L$ in this case. Hence the assertion is clear.

We now recall a classical lemma, which will be used frequently in the subsequent arguments.

Lemma 2.3 *Let L be a finite extension of F. Then* $\mathrm{Tr}_{L/F}(O_L) = \mathfrak{m}_F^{b(L/F)}$, *where* $b(L/F)$ *is the integral part of* $\mathrm{ord}_L(\delta(L/F))/e(L/F)$.

Proof. Put t equal to the integral part of $\mathrm{ord}_L(\delta(L/F))/e(L/F)$. Let π_F denote a local parameter of F. Now $te(L/F) \leqq \mathrm{ord}_L(\delta(L/F))$, and so

$$\pi_F^{-t} O_L \subset \delta(L/F)^{-1} ,$$

which gives the inclusion $\mathrm{Tr}_{L/F}(O_L) \subset \pi_F^t O_F$. On the other hand, we have $(t+1)e(L/F) > \mathrm{ord}_L(\delta(L/F))$, whence it follows from the definition of the different that $\mathrm{Tr}_{L/F}(O_L)$ is not contained in $\pi_F^{t+1} O_F$. Since $\mathrm{Tr}_{L/F}(O_L)$ is clearly an ideal of O_F, the proof is complete.

As always, we suppose F is a finite extension of $\mathbb{Q}_p$, and we let K be any extension of F lying inside $\overline{\mathbb{Q}}_p$. We say that K has *finite conductor* over F if $K \subset F^{(w)}$ for some fixed $w \in [-1, \infty)$. Recall that ord denotes the order function on $\overline{\mathbb{Q}}_p^{\times}$, normalised so that $\mathrm{ord}(p) = 1$.

Proposition 2.4 *The following assertions are equivalent*:
(i) *K has finite conductor over F*;
(ii) $\mathrm{ord}(\delta(F'/F))$ *is bounded as F' runs over all finite extensions of F contained in K.*

Remark. By the multiplicativity of the different, we see from (ii) that the proposition implies that K has finite conductor over F if and only if K has finite conductor over $\mathbb{Q}_p$. One can give a direct proof of this latter statement using ramification theory, but it is not entirely obvious. In any case, we shall omit all mention of the base field F in the future, and simply speak of K having finite conductor or not.

Proof. First assume that K has finite conductor over F, so that $K \subset F^{(u)}$ for some $u \in [-1, \infty)$. It follows that $f(F'/F) \leqq u + 1$ for all finite extensions F' of F which are contained in K. Hence, by Corollary 2.2, we have

$$\mathrm{ord}(\delta(F'/F)) \leqq (u+1)/e(F) ,$$

where $e(F)$ is the absolute ramification index of F, and this establishes the required boundedness. Conversely, assume that $\mathrm{ord}(\delta(F'/F)) \leqq C$ as F' ranges

over all finite extensions F' of F contained in K. We conclude immediately from the lower bound of Corollary 2.2 that

$$f(F'/F) \leqq 2e(F)C\,.$$

This implies that every such F' is contained in $F^{(w)}$ for any $w > 2e(F)C$, and so $K \subset F^{(w)}$ for any such w. This completes the proof.

In many of the following arguments, we will be primarily interested in the case when K is an infinite extension of $\mathbb{Q}_p$. Nevertheless, we shall need to study questions about K via finite extensions of $\mathbb{Q}_p$. We do this by writing K as a tower of finite extensions of $\mathbb{Q}_p$, say

$$K = \bigcup_{n=0}^{\infty} F_n, \quad F_n \subseteq F_{n+1} \quad \text{for all} \quad n \geqq 0,\ [F_n : \mathbb{Q}_p] < \infty\,. \tag{2.5}$$

It will not matter which particular tower we choose satisfying (2.5).

Proposition 2.5 *Assume that K has finite conductor. Then there exist finite cyclic extensions K' of K such that* $\mathrm{Tr}_{K'/K}(\mathfrak{m}_{K'}) \neq \mathfrak{m}_K$.

Remark. For each $t \geqq 0$, let Φ_t denote the unique subfield of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$ which is of degree p^t over $\mathbb{Q}_p$. Then the proof of Proposition 2.5 will show that we can take $K' = K\Phi_t$ whenever t is sufficiently large.

Proof. We claim that, provided n is sufficiently large, we have

$$\mathrm{Tr}_{F_n/\mathbb{Q}_p}(O_{F_n}) = p^b\mathbb{Z}_p\,, \tag{2.6}$$

where b is an integer $\geqq 0$, which is independent of n. Indeed, let us define $b_n \geqq 0$ by $\mathrm{Tr}_{F_n/\mathbb{Q}_p}(O_{F_n}) = p^{b_n}\mathbb{Z}_p$. Clearly $b_{n+1} \geqq b_n$ for all $n \geqq 0$. Define $r_n = \mathrm{ord}_{F_n}(\delta(F_n/\mathbb{Q}_p))$. Then, by Lemma 2.3, b_n is equal to the integer part of r_n/e_n, where $e_n = e(F_n)$ is the absolute ramification index of F_n. Hence $b_n \leqq r_n/e_n = \mathrm{ord}(\delta(F_n/\mathbb{Q}_p))$. But Proposition 2.4 shows that $\mathrm{ord}(\delta(F_n/\mathbb{Q}_p))$ is bounded because K has finite conductor. Hence b_n must be constant for all n greater than or equal to some fixed integer n_0, proving (2.6). As above, let Φ_t be the t-th layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$. In the rest of the proof, we will suppose that t is sufficiently large but fixed (in fact, we shall see below that we need $t > b+2$), and we consider the fields $F_n' = F_n\Phi_t$. We shall prove that, provided $t > b+2$, we have

$$\mathrm{Tr}_{F_n'/F_n}(\mathfrak{m}_{F_n'}) \subset p\mathfrak{m}_{F_n} \quad \text{for all} \quad n \geqq n_0\,. \tag{2.7}$$

Let us first note that (2.7) implies Proposition 2.5. Indeed, take $K' = K\Phi_t$. Choose x lying in $\mathfrak{m}_K$ but not in $p\mathfrak{m}_K$. If the trace map from $\mathfrak{m}_{K'}$ to $\mathfrak{m}_K$ was surjective, we would have $x = \mathrm{Tr}_{K'/K}(y)$ for some $y \in \mathfrak{m}_{K'}$. But then y belongs to $\mathfrak{m}_{F_n'}$ for all sufficiently large n. Since restriction plainly defines an isomorphism from $G(K'/K)$ onto $G(F_n'/F_n)$ for all sufficiently large n, we see

that this contradicts (2.7). We now turn to the proof of (2.7). Suppose that (2.7) is false for some integer $n \geqq n_0$. Since $\mathrm{Tr}_{F'_n/F_n}(\mathfrak{m}_{F'_n})$ is an ideal of O_{F_n}, we must therefore have

$$\mathrm{Tr}_{F'_n/F_n}(\mathfrak{m}_{F'_n}) \supseteq p\mathfrak{m}_{F_n} .$$

Taking traces of both sides to $\mathbb{Q}_p$, and recalling that (2.5) holds for $n \geqq n_0$, we deduce that

$$\mathrm{Tr}_{F'_n/\mathbb{Q}_p}(\mathfrak{m}_{F'_n}) \supseteq p\mathrm{Tr}_{F_n/\mathbb{Q}_p}(\mathfrak{m}_{F_n}) \supseteq p^{b+2}\mathbb{Z}_p .$$

But $\Phi_t \subset F'_n$, and so we obtain finally that

$$\mathrm{Tr}_{\Phi_t/\mathbb{Q}_p}(\mathfrak{m}_{\Phi_t}) \supseteq p^{b+2}\mathbb{Z}_p . \tag{2.8}$$

On the other hand, we claim that

$$\mathrm{Tr}_{\Phi_t/\mathbb{Q}_p}(\mathfrak{m}_{\Phi_t}) \subset p^t\mathbb{Z}_p . \tag{2.9}$$

Let ζ_t be a root of unity of exact order p^{t+1} if p is odd, and exact order 2^{t+2} if $p = 2$. Let $\Omega_t = \mathbb{Q}_p(\zeta_t)$, so that $\Omega_t \supset \Phi_t$ and $g = [\Omega_t : \Phi_t]$ is equal to $p-1$ or 2 according as p is odd or even. Now the trace to $\mathbb{Q}_p$ of any p-power root of unity $\neq 1$ is equal to 0, unless the root of unity is of exact order p, in which case the trace is equal to -1. Since $O_{\Omega_t} = \mathbb{Z}_p[\zeta_t]$, it follows that $\mathrm{Tr}_{\Omega_t/\mathbb{Q}_p}(O_{\Omega_t}) \subseteq g \cdot p^t \cdot \mathbb{Z}_p$. Hence

$$\mathrm{Tr}_{\Phi_t/\mathbb{Q}_p}(\mathfrak{m}_{\Phi_t}) \subseteq g^{-1}\mathrm{Tr}_{\Omega_t/\mathbb{Q}_p}(O_{\Omega_t}) \subseteq p^t\mathbb{Z}_p , \tag{2.10}$$

which establishes (2.9). But (2.8) and (2.9) are plainly contradictory when $t > b+2$. This completes the proof of Proposition 2.5.

Now, let K' be any finite extension of K. It is easy to see and well known (see [17], Chap. V, Sect. 4, Lemma 6) that one can then realize the extension K' over the fields F_n as follows. There exists an integer $n_0 \geqq 0$ and a finite extension F'_{n_0} of F_{n_0} satisfying:

$$F'_{n_0}K = K', \quad F'_{n_0} \cap K = F_{n_0}, \quad [K' : K] = [F'_{n_0} : F_{n_0}] . \tag{2.11}$$

Moreover, if K' is a Galois extension of K, then we can also choose F'_{n_0} to be a Galois extension of F_{n_0}. Once we have the field F'_{n_0}, we then define $F'_n = F'_{n_0}F_n$ for all $n \geqq n_0$.

Lemma 2.6 *For all fields K with $\mathbb{Q}_p \subset K \subset \overline{\mathbb{Q}}_p$, and all finite extensions K' of K, there exists $\eta = \eta(K'/K) \geqq 0$ such that*

$$\lim_{n\to\infty} \mathrm{ord}\,(\delta(F'_n/F_n)) = \eta . \tag{2.12}$$

Proof. We will show that $\mathrm{ord}(\delta(F'_n/F_n))$ is a decreasing sequence for all $n \geqq n_0$, whence the assertion of the lemma is clear, because we always have $\mathrm{ord}(\delta(F'_n/F_n)) \geqq 0$. Put $d = [K' : K]$. We claim that any basis of F'_n

over F_n is also a basis of F'_m over F_m for all $m \geqq n$. This is clear because $[F'_m : F_m] = [F'_n : F_n] = d$. For each $n \geqq n_0$, let $\omega_1(n), \ldots, \omega_d(n)$ be a basis of $O_{F'_n}$ as an O_{F_n}-module. Recall that the discriminant of F'_n over F_n, which we denote by $\Delta(F'_n/F_n)$, is the O_{F_n}-ideal generated by $\det(\sigma_j(\omega_i(n)))^2$, where $\sigma_1, \ldots, \sigma_d$ denote the distinct embeddings of F'_n in $\overline{\mathbb{Q}}_p$, which leave F_n fixed. Since $N_{F'_n/F_n}(\delta(F'_n/F_n)) = \Delta(F'_n/F_n)$, we see that

$$\text{ord}(\delta(F'_n/F_n)) = \frac{1}{d}\text{ord}(\Delta(F'_n/F_n))\,. \tag{2.13}$$

Now suppose that $m \geqq n$. Since $\omega_1(n), \ldots, \omega_d(n)$ are linearly independent over F_m, they generate over O_{F_m} a submodule of finite index in $O_{F'_m}$. If we define the $d \times d$ matrix $A = (a_{ih})$, where $\omega_i(n) = \sum_{h=1}^{d} a_{ih}\omega_i(m)$, we clearly have

$$\det(\sigma_j(\omega_i(n)))^2 = \det(A)^2\det(\sigma_j(\omega_i(m)))^2\,.$$

Since the entries of A are integers of O_{F_m}, we deduce that $\text{ord}(\Delta(F'_n/F_n)) \geqq \text{ord}(\Delta(F'_m/F_m))$. It now follows from (2.13) that $\text{ord}(\delta(F'_n/F_n)) \geqq \text{ord}(\delta(F'_m/F_m))$ whenever $m \geqq n$, and the proof of Lemma 2.6 is now complete.

Lemma 2.7 *If K' is a finite extension of K such that* $\lim_{n\to\infty}\text{ord}(\delta(F'_n/F_n)) = 0$, *then* $\text{Tr}_{K'/K}(\mathfrak{m}_{K'}) = \mathfrak{m}_K$.

Proof. The argument divides into two cases. First, assume that $e(F_n)$ is bounded as $n \to \infty$, which implies that there exists an integer n_1 so that K/F_{n_1} is unramified. Hence, by the multiplicativity of the different, we have $\delta(F'_{n+1}/F_{n+1}) = \delta(F'_n/F_n)$ for all $n \geqq n_1$. Hence, as the limit is 0, we must have $\delta(F'_n/F_n) = O_{F'_n}$ for all $n \geqq n_1$, i.e. F'_n/F_n is unramified for all $n \geqq n_1$. But then Lemma 2.3 shows that $\text{Tr}_{F'_n/F_n}(\mathfrak{m}_{F'_n}) = \mathfrak{m}_{F_n}$ for all $n \geqq n_1$, which plainly implies that $\text{Tr}_{K'/K}(\mathfrak{m}_{K'}) = \mathfrak{m}_K$. Secondly, suppose that $e(F_n) \to \infty$ as $n \to \infty$. Thus, if π_n denotes a local parameter of F_n, we have $\text{ord}(\pi_n) \to 0$ as $n \to \infty$. Define the integers $a_n \geqq 0$ for $n \geqq n_0$ by

$$\text{Tr}_{F'_n/F_n}(O_{F'_n}) = \pi_n^{a_n}O_{F_n}\,. \tag{2.14}$$

By Lemma 2.3, a_n is bounded above by $\text{ord}_{F'_n}(\delta(F'_n/F_n))/e(F'_n/F_n)$, and so we see that

$$\text{ord}(\pi_n^{a_n}) \leqq \text{ord}(\delta(F'_n/F_n))\,. \tag{2.15}$$

Hence we deduce that $\lim_{n\to\infty}\text{ord}(\pi_n^{a_n}) = 0$, whence also $\lim_{n\to\infty}\text{ord}(\pi_n^{a_n+1}) = 0$. If $x \in \mathfrak{m}_K$, we can find an $r \geqq n_0$ so that $x \in O_{F_r}$. Choose $n \geqq r$ so that $\text{ord}(\pi_n^{a_n+1}) < \text{ord}(x)$. Hence, by (2.14), $x \in \text{Tr}_{F'_n/F_n}(\pi_n O_{F'_n})$, and so x belongs to $\text{Tr}_{K'/K}(\mathfrak{m}_{K'})$. This completes the proof.

Lemma 2.8 *Assume K is not of finite conductor. Let F be any finite extension of $\mathbb{Q}_p$. Then, for each $w \in [-1, \infty)$, we have $[F_n : F_n \cap F^{(w)}] \to \infty$ as $n \to \infty$. In particular, $e(F_n) \to \infty$ as $n \to \infty$.*

Proof. We claim that K must be an infinite extension of $K \cap F^{(w)}$. Indeed, if this were not the case, we could write K as a compositum of $K \cap F^{(w)}$ and some finite extension of $\mathbb{Q}_p$. But then K would be a compositum of two fields of finite conductor, and so K itself would have finite conductor, contrary to our hypothesis. Hence we can choose a sequence $\{\beta_1, \beta_2, \ldots\}$ of elements of K, such that, if d_i denotes the degree of β_i over $K \cap F^{(w)}$, then $\{d_1, d_2, \ldots\}$ is a strictly increasing sequence. But $\beta_i \in F_{n_i}$ for some n_i. Hence $\beta_i \in F_n$ and β_i clearly has degree $\geqq d_i$ over $F_n \cap F^{(w)}$ for all $n \geqq n_i$. Thus $[F_n : F_n \cap F^{(w)}] \geqq d_i$ for all $n \geqq n_i$, and so $[F_n : F_n \cap F^{(w)}] \to \infty$ as $n \to \infty$. The last assertion follows because $\mathbb{Q}_p^{(0)}$ is the maximal unramified extension of $\mathbb{Q}_p$, and thus $e(F_n) = [F_n : F_n \cap \mathbb{Q}_p^{(0)}]$.

Proposition 2.9 *The following assertions are equivalent for K:*

(i) *K does not have finite conductor;*

(ii) *For every finite extension K' of K, we have* $\lim_{n \to \infty} \mathrm{ord}(\delta(F'_n/F_n)) = 0$;

(iii) *For every finite extension K' of K, we have* $\mathrm{Tr}_{K'/K}(\mathfrak{m}_{K'}) = \mathfrak{m}_K$.

Proof. We have (ii) implies (iii) by Lemma 2.7, and that (iii) implies (i) by Proposition 2.5. We now use a slight generalization of Tate's argument in [18] to show that (i) implies (ii). We assume K does not have finite conductor, and let K' be any finite extension of K. We can suppose that K' is Galois over K (if not, replace K' by its Galois closure over K, and use the multiplicativity of the different). Thus we can take F'_{n_0} to be Galois over F_{n_0}, and the same is then true for F'_n over F_n for all $n \geqq n_0$.

Our aim is to show that the limit in (ii) is 0. For brevity, put

$$H = F_{n_0}, \quad J = F'_{n_0}, \quad e = e(F_{n_0}) .$$

For each $w \in [-1, \infty)$, we again write $H^{(w)}$ for the fixed field of the w-th ramification subgroup of $G(\overline{\mathbb{Q}}_p/H)$. By the multiplicativity of the different, we have

$$\delta(F'_n/F_n) = \delta(F'_n/H) \cdot \delta(F_n/H)^{-1} .$$

Hence, applying Lemma 2.1 to both the extensions F'_n/H and F_n/H, we obtain

$$\mathrm{ord}(\delta(F'_n/F_n)) = e^{-1} \int_{-1}^{\infty} \left(\frac{1}{[F_n : F_n \cap H^{(w)}]} - \frac{1}{[F'_n : F'_n \cap H^{(w)}]} \right) \mathrm{d}w . \tag{2.16}$$

We can estimate the integral on the right as follows. Since $F'_{n_0} = J$ is a finite extension of H, there exists $w_0 \in [-1, \infty)$ such that $J \subset H^{(w_0)}$. Now we claim that

$$[F'_n : F'_n \cap H^{(w)}] = [F_n : F_n \cap H^{(w)}] \quad \text{for all} \quad w \geqq w_0 . \tag{2.17}$$

Granted (2.17), we see that the integrand on the right of (2.16) is zero for $w \geqq w_0$, and so

$$\operatorname{ord}(\delta(F_n'/F_n)) = e^{-1} \int_{-1}^{w_0} \left(\frac{1}{[F_n : F_n \cap H^{(w)}]} - \frac{1}{[F_n' : F_n' \cap H^{(w)}]} \right) \mathrm{d}w$$

$$\leqq e^{-1} \int_{-1}^{w_0} \frac{\mathrm{d}\, w}{[F_n : F_n \cap H^{(w)}]} .$$

But we clearly have $F_n \cap H^{(w)} \subseteq F_n \cap H^{(w_0)}$ for all $w \in [-1, w_0]$, and so

$$\operatorname{ord}(\delta(F_n'/F_n)) \leqq (w_0 + 1)/(e \cdot [F_n : F_n \cap H^{(w_0)}]) .$$

Since K does not have finite conductor, it follows from Lemma 2.8 that the right hand side of this inequality tends to 0 as $n \to \infty$, as required. Hence it remains only to prove (2.17). To alleviate the notation, put

$$R_n(w) = F_n \cap H^{(w)}, \quad R_n'(w) = F_n' \cap H^{(w)} .$$

Now the fact that $H^{(w)}$ is Galois over H implies that F_n and $H^{(w)}$ are linearly disjoint over $R_n(w)$, and so $[F_n : R_n(w)] = [F_n R_n'(w) : R_n'(w)]$. But we claim that $F_n R_n'(w) = F_n'$. Indeed, it is plain that $F_n R_n'(w) \subset F_n'$. On the other hand, $J \subset H^{(w)}$ since $w \geqq w_0$, and so $F_n' = JF_n \subset R_n'(w) F_n$. This proves (2.17), and completes the proof of Proposition 2.9.

Proposition 2.10 *The following two assertions are equivalent for* K :
(i) K *does not have finite conductor*;
(ii) $H^1(K, \overline{\mathfrak{m}}) = 0$, *where* $\overline{\mathfrak{m}}$ *denotes the maximal ideal of the ring of integers of* $\overline{\mathbb{Q}}_p$.

Remark. In Sect. 5 (see Proposition 5.3) we shall prove a curious analogue of this result involving formal groups attached to semi-stable abelian varieties defined over K. Also, we see that Proposition 2.10 shows that $H^1(K, \overline{\mathfrak{m}}) = 0$ implies that $H^1(L, \overline{\mathfrak{m}}) = 0$ for all fields L with $K \subset L \subset \overline{\mathbb{Q}}_p$. It does not seem easy to prove this statement directly.

Proof. Let K be any field which does not have finite conductor, and let K' be any finite cyclic extension of K. We will prove that

$$H^1(G(K'/K), \mathfrak{m}_{K'}) = 0 . \tag{2.18}$$

We first note that an induction argument shows that this result implies that $H^1(G(L/K), \mathfrak{m}_L) = 0$ for all finite Galois extensions L of K. Indeed, if L is any finite Galois extension of K, the fact that $G(L/K)$ is soluble implies that there exists a non-trivial cyclic extension K' of K with $K' \subset L$. Now we have the inflation – restriction sequence

$$0 \to H^1(G(K'/K), \mathfrak{m}_{K'}) \to H^1(G(L/K), \mathfrak{m}_L) \to H^1(G(L/K'), \mathfrak{m}_L)$$

The term on the left is 0 by (2.18), and the term on the right is 0 by induction on the order of $G(L/K)$ (to carry out this induction, we are using the fact that any extension of a field which does not have finite conductor also does not have finite conductor). Hence the term in the middle is 0, as required. Passing to the inductive limit over all finite Galois extensions L of K, we see that (2.18) shows that (i) implies (ii). Turning to the proof of (2.18), we put $\Omega = G(K'/K)$, and write τ for a generator of Ω. Then (2.18) is the assertion that $\mathfrak{m}_{K'}^0 = (\tau - 1)\mathfrak{m}_{K'}$, where $\mathfrak{m}_{K'}^0$ denotes the kernel of the trace map from $\mathfrak{m}_{K'}$ to $\mathfrak{m}_K$. As in the proof of Lemma 2.7, let π_n denote a local parameter of F_n, and let the integers $a_n \geqq 0$ be defined by (2.14). We write $O_{F_n'}^0$ for the kernel of the trace map from $O_{F_n'}$ to O_{F_n}.

Lemma 2.11 *Assume K' is a cyclic extension of K. Then, for all integers $n \geqq n_0$, we have*

$$\pi_n^{a_n} O_{F_n'}^0 \subset (\tau - 1) O_{F_n'} . \tag{2.19}$$

Proof. If A is an Ω-module, we define the Herbrand quotient $h_\Omega(A)$ to be

$$\#(H^2(\Omega, A))/\#(H^1(\Omega, A)) ,$$

it being assumed that both cohomology groups are finite. The crucial observation we need is that $h_\Omega(O_{F_n'}) = 1$, because $O_{F_n'}$ contains a free $O_{F_n}[\Omega]$-module of rank 1, which is of finite index in $O_{F_n'}$. Hence

$$\#(O_{F_n}/\pi_n^{a_n} O_{F_n}) = \#(O_{F_n'}^0/(\tau - 1)O_{F_n'}) . \tag{2.20}$$

Now the group on the right hand side of this last equation is an O_{F_n}-module, and so is isomorphic to a module of the form

$$\bigoplus_{i=1}^{r} O_{F_n}/\pi_n^{d_i} O_{F_n} , \tag{2.21}$$

where $d_1, \ldots, d_r$ are integers $\geqq 1$. It is plain from (2.20) that $\sum_{i=1}^r d_i = a_n$. Hence $\pi_n^{a_n}$ annihilates (2.21), which proves (2.19).

We can now complete the proof of (2.18). Take any $x \in \mathfrak{m}_{K'}^0$. Choose $n \geqq n_0$ so large that $x \in F_n'$ and $\mathrm{ord}(x) > \mathrm{ord}(\pi_n^{a_n+1})$. This is possible because $\mathrm{ord}(\pi_n^{a_n+1}) \to 0$ as $n \to \infty$ by Proposition 2.9 and the proof of Lemma 2.7. Hence $x \in \pi_n^{a_n+1} O_{F_n'}$ and has trace 0 to F_n. It follows from (2.19) that x belongs to $(\tau - 1)\pi_n O_{F_n'}$, and so x belongs to $(\tau - 1)\mathfrak{m}_{K'}$. This completes the proof that (i) implies (ii).

Before giving the proof that (ii) implies (i), we must establish the following generalization of Lemma 2.6, which is again valid for any field K with $\mathbb{Q}_p \subset K \subset \overline{\mathbb{Q}}_p$ and any finite extension K' of K. Suppose that, for all $n \geqq n_0$, we are given an O_{F_n}-submodule M_n of $O_{F_n'}$ satisfying the two hypotheses: (a) M_n has maximal rank $d = [K' : K]$, and (b) for all $m \geqq n$, $M_m \supset O_{F_m} M_n$. We define the discriminant $\Delta(M_n)$ of M_n to be the ideal of O_{F_n} generated by

$\det(\sigma_i(\omega_j(n)))^2$, where $\omega_1(n),\dots,\omega_d(n)$ is an O_{F_n}-basis of M_n, and $\sigma_1,\dots,\sigma_d$ are the distinct embeddings of F_n' into $\overline{\mathbb{Q}}_p$, which leave F_n fixed. Then we claim that

$$\lim_{n\to\infty} \operatorname{ord}(\Delta(M_n)) \tag{2.22}$$

exists in $\mathbb{R}$. The proof is exactly the same as that of Lemma 2.6 in that one notes again that the $\operatorname{ord}(\Delta(M_n))$ $(n \geqq n_0)$ form a decreasing sequence of non-negative real numbers. An immediate consequence of the existence of the limit (2.22) is that, for each $\varepsilon > 0$, there exists an integer $N(\varepsilon)$ such that, for all $m \geqq n \geqq N(\varepsilon)$, we have

$$0 \leqq \operatorname{ord}(\Delta(M_n)) - \operatorname{ord}(\Delta(M_m)) < \varepsilon\,. \tag{2.23}$$

We now interpret this last inequality algebraically. Let R be any finite O_{F_m}-module. By the structure theory, R will be isomorphic to a module of the form

$$\bigoplus_{i=1}^{r} O_{F_m}/\pi_m^{d_i} O_{F_m}\,,$$

where $d_1,\dots,d_r$ are integers $\geqq 1$. We then define the characteristic ideal $c_m(R)$ of R to be the ideal of O_{F_m} generated by π_m^{λ}, where $\lambda = \sum_{i=1}^{r} d_i$. We claim that, for all $m \geqq n \geqq n_0$, we have

$$\operatorname{ord}(c_m(M_m/O_{F_m}M_n)) = \tfrac{1}{2}(\operatorname{ord}(\Delta(M_n)) - \operatorname{ord}(\Delta(M_m)))\,. \tag{2.24}$$

To prove (2.24), we note that $\Delta(M_n)O_{F_m} = \Delta(M_n O_{F_m})$ for all $m \geqq n$. As above, let $\omega_1(n),\dots,\omega_d(n)$ be an O_{F_n}-basis of M_n. Clearly we can write

$$\omega_i(n) = \sum_{h=1}^{d} u_{i,h}\omega_i(m) \quad (m \geqq n)\,,$$

where $U = (u_{i,h})$ is a $d \times d$-matrix with entries in O_{F_m}. By the theory of elementary divisors, we have $\det U \cdot O_{F_m} = c_m(M_m/O_{F_m}M_n)$. On the other hand, it is also clear that

$$\Delta(M_n O_{F_m}) = (\det U)^2 \Delta(M_m)\,.$$

Combining these remarks, we deduce (2.24). If we now put together (2.23) and (2.24), we have shown that, for each $\varepsilon > 0$, there exists $N(\varepsilon)$ such that

$$\operatorname{ord}(c_m(M_m/O_{F_m}M_n)) < \varepsilon/2 \tag{2.25}$$

whenever $m \geqq n \geqq N(\varepsilon)$.

We now return to the proof that (ii) implies (i) in Proposition 2.10. Thus we assume that $H^1(K,\overline{\mathfrak{m}}) = 0$. Our strategy is to show that $\operatorname{Tr}_{K'/K}(\mathfrak{m}_{K'}) = \mathfrak{m}_K$ for all finite cyclic extensions K' of K. Indeed, by Proposition 2.5, this will imply that K does not have finite conductor, as required. Now, for all finite Galois extensions K' of K, we must have $H^1(G(K'/K),\mathfrak{m}_{K'}) = 0$, because the inflation restriction sequence shows that this group is a subgroup of $H^1(K,\overline{\mathfrak{m}}) = 0$. In particular, taking K' to be a finite cyclic extension of K we conclude that

$$\mathfrak{m}_{K'}^{0} = (\tau - 1)\mathfrak{m}_{K'}\,, \tag{2.26}$$

where $\mathfrak{m}_{K'}^0$ is the kernel of the trace map from $\mathfrak{m}_{K'}$ to $\mathfrak{m}_K$, and τ is a generator of $G(K'/K)$. Let the integers $d_n \geqq 0$ be defined by

$$\mathrm{Tr}_{F_n'/F_n}(\mathfrak{m}_{F_n'}) = \pi_n^{d_n}\mathfrak{m}_{F_n} . \tag{2.27}$$

We shall prove that

$$\mathrm{ord}(\pi_n^{d_n}) \to 0 \quad \text{as} \quad n \to \infty . \tag{2.28}$$

Let us first note that (2.28) does indeed prove that $\mathrm{Tr}_{K'/K}(\mathfrak{m}_{K'}) = \mathfrak{m}_K$. There are two possibilities. If $e(F_n)$ is constant for large n, then (2.28) implies that $d_n = 0$ for all sufficiently large n, whence the desired surjectivity of the trace is clear. If $e(F_n) \to \infty$ as $n \to \infty$, then (2.28) shows that $\mathrm{ord}(\pi_n^{d_n+1}) \to 0$ as $n \to \infty$. Given $x \in \mathfrak{m}_K$, we can then choose n so large that $x \in \mathfrak{m}_{F_n}$ and $\mathrm{ord}(x) > \mathrm{ord}(\pi_n^{d_n+1})$, and so by (2.27) it is again plain that x is a trace from $\mathfrak{m}_{F_n'}$, as required.

To prove (2.28), we apply the arguments of the penultimate paragraph to the modules

$$M_n = O_{F_n} \cdot 1 + \mathfrak{m}_{F_n'}^0 ,$$

where again $\mathfrak{m}_{F_n'}^0$ denotes the kernel of the trace map from $\mathfrak{m}_{F_n'}$ to $\mathfrak{m}_{F_n}$. Suppose we are given an $\varepsilon > 0$. There exists an integer $N(\varepsilon)$ such that (2.25) holds for all $m \geqq n \geqq N(\varepsilon)$. Fix an $n \geqq N(\varepsilon)$. By virtue of (2.26), we know that there exists an integer m such that

$$\mathfrak{m}_{F_n'}^0 \subset (\tau - 1)\mathfrak{m}_{F_m'}$$

(note that we need only find an m such that the generators of $\mathfrak{m}_{F_n'}^0$ as an O_{F_n}-module are contained in $(\tau - 1)\mathfrak{m}_{F_m'}$). In view of this inclusion, we see that

$$O_{F_m}M_n \subset O_{F_m} \cdot 1 + (\tau - 1)\mathfrak{m}_{F_m'} ,$$

and so there is a natural surjection

$$M_m/O_{F_m}M_n \twoheadrightarrow \frac{O_{F_m} + \mathfrak{m}_{F_m'}^0}{O_{F_m} + (\tau - 1)\mathfrak{m}_{F_m'}} \xrightarrow{\sim} \frac{\mathfrak{m}_{F_m'}^0}{(\tau - 1)\mathfrak{m}_{F_m'}} .$$

This proves that the characteristic ideal of the module on the right divides $c_m(M_m/O_{F_m}M_n)$. Thus, by (2.25), we have

$$\mathrm{ord}(c_m(\mathfrak{m}_{F_m'}^0/(\tau - 1)\mathfrak{m}_{F_m'})) < \varepsilon/2 . \tag{2.29}$$

But, as remarked in the proof of Lemma 2.11, the Herbrand quotient of $\mathfrak{m}_{F_m'}$ (which is isomorphic as an O_{F_m}-module to $O_{F_m'}$) is equal to 1. Interpreting the equality of the orders of the H^1 and H^2 in terms of characteristic ideals as O_{F_m}-modules, we deduce that

$$\mathrm{ord}(c_m(\mathfrak{m}_{F_m'}^0/(\tau - 1)\mathfrak{m}_{F_m'})) = \mathrm{ord}(c_m(\mathfrak{m}_{F_m}/\mathrm{Tr}_{F_m'/F_m}(\mathfrak{m}_{F_m'})))$$

But, by (2.27), the right hand side is none other than $\mathrm{ord}(\pi_m^{d_m})$. Hence (2.29) shows that $\mathrm{ord}(\pi_m^{d_m})$ is less than ε for all sufficiently large m. This proves (2.28), and so the proof of Proposition 2.10 is now complete.

We are at last in a position in which we can define what we mean by a deeply ramified extension of $\mathbb{Q}_p$. Combining our previous results, we see that the following conditions are equivalent for any field K with $\mathbb{Q}_p \subset K \subset \overline{\mathbb{Q}_p}$:

(i) K does not have finite conductor;

(ii) $\mathrm{ord}(\delta(F_n/\mathbb{Q}_p)) \to \infty$ as $n \to \infty$;

(iii) $H^1(K, \overline{\mathfrak{m}}) = 0$;

(iv) for every finite extension K' of K, we have $\mathrm{Tr}_{K'/K}(\mathfrak{m}_{K'}) = \mathfrak{m}_K$;

(v) for every finite extension K' of K, we have $\mathrm{ord}(\delta(F'_n/F_n)) \to 0$ as $n \to \infty$.

Here the fields F_n and F'_n are as given in (2.5) and just after (2.11). We shall say that K is *deeply ramified* if it satisfies these five equivalent conditions. Before discussing some examples of deeply ramified fields, it is useful to note the following necessary but not sufficient condition for K to be deeply ramified.

Lemma 2.12 *Assume that K is deeply ramified. Then K is infinitely wildly ramified in the sense that the power of p dividing the ramification index $e(F_n)$ of F_n over $\mathbb{Q}_p$ tends to ∞ as $n \to \infty$.*

Proof. Assume the power of p dividing $e(F_n)$ is bounded as $n \to \infty$. Then there exists an integer n_1 such that, if we put $F = F_{n_1}$, then F_n is a tamely ramified extension of F for all $n \geqq n_1$. But any finite extension L of F is tamely ramified if and only if $L \subset F^{(w)}$ for all $w > 0$. It follows that, for each $w > 0$, $F_n \subset F^{(w)}$ for all $n \geqq n_1$. Hence $K \subset F^{(w)}$ for all $w > 0$, which contradicts our hypothesis that K is deeply ramified.

We next discuss known examples of deeply ramified fields. We first remark that it is plain from (i) above that every algebraic extension of a deeply ramified field is again deeply ramified. Let F be any finite extension of $\mathbb{Q}_p$, and assume that K is an extension of F. Again using (i), we see that K is deeply ramified if and only if the Galois closure of K over F is deeply ramified. The classical example of a deeply ramified field (this is the example used by Tate [18]) is a field K which is a ramified $\mathbb{Z}_p$-extension of a finite extension F of $\mathbb{Q}_p$. The following immediate consequence of a theorem of Sen [15] provides a vast generalization of this classical example.

Theorem 2.13 *Let F be a finite extension of $\mathbb{Q}_p$, and let K be a Galois extension of F such that the Galois group of K over F is a p-adic Lie group. If the inertial subgroup of $G(K/F)$ is infinite, then K is deeply ramified.*

We will call a field K satisfying the hypotheses of Theorem 2.13 an infinitely ramified p-adic Lie extension of F. We now explain how to derive this theorem

from the principal result of [15]. Let I denote the inertial subgroup of $G(K/F)$, and let L be the fixed field of I, so that L is an unramified extension of F which is not, in general, complete. Let L' be the completion of L, and write K' for the compositum of K and L'. We first note that L' contains no non-trivial algebraic extension of L; indeed any such algebraic extension would have the same residue field and be non-ramified, and so would be trivial. It follows that the restriction mapping defines an isomorphism from $G(K'/L')$ onto $G(K/L) = I$. It is not difficult to see that the restriction mapping then defines an isomorphism from $G(K'/L')^{(w)}$ onto $G(K/L)^{(w)}$ for all $w \in [-1, \infty)$. But $G(K'/L')$ is itself a p-adic Lie group because it is isomorphic to the closed subgroup I of the p-adic Lie group $G(K/L)$. But the main result of [15] shows, in particular, that $G(K'/L')^{(w)}$ is of finite index in $G(K'/L') \xrightarrow{\sim} I$ for all $w \in [-1, \infty)$. As I is infinite, we conclude that $G(K/F)^{(w)} \neq 1$ for all $w \in [-1, \infty)$, and so K does not have finite conductor, as required.

One can immediately obtain from Theorem 2.13 many other examples of deeply ramified extensions. Any algebraic extension of F whose Galois closure over F contains an infinitely ramified p-adic Lie extension of F will be deeply ramified. Here are some specific examples of this kind. At the end of our discussion of Case IV in Sect. 5, there is an interesting example of a field P, which is not a Galois extension of $\mathbb{Q}_p$, but whose Galois closure M over $\mathbb{Q}_p$ has $G(M/\mathbb{Q}_p)$ a 2-dimensional p-adic Lie group. It follows that P is deeply ramified. A more concrete example (pointed out to us by P. Colmez) is the following. Let w_0 be any local parameter of $\mathbb{Q}_p$, and define $w_n = \sqrt[p]{w_{n-1}}$ for all $n \geqq 1$, where one can take any choice of the p-th root. Define $F_n = \mathbb{Q}_p(w_n)$ $(n = 0, 1, \ldots,)$, and put $K = \bigcup_{n=0}^{\infty} F_n$. Since F_n is generated over $\mathbb{Q}_p$ by a root of the Eisenstein polynomial $X^{p^n} - w_0$, it is clear that $\mathrm{ord}(\delta(F_n/\mathbb{Q}_p)) > n$ $(n = 1, 2, \ldots)$, and so K is deeply ramified by property (ii) above. The Galois closure of this field K over $\mathbb{Q}_p$ is again a 2-dimensional p-adic Lie extension, this time containing $\mathbb{Q}_p(\mu_{p^\infty})$. As another example, suppose that F is a finite extension of $\mathbb{Q}_p$ and that K is a Galois extension of F such that $G(K/F)$ is isomorphic to a subgroup of finite index in $PGL_2(\mathbb{Z}_p)$ (such fields K/F can be shown to exist). Then K/F must be infinitely ramified. Also, because the Lie algebra for $PGL_2(\mathbb{Z}_p)$ is simple, it follows that any infinite extension of F contained in K must be deeply ramified. However, we should stress that we believe there exist deeply ramified Galois extensions K of any finite extension F of $\mathbb{Q}_p$, with the property that no subfield K' of K is an infinitely ramified p-adic Lie extension of a finite extension of $\mathbb{Q}_p$. Finally, we mention a paper of Fesenko [3], which discusses the connection between deeply ramified extensions and arithmetically profinite extensions in the sense of Fontaine and Wintenberger [2], [20], and also gives some interesting examples. In another direction, we would like to note the article [4] by Fresnel and Matignon, and the Tokyo Ph.D. thesis [21] by Taguchi which extend Tate's paper [18] in different, but not unrelated, fashions to ours.

3 Applications to formal groups

It is a surprising and beautiful fact that many of the arguments of Sect. 2 about the formal additive group can be generalized almost immediately to arbitrary commutative formal groups defined over the ring of integers of a p-adic field. The aim of this section is to carry out this generalization, which is crucial for the applications to abelian varieties discussed in Sect. 4 and Sect. 5.

Let F be a finite extension of $\mathbb{Q}_p$. Let r be an integer $\geqq 1$, and let $\mathscr{F}$ be a commutative formal group law in r variables, defined over the ring O_F of integers of F. We recall that such a formal group is given by a family $f(X,Y) = (f_i(X,Y))$ of r formal power series in the $2r$ variables X_i, Y_j $(1 \leqq i,j \leqq r)$, with coefficients in O_F, which satisfy the axioms (i) $X = f(X,O) = f(O,X)$, (ii) $f(X,f(Y,Z)) = f(f(X,Y),Z)$, (iii) $f(X,Y) = f(Y,X)$. It follows immediately from the axioms that

$$f(X,Y) = X + Y + \text{ terms of degree } \geqq 2 \text{ in } X_i, Y_j \,. \tag{3.1}$$

Let K be any field with $F \subset K \subset \overline{\mathbb{Q}}_p$. As usual, we define $\mathscr{F}(\mathfrak{m}_K)$ to be the set $\mathfrak{m}_K^r$, endowed with the abelian group law

$$x \oplus y = f(x,y)\,;$$

even though K is not in general complete, the power series on the right plainly converge to an element of $\mathfrak{m}_K^r$, because of our hypothesis that the coefficients of F belong to a finite extension of $\mathbb{Q}_p$. Similarly, if $\mathfrak{a}$ is an ideal of $\mathfrak{m}_K$, $\mathscr{F}(\mathfrak{a})$ will denote the subgroup of $\mathscr{F}(\mathfrak{m}_K)$ which is given by $\mathfrak{a}^r$ with the group law $\oplus$. The basic examples of such $\mathscr{F}$ are $\hat{\mathbb{G}}_a$, where $f(X,Y) = X + Y$, $\hat{\mathbb{G}}_m$, where $f(X,Y) = X + Y + XY$, and the formal group attached to the Néron model of an abelian variety defined over F. However, the arguments of this section work for an arbitrary commutative formal group $\mathscr{F}$ over O_F. Our principal result is the following.

Theorem 3.1 *Let K be any extension of F which is deeply ramified. For all finite Galois extensions K' of K, we have*

$$H^i(G(K'/K), \mathscr{F}(\mathfrak{m}_{K'})) = 0 \quad (i \geqq 1)\,. \tag{3.2}$$

Corollary 3.2 *If K is a deeply ramified extension of F, then*

$$H^i(K, \mathscr{F}(\overline{\mathfrak{m}})) = 0 \quad (i \geqq 1)\,. \tag{3.3}$$

We begin the proof of Theorem 3.1 by studying the surjectivity of the trace map on the formal group $\mathscr{F}$. If K is any extension of F, and K' is a finite extension of K, we recall that the trace map

$$\mathscr{N}_{K'/K} : \mathscr{F}(\mathfrak{m}_{K'}) \to \mathscr{F}(\mathfrak{m}_K)$$

is defined by $\mathscr{N}_{K'/K}(x) = (\sigma_1 x) \oplus \cdots \oplus (\sigma_d x)$, where $\sigma_1, \ldots, \sigma_d$ denote the distinct embeddings of K' into $\overline{\mathbb{Q}_p}$ which fix K.

Proposition 3.3 *Assume K is an extension of F which is deeply ramified. Then, for all finite extensions K' of K, we have*

$$\mathcal{N}_{K'/K}(\mathcal{F}(\mathfrak{m}_{K'})) = \mathcal{F}(\mathfrak{m}_K)\,. \tag{3.4}$$

We will use the same notation as introduced in Sect. 2, including that given in (2.5) and (2.11). Again, π_n will denote a local parameter for the field F_n.

Lemma 3.4 *Assume s is an integer $\geqq 1$, and let $z \in (\pi_n^s O_{F'_n})^r$. Then, for all $n \geqq n_0$,*

$$\mathcal{N}_{F'_n/F_n}(z) \equiv \mathrm{Tr}_{F'_n/F_n}(z) \bmod \pi_n^{2s} \tag{3.5}$$

Proof. Of course, (3.5) means that this congruence holds for each component of the vectors in question. To prove (3.5), we note that (3.1) shows that

$$\mathcal{N}_{F'_n/F_n}(z) = \mathrm{Tr}_{F'_n/F_n}(z) + H_n(z)\,,$$

where $H_n(z)$ is a vector all of whose components are formal power series with coefficients in O_F in the components of $\sigma_1(z), \ldots, \sigma_d(z)$, which contain only monomials of degree $\geqq 2$. Hence $H_n(z) \equiv 0 \bmod \pi_n^{2s}$, as required.

Recall that the integers $a_n \geqq 0$ are defined for $n \geqq n_0$ by $\mathrm{Tr}_{F'_n/F_n}(O_{F'_n}) = \pi_n^{a_n} O_{F_n}$.

Lemma 3.5 *Assume that $n \geqq n_0$ and that $s \geqq a_n + 1$. For each $y \in \mathcal{F}(\pi_n^{s+a_n} O_{F_n})$, there exists $w \in \mathcal{F}(\pi_n^s O'_{F_n})$ such that*

$$y \ominus \mathcal{N}_{F'_n/F_n}(w) \in \mathcal{F}(\pi_n^{s+a_n+1} O_{F_n})\,. \tag{3.6}$$

Proof. Since π_n belongs to F_n, we have $\mathrm{Tr}_{F'_n/F_n}(\pi_n^s O_{F'_n}) = \pi_n^{s+a_n} O_{F_n}$. Hence the hypothesis made on y shows that there exists $w \in (\pi_n^s O_{F'_n})^r$ such that $y = \mathrm{Tr}_{F'_n/F_n}(w)$. Clearly we have $\mathcal{N}_{F'_n/F_n}(w)$ belongs to $\mathcal{F}(\pi_n^s O_{F_n})$. Hence, by virtue of (3.1) and (3.5), the following congruences

$$y \ominus \mathcal{N}_{F'_n/F_n}(w) \equiv y - \mathcal{N}_{F'_n/F_n}(w) \equiv y - \mathrm{Tr}_{F'_n/F_n}(w)$$

hold modulo π_n^{2s}. This implies (3.6) because $2s \geqq s + a_n + 1$ since we have $s \geqq a_n + 1$.

Lemma 3.6 *For all $n \geqq n_0$, we have*

$$\mathcal{N}_{F'_n/F_n}(\mathcal{F}(\mathfrak{m}_{F'_n})) \supset \mathcal{F}(\pi_n^{2a_n+1} O_{F_n})\,. \tag{3.7}$$

Proof. Take z to be any element in $\mathcal{F}(\pi_n^{2a_n+1} O_{F_n})$. We use induction to construct a sequence of elements

$$w_\lambda \in \mathcal{F}(\pi_n^{a_n+\lambda} O_{F'_n}) \quad (\lambda = 1, 2, \ldots)$$

such that

$$z \ominus \mathcal{N}_{F'_n/F_n}(w_1 \oplus \cdots \oplus w_\lambda) \in \mathcal{F}(\pi_n^{2a_n+\lambda+1} O_{F_n}) \quad (\lambda \geqq 1)\,. \tag{3.8}$$

Indeed, we see that (3.8) holds for $\lambda = 1$ by applying Lemma 3.5 with $s = a_n + 1$ and $y = z$. Assume now that (3.8) holds for λ, and again apply Lemma 3.5 with $s = a_n + \lambda + 1$ and y now given by the element on the left of (3.8). We deduce the existence of a $w_{\lambda+1}$ with all the required properties. Now let $\lambda \to \infty$. The limit $w = w_1 \oplus \cdots \oplus w_\lambda \oplus \cdots$ exists in $\mathscr{F}(\mathfrak{m}_{F'_n})$, and, by virtue of (3.8), we have $\mathscr{N}_{F'_n/F_n}(w) = z$. This completes the proof of (3.7).

We can now prove Proposition 3.3. Take $x \in \mathscr{F}(\mathfrak{m}_K)$. Since K is deeply ramified, we have $\lim \operatorname{ord}(\pi_n^{2a_n+1}) \to 0$ as $n \to \infty$ (see Lemma 2.7 and Proposition 2.9). Hence we can choose an integer $n \geqq n_0$ such that $x \in F_n$ and $\operatorname{ord}(\pi_n^{2a_n+1}) < \operatorname{ord}(x)$. Thus $x \in \mathscr{F}(\pi_n^{2a_n+1} O_{F_n})$, and so (3.7) shows that x is a norm from $\mathscr{F}(\mathfrak{m}_{F'_n})$. This completes the proof of Proposition 3.3.

Until further notice in this section, we shall assume that K' is now a finite cyclic extension of K, and we shall write τ for a generator of $G(K'/K)$. Under this assumption, Proposition 3.3 can be interpreted as stating

$$H^2(G(K'/K), \mathscr{F}(\mathfrak{m}_{K'})) = 0\,, \tag{3.9}$$

when K is deeply ramified. We now proceed to show that also

$$H^1(G(K'/K), \mathscr{F}(\mathfrak{m}_{K'})) = 0 \tag{3.10}$$

when K is deeply ramified. Let $\mathscr{F}(\mathfrak{m}_{K'})^0$ denote the kernel of $\mathscr{N}_{K'/K}$. Then, of course, (3.10) is equivalent to

$$\mathscr{F}(\mathfrak{m}_{K'})^0 = (\tau - 1)\mathscr{F}(\mathfrak{m}_{K'})\,. \tag{3.11}$$

We now set about proving this last statement. For each $n \geqq n_0$, we can take F'_n to be a cyclic extension of F_n, and we can view τ as a generator of $G(F'_n/F_n)$.

Lemma 3.7 *Assume that $n \geqq n_0$, and that $s \geqq a_n + 1$. If $y \in \mathscr{F}(\pi_n^{s+a_n} O_{F'_n})$ satisfies $\mathscr{N}_{F'_n/F_n}(y) = 0$, then there exists $w \in \mathscr{F}(\pi_n^s O_{F'_n})$ such that*

$$y \ominus (\tau(w) \ominus w) \in \mathscr{F}(\pi_n^{s+a_n+1} O_{F'_n})\,. \tag{3.12}$$

Remark. We shall apply this lemma recursively, and it is important to note that $y \ominus (\tau(w) \ominus w)$ will again be in the kernel of $\mathscr{N}_{F'_n/F_n}$.

Proof. Since $\mathscr{N}_{F'_n/F_n}(y) = 0$, we conclude from (3.5) that

$$\operatorname{Tr}_{F'_n/F_n}(y) \equiv 0 \bmod \pi_n^{2(s+a_n)}\,.$$

Hence, by the definition of a_n, there exists $u \in (\pi_n^{2s+a_n} O_{F'_n})^r$ such that $\operatorname{Tr}_{F'_n/F_n}(y - u) = 0$. But, by Lemma 2.11, we have

$$\pi_n^{s+a_n} O_{F'_n}^0 \subset (\tau - 1)\pi_n^s O_{F'_n}\,.$$

Hence we conclude that there exists $w \in (\pi_n^s O_{F'_n})^r$ such that $(\tau - 1)w = y - u$. We claim that this w satisfies (3.12). Indeed, by (3.1), we have

$$\tau(w) \ominus w \equiv (\tau - 1)w \bmod \pi_n^{2s}\,.$$

Hence, as $u = y - (\tau - 1)w$ belongs to $(\pi_n^{2s} O_{F_n'})^r$ by construction, we conclude from (3.1) that the following congruences

$$y \ominus (\tau(w) \ominus w) \equiv y - (\tau(w) \ominus w) \equiv y - (\tau(w) - w) \equiv 0$$

hold modulo π_n^{2s}. Since $s \geqq a_n + 1$, this establishes (3.12).

Lemma 3.8 *For all $n \geqq n_0$, we have*

$$\mathscr{F}(\pi_n^{2a_n+1} O_{F_n'})^0 \subset (\tau - 1)\mathscr{F}(\mathfrak{m}_{F_n'}) , \tag{3.13}$$

where $\mathscr{F}(\pi_n^{2a_n+1} O_{F_n'})^0$ denotes the kernel of $\mathscr{N}_{F_n'/F_n}$ on $\mathscr{F}(\pi_n^{2a_n+1} O_{F_n'})$.

Proof. Take z to be any element in the group on the left of (3.13). We use induction to construct a sequence of elements

$$w_\lambda \in \mathscr{F}(\pi_n^{a_n+\lambda} O_{F_n'}) \quad (\lambda = 1, 2, \ldots)$$

such that

$$z \ominus (\tau(w_1 \oplus \cdots \oplus w_\lambda) \ominus (w_1 \oplus \cdots \oplus w_\lambda)) \in \mathscr{F}(\pi_n^{2a_n+\lambda+1} O_{F_n'}) . \tag{3.14}$$

Indeed, we see that (3.14) holds for $\lambda = 1$ by applying Lemma 3.7 with $s = a_n + 1$ and $y = z$. Assume now that (3.14) holds for λ, and again apply Lemma 3.7 with $s = a_n + \lambda + 1$ and y now given by the element on the left of (3.14). We deduce the existence of a $w_{\lambda+1}$ with all the required properties. Now let $\lambda \to \infty$. The limit $w = w_1 \oplus \cdots \oplus w_\lambda \oplus \cdots$ exists in $\mathscr{F}(\mathfrak{m}_{F_n'})$, and, by virtue of (3.14), we have $z = \tau(w) \ominus w$. This completes the proof of (3.13).

We can now prove (3.11). Take $x \in \mathscr{F}(\mathfrak{m}_{K'})^0$. Since K is deeply ramified, we have $\lim_{n\to\infty} \mathrm{ord}(\pi_n^{2a_n+1}) \to 0$ as $n \to \infty$. Hence we can choose an integer $n \geqq n_0$ such that $x \in F_n'$ and $\mathrm{ord}(\pi_n^{2a_n+1}) < \mathrm{ord}(x)$. Thus $x \in \mathscr{F}(\pi_n^{2a_n+1} O_{F_n'})^0$, and so (3.13) shows that x is of the form $\tau(y) \ominus y$ for $y \in \mathscr{F}(\mathfrak{m}_{F_n'})$, thereby proving (3.11).

The proof of Theorem 3.1 is now easy to complete. Indeed, the above arguments establish (3.2) whenever K is deeply ramified and K' is a finite cyclic extension of K. Bearing in mind the fact that any field which contains a deeply ramified field is itself deeply ramified, a standard argument of devissage (see the proof of Proposition 2.10 for the case $i = 1$) shows that (3.2) holds for all finite Galois extensions K' of K, because $G(K'/K)$ is a soluble group. This establishes Theorem 3.1.

Finally, we point out that a greatly simplified version of the above arguments yields the following classical result.

Proposition 3.9 *Let L be a tamely ramified, finite extension of F. Then*

$$N_{L/F}(\mathscr{F}(\mathfrak{m}_L)) = \mathscr{F}(\mathfrak{m}_F) ; \tag{3.15}$$

$$\textit{If } L/F \textit{ is Galois, then } H^i(G(L/F), \mathscr{F}(\mathfrak{m}_L)) = 0 \quad \textit{for} \quad i \geqq 1 . \tag{3.16}$$

Proof. Since every tamely ramified extension can be broken up into a tower consisting of an unramified extension followed by an extension of degree prime to p, and since $\mathscr{F}(\mathfrak{m}_L)$ is a $\mathbb{Z}_p$-module, we see easily that it suffices to prove (3.15) and (3.16) when L/F is unramified. Assuming that L/F is unramified, we then have $\mathrm{Tr}_{L/F}(O_L) = O_F$. We now apply the arguments of Lemmas 3.5, 3.6, 3.7, and 3.8 to the special case in which

$$F_n = F, \quad F'_n = L, \quad a_n = 0$$

for all $n \geqq 0$. It follows from Lemma 3.6 that (3.15) is valid, and, since L/F is cyclic, this also establishes (3.16) for $i = 2$. On the other hand, Lemma 3.8 yields (3.16) for $i = 1$, thereby completing the proof of Proposition 3.9.

4 The local Kummer homomorphism

Let F be a finite extension of $\mathbb{Q}_l$, where l is any prime. Let A be an abelian variety of dimension g defined over F. We write A^t for the dual abelian variety of A. In this section we will study the image of the Kummer homomorphism $\kappa = \kappa_{A,K}$

$$\kappa : A(K) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K, A[p^\infty]) \tag{4.1}$$

for any algebraic extension K of F and any fixed prime p. Under various hypotheses one can describe the image of κ in an elementary way. We begin with the case $l \neq p$, where the result is very simple.

Proposition 4.1 *Assume* $l \neq p$. *Then* $\mathrm{Im}(\kappa) = 0$.

Proof. First assume that K is a finite extension of F. Then by a well-known theorem of Mattuck, we have an isomorphism

$$A(K) \cong \mathbb{Z}_l^{g[K:\mathbb{Q}_l]} \times (\text{a finite group}) \tag{4.2}$$

and hence clearly

$$A(K) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) = 0 \tag{4.3}$$

This is also true if K is an infinite algebraic extension of F, since $A(K) = \bigcup_{F'} A(F')$, where F' runs over all finite extension of F contained in K, and the result follows immediately.

Remark. For archimedean local fields, the above proposition and its proof are also valid. The points over $K = \mathbb{R}$ or $\mathbb{C}$ on an abelian variety form a compact abelian Lie group. Its connected component is isomorphic to a direct product of g or $2g$ copies of $\mathbb{R}/\mathbb{Z}$ as a group. Thus the tensor product with $\mathbb{Q}_p/\mathbb{Z}_p$ is again clearly zero. Alternatively, one could simply notice that $H^1(K, A[p^\infty])$ is either trivial or a finite group of exponent 2. But the image of κ is always

a divisible group and so must be zero. A similar argument also works in the nonarchimedean case for a finite extension K/F, $l \neq p$. $H^1(K, A[p^\infty])$ is again a finite group. (This follows easily from the result of Tate and Poitou that the Euler–Poincare characteristic of a finite p-primary G_K-module is zero and the fact that $H^0(K, A[p^\infty])$ and $H^0(K, A^t[p^\infty])$ are both finite.) Again the image of κ is divisible and so must be zero.

We assume in the rest of this section that $l = p$. We begin by discussing the image of κ when K is a finite extension of F. By Mattuck's theorem ((4.2) above), the fact that κ is injective and that $\mathbb{Z}_p \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Q}_p/\mathbb{Z}_p$, we see that

$$\text{Im}(\kappa) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{g[K:\mathbb{Q}_p]} . \tag{4.4}$$

As for $H^1(K, A[p^\infty])$, the result of Tate and Poitou concerning the Euler–Poincare characteristic gives the following:

$$\sum_{i=0}^{2} (-1)^i \text{corank}_{\mathbb{Z}_p}(H^i(K, A[p^\infty])) = -2g[K : \mathbb{Q}_p] \tag{4.5}$$

since $\text{corank}_{\mathbb{Z}_p}(A[p^\infty]) = 2g$. But $A^0(K, A[p^\infty])$ is the p-torsion on $A(K)$ and so is finite. Also $H^2(K, A[p^\infty])$ is dual to $H^0(K, T_p(A^t))$, which is zero. Therefore $H^2(K, A[p^\infty]) = 0$. It follows that $H^1(K, A[p^\infty])$ has $\mathbb{Z}_p$-corank $2g[K : \mathbb{Q}_p]$. The image of κ is a certain divisible subgroup with $\mathbb{Z}_p$-corank $g[K : \mathbb{Q}_p]$, which in general seems difficult to describe in an explicit way.

We now suppose that our abelian variety A has semistable reduction over F. Let $\mathscr{F}$ be the formal group over O_F attached to the Neron model for A over O_F. Then $\mathscr{F}$ is a formal group of finite height h and of dimension g, and we have $g \leqq h \leqq 2g$. Let $C = \mathscr{F}(\overline{\mathfrak{m}})[p^\infty]$. Then $C \cong (\mathbb{Q}_p/\mathbb{Z}_p)^h$ as a group and $C \subseteq A[p^\infty]$ is invariant under the action of G_F. We also have the following properties:

(a) $\mathscr{F}(\overline{\mathfrak{m}})$ is a divisible abelian group;

(b) C is a connected p-divisible group over O_F;

(c) $A[p^\infty]/C$ is an étale p-divisible group over O_F.

By (c), the action of I_F on $A[p^\infty]/C$ is trivial. By (b), C itself has no nontrivial quotient on which I_F (or even $I_{F'}$ for any finite extension F' of F) acts trivially. Indeed, such a quotient would be an étale p-divisible group over $O_{F'}$, but must also be connected. Let $W = T_p(C) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ which is a subspace of $V = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, and can be characterized in the following simple way: W is the G_F-invariant $\mathbb{Q}_p$-subspace of V of minimal dimension such that some subgroup of I_F of finite index acts trivially on V/W. The existence and uniqueness of such a subspace is obvious for the following reason. If W_1 and W_2 are any two G_F-invariant subspaces of V such that some open subgroup of I_F acts trivially on V/W_i $(i = 1, 2)$, then an open subgroup of I_F acts trivially on $V/(W_1 \cap W_2)$, because it injects into $V/W_1 \oplus V/W_2$. Note that in the semistable case we are discussing now, I_F itself acts trivially on V/W. Also C is simply the image of W under the map $V \to V/T_p(A) = A[p^\infty]$.

If A does not have semistable reduction over F, we still can define a G_F-invariant subspace W of V by using the above characterization. We then again define C to be the image of W in $A[p^\infty]$; we refer to it as the "canonical subgroup" of $A[p^\infty]$. It is of course G_F-invariant. We let $h = \mathrm{corank}_{\mathbb{Z}_p}(C)$. We will let D denote the quotient $A[p^\infty]/C$, which is a G_F-module of $\mathbb{Z}_p$-corank equal to $(2g-h)$. A well-known result in the theory of abelian varieties states that over some finite extension F' of F, the Neron model for A over $O_{F'}$ will have semistable reduction. If $\mathscr{F}'$ is the associated formal group, then it is clear from the above remarks that $C = \mathscr{F}'(\overline{\mathfrak{m}})[p^\infty]$. In particular, it follows that this last group is independent of the choice of F'. The height of $\mathscr{F}'$ is h and so we have $g \leqq h \leqq 2g$.

Our results will compare the image of the Kummer map κ to the image of the natural map $\lambda = \lambda_{A,K}$ induced by the inclusion $C \subseteq A[p^\infty]$:

$$\lambda : H^1(K, C) \to H^1(K, A[p^\infty]) \tag{4.6}$$

The following lemma allows us to pass to a finite extension and thus reduce to the semistable case. Here K is any algebraic extension of F. If B is an abelian group, we write B_{div} for the maximal divisible subgroup of B.

Lemma 4.2 *Let K' be a finite Galois extension of K, and let $\Delta = G(K'/K)$. Put*

$$\kappa = \kappa_{A,K}, \quad \kappa' = \kappa_{A,K'}, \quad \lambda = \lambda_{A,K}, \quad \lambda' = \lambda_{A,K'}$$

Then, if $\rho : H^1(K, A[p^\infty]) \to H^1(K', A[p^\infty])$ denotes the restriction map, we have

$$\mathrm{Im}(\kappa) = (\rho^{-1}(\mathrm{Im}(\kappa')))_{\mathrm{div}}, \quad \mathrm{Im}(\lambda)_{\mathrm{div}} = (\rho^{-1}(\mathrm{Im}(\lambda')))_{\mathrm{div}}.$$

Proof. We first note that, for every subset Z of $H^1(K', A[p^\infty])$, we have $\rho^{-1}(Z) = \rho^{-1}(Z^\Delta)$, because every element in the image of ρ is fixed by Δ. This enables us to restrict attention to the map

$$\varphi : H^1(K, A[p^\infty]) \to H^1(K', A[p^\infty])^\Delta$$

which is simply the map ρ with a different target group. One fact we will use is that both $\mathrm{Ker}(\varphi)$ and $\mathrm{Coker}(\varphi)$ are finite. This is because $\mathrm{Ker}(\varphi) = H^1(\Delta, A[p^\infty]^{G_{K'}})$ and $\mathrm{Coker}\,\varphi$ injects into $H^2(\Delta, A[p^\infty]^{G_{K'}})$, and both these cohomology groups are finite. We shall establish the lemma using the following general principle. Let B and B' be subgroups of $H^1(K, A[p^\infty])$ and $H^1(K', A[p^\infty])^\Delta$ such that $\varphi(B) \subset B'$ and $B'/\varphi(B)$ has finite exponent. Then we claim that

$$(\varphi^{-1}(B'))_{\mathrm{div}} = (B)_{\mathrm{div}} \,. \tag{4.7}$$

Indeed, one can easily verify that $\varphi^{-1}(B')/B$ has finite exponent, and (4.7) follows immediately from this. We first apply this principle when

$$B = \mathrm{Im}(\kappa), \quad B' = (\mathrm{Im}(\kappa'))^\Delta \,.$$

It is clear that $\varphi(B) \subset B'$, and the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \to & B' & \to & H^1(K', A[p^\infty])^\Delta & \to & H^1(K', A)(p)^\Delta & & \\ & & \uparrow & & \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \alpha} & & \\ 0 & \to & B & \to & H^1(K, A[p^\infty]) & \to & H^1(K, A)(p) & \to & 0 \end{array}$$

shows that $B'/\varphi(B)$ has finite exponent, because both $\mathrm{Coker}(\varphi)$ and $\mathrm{Ker}(\alpha) = H^1(\Delta, A(K'))(p)$ have finite exponent. Thus the first assertion of the lemma now follows from (4.7). Secondly, take

$$B = \mathrm{Im}(\lambda)\,, \quad B' = (\mathrm{Im}(\lambda'))^\Delta\,.$$

Again, it is clear that $\varphi(B) \subset B'$. Let

$$\pi : H^1(K, A[p^\infty]) \to H^1(K, D)\,, \quad \pi' : H^1(K', A[p^\infty]) \to H^1(K', D)$$

be the functorial maps induced by the canonical surjection of $A[p^\infty]$ onto D. We then have the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \to & B' & \to & H^1(K', A[p^\infty])^\Delta & \to & (\mathrm{Im}(\pi'))^\Delta & & \\ & & \uparrow & & \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \beta} & & \\ 0 & \to & B & \to & H^1(K, A[p^\infty]) & \to & \mathrm{Im}(\pi) & \to & 0\,, \end{array}$$

which shows that $B'/\varphi(B)$ is in fact finite because $\mathrm{Coker}(\varphi)$ and $\mathrm{Ker}(\beta)$ are both finite; $\mathrm{Ker}(\beta)$ is finite because it injects into $H^1(\Delta, D^{G_{K'}})$. The second assertion of the lemma now follows from (4.7), and the proof is complete.

Remark. Lemma 4.2 is not, in general, valid if K is an infinite Galois extension of F.

Our arguments in the rest of this section are based on diagram (4.8) below, whose rows are exact. We assume that A has semistable reduction over F, and let $\mathscr{F}$ be the formal group over O_F associated with the Neron model for A over O_F. Since $\mathscr{F}(\overline{\mathfrak{m}})$ is divisible, the Kummer homomorphism

$$\kappa_{\mathscr{F}} = \kappa_{\mathscr{F},K} : \mathscr{F}(\mathfrak{m}_K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(K, \mathscr{F}(\overline{\mathfrak{m}})[p^\infty])\,.$$

can be defined just as for A. Also we recall that $H^1(K, \mathscr{F}(\overline{\mathfrak{m}}))$ is a p-primary abelian group. The diagram compares the Kummer sequences over K for $\mathscr{F}$ and A. Here K can be any algebraic extension of F.

(4.8)

$$\begin{array}{ccccccccc} 0 & \to & \mathscr{F}(\mathfrak{m}_K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) & \overset{\kappa_{\mathscr{F}}}{\to} & H^1(K, C) & \to & H^1(K, \mathscr{F}(\overline{\mathfrak{m}}) & \to & 0 \\ & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \varepsilon} & & \\ 0 & \to & A(K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) & \overset{\kappa}{\to} & H^1(K, A[p^\infty]) & \to & H^1(K, A(\overline{K}))(p) & \to & 0 \end{array}$$

The vertical map δ is induced from the inclusion $\mathscr{F}(\mathfrak{m}_K) \subseteq A(K)$. Since for every finite extension L of F, the subgroup $\mathscr{F}(\mathfrak{m}_L)$ has finite index in $A(L)$, it

follows that δ is surjective. As a consequence, we see that $\mathrm{Im}(\kappa) = \lambda(\mathrm{Im}(\kappa_{\mathscr{F}}))$, and so

$$\mathrm{Im}(\kappa) \subseteq \mathrm{Im}(\lambda)\,. \tag{4.9}$$

We have proven (4.9) under the assumption that A has semistable reduction over F, but we then conclude from Lemma 4.2 that (4.9) holds without any hypothesis on A.

Here is our principal result. Let A be any abelian variety defined over F (we make no assumptions about the reduction of A). Let C be the canonical subgroup of $A[p^\infty]$; κ and λ are the maps in (4.1) and (4.6), which are defined with no restrictions on A.

Proposition 4.3 *Assume that K is a deeply ramified extension of F. Then* $\mathrm{Im}(\kappa) = \mathrm{Im}(\lambda)$.

Proof. If A has semistable reduction over F, the proposition follows from the basic result of section 3, namely the vanishing of $H^1(K, \mathscr{F}(\overline{\mathfrak{m}}))$. This implies that $\kappa_{\mathscr{F}}$ is surjective and so, by the remark above (4.9), we have proven Proposition 4.3 in this case. If we no longer assume that A has semistable reduction over F, we can certainly find a finite Galois extension F' of F such that A has semistable reduction over F. Put $\Delta = G(F'/F)$. Let $K' = KF'$, so that K' is deeply ramified also. Hence, by the above result, we have $\mathrm{Im}(\kappa') = \mathrm{Im}(\lambda')$. Hence Lemma 4.2 implies that $\mathrm{Im}(\kappa) = (\mathrm{Im}\,\lambda)_{\mathrm{div}}$. The next lemma then shows that $H^1(K, C)$ is divisible, whence $\mathrm{Im}\,\lambda$ is also divisible, since, as was remarked in Sect. 2, the fact that K is deeply ramified implies that the profinite degree of K over $\mathbb{Q}_p$ is infinitely divisible by p. Granted the lemma, this completes the proof of Proposition 4.3.

Lemma 4.4 *Let K be an algebraic extension of $\mathbb{Q}_p$ such that the profinite degree of K over $\mathbb{Q}_p$ is infinitely divisible by p. Let B be any divisible p-primary G_K-module. Then $H^1(K, B)$ is divisible.*

Proof. The fact that the profinite degree of K over $\mathbb{Q}_p$ is infinitely divisible by p implies that the p-primary subgroup of the Brauer group of every algebraic extension of K is 0, and it is well known (see [16]) that this implies that G_K has p-cohomological dimension equal to 1. Since B is divisible, we have the exact sequence of G_K-modules

$$0 \to B[p] \to B \xrightarrow{p} B \to 0\,.$$

Taking G_K-cohomology and noting that $H^2(K, B[p]) = 0$, it follows that multiplication by p is surjective on $H^1(K, B)$, as required.

The remainder of this section will concern the case $h = g$, including in particular the case where A has good, ordinary reduction over F. Even when K is a finite extension of F, the image of the Kummer homomorphism can be described in an elementary way in this case, and we have the following result.

Proposition 4.5 *Assume that $h = g$ and that K/F is a finite extension. Then* $\mathrm{Im}(\kappa) = \mathrm{Im}(\lambda)_{\mathrm{div}}$.

Proof. We begin again with the case where A has semistable reduction over F. It is enough to prove that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Im}(\lambda)) = g[K : \mathbb{Q}_p]$. For then the facts that $\mathrm{Im}(\kappa)$ is divisible, also has $\mathbb{Z}_p$-corank $g[K : \mathbb{Q}_p]$, and is contained in $\mathrm{Im}(\lambda)$ by (4.9) imply the proposition. The exact sequence

$$0 \to C \to A[p^\infty] \to D \to 0$$

gives another exact sequence

$$H^0(K, D) \xrightarrow{\mu} H^1(K, C) \xrightarrow{\lambda} H^1(K, A[p^\infty])$$

where the kernel of μ must be finite since $H^0(K, A[p^\infty])$ is obviously finite. Now the Euler–Poincaré characteristic of C over K is

$$\sum_{i=0}^{2} (-1)^i \mathrm{corank}_{\mathbb{Z}_p}(H^i(K, C)) = -g[K : \mathbb{Q}_p]$$

since we are assuming that $\mathrm{corank}_{\mathbb{Z}_p}(C) = g$. But clearly $H^0(K, C)$ is finite. Thus $H^1(K, C)$ has $\mathbb{Z}_p$-corank equal to $g[K : \mathbb{Q}_p] + e$, where $e = \mathrm{corank}_{\mathbb{Z}_p}(H^2(K, C))$. We will show that $e = \mathrm{corank}_{\mathbb{Z}_p}(H^0(K, D))$, and hence that indeed the $\mathbb{Z}_p$-corank of $\mathrm{Im}(\lambda)$ is $g[K : \mathbb{Q}_p]$. Let $V = T_p(A) \otimes \mathbb{Q}_p$, $W = T_p(C) \otimes \mathbb{Q}_p$, as before. Let V^t and W^t denote the corresponding $\mathbb{Q}_p$-spaces for the dual abelian variety. Since A is isogenous to A^t over F, we have $\dim_{\mathbb{Q}_p}(W) = \dim_{\mathbb{Q}_p}(W^t) = h$. Also the inertia group I_F acts trivially on both V/W and V^t/W^t. The Weil pairing induces a G_F-equivariant, non-degenerate pairing

$$V \times V^t \to \mathbb{Q}_p(1)\,.$$

Let $W^\perp$ be the orthogonal complement of W. Thus $W^\perp \cong \mathrm{Hom}(V/W, \mathbb{Q}_p(1))$ and so it is clear that $W^\perp$ has no quotient on which I_F acts trivially. But I_F acts trivially on

$$(W^\perp + W^t)/W^t \xrightarrow{\sim} W^\perp/(W^t \cap W^\perp)\,,$$

and so we conclude that $W^\perp \subset W^t$. Assuming $h = g$, it is then clear that $W^\perp = W^t$. Hence $W \xrightarrow{\sim} \mathrm{Hom}(V^t/W^t, \mathbb{Q}_p(1))$, and so, by Poitou–Tate duality, we have

$$e = \dim_{\mathbb{Q}_p}(H^2(K, W)) = \dim_{\mathbb{Q}_p}(H^0(K, V^t/W^t)) = \dim_{\mathbb{Q}_p}(H^0(K, V/W))$$

the last equality being true because A and A^t are isogenous over K. Thus we have $e = \mathrm{corank}_{\mathbb{Z}_p} H^0(K, D)$, as required.

If A is not semistable over F, then, as usual, we let F' be a finite Galois extension of F so that A over F' has semistable reduction. Then, in the notation of Lemma 4.2, we have $\mathrm{Im}(\kappa') = \mathrm{Im}(\lambda')_{\mathrm{div}}$. But, clearly, $\rho((\mathrm{Im}\,\lambda)_{\mathrm{div}}) \subseteq \mathrm{Im}(\lambda')_{\mathrm{div}}$, and so, by Lemma 4.2,

$$\mathrm{Im}(\lambda)_{\mathrm{div}} \subset (\rho^{-1}(\mathrm{Im}(\kappa')))_{\mathrm{div}} = \mathrm{Im}\,\kappa\,.$$

On the other hand, since $\mathrm{Im}(\kappa') \subset \mathrm{Im}(\lambda')$, Lemma 4.2 shows that $\mathrm{Im}\,\kappa \subset (\mathrm{Im}\,\lambda)_{\mathrm{div}}$. The proof of Proposition 4.5 is now complete.

It will be useful to know something about the quotient $\mathrm{Im}(\lambda)/\mathrm{Im}(\lambda)_{\mathrm{div}}$. In the case where A has good, ordinary reduction over F, we have the following precise result. Here $\tilde{A}$ denotes the reduction of the Neron model for A over O_F; $\mathscr{F}$ is as before the corresponding formal group.

Proposition 4.6 *Assume that* $[K : F] < \infty$ *and that* A *has good, ordinary reduction over* F. *Then*

$$\mathrm{Im}(\lambda)/\mathrm{Im}(\lambda)_{\mathrm{div}} \cong H^1(K, \mathscr{F}(\overline{\mathfrak{m}}))$$

and has the same order as the p*-primary subgroup of* $\tilde{A}(k)$, *where* $k = k_K$ *is the residue field for* K.

Proof. We first show that the map ε in diagram (4.8) is injective whenever A has good reduction. The exact sequence

$$0 \to \mathscr{F}(\overline{\mathfrak{m}}) \to A(\overline{K}) \to \tilde{A}(\overline{k}) \to 0$$

induces the exact cohomology sequence

$$A(K) \to \tilde{A}(k) \to H^1(K, \mathscr{F}(\overline{\mathfrak{m}})) \xrightarrow{\varepsilon} H^1(K, A(\overline{K}))$$

The injectivity of ε follows from the fact that the first map is surjective. Therefore (4.8) together with the surjectivity of δ show that

$$\mathrm{Im}(\lambda)/\mathrm{Im}(\kappa) \cong \mathrm{Im}(\varepsilon) \cong H^1(K, \mathscr{F}(\overline{\mathfrak{m}})) \tag{4.10}$$

just under the assumption that A has good reduction over F. This proves (4.10) for finite extensions K of F, and so all algebraic extensions K of F on passing to the inductive limit. When A has good ordinary reduction and $[K : F] < \infty$, the fact that $\mathrm{Im}(\kappa) = \mathrm{Im}(\lambda)_{\mathrm{div}}$ implies the isomorphism in the proposition. Moreover, since $H^1(K, C)$ has $\mathbb{Z}_p$-corank $g[K : \mathbb{Q}_p]$ (see the proof of Proposition 4.5, noting that $H^0(K, D)$ is now finite because K is a finite extension of F) and $\mathscr{F}(\mathfrak{m}_K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$ is a divisible group with the same $\mathbb{Z}_p$-corank, we see immediately from the top line of (4.8) that

$$H^1(K, \mathscr{F}(\overline{\mathfrak{m}})) \cong H^1(K, C)/H^1(K, C)_{\mathrm{div}} .$$

The exact sequence

$$0 \to T_p(C) \to W \to C \to 0 ,$$

where $W = T_p(C) \otimes \mathbb{Q}_p$, shows that $H^1(K, C)/H^1(K, C)_{\mathrm{div}}$ is isomorphic to the torsion subgroup of $H^2(K, T_p(C))$. But the Weil pairing shows that $\mathrm{Hom}(T_p(C), \mu_{p^\infty})$ is isomorphic to $\widetilde{A}^t[p^\infty]$. Thus Tate duality implies that $H^2(K, T_p(C))$ is dual to $H^0(K, \widetilde{A}^t[p^\infty])$, which in turn is isomorphic to the p-primary subgroup of $\widetilde{A}^t(k)$. Hence $H^2(K, T_p(C))$ is finite and has the same order as the p-primary subgroup of $\widetilde{A}^t(k)$. But since $\tilde{A}$ and $\widetilde{A}^t$ are isogenous over k, this order is the

same as that of the p-primary subgroup of $\tilde{A}(k)$. This completes the proof of Proposition 4.6.

We should point out that, under the hypotheses of Proposition 4.6, the above proof gives a canonical isomorphism of $\mathrm{Im}(\lambda)/\mathrm{Im}(\lambda)_{\mathrm{div}}$ with $\mathrm{Hom}(\tilde{A}^t(k), \mathbb{Q}_p/\mathbb{Z}_p)$. Thus its structure depends only on the residue field k of K. Also, if K/F is any finite Galois extension, then the action of $\mathrm{Gal}(K/F)$ on $H^1(K, \mathscr{F}(\overline{\mathfrak{m}}))$ and on $\mathrm{Im}(\lambda)/\mathrm{Im}(\lambda)_{\mathrm{div}}$ must be unramified. More generally, if K/F is any Galois extension and A has good, ordinary reduction over F, we obtain as a consequence that the action of $\mathrm{Gal}(K/F)$ on $H^1(K, \mathscr{F}(\overline{\mathfrak{m}}))$ and hence (by (4.10)) on $\mathrm{Im}(\lambda)/\mathrm{Im}(\kappa)$ is always unramified.

If $[K : F] = \infty$, then the conclusions in Propositions 4.5 or 4.6 may be false, even if A has good, ordinary reduction over F. Here is a simple example. Assume that A is an elliptic curve over F having good ordinary reduction. Then G_F acts on $\tilde{A}[p^\infty]$ by a certain unramified homomorphism $\varphi : G_F \to \mathbb{Z}_p^*$. Let K be the fixed field for the kernel of φ, so that K/F is an infinite unramified extension and $\mathrm{Gal}(K/F)$ is isomorphic to $\Delta \times \Gamma$, where Δ is a finite group and $\Gamma \cong \mathbb{Z}_p$. As a G_F-module, C is isomorphic to $\mu_{p^\infty} \otimes \varphi^{-1}$ (which can be identified with $\mathbb{Q}_p/\mathbb{Z}_p$ on which G_F acts by $\psi\varphi^{-1}$, where ψ is the cyclotomic character of G_F). Thus $H^1(K, C) \cong H^1(K, \mu_{p^\infty}) \otimes \varphi^{-1}$ for the action of $\mathrm{Gal}(K/F)$. But the structure of $H^1(K, \mu_{p^\infty})$ as a module over the Iwasawa algebra $\Lambda = \mathbb{Z}_p[[\Gamma]]$ can be described. (see Iwasawa [9], and also Greenberg [5], Sect. 3, Prop. 1). We immediately deduce the following description of the Λ-torsion submodule $t_\Lambda(X)$ of the Pontrjagin dual X of $H^1(K, C)$:

$$t_\Lambda(X) \xrightarrow{\sim} \mathbb{Z}_p(\varphi)\,,$$

where this is an isomorphism of $G(K/F)$-modules, with the right hand side being a copy of $\mathbb{Z}_p$ on which $G(K/F)$ acts via φ. As usual, if B is a discrete p-primary abelian group, we write $\widehat{B}$ for the Pontryagin dual of B. Now we have the exact sequence of Λ-modules

$$0 \to \widehat{\mathrm{Im}\,\lambda} \to X \to \widehat{\mathrm{Ker}\,\lambda} \to 0\,.$$

We claim that $t_\Lambda(\widehat{\mathrm{Im}\,\lambda}) = t_\Lambda(X)$. Indeed, $\mathrm{Ker}\,\lambda$ is a quotient of $H^0(K, D) = (\mathbb{Q}_p/\mathbb{Z}_p)(\varphi)$, and so $\widehat{\mathrm{Ker}\,\lambda}$ is a $G(K/F)$-submodule of $\mathbb{Z}_p(\varphi^{-1})$. As φ does not have finite order, we conclude that $t_\Lambda(X) \subset \widehat{\mathrm{Im}\,\lambda}$, as required. It follows that

$$t_\Lambda(\widehat{\mathrm{Im}\,\lambda}) \cong \mathbb{Z}_p(\varphi)\,.$$

If B is a discrete Λ-module, we write $\mathrm{div}_\Lambda(B)$ for the maximal Λ-divisible submodule of B (i.e. $\mathrm{div}_\Lambda(B)$ is the orthogonal complement under the dual pairing of the Λ-torsion submodule $t_\Lambda(\widehat{B})$ of $\widehat{B}$). Thus the above isomorphism is equivalent to

$$(\mathrm{Im}\,\lambda)/\mathrm{div}_\Lambda(\mathrm{Im}\,\lambda) \xrightarrow{\sim} (\mathbb{Q}_p/\mathbb{Z}_p)(\varphi^{-1})\,.$$

In particular, it follows that $\mathrm{Im}\,\lambda$ is a divisible abelian group (this also follows from Lemma 4.4). Let F' be any finite extension of F contained in K. Consider the image of $A(F')\otimes(\mathbb{Q}_p/\mathbb{Z}_p)$ under the composition of the following maps

$$A(F')\otimes(\mathbb{Q}_p/\mathbb{Z}_p)\to A(K)\otimes(\mathbb{Q}_p/\mathbb{Z}_p)\xrightarrow{\kappa}\mathrm{Im}(\lambda)\to\mathrm{Im}(\lambda)/\mathrm{div}_A(\mathrm{Im}\,\lambda)\,.$$

Using the facts that $A(F')\otimes(\mathbb{Q}_p/\mathbb{Z}_p)$ is a divisible group on which $\mathrm{Gal}(K/F')$ acts trivially and that $(\mathbb{Q}_p/\mathbb{Z}_p)(\varphi^{-1})^{\mathrm{Gal}(K/F')}$ is finite, it is clear that the image of $A(F')\otimes(\mathbb{Q}_p/\mathbb{Z}_p)$ is zero. Since this is so for all such $F'\subseteq K$, we see that $\mathrm{Im}(\kappa)\subseteq\mathrm{div}_A(\mathrm{Im}(\lambda))$. (In fact, one can show the equality $\mathrm{Im}(\kappa)=\mathrm{div}_A(\mathrm{Im}(\lambda))$). In this example, we have $\mathrm{Im}(\lambda)_{\mathrm{div}}=\mathrm{Im}(\lambda)$, whereas $\mathrm{Im}(\lambda)/\mathrm{Im}(\kappa)$ and $H^1(K,\mathscr{F}(\overline{\mathfrak{m}}))$ are nontrivial (and more precisely isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)(\varphi^{-1})$).

However, we will prove the equality $\mathrm{Im}(\kappa)=\mathrm{Im}(\lambda)$ for a class of fields larger than that covered by Proposition 4.3, assuming that $h=g$. The result is the following.

Proposition 4.7 *Assume that $h=g$ and that K/F is infinitely wildly ramified. Then* $\mathrm{Im}(\kappa)=\mathrm{Im}(\lambda)$.

Proof. Using Lemma 4.2, one can reduce to the case where A has semistable reduction over F. For otherwise, by passing to a finite Galois extension F' of F where A does have semistable reduction, the extension K'/F', where $K'=KF'$, will obviously be infinitely wildly ramified. Then the equality $\mathrm{Im}(\kappa')=\mathrm{Im}(\lambda')$ will imply $\mathrm{Im}(\kappa)=\mathrm{Im}(\lambda)$ by Lemma 4.2, since Lemma 4.4 shows that $\mathrm{Im}(\lambda)$ is divisible. Thus we assume A is semistable over F. Then $D=A[p^\infty]/C$ is an unramified G_F-module. The same is true for the module $D^t=A^t[p^\infty]/C^t$, corresponding to the dual abelian variety A^t.

Let $K=\bigcup_n F_n$, where F_n is a finite extension of F and $F_n\subset F_{n+1}$ for $n\geqq 1$. Denote κ_{A,F_n} by κ_n and λ_{A,F_n} by λ_n. The equality $\mathrm{Im}(\kappa)=\mathrm{Im}(\lambda)$ is equivalent to the assertion that

$$\varinjlim(\mathrm{Im}(\lambda_n)/\mathrm{Im}(\kappa_n))=0\,,$$

where the maps are induced by restriction

$$H^1(F_n,A[p^\infty])\to H^1(F_m,A[p^\infty])$$

for $m\geqq n$. By Proposition 4.5, we have $\mathrm{Im}(\kappa_n)=\mathrm{Im}(\lambda_n)_{\mathrm{div}}$, and hence it is enough to prove that

$$\varinjlim(H^1(F_n,C)/H^1(F_n,C)_{\mathrm{div}})=0\,. \tag{4.11}$$

Let F' be any finite extension of F contained in K. One has a canonical homomorphism of $H^1(F',C)/H^1(F',C)_{\mathrm{div}}$ to the torsion subgroup of $H^2(F',T_p(C))$. Also, since $h=g$, the Weil pairing induces an isomorphism

$$\mathrm{Hom}_{\mathrm{cont}}(T_p(C),\mu_{p^\infty})\cong D^t$$

(see the proof of Proposition 4.5). Thus $H^2(F', T_p(C))$ is dual to $H^0(F', D^t)$, which we denote more briefly by $D^t(F')$. Note that the group $D^t(F')$ depends only on the residue field $k_{F'}$. The same statement is obviously true for $D^t(F')/D^t(F')_{\text{div}}$ and also therefore for its dual $H^2(F', T_p(C))_{\text{tor}}$. We let $R(F') = D^t(F')/D^t(F')_{\text{div}}$.

To prove (4.11), it suffices to show that

$$\varinjlim H^2(F_n, T_p(C))_{\text{tor}} = 0 \,. \tag{4.12}$$

Here again the maps come from the restriction homomorphisms

$$\rho_{n,m} : H^2(F_n, T_p(C)) \to H^2(F_m, T_p(C))$$

for $m \geqq n$. Now $\rho_{n,m}$ is adjoint to the corestriction map (the norm map) $\gamma_{m,n} : D^t(F_m) \to D^t(F_n)$. Let $\delta_{m,n} : R(F_m) \to R(F_n)$ be the map induced by $\gamma_{m,n}$. It is enough then to prove

$$\varprojlim R(F_n) = 0 \,. \tag{4.13}$$

The facts that $R(F')$ depends only on $k_{F'}$ and that the ramification indices $e(F'/F)$ are divisible by arbitrarily high powers of p (for $F \subseteq F' \subseteq K$) will give (4.13).

Clearly there exists an n_0 such that, for $n \geqq n_0$, the $\mathbb{Z}_p$-corank of $D^t(F_n)$ is constant. Let F', F'' be finite extensions of F, with $F_{n_0} \subseteq F' \subseteq F'' \subseteq K$. The map $\varepsilon : R(F') \to R(F'')$ induced by the inclusion $D^t(F') \subseteq D^t(F'')$ is injective. If F''/F' is totally ramified, then ε is in fact an isomorphism. The corestriction map $\delta : R(F'') \to R(F')$ must then have image

$$\delta(R(F'')) \subseteq e(F''/F')R(F') \tag{4.14}$$

because $\delta \circ \varepsilon$ is multiplication by $[F'' : F']$. But (4.14) is clearly true even if F''/F' is not totally ramified since F''/L is totally ramified and has degree $e(F''/F')$, where L denotes the maximal unramified extension of F' contained in F''.

For any $n \geqq n_0$, $R(F_n)$ is a finite p-group. Let p^a be the exponent of $R(F_n)$. Choose $m > n$ so that $p^a | e(F_m/F_n)$. Then (4.14) shows that $\delta_{m,n}(R(F_m))$ is zero. This proves (4.13).

We would like to end this section by describing a more direct and simple approach to proving Propositions 4.5 and 4.7 in the case where A has good, ordinary reduction over F. For Proposition 4.7, we will also assume that K/F is Galois. As before, let $C = \text{Ker}(A[p^\infty] \to \tilde{A}[p^\infty])$ so that C is a G_F-submodule of $A[p^\infty]$ having $\mathbb{Z}_p$-corank g. For Proposition 4.5, it suffices to show that $\text{Im}(\kappa) \subseteq \text{Im}(\lambda)$ and that $\text{corank}_{\mathbb{Z}_p}(H^1(K, C)) = g[K : \mathbb{Q}_p]$. For then, the maximal divisible subgroup of $\text{Im}(\lambda)$ will contain $\text{Im}(\kappa) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{g[K:\mathbb{Q}_p]}$ and have the same $\mathbb{Z}_p$-corank. Thus, $\text{Im}(\kappa) = \text{Im}(\lambda)_{\text{div}}$.

The inclusion $\text{Im}(\kappa) \subseteq \text{Im}(\lambda)$ is quite easy to verify. Let $\alpha = P \otimes (1/p^t) \in A(K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$. Put $\varphi_\alpha(\sigma) = \sigma(R) - R$ for all $\sigma \in G_K$, where $R \in A(\overline{\mathbb{Q}}_p)$

satisfies $p^t R = P$. The cocycle φ_α determine a typical class in $\mathrm{Im}(\kappa)$. Now $\mathrm{Im}(\lambda)$ is the kernel of the natural map

$$H^1(K, A[p^\infty]) \to H^1(K, \tilde{A}[p^\infty])\,. \tag{4.15}$$

Under this map, the class of φ_α is sent to the class of $\widetilde{\varphi}_\alpha$, where $\widetilde{\varphi}_\alpha(\sigma) = \sigma(\widetilde{R}) - \widetilde{R}$. Here $\widetilde{R}$ is the image of R under the reduction map $A(\overline{\mathbb{Q}}_p) \to \tilde{A}(\bar{k})$, where $k = k_K$ and $\bar{k} = k_{\overline{\mathbb{Q}}_p}$ is an algebraic closure of k. But $\tilde{A}(\bar{k})$ is a torsion group and $\tilde{A}[p^\infty]$ is its p-primary subgroup. Thus the map

$$H^1(K, \tilde{A}[p^\infty]) \to H^1(K, \tilde{A}(\bar{k}))$$

is obviously injective. The 1-cocycle $\widetilde{\varphi}_\alpha$ is a coboundary for the G_K-module $\tilde{A}(\bar{k})$ and hence the class of φ_α must be in the kernel of (4.15). Hence $\mathrm{Im}(\kappa) \subseteq \mathrm{Im}(\lambda)$.

The assertion that $H^1(K, C)$ has $\mathbb{Z}_p$-corank $g[K : \mathbb{Q}_p]$ is implicit in the proof of Proposition 4.5 and can be verified by using the results of Poitou–Tate. The Euler–Poincare characteristic for the G_K-module C is $-g[K : \mathbb{Q}_p]$. But $H^0(K, C)$ is clearly finite. The Weil pairing gives an isomorphism

$$C \cong \mathrm{Hom}(T_p(\widetilde{A}^t), \mu_{p^\infty})\,.$$

Hence $H^2(K, C)$ is dual to $H^0(K, T_p(\widetilde{A}^t))$, which is 0. Thus, in fact,

$$H^2(K, C) = 0\,,$$

when A has good, ordinary reduction. It follows that $\mathrm{corank}_{\mathbb{Z}_p}(H^1(K, C)) = g[K : \mathbb{Q}_p]$, as needed.

As explained previously, $H^1(K, C)/H^1(K, C)_{\mathrm{div}}$ is isomorphic to $H^2(K, T_p(C))$, which is finite and dual to $H^0(K, \widetilde{A}^t[p^\infty])$. This is just the p-primary subgroup of $\widetilde{A}^t(k_K)$. Thus its order depends only on the residue field of the finite extension K of F. Thus the order of $\mathrm{Im}(\lambda)/\mathrm{Im}(\kappa)$ is bounded for all finite extensions K of F with given residue field. If K/F is now an infinite extension of F with finite residue field, it follows that the order of $\mathrm{Im}(\lambda)/\mathrm{Im}(\kappa)$ is finite. If K/F is infinitely wildly ramified, then $H^1(K, C)$ is divisible by Lemma 4.4 and consequently so is $\mathrm{Im}(\lambda)$. Hence the equality $\mathrm{Im}(\kappa) = \mathrm{Im}(\lambda)$ follows. Somewhat more generally, assume that K/F is Galois and infinitely wildly ramified. Let $\mathcal{G} = \mathrm{Gal}(K/F)$ and let $\mathcal{G}_0$ be its inertia subgroup. Then $\mathcal{G}/\mathcal{G}_0$ is topologically cyclic and so $\mathcal{G}$ is a semidirect product, i.e. there exists a subgroup $\mathcal{H}$ mapped isomorphically to $\mathcal{G}/\mathcal{G}_0$ by the canonical homomorphism. One then sees that $K = \bigcup_{n \geqq 1} F_n$, where F_n/F is infinitely wildly ramified with finite residue field for all $n \geqq 1$. The above discussion shows that $\mathrm{Im}(\kappa_{F_n}) = \mathrm{Im}(\lambda_{F_n})$. But then it follows that $\mathrm{Im}(\kappa) = \mathrm{Im}(\lambda)$, proving Proposition 4.7 when A has good, ordinary reduction over F and K/F is a Galois extension which is infinitely wildly ramified.

Finally, we mention an interesting consequence of our description of the image of the Kummer map.

Proposition 4.8 *Let K be any infinitely wildly ramified extension of $\mathbb{Q}_p$ such that $\mathrm{Im}(\kappa) = \mathrm{Im}(\lambda)$. Let D be the G_F-module $D = A[p^\infty]/C$. Then there is a canonical isomorphism*

$$H^1(K, A(\overline{\mathbb{Q}}_p))(p) \xrightarrow{\sim} H^1(K, D)\ . \tag{4.16}$$

Proof. We simply compare the exact bottom row of (4.8) (which, of course, holds without any assumption on A), with the exact sequence of Galois cohomology

$$0 \to \mathrm{Im}(\lambda) \to H^1(K, A[p^\infty]) \to H^1(K, D) \to 0\ .$$

Note that the map on the right of this last exact sequence is surjective because G_K has cohomological dimension 1 (cf. the proof of Lemma 4.4). This completes the proof.

The usefulness of Proposition 4.8 is that it is usually much easier to study the cohomology of the divisible torsion module D rather than of $A(\overline{\mathbb{Q}}_p)$. In particular, one can easily derive some classical results of Iwasawa theory from it. Let K be a ramified $\mathbb{Z}_p$-extension of F, let $\Gamma = G(K/F)$, and let us write $\Lambda = \mathbb{Z}_p[[\Gamma]]$ for the Iwasawa algebra of Γ. As usual, if M is a G_F-module, we put $M(K) = M^{G_K}$, where $G_K = G(\overline{\mathbb{Q}}_p/K)$. In the following result, we continue to make no hypothesis on the nature of the reduction of A.

Proposition 4.9 *Let K be any ramified $\mathbb{Z}_p$-extension of F. Then*:

(i) *The Pontrjagin dual of $H^1(K, A(\overline{\mathbb{Q}}_p))(p)$ is a finitely generated Λ-module of Λ-rank equal to $(2g-h)[F:\mathbb{Q}_p]$. Its Λ-torsion submodule is pseudo-isomorphic to $\mathrm{Hom}(D, \mu_{p^\infty})(K)$.*

(ii) *If $A^t[p^\infty](K)$ is finite, then the Pontrjagin dual of $H^1(K, A(\overline{\mathbb{Q}}_p))(p)$ has no non-zero Λ-torsion.*

(iii) *The Pontrjagin dual of $A(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is a finitely generated Λ-module of Λ-rank equal to $h[F:\mathbb{Q}_p]$.*

Proof. We simply apply standard arguments of Iwasawa theory, based on Tate's Euler characteristic theorem (see Sect. 3 of [5]). Since D has $\mathbb{Z}_p$-corank equal to $2g-h$, (i) is given by applying Proposition 1 of Sect. 3 of [5] to $H^1(K, D)$. To prove (iii), we dualize the Kummer exact sequence

$$0 \to A(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(K, A[p^\infty]) \to H^1(K, A(\overline{\mathbb{Q}}_p))(p) \to 0\ ,$$

and apply Proposition 1 of Sect. 3 of [5] to both $H^1(K, D)$ and $H^1(K, A[p^\infty])$. Finally, to prove (ii) we use Corollary 1 of Sect. 3 of [5], recalling that $\mathrm{Hom}(A[p^\infty], \mu_{p^\infty}) = T_p(A^t)$ by the Weil pairing. This complete the proof.

5 Universal norms

Again, F will denote a finite extension of $\mathbb{Q}_p$, and A an abelian variety defined over F. We write A^t for the dual abelian variety over F. In general, we shall use the notation given in the introduction. Thus, if X is a torsion abelian group, $X(p)$ will denote its p-primary subgroup, and, if X is a profinite abelian group, X_p will denote its maximal pro-p-subgroup. Let K be any extension of F contained in $\overline{\mathbb{Q}}_p$, and let

$$r_{K/F} : H^1(F, A(\overline{\mathbb{Q}}_p))(p) \to H^1(K, A(\overline{\mathbb{Q}}_p))(p) \tag{5.1}$$

be the restriction map. As explained in Sect. 1, if we define the group of universal norms on A^t from K to be

$$N_{K/F}(A^t) = \bigcap_{F'} N_{F'/F}(A^t(F')) ,$$

where F' runs over all finite extensions of F contained in K, then Tate duality gives rise to a canonical dual pairing between $\mathrm{Im}(r_{K/F})$ and $N_{K/F}(A^t)_p$. Our aim in this section is to find an explicit description of $\mathrm{Im}(r_{K/F})$, or equivalently of $N_{K/F}(A^t)_p$, in terms of the G_F-module $A[p^\infty]$. Our method of proof works for any field K for which $\mathrm{Im}(\kappa) = \mathrm{Im}(\lambda)$, where κ and λ are the maps defined in (4.1) and (4.6). The results we obtain seem to include all special cases about universal norms treated in the literature (in particular, see [8], [10], [11], [12], [14], [19]), and to go considerably further.

We begin by making some general remarks about the group of universal norms. Let F' be any finite extension of F which is contained in K. Then $N_{F'/F}(A^t(F'))$ is a closed subgroup of $A^t(F)$, because $N_{F'/F}$ is continuous and $A^t(F')$ is compact. Hence $N_{K/F}(A^t)$ is also a closed subgroup of $A^t(F)$, and so, by (4.2), must be of the form

$$N_{K/F}(A^t) \xrightarrow{\sim} \mathbb{Z}_p^u \times (\text{a finite group}) , \tag{5.2}$$

where $u = u(A^t, K/F)$ is an integer satisfying $0 \leqq u \leqq g[F : \mathbb{Q}_p]$, and, as earlier, g is the dimension of A and A^t. Let q be a prime different from p, and let $N_{K/F}(A^t)_q$ be the maximal pro-q-subgroup of $N_{K/F}(A^t)$. It follows from (5.2) that $N_{K/F}(A^t)_q$ is a finite group, and (4.2) shows that

$$N_{K/F}(A^t)_q = \bigcap_{F'} N_{F'/F}(A^t[q^\infty](F')) ,$$

where F' runs over all finite extensions of F contained in K, and $A^t[q^\infty](F')$ denotes the subgroup of $A^t[q^\infty]$ consisting of elements fixed by the Galois group of $\overline{\mathbb{Q}}_p$ over F'. Hence we note that $N_{K/F}(A^t)_q$ is determined by the G_F-module $A^t[q^\infty]$. Alternatively, one could use Tate duality applied to the q-primary parts to assert that the q-primary subgroup of $A^t(F)/N_{K/F}(A^t)$ is dual to the kernel of the restriction map from $H^1(F, A[q^\infty])$ to $H^1(K, A[q^\infty])$. This observation will be useful later in the proof of Proposition 5.7. We next note

that the study of $N_{K/F}(A^t)$ is really only non-trivial when K is an infinitely wildly ramified extension of F.

Lemma 5.1 *Let K be an extension of F which is not infinitely wildly ramified. Then $N_{K/F}(A^t)$ is of finite index in $A^t(F)$.*

Proof. Assume that K is not infinitely wildly ramified. Then we can reduce to the tame situation by noting that we can find a field F_1 with $F \subset F_1 \subset K$ such that F_1/F is finite and K/F_1 is tamely ramified. As

$$N_{F_1/F}(N_{K/F_1}(A^t)) \subset N_{K/F}(A^t)\,,$$

it plainly suffices to show that $N_{K/F_1}(A^t)$ is of finite index in $A^t(F_1)$. To prove this latter statement it suffices to show that, as L_1 runs over all finite extensions of F_1 contained in K, the index of $N_{L_1/F_1}(A^t(L_1))$ in $A^t(F_1)$ is bounded above by a quantity which does not depend on L_1. Let $\mathscr{F}_1^t$ denote the formal group over O_{F_1} which is attached to the Néron model of A^t over F_1. Put $W_1 = A^t(F_1)/\mathscr{F}_1^t(\mathfrak{m}_{F_1})$, so that W_1 is a finite abelian group. If L_1 is an arbitrary extension of F_1 contained in K, then L_1/F_1 is tamely ramified, and so $N_{L_1/F_1}(\mathscr{F}_1^t(\mathfrak{m}_{L_1})) = \mathscr{F}_1^t(\mathfrak{m}_{F_1})$ by Proposition 3.9. It follows that $A^t(F_1)/N_{L_1/F_1}(A^t(L_1))$ is isomorphic to a quotient of W_1, and hence has order bounded by the order of W_1, which is independent of L_1. This completes the proof of Lemma 5.1.

We recall from Sect. 4 that we have the canonical exact sequence of G_F-modules

$$0 \to C \to A[p^\infty] \to D \to 0\,, \tag{5.3}$$

and we now proceed to show that this sequence provides a rather precise description of $N_{K/F}(A^t)_p$ in many cases. To this end, we consider the map

$$\pi_F : H^1(F, A[p^\infty]) \to H^1(F, D) \tag{5.4}$$

which is induced by (5.3), and also the restriction map

$$\rho_{K/F} : H^1(F, D) \to H^1(K, D)\,. \tag{5.5}$$

Since it is now important to distinguish between the base field F and the extension K, we shall write κ_K for the Kummer map (4.1), and λ_K for the map (4.6). For simplicity, we put

$$\Omega(A, K/F) = \mathrm{Im}(\pi_F)/(\mathrm{Im}(\pi_F) \cap \mathrm{Ker}(\rho_{K/F}))\,. \tag{5.6}$$

Theorem 5.2 *Let K be an algebraic extension of F such that* $\mathrm{Im}(\kappa_K) = \mathrm{Im}(\lambda_K)$. *Then we have*:
(i) *a canonical isomorphism* $\mathrm{Im}(r_{K/F}) \xrightarrow{\sim} \Omega(A, K/F)$;
(ii) *a canonical dual pairing*

$$N_{K/F}(A^t)_p \times \Omega(A, K/F) \to \mathbb{Q}_p/\mathbb{Z}_p\,.$$

In particular, the integer $u = u(A,K/F)$ *appearing in* (5.1) *is equal to the* $\mathbb{Z}_p$*-corank of* $\Omega(A,K/F)$.

Remark. Proposition 4.3 shows that the conclusions of Theorem 5.2 are valid for all A when K is deeply ramified. If we only assume the weaker condition that K is infinitely wildly ramified, then Proposition 4.7 shows that the conclusions of Theorem 5.2 hold for those A satisfying $h = g$.

Proof. It suffices to prove (i), since Tate duality provides a canonical dual pairing between $\mathrm{Im}(r_{K/F})$ and $N_{K/F}(A^t)_p$. We plainly have the commutative diagram

$$\begin{array}{ccc} H^1(K,A[p^\infty]) & \xrightarrow{\beta_K} & H^1(K,A(\overline{\mathbb{Q}}_p))(p) \\ \uparrow{\scriptstyle s_{K/F}} & & \uparrow{\scriptstyle r_{K/F}} \\ H^1(F,A[p^\infty]) & \xrightarrow{\beta_F} & H^1(F,A(\overline{\mathbb{Q}}_p))(p)\,, \end{array}$$

where the horizontal maps are induced by the inclusion of $A[p^\infty]$ in $A(\overline{\mathbb{Q}}_p)$, and where the vertical maps are the restriction maps. Now the exact sequence of Kummer theory for A shows that both β_F and β_K are surjective. In particular, the surjectivity of β_F and the commutativity of the diagram imply that

$$\mathrm{Im}(r_{K/F}) = \mathrm{Im}(r_{K/F} \circ \beta_F) = \mathrm{Im}(\beta_K \circ s_{K/F})\,. \tag{5.7}$$

We can analyse the group on the right by noting that $\mathrm{Ker}(\beta_K) = \mathrm{Im}(\kappa_K)$ by the exact sequence of Kummer theory. Also, $\mathrm{Im}(\lambda_K) = \mathrm{Ker}(\pi_K)$, by the long exact sequence of cohomology from (5.3). Hence our hypothesis that $\mathrm{Im}(\lambda_K) = \mathrm{Im}(\kappa_K)$ tells us that there is an injection j of $H^1(K,A(\overline{\mathbb{Q}}_p))(p)$ into $H^1(K,D)$ making the following diagram commutative

$$\begin{array}{ccc} H^1(K,A[p^\infty]) & \xrightarrow{\beta_K} & H^1(K,A(\overline{\mathbb{Q}}_p))(p) \\ & \searrow{\scriptstyle \pi_K} & \downarrow{\scriptstyle j} \\ & & H^1(K,D). \end{array} \tag{5.8}$$

The map j induces an isomorphism from $H^1(K,A(\overline{\mathbb{Q}}_p))(p)$ onto $\mathrm{Im}(\pi_K)$, which, in turn, induces an isomorphism

$$\mathrm{Im}(\beta_K \circ s_{K/F}) \xrightarrow{\sim} \mathrm{Im}(\pi_K \circ s_{K/F})\,.$$

But now we have the commutative diagram

$$\begin{array}{ccc} H^1(K,A[p^\infty]) & \xrightarrow{\pi_K} & H^1(K,D) \\ \uparrow{\scriptstyle s_{K/F}} & & \uparrow{\scriptstyle \rho_{K/F}} \\ H^1(F,A[p^\infty]) & \xrightarrow{\pi_F} & H^1(F,D)\,, \end{array} \tag{5.9}$$

and so (5.7) and our previous remark gives canonical isomorphisms

$$\mathrm{Im}(r_{K/F}) \xrightarrow{\sim} \mathrm{Im}(\rho_{K/F} \circ \pi_F) \xrightarrow{\sim} \Omega(A,K/F)\,. \tag{5.10}$$

Assertion (i) of Theorem 5.2 is now given by (5.10).

The proof of Theorem 5.2 can be made more explicit as follows. Let $A^t(F)_p$ be the maximal pro-p-subgroup of $A^t(F)$, and let

$$\langle\ ,\ \rangle_F : H^1(F, A(\overline{\mathbb{Q}}_p))(p) \times A^t(F)_p \to \mathbb{Q}_p/\mathbb{Z}_p \tag{5.11}$$

be the Tate pairing. Now, since β_F is surjective, we can define an inclusion reversing bijection between the set of subgroups of $H^1(F, A[p^\infty])$ which contain $\mathrm{Ker}(\beta_F)$ and the set of closed subgroups of $A^t(F)_p$, by mapping such a subgroup X of $H^1(F, A[p^\infty])$ to the orthogonal complement of $\beta_F(X)$ under (5.11). Note that we always have

$$\mathrm{Ker}(\beta_F) \subset \mathrm{Ker}(\pi_F)$$

as was pointed out in (4.9) of Sect. 4 (but this will not, in general, be an equality because F is a finite extension of $\mathbb{Q}_p$). We define U_F to be the subgroup of $A^t(F)_p$ which corresponds to $\mathrm{Ker}(\pi_F)$, that is

$$U_F = \text{orthogonal complement of } \beta_F(\mathrm{Ker}(\pi_F)) \text{ under (5.11)}. \tag{5.12}$$

This subgroup U_F will play an important role in the arguments of the rest of this section. It is clear from the above remarks that (5.11) induces an isomorphism

$$U_F \xrightarrow{\sim} (H^1(F, A(\overline{\mathbb{Q}}_p))(p))/\beta_F(\mathrm{Ker}(\pi_F))^\wedge \xrightarrow{\sim} \mathrm{Im}(\pi_F)^\wedge\ , \tag{5.13}$$

where, as before, the symbol $^\wedge$ denotes the Pontrjagin dual. On the other hand, Tate duality shows that the subgroup of $H^1(F, A[p^\infty])$ which corresponds to $N_{K/F}(A^t)_p$ is equal to $\mathrm{Ker}(r_{K/F} \circ \beta_F)$. But we claim, in fact, that

$$\mathrm{Ker}(r_{K/F} \circ \beta_F) = \mathrm{Ker}(\rho_{K/F} \circ \pi_F)\ , \tag{5.14}$$

because of our hypothesis that $\mathrm{Im}(\kappa_K) = \mathrm{Im}(\lambda_K)$. Indeed, as remarked above, we have $r_{K/F} \circ \beta_F = \beta_K \circ s_{K/F}$. Now (5.8) shows that

$$\mathrm{Ker}(\beta_K \circ s_{K/F}) = \mathrm{Ker}(j \circ \beta_K \circ s_{K/F}) = \mathrm{Ker}(\pi_K \circ s_{K/F})\ .$$

Then (5.14) follows from (5.9), which gives the equality $\pi_K \circ s_{K/F} = \rho_{K/F} \circ \pi_F$. Since we obviously have $\mathrm{Ker}(\pi_F)$ is contained in $\mathrm{Ker}(\rho_{K/F} \circ \pi_F)$, it follows that $N_{K/F}(A^t)_p \subset U_F$. More precisely, $N_{K/F}(A^t)_p$ is completely determined by $\mathrm{Ker}(\rho_{K/F} \circ \pi_F)$, which, in turn, is determined by the subgroup $\mathrm{Im}(\pi_F) \cap \mathrm{Ker}(\rho_{K/F})$ of $H^1(F, D)$. We also obtain isomorphisms

$$U_F/N_{K/F}(A^t)_p \xrightarrow{\sim} (\mathrm{Ker}(\rho_{K/F} \circ \pi_F)/\mathrm{Ker}(\pi_F))^\wedge \xrightarrow{\sim} (\mathrm{Im}(\pi_F) \cap \mathrm{Ker}(\rho_{K/F}))^\wedge\ . \tag{5.15}$$

Of course, (5.13) and (5.15) imply, in particular, assertion (ii) of Theorem 5.2. In any case, this completes the proof of Theorem 5.2.

We remark that, if A has semistable reduction over F, then there is a simple alternative description of the subgroup U_F of $A^t(F)$, which is defined by (5.12). Let $\mathscr{F}$ denote the formal group over O_F which is attached to the Néron model of A over O_F. Then, as was remarked in Sect. 4, we have $C = \mathscr{F}(\overline{\mathfrak{m}})[p^\infty]$.

Also the diagram (4.8) yields, in particular, the commutative diagram with exact rows

$$\begin{array}{ccccc} H^1(F,C) & \to & H^1(F,\mathscr{F}(\overline{\mathfrak{m}})) & \to & 0 \\ \downarrow{\scriptstyle \lambda_F} & & \downarrow{\scriptstyle \varepsilon_F} & & \\ H^1(F,A[p^\infty]) & \overset{\beta_F}{\to} & H^1(F,A(\overline{\mathbb{Q}}_p))(p) & \to & 0\,. \end{array}$$

Now we have $\mathrm{Ker}(\pi_F) = \mathrm{Im}(\lambda_F)$, and so the diagram implies that

$$\beta_F(\mathrm{Ker}\,\pi_F) = \mathrm{Im}(\beta_F \circ \lambda_F) = \mathrm{Im}(\varepsilon_F)\,. \tag{5.16}$$

Hence U_F is the maximal pro-p subgroup of $A^t(F)$ which is orthogonal to $\mathrm{Im}(\varepsilon_F)$ under the Tate pairing (5.10). In particular, we have

$$A^t(F)_p/U_F \overset{\sim}{\to} \mathrm{Im}(\varepsilon_F)^\wedge\,. \tag{5.17}$$

In view of Theorem 5.2, it is clearly of interest to determine $\mathrm{Im}(\pi_F)$, and, in particular, to calculate its $\mathbb{Z}_p$-corank.

Proposition 5.3 *If A has potential good reduction, then π_F is surjective, and the $\mathbb{Z}_p$-corank of $H^1(F,D)$ is equal to $(2g-h)[F:\mathbb{Q}_p]$.*

Proof. We postpone as far as possible in the proof any hypothesis about the nature of the reduction of A. We have the Weil pairing

$$T_p(A^t) \times A[p^\infty] \to \mu_{p^\infty}\,. \tag{5.18}$$

The first consequence we can deduce from (5.18) is that

$$H^2(F,A[p^\infty]) = 0\,, \tag{5.19}$$

since Tate duality and (5.18) imply that this group is dual to $H^0(F,T_p(A^t)) = 0$. Taking G_F-cohomology of (5.3), and recalling that G_F has cohomological dimension equal to 2, we deduce that $H^2(F,D) = 0$, and that we have the exact sequence

$$H^1(F,A[p^\infty]) \overset{\pi_F}{\to} H^1(F,D) \to H^2(F,C) \to 0\,. \tag{5.20}$$

Since $H^2(F,D) = 0$ and D is a divisible G_F-module of $\mathbb{Z}_p$-corank equal to $2g-h$, the Euler characteristic theorem implies that

$$\mathrm{corank}_{\mathbb{Z}_p} H^1(F,D) = (2g-h)[F:\mathbb{Q}_p] + \mathrm{corank}_{\mathbb{Z}_p} H^0(F,D)\,. \tag{5.21}$$

On the other hand, Tate duality shows that $H^2(F,C)$ is dual to $H^0(F,\mathrm{Hom}(C,\mu_{p^\infty}))$. Now let $R = (C)^\perp$ be the orthogonal complement of C in the Weil pairing (5.18), so that

$$\mathrm{Hom}(C,\mu_{p^\infty}) \overset{\sim}{\to} T_p(A^t)/R\,; \tag{5.22}$$

note that this isomorphism also shows that $T_p(A^t)/R$ is a free $\mathbb{Z}_p$-module. Now $R = \mathrm{Hom}(D,\mu_{p^\infty})$. Let I_F denote the inertial subgroup of G_F. Since I_F acts

on D via a finite quotient, it is clear that there is no non-zero quotient of R, which is a free $\mathbb{Z}_p$-module and a G_F-module, on which I_F acts via a finite quotient. Moreover, since I_F acts via a finite quotient on the free $\mathbb{Z}_p$-module $T_p(D^t) = T_p(A^t[p^\infty])/T_p(C^t)$, the same assertion is true for its G_F-submodule

$$(R + T_p(C^t))/T_p(C^t) \xrightarrow{\sim} R/(R \cap T_p(C^t)) .$$

But the module on the right is a free $\mathbb{Z}_p$-module and a quotient of R on which I_F acts via a finite quotient, and so we must have $R \subset T_p(C^t)$. We then have the exact sequence

$$0 \to T_p(C^t)/R \to T_p(A^t)/R \to T_p(D^t) \to 0 . \tag{5.23}$$

But it was remarked at the beginning of Sect. 4 that C^t has the additional property that I_F does not act on a non-zero quotient of C^t via a finite quotient. It follows that there is no non-zero quotient of $T_p(C^t)$, which is a free $\mathbb{Z}_p$-module, on which I_F acts via a finite quotient, and so $(T_p(C^t)/R)^{G_F} = 0$. Taking G_F-invariants of (5.23), we obtain an injection

$$(T_p(A^t)/R)^{G_F} \hookrightarrow T_p(D^t)^{G_F} . \tag{5.24}$$

In view of (5.22), this certainly implies that we always have

$$\mathrm{corank}_{\mathbb{Z}_p} (H^2(F, C)) \leqq \mathrm{corank}_{\mathbb{Z}_p} (H^0(F, D^t)) \tag{5.25}$$

Note also that, since A is isogenous to A^t over F, the $\mathbb{Z}_p$-coranks of $H^0(F, D)$ and $H^0(F, D^t)$ are equal. All of this holds so far without any hypothesis on the reduction of A. Let us now suppose that A has potential good reduction, and let F' denote a finite extension of F over which A achieves good reduction. The dual abelian variety A^t will also have good reduction over F'. Let $\tilde{A}^t$ denote the reduction of A^t over F'. Then $D^t = \tilde{A}^t[p^\infty]$, whence $(D^t)^{G_F}$ is clearly finite, and so $T_p(D^t)^{G_F} = 0$. It follows from (5.24) that $(T_p(A^t)/R)^{G_F} = 0$, and thus $H^2(F, C) = 0$. The assertions of Proposition 5.3 are now clear from (5.20) and (5.21), because $H^0(F, D) = \tilde{A}[p^\infty]^{G_F}$ is also finite. This completes the proof of Proposition 5.4.

We now study a number of special cases of Theorem 5.2.

Case I. $h = 2g$.
This case is, of course, equivalent to $D = 0$. Hence Theorem 5.2 proves that, for any deeply ramified extension K of F, the group of universal norms $N_{K/F}(A^t)$ is finite and of order prime to p. When K is a ramified $\mathbb{Z}_p$-extension of F, this result is classical.

Case II. $h > g$.
This leads us to an interesting new criterion for an extension K of F to be deeply ramified. A result of McCallum (Theorem 1 of [13]) asserts that if K is an extension of F of finite conductor, then $N_{K/F}(A)$ is necessarily of finite index in $A(F)$.

Proposition 5.4 *Let A be a semistable abelian variety defined over F, and let $\mathscr{F}$ be the corresponding formal group over O_F. Assume that $\mathscr{F}$ has height $h > g = \dim(A)$. Let K be any algebraic extension of F. Then K is deeply ramified if and only if $H^1(K, \mathcal{F}(\overline{\mathfrak{m}})) = 0$.*

Proof. If K is deeply ramified, we have already shown in Sect. 3 that $H^1(K, \mathscr{F}(\overline{\mathfrak{m}})) = 0$ for all formal groups which are defined over the ring of integers of some finite extension of $\mathbb{Q}_p$ which is contained in K.

Now assume that $\mathscr{F}$ is as in Proposition 5.4. We first observe that, if L is any finite extension of F, then $H^1(L, \mathscr{F}(\overline{\mathfrak{m}}))$ has positive $\mathbb{Z}_p$-corank, and so is certainly non-zero. Indeed, since $\mathscr{F}(\overline{\mathfrak{m}})$ is divisible, we have the Kummer sequence (cf. (4.8))

$$0 \to \mathscr{F}(\mathfrak{m}_L) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(L, C) \to H^1(L, \mathscr{F}(\overline{\mathfrak{m}})) \to 0 .$$

The term on the left has $\mathbb{Z}_p$-corank equal to $g[L : \mathbb{Q}_p]$, and the Euler characteristic theorem shows that the $\mathbb{Z}_p$-corank of the middle term is $\geqq h[L : \mathbb{Q}_p]$. Hence $H^1(L, \mathscr{F}(\overline{\mathfrak{m}}))$ has $\mathbb{Z}_p$-corank $\geqq (h - g)[L : \mathbb{Q}_p]$, which is strictly positive because $h > g$.

Now let K be an algebraic extension of F such that $H^1(K, \mathscr{F}(\overline{\mathfrak{m}})) = 0$. We deduce from (4.8) that $\mathrm{Im}(\kappa_{A,K}) = \mathrm{Im}(\lambda_{A,K})$. Now let L be any finite extension of F contained in K. We deduce immediately from Theorem 5.2 that the $\mathbb{Z}_p$-rank of $N_{K/L}(A^t)_p$ is bounded above by the $\mathbb{Z}_p$-corank of $H^1(L, D)$, and hence, by the Euler characteristic theorem (see (5.21)), we have

$$\mathrm{rank}_{\mathbb{Z}_p}(N_{K/L}(A^t)_p) \leqq (2g - h)[L : \mathbb{Q}_p] + \mathrm{corank}_{\mathbb{Z}_p}(H^0(L, D)) . \tag{5.26}$$

But the $\mathbb{Z}_p$-corank of $H^0(L, D)$ is clearly at most $(2g - h)$, and we have $2g - h < g$ because $h > g$. On the other hand, $A(L)_p$ has $\mathbb{Z}_p$-rank equal to $g[L : \mathbb{Q}_p]$. Hence $N_{K/L}(A^t)$ cannot have finite index in $A^t(L)$ provided we choose L so that

$$[L : \mathbb{Q}_p] > (2g - h)/(h - g) . \tag{5.27}$$

But it was remarked above that $H^1(K, \mathscr{F}(\overline{\mathfrak{m}})) = 0$ certainly implies that K is an infinite extension of F, and thus we can clearly choose L so that (5.27) is satisfied. But then McCallum's theorem [13] implies that K does not have finite conductor over L, and hence K is deeply ramified. This completes the proof of Proposition 5.4.

Remark. It seems quite possible that the equivalence of $H^1(K, \mathscr{F}(\overline{\mathfrak{m}})) = 0$ and K being deeply ramified is valid for any commutative formal group $\mathscr{F}$ defined over the ring of integers of some finite extension of $\mathbb{Q}_p$ contained in K, provided that the height of h of $\mathscr{F}$ is strictly greater than the dimension g of $\mathscr{F}$. It would be interesting to find a proof of this statement.

Case III. A has good reduction over F and K/F is Galois.
Suppose now that A has good reduction over F, and let $\tilde{A}$ denote the reduction of A. We then have $D = \tilde{A}[p^\infty]$. By Proposition 5.2, we know that π_F is surjective in this case, and $\mathrm{Im}(\pi_F)$ has $\mathbb{Z}_p$-corank equal to $(2g-h)[F:\mathbb{Q}_p]$. Assume further that K is a Galois extension of F, and write $\mathcal{G} = G(K/F)$. Then $\mathrm{Ker}(\rho_{K/F}) = H^1(\mathcal{G}, D(K))$, where $D(K)$ denotes the subgroup of D which is fixed by $G(\overline{\mathbb{Q}}_p/K)$, which is plainly equal to the p-primary subgroup of $\tilde{A}(k_K)$ (here k_K denotes the residue field of K). Suppose now that K is deeply ramified. We deduce immediately from (5.7) that $u = u(A, K/F)$ is given by

$$u = (2g-h)[F:\mathbb{Q}_p] - \mathrm{corank}_{\mathbb{Z}_p}(H^1(\mathcal{G}, D(K))) \,. \tag{5.28}$$

Only the second term on the right depends on K, and indeed this can vary with K. For example, if $K = \overline{\mathbb{Q}}_p$, then $H^1(\mathcal{G}, D(K)) = H^1(F, D)$, and so $u = 0$. On the other hand, if the residue field k_K of K is finite, then $D(K)$ is finite, and thus $u = (2g-h)[F:\mathbb{Q}_p]$. In fact, under these hypotheses, one has the stronger result that the universal norm group $N_{K/F}(A^t)$ is almost independent of K.

Proposition 5.5 *Assume that A has good reduction over F. Let K be a Galois extension of F which is deeply ramified, and whose residue field k_K is finite. Then $N_{K/F}(A^t)_p$ is a subgroup of finite index in U_F.*

Proof. This follows immediately from (5.15) and the fact that $\mathrm{Ker}(\rho_{K/F})$ is finite. In fact, we have the precise statement

$$U_F/N_{K/F}(A^t)_p \xrightarrow{\sim} H^1(\mathcal{G}, \tilde{A}(k_K)(p))^\wedge \,. \tag{5.29}$$

We now make several remarks about the Proposition. If one assumes that K/F is totally ramified, then $k_K = k_F$, and so (5.29) shows that $U_F/N_{K/F}(A^t)_p$ is isomorphic as a group to $\mathrm{Hom}(\mathcal{G}, \tilde{A}(k_F)(p))$. This latter group has a bound for its order which depends only on F and g, and does not depend on K or A. On the other hand, it will be useful later to know that there is always an extension K of F satisfying the hypotheses of the above proposition such that $N_{K/F}(A^t)_p = U_F$. Suppose first that p is odd. Let F' be any ramified quadratic extension of F, and take K to be any $\mathbb{Z}_p$-extension of F' such that K/F is Galois and $G(F'/F)$ acts on $G(K/F')$ by the non-trivial character of $G(F'/F)$. The existence of such K follows from local class field theory. It is clear that K is a totally ramified extension of F, and thus $k_K = k_F$. Moreover, we have $\mathrm{Hom}(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) = 0$, since F' is plainly the maximal abelian extension of F contained in K. Hence (5.29) shows that $N_{K/F}(A^t)_p = U_F$. But K is deeply ramified because it is a ramified $\mathbb{Z}_p$-extension of F', and so provides the required example in this case. Suppose next that $p = 2$. Take F' to be any finite tamely ramified Galois extension of F such that (i) $[F':F]$ is odd, and (ii) the inertial subgroup I of $G(F'/F)$ is non-trivial. Let L' be the composite of all $\mathbb{Z}_2$-extensions of F'. Then L' is Galois over F, and I operates on $G(L'/F')$ via inner automorphisms; moreover, this action of I is semi-simple because $\#(I)$

is odd. Let K be the fixed field of $G(L'/F')^I$, so that I acts non-trivially on any non-zero quotient of $G(K/F')$ which is an I-module. In particular, it follows that $k_K = k_{F'}$. It is also clear that K is deeply ramified because it certainly contains a ramified $\mathbb{Z}_2$-extension of F'. Moreover, we have, with $M = \widetilde{A}(k_{F'})(2)$,

$$H^1(G(F'/F), M) = 0\ , \quad H^1(G(K/F'), M)^I = 0\ ;$$

the first equality is true because $[F' : F]$ is odd, and the second holds because $G(K/F')$ has no non-zero I-quotient on which I acts trivially. Hence we have $H^1(G(K/F), M) = 0$, and so again K satisfies $N_{K/F}(A^t)_p = U_F$.

When A has good reduction over F, and K is a ramified $\mathbb{Z}_p$-extension of F, the fact that $N_{K/F}(A^t)$ has finite index in a group which does not depend on K is implicit in [14].

We add one final general remark to this discussion of abelian varieties with good reduction over F. It was pointed out earlier (see the beginning of the proof of Proposition 4.6) that the map

$$\varepsilon_F : H^1(F, \mathscr{F}(\overline{\mathfrak{m}})) \to H^1(F, A(\overline{\mathbb{Q}}_p))$$

is injective. Hence we deduce from (5.17) that there is a canonical isomorphism

$$A^t(F)_p/U_F \xrightarrow{\sim} H^1(F, \mathscr{F}(\overline{\mathfrak{m}}))^\wedge\ . \tag{5.30}$$

Of course, this last isomorphism depends only on F, and has nothing to do with the field K.

Case IV. A has good ordinary reduction over F.
We assume that A has good ordinary reduction over F. Thus $h = g$, and so (5.13) and Proposition 5.3 implies that U_F is of finite index in $A^t(F)_p$. More precisely, combining (5.30) with the remarks at the end of the proof of Proposition 4.6, we obtain an isomorphism

$$A^t(F)_p/U_F \xrightarrow{\sim} \tilde{A}^t(k_F)(p)\ . \tag{5.31}$$

Let $A_1^t(F)$ denote the kernel of the reduction homomorphism from $A^t(F)$ to $\tilde{A}^t(k_F)$.

Proposition 5.6 *Assume that A has good ordinary reduction over F. Then* $U_F = A_1^t(F)$.

Proof. We claim that the index of both U_F and $A_1^t(F)$ in $A^t(F)$ is equal to $\#(\tilde{A}^t(k_F))$. Indeed, this is clear for $A_1^t(F)$ because the reduction map is surjective. It is also true for U_F by (5.31) and the fact that

$$A^t(F)/A^t(F)_p \xrightarrow{\sim} \bigoplus_{q \neq p} \tilde{A}^t(k_F)(q)\ ;$$

this last isomorphism is valid because $A_1^t(F)$ is uniquely divisible by any prime $q \neq p$. We will now prove the inclusion $U_F \subset A_1^t(F)$, which will

clearly complete the proof of the proposition. By the remark after the proof of Proposition 5.5, there exists a deeply ramified extension K of F such that $N_{K/F}(A^t)_p = U_F$. Let p^t denote the order of the p-primary subgroup of $\tilde{A}^t(k_F)$. Then Lemma 2.12 implies that there exists a finite extension F' of F contained in K such that p^t divides the ramification index $e(F'/F)$ of F' over F. But then, for each $a \in A^t(F')$, the reduction of $N_{F'/F}(a)$ must belong to $p^t\tilde{A}^t(k_F)$, and so has order prime to p. It follows immediately that $N_{K/F}(A^t)_p$ is contained in $A_1^t(F)$. Thus $U_F \subset A_1^t(F)$, as required.

It may be of interest at this point to recall a result of McCallum [13]. We drop for this paragraph all assumptions about the nature of the reduction of A. Let $\mathscr{F}^t$ denote the formal group attached to the Neron model of A^t over O_F. Then we have the filtration

$$A^t(F) \supseteq A_0^t(F) \supseteq A_1^t(F)\,,$$

where $A_1^t(F) = \mathscr{F}^t(\mathfrak{m}_F)$, and $A_0^t(F)$ is the group of points specializing to the connected component of the Néron model of A^t. When we speak of orthogonal complements in this paragraph, we shall mean with respect to the Tate pairing of $A^t(F)$ and $H^1(F, A(\overline{\mathbb{Q}}_p))$ into $\mathbb{Q}/\mathbb{Z}$. It has long been known that the exact orthogonal complement of $A_0^t(F)$ is $H^1(G(F^{nr}/F),\ A(F^{nr}))$, where F^{nr} is the maximal unramified extension of F (see [13]). McCallum proves in [13] that $A_0^t(F)_p$ is the exact orthogonal complement of $H^1(G(F^{tr}/F), A(F^{tr}))$, where F^{tr} is the maximal tamely ramified extension of F. He also gives a subgroup of the annihilator of $A_1^t(F)$, without determining the exact annihilator. We can view Proposition 5.6 as determining the exact annihilator of $A_1^t(F)$ in the case when A has good ordinary reduction.

Since we are assuming that A has good, ordinary reduction over F, we know from Proposition 4.7 that $\mathrm{Im}(\kappa_K) = \mathrm{Im}(\lambda_K)$ for all extension K of F which are infinitely wildly ramified. Thus, our results in this section apply to all K satisfying this hypothesis. In particular, we get the following result by combining (5.29) and (5.31), and noting that, for each prime $q \neq p$, the reduction map induces an isomorphism from $A[q^\infty](K)$ onto the q-primary part of $\tilde{A}(k_K)$ (see the remark made just before Lemma 5.1).

Proposition 5.7 *Assume that A has good, ordinary reduction over F, and that K/F is an infinitely wildly ramified Galois extension such that the residue field k_K is finite. Then $N_{K/F}(A^t)$ has finite index in $A^t(F)$, and this index is given by*

$$[A^t(F) : N_{K/F}(A^t)] = \#(\tilde{A}^t(k_F)(p)) \cdot \#(H^1(\mathscr{G}, \tilde{A}(k_K))) \tag{5.32}$$

where $\mathscr{G} = G(K/F)$.

If the residue field k_K is not finite, then the universal norm group $N_{K/F}(A^t)$ could be of infinite index in $A^t(F)$, or $N_{K/F}(A^t)$ could even be finite. Indeed, assuming K is deeply ramified and that K is Galois over F, we see that $N_{K/F}(A^t)$ is finite if and only if $H^1(\mathscr{G}, \tilde{A}(k_K)(p))$ has $\mathbb{Z}_p$-corank equal to $g[F : \mathbb{Q}_p]$;

here $\mathscr{G} = G(K/F)$. We will be content to simply discuss the special case when $F = \mathbb{Q}_p$, and A is an elliptic curve over $\mathbb{Q}_p$ with good, ordinary reduction. The action of $G_{\mathbb{Q}_p}$ on $\tilde{A}[p^\infty]$ is given by an unramified homomorphism $\varphi : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$, whose image must clearly be infinite. Hence, if L denotes the fixed field of the kernel of φ, then $G(L/\mathbb{Q}_p) = \Delta \times \Gamma$, where Δ is finite and $\Gamma \xrightarrow{\sim} \mathbb{Z}_p$. Note that the order of Δ is always prime to p since $G(L/\mathbb{Q}_p)$ is topologically cyclic because L is unramified over $\mathbb{Q}_p$. Recall that $D = \tilde{A}[p^\infty]$, and let ρ_L denote the restriction map from $H^1(\mathbb{Q}_p, D)$ to $H^1(L, D)$. It is easy to see that ρ_L is injective because Γ operates non-trivially on D. By Proposition 5.3, $H^1(\mathbb{Q}_p, D)$ has $\mathbb{Z}_p$-corank equal to 1, and hence contains a unique subgroup $\mathscr{H}$ isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$. Thus, since ρ_L is injective and $G_L = G(\overline{\mathbb{Q}}_p/L)$ acts trivially on D, there exists a $\mathbb{Z}_p$-extension M of L such that

$$\rho_L(\mathscr{H}) = \mathrm{Hom}(G(M/L), D)\ . \tag{5.33}$$

Clearly M is Galois over $\mathbb{Q}_p$, and $G(L/\mathbb{Q}_p)$ operates on $G(M/L)$ via the homomorphism φ. Note also that M is determined only by the reduction $\tilde{A}$ of A. It is also plain that the $\mathbb{Z}_p$-extension M over L is ramified, and so is infinitely wildly ramified.

Proposition 5.8 *Let K be a Galois extension of $\mathbb{Q}_p$. Let A be an elliptic curve over $\mathbb{Q}_p$ with good, ordinary reduction. Let $M = M_{\tilde{A}}$ be the field defined above by* (5.33). *Then $N_{K/\mathbb{Q}_p}(A)$ is finite if and only if $K \supseteq M$.*

Proof. As above, let ρ_K denote the restriction map from $H^1(\mathbb{Q}_p, D)$ to $H^1(K, D)$, so that $\mathrm{Ker}(\rho_K) = H^1(\mathscr{G}, D(K))$, where $\mathscr{G} = G(K/\mathbb{Q}_p)$. But $D(K)$ is either finite or coincides with D. Suppose first that $K \supseteq M$, which implies that $\mathrm{Ker}(\rho_K) \supseteq \mathscr{H}$. Now K is infinitely wildly ramified because M is, and so Theorem 5.2 tells us that $N_{K/\mathbb{Q}_p}(A)_p$ is dual to $H^1(\mathbb{Q}_p, D)/\mathrm{Ker}(\rho_K)$, which is clearly finite. Conversely, assume that $N_{K/\mathbb{Q}_p}(A)$ is finite. Then, by Lemma 5.1, K must be infinitely wildly ramified. Thus the hypothesis of Theorem 5.2 is valid by Proposition 4.7. Hence the conclusion of Theorem 5.2 tells us that $\mathrm{Ker}(\rho_K)$ must be infinite, whence $D(K) = D$, and so $L \subseteq K$. But $\mathrm{Ker}(\rho_K) \supseteq \mathscr{H}$, and thus $\rho_L(\mathscr{H})$ must restrict to zero in $\mathrm{Hom}(G(\overline{\mathbb{Q}}_p/K), D)$, which shows that $K \supseteq M$, as required. This completes the proof of Proposition 5.8.

We make one final remark related to Proposition 5.8. One can easily see that $G(M/\mathbb{Q}_p)$ is a semi-direct product

$$G(M/\mathbb{Q}_p) = HJ\ ,$$

where $J = G(M/L)$ is normal, and H is isomorphic to $G(L/\mathbb{Q}_p)$. Let P be the fixed field of H. Note that P has finite residue field and is deeply ramified because its Galois closure M over $\mathbb{Q}_p$ is a 2-dimensional p-adic Lie extension of $\mathbb{Q}_p$ with infinite inertial subgroup (as mentioned at the end of Sect. 2, a field K is deeply ramified if and only if its Galois closure over $\mathbb{Q}_p$ is deeply ramified). Also, $H^1(G(M/P), D) = 0$ because H is topologically cyclic and

acts non-trivially on D. Since $\mathscr{H} \subset \mathrm{Ker}(\rho_M)$, it follows that $\mathscr{H} \subset \mathrm{Ker}(\rho_P)$. Hence $N_{P/\mathbb{Q}_p}(A)$ is finite by Theorem 5.1. Note that this does not contradict Proposition 5.7, since $P/\mathbb{Q}_p$ is not Galois.

Case V. Elliptic curves over $\mathbb{Q}_p$ with split multiplicative reduction.
Such an elliptic curve A is a Tate curve. Let $q_A \in \mathbb{Q}_p^\times$ denote the Tate period for A. One has an exact sequence

$$0 \to \mu_{p^\infty} \to A[p^\infty] \to \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

of $G_{\mathbb{Q}_p}$-modules. Thus $D = \mathbb{Q}_p/\mathbb{Z}_p$, and so

$$H^1(\mathbb{Q}_p, D) = \mathrm{Hom}(G(\mathbb{Q}_p^{ab}/\mathbb{Q}_p), D)\,,$$

where $\mathbb{Q}_p^{ab}$ is the maximal abelian extension of $\mathbb{Q}_p$, has $\mathbb{Z}_p$-corank equal to 2. Now the exact sequence

$$H^1(\mathbb{Q}_p, A[p^\infty]) \xrightarrow{\pi} H^1(\mathbb{Q}_p, D) \to H^2(\mathbb{Q}_p, \mu_{p^\infty}) \to 0$$

and the fact that $H^2(\mathbb{Q}_p, \mu_{p^\infty})$ has $\mathbb{Z}_p$-corank equal to 1 shows that $\mathrm{Im}(\pi)$ has $\mathbb{Z}_p$-corank equal to 1 in this case. Thus $\mathrm{Im}(\pi)_{\mathrm{div}} = \mathrm{Hom}(G(K_A/\mathbb{Q}_p), D)$, where K_A is a uniquely determined $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$. If K is any ramified $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$, then $N_{K/\mathbb{Q}_p}(A)$ is finite if and only if $\mathrm{Ker}(\rho_K) \cap \mathrm{Im}(\pi)$ is of finite index in $\mathrm{Im}(\pi)$ (by Theorem 5.2), or equivalently if and only if $\mathrm{Im}(\pi)_{\mathrm{div}} \subseteq \mathrm{Ker}(\rho_K)$. But

$$\mathrm{Ker}(\rho_K) = H^1(G(K/\mathbb{Q}_p), D) = \mathrm{Hom}(G(K/\mathbb{Q}_p), D)\,,$$

and consequently $N_{K/\mathbb{Q}_p}(A)$ is finite if and only if $K = K_A$.

On the other hand, the Tate parametrization

$$A(K) = K^\times/q_A^{\mathbb{Z}}$$

allows us to determine the universal norm group in $A(\mathbb{Q}_p) = \mathbb{Q}_p^\times/q_A^{\mathbb{Z}}$. By local class field theory, the universal norms for the multiplicative group

$$N_{K/\mathbb{Q}_p}(K^\times) = \bigcap_F N_{F/\mathbb{Q}_p}(F^\times)\,,$$

where F runs over all finite extensions of $\mathbb{Q}_p$ contained in K, must be of the form $N_{K/\mathbb{Q}_p}(K^\times) = \mu \cdot q_K^{\mathbb{Z}}$, where μ denotes the group of roots of unity in $\mathbb{Q}_p$, and q_K lies in $\mathbb{Q}_p^\times$ but not in $\mathbb{Z}_p^\times$. Moreover

$$\mathbb{Q}_p^\times/(\mu \cdot q_K^{\mathbb{Z}}) \xrightarrow{\sim} G(K/\mathbb{Q}_p) = \mathbb{Z}_p\,.$$

But then, by the Tate parametrization, $N_{K/\mathbb{Q}_p}(A)$ is finite if and only if $q_A^{\mathbb{Z}}$ and $\mu \cdot q_K^{\mathbb{Z}}$ are commensurable, or equivalently that the image of q_A in $\mathbb{Q}_p^\times/\mu \cdot q_K^{\mathbb{Z}}$ is of finite order. But this last group is torsion-free. Thus $N_{K/\mathbb{Q}_p}(A)$ is finite precisely when $q_A \in N_{K/\mathbb{Q}_p}(K^\times)$. Moreover, K is uniquely determined by this

inclusion. Hence we obtain the following result, which is also proven in a somewhat different and more direct manner in [6].

Proposition 5.9 *Let A be an elliptic curve over $\mathbb{Q}_p$ with split multiplicative reduction. Then*

$$(\mathrm{Im}\,\pi)_{\mathrm{div}} = \mathrm{Hom}(G(K/\mathbb{Q}_p), D)\,,$$

where $K = K_A$ is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$ such that the Tate period q_A is a universal norm for K.

Acknowledgements. This paper was begun and finished while the first author was at the Ecole Normale Supérieure, Paris, and he wishes to thank it for its hospitality on both occasions. The second author, who was partially supported by a grant from the National Science Foundation, wishes also to thank the Isaac Newton Institute, the Centre Nationale de la Recherche Scientifique, the Universities of Paris-Sud, Paris-Nord, Strasbourg, Pierre et Marie Curie, and Tokyo Metropolitan University for their hospitality during 1993–94.

References

1. Bloch, S., Kato, K.: L-functions and Tamagawa numbers of motives. In: Grothendieck Festschrift 1, Progress in Math., Birkhäuser **86**, 333–400 (1990)
2. Fesenko, I., Vostokov, S.: Local Fields and their Extensions. Translations of Math. Monographs, Am. Math. Soc. **121** (1994)
3. Fesenko, I.: On deeply ramified extensions (to appear)
4. Fresnel, J., Matignon, M.: Produit tensoriel topologique de corps values. Can. J. Math. **35**, 218–273 (1983)
5. Greenberg, R.: Iwasawa theory for p-adic representations. In: Algebraic Number Theory. Advanced Studies Pure Math. **17**, 97–137 (1989)
6. Greenberg, R., Stevens, G.: p-adic L-functions and p-adic periods of modular forms. Invent. Math. **111**, 407–447 (1993)
7. Harris, M.: p-adic representations arising from descent on abelian varieties. Comp. Math. **39**, 177–245 (1979)
8. Hazewinkel, M.: Norm maps for formal groups I J. Algebra **32**, 89–108 (1974); II, Crelle 268/269 (1974), 222–250; III, Duke Math. J. **44**, 305–314 (1977); IV, Michigan Math. J. **25**, 245–255 (1978)
9. Iwasawa, K.: On $\mathbb{Z}_l$-extensions of algebraic number fields. Ann. of Math. **98**, 246–326 (1973)
10. Kurcanov, P.: The universal Γ-norms of formal groups over a local field. Ukr. Math. J. **28**, 396–398 (1976)
11. Lubin, J., Rosen, M.: The norm map for ordinary abelian varieties. J. Algebra **52**, 236–240 (1978)
12. Mazur, B.: Rational points of abelian varieties with values in towers of number fields. Invent. Math. **18**, 183–266 (1972)
13. McCallum, W.: Tate duality and wild ramification. Math. Ann. **288**, 553–558 (1990)
14. Schneider, P.: Arithmetic of formal groups and applications I: Universal norm subgroups. Invent. Math. **87**, 587–602 (1987)
15. Sen, S.: Ramification in p-adic Lie extensions. Invent. Math. **17**, 44–50 (1972)
16. Serre, J.-P.: Cohomologie Galoisienne. Lecture Notes Math. **5**, Springer, 1965
17. Serre, J.-P.: Corps Locaux. Hermann, 1968
18. Tate, J.: p-divisible groups In: "Proceedings of a conference on local fields (Driebergen, 1966)", 158–183, Springer, 1967

19. Vvedenskij, O.: On universal norms of formal groups defined over the ring of integers of a local field. Math. USSR. Izv. **7**, 733–747 (1973)
20. Wintenberger, J.-P.: Le corps des normes de certaines extensions infinies de corps locaux; applications. Ann. Scient. Ec. Norm. Sup. **16**, 59–89 (1983)
21. Taguchi, Y.: The arithmetic of Drinfeld modules Ph.D. thesis. Tokyo University, 1992