J. reine angew. Math. **532** (2001), 179—222

Journal für die reine und angewandte Mathematik

Special fibers of Néron models and wild ramification

By *Qing Liu* at Talence and *Dino Lorenzini* at Athens

Introduction

Let K be a field with a discrete valuation v. Let $\mathcal{O}_K$ denote the ring of integers of K, with maximal ideal (π). Let k be the residue field of $\mathcal{O}_K$, assumed to be algebraically closed of characteristic $p \geqq 0$. Let G/K be a semi-abelian variety with Néron model $\mathcal{G}/\mathcal{O}_K$. Let $\mathcal{G}_k/k$ be the special fiber of $\mathcal{G}/\mathcal{O}_K$, and let $\mathcal{G}_k^0/k$ denote the connected component of 0 in $\mathcal{G}_k$. The group of components of $\mathcal{G}$ is the finitely generated abelian group $\Phi(G) := \mathcal{G}_k/\mathcal{G}_k^0$. When no confusion may occur, we shall denote $\Phi(G)$ simply by Φ or Φ_K. We shall say that $\mathcal{G}/\mathcal{O}_K$ is *split*, or that G/K *has split reduction*, if the extension

$$0 \to \mathcal{G}_k^0 \to \mathcal{G}_k \xrightarrow{c} \Phi(G) \to 0 \tag{1}$$

is split: in other words, $\mathcal{G}$ is split if and only if $\mathcal{G}_k(k)$ is isomorphic as an abelian group to the product $\mathcal{G}_k^0(k) \times \Phi(G)$. Thus, when $\Phi(G)$ is a finite group, $\mathcal{G}$ is split if and only if, for each $\varphi \in \Phi(G)$, there exists $\tilde{\varphi} \in \mathcal{G}_k(k)$ with $\mathrm{ord}(\tilde{\varphi}) = \mathrm{ord}(\varphi)$ such that $c(\tilde{\varphi}) = \varphi$. If the extension (1) is not split, we shall say that $\mathcal{G}$ *is not split*. Since Néron models commute with completion of K, we will assume in this paper that K is *complete*.

The core of this article is a detailed study of the case of elliptic curves and of the case of norm tori and their duals, with applications to abelian varieties with potentially purely multiplicative reduction. In all cases studied, we find that there exists a constant c depending only on the dimension of G such that, if G has totally not split reduction (see 1.2), then the Swan conductor of G/K is positive and bounded by c. We also find that there is a constant d, depending only on the dimension of G, such that G_M/M has split reduction for any tame extension M/K of degree greater than d. Clearly this suggests the possibility that similar statements may hold for more general tori and abelian varieties.

This paper is organized as follows. We have collected in the first section several general statements regarding the splitting property of Néron models. Section two contains a detailed study of the case of elliptic curves. Section three provides examples of the behaviour of the splitting property under several standard constructions, such as under isogeny, tame base extension, and Weil restriction of scalars. The cases of norm tori and their duals are studied in section four. Section five provides an explicit equation describing the Néron model of the norm torus $R^1_{L/K}\mathbb{G}_{m,L}$ when $[L:K]=p$. In section six, the results on tori are applied to the case of abelian varieties with potentially purely multiplicative reduction. The article ends with a discussion of possible generalizations of our main theorems to larger classes of semi-abelian varieties.

1. General facts

Before turning to a detailed study of the case of elliptic curves and of the case of tori in the next sections, let us make below a few general remarks on the splitting property. Non-trivial examples of abelian varieties of dimension bigger than 1 that are split are given in 3.7, and examples that are not split are provided in 6.5. Recall that for any commutative group H, H_{tors} denotes the torsion subgroup of H, H_p denotes the p-part of H_{tors} and $H[n]$ denotes the subgroup of elements of order dividing n. The next lemma is elementary.

Lemma 1.1. *Let $0 \to H^0 \to H \xrightarrow{c} \Psi \to 0$ be an exact sequence of commutative groups. Let $n \geqq 1$ be an integer. Let J be a subgroup of H^0 such that $H^0 = J + nH^0$. Denote by $n_H\colon H \to H$ the multiplication-by-n map on H. Then $c(n_H^{-1}(J)) = \Psi[n]$.*

1.2. Let $0 \to H^0 \to H \xrightarrow{c} \Psi \to 0$ be an exact sequence of finitely generated commutative groups. We shall say that this exact sequence is *totally not split* (at a prime p) if $p|\mathrm{ord}(\Psi_{\mathrm{tors}})$ and if, for any element $\varphi \in \Psi$ of order p, there does not exist $\tilde{\varphi} \in H$ of order p such that $c(\tilde{\varphi}) = \varphi$. Thus, a sequence is totally not split if and only if $\Psi[p] \neq \{0\}$ and the natural map $H[p] \to \Psi[p]$ is identically zero. Let G/K be a semi-abelian variety (all semi-abelian varieties over K are assumed to be connected in this article). Let $\mathscr{G}/\mathcal{O}_K$ be its Néron model. Let us say that $\mathscr{G}$ is *totally not split*, or that G has *totally not split reduction*, if the exact sequence (1) is totally not split. An example of a torus whose reduction is only not split, but not totally not split, can be found in 4.13.

Semi-abelian varieties in general admit a Néron lft-model, where lft stands for locally of finite type ([BLR], 10.2/2). In this article, we drop the lft-model notation and talk only of Néron models, the context making it clear whether the model is of finite type. It is shown in [Xar], 2.18, that the group of components of a torus is a finitely generated abelian group. It follows then from [B-X], 4.11 (ii), that the group of components of the Néron model of any semi-abelian variety is a finitely generated abelian group. Another proof of this fact can be obtained using the proof of 4.11 (i) of loc. cit.

Remark 1.3. The proof of [B-X], 4.11 (ii), uses Lemma 4.2 of loc. cit., which is incorrect in the case of perfect residue fields. The authors of [B-X] have informed us that they can provide a different proof of 4.11 (ii) without using 4.2.

Proposition 1.4. *Let G/K be a semi-abelian variety. Let $\mathscr{G}/\mathcal{O}_K$ be its Néron model. Then the following properties are true.*

(a) *Let $\varphi \in \Phi(G)$ be an element of finite order n prime to p. Then φ lifts to an element of $\mathscr{G}_k$ of order n.*

(b) *The complex*

$$0 \to \mathcal{G}^0_{k,p} \to \mathcal{G}_{k,p} \to \Phi(G)_p \to 0 \tag{2}$$

is exact.

(c) *$\mathcal{G}$ is split if and only if* (2) *is split.*

(d) *$\mathcal{G}$ is totally not split if and only if* (2) *is totally not split.*

(e) *Suppose that $\Phi(G)_p$ is cyclic and that $\mathcal{G}^0_{k,p}$ is killed by p. Then $\mathcal{G}$ is totally not split if and only if it is not split.*

Proof. (a) Since $\mathcal{G}^0_k/k$ is a smooth commutative group scheme and $p \nmid n$, the multiplication-by-n map $\mathcal{G}^0_k \to \mathcal{G}^0_k$ is surjective. Now we can apply Lemma 1.1 with $J = 0$ to the sequence (1).

(b) The only non-trivial fact to prove is that $\mathcal{G}_{k,p} \to \Phi(G)_p$ is surjective. The group $\mathcal{G}^0_k$ is extension of a semi-abelian variety by an unipotent group U/k. Since the multiplication by n is surjective for any integer n on any semi-abelian variety, we have $\mathcal{G}^0_k = U + n\mathcal{G}^0_k$. Lemma 1.1 shows that any element $\varphi \in \Phi(G)[p^r]$ lifts to an element $\tilde{\varphi} \in \mathcal{G}_k$ such that $p^r\tilde{\varphi} \in U$. Hence, $\tilde{\varphi} \in \mathcal{G}_{k,p}$.

(c) The condition is clearly necessary. Let us show that it is sufficient. The group of components $\Phi(G)$ is the direct sum of finitely many cyclic (finite or infinite) groups. Thus, to show that $\mathcal{G}$ is split, it is enough to show that any element $\varphi \in \Phi(G)$ lifts to an element of $\mathcal{G}_k$ of same order. If the order of φ is infinite (resp. a power of p), then the assertion is clear (resp. follows from the hypothesis). So we can assume that φ has order n prime to p. Then the assertion follows from (a). Assertion (d) follows from the definition.

(e) If $\mathcal{G}$ is not totally not split, then by (d) there exists an element $\varphi \in \Phi(G)_p$ of order p which lifts to an element $\tilde{\varphi} \in \mathcal{G}_{k,p}$ of order p. Let $\tilde{\lambda} \in \mathcal{G}_{k,p}$ be a preimage of a generator λ of $\Phi(G)_p$. Then $\varphi = p^r\lambda$ for some $r \geqq 0$. This implies that λ has order p^{r+1}. We have $p^r\tilde{\lambda} - \tilde{\varphi} \in \mathcal{G}^0_{k,p}$, so by hypothesis $p(p^r\tilde{\lambda} - \tilde{\varphi}) = 0$. Thus, $\tilde{\lambda}$ has order p^{r+1} and $\mathcal{G}$ is split by (c).

Corollary 1.5. *If $p \nmid |\Phi(G)_{\mathrm{tors}}|$, then $\mathcal{G}$ is split.*

Proof. Follows from 1.4 (c).

Proposition 1.6. *Assume that $\mathcal{G}^0_k/k$ is a semi-abelian variety. Then $\mathcal{G}$ is split.*

Proof. According to 1.4 (c), we only need to show that (2) is split. As at the end of the proof of 1.4 (b), we find that any element $\varphi \in \Phi(G)[p^r]$ lifts to an element $\tilde{\varphi} \in \mathcal{G}_k$ such that $p^r\tilde{\varphi} \in U$. Since by hypothesis $U = 0$, (2) is split.

Let T/K be a torus of dimension d. Recall that there exists a finite Galois extension L/K minimal with the property that T_L/L is isomorphic to $\mathbb{G}^d_{m,L}$. The field L/K is called the splitting field of T.

Corollary 1.7. *Let T/K be a torus of dimension d with Néron model $\mathscr{T}$. If L/K is tame, then $\mathscr{T}$ is split. In particular, if $p > d+1$, then T/K has split reduction.*

Proof. It is shown in [Xar], 2.18, that the torsion part of $\Phi(T)$ is killed by $[L:K]$. Hence, the assertion follows from Corollary 1.5. Since $\mathrm{Gal}(L/K)$ is a subgroup of $\mathrm{GL}_d(\mathbb{Z})$, we find that if a prime ℓ divides $[L:K]$, then $\ell \leqq d+1$.

Let A/K be an abelian variety. Recall that there exists a Galois extension L/K minimal with the property that A_L/L has semistable reduction. Recall also that the connected component $\mathscr{A}_k^0/k$ is the extension of an abelian variety by a commutative linear group. The dimension of the toric part of this linear group, t_K, is called the *toric rank* of $\mathscr{A}$.

Proposition 1.8. *Let A/K be an abelian variety whose Néron model $\mathscr{A}/\mathcal{O}_K$ has toric rank equal to* 0. *Then $\Phi(A)$ is killed by $[L:K]^2$.*

Proof. Proposition 2.15 in [Lor2] shows that the prime-to-p part of $\Phi(A)$ is killed by $[L:K]^2$. To prove the general case, we proceed as follows. Consider the subgroups $\Theta_2 \subseteqq \Theta_1$ of $\Phi(A)$ introduced on page 480 of [B-X]. Since $t_K = 0$ by hypothesis, we find that $\Theta_1 = \Phi(A)$. It follows from [B-X], 5.9, that Θ_1/Θ_2 is killed by $[L:K]$. Let $\Psi_{K,L}$ denote the kernel of the natural map $\Phi(A) \to \Phi(A_L)$. Then $[L:K]$ kills $\Psi_{K,L}$ ([ELL], Thm. 1). To conclude the proof of the proposition, it is sufficient to note that the subgroup Θ_2 is contained in $\Psi_{K,L}$. Indeed, consider the rigid analytic uniformization of A/K as in [B-X], §1:

$$\begin{array}{ccccc} & & T & & \\ & & \downarrow & & \\ \Lambda & \longrightarrow & G & \longrightarrow & A \\ & & \downarrow & & \\ & & B & & \end{array}$$

with T/K a torus, B/K an abelian variety with potentially good reduction, and Λ/K a lattice. The group Θ_2 is defined to be the image under the natural map $\Phi(G) \to \Phi(A)$ of the subgroup $\Phi(G)_{\mathrm{tors}}$. The change of base L/K induces natural maps

$$\begin{array}{ccc} \Phi(G) & \longrightarrow & \Phi(A) \\ \downarrow & & \downarrow \\ \Phi(G_L) & \longrightarrow & \Phi(A_L). \end{array}$$

It follows from [B-X], 4.11 (see 1.3), that the map $\Phi(T_L) \to \Phi(G_L)$ is an isomorphism (recall that $\Phi(B_L) = (0)$). Thus, $\Phi(G_L)$ is free since $\Phi(T_L)$ is. Hence, the image of $\Phi(G)_{\mathrm{tors}}$ in $\Phi(G_L)$ is trivial.

Corollary 1.9. *Let A/K be an abelian variety whose Néron model $\mathscr{A}/\mathcal{O}_K$ has toric rank equal to zero. If the extension L/K is tame, then $\mathscr{A}$ is split. In particular, if $p > 2\dim A + 1$, then $\mathscr{A}$ is split.*

Proof. If $\mathscr{A}$ is not split, then $p \mid |\Phi(A)|$ (Corollary 1.5). Then $p \mid [L:K]$. It is shown in [S-T], p. 497, that $p > 2\dim A + 1$ does not divide $[L:K]$.

Question 1.10. Let G/K be any semi-abelian variety. Let L/K denote the extension minimal with the property that G_L/L has semistable reduction. If L/K is tame, is it true that G/K has split reduction? In other words, is it true that the Swan conductor $\delta(G)$, recalled in 1.12 below, is positive if G does not have split reduction?

Proposition 1.11. *Let G_1 and G_2 be semi-abelian varieties over K. Let $f: G_1 \to G_2$ be an isogeny of degree n prime to p. Then G_1 has split reduction if and only if G_2 has split reduction.*

Proof. There exists an isogeny $g: G_2 \to G_1$ such that $g \circ f: G_1 \to G_1$ is the multiplication by n on G_1 ([BLR], 7.3/5). The isogeny g has degree a power of n and, hence, prime to p. Consider the morphisms of the associated Néron lft-models $\mathscr{G}_1 \to \mathscr{G}_2$ and $\mathscr{G}_2 \to \mathscr{G}_1$, induced respectively by f and g. Then, by uniqueness of the extension, the composition $\mathscr{G}_1 \to \mathscr{G}_2 \to \mathscr{G}_1$ is the multiplication by n on $\mathscr{G}_1$. This implies immediately that $\mathscr{G}_1 \to \mathscr{G}_2$ induces an injection $\Phi(G_1)_p \to \Phi(G_2)_p$. Applying the result to the isogeny g, we see that $\Phi(G_1)_p \to \Phi(G_2)_p$ is in fact an isomorphism. Now the proposition follows from Proposition 1.4, (b) and (c).

Note that the proof above shows that f induces an isomorphism $\Phi(G_1)^{(n)} \simeq \Phi(G_2)^{(n)}$ on the prime-to-n parts of the groups of components.

1.12. In this article, we investigate possible relationships between the splitting properties of the Néron model of a semi-abelian variety G and the size of its Swan conductor $\delta(G)$. We recall briefly below the definition of $\delta(G)$ and list some of its properties (see [Ser2], §2.1, for more details). Let Γ_K be the absolute Galois group $\mathrm{Gal}(K^s/K)$. Recall that we assume that K is complete with algebraically closed residue field. Thus Γ_K is equal to its inertia subgroup. Let ℓ be a prime different from p. Let $T_\ell(G)$ denote the Tate module of G, and set $V_\ell(G) := T_\ell(G) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Consider the ℓ-adic representation

$$\rho: \Gamma_K \to \mathrm{Aut}\big(V_\ell(G)\big)$$

corresponding to the action of Γ_K on $T_\ell(G)$. Let T and B be respectively the toric and abelian parts of G. There is a finite Galois extension L/K such that Γ_L acts trivially on $T_\ell(T)$ and unipotently on $T_\ell(B)$. Since $T_\ell(G)$ is an extension of $T_\ell(B)$ by $T_\ell(T)$ (see Proposition 6.4 (a)), Γ_L acts unipotently on $V_\ell(G)$. Let V_n denote the set of elements $x \in V_\ell(G)$ such that $\big(\rho(\sigma) - 1\big)^n x = 0$ for all $\sigma \in \Gamma_K$. Let $gr\big(V_\ell(G)\big) := \bigoplus_{n=0}^{\infty} V_{n+1}/V_n$. Then Γ_K acts on $gr\big(V_\ell(G)\big)$ through the finite group $\Gamma := \Gamma_K/\Gamma_L = \mathrm{Gal}(L/K)$. For $\sigma \in \Gamma_K$, the trace of $\rho(\sigma)$ on $V_\ell(G)$ depends only on the image of σ in Γ, and we obtain a function $\mathrm{Tr}_\rho: \Gamma \to \mathbb{Q}_\ell$. The *Swan conductor* of $V_\ell(G)$ is defined as the scalar product

$$\delta\big(V_\ell(G)\big) := |\Gamma|^{-1} \sum_{\gamma \in \Gamma} \mathrm{Tr}_\rho(\gamma) b_\Gamma(\gamma),$$

where $b_\Gamma: \Gamma \to \mathbb{Z}$ is the Swan character.

The conductor $\delta(V_\ell(G))$ is always a non-negative integer. It equals 0 if and only if the p-Sylow subgroup of Γ_K acts trivially on $V_\ell(G)$. The latter is equivalent to saying that G acquires semi-abelian reduction (i.e. $\mathscr{G}_k^0$ is semi-abelian over k) after a finite tamely ramified extension of K.

It is easy to check from the above definition that if $0 \to V' \to V_\ell(G) \to V'' \to 0$ is an exact sequence of $\mathbb{Q}_\ell[\Gamma_K]$-modules, then $\delta(V_\ell(G)) = \delta(V') + \delta(V'')$. It is well-known that $\delta(V_\ell(B))$ and $\delta(V_\ell(T))$ are integers independent of $\ell \neq p$. The Swan conductor $\delta(G)$ is defined to be $\delta(V_\ell(G))$ for any $\ell \neq p$.

2. The case of elliptic curves

Let E/K be an elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3}$$

with $a_i \in \mathcal{O}_K$ for $i \in \{1, 2, 3, 4, 6\}$. Note that when $a_i \in \pi\mathcal{O}_K$ for all $i = 1, \dots, 6$, then the reduced equation has a singular point at $(0, 0)$. We shall repeatedly use the following fact. If $|\Phi(E)| > 1$, then there exist a minimal Weierstrass equation (3) for E/K with $v(a_i) > 0$ for all i, and a point $P = (x, y)$ in $E(K)$ with $v(x) > 0$. Indeed, let $E^0(K)$ denote the set of points in $E(K)$ whose reduction in the Weierstrass model modulo π is not $(0, 0)$. Then $\Phi(E) \cong E(K)/E^0(K)$ (see [Si2], IV.9.2).

Let us record here that under a translation $x = z + b$, the equation (3) becomes

$$\begin{aligned} y^2 + a_1zy + (a_3 + ba_1)y = z^3 + (3b + a_2)z^2 + (3b^2 + 2a_2b + a_4)z \\ + (b^3 + a_2b^2 + a_4b + a_6). \end{aligned} \tag{4}$$

Recall the formuli

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

If $P = (x, y) \in E(K)$ is not a point of order 2, the point $2P$ has the following x-coordinate:

$$x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}. \tag{5}$$

We denote by $t(E)$ the type of special fiber of the regular minimal model of E/K over $\mathcal{O}_K$, following Kodaira's notation:

$$t(E) \in \{\mathrm{I}_n\ (n \geqq 0), \mathrm{I}_n^*\ (n \geqq 0), \mathrm{II}, \mathrm{II}^*, \mathrm{III}, \mathrm{III}^*, \mathrm{IV}, \mathrm{IV}^*\}.$$

The cases of reduction I_{2n}^*, $n \geqq 0$, are the only cases where the group Φ is not cyclic. In this case the exact sequence (1) may be not split but not totally not split.

Let m denote the number of irreducible components in the special fiber of the minimal regular model of E/K. Let $\delta(E)$ denote the Swan conductor of E (called the wild part of the conductor of E in [Si2]). Recall Ogg's formula when the reduction of E is additive ([Ogg], Theorem 2, where the proof is incomplete, and [Sai], Corollary 2):

$$v(\Delta) = 2 + \delta(E) + (m - 1).$$

Theorem 2.1. *Fix a type t of special fiber of an elliptic curve. Then there exists a constant $c = c(t)$ such that, if K is any discrete valuation field and E/K is any elliptic curve with reduction of type t over $\mathcal{O}_K$ whose Néron model $\mathcal{E}/\mathcal{O}_K$ is not split, then $1 \leqq \delta(E) \leqq c$. More precisely,*

(a) *if $\mathcal{E}/\mathcal{O}_K$ is totally not split, then $1 \leqq \delta(E) \leqq 3$;*

(b) *if $\mathcal{E}/\mathcal{O}_K$ is not split but not totally not split, then $t = \mathrm{I}_{2n}^*$ and $1 \leqq \delta(E) \leqq 2n + 3$.*

The proof of Theorem 2.1 is a case by case analysis that will occupy the remainder of this section. The basic idea is the following. Let φ be an element of Φ. Let $P \in E(K)$ be a rational point whose specialization in $\mathcal{E}_k$ lies in the connected component corresponding to φ. Let d be the order of φ. We can assume that d is divisible by p and that $\mathcal{E}_k$ is additive (Proposition 1.4 (a) and 1.6). Then d is a power of p. Since $\mathcal{E}_k^0$ is killed by p, φ lifts to an element of $\mathcal{E}_k$ of order d if and only if the image of P in $\mathcal{E}_k$ has order d. To determine the order of the image of P, we take advantage of the fact that the multiplication-by-2 map on an elliptic curve is given by simple and explicit formuli, and that the reduction map $E(K) \to \mathcal{E}_k(k)$ is easy to compute.

We are going to discuss the splitting of $\mathcal{E}$ following Tate's algorithm, as in [Si2], IV.9.4. The cases where the reduction of E is of type I_0 (good reduction), I_n ($n \geqq 1$), multiplicative reduction, II and II* (where $|\Phi| = 1$) are all split cases (see 1.5 and 1.6). Moreover, when $p = 2$, IV and IV* (where $|\Phi| = 3$) are also split cases, and when $p = 3$, I_n^*, III, and III* are split. When the reduction is not split, the extension L/K is wild (1.9) and, thus, $\delta(E) \geqq 1$.

2.2. The case $p = 2$.

2.3. Reduction of type III ($\Phi = \mathbb{Z}/2\mathbb{Z}$). Here

a_1	a_2	a_3	a_4	a_6
$\geqq 1$	$\geqq 1$	$\geqq 1$	1	$\geqq 2$

and

b_2	b_4	b_6	b_8
$\geqq 2$	$\geqq 2$	$\geqq 2$	2

.

In all tables of coefficients in this article, the inequalities in the second line relate to the valuation over K of the corresponding coefficient appearing on the first line. Let $P = (x, y) \in E(K)$ be such that $v(x) \geqq 1$. Then $v(x(2P)) = v(-b_8/b_6)$, using formula

(5). We find that

$$\begin{aligned}\mathscr{E} \text{ is not split} &\Leftrightarrow v(b_6) = v(b_8) = 2\\ &\Leftrightarrow v(a_3) = 1 \Leftrightarrow v(\Delta) = 4\\ &\Leftrightarrow \delta = 1.\end{aligned}$$

2.4. Reduction of type III* ($\Phi = \mathbb{Z}/2\mathbb{Z}$). Here

a_1	a_2	a_3	a_4	a_6
$\geqq 1$	$\geqq 2$	$\geqq 3$	3	$\geqq 5$

and

b_2	b_4	b_6	b_8
$\geqq 2$	$\geqq 4$	$\geqq 6$	6

.

Let $P = (x, y) \in E(K)$ be such that $v(x) \geqq 1$. Then the equation (3) immediately shows that $v(x) > 1$, and that if $v(x) = 2$ then $v(a_4x + a_6) \geqq 6$. Thus it is possible to find $b \in \pi^2\mathcal{O}_K$ such that $v(b^3 + a_2b^2 + a_4b + a_6) \geqq 6$. Consider the translation $x = z + b$. We find that the new coefficients a_i in equation (4) still satisfy all the inequalities for type III* and that, in addition, the new coefficient a_6 is divisible by π^6. It is easy to check that when such is the case, a point $P = (x, y)$ with $v(x) > 1$ satisfies in fact $v(x) \geqq 3$. Then for such a point, $v\big(x(2P)\big) = v(-b_8/b_6)$. We conclude that

$$\mathscr{E} \text{ is not split} \Leftrightarrow v(b_6) = v(b_8) = 6 \Leftrightarrow v(a_3) = 3.$$

Note that $v(a_1) = 1 \Leftrightarrow v(b_2) = 2$, and $v(b_2) = 2$ implies that $v(\Delta) = 10$. The case $v(b_2) = 3$ requires $K = \mathbb{Q}_2^{nr}$ and $v(a_2) \leqq 1$. Since in our case $v(a_2) \geqq 2$, this case cannot happen. If $\mathscr{E}$ is not split, then $v(b_2) \geqq 4$ implies that $v(\Delta) = 12$. Since $m = 8$ in the case III*, we find that

$$\mathscr{E} \text{ is not split} \Rightarrow \delta = 1 \text{ or } 3.$$

The case $\delta = 2$ cannot happen when the reduction is III*. Note that an elliptic curve with reduction III* and $v(a_1) = 1$ and $v(a_3) > 3$ has $\delta = 1$ but is split. Thus the exponent δ does not characterize the splitting of $\mathscr{E}$ (see also Remark 6.7).

2.5. Reduction of type I^*_{2n+1}, $n \geqq 0$ ($\Phi = \mathbb{Z}/4\mathbb{Z}$). Here

a_1	a_2	a_3	a_4	a_6
$\geqq 1$	1	$n+2$	$\geqq 2n+2$	$\geqq 2n+4$

and

b_2	b_4	b_6	b_8
$\geqq 2$	$\geqq n+3$	$2n+4$	$2n+5$

.

Using the fact that the valuation of a_3 is specified, we find that there exists a point $P = (0, y)$ in $E(K)$. Then

$$\xi := x(2P) = -b_8/b_6.$$

The above table shows that $v(-b_8/b_6) = 1$. Hence, $2P$ reduces to the singular point of the usual Weierstrass model and, thus, P reduces on a component of degree 4 in the Néron model of E. We find that

$$x(4P) = \frac{\xi^4 - b_4\xi^2 - 2b_6\xi - b_8}{4\xi^3 + b_2\xi^2 + 2b_4\xi + b_6}.$$

Thus,

$$\mathscr{E} \text{ is not split} \Leftrightarrow v\big(x(4P)\big) = 0 \Leftrightarrow v(b_2) = 2.$$

Note that since $\Phi(E)_p$ is cyclic, $\mathscr{E}$ not split is equivalent to $\mathscr{E}$ totally not split (1.4 (e)). When $\mathscr{E}$ is not split, we have

$-b_2^2b_8$	$-8b_4^3$	$-27b_6^2$	$9b_2b_4b_6$
$2n+9$	$\geqq 3n+12$	$4n+8$	$\geqq 3n+9$

Hence, in the case I_1^*, $v(\Delta) = 8$, and in the case I_{2n+1}^*, $n \geqq 1$, $v(\Delta) = 2n+9$. In all cases, $v(\Delta)$ is minimal. In I_{2n+1}^*, the number of components equals $2n+6$. Thus

$$v(\Delta) = 8 \Leftrightarrow \delta = 1 \quad (\text{minimal for } \mathrm{I}_1^*),$$
$$v(\Delta) = 2n+9 \Leftrightarrow \delta = 2 \quad (\text{minimal for } \mathrm{I}_{2n+1}^*, n \geqq 1).$$

Note that when $v(b_2) = 2$, then $v(c_4) = v(b_2^2 - 24b_4) = 4$. Hence,

$$v(j) = v\left(\frac{c_4^3}{\Delta}\right) = 12 - 2n + 9 < 0 \quad \text{if } n = 2, 3, \dots.$$

In cases I_1^* and I_3^*, E/K has potentially good reduction. In all other cases, the curve has potentially multiplicative reduction.

2.6. Reduction of type I_0^* ($\Phi = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). Here

a_1	a_2	a_3	a_4	a_6
$\geqq 1$	$\geqq 1$	$\geqq 2$	$\geqq 2$	$\geqq 3$

and

b_2	b_4	b_6	b_8
$\geqq 2$	$\geqq 3$	$\geqq 4$	$\geqq 4$

The condition to be of type I_0^* with the above coefficients is $v(a_2^2a_4^2 - 27a_6^2) = 6$. More precisely, the polynomial

$$P(t) = t^3 + (a_2/\pi)t^2 + (a_4/\pi^2)t + a_6/\pi^3$$

must have distinct roots modulo π. Since we work over a strictly henselian field, we conclude that there exist α_1, α_2, and α_3 in $\mathcal{O}_K$ such that

$$x^3 + a_2x^2 + a_4x + a_6 = (x - \pi\alpha_1)(x - \pi\alpha_2)(x - \pi\alpha_3).$$

Lemma 2.7. *Let $P_i = (\pi\alpha_i, 0) \in E(K)$, $i = 1, 2, 3$. Then the images of P_1, P_2, and P_3 in Φ are three distinct points of order 2.*

Proof. The lemma follows immediately from the description of the minimal regular model of E/K obtained in Tate's algorithm, as in [Si2], IV.9.4. The details are left to the reader.

It is easy to check that by using the translation $x = z + \pi\alpha_3$, we obtain a new Weierstrass equation with $\alpha_3 = 0$ and with each new coefficients a_i satisfying the same inequalities listed above for type I_0^*. Moreover, the new coefficients $a_2 = \pi(\alpha_1 + \alpha_2)$ and $a_4 = \pi^2\alpha_1\alpha_2$ have valuation 1 and 2 respectively. The new coefficient a_6 is zero. In this case, $v(x(2P_3)) = v(-b_8/b_6)$. Note that if $v(a_4) = 2$, then $v(b_8) = 4$. It follows that $v(b_6) = v(b_8) = 4$ if and only if the image of P_3 in Φ has a preimage in $\mathscr{E}_k$ of order 4.

Claim 2.8. *If $\mathscr{E}$ is not split and $v(a_1) \geqq 2$, then $v(\Delta) = 8$ and $\mathscr{E}$ is totally not split. If $\mathscr{E}$ is not split and $v(a_1) = 1$, then $v(\Delta) = 8$ or 9. The case $v(\Delta) = 9$ can occur only when $\mathscr{E}$ is totally not split.*

Proof. If $\mathscr{E}$ is not split, then the above discussion implies that we can assume that E/K has a Weierstrass equation with $a_6 = 0$ and

a_1	a_2	a_3	a_4
$\geqq 1$	1	2	2

and

b_2	b_4	b_6	b_8
$\geqq 2$	$\geqq 3$	4	4

.

(Indeed, $v(b_6) = 4$ implies that $v(a_3) = 2$.) We leave it to the reader to verify that if $v(a_1) \geqq 2$, then $v(\Delta) = 8$. Let us assume now that $v(a_1) = 1$. If $v(\Delta) > 8$, then $v(-b_2^2 b_8 - 27b_6^2) > 8$, and thus $v(a_1^4 a_4^2 - 27a_3^4) > 8$. But $a_1^4 a_4^2 - 27a_3^4$ is congruent to $a_1^4 a_4^2 - a_3^4$ modulo π^9, and we find that $v(a_1^2 a_4 \pm a_3^2) \geqq 5$. The congruences below are now all modulo π^{10}:

$$
\begin{aligned}
\Delta &\equiv -(a_1^4 + 8a_1^2 + 16a_2^2)b_8 - 27b_6^2 + 9b_2 b_4 b_6 \\
&\equiv -a_1^4 b_8 + b_6^2 + b_2 b_4 b_6 \\
&\equiv -a_1^4(-a_1 a_3 a_4 + a_2 a_3^2 - a_4^2) + a_3^4 + (a_1^2 + 4a_2)(2a_4 + a_1 a_3)(a_3^2 + 4a_6) \\
&\equiv +a_1^4 a_4^2 + a_3^4 + a_1^5 a_3 a_4 - a_1^4 a_2 a_3^2 + a_1^2(a_2 a_4 + a_1 a_3)a_3^2 \\
&\equiv -2a_3^2 + a_1^5 a_3 a_4 - a_1^4 a_2 a_3^2 + 2a_1^2 a_4 + a_1^3 a_3^3 \\
&\equiv a_1^3(a_1^2 a_3 a_4 - a_1 a_2 a_3^2 + a_3^3) \\
&\equiv a_1^3 a_3(a_1^2 a_4 - a_1 a_2 a_3 + a_3^2) \\
&\equiv a_1^3 a_3(-a_1 a_2 a_4).
\end{aligned}
$$

Thus, $v(\Delta) \geqq 9$ and $v(\Delta) = 9$ if $v(a_1) = 1$.

Consider the numerator N_i of $x(2P_i)$, $i = 1, 2$. We claim that N_i is exactly divisible by π^4. Indeed, if $v(x) = 1$, then $x^4 - b_4x^2 - 2b_6x - b_8$ is congruent to $(x^2 - a_4)^2$ modulo π^4. Thus, $v(N_i) = 2v(\pi^2\alpha_i^2 - \pi^2\alpha_1\alpha_2)$. Since α_1 is not congruent to α_2 modulo π, our claim follows. Let us now consider the denominator D_i of $x(2P_i)$, $i = 1, 2$. By definition,

$$4x^3 + b_2x^2 + 2b_4x + b_6 = 4(x^3 + a_2x^2 + a_4x + a_6) + (a_1x + a_3)^2.$$

Thus, $v(D_i) = 2v(a_1\pi\alpha_i + a_3)$. Hence, if $v(a_1) \geqq 2$, then $\mathscr{E}$ is totally not split and $v(\Delta) = 8$. Assume now that $v(a_1) = 1$. Write $a_1 = A_1\pi$ and $a_3 = A_3\pi^2$ with A_1 and A_3 units. Note now that

$$(A_1\alpha_1 + A_3)(A_1\alpha_2 + A_3) = (A_1^2\alpha_1\alpha_2 + A_3^2) + A_1A_3(\alpha_1 + \alpha_2)$$

and that π does not divide $\alpha_1 + \alpha_2$. On the other hand, if $v(\Delta) = 9$, then $v(a_1^2a_4 \pm a_3^2) \geqq 5$. It follows that if $v(\Delta) = 9$, then $v(A_1\alpha_i + A_3) = 0$ and, thus, $\mathscr{E}$ is totally not split. This concludes the proof of 2.8.

The type I_0^* has 5 components, and one easily checks that the case $\delta = 1$ cannot happen with type I_0^*. We conclude from the above discussion that if $\mathscr{E}$ is not split, then $\delta = 2$ or 3. The case $\delta = 3$ happens only when $\mathscr{E}$ is totally not split.

2.9. Reduction of type I_{2n}^*, $n \geqq 1$ ($\Phi = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). Here

a_1	a_2	a_3	a_4	a_6
$\geqq 1$	1	$\geqq n+2$	$n+2$	$\geqq 2n+3$

and

b_2	b_4	b_6	b_8
$\geqq 2$	$\geqq n+3$	$\geqq 2n+4$	$2n+4$

.

It is easy to check that a point $P = (x, y)$ in $E(K)$ either has $v(x) = 1$, or has $v(x) \geqq n + 1$. Let $X := x/\pi^{n+1}$ and $Y := y/\pi^{n+1}$ and consider the equation

$$g(X, Y) := Y^2 + a_1XY + (a_3/\pi^{n+1})Y - [\pi^{n+1}X^3 + a_2X^2 + (a_4/\pi^{n+1})X + a_6/\pi^{2n+2}].$$

By hypothesis,

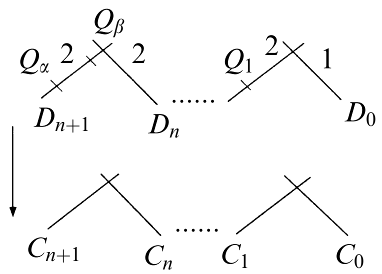
$$a_2X^2 + (a_4/\pi^{n+1})X + a_6/\pi^{2n+2} = a_2(X - \alpha)(X - \beta) \tag{6}$$

for some $\alpha, \beta \in \mathcal{O}_K$, $\alpha - \beta \notin \pi\mathcal{O}_K$. Thus, a point $P = (x, y)$ in $E(K)$ with $v(x) \geqq n + 1$ is such that either $x \equiv \alpha\pi^{n+1}$ or $x \equiv \beta\pi^{n+1}$ modulo π^{n+2}. Let $P_i := (x_i, y_i) \in E(K)$ be such that $v(x_1) = 1$, $v(x_2 - \alpha\pi^{n+1}) \geqq n + 2$ and $v(x_3 - \beta\pi^{n+1}) \geqq n + 2$.

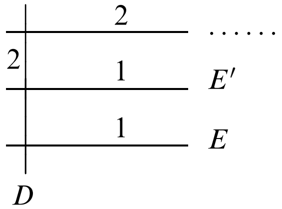
Lemma 2.10. *The reduction map* $\{\infty, P_1, P_2, P_3\} \to \Phi$ *is surjective.*

Sketch of proof. Recall that the Néron model of E/K is obtained from the minimal regular model $\mathscr{X}/\mathcal{O}_K$ of E/K by removing the singular points of $\mathscr{X}_k/k$. Thus, to prove our claim, it is sufficient to show that ∞, P_1, P_2, and P_3 reduce to four distinct components of multiplicity 1 in $\mathscr{X}_k$.

Consider the following model $\mathscr{Y}/\mathcal{O}_K$ of $\mathbb{P}^1/K$. Start with $\mathscr{Y}_0 = U \cup U'$, where $U = \operatorname{Spec} \mathcal{O}_K[x]$ and $U' = \operatorname{Spec} \mathcal{O}_K[1/x]$. Blow up the origin in $(\mathscr{Y}_0)_k$ to get $\mathscr{Y}_1$. Blow up the origin in the exceptional fiber of $(\mathscr{Y}_1)_k$ to get $\mathscr{Y}_2$. Continue in a similar fashion to construct $\mathscr{Y}_i$ from $\mathscr{Y}_{i-1}$. Let $\mathscr{Y} := \mathscr{Y}_{n+1}$. The special fiber of $\mathscr{Y}$ is a chain of $n+2$ smooth rational $\mathbb{P}^1/k$, say $C_0, \dots, C_{n+1}$, with C_0 denoting the component corresponding to $(\mathscr{Y}_0)_k$. Consider the model $\mathscr{Z}/\mathcal{O}_K$ of E/K obtained as the integral closure of $\mathscr{Y}$ in $K(E)$. Then $\mathscr{Z}_k$ is the union of $n+2$ smooth rational curves, say $D_0, \dots, D_{n+1}$, each having multiplicity 2 in $\mathscr{Z}_k$ except for the preimage D_0 of C_0, which has multiplicity 1. The scheme $\mathscr{Z}$ has two singular points Q_α and Q_β on $D_{n+1}$and a singular point Q_1 on D_1. Each of these points lie on the smooth locus of $\mathscr{Z}_k^{\mathrm{red}}$. The singularity of $\mathscr{Z}$ at Q_1 (resp. Q_α, Q_β) is resolved by the blow-up of Q_1 (resp. the blow-up of Q_α, Q_β). The three exceptional fibers have multiplicity one.



Let $\mathscr{V} \to \mathscr{Z}$ denote the blow-up of the three points Q_1, Q_α, Q_β, with exceptional fibers E_1, E_α and E_β. The normal model $\mathscr{V}$ contains two configurations in $\mathscr{V}_k$ of the form



such that $\mathscr{V}$ is regular at every closed point of E and E'. Let $\mathscr{W} \to \mathscr{V}$ denote the minimal desingularisation of $\mathscr{V}$. Then $(E \cdot E)_{\mathscr{W}} < -1$ and $(E' \cdot E')_{\mathscr{W}} < -1$. Similarly $(D \cdot D)_{\mathscr{W}} < -1$. Let $\mathscr{W} \to \mathscr{X}$ denote the contraction to the minimal regular model. It follows that D, E, and E' do not contract to points in $\mathscr{X}$.

The reader can check that a point $(x,y) \in E(K)$ reduces in $\mathscr{X}_k$ to the component corresponding to E_1 (resp. E_α or E_β) if $v(x) = 1$ (resp. if $v(x - \alpha\pi^{n+1}) \geqq n+2$, resp. if $v(x - \beta\pi^{n+1}) \geqq n+2$). Indeed, the integral closure of $\mathcal{O}_K[x/\pi^{n+1}]$ in $K(E)$ is the ring

$$\mathcal{O}_K[X, Y]/g(X, Y),$$

and we let the points Q_α and Q_β correspond to the maximal ideals $(\pi, Y, X-\alpha)$ and $(\pi, Y, X-\beta)$. This concludes the proof of Lemma 2.10.

Note that in the equicharacterstic zero case, the reduction map in 2.10 is also considered, using a different method, in [C-Z], 2.25.

Denote by φ_1 , φ_α, and φ_β the elements of Φ corresponding respectively to the components E_1, E_α, and E_β. Consider now a point $P = (x,y)$ in $E(K)$ with $v(x) = 1$ (e.g.,

$P = P_1$). Then the valuation of the numerator N of $x(2P)$ is equal to 4, and the denominator D of $x(2P)$ is congruent to b_2x^2 modulo π^4. Thus $v(b_2) = 2$ if and only if the image of P in $\mathscr{E}_k$ has order > 2. This is also equivalent to saying that φ_1 does not lift to an element of $\mathscr{E}_k$ of order 2. In particular, if $v(b_2) = 2$, then $\mathscr{E}$ is not split. Assume now that $v(x) \geqq n+1$ (e.g., when $P = P_2$ or P_3). Then $v(N) = v(b_8) = 2n+4$, and D is congruent to $b_2x^2 + b_6$ modulo π^{2n+4}. Hence, if $v(b_2) > 2$, we find that $\mathscr{E}$ is not split if $v(b_8) = v(b_6)$. In conclusion, $\mathscr{E}$ is not split if and only if $v(b_2) = 2$, or $v(b_2) > 2$ and $v(b_8) = v(b_6)$.

Proposition 2.11. *Assume that E/K has reduction of type I_{2n}^*, $n > 0$. Then*:

(a) *$\mathscr{E}/\mathcal{O}_K$ is totally not split if and only if $v(\Delta) = 2n+8$ and $v(b_8 + a_4^2) = 2n+5$.*

(b) *If $\mathscr{E}/\mathcal{O}_K$ is not split, then $v(\Delta) \leqq 4n+9$.*

Proof. (a) We saw above that φ_1 does not lift to an element of $\mathscr{E}_k$ of order 2 if and only if $v(b_2) = 2$. It is easy to check that this equality is equivalent to $v(\Delta) = 2n+8$, and also to $v(a_1) = 1$. Let us now assume that $v(b_2) = 2$. We need to show that φ_α or φ_β lifts to an element of $\mathscr{E}_k$ of order 2 if and only if $v(b_8 + a_4^2) > 2n+5$ (use the fact that $v(b_8 + a_4^2) \geqq 5$ in general). Since φ_α or φ_β lifting to an element of $\mathscr{E}_k$ of order 2 is equivalent to $2P_2$ or $2P_3$ reducing to the identity in $\mathscr{E}_k$, we can use the above discussion to find that $2P_i$ $(i = 2,3)$ reduces to the identity if and only if $v\big(b_2x(P_i)^2 + b_6\big) > 2n+4$. It is easily checked that the latter is equivalent to $v\big(a_1x(P_i) + a_3\big) > n+2$. Substituing $-a_3/a_1$ for $x(P_i)$ in equation (6), we see that either φ_α or φ_β lifts to an element of order 2 if and only if $v\big(a_2(a_3a_1^{-1})^2 + a_4(a_3a_1^{-1}) + a_6\big) > 2n+3$ or, equivalently,

$$v(a_2a_3^2 + a_1a_3a_4 + a_1^2a_6) > 2n+5. \tag{7}$$

Looking at the formula for b_8, we find that this last inequality is equivalent to $v(b_8 + a_4^2) > 2n+5$.

Let us now prove statement (b) of the proposition only in the case $\mathrm{char}(K) = 0$. The case where $\mathrm{char}(K) = 2$ is similar and is left to the reader. Let $e := v(2)$ and $v := v(a_1)$. Consider first the case where $e < v$. In this case $v(b_2) = 2e+1$ and $v(b_4) = e+n+2$. Moreover, since $\mathscr{E}$ is not split and $v(b_2) > 2$, we have $v(b_6) = v(b_8) = 2n+4$. Thus, $v(a_3) = n+2$. We find that

$-b_2^2b_8$	$-8b_4^3$	$-27b_6^2$	$9b_2b_4b_6$
$4e+2n+6$	$6e+3n+6$	$4n+8$	$3e+3n+7$

Clearly, $v(8b_4^3) > v(b_2b_4b_6)$. Thus $v(\Delta) \leqq 4n+8$ unless two of the numbers $4e+2n+6$, $4n+8$, and $3e+3n+7$ are equal and not bigger than $4n+8$.

The equality $4e+2n+6 = 3e+3n+7$ occurs if $e = n+1$, but in this case $4e+2n+6 > 4n+8$ and $v(\Delta) = 4n+8$.

The equality $3e+3n+7 = 4n+8$ occurs if $3e = n+1$, but in this case $4e+2n+6 < 4n+8$, so that $v(\Delta) < 4n+8$.

The equality $4e+2n+6=4n+8$ occurs if $2e=n+1$. In this case, $3e+3n+7>4n+8$, and we may not conclude that $v(\Delta)\leqq 4n+8$. Let us thus assume that n is odd and $e=(n+1)/2$. Let us consider first the case where $n\geqq 3$, so $e\geqq 2$. Then $v(b_2b_4b_6)\geqq 4n+10$. We claim that

$$v(\Delta)=v(-b_2^2b_8-27b_6^2)=4n+8 \text{ or } 4n+9.$$

All congruences below are modulo π^{4n+10}:

$$\begin{aligned}\Delta\equiv -b_2^2b_8-27b_6^2 &\equiv -b_2^2b_8+b_6^2\\ &\equiv -(4a_2+a_1^2)^2b_8+(a_3^2+4a_6)^2\\ &\equiv -16a_2^2b_8+a_3^4\\ &\equiv -16a_2^2(-a_4^2+a_2a_3^2)+a_3^4\\ &\equiv a_3^4-16a_2^2a_4^2-16a_2^3a_3^2.\end{aligned}$$

If $v(\Delta)>4n+8$, then $v(a_3^4-16a_2^2a_4^2)>4n+8$, which implies that $v(a_3^2-4a_2a_4)$ and $v(a_3^2+4a_2a_4)$ are both larger than $2n+4$. Thus

$$-b_2^2b_8-27b_6^2\equiv -16a_2^3a_3^2 \mod \pi^{4n+10}$$

and in this case $v(\Delta)=4n+9$.

Consider now the case $n=1$, so that $e=1$. In this case, $v(b_2b_4b_6)=4n+9$, and a slight change needs to be made in the above proof. We claim that

$$v(\Delta)=v(-b_2^2b_8-27b_6^2+9b_2b_4b_6)=4n+8 \text{ or } 4n+9.$$

We work again with congruences modulo π^{4n+10}:

$$\begin{aligned}-b_2^2b_8-27b_6^2+9b_2b_4b_6 &\equiv -16a_2^2b_8+a_4^3+b_2b_4b_6\\ &\equiv a_4^3-16a_2^2a_4^2+32a_2^2a_4^2-16a_2^3a_3^2+8a_2a_4a_3^2.\end{aligned}$$

If $v(\Delta)>4n+8$, then $v(a_3^2\pm 4a_2a_4)\geqq 2n+5$. Thus

$$\begin{aligned}\Delta &\equiv 8a_2a_4(4a_2a_4+a_3^2)-16a_2^3a_3^2\\ &\equiv -16a_2^3a_3^2.\end{aligned}$$

It follows that $v(\Delta)=4n+9=13$ in this case too.

Let us now consider the case where $e\geqq v$. Then $v(b_2)=2v$ and $v(b_4)\geqq v+n+2$, with equality if $e>v$. It is easy to check that if $v=1$, then $v(\Delta)=2n+8$. Thus, we may assume that $v > 1$. We find that

$-b_2^2 b_8$	$-8b_4^3$	$-27b_6^2$	$9b_2b_4b_6$
$4v+2n+4$	$\geqq 6v+3n+6$	$4n+8$	$\geqq 3v+3n+6$

.

If $4v+2n+4 \geqq 3v+3n+6$, then $v \geqq n+2$. If such is the case, $3v+3n+6 > 4n+8$ and $v(\Delta) = 4n+8$. If $4n+8 \geqq 3v+3n+6$ then $n+2 \geqq 3v$. If such is the case, then $4v+2n+4 < 3v+3n+6$ and $v(\Delta) = 4v+2n+4 < 4n+8$. If $4v+2n+4 = 4n+8$, we find that $v = (n+2)/2$. Thus n is even. Then

$$v(b_2b_4b_6) - 4n + 8 \geqq n/2 + 1 \geqq 2.$$

We claim that

$$v(\Delta) = v(-b_2^2 b_8 - 27b_6^2) = 4n+8 \text{ or } 4n+9.$$

We work again with congruences modulo π^{4n+10}:

$$\begin{aligned}\Delta \equiv -b_2^2 b_8 - 27b_6^2 &\equiv -b_2^2 b_8 + b_6^2 \\ &\equiv -a_1^4 b_8 + a_3^4 \\ &\equiv -a_1^4(-a_4^2 + a_2 a_3^2) + a_3^4 \\ &\equiv a_1^4 a_4^2 - a_3^4 - a_1^4 a_2 a_3^2.\end{aligned}$$

If $v(\Delta) > 4n+8$, then $v(a_1^2 a_2 \pm a_3^2) \geqq 2n+5$. Thus

$$\Delta \equiv -a_1^4 a_2 a_3^2 \bmod \pi^{4n+10}$$

and $v(\Delta) = 4n+9$. This concludes the proof of Proposition 2.11.

Assume that $\mathscr{E}/\mathcal{O}_K$ is not split and that E/K has reduction of type I_{2n}^*, $n > 0$. Then the number of components is $m = 2n+5$. Thus, $\delta(E) \leqq 2n+3$. If $\mathscr{E}/\mathcal{O}_K$ is totally not split, then $\delta(E) = 2$. This concludes the proof of Theorem 2.1 when $p = 2$.

2.12. The case $p = 3$.

2.13. Reduction of type IV ($\Phi = \mathbb{Z}/3\mathbb{Z}$). Here

a_1	a_2	a_3	a_4	a_6
$\geqq 0$	$\geqq 0$	$\geqq 1$	$\geqq 1$	$\geqq 2$

and

b_2	b_4	b_6	b_8
$\geqq 1$	$\geqq 1$	2	$\geqq 3$

.

Since $p = 3$, $E[2](K)$ injects in the special fiber $\mathscr{E}_k(k)$. Since $\Phi = \mathbb{Z}/3\mathbb{Z}$ and $\mathscr{E}_k^0(k)$ is additive, we find that $E[2](K)$ must be trivial. Hence, the equation

$$4x^3 + b_2x^2 + 2b_4x + b_6 = 0$$

has no solutions in K. One easily sees that this fact implies that $v(b_4) \geqq 2$. Since $p = 3$, we can replace y by $\frac{1}{2}(y - a_1x - a_3)$ to obtain a new equation for E with $a_1 = 0 = a_3$ and

a_2	a_4	a_6
$\geqq 1$	$\geqq 2$	2

and

b_2	b_4	b_6	b_8
$\geqq 1$	$\geqq 2$	2	$\geqq 3$

.

Note that now $b_2 = 4a_2$, $b_4 = 2a_4$, $b_6 = 4a_6$ and $b_8 = 4a_2a_6 - a_4^2$. Knowing that $v(b_4) \geqq 2$ in the initial equation allows us to show that $v(b_8) \geqq 3$ in the second equation for E. Let $P = (0, y(P))$ with $y(P)^2 = a_6$. Such a point reduces in Φ to a generator. We now use the following formuli to analyze the reduction of $3P = (x(3P), y(3P))$ in the connected component of $\mathscr{E}_k/k$:

$$(8) \qquad x(3P) = \left(\frac{y(2P) - y(P)}{x(2P)}\right)^2 - a_2 - x(2P),$$

$$y(2P) = -\frac{a_4x(2P)}{2y(P)} - \frac{a_6}{y(P)},$$

$$x(2P) = \frac{-b_8}{b_6}.$$

It follows from the above formuli that $\mathscr{E}_k$ is not split if and only if

$$v(y(2P) - y(P)) \geqq v(-b_8/b_6) = v(b_8) - 2.$$

Since

$$y(2P) - y(P) = \frac{-a_4x(2P) - 4a_6}{2y(P)},$$

and $v(a_6) = 2$, $v(a_4) \geqq 2$, and $v(x(2P)) \geqq 1$, we find that the valuation of $y(2P) - y(P)$ must be equal to 1. It follows that $\mathscr{E}_k$ is not split if and only if $v(a_2) = 1$, since $b_8 = 4a_2a_6 - a_4^2$. Thus,

$$\mathscr{E}_k \text{ is not split} \Leftrightarrow v(b_2) = 1 \quad \text{and} \quad v(b_8) = 3$$
$$\Leftrightarrow v(\Delta) = 5$$
$$\Leftrightarrow \delta = 1.$$

2.14. Reduction of type IV* ($\Phi = \mathbb{Z}/3\mathbb{Z}$). Here

a_1	a_2	a_3	a_4	a_6
$\geqq 1$	$\geqq 2$	$\geqq 2$	$\geqq 3$	$\geqq 4$

and

b_2	b_4	b_6	b_8
$\geqq 1$	$\geqq 3$	4	$\geqq 5$

in Tate's algorithm. Since $p = 3$ and $\Phi = \mathbb{Z}/3\mathbb{Z}$ we find that $E[2](K)$ must be trivial. Hence, the equation $4x^3 + b_2x^2 + 2b_4x + b_6 = 0$ has no solutions in K. One easily sees that this fact implies that $v(b_2) \geqq 2$. Since $p = 3$, we can replace y by $\frac{1}{2}(y - a_1x - a_3)$ to obtain a new equation for E with $a_1 = 0 = a_3$ and

a_2	a_4	a_6
$\geqq 2$	$\geqq 3$	4

and

b_2	b_4	b_6	b_8
$\geqq 2$	$\geqq 3$	4	$\geqq 6$

(where now $b_8 = 4a_2a_6 - a_4^2$). Let $P = (0, y(P))$ with $y(P) = a_6^2$. Such a point reduces to a generator in Φ. Using the formuli (8), we find again that $\mathscr{E}_k$ is not split if and only if

$$v(y(2P) - y(P)) \geqq v(-b_8/b_6) = v(b_8) - 4.$$

Since

$$y(2P) - y(P) = \frac{-a_4x(2P) - 4a_6}{2y(P)},$$

we find that $v(y(2P) - y(P)) = 2$. Thus,

$$\begin{aligned} \mathscr{E}_k \text{ is not split} &\Leftrightarrow v(b_8) = 6 \\ &\Rightarrow v(\Delta) = 9 \text{ or } 10 \\ &\Rightarrow \delta = 1 \text{ or } 2. \end{aligned}$$

Note that $v(\Delta) = 9$ if and only if $v(a_4) = 3$. When $v(a_4) > 3$ and $\mathscr{E}_k$ is not split, then $v(a_2) = 2$ and $v(\Delta) = 10$. This concludes the proof of Theorem 2.1.

3. Remarks and examples

Example 3.1. Let $p = 2$ and $n \in \mathbb{N}$, and let K be such that $e := v(2) < (n+1)/2$. Let $\alpha, \beta \in \mathcal{O}_K^*$ and consider the curve E/K

$$y^2 + \pi^{n+2}y = x^3 + \pi\alpha x^2 + \pi^{n+2}\beta x.$$

Its reduction is I_{2n}^*. This curve is such that $v(\Delta) = 4e + 2n + 6 < 4n + 8$ and $\delta = 4e$. Let $P = (0,0)$. Then the reduction of $2P$ is $(\bar{\beta}^2, \bar{\beta}^3)$. Thus the reduction of P has order 4 in $\mathscr{E}_k$ and E/K is not split.

Theorem 2.1 shows that $\delta(E) \leqq 2n + 3$. Choosing K such that $e = n/2$ when n is even and $(n-1)/2$ when n is odd produces examples of curves that do not have split reduction and with $\delta(E) = 2n$ when n is even and $\delta(E) = 2n - 2$ when n is odd. This example shows that there is no absolute bound, independent of the type of reduction,for the Swan conductor δ of elliptic curves with non-split reduction.

Remark 3.2. Let E/K be an elliptic curve. Let M/K be a finite extension. We show in this remark that the splitting type of the special fiber of the Néron model of E_M/M is not easily predictable, even when the extension M/K is tame. In particular, we will show below that *E/K having split reduction and M/K being tame does not always imply that E_M/M has split reduction*. On a more positive note, Proposition 3.3 below implies that if E/K does not have split reduction, then E_M/M has split reduction if $[M:K]$ is large enough.

Let $p = 2$. Consider an elliptic curve E/K with reduction of type II^* ($\Phi = \{1\}$), so that E/K has split reduction. We are going to show that the Néron model of E_M/M may not be split if $[M:K] = 3$. With type II^*, we have

a_1	a_2	a_3	a_4	a_6
$\geqq 1$	$\geqq 2$	$\geqq 3$	$\geqq 4$	5

Let $\pi = \eta^3$. After dividing the equation (3) by η^2 and changing variables $Y := y/\eta^6$ and $X := x/\eta^4$, we find an equation of the form

$$Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6',$$

with

a_1'	a_2'	a_3'	a_4'	a_6'
$\geqq 1$	$\geqq 2$	$\geqq 3$	$\geqq 4$	$= 3$

The reduction is of type I_0^*, according to Tate's Algorithm [Si2], IV.9.4. As we noted after 2.7, we can find x_0 with $v_M(x_0) = 1$ such that the translation $X \to X + x_0$ produces a new equation

$$Y^2 + a_1'XY + (a_1'x_0 + a_3')Y = X^3 + \cdots + a_6''$$

with $a_6'' = 0$. In this case, the discussion after 2.7 implies that E_M/M does not have split reduction if $v_M(a_1'x_0 + a_3') = 2$. Then E_M/M does not have split reduction if $v_M(a_1') = 1$ or, equivalently, if $v(a_1) = 1$.

Proposition 3.3. *Let E/K be an elliptic curve. Let M/K be any tamely ramified extension of degree $m \geqq 4$. Then E_M/M has split reduction.*

Proof. Recall that for any tame extension M/K,

$$\delta(E_M/M) = [M:K]\delta(E/K).$$

If $\delta(E/K) = 0$, then $\delta(E_M/M) = 0$. Hence, E_M has split reduction (Theorem 2.1). Assume from now on that $\delta(E/K) \geqq 1$. Then $\delta(E_M/M) \geqq m \geqq 4$. According to Theorem 2.1,

E_M/M has split reduction except possibly when $p = 2$ and E_M has reduction of type I_{2n}^*, $n > 0$. Consider this remaining case. Our next lemma implies that E/K has also reduction of type $\mathrm{I}_{2n'}^*$, $n' > 0$.

Lemma 3.4. *Let $p = 2$. Let E/K be an elliptic curve with reduction of type t. Let M/K be any finite extension of odd degree m. Then the reduction of E_M/M is of type t', as in the following table*:

t	t'
I_n $(n \geqq 0)$	I_{nm}
I_n^* $(n \geqq 0)$	I_{nm}^*
II or II*	II or II* or I_0^*
III or III*	III or III* or I_0
IV or IV*	IV or IV*

.

Sketch of proof. This lemma is well-known but we have been unable to find a reference for it in the literature. Let $\mathscr{X}/\mathcal{O}_K$ denote the minimal regular model of E/K whose special fiber has smooth components intersecting with normal crossings. A regular model $\mathscr{Z}/\mathcal{O}_M$ of E_M/M can be constructed as the minimal desingularization of the normalization $\mathscr{Y}$ of the base change $\mathscr{X} \times_{\mathrm{Spec}(\mathcal{O}_K)} \mathrm{Spec}(\mathcal{O}_M)$. The singularities of the normal model $\mathscr{Y}$ are well-understood when the extension M/K is tame: each singularity is resolved by a single chain of rational curves (Hirzebruch-Young singularities). Except for the case $t = \mathrm{I}_n$, the graph associated to the special fiber of $\mathscr{X}$ is a tree. This tree has a single node of multiplicity $r = 6$ when t is II or II*, a single node of multiplicity $r = 4$ when t is III or III*, a single node of multiplicity $r = 3$ when t is IV or IV*, and two nodes of multiplicity $r = 2$ when t is I_n^* and $n > 0$. The key to the proof of the lemma is to note that in each of the cases where the graph of $\mathscr{X}$ has a single node of multiplicity r, the graph of the special fiber of $\mathscr{Y}$ must be a tree with a single node of multiplicity $r/\gcd(r, m)$.

Let us return to the proof of 3.3. Let $\mathscr{W}$ be the minimal Weierstrass model of E/K. Then $\mathscr{E}^0$ is an open subset of $\mathscr{W}$. Consider the equation (3) of $\mathscr{W}$. It follows from Tate's algorithm that $v(a_6) \geqq 3$ and, thus, $v_M(a_6) \geqq 12$. Moreover, $v_M(a_i) \geqq 4$. So (3) is not minimal for E_M. Denote by $\mathscr{E}'$ the Néron model of E_M. Then the canonical map $\mathscr{E}_k^0 \to \mathscr{E}_k'^0$ is the zero map, as can be easily checked by noting that a point $(x, y) \in E(K)$ that reduces to a point of $\mathscr{E}_k^0(k)$ must reduce, under the reduction map of E_M/M, to the point $(0, 0) \in \mathscr{E}_k'^0(k)$. Since m kills the kernel of the natural map $\Phi_K \to \Phi_M$ (see [Lor2], 3.1, (5) and (10)), we find that $\Phi_K \to \Phi_M$ is an isomorphism. Let $\varphi \in \Phi_M = \Phi_K$ be an element of order 2. Let $x \in \mathscr{E}_k$ be in the preimage of φ. Let x' be the image of x in $\mathscr{E}_k'$. Since $2x \in \mathscr{E}_k^0$, we find that $2x' = 0$. Since x' is in the preimage of φ, E_M/M has split reduction.

Remark 3.5. Let E/K be an elliptic curve, and denote by L/K the extension minimal with the property that E_L/L has semistable reduction. Recall that in the case of elliptic curves, if 3 divides $[L : K]$, then 3 exactly divides $[L : K]$. It is shown in [ELL] that $[L : K]$ kills the group Φ_K when the curve E has potentially good reduction. It is thus natural to wonder whether $[L : K]$ also kills $\mathscr{E}_k/k$ when Φ_K is not trivial. The following example shows that the answer to this question is negative in general. Take the curve 54B3 in [Cre]:

$$y^2 + xy + y = x^3 - x^2 - 14x + 29,$$

which has reduction of type IV when $p = 3$. The point $P = (3,1)$ has order 9 in $E(\mathbb{Q})$, with $2P = (-3,7)$ and $3P = (1,-5)$. We find that $(0,1)$ is the singular point in the special fiber. Since $3P$ does not reduce to ∞, we find that $\bar{P}$ has order 9 in the special fiber and, thus, $\mathscr{E}_k$ is not split and $[L : K]$ does not kill $\mathscr{E}_k$.

Remark 3.6. The following examples show that the possible relationships between the splitting types of the special fibers of the Néron models of two isogenous curves are not easily predictable. Consider the four curves of conductor 40 in the tables [Cre]. These four curves are all isogenous, with the curves A1, A2, and A3 not split, and the curve A4 split. Note that the curves A2 and A4 both have reduction of type III* (while A1 is of type I_1^* and A3 is of type III).

Remark 3.7. One strategy for determining whether a Néron model $\mathscr{G}/K$ is split is to find a torsion point in $G(K)$ (and not in $\mathscr{G}(k)$) with the appropriate order and reduction. However, since there is no relationship in general between $G[p](K)$ and the p-part of Φ_K when $\mathrm{char}(k) = p$, this method has a very limited scope of application. We shall only use this method below to exhibit an example of a jacobian of dimension g with additive and split reduction when $p^s = 2g + 1$. Note however that this method may possibly be used to discuss the splitting property of the Néron model of the jacobian of the modular curve $X_0(mp^r)/\mathbb{Q}_p^{nr}$ when $p \geqq 5$. Indeed, it is proven in [Lor4], 2.3, that the p-part of the group of components is in the image, under the reduction map, of the cuspidal torsion subgroup.

Let $p \geqq 3$ be prime and let $g \geqq 1$. Consider the proper smooth completion X/K of the affine plane curve given by the equation

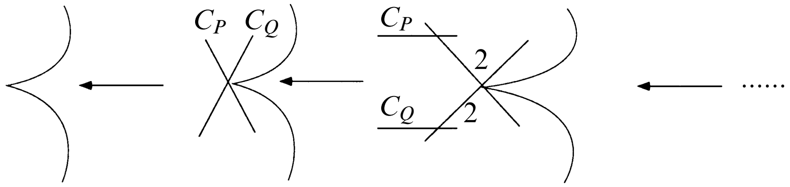
$$y^2 = x^{2g+1} + \pi^2.$$

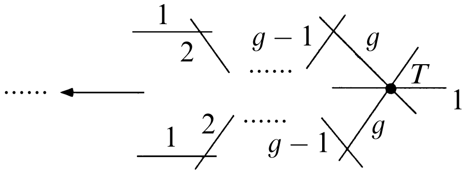
The curve X/K has genus g. Let A/K be its Jacobian. Let $P := (0, \pi)$ and $Q := (0, -\pi)$. The point $P - Q$ belongs to $A(K)$ and has order $2g + 1$. We claim that the group of components Φ_K of the Néron model $\mathscr{A}/\mathcal{O}_K$ of A/K is cyclic of order $2g + 1$ and that $P - Q$ reduces to a generator of Φ_K. Thus A/K has split reduction. To prove our claim, we shall exhibit a regular model $\mathscr{X}/\mathcal{O}_K$ of X/K.

Consider the following model $\mathscr{X}_0/\mathcal{O}_K$ of X/K. The scheme $\mathscr{X}_0$ is the plane projective curve in $\mathbb{P}^2/\mathcal{O}_K$ given by the equation $y^2z^{2g-1} = x^{2g+1} + \pi^2z^{2g+1}$. We shall now describe pictorially the sequence of blow-ups

$$\mathscr{X}_0 \leftarrow \mathscr{X}_1 \leftarrow \cdots \leftarrow \mathscr{X}_g$$

that leads to a regular scheme $\mathscr{X}_g/\mathcal{O}_K$. More precisely, we describe below the special fibers of the schemes $\mathscr{X}_i$:

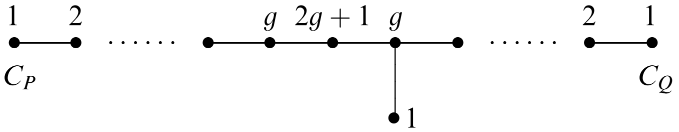




The triple point T in the model $\mathscr{X}_g$ is seen in the chart

$$\operatorname{Spec}\mathcal{O}_K\left[x, y, \frac{y}{x^g}, \frac{\pi}{x^g}\right]/(y/x^g)^2 - \left(x + (\pi/x^g)^2\right).$$

All irreducible components appearing in the pictures above are smooth $\mathbb{P}^1$. We leave the details of this computation to the reader. The blow-up $\mathscr{X}/\mathcal{O}_K$ of the point T is a model with normal crossings whose associated graph is a tree. Thus A/K has purely additive reduction ([BLR], Thm. 4 on p. 267, and 9.2/9, 9.2/10). The tree is represented below:



One checks easily that P and Q reduce to two distinct components of multiplicity 1, say C_P and C_Q. Indeed, consider the following chart of $\mathscr{X}_1$:

$$U = \operatorname{Spec}\mathcal{O}_K\left[x, y, \frac{y}{\pi}, \frac{x}{\pi}\right]/(y/\pi)^2 - \left((x/\pi)^{2g+1}\pi^{2g-1} + 1\right).$$

The special fiber of U consists of two affine curves, and P reduces into the component $y/\pi = 1$ while Q reduces into the component $y/\pi = -1$. It is shown in [BLR], 9.6/6, that $\Phi_K \cong \mathbb{Z}/(2g+1)\mathbb{Z}$. That $P - Q$ reduces to a generator is shown in [Lor3], 4.4.

Let p^c be the largest power of p that divides the order of an element of Φ. The following examples show that in general, as expected, the fact that the special fiber $\mathscr{E}_k$ is not split does not provide any indication as to whether the group $E(K)$ contains a point of order p^{c+1}.

Example 3.8. Let $p = 2$. Let E/K be an elliptic curve with reduction of type III. Assume that $\mathscr{E}_k/k$ is not split, so that $\mathscr{E}_k(k)$ contains a point of order 4. We exhibit below such an elliptic curve with no 4-torsion points in $E(K)$. Suppose that $P = (x, y)$ is a point of order 4 in $E(K)$. Let $u := x(2P)$. Then $v(u) = 0$ since $\mathscr{E}_k/k$ is not split. The coordinate $x := x(P)$ is solution of the equations

$$\begin{cases} (x^4 - b_4x^2 - b_6x - b_8)(4x^3 + b_2x^2 + 2b_4x + b_6)^{-1} = u, \\ u^3 + b_2u^2/4 + b_4u/2 + b_6/4 = 0. \end{cases}$$

It follows that

$$\begin{cases} v(-b_8 + ub_6) \geqq 4, \\ v(a_4^2 + ua_3^2) \geqq 3 \end{cases}$$

so that $v(a_3^8 + a_1^2a_3^2a_4^4 + 2^2a_4^6) \geqq 9$. It is easy to exhibit examples where this last congruence cannot be satisfied, such as in

$$y^2 + 2xy + 2y = x^3 + 2x + 4.$$

Example 3.9. Consider the curve 24A4 in [Cre]: $y^2 = x^3 - x^2 + x$. Its reduction is of type III when $p = 2$. The singular point is $(1,1)$ in reduction. Let $P = (1,1)$. This point has order 4 and $2P = (0,0)$. Thus the extension $\mathscr{E}_k$ is not split.

Remark 3.10. Let F/K be a finite extension and let A/F be any abelian variety. It is natural to wonder what are the possible relationships between the splitting type of A/F and that of its Weil restriction $\mathrm{Res}_{F/K}(A)/K$. Let us note first that $\Phi_K(\mathrm{Res}_{F/K}(A)/K)$ is isomorphic to $\Phi_F(A)$ ([ELL], proof of Theorem 1), so that if p does not divide $|\Phi_F(A)|$, then A/F has split reduction, and $\mathrm{Res}_{F/K}(A)/K$ has split reduction for any extension F/K. The following example shows that the hypothesis that A/F has split reduction does not imply, in general, that $\mathrm{Res}_{F/K}(A)/K$ has split reduction, even when F/K is a tame extension.

Let $p = 3$ and let F/K be a quadratic extension. Let E/K be an elliptic curve with reduction of type IV* ($|\Phi_K| = 3$) with $v(b_8) = 6$ and $\delta(E) = 2$. Then E/K does not have split reduction (see 2.14). Moreover, E_F/F has split reduction: Indeed, since $\delta(E_F) = 4$, Theorem 2.1 shows that to prove our claim, it suffices to show that the reduction of E_F is not of type I_{2n}^* for $n \geqq 0$. Since the kernel of the map $\Phi_K(E) \to \Phi_F(E_F)$ is killed by $[F:K]$ ([ELL], Theorem 1), we find that 3 divides $|\Phi_F(E_F)|$ and, thus, E_F cannot have reduction of type I_{2n}^* for $n \geqq 0$. It is shown in [Mil], Proposition 7 and following example, that $\mathrm{Res}_{F/K}(E_F)/K$ is isogenous over K to the product of E/K by its quadratic twist E_d/K, and that the isogeny can be chosen to have degree 4. Thus, since $E \times E_d$ does not have split reduction, Proposition 1.11 implies that $\mathrm{Res}_{F/K}(E_F)/K$ cannot have split reduction either.

4. Norm tori and their duals

Let T/K be an algebraic torus. Such a group scheme has a Néron model $\mathscr{T}/\mathcal{O}_K$, locally of finite type ([BLR], 10.1/6). When the special fiber $\mathscr{T}_k$ is a unipotent group, the group scheme $\mathscr{T}$ is of finite type over $\mathcal{O}_K$ ([BLR], 10.2/1). In this section, we study the splitting properties of $\mathscr{T}$ when T is a norm torus or its dual. Our main result is Theorem 4.6 below.

Let F/K be any finite separable extension, and denote by L/K its Galois closure over K. Let $\Gamma = \mathrm{Gal}(L/K)$ and $\Delta = \mathrm{Gal}(L/F)$. Let $g_1, \dots, g_n \in \Gamma$ be such that $\Gamma/\Delta = \{g_1\Delta, \dots, g_n\Delta\}$. Let $\{\delta_1, \dots, \delta_n\}$ be the basis of the permutation module $\mathbb{Z}[\Gamma/\Delta]$

defined by the $g_i\Delta$'s. Consider the exact sequence of $\mathrm{Gal}(K^s/K)$-modules

$$0 \to \mathbb{Z} \xrightarrow{\varepsilon} \mathbb{Z}[\Gamma/\Delta] \to \mathrm{Coker}(\varepsilon) \to 0 \tag{9}$$

where $\varepsilon(1) := \sum_{i=1}^{n} \delta_i$. By definition, this exact sequence of $\mathrm{Gal}(K^s/K)$-modules induces an exact sequence of tori over K

$$0 \to R^1_{F/K}\mathbb{G}_{m,F} \to R_{F/K}\mathbb{G}_{m,F} \to \mathbb{G}_{m,K} \to 0,$$

where the torus $R_{F/K}\mathbb{G}_{m,F}$ is the Weil restriction of $\mathbb{G}_{m,F}$, and the map $R_{F/K}\mathbb{G}_{m,F} \to \mathbb{G}_{m,K}$ is the norm map. Denote by $T := R^1_{F/K}\mathbb{G}_m$ the associated norm torus. Then

$$R_{F/K}\mathbb{G}_{m,F}(K) = F^*, \quad \text{and} \quad T(K) = \{z \in F^* \mid N_{F/K}(z) = 1\}.$$

The universal property of the Weil restriction implies the existence of a canonical closed immersion $\mathbb{G}_{m,K} \to R_{F/K}\mathbb{G}_{m,F}$. Let S/K be the quotient torus defined by the exact sequence

$$0 \to \mathbb{G}_{m,K} \to R_{F/K}\mathbb{G}_{m,F} \to S \to 0. \tag{10}$$

The associated exact sequence of groups of characters

$$0 \to X(S) \to \mathbb{Z}[\Gamma/\Delta] \xrightarrow{r} \mathbb{Z} \to 0 \tag{11}$$

is defined by the augmentation map $r\left(\sum_{1 \leqq i \leqq n} m_i\delta_i\right) := \sum_{1 \leqq i \leqq n} m_i$. For any Γ-module N, let us denote by $N^\wedge := \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Z})$ its dual. Recall that the Γ-module structure on $N^\wedge$ is as follows: For any $f \in N^\wedge$, $g \in \Gamma$, and $x \in N$, set $(gf)(x) := f(g^{-1}x)$. Recall that if T/K is the torus corresponding to N, then the torus corresponding to $N^\wedge$ is called the dual of T. The next lemma is well-known.

Lemma 4.1. *Let F/K be a finite separable extension. Let $S := (R_{F/K}\mathbb{G}_{m,F})/\mathbb{G}_{m,K}$ be the quotient torus. Then*:

(a) *The torus S is isomorphic to the dual of T.*

(b) *If F/K is a cyclic extension, then S and T are isomorphic.* (*See* 4.17 *for the converse.*)

Proof. (a) Let $\{\delta_i^\wedge\}_i$ be the dual basis of $\{\delta_i\}_i$. There is a (non-canonical) isomorphism of Γ-modules $\mathbb{Z}[\Gamma/\Delta] \simeq \mathbb{Z}[\Gamma/\Delta]^\wedge$ defined by $\delta_i \mapsto \delta_i^\wedge$. We then have a commutative diagram of homomorphisms of Γ-modules

$$\begin{array}{ccccccccc}
0 & \longrightarrow & X(S) & \longrightarrow & \mathbb{Z}[\Gamma/\Delta] & \xrightarrow{r} & \mathbb{Z} & \longrightarrow & 0 \\
 & & & & \downarrow & & \| & & \\
0 & \longrightarrow & X(T)^\wedge & \longrightarrow & \mathbb{Z}[\Gamma/\Delta]^\wedge & \xrightarrow{\varepsilon^\wedge} & \mathbb{Z} & \longrightarrow & 0.
\end{array}$$

Thus $X(S)$ is isomorphic to $X(T)^{\wedge}$ which, by definition, is the character module of the dual of T.

(b) By assumption, $F = L$ and $\Delta = 0$. Let σ be a generator of Γ. Then one easily checks that the complex of Γ-modules

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\varepsilon} \mathbb{Z}[\Gamma] \xrightarrow{\sigma-1} \mathbb{Z}[\Gamma] \xrightarrow{r} \mathbb{Z} \longrightarrow 0$$

is exact. Hence $X(T) = \operatorname{coker}(\varepsilon)$ is isomorphic to $X(S) = \ker(r)$.

Proposition 4.2. *Let $0 \to T_1 \to T_2 \to T_3 \to 0$ be an exact sequence of tori over K with T_1/K split. Let $\mathscr{T}_i/\mathcal{O}_K$ be the Néron model of T_i, $i = 1, 2, 3$. Then the following sequences of groups are exact*:

(a) $0 \to \Phi(T_1) \to \Phi(T_2) \to \Phi(T_3) \to 0$,

(b) $0 \to \mathscr{T}^0_{1,k}(k) \to \mathscr{T}^0_{2,k}(k) \to \mathscr{T}^0_{3,k}(k) \to 0$, *and*

(c) $0 \to \mathscr{T}_{1,k}(k) \to \mathscr{T}_{2,k}(k) \to \mathscr{T}_{3,k}(k) \to 0$.

Proof. (a) Let us first show that the map $\Phi(T_1) \to \Phi(T_2)$ is injective. Let L/K denote an extension such that $(T_2)_L/L$ has semistable reduction. Since both $(T_1)_L$ and $(T_2)_L$ are split tori, we find that the map $\Phi\big((T_1)_L\big) \to \Phi\big((T_2)_L\big)$ is injective. Since T_1/K is a split torus, the map $\Phi(T_1) \to \Phi\big((T_1)_L\big)$ is also injective. It follows that the map $\Phi(T_1) \to \Phi(T_2)$ is injective. Since $\Phi(T_1) \to \Phi(T_2) \to \Phi(T_3) \to 0$ is exact because T_1/K is split ([B-X], 4.2 and 4.9), we get the exactness of (a).

(b) follows easily from (a) and (c). So it remains to prove (c). Let $j\colon \operatorname{Spec} K \to \operatorname{Spec} \mathcal{O}_K$ be the canonical map. Then j_*T_i, as sheaf on the smooth site $\operatorname{Spec}(\mathcal{O}_K)_{\mathrm{sm}}$, is represented by the Néron model $\mathscr{T}_i$. Since T_1 is a split torus, $R^1j_*T_1 = 0$ on the smooth site (see [Mil2], beginning of the proof of III.C.10) and we have an exact sequence

$$0 \to \mathscr{T}_1 \to \mathscr{T}_2 \to \mathscr{T}_3 \to 0 \qquad (12)$$

of sheaves on the smooth site $\operatorname{Spec}(\mathcal{O}_K)_{\mathrm{sm}}$. To prove (c), it is enough to show that (12) is exact as complex of group schemes (recall that k is algebraically closed). What follows is inspired by conversations with C.-L. Chai.

Lemma 4.3. *Let $\mathscr{S}$ be any scheme. Let $\mathscr{T}_2/\mathscr{S}$ and $\mathscr{T}_3/\mathscr{S}$ be two group schemes over $\mathscr{S}$, each flat* (*and, thus, faithfully flat*) *and locally of finite presentation over $\mathscr{S}$. Let $\phi\colon \mathscr{T}_2 \to \mathscr{T}_3$ be a morphism of group schemes over $\mathscr{S}$, and let $\mathscr{T}$ denote the kernel of ϕ* (*as group scheme*). *Then*:

(a) *If $\phi\colon \mathscr{T}_2 \to \mathscr{T}_3$ induces a surjective map of sheaves on $\mathscr{S}_{\mathrm{fppf}}$, then $\mathscr{T}/S$ is flat.*

(b) *If $\phi\colon \mathscr{T}_2 \to \mathscr{T}_3$ induces a surjective map of sheaves on $\mathscr{S}_{\mathrm{sm}}$, and both $\mathscr{T}_2/\mathscr{S}$ and $\mathscr{T}_3/\mathscr{S}$ are smooth over $\mathscr{S}$, then $\mathscr{T}/\mathscr{S}$ is smooth.*

Proof. The surjectivity of the map of sheaves on $\mathcal{S}_{\mathrm{fppf}}$ implies the existence of a faithfully flat morphism $f: \mathcal{W} \to \mathcal{T}_3$ and a commutative diagram

$$\begin{array}{ccc} \mathcal{T}_2 & \longrightarrow & \mathcal{T}_3 \\ {\scriptstyle s}\uparrow & & \Vert \\ \mathcal{W} & \xrightarrow{\ f\ } & \mathcal{T}_3. \end{array}$$

When the map is surjective on $\mathcal{S}_{\mathrm{sm}}$ and $\mathcal{T}_3$ is smooth, we may assume in addition that f is smooth. The existence of the section s and the fact that $\mathcal{T}_2$ and $\mathcal{T}_3$ are group schemes imply the existence of an isomorphism of schemes over $\mathcal{W}$ between $\mathcal{T}_2 \times_{\mathcal{T}_3} \mathcal{W}$ and $\mathcal{T} \times_{\mathcal{S}} \mathcal{W}$. The scheme $\mathcal{T}_2 \times_{\mathcal{T}_3} \mathcal{W}$ is flat over $\mathcal{S}$ since $\mathcal{T}_2/\mathcal{S}$ is flat. This scheme is smooth over $\mathcal{S}$ if $\mathcal{T}_2/\mathcal{S}$ is smooth and f is smooth. Thus, $\mathcal{T} \times_{\mathcal{S}} \mathcal{W}$ is flat over $\mathcal{S}$, and smooth over $\mathcal{S}$ under the hypotheses of Part (b). Since $\mathcal{T} \times_{\mathcal{S}} \mathcal{W}$ is faithfully flat over $\mathcal{T}$, we conclude that $\mathcal{T}/\mathcal{S}$ is flat, and Part (a) is proved. When $\mathcal{T} \times_{\mathcal{S}} \mathcal{W} \to \mathcal{S}$ is smooth, each fiber of this map is smooth. Recall that a product of varieties is smooth if and only if each factor is smooth. It follows that the fibers of $\mathcal{T}/\mathcal{S}$ are smooth. Since $\mathcal{T}/\mathcal{S}$ is flat, it is then smooth, and our lemma is proved.

Let $\mathcal{S} = \mathrm{Spec}(\mathcal{O}_K)$. Both $\mathcal{T}/\mathcal{S}$ and $\mathcal{T}_1/\mathcal{S}$ are smooth over $\mathcal{S}$ and represent the kernel of the morphism of sheaves on $\mathcal{S}_{\mathrm{sm}}$ associated with the morphism $\mathcal{T}_2 \to \mathcal{T}_3$. Hence, $\mathcal{T}$ is isomorphic to $\mathcal{T}_1$. Proposition 4.2 follows since $\mathcal{T}_2 \to \mathcal{T}_3$ is obviously surjective as morphism of schemes when it is surjective as map of sheaves for the smooth topology.

Let $R := R_{F/K}\mathbb{G}_{m,F}$. Let $\mathcal{G}_m/\mathcal{O}_K$, $\mathcal{R}/\mathcal{O}_K$, and $\mathcal{S}/\mathcal{O}_K$ denote respectively the Néron models of $\mathbb{G}_{m,K}$, R, and S.

Corollary 4.4. *Let F/K be a finite separable extension of degree n. Let $S := (R_{F/K}\mathbb{G}_{m,F})/\mathbb{G}_{m,K}$ be the quotient torus. Then*:

(a) *Let $A := \mathcal{O}_F \otimes_{\mathcal{O}_K} k$. Then the following complex of groups is exact*:

$$0 \to \mathcal{G}^0_{m,k}(k) \to R_{A/k}\mathbb{G}_{m,A}(k) \to \mathcal{S}^0_k(k) \to 0. \tag{13}$$

(b) $\Phi(S) \simeq \mathbb{Z}/n\mathbb{Z}$.

Proof. Note that $\mathcal{G}^0_m = \mathbb{G}_{m,\mathcal{O}_K}$ and $\mathcal{R}^0 = R_{\mathcal{O}_F/\mathcal{O}_K}(\mathbb{G}_{m,\mathcal{O}_F})$ ([N-X], 3.1). Proposition 4.2 applied to the exact sequence (10) shows that both the sequence (13) and the sequence

$$0 \to \Phi(\mathbb{G}_m) \to \Phi(R) \to \Phi(S) \to 0 \tag{14}$$

are exact. The exact sequence (14) is canonically isomorphic to

$$0 \to K^*/\mathcal{O}_K^* \to F^*/\mathcal{O}_F^* \to \Phi(S) \to 0, \tag{15}$$

where the first map is induced by the natural inclusion $K \subset F$. Since F/K is totally ramified, we find that $\Phi(S) \simeq F^*/K^* \simeq \mathbb{Z}/n\mathbb{Z}$.

Let F/K be a finite separable extension of degree n. A uniformizing element t of F satisfies an Eisenstein equation

$$(16) \qquad t^n + a_1 t^{n-1} + a_2 t^{n-2} + \cdots + a_n = 0$$

with $a_i \in \pi\mathcal{O}_K$ and $v(a_n) = 1$. Set $a_0 := 1$. The different of the extension F/K is given by

$$v_F(\mathcal{D}_{F/K}) = \min_{0 \leqq i \leqq n-1} \{n(v(a_i) + v(n-i)) + n - 1 - i\}.$$

Let S be any torus over K. Let $T_\ell(S)$ denote the Tate module of S. Recall that when ℓ is a prime different from p, the Galois module $T_\ell(S)$ has rank $\dim(S)$ over $\mathbb{Z}_\ell$, and the evaluation of characters $S \times X(S) \to \mathbb{G}_m$ induces Galois isomorphisms between $S[\ell^n](K^s)$ and $\mathrm{Hom}(X(S)/\ell^n X(S), \mathbb{G}_m[\ell^n](K^s))$. It follows, under our assumption on K, that $T_\ell(S)$ is isomorphic, as Galois module, to the dual of $X(S) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Thus the Swan conductor (see 1.12) $\delta(S)$ is that of the representation $\Gamma \to \mathrm{Aut}(X(S) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell)$.

Lemma 4.5. *Let S be the quotient torus $(R_{F/K}\mathbb{G}_{m,F})/\mathbb{G}_{m,K}$. Then the Swan conductor $\delta(S)$ of S is given by $\delta(S) = v_F(\mathcal{D}_{F/K}) - (n-1)$.*

Proof. Since the Swan conductor is an additive function on exact sequences, and since the Swan conductor of the trivial representation is zero, we conclude from the exact sequence (11) that $\delta(S)$ is the Swan conductor of the permutation representation $\rho: \Gamma \to \mathrm{Aut}(\mathbb{Q}_\ell[\Gamma/\Delta])$. By definition,

$$\delta(\rho) = f(\rho) - \dim_{\mathbb{Q}_\ell} \mathbb{Q}_\ell[\Gamma/\Delta]/\mathbb{Q}_\ell[\Gamma/\Delta]^\Gamma = f(\rho) - (n-1)$$

where $f(\rho)$ is the Artin conductor of ρ (see [Ser], VI, §2 for the definition of f). On the other hand, $\rho = \mathrm{ind}_\Delta^\Gamma(1_\Delta)$ with $1_\Delta: \Delta \to \mathrm{Aut}(\mathbb{Q}_\ell)$ being the unit representation of Δ. Hence,

$$f(\rho) = v_F(\mathcal{D}_{F/K}) \deg(1_\Delta) + f(1_\Delta) = v_F(\mathcal{D}_{F/K})$$

([Ser], VI, §2, Corollary of Proposition 4) and the lemma is proved.

We may now state and prove the main theorem of this section.

Theorem 4.6. *Let F/K be a finite separable extension of degree n. Let S be the quotient torus $(R_{F/K}\mathbb{G}_{m,F})/\mathbb{G}_{m,K}$. Let $\delta(S)$ be the Swan conductor of S.*

(a) *The torus S has totally not split reduction if and only if* $1 \leqq \delta(S) \leqq \dim S$.

(b) *The torus S/K has split reduction if and only if $v(a_i) \geqq 2$ for every coefficient a_i in equation* (16) *such that $v(i) \leqq v(n) - 1$.*

(c) *If $\delta(S) \geqq (\dim S + 1)\,\mathrm{ord}_p(\dim S + 1) v_K(p)$, then S/K has split reduction.*

Proof. Fix uniformizing elements t and π of F and K, respectively. We have an explicit description of the reduction map $S(K) \to \mathcal{S}_k(k)$. Let $z \in S(K)$. Let $y \in R(K) = F^*$ be a preimage of z. Using the exact sequence (15), we see that the image of z in $\Phi(S)$ has order, say m, equal to the order of $v_F(y)$ in $\mathbb{Z}/n\mathbb{Z}$. Now consider $mz \in S(K)$, which reduces to a point of $\mathscr{S}_k^0$. Recall that $\mathscr{R}^0(\mathcal{O}_K) = \mathcal{O}_F^*$, $\mathscr{G}_m^0(\mathcal{O}_K) = \mathcal{O}_K^*$, and that the kernel of the map $\mathscr{R}^0(\mathcal{O}_K) \to \mathscr{R}_k^0(k)$, that is, the kernel of $\mathcal{O}_F^* \to (\mathcal{O}_F \otimes_{\mathcal{O}_K} k)^*$, is $1 + \pi\mathcal{O}_F$. Using these facts and the exact sequence (13), we see that mz reduces to $0 \in \mathscr{S}_k$ if and only if there exists $x \in K^*$ such that $y^m x^{-1} \in 1 + \pi\mathcal{O}_F$.

Claim 4.7. *Let $u_0 := t^n \pi^{-1} \in \mathcal{O}_F^*$. Let $m \in \mathbb{N}$ be a divisor of n. We claim that there exists a point in $\mathscr{S}_k$ of order m whose image in $\Phi(S)$ also has order m if and only if u_0 is a m-th power in $\mathcal{O}_F/\pi\mathcal{O}_F$.*

According to the above discussion, the existence of the desired point in $\mathscr{S}_k$ is equivalent to the existence of $x \in K^*$, $y \in F^*$ such that

$$\begin{cases} v_F(y) \equiv n/m \bmod n, \\ y^m x^{-1} \in 1 + \pi\mathcal{O}_F. \end{cases}$$

Suppose that such x and y exist. Multiplying x and y by suitable powers of π, we are reduced to the case where $v_F(y) = n/m$. Thus, $v(x) = 1$. Write $y = t^{n/m}u^{-1}$, with $u \in \mathcal{O}_F^*$. Then

$$u_0 = y^m u^m \pi^{-1} \in u^m (x\pi^{-1})(1 + \pi\mathcal{O}_F) \subseteq \mathcal{O}_F^m + \pi\mathcal{O}_F$$

because $\mathcal{O}_K = \mathcal{O}_K^m + \pi\mathcal{O}_K$. Conversely, if $u_0 \equiv v^m \bmod \pi$, then we can take $y = t^{n/m}v^{-1}$ and $x = \pi$.

Recall that if n is prime to p, then $\mathscr{S}_k$ is split (4.4 (b) and 1.5) and $\delta(S) = 0$. Assume now that p divides n. Then $\mathscr{S}_k$ is totally not split if and only if $t^n\pi^{-1}$ is not a p-th power in $\mathcal{O}_F/\pi\mathcal{O}_F$. The latter is equivalent to the following property in equation (16): There exists $1 \leqq i \leqq n-1$ with $\gcd(p, i) = 1$ and $v(a_i) = 1$. In terms of the different, this means that $v_F(\mathscr{D}_{F/K}) \leqq 2n - 2$. Thus, part (a) follows from Lemma 4.5. The proof of (b) is similar and the details are left to the reader.

To prove part (c), we note that $v_F(nt^{n-1}) = n\,\mathrm{ord}_p(n)v_K(p) + n - 1$. If $\delta(S) \geqq n\,\mathrm{ord}_p(n)v_K(p)$, then

$$v_F(\mathscr{D}_{F/K}) = \delta(S) + n - 1 \geqq v_F(nt^{n-1}).$$

It follows immediately from this inequality that the criterion given in (b) is satisfied and that S/K has split reduction.

Corollary 4.8. *Let F/K be a cyclic extension. Let $T = R^1_{F/K}(\mathbb{G}_{m,F})$ be the norm torus. Then T has totally not split reduction if and only if $1 \leqq \delta(T) \leqq \dim T$.*

Proof. Follows from Theorem 4.6 (a) and Lemma 4.1 (b).

Let us now extend the results of 4.6 to a slightly larger class of tori, the tori of the form S_M/M, where M/K is a finite extension.

Proposition 4.9. *Fix an algebraic closure $\overline{K}$ of K. Let $M \subset \overline{K}$ be a finite extension of K. Denote by F' the compositum FM in $\overline{K}$. Let S/K be the quotient torus $(R_{F/K}\mathbb{G}_{m,F})/\mathbb{G}_{m,K}$. Let $V := (R_{F'/M}\mathbb{G}_{m,F'})/\mathbb{G}_{m,M}$. Let $\mathscr{S}'/\mathcal{O}_M$ and $\mathscr{V}/\mathcal{O}_M$ be the Néron models of S_M and V.*

(a) *Assume that either F/K or M/K is Galois. Let $r := [F:K][M:K]/[F':K]$. There is a natural exact sequence of group schemes*

$$0 \to \mathbb{G}_{m,M}^{r-1} \to S_M \to V^r \to 0.$$

(b) *The map $S_M \to V^r$ in the above exact sequence induces a homomorphism $\Phi(S_M)_{\mathrm{tors}} \to \Phi(V)^r$ which, when composed with any projection to $\Phi(V)$, is an isomorphism*

$$\Phi(S_M)_{\mathrm{tors}} \simeq \Phi(V) = \mathbb{Z}/[F':M]\mathbb{Z}.$$

(c) *Let q be a divisor of $[F':M]$. An element φ of $\Phi(V)$ of order q lifts to an element of $\mathscr{V}_k$ of order q if and only if a preimage of order q of φ in $\Phi(S_M)$ lifts to an element of $\mathscr{S}'_k$ of order q.*

(d) *Assume that F/K is tamely ramified. Then S_M/M has split reduction.*

(e) *Assume that M/K is tamely ramified. If either $[M:K] \geqq [F:K]$ or S has split reduction, then S_M/M has split reduction.*

Proof. Consider first the following general argument. Let $D = \bigoplus_{1 \leqq i \leqq r} F_i$ be a direct sum of finite separable M-algebras with F_i a domain for all i. Let U be the quotient torus $R_{D/M}(\mathbb{G}_{m,D})/\mathbb{G}_{m,M}$. The scheme $\operatorname{Spec} D$ is the disjoint union of the $\operatorname{Spec} F_i$'s. Thus

$$R_{D/M}(\mathbb{G}_{m,D}) = \prod_{1 \leqq i \leqq r} R_{F_i/M}(\mathbb{G}_{m,F_i}).$$

Let $S_i = (R_{F_i/M}\mathbb{G}_{m,F_i})/\mathbb{G}_{m,M}$. We have a canonical commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_{m,M} & \longrightarrow & R_{D/M}(\mathbb{G}_{m,D}) & \longrightarrow & U & \longrightarrow & 0 \\ & & \Delta\big\downarrow & & \big\| & & \big\downarrow & & \\ 0 & \longrightarrow & \mathbb{G}_{m,M}^r & \longrightarrow & R_{D/M}(\mathbb{G}_{m,D}) & \longrightarrow & \prod_{1 \leqq i \leqq r} S_i & \longrightarrow & 0, \end{array} \tag{17}$$

where Δ is the diagonal morphism. This leads to an exact sequence

$$0 \to \mathbb{G}_{m,M}^{r-1} \to U \to \prod_{1 \leqq i \leqq r} S_i \to 0, \tag{18}$$

where the first term of the sequence is identified with $\operatorname{Coker}(\Delta)$. To prove (a), let $D := F \otimes_K M$. Then $S_M = U$. Our hypothesis on F/K and M/K insures that $r = [F:K][M:K]/[F':K]$ and that $F_i \simeq F'$ for all $i \leqq r$. So $S_i \simeq V$ and part (a) is proved.

To prove (b), we first note that it follows from Proposition 4.2 that the complexes of component groups associated to both horizontal lines in (17) and to (18) are exact.

Let $n_i := [F_i : M]$, so that $\Phi(S_i)$ can be identified with $\mathbb{Z}/n_i\mathbb{Z}$. Let us also identify $\Phi\big(R_{D/M}(\mathbb{G}_{m,D})\big)$ with $\mathbb{Z}^r$. Then the exact sequence of groups of components associated with the second line in (17) becomes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Phi(\mathbb{G}_{m,M}^r) & \longrightarrow & \Phi\big(R_{D/M}(\mathbb{G}_{m,D})\big) & \longrightarrow & \prod_{1 \leqq i \leqq r} \Phi(S_i) & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \\ 0 & \longrightarrow & \mathbb{Z}^r & \xrightarrow{\alpha} & \mathbb{Z}^r & \xrightarrow{\beta} & \prod_{1 \leqq i \leqq r} \mathbb{Z}/n_i\mathbb{Z} & \longrightarrow & 0, \end{array}$$

where α is defined by $\alpha(a_1, \ldots, a_r) := (a_1 n_1, \ldots, a_r n_r)$ and β is the canonical surjection. Let $n_0 := \gcd\{n_i\}_{1 \leqq i \leqq r}$. One checks easily that the map $\Phi(U)_{\mathrm{tors}} \to \prod_i \Phi(S_i)$ can be identified with the canonical map $\mathbb{Z}/n_0\mathbb{Z} \to \prod_{1 \leqq i \leqq r} \mathbb{Z}/n_i\mathbb{Z}$. Now take again $D := F \otimes_K M$ and we get part (b).

(c) Let $\mathscr{G}_m/\mathcal{O}_M$ be the Néron model of $\mathbb{G}_{m,M}/M$. Consider the commutative diagram

$$\begin{array}{ccccc} (\mathscr{G}_{m,k}^0)^{r-1} & \longrightarrow & (\mathscr{S}_k')^0 & \longrightarrow & (\mathscr{V}_k^0)^r \\ \downarrow & & \downarrow & & \downarrow \\ \mathscr{G}_{m,k}^{r-1} & \longrightarrow & \mathscr{S}_k' & \longrightarrow & \mathscr{V}_k^r \\ \downarrow & & \downarrow & & \downarrow \\ \Phi(\mathbb{G}_{m,M})^{r-1} & \longrightarrow & \Phi(S_M) & \longrightarrow & \Phi(V)^r. \end{array}$$

The three columns in the diagram are exact. Proposition 4.2 shows that the three rows are also exact. Part (c) is then easily derived from the fact that $(\mathscr{G}_{m,k}^0)^{r-1}$ is $[F' : M]$-divisible.

(d) Assume that F/K is tame and, hence, Galois. Then $[F' : M]$ divides $[F : K]$. It follows from (b) that the p-part of $\Phi(S_M)$ is trivial and, thus, S_M has split reduction (4.4 and 1.5).

(e) Assume that M/K is tame and, hence, Galois. Let $n := [F : K]$ and $m := [M : K]$. Using (d), we may assume that $p|n$. To prove (e), it is sufficient, according to (c), to show that V/M has split reduction.

Recall that t denotes an uniformizing element of F. Let $m_1 := [F' : F]$, which divides m and let $n_1 := [F' : M]$, so that $nm_1 = n_1 m$. Then $t_{F'} := t^{1/m_1}$ and $\pi_M := \pi^{1/m}$ are uniformizing elements of F' and M, respectively. Using 4.7, we find that V has split reduction if and only if $t_{F'}^{n_1}\pi_M^{-1}$ is an n_1-th power in $\mathcal{O}_{F'}/\pi_M\mathcal{O}_{F'}$. Clearly, $t_{F'}^{n_1}\pi_M^{-1} = (t^n\pi^{-1})^{1/m}$. Since the formal group $1 + t_{F'}\mathcal{O}_{F'}$ is q-divisible for any integer q prime to p, we find that so is the group $(\mathcal{O}_{F'}/\pi_M\mathcal{O}_{F'})^*$. It follows that V has split reduction if and only if $t^n\pi^{-1}$ is an n-th power in $(\mathcal{O}_{F'}/\pi_M\mathcal{O}_{F'})^*$ or, equivalently, if

$$t^n\pi^{-1} \in \mathcal{O}_{F'}^{*n}(1 + \pi_M\mathcal{O}_{F'}) = \mathcal{O}_{F'}^{*n}(1 + t_{F'}^{n_1}\mathcal{O}_{F'}).$$

Note now that $t^n\pi^{-1} \in \mathcal{O}_K^*(1 + t\mathcal{O}_F) = \mathcal{O}_K^{*n}(1 + t\mathcal{O}_F)$. If $m \geqq n$, then $m_1 \geqq n_1$ and

$$t^n\pi^{-1} \in \mathcal{O}_K^{*n}(1 + t\mathcal{O}_F) \subseteqq \mathcal{O}_{F'}^{*n}(1 + t_{F'}^{m_1}\mathcal{O}_{F'}) \subseteqq \mathcal{O}_{F'}^{*n}(1 + t_{F'}^{n_1}\mathcal{O}_{F'}).$$

Hence, V has split reduction. Assume now that S has split reduction. Then 4.7 implies that $t^n\pi^{-1} \in \mathcal{O}_F^{*n}(1 + \pi\mathcal{O}_F)$. Thus $t^n\pi^{-1} \in \mathcal{O}_{F'}^{*n}(1 + t_{F'}^{mm_1}\mathcal{O}_{F'})$ and V also has split reduction.

Corollary 4.10. *Let M/K be a finite Galois extension. Then S_M has totally not split reduction if and only if* $1 \leqq \delta(S_M) \leqq \dim S_M$.

Proof. Proposition 4.9 (a) implies that $\delta(S_M) = r\delta(V)$ and

$$\dim S_M = r \dim V + (r - 1).$$

So $1 \leqq \delta(S_M) \leqq \dim S_M$ is equivalent to $1 \leqq \delta(V) \leqq \dim V$. Theorem 4.6 applied to V implies that $1 \leqq \delta(V) \leqq \dim V$ is equivalent to V having totally not split reduction. We conclude the proof using Proposition 4.9 (c).

Corollary 4.11. *Let S be the quotient torus $(R_{F/K}\mathbb{G}_{m,F})/\mathbb{G}_{m,K}$. Then S_M/M has split reduction over any tame extension M/K such that $[M : K] \geqq \dim S + 1$.*

Proof. Follows from 4.9 (e).

Remark 4.12. Let S/K be as in 4.6. The identity component $\mathscr{S}_k^0$ of $\mathscr{S}_k$ can be explicitly described. Let W_r/k denote the Witt group of dimension r. The main argument in the proof of Théorème 2.1 in [K-S] shows that

$$\mathscr{S}_k^0 = \prod_{1 \leqq i \leqq n-1,\, (i,p)=1} W_{r_i},$$

where $r_i := \min\{r | p^r \geqq n/i\}$. It is interesting to note that the structure of $\mathscr{S}_k^0$ depends only on $[F : K]$, while that of $\mathscr{S}_k$ depends strongly on the extension F/K itself.

Remark 4.13. Consider the torus S as in Theorem 4.6, with F/K defined by the equation $t^{p^2} + \pi t^p + \pi = 0$. By construction, the group $\Phi(S)$ is cyclic of order p^2. The reduction of S is not totally not split but it is not split either. Note that $\delta(S) = v_F(p) + p^2 + p - 1$ when $v_F(p)$ is large. Thus $\delta(S)$ is not bounded by a constant depending only on the dimension of S, even though the reduction of S is not split.

Remark 4.14. The class of tori for which a statement such as Theorem 4.6 holds can be slightly enlarged as follows. Indeed, there are situations where the quotient torus S/K of 4.6 is isogenous, but not isomorphic, to other tori S'/K. Hence, it is natural to ask about the splitting property of such tori S'. It turns out that in some situations, it is always possible to find an isogeny between S and S' of degree prime to p. Thus, Proposition 1.11 can be applied and S/K has split reduction if and only if S'/K has split reduction. We thank Bas Edixhoven for the proof of the following lemma.

Lemma 4.15. *Let T/K be a torus with* $\mathrm{Gal}(\overline{K}/K)$ *acting on $X(T)$ through a finite cyclic group $\langle\sigma\rangle$. Assume that the minimal polynomial $f(x)$ of the image of σ in* $\mathrm{Aut}(X(T))$ *is irreducible and equal to the characteristic polynomial. Let T'/K be any torus isogenous* *over K to T. Then there exists an isogeny (defined over K) between T and T' of degree prime to p.*

Proof. Let R denote the ring $\mathbb{Z}[x]/(f)$. Since f is a cyclotomic polynomial, we find that R is a Dedekind domain. The Galois action endows $X(T)$ with the structure of a locally free R-module of rank 1. The set of isomorphism classes of such modules is in bijection with the ideal class group $\mathscr{C}(R)$ of R ([New], III.13). The group $\mathscr{C}(R)$ is generated by finitely many maximal ideals $M_1, \dots, M_r$ of R. Let $(\ell_i) := M_i \cap \mathbb{Z}$. The set of generators can always be chosen such that $\ell_i \neq p$, for all $i = 1, \dots, r$. Two tori T and T' isogenous over K correspond to two ideal classes of R. Two such ideal classes become equal in the class group of $R[1/\ell_1 \cdots \ell_r]$. Hence, there exists an isogeny over K between T and T' of degree $\ell_1^{a_1} \cdots \ell_r^{a_r}$ for some $a_i \in \mathbb{N}$.

The above lemma applies for instance to the case where L/K is a Galois extension of degree p and the class group of the cyclotomic field $\mathbb{Q}(\xi_p)$ is not trivial. Then there exists a torus T'/K, not isomorphic to $T := R^1_{L/K}\mathbb{G}_m$, and such that $T'_L \cong (\mathbb{G}_m^{p-1})_L$ and $\Phi(T') \cong \mathbb{Z}/p\mathbb{Z}$. Two such tori are isogenous through an isogeny of degree prime to p and have thus the same splitting properties.

Remark 4.16. Let T/K be a torus. It is natural to ask whether there is a relationship between the type of splitting of the Néron model of T and the type of splitting of the Néron model of the dual of T. We give an example below of a torus T whose Néron model $\mathscr{T}$ is split and whose dual S has a non-split Néron model $\mathscr{S}$. Let $p = 3$. Consider the norm torus $T := R^1_{F/K}\mathbb{G}_{m,F}$, defined by a non-Galois cubic extension F/K with $3 \leqq v_F(\mathscr{D}_{F/K}) \leqq 4$. Let $S := T^\wedge$. Then $\mathscr{S}$ is not split (4.1 and 4.6) while $\mathscr{T}$ is split because $\Phi(T) = 0$, as shown in our next proposition.

Proposition 4.17[1]**.** *Let F/K be a finite separable extension with Galois closure L/K, and $F \neq K$. Let $\Delta := \mathrm{Gal}(L/F)$ and $\Gamma := \mathrm{Gal}(L/K)$. Let $T := R^1_{F/K}\mathbb{G}_{m,F}$ be the norm torus with Néron model $\mathscr{T}/\mathcal{O}_K$. Then*:

(1) *$\mathscr{T}_k^0$ is unipotent and $\Phi(T)$ is a finite group killed by $[L : K]$, canonically isomorphic to the cokernel of the map $\Delta^{\mathrm{ab}} \to \Gamma^{\mathrm{ab}}$ (where $\Gamma^{\mathrm{ab}} := \Gamma/[\Gamma, \Gamma]$).*

(2) *If Γ is abelian, then $\Phi(T) \cong \Gamma$.*

(3) *Assume that Γ is not abelian and is the semi-direct product of Δ and a normal cyclic subgroup H of prime order. Assume that Δ is abelian, and that $\gcd(|\Delta|, |H|) = 1$. Then $\Phi(T) = \{0\}$.*

(4) *Let S denote the dual torus of T. Then S is isomorphic to T if and only if F/K is a cyclic extension.*

Proof. Denote $N = X(T)$. Let us consider the long exact cohomology sequence associated to (9):

[1] We thank the referee and X. Xarles for providing us with sharpened versions of the original statement of this proposition.

$$0 \to \mathbb{Z} \to (\mathbb{Z}[\Gamma/\Delta])^{\Gamma} \to N^{\Gamma} \to H^1(\Gamma, \mathbb{Z})$$
$$\to H^1(\Gamma, \mathbb{Z}[\Gamma/\Delta]) \to H^1(\Gamma, N) \to H^2(\Gamma, \mathbb{Z}) \xrightarrow{h} H^2(\Gamma, \mathbb{Z}[\Gamma/\Delta]).$$

Recall that since $\mathbb{Z}$ is endowed with the trivial action, $H^1(\Gamma, \mathbb{Z}) = \mathrm{Hom}(\Gamma, \mathbb{Z}) = \{0\}$. On the other hand, one checks that $(\mathbb{Z}[\Gamma/\Delta])^{\Gamma} = (\sum_i \delta_i)\mathbb{Z}$. Thus we find that $N^{\Gamma} = \{0\}$. It follows from [N-X], Theorem 1.3, that $\mathscr{T}_k^0$ is unipotent. It follows then from [Xar], Corollary 2.19, that $\Phi(T)$ is finite and isomorphic to $\mathrm{Hom}_{\mathbb{Z}}(H^1(\Gamma, N), \mathbb{Q}/\mathbb{Z})$. Then $|\Gamma| = [L : K]$ kills $H^1(\Gamma, N)$ ([Ser], VII, §7, Prop. 6).

Eckmann-Shapiro's lemma provides a canonical isomorphism

$$H^i(\Gamma, \mathbb{Z}[\Gamma/\Delta]) \simeq H^i(\Delta, \mathbb{Z})$$

for all $i \geqq 1$. So $H^1(\Gamma, \mathbb{Z}[\Gamma/\Delta]) \simeq H^1(\Delta, \mathbb{Z}) = 0$. Thus $H^1(\Gamma, N)$ is isomorphic to the kernel of h. By the same lemma, $H^1(\Gamma, N)$ is isomorphic to the kernel of $H^2(\Gamma, \mathbb{Z}) \xrightarrow{\mathrm{Res}} H^2(\Delta, \mathbb{Z})$. Recall that when $i > 0$, $H^i(\Gamma, \mathbb{Q}) = \{0\}$ since multiplication by $|\Gamma|$ is an isomorphism on $\mathbb{Q}$ and $H^i(\Gamma, \mathbb{Q})$ is killed by $|\Gamma|$ ([Ser], loc.cit.). Thus the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

induces an isomorphism $H^1(\Gamma, \mathbb{Q}/\mathbb{Z}) \to H^2(\Gamma, \mathbb{Z})$ for any finite group Γ. Hence, $H^1(\Gamma, N)$ is isomorphic to the kernel of $H^1(\Gamma, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{Res}} H^1(\Delta, \mathbb{Q}/\mathbb{Z})$. Or equivalently to the kernel of $\mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\Delta, \mathbb{Q}/\mathbb{Z})$. Dualizing this last map finishes the proof of Part (1). To prove (2), observe that when Γ is abelian, then Δ is trivial since F/K is already Galois.

To prove (3), note that since $\Gamma/H \simeq \Delta$ is commutative, $|H|$ is prime and Γ is not commutative, we have $[\Gamma, \Gamma] = H$. Thus $\mathrm{Hom}(\Gamma/H, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z})$ is an isomorphism. By assumption, the composition $\Delta \to \Gamma \to \Gamma/H$ is an isomorphism. This implies that $\mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\Delta, \mathbb{Q}/\mathbb{Z})$ is an isomorphism, so that $\Delta^{\mathrm{ab}} \to \Gamma^{\mathrm{ab}}$ has trivial cokernel.

To prove (4), we need only to show, in view of 4.1 (b), that if S and T are isomorphic, then F/K is cyclic. From 4.4 (b) and part (1), we know that

$$|\Phi(S)| = [F : K] = |\Gamma|/|\Delta| = |\Gamma^{\mathrm{ab}}|/|\Delta^{\mathrm{ab}}|.$$

Thus, $[\Gamma, \Gamma] = [\Delta, \Delta]$, which implies that Δ is a normal subgroup. Hence, Δ is trivial, and Γ must be cyclic of order n.

Remark 4.18. Consider a finite separable extension F/K. The torsion subgroup of $S(K)$, where $S = R_{F/K}(\mathbb{G}_{m,F})/\mathbb{G}_{m,K}$, is easy to compute. Indeed, a point in $S(K)$ has order $m > 1$ if and only if there exists $y \in F^* \backslash K^*$ such that $y^m \in K^*$ and $y^d \notin K^*$ for all proper divisors d of m. The reduction of such a torsion point can also be determined. For instance, when $[F : K] = p$, we find that $S(K)_{\mathrm{tors}}$ is trivial or is generated by an element Q of order p. When $S(K)_{\mathrm{tors}}$ is not trivial, Q reduces to a generator of $\Phi(S)$ if $F = K(\alpha)$ with $\alpha^p \in \mathcal{O}_K$ and $v(\alpha^p)$ prime to p, and reduces to the identity in $\Phi(S)$ if $F = K(\alpha)$ with $\alpha^p \in \mathcal{O}_K^*$. In the latter case, Q may reduce to the identity element of $\mathcal{S}_k$. This is the case when $\alpha^p = 1 + \pi^d u$, with d large enough and $u \in \mathcal{O}_K^*$.

5. Explicit Néron models

Let L/K be a cyclic extension of degree p. Let $T = R^1_{L/K}\mathbb{G}_m$ be the norm torus. Since the torus T can be given by an explicit equation, one may hope that its Néron model may also be described in some explicit way. We show below in Proposition 5.6 that, indeed, the Néron model $\mathcal{T}/\mathcal{O}_K$ of T/K can be described by a single equation, and that, surprisingly, this equation can be written down in a simple way. Using this equation, we give a direct proof that $\mathcal{T}_k^0 \cong \mathbb{G}_a^{p-1}$ (4.12), and that $\mathcal{T}_k$ is not split if and only if the Swan conductor $\delta(T)$ of T is equal to $p-1$ (4.8).

To construct the Néron model $\mathcal{T}/\mathcal{O}_K$, we first construct explicitly a smooth model $\mathcal{U}$ of T (not necessarily a group scheme) having the properties of Proposition 5.1 below. It follows then from 5.1 that $\mathcal{U}$ is the Néron model of T.

Proposition 5.1. *Let $\mathcal{O}_K$ be a strictly Henselian discrete valuation ring. Let G be a smooth algebraic variety over K admitting a Néron model of finite type $\mathcal{G}$ over $\mathcal{O}_K$. Let $\mathcal{G}'$ be a smooth model of G over $\mathcal{O}_K$ such that*:

(a) *The canonical map $\mathcal{G}'(\mathcal{O}_K) \to G(K)$ is surjective.*

(b) *The number of connected components of $\mathcal{G}'_k$ is less than or equal to the number of components of $\mathcal{G}_k$.*

Then $\mathcal{G}'$ is isomorphic to $\mathcal{G}$.

Proof. By the universal property of the Néron model, the isomorphism $\mathcal{G}'_K \to \mathcal{G}_K$ extends to a birational morphism $f\colon \mathcal{G}' \to \mathcal{G}$. Since $\mathcal{G}(\mathcal{O}_K) \to \mathcal{G}_k(k)$ is surjective, property (a) implies that $f_k\colon \mathcal{G}'_k \to \mathcal{G}_k$ is surjective. For any generic point ξ of $\mathcal{G}_k$, there exists $\eta \in f^{-1}(\xi)$. Since $\mathcal{G}$ is normal, f is an isomorphism at η. So property (b) and the surjectivity of f imply that f is an isomorphism at any one-codimensional point of $\mathcal{G}'$. According to the Theorem of van der Waerden ($\mathcal{G}$ is regular), the exceptional locus of the birational morphism f if either empty or pure of codimension 1 (see, e.g., [Mum], III.9, Proposition 1). In our case, it must be empty. Hence, f is an isomorphism.

5.2. Let L/K be any extension of degree p. A uniformizing element t of L satisfies an Eisenstein equation

$$t^p - s_1 t^{p-1} + s_2 t^{p-2} + \cdots + (-1)^p s_p = 0 \tag{19}$$

with $s_i \in \pi\mathcal{O}_K$ and $v(s_p) = 1$. Set $s_0 = p$ so that the different of the extension L/K is given by

$$v_L(\mathcal{D}_{L/K}) = \min_{0 \leqq i \leqq p-1} \{pv(s_i) + p - 1 - i\}$$

(see, e.g., [Ser], p. 67). Note that when L/K is Galois, then $v_L(\mathcal{D}_{L/K}) = (p-1)v_L(\sigma(t) - t)$, where σ is any generator of $\mathrm{Gal}(L/K)$ ([Ser], p. 72). Therefore, $v_L(\mathcal{D}_{L/K})$ is divisible by $p-1$ in this case. Let $0 \leqq m \leqq p-1$ be the unique integer such that $v_L(\mathscr{D}_{L/K}) = pv(s_m) + p - 1 - m$. Let

$$r := \big(v(s_m) - m\big)/(p-1).$$

Recall that (4.5) the Swan conductor $\delta(T)$ of T is

$$\delta(T) = v_L(\mathscr{D}_{L/K}) - (p-1) = (p-1)(pr+m).$$

Let T be the norm torus $R^1_{L/K}\mathbb{G}_{m,L}$. Since $\{1, t, \dots, t^{p-1}\}$ is a basis of L/K, T is given by

$$T = \operatorname{Spec} \frac{K[x_0, \dots, x_{p-1}]}{N_{L/K}(1 + x_0 + x_1 t + \cdots + x_{p-1}t^{p-1}) - 1}.$$

Lemma 5.3. *Let $A = \mathbb{Z}[s_1, \dots, s_p, y_0, \dots, y_{p-1}]$ be the ring of polynomials in $2p$ variables. Let*

$$B = A[u]/\big(u^p - s_1 u^{p-1} + \cdots + (-1)^p s_p\big).$$

Let t be the image of u in B, and denote by $N \in A$ the norm $N_{B/A}(y_0 + y_1 t + \cdots + y_{p-1}t^{p-1})$. Then the following properties hold:

(a) *N is homogeneous of degree p in the variables $y_0, \dots, y_{p-1}$.*

(b) *Let $0 \leqq j \leqq p-1$. Then the coefficient of y_j^p in N is s_p^j and, if $j \neq 0$, the coefficient of $y_0^{p-1}y_j$ is $\operatorname{Tr}_{B/A}(t^j)$.*

(c) *The coefficient of $y_0^{\lambda_0} \cdots y_{p-1}^{\lambda_{p-1}}$ in N belongs to the ideal $(ps_p, s_1, \dots, s_{p-1})$ if at least two of the λ_i's are not zero.*

Proof. (a) is clear because $N_{B/A}(ab) = a^p N_{B/A}(b)$ for any $a \in A$ and for any $b \in B$.

(b) It is enough to compute $N_{B/A}(y_0 + t^j y_j)$. Let

$$f(Z) := Z^p - s_{j,1}Z^{p-1} + \cdots + (-1)^p s_{j,p}$$

be the irreducible polynomial of t^j over A $(p-1 \geqq j \geqq 1)$. Then

$$\begin{aligned} N_{B/A}(y_0 + t^j y_j) &= y_j^p N_{B/A}(y_0/y_j + t^j) \\ &= y_j^p (-1)^p f(-y_0/y_j) \\ &= y_0^p + s_{j,1}y_0^{p-1}y_j + \cdots + s_{j,p}y_j^p. \end{aligned}$$

Since $s_{j,1} = \operatorname{Tr}_{B/A}(t^j)$ and $s_{j,p} = N_{B/A}(t^j) = s_p^j$, (b) follows.

(c) Let $\mathfrak{p}$ be the ideal of A generated by $(p, s_1, \dots, s_{p-1})$. Then the image of N in $B/\mathfrak{p}B$ is the norm of $y_0 + y_1 t + \cdots + y_{p-1}t^{p-1}$ in the inseparable extension

$A/\mathfrak{p} \to B/\mathfrak{p}B = A/\mathfrak{p}[u]/(u^p - s_p)$. Recall that in an inseparable extension of degree p, Norm $(z) = z^p$ for all z. Thus

$$N \equiv y_0^p + s_p y_1^p + \cdots + s_p^{p-1} y_{p-1}^p \bmod (p, s_1, \ldots, s_{p-1}).$$

We also have $N \equiv y_0^p \bmod (s_1, \ldots, s_{p-1}, s_p)$. Since in $\mathbb{Z}[s_p]$, $(s_p) \cap (p) = (ps_p)$, the two congruence relations above imply (c).

Lemma 5.4. *Keep the notation introduced in* 5.2. *Let*

$$b = (1 + a_0) + a_1 t + \cdots + a_{p-1} t^{p-1} \in L, \quad a_i \in K$$

be such that $N_{L/K}(b) = 1$. *Then*

$$v(a_j) \geqq \begin{cases} r + 1 & \text{if } m > 0 \text{ and } 0 \leqq j \leqq m - 1, \\ r & \text{if } m \leqq j \leqq p - 1. \end{cases}$$

Proof. Since $0 = v_L(N_{L/K}(b)) = pv_L(b)$, we have $b \in \mathcal{O}_L$. Hence, $a_j \in \mathcal{O}_K$ for all j. According to Lemma 5.3, we have $N_{L/K}(b) = 1$, with

$$N_{L/K}(b) = (1 + a_0)^p + s_p a_1^p + \cdots + s_p^{p-1} a_{p-1}^p + \text{an expression in } IJ,$$

where $I = (ps_p, s_1, \ldots, s_{p-1})$ and $J := (a_1, \ldots, a_{p-1})$. Thus

$$\begin{aligned} (20) \qquad & v\big((1 + a_0)^p - 1 + s_p a_1^p + \cdots + s_p^{p-1} a_{p-1}^p\big) \\ & \geqq \min_{1 \leqq i \leqq p-1} \{v(s_i), v(p) + 1\} + \min_{1 \leqq j \leqq p-1} \{v(a_j)\}. \end{aligned}$$

Assume that $m \neq 0$. Then, since $v(s_i) \geqq v(s_m)$ for all $0 \leqq i \leqq p - 1$, we get

$$v\big((1 + a_0)^p - 1 + s_p a_1^p + \cdots + s_p^{p-1} a_{p-1}^p\big) \geqq v(s_m) + \min_{1 \leqq j \leqq p-1} \{v(a_j)\}.$$

If $m = 0$, then $v(s_i) \geqq v(s_0) + 1$ for all $i \geqq 1$, and we have a stronger inequality

$$(21)\ v\big((1 + a_0)^p - 1 + s_p a_1^p + \cdots + s_p^{p-1} a_{p-1}^p\big) \geqq v(s_0) + 1 + \min_{1 \leqq j \leqq p-1} \{v(a_j)\}.$$

Let $1 \leqq j_0 \leqq p - 1$ be such that $v(a_{j_0}) = \min_{1 \leqq j \leqq p-1} \{v(a_j)\}$. Let $e' := v(p)/(p - 1)$. Assume first that $v(a_0) < e'$. Then $v\big((1 + a_0)^p - 1\big) = pv(a_0)$, and the inequality (20) becomes

$$(22) \qquad \min_{0 \leqq j \leqq p-1} \{pv(a_j) + j\} \geqq v(s_m) + v(a_{j_0})$$

(recall that $v(s_p) = 1$). In particular, $pv(a_{j_0}) + j_0 \geqq v(s_m) + v(a_{j_0})$ and, thus,

$$v(a_{j_0}) \geqq r + \frac{m - j_0}{p - 1}.$$

Substituing this inequality in (22) and using the fact that $j_0 \leqq p-1$ implies that, for all $j \leqq p-1$,

$$v(a_j) \geqq r + \frac{pm - (p-1)(j+1)}{p(p-1)}.$$

This last inequality implies the statement of the lemma except when $m = 0$ and $j = p-1$. In this case, we remark that one can substitute $v(s_m)$ by $v(s_m)+1$ in inequality (22) because of (21), thus $v(a_{p-1}) > r-1$ and $v(a_{p-1}) \geqq r$.

Now assume that $v(a_0) \geqq e'$. Then the lemma is already true for $j = 0$ because $e' \geqq r + m/p$. The inequality (20) implies that

$$\min_{1 \leqq j \leqq p-1} \{pv(a_j) + j\} \geqq v(s_m) + v(a_{j_0}).$$

If $v(s_m) + v(a_{j_0}) < pe'$, then the proof of the lemma is the same as in the case $v(a_0) < e'$. Assume now $v(s_m) + v(a_{j_0}) \geqq pe'$. Let $1 \leqq j \leqq p-1$. Then $pv(a_j) + j \geqq pe' \geqq pr + m$. Thus $p\big(v(a_j) - r\big) \geqq m - j$. So $v(a_j) > r$ if $j < m$ and $v(a_j) \geqq r$ if $m \leqq j \leqq p-1$. Hence, the lemma is proved.

Let $\pi := s_p$. The element π is a uniformizing element of K. Make the change of variables

$$x_j = \begin{cases} \pi^{r+1} X_j & \text{if } m > 0 \text{ and } 0 \leqq j \leqq m-1, \\ \pi^r X_j & \text{if } m \leqq j \leqq p-1. \end{cases}$$

We have a new equation $F(X_0, \dots, X_{p-1}) = 0$ for the torus T, with

$$F(X_0, \dots, X_{p-1}) = N_{L/K}\left(1 + \sum_{0 \leqq j \leqq m-1} \pi^{r+1} t^j X_j + \sum_{m \leqq j \leqq p-1} \pi^r t^j X_j\right) - 1.$$

Lemma 5.5. *With the above notation,* $F(X_0, \dots, X_{p-1}) \in \pi^{pr+m} \mathcal{O}_K[X_0, \dots, X_{p-1}]$ *and*

$$F(X_0, \dots, X_{p-1}) \pi^{-(pr+m)} \equiv X_m^p + uX_m \mod [\pi]$$

for some $u \in \mathcal{O}_K^*$.

Proof. Recall that for any $i \leqq p-1$, one has $v(s_i) \geqq v(s_m) = (p-1)r + m$, and $v(ps_p) = v(s_0) + 1 > (p-1)r + m$. Let $1 \leqq j \leqq p-1$. Let $\pi_j := \mathrm{Tr}_{L/K}(t^j)$. Then $\pi_1 - s_1 = 0$, and

$$\pi_j + (-1)^j j s_j = \sum_{1 \leqq \ell \leqq j-1} (-1)^{\ell+1} s_\ell \pi_{j-\ell}$$

(see for instance [BA], IV, §6, formula (26)). Thus, we see by induction that $v(\pi_j) \geqq v(s_m)$, and that equality holds if and only if $v(s_j) = v(s_m)$. We assume from now on that $m \geqq 1$. The case where $m = 0$ is similar and is left to the reader. Apply Lemma 5.3 with $y_0 = 1 + \pi^r X_0$, and $y_j = x_j$, $j > 0$. It follows from Lemma 5.3 and from the computation of the valuations of the coefficients of $(1+\pi^{r+1}X_0)^p - 1$, that the coefficients of $F(X_0, \dots, X_{p-1})$ all have valuation at least $pr+m$, and those that can possibly reach the minimum are the coefficients of the monomials in $s_p^m(\pi^r X_m)^p$ and $\pi_j y_j y_0^{p-1}$, $1 \leqq j \leqq p-1$. But note now that if $j \neq m$ and $v(\pi_j) = v(s_m)$, then $v(s_j) = v(s_m)$ and, thus, by definition of m, we must have $j < m$. Hence, for such a j, $x_j = \pi^{r+1}X_j$. It follows that the only monomials of F with coefficients of valuation $pr+m$ are $s_p^m \pi^r X_m^p$ and $\mathrm{Tr}_{L/K}(t^m)\pi^r X_m$ (appearing as a monomial of $\mathrm{Tr}_{L/K}(t^m)\pi^r X_m y_0^{p-1}$). Since $s_p = \pi$ by hypothesis, the lemma is proved.

Proposition 5.6. *Let L/K be a cyclic extension of degree p. Let $T = R^1_{L/K}\mathbb{G}_{m,L}$ be the norm torus. Let $G(X_0, \dots, X_{p-1}) := F(X_0, \dots, X_{p-1})\pi^{-(pr+m)}$. Let*

$$\mathscr{U} := \mathrm{Spec}\,\mathcal{O}_K[X_0, \dots, X_{p-1}]/(G).$$

Then $\mathscr{U}/\mathcal{O}_K$ is the Néron model of T/K.

Proof. Since Néron models commute with étale base change, we may assume that K is strictly henselian. Keep the notation of Lemmas 5.4 and 5.5. It is easy to check that $\mathscr{U}$ is a smooth model of T over $\mathcal{O}_K$ and that $\mathscr{U}_k$ has p connected components. Lemma 5.4 implies that the canonical map $\mathscr{U}(\mathcal{O}_K) \to \mathscr{U}_K(K)$ is surjective. Thus, Proposition 5.1 shows that $\mathscr{U}$ is isomorphic to $\mathscr{T}$.

Corollary 5.7. *Let L/K be a cyclic extension of degree p. Let $T = R^1_{L/K}\mathbb{G}_{m,L}$ be the norm torus. Let $\mathscr{T}$ be the Néron model of T over $\mathcal{O}_K$. Then $\mathscr{T}_k^0 \cong \mathbb{G}_a^{p-1}$, and $\mathscr{T}_k$ is (totally) not split if and only if the conductor $\delta(T)$ of T is equal to $p-1$.*

Proof. A proof of this statement without the use of an explicit equation is found in 4.12 and 4.8. Let us now give a proof based on the explicit description of the Néron model of T. Let $\mathscr{U} := \mathrm{Spec}\,\mathcal{O}_K[X_0, \dots, X_{p-1}]/(G)$. Our previous proposition shows that $\mathscr{U}$ is isomorphic to $\mathscr{T}$. The identity element of T is $X_0 = \cdots = X_{p-1} = 0$. Using Lemma 5.5, we see that the identity component $\mathscr{T}_k^0$ of $\mathscr{T}_k$ is the closed subset $V(\pi, X_m)$. Let $Q \in T(K)$. Let $\tilde{Q} \in \mathscr{T}_k$ be its specialization in $\mathscr{T}_k$. The point Q can be represented by an element

$$q = 1 + \sum_{0 \leqq j \leqq m-1} \pi^{r+1} t^j b_j + \sum_{m \leqq j \leqq p-1} \pi^r t^j b_j \in L$$

with $b_j \in \mathcal{O}_K$ and $N_{L/K}(q) = 1$. Write

$$w := q - 1 = \pi^r t^m (b_m + t\alpha), \quad \text{for some } \alpha \in \mathcal{O}_L.$$

Note that the condition $v(b_m) = 0$ is equivalent to $\tilde{Q} \notin \mathscr{T}_k^0$. The point pQ is represented by q^p. Write

$$q^p = 1 + \sum_{0 \leqq j \leqq m-1} \pi^{r+1} t^j c_j + \sum_{m \leqq j \leqq p-1} \pi^r t^j c_j$$

with $c_j \in \mathcal{O}_K$. It follows that:

$$\sum_{0 \leqq j \leqq m-1} \pi^{r+1} t^j c_j + \sum_{m \leqq j \leqq p-1} \pi^r t^j c_j = w^p + pw(1 + w\beta), \quad \text{for some } \beta \in \mathcal{O}_L.$$

Since the coefficients c_j belong to $\mathcal{O}_K$, we find that the v_L-valuation of the left hand side is the minimum of the v_L-valuations of each summand. Recall that the conditions $r = 0$ and $m = 1$ are equivalent to $\delta(T) = p - 1$. Comparing the v_L-valuations of both sides in the above equation, we easily see that, if $r = 0$, $m = 1$, and $v(b_m) = 0$, then $v(c_0) = 0$. So $p\tilde{Q} \in \mathcal{T}_k^0$ is not the identity element. Thus, $\mathcal{T}_k$ is not split in this case. The reader will check that, if either $\delta(T) > p - 1$ or $v(b_m) \geqq 1$, then $v(c_j) > 0$ for all $0 \leqq j \leqq p - 1$. Hence, $p\tilde{Q} = 0$. In particular, in the case $v(b_m) \geqq 1$, this shows that $p\mathcal{T}_k^0 = 0$, so that $\mathcal{T}_k^0 \simeq \mathbb{G}_a^{p-1}$ for any $\delta(T)$. When $\delta(T) > p - 1$, this shows that $p\mathcal{T}_k = 0$, and thus $\mathcal{T}_k$ is split.

6. Abelian varieties with rigid analytic uniformization

Let A/K be an abelian variety over K. Then A can be uniformized as follows. There exist a semi-abelian variety G and a lattice Λ in G such that the following sequence of rigid analytic groups is exact ([B-X], Theorem 1.2):

$$0 \to \Lambda \to G \to A \to 0 \tag{23}$$

and G is an (algebraic) extension

$$0 \to T \to G \to B \to 0$$

of an abelian variety B with potentially good reduction by a torus T. Denote by $\mathcal{L}$, $\mathcal{G}$, $\mathcal{T}$, $\mathcal{B}$, and $\mathcal{A}$, the associated Néron models. The exact sequence (23) induces an isomorphism

$$\mathcal{G}_k^0 \simeq \mathcal{A}_k^0 \tag{24}$$

([B-X], Theorem 2.3) and an exact sequence

$$0 \to \Phi(\Lambda) \to \Phi(G) \to \Phi(A)$$

([B-X], Theorem 4.12). Since Λ is a discrete group, $\mathcal{L}$ is locally finite over $\mathcal{O}_K$. Thus $\Lambda(K) \simeq \mathcal{L}_k(k) \simeq \Phi(\Lambda)$. In particular, $\Phi(\Lambda)$ is torsion free. Thus

$$0 \to \Phi(G)_{\mathrm{tors}} \to \Phi(A) \tag{25}$$

is exact. Putting (24) and (25) together with Proposition 1.4, we obtain a commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{G}_{k,p}^0 & \longrightarrow & \mathcal{G}_{k,p} & \longrightarrow & \Phi(G)_p & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{A}_{k,p}^0 & \longrightarrow & \mathcal{A}_{k,p} & \longrightarrow & \Phi(A)_p & \longrightarrow & 0 \end{array} \tag{26}$$

with injective vertical arrows.

Proposition 6.1. *Let A/K be an abelian variety uniformized as in* (23). *Then*:

(a) *If $\mathscr{A}$ is split, then so is $\mathscr{G}$.*

(b) *If $\Phi(G)_p \neq (0)$ and $\mathscr{A}$ is totally not split, then so is $\mathscr{G}$.*

Proof. Follows from the diagram (26) and Proposition 1.4.

Let $\Gamma_K := \mathrm{Gal}(K^s/K)$. Consider $\Lambda(K^s)$ as a Γ_K-module.

Proposition 6.2. *Let A/K be an abelian variety uniformized as in* (23). *Then there exists a canonical isomorphism*

$$\Lambda(K^s) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq X(T)^{\wedge} \otimes_{\mathbb{Z}} \mathbb{Q} \tag{27}$$

of $\mathbb{Q}[\Gamma_K]$-modules.

Proof. For any semi-abelian variety H/K with Néron model $\mathscr{H}/\mathcal{O}_K$, we denote by $H^0(K)$ the subgroup of points of $H(K)$ which reduce to the identity component of $\mathscr{H}_k$. Since K is complete and, hence, henselian, the reduction map induces an isomorphism $H(K)/H^0(K) \to \Phi(H)$. For any finite Galois extension M/K, we endow $\Phi(H_M)$ with the structure of $\mathrm{Gal}(M/K)$-module via the isomorphism $H_M(M)/H_M^0(M) \to \Phi(H_M)$. The morphisms $\Lambda \to G$ and $T \to G$ induce canonical maps of Galois modules

$$\Lambda(M) \xrightarrow{\alpha_M} \Phi(G_M), \quad \text{and} \quad \Phi(T_M) \xrightarrow{\beta_M} \Phi(G_M).$$

Let L/K be a finite Galois extension such that T_L is a split torus, B_L has good reduction and Λ_L is constant (e.g., take L/K such that A_L has semi-abelian reduction). Then Γ_K acts on Λ and $X(T)$ through the quotient $\Gamma := \mathrm{Gal}(L/K)$. So it is enough to exhibit an isomorphism of $\mathbb{Q}[\Gamma]$-modules between $\Lambda(K^s) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $X(T)^{\wedge} \otimes_{\mathbb{Z}} \mathbb{Q}$. The hypothesis on L implies that α_L is injective ([B-X], top of page 462) and that β_L is an isomorphism ([B-X], bottom of page 461). Thus, we obtain a natural injection

$$\beta_L^{-1} \circ \alpha_L \colon \Lambda(K^s) \to \Phi(T_L).$$

By definition of a lattice, the rank of $\Lambda(L) = \Lambda(K^s)$ is equal to $\dim T_L$ and, hence, equal to the rank of $\Phi(T_L)$. So $\Lambda(L) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \Phi(T_L) \otimes_{\mathbb{Z}} \mathbb{Q}$ as $\mathbb{Q}[\Gamma]$-modules. Consider now the evaluation pairing

$$T_L(L) \times X(T) \to \mathbb{Q}$$

defined by $(z, \chi) \mapsto [L:K]^{-1} v_L\big(\chi(z)\big)$ (we divide by $[L:K]$ to make the pairing independent of L). This pairing is well-defined because the image of $T(L)$ by χ is in L^* since χ is defined over L. It is clearly compatible with the action of Γ. The morphism χ extends to a morphism of Néron models and, thus, the image of $T^0(L)$ is in $\mathcal{O}_L$. It follows that the pairing factorises to a pairing

$$\Phi(T_L) \times X(T) = \big(T_L(L)/T_L^0(L)\big) \times X(T) \to [L:K]^{-1}\mathbb{Z}. \tag{28}$$

Now it is easy to check that this pairing is perfect because T_L is a split torus. This implies that $\Phi(T_L) \simeq X(T)^{\wedge} \otimes_{\mathbb{Z}} [L:K]^{-1}\mathbb{Z}$. Thus the proposition is proved.

Remark 6.3. Using the injection $\beta_L^{-1} \circ \alpha_L\colon \Lambda(L) \to \Phi(T_L)$, the pairing (28) induces a Galois pairing $\Lambda \times X(T) \to \mathbb{Q}$. This should be a generalization of the pairing in [B-X], bottom of page 478.

Proposition 6.4. *Let ℓ be a prime different from* char(K). *Let $T_\ell(N)$ denote the Tate module of any group N. Let A/K be an abelian variety uniformized as in* (23).

(a) *There are two natural exact sequences of Γ_K-modules*

$$0 \to T_\ell(G) \to T_\ell(A) \to \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to 0$$

and

$$0 \to T_\ell(T) \to T_\ell(G) \to T_\ell(B) \to 0.$$

(b) *Let $\delta(A)$, $\delta(B)$, and $\delta(T)$ be the Swan conductors of A, B, and T, respectively. Then*

$$\delta(A) = 2\delta(T) + \delta(B).$$

Proof. (a) The exact sequence (23) gives rise to an exact sequence of Γ_K-modules

$$0 \to \Lambda(K^s) \to G(K^s) \to A(K^s) \to 0.$$

Since Λ is torsion free and G is ℓ^n-divisible for any $n \geqq 1$, we have an exact sequence

$$0 \to G[\ell^n] \to A[\ell^n] \to \Lambda/\ell^n\Lambda \to 0.$$

Passing to the inverse limit, we get the desired exact sequence (note that $T_\ell(A) \to \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ is surjective because $G[\ell^{n+1}] \to G[\ell^n]$ is surjective). The second exact sequence is proved in a similar manner.

(b) Let ℓ be a prime different from p. From part (a) we find that

$$\delta(A) = \delta(G) + \delta(\Lambda) = \delta(T) + \delta(B) + \delta(\Lambda).$$

According to the previous proposition, $\delta(\Lambda) = \delta(T)$. This proves part (b).

Remark 6.5. Consider the torus S introduced in Theorem 4.6. Proposition 6.1 (a), shows that any abelian variety A uniformized by such a torus does not have split reduction if S does not have split reduction. Since we have an explicit criterion to determine whether S is split, we thus can provide non-trivial examples of abelian varieties that are not split.

Corollary 6.6. *Let A/K be an abelian variety that has potentially purely multiplicative reduction with uniformization by a torus S/K as in* 4.6. *If A/K has totally not split reduction, then* $2 \leqq \delta(A) \leqq 2\dim(A)$.

Proof. Since S has purely additive reduction over $\mathcal{O}_K$, so does A. Let L/K denote the extension minimal with the property that A_L/L has semi-stable reduction. The extension L/K is wild since p divides $|\Phi(A)|$ by hypothesis (1.9). Proposition 6.2 shows that $\mathrm{Gal}(K^s/K)$ acts on $T_\ell(S)$ and $\Lambda(K^s)$ through the same finite group. Proposition 6.4 (a) shows that this finite group is $\mathrm{Gal}(L/K)$. By hypothesis, S is the canonical quotient of $R_{F/K}\mathbb{G}_{m,F}$, where F/K is a subextension of L/K. If $F = L$, then clearly p divides $[F:K]$. If F/K is not Galois, then again p must divide $[F:K]$ since L/K is totally ramified. It follows that the group $\Phi_p(S)$ is always not trivial, and we can apply Proposition 6.1 to show that S has totally not split reduction. It follows from 4.6 (a) and 6.4 that $2 \leqq \delta(A) \leqq 2\dim(A)$.

Note that the case where $\dim(A) = 1$ was treated already by direct computations in the proof of Theorem 2.1 (see 2.5 and 2.9).

Remark 6.7. Let A be an abelian variety over K with Tate module $T_\ell(A)$. Denote by ρ_ℓ the natural representation $\Gamma_K \to \mathrm{Aut}(T_\ell(A))$. Let $\mathscr{A}$ be the Néron model of A over $\mathcal{O}_K$. In the case where A is the Jacobian of a proper smooth curve C/K, the combinatorial data associated with the special fiber (called the type of the special fiber) of a regular model of C is enough information to completely determine the group $\Phi(A)$, and most of the structure of the scheme $\mathscr{A}_k^0$. In case $\dim(A) = 1$, the type of the special fiber completely determines $\mathscr{A}_k^0$. In this article, we have been able to exhibit in some cases a relationship between the group structure of $\mathscr{A}_k$ and the representation ρ_ℓ. It is thus natural to ask whether the representation ρ_ℓ plus the type of the special fiber of a regular model of C is enough information to completely determine the group structure of $\mathscr{A}_k$. In what follows, we give an example which shows that the answer to this question is negative.

Suppose $\mathrm{char}(K) = 0$ and $\mathrm{char}(k) = 2$. Fix an integer $n \geqq 3$. Let E be an elliptic curve with reduction type I_{2n}^*. Let

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6$$

be the minimal Weierstrass equation of E given in Tate's algorithm (2.9). In particular, $v(b_4) \geqq n+3$ and $v(b_6) \geqq 2n+4$. We may choose $v(a_1) = 1$, so that $v(b_2) = 2$. Then $v(c_4) = 4$ and $v(\Delta) = 2n+8 > 3v(c_4)$. Hence, E has potentially multiplicative reduction and $v(j) = -(2n-4)$. Moreover, E achieves multiplicative reduction over the quadratic extension $L := K(\sqrt{-c_4/c_6})$ (see [Si2], V.5.5.3). Since $v(b_4) \geqq 4$ and $v(b_6) \geqq 6$, and since any element of $1 + 4\mathcal{O}_K$ is a square in $\mathcal{O}_K$, it is easily checked that $L = K(\sqrt{b_2})$ (see page 443 of [Si2]). Let E' be the elliptic curve over K defined by

$$y^2 + (a_1x + a_3')y = x^3 + a_2x^2 + a_4x + a_6$$

with $v(a_3') \geqq n+2$. Then E' has exactly the same type of reduction as E, with $b_2(E') = b_2(E)$ and $v(j(E')) = v(j)$. Thus, E' has multiplicative reduction over L. Lemma 6.8 below shows that the ℓ-adic representations of E and E' are isomorphic.

Let $\mathscr{E}$ and $\mathscr{E}'$ be the Néron models of E and E' respectively. We can choose a_3 and a_3' in such a way that the inequality $v(b_8 + a_4^2) > 2n+5$ is satisfied in the case of a_3 but not in the case of a_3'. Then $\mathscr{E}_k'$ is totally not split, but $\mathscr{E}_k$ is not (see Proposition 2.11). Hence, $\mathscr{E}_k'$ is not isomorphic to $\mathscr{E}_k$.

The exact sequence of Proposition 6.4 (a) does not determine completely, in general, the structure of $T_\ell(A)$. However, for elliptic curves E with potentially multiplicative reduction, the structure of $T_\ell(E)$ is well known. The proof of the following lemma is left to the reader.

Lemma 6.8. *Let E/K be an elliptic curve with additive and potentially multiplicative reduction. Let L/K be the quadratic separable extension such that E_L has multiplicative reduction. Let j be the modular invariant of E. Let $\ell \neq p$ be a prime, and let $\chi_\ell \colon \Gamma_K \to \mathrm{GL}(\mathbb{Z}_\ell)$ be the cyclotomic character obtained from the action of Γ_K on the Tate module $T_\ell(\mathbb{G}_m)$. Then there exists a basis $\{\xi, \theta\}$ of $T_\ell(E)$ such that, for any $\tau \in \Gamma_K$, the matrix of τ in this basis is*

$$\varepsilon(\tau) \cdot \begin{pmatrix} 1 & -\chi_\ell(\tau)v(j) \\ 0 & 1 \end{pmatrix},$$

where $\varepsilon(\tau) = 1$ if $\tau \in \mathrm{Gal}(K^s/L)$ and $\varepsilon(\tau) = -1$ otherwise.

In view of the main results of this paper, Theorems 2.1, 4.6, 4.9, and 6.6, it is natural to ask the following questions. All discrete valuation fields below are of residue characteristic $p > 0$.

Question 6.9. Let $g > 0$ and consider all the abelian varieties A of dimension g over a discrete valuation field, and whose Néron model $\mathscr{A}$ has toric rank equal to zero. Is there a constant c, depending on g but not on the field, such that if the special fiber of $\mathscr{A}$ is totally not split, then the Swan conductor $\delta(A)$ is bounded by c? As phrased, this question has an obvious negative answer in general. Indeed, consider an abelian variety B/K with purely additive reduction that is totally not split. Consider an elliptic curve E/K with additive reduction, large conductor $\delta(E)$ and such that $\Phi(E) = \{0\}$ (take for instance $y^2 = x^3 + \pi$, whose Swan conductor is $4v_K(2)$). Then the abelian variety $A := B \times E$ has purely additive reduction, is totally not split, but the conductor of such an abelian variety is not bounded by a constant that depends only on g. Hence, we are lead to ask the above question for more restricted classes of abelian varieties. For instance, one may ask the same question for simple abelian varieties whose Néron model is totally not split; or for the more restricted class of abelian varieties such that the representation of the inertia group I on the Tate module $T_\ell(A)$, $\ell \neq p$, is irreducible.

Question 6.10. Let A/K be an abelian variety. The Swan conductor of A/K is bounded by a constant f depending on $\dim(A)$ and on $v_K(p)$ only ([B-K], 6.2). Is there a bound c depending on $\dim(A)$ and on $v_K(p)$ only such that, if $\delta(A) > c$, then A/K has split reduction? Such a bound was shown to exist for a torus of the form S/K in 4.6 (c). It would be interesting to check whether, in the known examples where the bound f is achieved, the abelian varieties all have split reduction.

For instance, Example 6.5 in [B-K] (see also 3.1 in [LRS]) is the case of the jacobian A/K of the hyperelliptic curve X/K given by the affine equation $y^2 = x^{p^s} - \pi_K$ (with p odd). Consider the model $\mathscr{X}/\mathcal{O}_K$ of X/K given as the normalization of the projective curve $y^2 z^{p^s-2} = x^{p^s} - \pi_K z^{p^s}$ in $\mathbb{P}^2/\mathcal{O}_K$. The point $(0:0:1)$ is singular in the special fiber, but regular in $\mathscr{X}$. Thus the special fiber has arithmetical genus at least $(p^s-1)/2$, which is the genus of X. Hence, the model $\mathscr{X}/\mathcal{O}_K$ is regular, with an irreducible special fiber. It follows that the group of components of $\mathscr{A}/\mathcal{O}_K$ is trivial and, thus, A/K has split reduction. In

[B-K], 6.6, the first example consists of the Weil restriction $R_{M/K}(B)$, of the jacobian B/M of the hyperellipic curve given by the equation $y^2 = x^p - \pi_M$. As above, this curve has a regular model over $\mathcal{O}_M$ with an irreducible special fiber and, hence, the Néron model of its jacobian has trivial group of components. Since $\Phi_K(R_{M/K}(B))$ is isomorphic to $\Phi_M(B)$ ([ELL], proof of Thm. 1), we find that $R_{M/K}(B)$ has split reduction.

It follows from 6.3 in [B-K] that the jacobian A_r/K of the hyperelliptic curve X_r/K given by the affine equation $y^2 = x^{p^s} - \pi_K^r$, with p odd and coprime to r, also reaches the bound for the conductor of an abelian variety of genus $(p^s - 1)/2$. We believe that the group $\Phi_K(A_r)$ is trivial if r is odd and cyclic of order p^s if r is even. Moreover, in the latter case, $A_r(K)$ contains a torsion point of order p^s which reduces to the generator of $\Phi_K(A_r)$. Thus, the jacobian A_r may have split reduction in all cases. The case $r = 1$ is proved above, and the case $r = 2$ is discussed in 3.7. We leave it to the reader to check our claim for the remaining cases following the method of 3.7. As in [B-K], we may also consider the Weil restriction $R_{M/K}(B_r)$ of the jacobian B_r/M of the hyperellipic curve given by the equation $y^2 = x^p - \pi_M^r$. As we showed in 3.10, the splitting properties of a Weil restriction are not well understood.

Question 6.11. Let G/K be a semi-abelian variety that does not have split reduction.

(a) Is it always possible to find a tame extension M/K such that G_M/M has split reduction?

(b) Does there exist a constant c depending on $\dim(G)$ only such that if M/K is any tame extension of degree at least c, then G_M/M has split reduction?

Both questions have a positive answer when $\dim(G) = 1$ or G is a quotient torus S (see 3.3 and 4.11). Note that if the condition that M/K is tame is dropped, then the answer to (a) is obviously positive. Indeed, take $M = L$, where L/K is such that G_L/L has semi-stable reduction. Then G_L/L is split (1.6). Note that our assumption that G does not have split reduction implies, at least for tori and abelian varieties with toric rank equal to zero, that L/K is not tame (1.7 and 1.9).

References

[BLR] *S. Bosch*, *W. Lütkebohmert*, and *M. Raynaud*, Néron Models, Erg. Math. 3. Folge **21**, Springer, 1990.

[B-X] *S. Bosch* and *X. Xarles*, Component groups of Néron models via rigid uniformization, Math. Ann. **306** (1996), 459–486.

[BA] *Bourbaki*, Eléments de Mathématique, Algèbre, Masson, 1981.

[B-K] *A. Brumer* and *K. Kramer*, The conductor of an abelian variety, Comp. Math. **92** (1994), 227–248.

[C-Z] *D. Cox* and *S. Zucker*, Intersection numbers of sections of elliptic surfaces, Invent. Math. **53** (1979), 1–44.

[Cre] *J. E. Cremona*, Algorithms for modular elliptic curves, Cambridge University Press, 1992.

[ELL] *B. Edixhoven*, *Q. Liu*, and *D. Lorenzini*, The p-part of the group of components of a Néron model, J. Alg. Geom. **5** (1996), 801–813.

[K-S] *B. Kunyavskii* and *J.-J. Sansuc*, Réduction des groupes algébriques commutatifs, J. Math. Soc. Japan, to appear.

[LRS] *P. Lockhart*, *M. Rosen*, and *J. Silverman*, An upper bound for the conductor of an abelian variety, J. Alg. Geom. **2** (1993), 569–601.

[Lor1] *D. Lorenzini*, Groups of components of Néron models of Jacobians, Comp. Math. **73** (1990), 145–160.

[Lor2] *D. Lorenzini*, On the group of components of a Néron model, J. reine angew. Math. **445** (1993), 109–160.

[Lor3] *D. Lorenzini*, Reduction of points in the group of components of a Néron model of a jacobian, J. reine angew. Math. **527** (2000), 117–149.

[Lor4] *D. Lorenzini*, Torsion points on the modular Jacobian $J_0(N)$, Comp. Math. **96** (1995), 149–172.
[Mil] *J. S. Milne*, On the arithmetic of abelian varieties, Invent. Math. **17** (1972), 177–190.
[Mil2] *J. S. Milne*, Arithmetic duality theorems, Academic Press, 1986.
[Mum] *D. Mumford*, The Red Book of Varieties and Schemes, Lect. Notes Math. **1358**, Springer, 1988.
[N-X] *E. Nart* and *X. Xarles*, Additive reduction of algebraic tori, Arch. Math. **57** (1991), 460–466.
[New] *M. Newman*, Integral matrices, Academic Press, 1972.
[Ogg] *A. P. Ogg*, Elliptic curves and wild ramification, Am. J. Math. **89** (1967), 1–21.
[Sai] *T. Saito*, Conductor, discriminant, and the Noether formula of arithmetic surfaces, Duke Math. J. **57** (1988), 151–173.
[Ser] *J.-P. Serre*, Corps Locaux, Hermann, 1968.
[Ser2] *J.-P. Serre*, Facteurs locaux des fonctions zêta, Oeuvres **II**, Springer Verlag (1985), 581–592.
[S-T] *J.-P. Serre* and *J. Tate*, Good reduction of abelian varieties, Ann. Math. **88** (1968), 492–517.
[Si2] *J. Silverman*, Advanced Topics in the Arithmetic of Elliptic Curves, Grad. Texts Math. **151**, Springer-Verlag, 1994.
[Xar] *X. Xarles*, The scheme of connected components of the Néron model of an algebraic torus, J. reine angew. Math. **437** (1993), 167–179.

Laboratoire de Mathématiques Pures, Université Bordeaux 1, 33405 Talence Cedex, France
e-mail: liu@math.u-bordeaux.fr

Department of Mathematics, University of Georgia, Athens, GA 30602, USA
e-mail: lorenzini@math.uga.edu

Eingegangen 22. Oktober 1999, in revidierter Fassung 24. Mai 2000