Advances in Mathematics 356 (2019) 106818

Contents lists available at ScienceDirect

Advances in Mathematics

www.elsevier.com/locate/aim

Hasse principles for multinorm equations

E. Bayer-Fluckiger [a,*], T.-Y. Lee [a,b], R. Parimala [c]

[a] EPFL-FSB-MATHGEOM-CSAG, Station 8, 1015 Lausanne, Switzerland
[b] Technische Universität Dortmund, Fakultät für Mathematik, Lehrstuhl LSVI, Vogelpothsweg 87, 44227 Dortmund, Germany
[c] Department of Mathematics & Computer Science, Emory University, Atlanta, GA 30322, USA

ARTICLE INFO

Article history:
Received 22 August 2018
Received in revised form 6 September 2019
Accepted 11 September 2019
Available online 25 September 2019
Communicated by A. Asok

MSC:
11G35
12G05
14G05
14G25

Keywords:
Multinorm
Tori
Shafarevich groups
Local-global principles
Brauer-Manin obstructions

ABSTRACT

A classical result of Hasse states that the norm principle holds for finite cyclic extensions of global fields, in other words local norms are global norms. We investigate the norm principle for finite dimensional commutative étale algebras over global fields; since such an algebra is a product of separable extensions, this is often called the multinorm principle. Under the assumption that the étale algebra contains a cyclic factor, we give a necessary and sufficient condition for the Hasse principle to hold, in terms of an explicitly constructed element of a finite abelian group. This can be seen as an explicit description of the Brauer-Manin obstruction to the Hasse principle.

* Corresponding author.
E-mail addresses: eva.bayer@epfl.ch (E. Bayer-Fluckiger), tingyu.lee@gmail.com (T.-Y. Lee), parimala@mathcs.emory.edu (R. Parimala).

https://doi.org/10.1016/j.aim.2019.106818
0001-8708/© 2019 Elsevier Inc. All rights reserved.

0. Introduction

Let k be a global field, and L be a finite dimensional commutative étale algebra over k. We say that the *Hasse norm principle* holds for L if the local-global principle holds for the equation

$$N_{L/k}(t) = c \tag{0.1}$$

for all $c \in k^{\times}$; this terminology is inspired by Hasse's result that the norm principle holds in the case of *cyclic extensions* ([7], [8] §I (3.11) and §II (15)). Over the years, the norm principle for separable field extensions attracted a lot of attention; it is known not to hold in general, and many positive results are also available, see for instance [11], pages 308-309 for a survey; for more recent results, see [1], [5], and the references therein.

It is natural to ask for Hasse principles in the case when L is a finite dimensional commutative *étale algebra*, and not just a field extension. Since L is by definition a product of separable extensions, the equation (0.1) is often called a multinorm equation.

This more general problem was also studied extensively, in particular by Hürlimann ([9]), Colliot-Thélène and Sansuc (unpublished), Platonov and Rapinchuk (see [11], sections 6.3 and 9.3), Prasad and Rapinchuk ([14], Section 4), Pollio and Rapinchuk ([13]), Demarche and Wei ([4]), Pollio ([12]). Multinorm equations also arise when dealing with classical groups of type A_n (see for instance [14] Prop. 4.2).

In spite of many interesting results, some quite simple cases were still open. We illustrate this, as well as our results, by the following example:

Example. Assume that L is a product of n non-isomorphic quadratic field extensions of k. If $n = 1$ or $n = 2$, then the Hasse principle holds for L - this is clear for $n = 1$, and easy for $n = 2$ (for instance, it is a consequence of [9], Proposition 3.3). It is also well-known that it does not hold in general when $n = 3$ (see for instance [3]). In the present paper, we show that *the Hasse principle holds if* $n \geq 4$.

To obtain this result and others, let us assume that one of the factors of L is a *cyclic field extension* of k. Under this hypothesis, we construct a finite abelian group $\text{Ш}(L)$ having the property that

$$\text{Ш}(L) = 0 \iff \text{the Hasse principle holds for } L$$

(cf. Section 5). Assume now that $\text{Ш}(L) \neq 0$, and that $c \in k^{\times}$ is such that (0.1) has a solution locally everywhere. Then we construct a homomorphism

$$\alpha_c : \text{Ш}(L) \to \mathbb{Q}/\mathbb{Z}$$

such that

$$(0.1) \text{ has a solution over } k \iff \alpha_c = 0$$

(see Sections 6 and 7, in particular Theorem 7.1).

These results can be summarized as follows: let I_L be the idèle group of L. Then sending $c \in k^\times$ to α_c gives rise to an isomorphism

$$k^\times \cap N_{L/k}(I_L)/N_{L/k}(L^\times) \to Ш(L)^*$$

(where $Ш(L)^*$ is the dual of $Ш(L)$, cf. Corollary 7.12).

We also give a necessary and sufficient condition for the Hasse principle to hold when one of the factors is metacyclic (see Proposition 7.13).

The results are easy to use. To illustrate this, we consider the case where L is a *product of cyclic extensions*; assume that $L = \prod_{i \in J} K_i$, where K_i/k is a cyclic extension of degree d_i. Let $\mathcal{P}$ be the set of prime numbers dividing $\prod_{i \in J} d_i$. For all $p \in \mathcal{P}$ and all $i \in J$, let $K_i(p)$ be the largest subfield of K_i such that $[K_i(p) : k]$ is a power of p, and set $L(p) = \prod_{i \in J} K_i(p)$. Then we have

$$Ш(L) = \underset{p \in \mathcal{P}}{\oplus} Ш(L(p)),$$

(see Proposition 8.6).

For any cyclic field extension K/k of prime power degree, we denote by K_{prim} the unique subfield of K of degree p over k. Set

$$L(p)_{\text{prim}} = \prod_{i \in J} K_i(p)_{\text{prim}}.$$

Then we have

$$Ш(L) = 0 \iff \underset{p \in \mathcal{P}(L)}{\oplus} Ш(L(p)_{\text{prim}}) = 0,$$

(cf. Theorem 8.1), and

$$Ш(L(p)_{prim}) \simeq (\mathbb{Z}/p\mathbb{Z})^{m_p(L)},$$

where $\mathcal{P}(L)$ is a set of prime numbers (subset of $\mathcal{P}$), and $m_p(L)$ is a positive integer; both are determined explicitly (see Theorem 8.2).

The paper is structured as follows. Sections 1–4 contain some preliminary results, including a new proof of a proposition of Hürlimann, [9] Prop. 3.3. The group $Ш(L)$ is defined in Section 5, and the homomorphism α_c in Section 6. In both sections, we start with the case where the étale algebra L has a cyclic factor of prime power degree, which is the essential case. We also show how one can reduce the exponent of the prime number, using the exact sequence of Proposition 5.10 - this is then used in inductive arguments. The main result is proved in Section 7 (see Theorem 7.1). Section 8 contains the application of the above results to the special case where all the factors of the étale algebra are cyclic.

Note that the results of this paper are related to the Brauer-Manin obstruction. Indeed, for $c = 1$, the equation (0.1) yields the so-called *norm-one-torus* defined by L/k (see 1.2 for details); we denote this torus by $T_{L/k}$. When k is an algebraic number field, then one can deduce from [15] that the only obstruction to the Hasse principle is the Brauer-Manin obstruction, and is an element of the group $Ш^2(k, \hat{T}_{L/k})^*$. We show that $Ш(L) \simeq Ш^2(k, \hat{T}_{L/k})$ (see Proposition 5.16), hence our results provide an explicit description of the Brauer-Manin obstruction.

We thank the referee for several very useful comments. The second named author wishes to acknowledge support from the Alexander von Humboldt Foundation. The third named author is partially supported by the NSF grants DMS 1801951 and FRG 1463882.

1. Notation, definitions and basic facts

1.1. Weil restriction

If $f : R \to R'$ is a homomorphism of commutative rings such that R' is a projective R-module of finite type, and if W is an affine R'-scheme, then we denote by $\mathrm{R}_{R'/R}W$ the Weil restriction (see for instance [10], Appendice 2).

1.2. Etale algebras, tori and characters

Let k be a field, let k_s be a separable closure of k and set $\Gamma_k = \mathrm{Gal}(k_s/k)$. We fix once and for all this separable closure k_s, and all separable extensions of k that will appear in the paper will be contained in k_s. We use standard notation in Galois cohomology; in particular, if M is a discrete Γ_k-module and i is an integer ≥ 0, we set $H^i(k, M) = H^i(\Gamma_k, M)$.

If L is a commutative étale k-algebra of finite rank, we denote by $N_{L/k}$ the norm map, and set $T_{L/k} = \mathrm{R}^{(1)}_{L/k}(\mathbb{G}_m)$; then $T_{L/k}$ is the k-torus determined by the exact sequence

$$1 \longrightarrow T_{L/k} \longrightarrow \mathrm{R}_{L/k}(\mathbb{G}_m) \xrightarrow{N_{L/k}} \mathbb{G}_m \longrightarrow 1 \ . \tag{1.1}$$

For a k-torus T, we denote by $\hat{T} = \mathrm{Hom}(T, \mathbb{G}_m)$ its character group. If K/k is a finite separable extension, set $\Gamma_K = \mathrm{Gal}(k_s/K)$. If moreover M is a discrete Γ_K-module, set $\mathrm{I}_{K/k}(M) = \mathrm{Ind}_{\Gamma_K}^{\Gamma_k}(M)$.

The following lemmas will be used several times in the sequel

Lemma 1.1. *Let F/k be a separable extension of finite degree, and let L be the product of n copies of F. Then we have*

(i) $T_{L/k} \simeq \mathrm{R}_{F/k}(\mathbb{G}_m)^{n-1} \times T_{F/k}$.
(ii) $H^1(k, \hat{T}_{L/k}) \simeq H^1(k, \hat{T}_{F/k})$.

Proof. The isomorphism $(\mathrm{R}_{F/k}(\mathbb{G}_m))^n \to (\mathrm{R}_{F/k}(\mathbb{G}_m))^n$ sending $(b_1, ..., b_n)$ to $(b_1, ..., b_{n-1}, b_1 ... b_{n-1} b_n)$ induces an isomorphism $T_{L/k} \simeq \mathrm{R}_{F/k}(\mathbb{G}_m)^{n-1} \times T_{F/k}$. This proves (i). By (i), we have $\hat{T}_{L/k} \simeq \mathrm{I}_{F/k}(\mathbb{Z})^{n-1} \oplus \hat{T}_{F/k}$; since $H^1(k, \mathrm{I}_{F/k}(\mathbb{Z})) = 0$, this implies (ii).

Lemma 1.2. *Let K/k be a cyclic extension of degree d. Then there exists an isomorphism*

$$H^1(k, \hat{T}_{K/k}) \to \mathbb{Z}/d\mathbb{Z}$$

which is functorial with respect to base change.

Proof. Let σ be a generator of $\mathrm{Gal}(K/k)$. Consider the exact sequence

$$1 \to \mathbb{G}_m \to \mathrm{R}_{K/k}(\mathbb{G}_m) \to T_{K/k} \to 1,$$

where the map from $\mathrm{R}_{K/k}(\mathbb{G}_m)$ to $T_{K/k}$ sends x to $x/\sigma(x)$, and its dual sequence

$$0 \to \hat{T}_{K/k} \to \mathrm{I}_{K/k}(\mathbb{Z}) \to \mathbb{Z} \to 0.$$

This exact sequence induces

$$\mathrm{I}_{K/k}(\mathbb{Z})^{\Gamma_k} \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow H^1(k, \hat{T}_{K/k}) \longrightarrow H^1(k, \mathrm{I}_{K/k}(\mathbb{Z})) = 0 \ .$$

We have $\mathrm{I}_{K/k}(\mathbb{Z})^{\Gamma_k} \simeq \mathbb{Z}$, generated by the sum of the elements of $\mathrm{Gal}(K/k)$, and the map ϵ is multiplication by d; hence we obtain an isomorphism $H^1(k, \hat{T}_{K/k}) \to \mathbb{Z}/d\mathbb{Z}$ which is independent of the choice of the generator σ.

1.3. The multinorm problem

Let L be an étale k-algebra, and let $c \in k^*$. Let X_c be the affine k-variety determined by the equation $N_{L/k}(t) = c$. Then X_c is a torsor under the torus $T_{L/k}$ defined in 1.2, hence defines a class $[X_c] \in H^1(k, T_{L/k})$; the variety X_c has a k-point if and only if $[X_c] = 0$. Hence we have

$$c \in N_{L/k}(L^\times) \iff X_c(k) \neq \emptyset \iff [X_c] = 0.$$

2. A construction

Let k be a field, and let L be a commutative étale k-algebra of finite rank; assume that *L is not a field*. We keep the notation of the previous section. The aim of this section is to introduce a k-torus that will play a basic role in the study of the cohomology of the torus $T_{L/k}$, and of the multinorm problem.

Let us write $L = K \times K'$, where K and K' are étale k-algebras, and set $E = K \otimes_k K'$.

The norm maps $N_{K/k} : K \to k$ and $N_{K'/k} : K' \to k$ induce $N_{E/K'} : E \to K$ and $N_{E/K} : E \to K'$. Let $f : \mathrm{R}_{E/k}(\mathbb{G}_m) \to \mathrm{R}_{L/k}(\mathbb{G}_m)$ be defined by $f(x) = (N_{E/K}(x)^{-1}, N_{E/K'}(x))$. It is clear that the image of f is contained in $T_{L/k}$. Moreover, f is surjective as a map of algebraic groups (easily checked after base change to the separable closure k_s of k).

Consider the torus $S_{K,K'}$ defined by the exact sequence

$$1 \longrightarrow S_{K,K'} \longrightarrow \mathrm{R}_{E/k}(\mathbb{G}_m) \xrightarrow{f} T_{L/k} \longrightarrow 1 \ .$$

Note that $S_{K,K'}$ also fits in the exact sequence

$$1 \longrightarrow S_{K,K'} \longrightarrow \mathrm{R}_{K'/k}(T_{E/K'}) \xrightarrow{N_{E/K}} T_{K/k} \longrightarrow 1 \ , \tag{2.1}$$

where $T_{E/K'}$ is defined by the exact sequence of K'-tori

$$1 \to T_{E/K'} \to R_{E/K'}(\mathbb{G}_m) \overset{N_{E/K'}}{\longrightarrow} \mathbb{G}_m \to 1.$$

3. Tate-Shafarevich groups

We keep the notation of the previous sections, and assume that k is a global field. Let Ω_k be the set of all places of k; if $v \in \Omega_k$, we denote by k_v the completion of k at v.

For any k-torus T, set $\text{Ш}^i(k,T) = \mathrm{Ker}(H^i(k,T) \to \prod\limits_{v \in \Omega_k} H^i(k_v,T))$. If M is a Γ_k-module, set $\text{Ш}^i(k,M) = \mathrm{Ker}(H^i(k,M) \to \prod\limits_{v \in \Omega_k} H^i(k_v,M))$. Recall that by Poitou-Tate duality, we have $\text{Ш}^2(k,\hat{T}) \simeq \text{Ш}^1(k,T)^*$.

3.1. Hasse principle for the multinorm problem

Let L be an étale k-algebra, and let $c \in k^\times$. If $X_c(k_v) \neq \emptyset$ for all $v \in \Omega_k$, then we have $[X_c] \in \text{Ш}^1(k,T_{L/k})$. In particular, the Hasse principle holds for all $c \in k^\times$ if and only if $\text{Ш}^1(k,T_{L/k}) = 0$.

We have the following relationship between the Tate-Shafarevich groups of the torus $T_{L/k}$, and the torus $S_{K,K'}$ defined in §2:

Lemma 3.1. *We have* $Ш^1(k, T_{L/k}) \simeq Ш^2(k, S_{K,K'})$.

Proof. By the definition of the torus $S_{K,K'}$, we have the exact sequence

$$1 \longrightarrow S_{K,K'} \longrightarrow \mathrm{R}_{E/k}(\mathbb{G}_m) \xrightarrow{f} T_{L/k} \longrightarrow 1 \ ,$$

giving rise to the cohomology exact sequence

$$0 \to H^1(k, T_{L/k}) \to H^2(k, S_{K,K'}) \to H^2(k, \mathrm{R}_{E/k}(\mathbb{G}_m)).$$

By the corresponding cohomology exact sequence over k_v for all $v \in \Omega_k$ and the Brauer-Hasse-Noether Theorem, we have $Ш^2(k, \mathrm{R}_{E/k}(\mathbb{G}_m)) = 0$, hence $Ш^1(k, T_{L/k}) \simeq Ш^2(k, S_{K,K'})$, as claimed.

We now compute the group $Ш^2(k, \hat{T}_{K/k})$ for a cyclic extension K/k - note that by Poitou-Tate duality, this is equivalent to Hasse's cyclic norm principle, which is the following proposition:

Proposition 3.2. *Let K/k be a cyclic extension. Then* $Ш^1(k, T_{K/k}) = 0$.

Proof. We give a proof for the convenience of the reader. Let σ be a generator of $\mathrm{Gal}(K/k)$. Consider the exact sequence

$$1 \to \mathbb{G}_m \to \mathrm{R}_{K/k}(\mathbb{G}_m) \to T_{K/k} \to 1,$$

where the map from $\mathrm{R}_{K/k}(\mathbb{G}_m)$ to $T_{K/k}$ sends x to $x/\sigma(x)$. This sequence gives rise to an injection $H^1(k, T_{K/k}) \to H^2(k, \mathbb{G}_m)$. By the Brauer-Hasse-Noether theorem, we have $Ш^2(k, \mathbb{G}_m) = 0$, hence $Ш^1(k, T_{K/k}) = 0$.

Corollary 3.3. *Let K/k be a cyclic extension. Then* $Ш^2(k, \hat{T}_{K/k}) = 0$.

This follows from the previous proposition, combined with Poitou-Tate duality.

4. A result of Hürlimann

Using the above lemmas, we generalize a result of Hürlimann ([9] Prop. 3.3).

Proposition 4.1. *Let K/k be a cyclic extension of k, and let K'/k be a separable extension of finite degree. Let $c \in k^\times$. Then the local-global principle holds for the multinorm equation $N_{K/k}(x)N_{K'/k}(y) = c$.*

Proof. Set $L = K \times K'$; the assertion is equivalent to the vanishing of $Ш^1(k, T_{L/k})$. By Lemma 3.1, we have $Ш^1(k, T_{L/k}) \simeq Ш^2(k, S_{K,K'})$. By Poitou-Tate duality we have

$Ш^2(k, S_{K,K'}) \simeq Ш^1(k, \hat{S}_{K,K'})^*$, hence it suffices to prove that $Ш^1(k, \hat{S}_{K,K'}) = 0$. Since K/k is a cyclic extension, the algebra $E = K \otimes_k K'$ is isomorphic to a product of copies of F, where F/K' is some cyclic field extension. Set $d = [K : k]$ and $f = [F : K']$.

Consider the dual sequence of (2.1):

$$0 \longrightarrow \hat{T}_{K/k} \xrightarrow{\iota} \mathrm{I}_{K'/k}(\hat{T}_{E/K'}) \xrightarrow{\rho} \hat{S}_{K,K'} \longrightarrow 0\ , \tag{4.1}$$

and the sequence induced by (4.1)

$$H^1(k, \hat{T}_{K/k}) \xrightarrow{\iota^1} H^1(k, \mathrm{I}_{K'/k}(\hat{T}_{E/K'})) \xrightarrow{\rho^1} H^1(k, \hat{S}_{K,K'}) \xrightarrow{\delta} H^2(k, \hat{T}_{K/k}). \tag{4.2}$$

We have $H^1(k, \mathrm{I}_{K'/k}(\hat{T}_{E/K'})) \simeq H^1(K', \hat{T}_{E/K'})$; Lemmas 1.1 (ii) and 1.2 imply that $H^1(K', \hat{T}_{E/K'}) \simeq H^1(K', \hat{T}_{F/K'}) \simeq \mathbb{Z}/f\mathbb{Z}$. The map ι^1 is the natural projection from $\mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/f\mathbb{Z}$, therefore ι^1 is surjective. This implies that $\delta : H^1(k, \hat{S}_{K,K'}) \to H^2(k, \hat{T}_{K/k})$ is injective; moreover, δ induces an injection $Ш^1(k, \hat{S}_{K,K'}) \to Ш^2(k, \hat{T}_{K/k})$. Since K/k is a cyclic extension, we have $Ш^2(k, \hat{T}_{K/k}) = 0$ by Corollary 3.3. The proposition then follows.

5. The group $Ш(K, K')$

We keep the notation of the previous sections: in particular, $L = K \times K'$, where K and K' are étale k-algebras, and $E = K \otimes K'$. In addition, we now assume that K/k is a *cyclic extension*. Under this hypothesis, we define a finite abelian group $Ш(K, K')$ using the local splitting patterns of E, and we show that $Ш^1(k, T_{L/k})$ is isomorphic to the dual of $Ш(K, K')$.

Let $K' = \prod_{i \in \mathcal{I}} K_i$, where the K_i/k are field extensions. Then we have $E = \prod_{i \in \mathcal{I}} E_i$, with $E_i = K \otimes K_i$.

If $v \in \Omega_k$ and if A is a commutative k-algebra, set $A^v = A \otimes_k k_v$.

5.1. The prime power degree case

Suppose that K is a cyclic extension of degree p^e, where p is a prime number. We start with some notation and definitions. For each $i \in \mathcal{I}$, let M_i be a cyclic extension of K_i such that E_i is isomorphic to a product of copies of M_i. Let $p^{e_i} = [M_i : K_i]$; without loss of generality, we assume that $e_i \geq e_{i+1}$ for $1 \leq i \leq m-1$.

Let s and t be positive integers. For $s \geq t$, let $\pi_{s,t}$ be the canonical projection $\mathbb{Z}/p^s\mathbb{Z} \to \mathbb{Z}/p^t\mathbb{Z}$. For $x \in \mathbb{Z}/p^s\mathbb{Z}$ and $y \in \mathbb{Z}/p^t\mathbb{Z}$, we say that x *dominates* y if $s \geq t$ and $\pi_{s,t}(x) = y$; if this is the case, we write $x \succeq y$. For $x \in \mathbb{Z}/p^s\mathbb{Z}$ and $y \in \mathbb{Z}/p^t\mathbb{Z}$, let $\delta(x, y)$ be the greatest nonnegative integer $d \leq \min\{s, t\}$ such that $\pi_{s,d}(x) = \pi_{t,d}(y)$. We have $\delta(x, y) = \min\{s, t\}$ if and only if $x \succeq y$ or $y \succeq x$.

Let $\mathcal{I} = \{1, ..., m\}$. For $a = (a_1, ..., a_m) \in \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z}$ and $n \in \mathbb{Z}/p^{e_1}\mathbb{Z}$, let $I_n(a)$ be the set $\{i \in \mathcal{I} |\ n \succeq a_i\}$ and let $I(a) = (I_0(a), ..., I_{p^{e_1}-1}(a))$.

Let $\mathcal{E}$ be the set of p^{e_1}-tuples $(I_0, ..., I_{p^{e_1}-1})$, where $I_0, ..., I_{p^{e_1}-1}$ are subsets of $\mathcal{I}$ such that $\bigcup_{0 \leq n \leq p^{e_1}-1} I_n = \mathcal{I}$. Now we characterize the image of the map

$$I : \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z} \to \mathcal{E}.$$

An element $(I_0, ..., I_{p^{e_1}-1}) \in \mathcal{E}$ is said to be *coherent* if for all n_1, $n_2 \in \mathbb{Z}/p^{e_1}\mathbb{Z}$ we have:

(1) If $i \in I_{n_1} \cap I_{n_2}$, then $\pi_{e_1,e_i}(n_1) = \pi_{e_1,e_i}(n_2)$.
(2) If $i \in I_{n_1}$ and $\pi_{e_1,e_i}(n_1) = \pi_{e_1,e_i}(n_2)$, then $i \in I_{n_2}$.

Let $\mathcal{E}^c$ be the subset of all coherent elements in $\mathcal{E}$. For $a \in \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z}$, it is clear that $I(a)$ is a coherent element. Conversely for a coherent element $(I_0, ..., I_{p^{e_1}-1}) \in \mathcal{E}^c$, we set $a_i = \pi_{e_1,e_i}(n)$ for $i \in I_n$. Note that condition (1) of the definition of a coherent element ensures that the a_i's are well-defined. Hence $a = (a_1, ..., a_m)$ is a well-defined element in $\underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z}$; condition (2) implies that $I(a) = (I_0, ..., I_{p^{e_1}-1})$. This shows that I is a bijection between $\underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z}$ and $\mathcal{E}^c$.

If w is a place of K_i, we denote by K_i^w the completion of K_i at w. Given a positive integer $0 \leq d \leq e$ and $i \in \mathcal{I}$, let Σ_i^d be the set of all places $v \in \Omega_k$ such that at each place w of K_i above v, the algebra $K \otimes K_i^w$ is isomorphic to a product of isomorphic field extensions of degree at most p^d of K_i^w. Let $\Sigma_i = \Sigma_i^0$, in other words, Σ_i is the set of all places $v \in \Omega_k$ where E_i^v is isomorphic to a product of copies of K_i^v.

Let $(I_0, ..., I_{p^{e_1}-1}) \in \mathcal{E}^c$. For $n_1 \in \mathbb{Z}/p^{e_1}\mathbb{Z}$ and $i \in \mathcal{I}$, set $\delta(n_1, i) = \delta(n_1, \pi_{e_1,e_i}(n_2))$, where n_2 is an element in $\mathbb{Z}/p^{e_1}\mathbb{Z}$ such that $i \in I_{n_2}$. Since $(I_0, ..., I_{p^{e_1}-1})$ is coherent, $\delta(n_1, i)$ is independent of the choice of n_2 and hence is well-defined. Note that if we let $a = (a_1, ..., a_m)$ be the element in $\underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z}$ corresponding to $(I_0, ..., I_{p^{e_1}-1})$, then $\delta(n_1, i) = \delta(n_1, a_i)$. For $I_n \subsetneqq \mathcal{I}$, define

$$\Omega(I_n) = \underset{i \notin I_n}{\cap} \Sigma_i^{\delta(n,i)}. \tag{5.1}$$

For $I_n = \mathcal{I}$, we set $\Omega(I_n) = \Omega_k$.

Set

$$G = G_k(K, K') = \{(a_1, ..., a_m) \in \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z} | \bigcup_{n \in \mathbb{Z}/p^{e_1}\mathbb{Z}} \Omega(I_n(a)) = \Omega_k\}.$$

Lemma 5.1. *The set G is a subgroup of $\underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z}$.*

Proof. Let $a = (a_1, ..., a_m)$ and $b = (b_1, ..., b_m)$ be elements of G. By the definition of G, for each $v \in \Omega_k$, there exist some n, $n' \in \mathbb{Z}/p^{e_1}\mathbb{Z}$ such that $v \in \Omega(I_n(a))$ and $v \in \Omega(I_{n'}(b))$. We claim that

$$v \in \Omega(I_{n+n'}(a+b)).$$

This is clear when $I_{n+n'}(a+b) = \mathcal{I}$. Suppose that $I_{n+n'}(a+b) \neq \mathcal{I}$. First note that $\delta(n+n', a_i+b_i) \geq \min\{\delta(n, a_i), \delta(n', b_i)\}$ and that $\min\{\delta(n, a_i), \delta(n', b_i)\} \leq e_i$ for all $i \in \mathcal{I}$. Pick an arbitrary $i \notin I_{n+n'}(a+b)$. Without loss of generality, we suppose that $\min\{\delta(n, a_i), \delta(n', b_i)\} = \delta(n, a_i)$. If $i \notin I_n(a)$, we have $v \in \Sigma_i^{\delta(n,a_i)} \subseteq \Sigma_i^{\delta(n+n',a_i+b_i)}$; hence we have $v \in \Omega(I_{n+n'}(a+b))$.

If $i \in I_n(a)$, then by definition $\delta(n, a_i) = e_i$. We have $\delta(n, a_i) \leq \delta(n', b_i)$ by assumption, hence $\delta(n', b_i) \geq e_i$. But $\delta(n', b_i) \leq e_i$, therefore we have $\delta(n', b_i) = e_i$, and hence $i \in I_{n'}(b)$. This implies that $i \in I_{n+n'}(a+b)$, and this is a contradiction. This completes the proof of the lemma.

Let D be the subgroup of $\underset{i\in\mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z}$ generated by the diagonal element $(1, ..., 1)$, and note that D is contained in G. Set

$$Ш_k(K, K') = G/D.$$

Example 5.2. Assume that $k = \mathbb{Q}$, and that $L = \mathbb{Q}(\sqrt{a}) \times \mathbb{Q}(\sqrt{b}) \times \mathbb{Q}(\sqrt{ab})$, where a, b are distinct square-free integers. Set $K = \mathbb{Q}(\sqrt{a})$, $K_1 = \mathbb{Q}(\sqrt{b})$ and $K_2 = \mathbb{Q}\sqrt{ab})$. Then with the above notation we have $\mathcal{I} = \{1, 2\}$, and $E_1 = E_2 = \mathbb{Q}(\sqrt{a}, \sqrt{b})$, hence $e = e_1 = e_2 = 1$. This implies that either $Ш(K, K') = 0$, or $Ш(K, K') \simeq \mathbb{Z}/2\mathbb{Z}$. Note that

$$\text{there exists } v \in \Omega_k \text{ such that } E_1^v \text{ is a field} \iff \Sigma_1 \cup \Sigma_2 \neq \Omega_k,$$

hence

$$Ш(K, K') = 0 \iff \text{there exists } v \in \Omega_k \text{ such that } E_1^v \text{ is a field.}$$

Set now $a = 13$, $b = 17$: then there exists no $v \in \Omega_k$ such that E_1^v is a field, therefore $Ш(K, K') = \mathbb{Z}/2\mathbb{Z}$. Note that it is well-known that the multinorm principle fails in this case (see for instance [3], Proposition 5.1).

Theorem 5.3. *Suppose that K/k is a cyclic extension of degree p^e, where p is a prime number. Then $Ш^1(k, \hat{S}_{K,K'}) \simeq Ш(K, K')$.*

Proof. Consider the dual sequence of (2.1),

$$0 \longrightarrow \hat{T}_{K/k} \xrightarrow{\iota} \mathrm{I}_{K'/k}(\hat{T}_{E/K'}) \xrightarrow{\rho} \hat{S}_{K,K'} \longrightarrow 0 \ , \tag{5.2}$$

and the exact sequence induced by (5.2),

$$H^1(k,\hat{T}_{K/k}) \xrightarrow{\iota^1} H^1(k,\mathrm{I}_{K'/k}(\hat{T}_{E/K'})) \xrightarrow{\rho^1} H^1(k,\hat{S}_{K,K'}) \to H^2(k,\hat{T}_{K/k}). \tag{5.3}$$

We have $Ш^2(k,\hat{T}_{K/k}) = 0$ by Corollary 3.3, therefore $Ш^1(k,\hat{S}_{K,K'})$ is in the image of ρ^1.

Note that $H^1(k,\mathrm{I}_{K_i/k}(\hat{T}_{E_i/K_i})) \simeq H^1(K_i,\hat{T}_{E_i/K_i})$, and that by Lemma 1.1 (ii), we have $H^1(K_i,\hat{T}_{E_i/K_i}) \simeq H^1(K_i,\hat{T}_{M_i/K_i})$. Moreover, by Lemma 1.2, we have $H^1(K_i,\hat{T}_{M_i/K_i}) \simeq \mathbb{Z}/p^{e_i}\mathbb{Z}$.

In the following we identify $H^1(k,\hat{T}_{K/k})$ to $\mathbb{Z}/p^e\mathbb{Z}$ and $H^1(k,\mathrm{I}_{K_i/k}(\hat{T}_{E_i/K_i}))$ to $\mathbb{Z}/p^{e_i}\mathbb{Z}$ for $1 \le i \le m$. Under this identification, the map

$$\iota^1 : H^1(k,\hat{T}_{K/k}) \to H^1(k,\mathrm{I}_{K'/k}(\hat{T}_{E/K'})) = \bigoplus_{i\in\mathcal{I}} H^1(k,\mathrm{I}_{K_i/k}(\hat{T}_{E_i/K_i}))$$

sends $\mathbb{Z}/p^e\mathbb{Z}$ to $\bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z}$ by the natural projections. Therefore we can rewrite the exact sequence (5.3) as follows:

$$\mathbb{Z}/p^e\mathbb{Z} \xrightarrow{\iota^1} \bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z} \xrightarrow{\rho^1} H^1(k,\hat{S}_{K,K'}) \to H^2(k,\hat{T}_{K/k}), \tag{5.4}$$

where ι^1 is the natural projection from $\mathbb{Z}/p^e\mathbb{Z}$ to $\mathbb{Z}/p^{e_i}\mathbb{Z}$ for each i. Note that the image of ι^1 is the subgroup D, and we have the exact sequence

$$0 \to (\bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z})/D \xrightarrow{\rho^1} H^1(k,\hat{S}_{K,K'}) \to H^2(k,\hat{T}_{K/k}). \tag{5.5}$$

Let $a = (a_1, ..., a_m) \in \bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z}$ and $[a]$ be its image in $(\bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z})/D$. We claim that $\rho^1([a])$ is in $Ш^1(k,\hat{S}_{K,K'})$ if and only if $a \in G$.

We denote by a^v the image of a in $\bigoplus_{i=1}^{m} H^1(k_v,\mathrm{I}_{K_i^v/k_v}(\hat{T}_{E_i^v/K_i^v}))$, and by D_v the image of D in this sum.

By the exact sequence (5.5) over k_v, we have $\rho^1([a]) \in Ш^1(k,\hat{S}_{K,K'})$ if and only if $a^v \in D_v$ for all places $v \in \Omega_k$. Therefore, it suffices to prove that $a \in G$ if and only if $a^v \in D_v$ for all places $v \in \Omega_k$.

Suppose that $a \in G$, and let $v \in \Omega_k$. Then there exists $n \in \mathbb{Z}/p^{e_1}\mathbb{Z}$ such that $v \in \Omega(I_n(a))$. If $I_n(a) = \mathcal{I}$, then clearly $a \in D \subseteq G$. Suppose that $I_n(a) \neq \mathcal{I}$. This implies that for each $i \notin I_n(a)$ and for each place w of K_i above v, the étale algebra $K_i^w \otimes K$ is isomorphic to a product of field extensions of K_i^w of degree at most $\delta(n,i)$. Let $\delta_i = \delta(n,i) = \delta(n,a_i)$. Note that

$$H^1(k_v,\mathrm{I}_{K_i^v/k_v}(\hat{T}_{E_i^v/K_i^v})) = H^1(K_i^v,\hat{T}_{E_i^v/K_i^v}).$$

We have

$$H^1(K_i^v, \hat{T}_{E_i^v/K_i^v}) \simeq \underset{w|v}{\oplus} H^1(K_i^w, \hat{T}_{K_i^w \otimes K/K_i^w}) \simeq \underset{w|v}{\oplus} \mathbb{Z}/p^{e_{i,w}}\mathbb{Z},$$

where $e_{i,w} \leq \delta_i$, and the localization map $H^1(K_i, \hat{T}_{E_i/K_i}) \to H^1(K_i^v, \hat{T}_{E_i^v/K_i^v})$ is the canonical projection $\pi_{e_i,e_{i,w}}$ from $\mathbb{Z}/p^{e_i}\mathbb{Z}$ to each component $\mathbb{Z}/p^{e_{i,w}}\mathbb{Z}$. Since for all $i \notin I_n(a)$ we have $e_{i,w} \leq \delta_i$, and $\pi_{e_i,\delta_i}(a_i) = \pi_{e_1,\delta_i}(n)$, this implies that $a^v = (n, ..., n)^v$.

Suppose conversely that $a^v \in D_v$ for all $v \in \Omega_k$ and $a \notin G$. Then $a \notin D$, and there exists a place $v \in \Omega_k$ such that $v \notin \underset{n \in \mathbb{Z}/p^{e_1}\mathbb{Z}}{\cup} \Omega(I_n(a))$. Since $a^v \in D_v$, there exists $n' \in \mathbb{Z}/p^e\mathbb{Z}$ such that $a^v = (\iota^1(n'))_v$. Let $n = \pi_{e,e_1}(n')$. As $v \notin \Omega(I_n(a))$, there exists $i \notin I_n(a)$ and a place w of K_i above v such that $K_i^w \otimes K$ is isomorphic to a product of field extensions of degree $p^{e_{i,w}}$ of K_i^w, with $e_{i,w} > \delta_i$. Then by the definition of $\delta_i = \delta(n, a_i)$, we have $\pi_{e_i,e_{i,w}}(a_i) \neq \pi_{e_1,e_{i,w}}(n)$. Hence the localization a_i^v of the i-th coordinate of a is not equal to the localization of the i-th coordinate of $(n, ..., n)$, which is a contradiction. Our claim then follows. Therefore, we have $Ш^1(k, \hat{S}_{K,K'}) \simeq Ш(K, K')$.

Corollary 5.4. *Suppose that K/k is a cyclic extension of degree p^e, where p is a prime number. Then $Ш^1(k, T_{K,K'}) \simeq Ш(K, K')^*$.*

Proof. By Lemma 3.1, we have $Ш^1(k, T_{L/k}) \simeq Ш^2(k, S_{K,K'})$. Theorem 5.3 implies that $Ш^1(k, \hat{S}_{K,K'}) \simeq Ш(K, K')$. By Poitou-Tate duality, we have $Ш^2(k, S_{K,K'}) \simeq Ш^1(k, \hat{S}_{K,K'})^*$, hence the corollary is proved.

5.2. The group $Ш(K/K_0, K')$

Let K_0 be the unique subfield of K such that $[K_0 : k] = p^{e-1}$. The proof of the main theorem in the prime power case uses induction on e, and the comparison of the groups $Ш(K, K')$ and $Ш(K_0, K')$. We first define a homomorphism $F : Ш(K_0, K') \to Ш(K, K')$, and then determine the cokernel of F, denoted by $Ш(K/K_0, K')$.

Note that if $e = 1$, then $K_0 = k$, and hence $Ш(K_0, K')$ is trivial; in this case, $Ш(K/K_0, K')$ is the group $Ш(K, K')$ itself.

The homomorphism $Ш(K_0, K') \to Ш(K, K')$.

Recall that we have $K' = \prod_{i \in \mathcal{I}} K_i$, that $E_i = K \otimes K_i$, and that E_i is the product of copies of a cyclic extension of degree p^{e_i} of K_i. Set $E_i^0 = K_0 \otimes K_i$. Then E_i^0 also splits as a product of copies of a cyclic extension of K_i; let us denote by p^{f_i} the degree of this extension.

Proposition 5.5. *For all $i \in \mathcal{I}$, we have $f_i \leq e_i$. If moreover $e_i \neq 0$, then $e_i = f_i + 1$.*

This is an immediate consequence of the following proposition:

Proposition 5.6. *Let F/k be a field extension, and let $K \otimes_k F$ be a product of cyclic field extensions of F of degree p^{e_F}; let $K_0 \otimes_k F$ be a product of cyclic field extensions of F of degree p^{f_F}. Then we have*

(i) *$f_F \leq e_F$;*
(ii) *$f_F \geq e_F - 1$;*
(iii) *If $e_F \neq 0$, then $e_F = f_F + 1$.*

Proof. If n is a positive integer, let us denote by C_n the cyclic group of order n. Let us consider the homomorphisms

$$\Gamma_F \xrightarrow{\iota} \Gamma_k \xrightarrow{\phi_K} C_{p^e} \xrightarrow{\pi} C_{p^{e-1}} \to 1,$$

where ι is the inclusion of Γ_F into Γ_k, the homomorphism $\phi_K : \Gamma_k \to C_{p^e}$ corresponds to the cyclic extension K/k, and $\pi : C_{p^e} \to C_{p^{e-1}}$ is the quotient of C_{p^e} by its unique subgroup of order p. Note that the image of $\phi_K \circ \iota$ is the Galois group of the cyclic factors of $K \otimes_k F$, and hence is of order p^{e_F}; similarly, the image of $\pi \circ \phi_K \circ \iota$ is the Galois group of the cyclic factors of $K_0 \otimes_k F$, and hence is of order p^{f_F}. Therefore we have $f_F \leq e_F$. Moreover, if $e_F \neq 0$, then the image of $\phi_K \circ \iota$ contains the unique subgroup of order p of C_{p^e}, and hence $e_F = f_F + 1$. This completes the proof of the proposition.

For all $i \in \mathcal{I}$, let $F_i : \mathbb{Z}/p^{f_i}\mathbb{Z} \to \mathbb{Z}/p^{e_i}\mathbb{Z}$ be the inclusion of the subgroup of order p^{f_i} in the group $\mathbb{Z}/p^{e_i}\mathbb{Z}$, and set $F_{K/K_0} = F = \underset{i \in \mathcal{I}}{\oplus} F_i$.

Proposition 5.7. *The map $F : \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{f_i}\mathbb{Z} \to \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z}$ induces an injective homomorphism $F : Ш(K_0, K') \to Ш(K, K')$.*

Proof. Let us recall some notation from 5.1, for K and K_0: For all $i \in \mathcal{I}$ and for all positive integers d, we denote by $\Sigma(K)_i^d$ (respectively $\Sigma(K_0)_i^d$) the set of all places $v \in \Omega_k$ such that at each place w of K_i above v, the algebra $K \otimes K_i^w$ (respectively $K_0 \otimes K_i^w$) is isomorphic to a product copies of a cyclic extension of degree at most p^d of K_i^w. Recall that

$$G = G(K, K') = \{a \in \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z} \ \mid \bigcup_{n \in \mathbb{Z}/p^{e_1}\mathbb{Z}} \Omega(I_n(a)) = \Omega_k\},$$

and that D is the diagonal subgroup of G. Similarly, set

$$G_0 = G(K_0, K') = \{b \in \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{f_i}\mathbb{Z} \ \mid \bigcup_{n \in \mathbb{Z}/p^{f_1}\mathbb{Z}} \Omega(I_n(b)) = \Omega_k\},$$

and let D_0, be the diagonal subgroup of G_0. Then we have $Ш(K, K') = G/D$ and $Ш(K_0, K') = G_0/D_0$.

Let $b \in G_0$, and let us show that $F(b) \in G$. Let $v \in \Omega_k$. Then there exists $r \in \mathbb{Z}/p^{f_1}\mathbb{Z}$ such that $v \in \Sigma(K_0)_i^{\delta(r,i)}$ for all $i \in \mathcal{I}$ such that $i \notin I_r(b)$. Note that for all positive integers δ, we have $\Sigma(K_0)_i^{\delta} \subset \Sigma(K)_i^{\delta+1}$. Set $n = F_1(r) \in \mathbb{Z}/p^{e_1}\mathbb{Z}$; then we have $\delta(n, F_i(b_i)) = \delta(r, b_i) + 1$. Hence we have $v \in \Sigma(K)_i^{\delta(r,b_i)+1}$, and therefore $F(b) \in G$.

It is clear that F is injective.

Remark 5.8. For any subextension N/k of K/k, let $F_{K/N} : Ш(N, K') \to Ш(K, K')$ be the injective homomorphism obtained by successive applications of Proposition 5.7.

The group $Ш(K/K_0, K')$**.**

As we will see, the cokernel of F is isomorphic to the group $Ш(K/K_0, K')$, defined as follows:

For all $i \in \mathcal{I}$, set $r_i = \min\{1, e_i\}$. For all $c \in \underset{i\in\mathcal{I}}{\oplus} \mathbb{Z}/p^{r_i}\mathbb{Z}$ and $n \in \mathbb{Z}/p\mathbb{Z}$, set $I_n^1(c) = \{i \in \mathcal{I} \ \ |n \succeq c_i\}$. If $I_n^1(c) \neq \mathcal{I}$, set $\Omega(I_n^1(c)) = \underset{i \notin I_n^1(c)}{\cap} \Sigma_i$; if $I_n^1(c) = \mathcal{I}$, set $\Omega(I_n^1(c)) = \Omega_k$. Set

$$G(K/K_0, K') = \{c \in \underset{i\in\mathcal{I}}{\oplus} \mathbb{Z}/p^{r_i}\mathbb{Z} \ \ | \bigcup_{n \in \mathbb{Z}/p^{r_1}\mathbb{Z}} \Omega(I_n^1(c)) = \Omega_k\},$$

let $D(K/K_0, K')$ be the diagonal subgroup of $G(K/K_0, K')$, and set

$$Ш(K/K_0, K') = G(K/K_0, K')/D(K/K_0, K').$$

Lemma 5.9. *The projection* $\pi : \underset{i\in\mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z} \to \underset{i\in\mathcal{I}}{\oplus} \mathbb{Z}/p^{r_i}\mathbb{Z}$ *induces a homomorphism* $\pi : Ш(K, K') \to Ш(K/K_0, K')$.

Proof. Let $a \in G$, and set $\overline{a} = \pi(a)$. Let us show that $\overline{a} \in G(K/K_0, K')$. Let $v \in \Omega_k$; then there exists $s \in \mathbb{Z}/p^{e_1}\mathbb{Z}$ such that $v \in \Omega(I_s(a))$. Set $n = \pi_{e_1,1}(s)$, and let us prove that $v \in \Omega(I_n^1(\overline{a}))$. This is clear if $I_n^1(\overline{a}) = \mathcal{I}$. Suppose that $I_n^1(\overline{a}) \neq \mathcal{I}$. If $i \in \mathcal{I}$ is such that $i \notin I_n^1(\overline{a})$, then we have $i \notin I_s(a)$, and therefore $v \in \Sigma_i^{\delta(s,a_i)}$. Since $n = \pi_{e_1,1}(s)$ and $i \notin I_n^1(\overline{a})$, we have $\delta(s, a_i) = 0$, and hence $v \in \Sigma_i$. Therefore we have $\overline{a} \in G(K/K_0, K')$, as claimed, and this completes the proof of the lemma.

Proposition 5.10. *The sequence*

$$0 \to Ш(K_0, K') \xrightarrow{F} Ш(K, K') \xrightarrow{\pi} Ш(K/K_0, K') \to 0$$

is exact.

Proof. It is clear that F is injective, and that $\pi \circ F = 0$; it remains to check that π is surjective, and that $\mathrm{Ker}(\pi) \subset \mathrm{Im}(F)$. Let us check the second assertion first. Let $a \in Ш(K, K')$ be such that $\pi(a) = 0$. Then there exists $b \in \underset{i\in\mathcal{I}}{\oplus} \mathbb{Z}/p^{f_i}\mathbb{Z}$ such that

$F(b) = a$; let us check that $b \in Ш(K_0, K')$. Let $v \in \Omega_k$. Then there exists $n \in \mathbb{Z}/p^{e_1}\mathbb{Z}$ such that $v \in \Omega(I_n(a))$. If $i \in I_n(a)$, then we have $\pi_{e_1,e_i}(n) = a_i$. Since $a_i = F_i(b_i)$, this implies that there exists $r \in \mathbb{Z}/p^{f_1}\mathbb{Z}$ such that $n = F_1(r)$ and $I_n(a) = I_r(b)$. Let us show that $v \in \Omega(I_r(b))$. For all $i \in \mathcal{I}$ such that $i \notin I_n(a)$, we have $v \in \Sigma(K)_i^{\delta(n,a_i)}$. Note that $\delta(n, a_i) = \delta(r, b_i) + 1$ and $[K : K_0] = p$. Hence $v \in \Sigma(K)_i^{\delta(n,a_i)}$ implies that $v \in \Sigma(K_0)_i^{\delta(r,b_i)}$. Therefore we have $v \in \Omega(I_r(b))$, as claimed, and this implies that $b \in Ш(K_0, K')$. Let us now prove that π is surjective. Let $\overline{a} \in Ш(K/K_0, K')$. For each $n \in \mathbb{Z}/p\mathbb{Z}$, let us fix a lifting $r(n) \in \mathbb{Z}/p^{e_1}\mathbb{Z}$. If $i \in I_n^1(\overline{a})$, set $a_i = \pi_{e_1,e_i}(r(n))$. Let us check that $a_i \in \mathbb{Z}/p^{e_i}\mathbb{Z}$ is well-defined. Suppose that $n_1, n_2 \in \mathbb{Z}/p\mathbb{Z}$ are such that $i \in I_{n_1}^1(\overline{a}) \cap I_{n_2}^1(\overline{a})$; then we have $\pi_{1,r_i}(n_1) = \pi_{1,r_i}(n_2)$. If $n_1 \neq n_2$, then this implies that $r_i = 0$, hence $e_i = 0$. We have $\pi_{e_1,e_i}(r(n_1)) = \pi_{e_1,e_i}(r(n_2))$ in this case, hence a_i is well-defined. Let us check that $a \in Ш(K, K')$. Since $\overline{a} \in Ш(K/K_0, K')$, we have $\bigcup\limits_{n \in \mathbb{Z}/p^{r_1}\mathbb{Z}} \Omega(I_n^1(\overline{a})) = \Omega_k$. Let $v \in \Omega_k$; then there exists $n \in \mathbb{Z}/p\mathbb{Z}$ such that $v \in \Omega(I_n^1(\overline{a}))$. Let $r = r(n)$; we claim that $v \in \Omega(I_r(a))$. If $I_n^1(\overline{a}) = \mathcal{I}$, then we have $I_r(a) = \mathcal{I}$, and the claim is clear. Suppose that $I_n^1(\overline{a}) \neq \mathcal{I}$. If $i \notin I_r(a)$, then we have $i \notin I_n^1(\overline{a})$ by construction, hence $v \in \Sigma_i$. Since $\Sigma_i \subset \Sigma_i(K)^{\delta(r,a_i)}$, the claim follows. This completes the proof of the proposition.

The group $Ш(K/K_0, K')$ and partitions.

In this section we give some properties of $G(K/K_0, K')$ in terms of partitions of $\mathcal{I}$. This will be useful in the proof of the main theorem (Theorem 7.1).

Lemma 5.11. *The set $G(K/K_0, K')$ is in bijective correspondence with the partitions $(J_0, ..., J_{p-1})$ of the set $\{i \in \mathcal{I} \mid r_i = 1\}$ such that $\bigcup\limits_{n \in \mathbb{Z}/p\mathbb{Z}} \Omega(J_n) = \Omega_k$.*

Proof. Recall that we have $r_i = 0$ or 1. Set $\mathcal{I}' = \{i \in \mathcal{I} \mid r_i = 1\}$. Let $a \in G(K/K_0, K')$, and set $I^1(a) \cap \mathcal{I}' = (I_0^1(a) \cap \mathcal{I}', ..., I_{p-1}^1(a) \cap \mathcal{I}')$; note that $I^1(a) \cap \mathcal{I}'$ is a partition of $\mathcal{I}'$. Hence the set $G(K/K_0, K')$ is then in bijective correspondence with the partitions $(J_0, ..., J_{p-1})$ of $\mathcal{I}'$ such that $\bigcup\limits_{n \in \mathbb{Z}/p\mathbb{Z}} \Omega(J_n) = \Omega_k$, as claimed.

In the sequel, we identify $G(K/K_0, K')$ with the set of these partitions. We also note a consequence for the case where K is of degree p, in other words, if $e = 1$. If K/k is of prime degree, then either E_i is a field extension of K_i, or E_i is a product of copies of K_i. Let J be the subset of I such that E_i is a field extension of K_i if $i \in J$, and that E_i is a product of copies of K_i if $i \notin J$.

Lemma 5.12. *Assume that K/k is a degree p extension. Then $G(K, K')$ is in bijective correspondence with the partitions $(J_0, ..., J_{p-1})$ of J such that $\bigcup\limits_{n \in \mathbb{Z}/p\mathbb{Z}} \Omega(J_n) = \Omega_k$.*

Proof. Since $e = 1$, we have $K_0 = k$ and $G(K/K_0, K') = G(K, K')$. Hence the lemma follows from Lemma 5.11.

Let K_{prim} be the unique subfield of K of degree p over k.

Proposition 5.13. *The group* $Ш(K/K_0, K')$ *is a subgroup of* $Ш(K_{\mathrm{prim}}, K')$.

Proof. J be the subset of $i \in \mathcal{I}$ such that $K_{\mathrm{prim}} \otimes_k K_i$ is a field extension. Then $G(K_{\mathrm{prim}}, K')$ is in bijection with the set of partitions $(I_0, \dots, I_{p-1})$ of J such that $\underset{n\in\mathbb{Z}/p\mathbb{Z}}{\cup} \Omega_{K_{\mathrm{prim}}}(I_n) = \Omega_k$, where $\Omega_{K_{\mathrm{prim}}}(I_n) = \cap_{i\notin I_n} \Sigma_i(K_{\mathrm{prim}})$ (see Lemma 5.12).

Note that $J = \{i \in \mathcal{I} \mid r_i = 1\}$. Hence by Lemma 5.11, the set $G(K/K_0, K')$ is in bijection with the set of partitions $(I_0, \dots, I_{p-1})$ of J such that $\underset{n\in\mathbb{Z}/p\mathbb{Z}}{\cup} \Omega_K(I_n) = \Omega_k$, where $\Omega_K(I_n) = \cap_{i\notin I_n} \Sigma_i(K)$.

Note that $\Sigma_i(K_{\mathrm{prim}}) \subset \Sigma_i(K)$ for all $i \in \mathcal{I}$. Hence $G(K/K_0, K') \subset G(K_{\mathrm{prim}}, K')$, and this implies that $Ш(K/K_0, K')$ is a subgroup of $Ш(K_{\mathrm{prim}}, K')$.

Proposition 5.14. *If* $Ш(K_{\mathrm{prim}}, K') = 0$, *then* $Ш(K, K') = 0$.

Proof. By Proposition 5.13, we have $Ш(K/K_0, K') = 0$; hence Proposition 5.10 implies that $Ш(K, K') = Ш(K_0, K')$. Repeating this argument, we see that $Ш(K, K') = Ш(K_{\mathrm{prim}}, K')$. But $Ш(K_{\mathrm{prim}}, K') = 0$ by hypothesis, hence $Ш(K, K') = 0$, as claimed.

The following lemma will be useful in the sequel.

Lemma 5.15. *Let* $(I_0, \dots, I_{p-1}) \in G(K/K_0, K')$, *and let* r, r' *be two distinct elements of* $\mathbb{Z}/p\mathbb{Z}$. *Set* $J_r = I_r$, $J_{r'} = \underset{n\neq r}{\cup} I_n$, *and* $J_n = \emptyset$ *if* $n \neq r, r'$. *Then* $(J_0, \dots, J_{p-1}) \in G(K/K_0, K')$. *If moreover* $(I_0, \dots, I_{p-1}) \notin D(K/K_0, K')$ *and* $I_r \neq \emptyset$, *then* $(J_0, \dots, J_{p-1}) \notin D(K/K_0, K')$.

Proof. Let us show that $\Omega(J_r) \cup \Omega(J_{r'}) = \Omega_k$. Let $v \in \Omega_k$ be such that $v \notin \Omega(J_r)$. Since we have $\underset{n\in\mathbb{Z}/p\mathbb{Z}}{\cup} \Omega(I_n) = \Omega_k$, there exists $n(v) \in \mathbb{Z}/p\mathbb{Z}$ with $n(v) \neq r$ such that $v \in \Omega(I_{n(v)})$. Since $n(v) \neq r$, we have $\Omega(I_{n(v)}) \subset \underset{i\in I_r}{\cap} \Sigma_i = \Omega(J_{n'})$. Therefore we have $\Omega(J_r) \cup \Omega(J_{r'}) = \Omega_k$, and hence $(J_0, \dots, J_{p-1}) \in G(K/K_0, K')$.

Let us prove the second statement. If $(J_0, \dots, J_{p-1}) \in D(K/K_0)$, then either $J_r = \mathcal{I}'$ or $J_{r'} = \mathcal{I}'$; we have $I_r = \mathcal{I}'$ in the first case, hence $(I_0, \dots, I_{p-1}) \in D(K/K_0, K')$, and $I_r = \emptyset$ in the second case. This completes the proof of the lemma.

5.3. The general case

Recall that K/k is a cyclic extension of degree d, and let $\mathcal{P}$ be the set of prime numbers dividing d. For all $p \in \mathcal{P}$, let $K(p)$ be the largest subfield of K such that $[K(p) : k]$ is a power of p and set $d(p) = [K(p) : k]$. Set

$$\text{Ш}(K, K') = \underset{p\in\mathcal{P}}{\oplus} \text{Ш}(K(p), K').$$

Proposition 5.16. *We have* $\text{Ш}^1(k, \hat{S}_{K,K'}) \simeq \text{Ш}(K, K')$.

Proof. By 5.3 we have $\text{Ш}^1(k, \hat{S}_{K(p),K'}) \simeq \text{Ш}(K(p), K')$, hence it suffices to show that $\text{Ш}^1(k, \hat{S}_{K,K'}) \simeq \prod_{p\in\mathcal{P}} \text{Ш}^1(k, \hat{S}_{K(p),K'})$. For every $p \in \mathcal{P}$, set $E(p) = K(p) \otimes_k K'$ and $L(p) = K(p) \times K'$. The inclusion $K(p) \to K$ induces maps $\epsilon_p : T_{K(p)/k} \to T_{K/k}$, $\epsilon_p : T_{E(p)/K'} \to T_{E/K'}$ and $\epsilon_p : S_{K(p),K'} \to S_{K,K'}$. We have the commutative diagram, coming from cohomology exact sequences associated to the dual sequences of (2.1):

$$\begin{tikzcd}
H^1(k, \hat{T}_{K/k}) \arrow[r, "\iota^1"] \arrow[d, "\oplus\hat{\epsilon}_p^1"'] & H^1(k, \mathrm{I}_{K'/k}(\hat{T}_{E/K'})) \arrow[r, "\rho^1"] \arrow[d, "\oplus\hat{\epsilon}_p^1"'] & H^1(k, \hat{S}_{K,K'}) \arrow[r] \arrow[d, "\oplus\hat{\epsilon}_p^1"'] & \ldots \\
\underset{p\in\mathcal{P}}{\oplus} H^1(k, \hat{T}_{K(p)/k}) \arrow[r, "\iota^1"] & \underset{p\in\mathcal{P}}{\oplus} H^1(k, \mathrm{I}_{K'/k}(\hat{T}_{E(p)/K'})) \arrow[r, "\rho^1"] & \underset{p\in\mathcal{P}}{\oplus} H^1(k, \hat{S}_{K(p),K'}) \arrow[r] & \ldots
\end{tikzcd} \tag{5.6}$$

where the vertical maps are induced by the maps ϵ_p. Set $\hat{\epsilon}^1 = \oplus\hat{\epsilon}_p^1$.

For all $i \in \mathcal{I}$, let M_i be a cyclic extension of K_i such that E_i is isomorphic to a product of copies of M_i, and let $d_i = [M_i : K_i]$. If p is a prime divisor of $[K : k]$, set $E_i(p) = K(p) \otimes_k K_i$, and let $M_i(p)$ be a cyclic extension of K_i such that $E_i(p)$ is isomorphic to a product of copies of $M_i(p)$; set $d_i(p) = [M_i(p) : K_i]$. Note that $d_i(p)$ is the highest power of p dividing d_i, and that $d_i = \prod_{p\in\mathcal{P}} d_i(p)$.

Note that $H^1(k, \mathrm{I}_{K_i/k}(\hat{T}_{E_i/K_i})) \simeq H^1(K_i, \hat{T}_{E_i/K_i})$, and that by Lemma 1.1 (ii), we have $H^1(K_i, \hat{T}_{E_i/K_i}) \simeq H^1(K_i, \hat{T}_{M_i/K_i})$. Moreover, by Lemma 1.2, we have $H^1(K_i, \hat{T}_{M_i/K_i}) \simeq \mathbb{Z}/d_i\mathbb{Z}$. Similarly, we have $H^1(k, \mathrm{I}_{K_i(p)/k}(\hat{T}_{E_i(p)/K_i})) \simeq \mathbb{Z}/d_i(p)\mathbb{Z}$. Note that the morphism ϵ_p^1 restricted to each $H^1(k, \mathrm{I}_{K_i/k}(\hat{T}_{E_i/K_i}))$

$$\hat{\epsilon}_p^1 : H^1(k, \mathrm{I}_{K_i/k}(\hat{T}_{E_i/K_i})) \simeq \mathbb{Z}/d_i\mathbb{Z} \to H^1(k, \mathrm{I}_{K_i/k}(\hat{T}_{E_i(p)/K_i})) \simeq \mathbb{Z}/d_i(p)\mathbb{Z}$$

is the canonical projection $\mathbb{Z}/d_i\mathbb{Z} \to \mathbb{Z}/d_i(p)\mathbb{Z}$. Hence by the Chinese reminder theorem, the morphism $\hat{\epsilon}^1$ restricted to each $H^1(k, \mathrm{I}_{K_i/k}(\hat{T}_{E_i/K_i}))$

$$\underset{p\in\mathcal{P}}{\oplus} \hat{\epsilon}_p^1 : H^1(k, \mathrm{I}_{K_i/k}(\hat{T}_{E_i/K_i})) \to \underset{p\in\mathcal{P}}{\oplus} H^1(k, \mathrm{I}_{K_i/k}(\hat{T}_{E_i(p)/K_i}))$$

is an isomorphism. Similarly,

$$\underset{p\in\mathcal{P}}{\oplus} \hat{\epsilon}_p^1 : H^1(k, \hat{T}_{K/k}) \simeq \mathbb{Z}/d\mathbb{Z} \to \underset{p\in\mathcal{P}}{\oplus} H^1(k, \hat{T}_{K(p)/k}) \simeq \underset{p\in\mathcal{P}}{\oplus} \mathbb{Z}/d(p)\mathbb{Z}$$

is also an isomorphism.

By Corollary 3.3, we have $Ш^2(k, \hat{T}_{K/k}) = 0$ and $Ш^2(k, \hat{T}_{K(p)/k}) = 0$, hence $Ш^1(k, \hat{S}_{K,K'})$ and $Ш^1(k, \hat{S}_{K(p),K'})$ are in the image of the maps ρ^1. Now we show that $\hat{\epsilon}^1 : Ш^1(k, \hat{S}_{K,K'}) \to \bigoplus_{p\in\mathcal{P}} Ш^1(k, \hat{S}_{K(p),K'})$ is injective. Let $\beta \in Ш^1(k, \hat{S}_{K,K'})$. Suppose that $\hat{\epsilon}^1(\beta) = 0$. As $Ш^1(k, \hat{S}_{K,K'})$ is in the image of ρ^1, there is $\gamma \in H^1(k, \mathrm{I}_{K'/k}(\hat{T}_{E/K'}))$ such that $\rho^1(\gamma) = \beta$. By the commutativity of the diagram, we have $\rho^1(\hat{\epsilon}^1(\gamma)) = \hat{\epsilon}^1(\rho^1(\gamma)) = 0$. Hence there is $\zeta \in \bigoplus_{p\in\mathcal{P}} H^1(k, \hat{T}_{K(p)/k})$ such that $\iota^1(\zeta) = \hat{\epsilon}^1(\gamma)$. Then $\hat{\epsilon}^1 \circ \iota^1 \circ (\hat{\epsilon}^1)^{-1}(\zeta) = \hat{\epsilon}^1(\gamma)$. As

$$\hat{\epsilon}^1 : H^1(k, \mathrm{I}_{K'/k}(\hat{T}_{E/K'})) \to \bigoplus_{p\in\mathcal{P}} H^1(k, \mathrm{I}_{K'/k}(\hat{T}_{E(p)/K'}))$$

is an isomorphism, we have $\iota^1 \circ (\hat{\epsilon}^1)^{-1}(\zeta) = \gamma$ and hence $\beta = \rho^1(\gamma) = 0$. This proves the injectivity.

As $Ш^2(k, \hat{T}_{K(p)/k}) = 0$ by Corollary 3.3, the group $Ш^1(k, \hat{S}_{K(p),K'})$ is in the image of the maps ρ^1 for all $p \in \mathcal{P}$. Since $H^1(k, \mathrm{I}_{K_i/k}(\hat{T}_{E_i/K_i})) \to \bigoplus_{p\in\mathcal{P}} H^1(k, \mathrm{I}_{K_i/k}(\hat{T}_{E_i(p)/K_i}))$ is an isomorphism, we see that

$$\hat{\epsilon}^1 : Ш^1(k, \hat{S}_{K,K'}) \to \bigoplus_{p\in\mathcal{P}} Ш^1(k, \hat{S}_{K(p),K'})$$

is surjective. This completes the proof of the proposition.

Note that the proposition, together with Lemma 3.1, implies that $Ш(K, K')$ does not depend on the decomposition of L as $L = K \times K'$. We will also use the notation $Ш(L) = Ш(K, K')$, where $L = K \times K'$ is any decomposition of L with K/k a cyclic extension.

In summary, we proved

Corollary 5.17. *We have* $Ш(L)^* \simeq Ш^1(k, T_{L/k})$.

Example 5.18. Let p and q be two distinct odd prime numbers, with $p > q$. For all positive integers n, let ζ_n be a primitive nth root of unity. Let $k = \mathbf{Q}$, and

$$L = \mathbb{Q}(\zeta_{p^2}) \times \mathbb{Q}(\zeta_{pq}) \times \mathbb{Q}(\zeta_{q^2}).$$

Since $\mathbb{Q}(\zeta_{p^2})$ and $\mathbb{Q}(\zeta_{q^2})$ are both cyclic, we can determine $Ш(L)$ in two ways; this shows that the order of $Ш(L)$ divides $p - 1$, and that

$$Ш(L) = Ш(\mathbb{Q}(\zeta_p) \times \mathbb{Q}(\zeta_{pq}) \times \mathbb{Q}(\zeta_{q^2})).$$

But since $\mathbb{Q}(\zeta_p)$ is a subfield of $\mathbb{Q}(\zeta_{pq})$, we have $Ш(\mathbb{Q}(\zeta_p)\times\mathbb{Q}(\zeta_{pq})\times\mathbb{Q}(\zeta_{q^2})) = Ш(\mathbb{Q}(\zeta_p)\times \mathbb{Q}(\zeta_{q^2}))$. Note that by Proposition 4.1 we have $Ш(\mathbb{Q}(\zeta_p) \times \mathbb{Q}(\zeta_{q^2})) = 0$, hence we have

$$Ш(L) = 0.$$

6. The Brauer-Manin map

We keep the notation of the previous section: in particular, $L = K \times K'$, where K is a cyclic extension of k of degree d, K' is an étale k-algebra, and $E = K \otimes K'$. We write $K' = \prod_{i \in \mathcal{I}} K_i$, where the K_i/k are field extensions, and $E = \prod_{i \in \mathcal{I}} E_i$, with $E_i = K \otimes K_i$. The group $Ш(L) = Ш(K, K')$ is defined in the previous section.

Let $c \in k^\times$ and recall that X_c is the affine k-variety defined by the equation

$$N_{L/k}(t) = c.$$

Assume that $X_c(k_v) \neq \emptyset$ for all $v \in \Omega_k$. In the following, we define a homomorphism $\alpha_c : Ш(L) \to \mathbb{Q}/\mathbb{Z}$ such that $X_c(k) \neq \emptyset$ if and only if $\alpha_c = 0$; the map α_c will be called the *Brauer-Manin map* associated to c. We choose this terminology, because this map is an analog of the map given by the Brauer-Manin pairing on X_c.

6.1. Local points

We start with some preliminary results. We are assuming that $\prod X_c(k_v) \neq \emptyset$; as we will see, this set contains elements satisfying certain finiteness conditions. More precisely, we introduce the notion of *local points* - these can be thought of as adelic points of X_c.

We first recall the notion of cyclic algebra. Let us choose a generator g of the cyclic group $\mathrm{Gal}(K/k)$, and let $\phi : \Gamma_k \to \mathbb{Z}/d\mathbb{Z}$ be given by the composition of the isomorphism $\mathrm{Gal}(K/k) \to \mathbb{Z}/d\mathbb{Z}$ sending g to 1 with the surjection $\Gamma_k \to \mathrm{Gal}(K/k)$. Let us consider the exact sequence $0 \to \mathbb{Z} \xrightarrow{\times d} \mathbb{Z} \to \mathbb{Z}/d\mathbb{Z} \to 0$, and let $\delta : H^1(k, \mathbb{Z}/d\mathbb{Z}) \to H^2(k, \mathbb{Z})$ be the connecting homomorphism of the associated cohomology exact sequence. If $c \in k^\times$, let us denote by (c) the corresponding element of $H^0(k, \mathbb{G}_m)$. The cup product $\delta(\phi).(c)$ is an element of $H^2(k, \mathbb{G}_m)$, and via the identification $H^2(k, \mathbb{G}_m) \simeq \mathrm{Br}(k)$ it is mapped to the class of the cyclic algebra defined by K and c (see for instance [6], Proposition 4.7.3). We denote this cyclic algebra by (K, c).

The first observation is the following:

Lemma 6.1. *Suppose that E_i is isomorphic to a product of copies of a field M_i, and set $[M_i : K_i] = d_i$. Then for any $x \in K_i^\times$, the order of the cyclic algebra $(K, N_{K_i/k}(x))$ divides d_i. In particular, if $d_i = 1$, then for any $x \in K_i^\times$, the algebra $(K, N_{K_i/k}(x))$ splits.*

Proof. Given $x \in K_i^\times$, consider the class of the cyclic algebra $(M_i, x) = \delta(\phi|_{K_i}).(x)$, where $\phi|_{K_i} : \Gamma_{K_i} \to \mathbb{Z}/d\mathbb{Z}$ is the restriction of ϕ to Γ_{K_i}. Let r be the order of (M_i, x) in $\mathrm{Br}(K_i)$. Since M_i is of degree d_i over K_i, we have $r | d_i$. By the projection formula ([6] Prop. 3.4.10), the corestriction of (M_i, x) is $(K, N_{K_i/k}(x))$. Therefore the order of $(K, N_{K_i/k}(x))$ divides d_i.

Let $x = (x^v) \in \prod_{v \in \Omega_k} X_c(k_v)$, and let us write $x^v = (x_0^v, x_1^v, \dots, x_m^v)$, with $x_0^v \in K^v$ and $x_i^v \in K_i^v$ for $i \in \mathcal{I}$. Let us consider the invariant map $\mathrm{inv} : \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}$ and set $b_i^v(x) = b_i^v(x_i^v) = \mathrm{inv}(K^v, N_{K_i^v/k_v}(x_i^v)) \in \frac{1}{d_i}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$. Note that if d_i is odd, then $b_i^v(x) = 0$ for all infinite places $v \in \Omega_k$.

We say that $x = (x_i^v) \in \prod_{v \in \Omega_k} X_c(k_v)$ is a *local point* of X_c if for each $i \in \mathcal{I}$, we have $b_i^v(x) = 0$ for almost all $v \in \Omega_k$. The following lemma implies the existence of local points whenever $\prod_{v \in \Omega_k} X_c(k_v) \neq \emptyset$.

Lemma 6.2. *Assume that* $\prod_{v \in \Omega_k} X_c(k_v) \neq \emptyset$. *Then there exists*

$$x = (x_i^v) \in \prod_{v \in \Omega_k} X_c(k_v)$$

such that $b_i^v(x) = 0$ *for almost all* $v \in \Omega_k$, *and for all* $i \in \mathcal{I}$.

Proof. For each $v \in \Omega_k$ such that $(K, c)^v$ is split, there exists $x_0^v \in K^v$ such that $N_{K^v/k_v}(x_0^v) = c$. Then $x = (x_0^v, 1, ..., 1)$ is a k_v-point of X_c, and $b_i^v(x) = 0$ for all $i \in \mathcal{I}$. Since $(K, c)^v$ is split for almost all places $v \in \Omega_k$, the lemma follows.

We now prove some properties of local points which will be used later. The next lemma is an analog of the classical reciprocity formula that appears in the classical Brauer-Manin obstruction.

Lemma 6.3. *Let* $x = (x_i^v) \in \prod_{v \in \Omega_k} X_c(k_v)$ *be a local point of* X_c. *Then we have*

$$\sum_{v \in \Omega_k} \sum_{i \in \mathcal{I}} b_i^v(x) = 0.$$

Proof. Let us write $x^v = (x_0^v, x_1^v, \dots, x_m^v)$, with $x_0^v \in K^v$ and $x_i^v \in K_i^v$ for $i \in \mathcal{I}$. For all $i \in \mathcal{I}$, set $y_i^v = N_{L_i^v/k_v}(x_i^v)$. Set $y_0^v = N_{K^v/k_v}(x_0^v)$, and note that $y_0^v \prod_{i \in \mathcal{I}} y_i^v = c$. We have

$$\sum_{i \in \mathcal{I}} b_i^v(x) = \sum_{i \in \mathcal{I}} \mathrm{inv}(K^v, y_i^v) = \mathrm{inv}(K^v, \prod_{i \in \mathcal{I}} y_i^v) = \mathrm{inv}(K^v, c/y_0^v) = \mathrm{inv}(K^v, c).$$

Since $c \in k^\times$, the Brauer-Hasse-Noether Theorem implies that $\sum_{v \in \Omega_k} \mathrm{inv}(K^v, c) = 0$. Hence we have $\sum_{v \in \Omega_k} \sum_{i \in \mathcal{I}} b_i^v(x) = 0$, as claimed.

Lemma 6.4. *Let* $x = (x_i^v)$ *be a local point of* X_c, *and set* $b_i^v = b_i^v(x) = \mathrm{inv}(K^v, N_{K_i^v/k_v}(x_i^v))$. *For all* $i \in \mathcal{I}$, *let* $\tilde{x}_i^v \in K_i^v$ *and set*

$$\tilde{b}_i^v = \mathrm{inv}(K^v, N_{K_i^v/k_v}(\tilde{x}_i^v)).$$

Suppose that for all $i \in \mathcal{I}$ we have $\tilde{b}_i^v = 0$ for almost all $v \in \Omega_k$, and that $\sum\limits_{i\in\mathcal{I}} b_i^v = \sum\limits_{i\in\mathcal{I}} \tilde{b}_i^v$ for all $v \in \Omega_k$. Then for all $v \in \Omega_k$, there exists $\tilde{x}_0^v \in K^v$ such that $\tilde{x} = (\tilde{x}_i^v)$ is a local point of X_c.

Proof. Let $\tilde{y}_i^v = N_{K_i^v/k_v}(\tilde{x}_i^v)$ and $y_i^v = N_{K_i^v/k_v}(x_i^v)$. Since $\sum\limits_{i\in\mathcal{I}} b_i^v = \sum\limits_{i\in\mathcal{I}} \tilde{b}_i^v$, the algebras $(K^v, \prod\limits_{i\in\mathcal{I}} y_i^v)$ and $(K^v, \prod\limits_{i\in\mathcal{I}} \tilde{y}_i^v)$ are isomorphic, hence there exists some $z \in K^v$ such that $(\prod\limits_{i\in\mathcal{I}} y_i^v)(\prod\limits_{i\in\mathcal{I}} \tilde{y}_i^v)^{-1} = N_{K^v/k_v}(z)$. Therefore $(x_0^v z, \tilde{x}_1^v, ..., \tilde{x}_m^v)$ is a k_v-point of X_c.

Lemma 6.5. *Let $x = (x_i^v)$ be a local point of X_c, and set $b_i^v = b_i^v(x) = \mathrm{inv}(K^v, N_{K_i^v/k_v}(x_i^v))$. Suppose that for all $i \in \mathcal{I}$, we have $\sum\limits_{v\in\Omega_k} b_i^v = 0$. Then X_c has a k-point.*

Proof. By the Brauer-Hasse-Noether Theorem, for every $i \in \mathcal{I}$ there exists a central simple algebra A_i over k such that $\mathrm{inv}(A_i) = b_i^v$ for all $v \in \Omega_k$. Set $y_i^v = N_{K_i^v/k_v}(x_i^v)$. Since (K^v, y_i^v) splits over K^v for all v, the algebra A_i also splits over K. Hence there exists $\tilde{y}_i \in k$ such that A_i is Brauer equivalent to $(K, \tilde{y}_i)$ (see [6] Cor. 4.7.6). Since $(K, \prod\limits_{i\in\mathcal{I}} \tilde{y}_i)_v \simeq (K^v, \prod\limits_{i\in\mathcal{I}} y_i^v) \simeq (K, c)_v$, the Brauer-Hasse-Noether Theorem implies that $(K, \prod\limits_{i\in\mathcal{I}} \tilde{y}_i) \simeq (K, c)$, and hence $\prod\limits_{i\in\mathcal{I}} \tilde{y}_i = cN_{K/k}(w)$ for some $w \in K^\times$. Moreover, we claim that the element $\tilde{y}_i$ belongs to the group $N_{K/k}(K^\times)N_{K_i/k}(K_i^\times)$. To see this, we note that

$$(K, \tilde{y}_i)_v = (K, y_i^v) = (K, N_{K_i^v/k_v}(x_i^v)).$$

Hence we have $\tilde{y}_i \in N_{K/k}(J_K)N_{K_i/k}(J_i)$ where J_i is the idèle group of K_i, for all $i \in \mathcal{I}$, and J_K is the idèle group of K. By Proposition 4.1, we have $\tilde{y}_i = N_{K/k}(w_i)N_{K_i/k}(z_i)$ for some $w_i \in K^\times$ and $z_i \in K_i^\times$. Therefore $\prod\limits_{i\in\mathcal{I}} \tilde{y}_i = \prod\limits_{i\in\mathcal{I}} N_{K/k}(w_i)N_{K_i/k}(z_i) = cN_{K/k}(w)$ and $(w^{-1}\prod\limits_{i\in\mathcal{I}} w_i, z_1, ..., z_m)$ is a k-point of X_c. This completes the proof of the lemma.

6.2. Brauer-Manin map - the prime power degree case

Now suppose that K is a cyclic extension of degree $d = p^e$, where p is a prime. Let $x = (x_i^v) \in \prod\limits_{v\in\Omega_k} X_c(k_v)$ be a local point of X_c. Let M_i be a cyclic extension of K_i such that the algebra E_i is isomorphic to a product of copies of M_i; then the degree of M_i is p^{e_i} for some $0 \le e_i \le e$. Without loss of generality, we assume that $(e_1, ..., e_m)$ is a decreasing sequence. Let us define

$$\alpha_c : \text{Ш}(K, K') \to \mathbb{Q}/\mathbb{Z}$$

by $\alpha_c(a_1, ..., a_m) = \sum\limits_{v \in \Omega_k} \sum\limits_{i \in \mathcal{I}} a_i b_i^v(x)$, where $(a_1, ..., a_m) \in G \subseteq \bigoplus\limits_{i \in \mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z}$. Note that by Lemma 6.1, we have $b_i^v(x) \in \frac{1}{p^{e_i}}\mathbb{Z}/\mathbb{Z}$. Hence $a_i b_i^v(x)$ is well-defined. Moreover, by Lemma 6.3, the map α_c vanishes on the subgroup D of G; hence, the map $\alpha_c : Ш(K, K') \to \mathbb{Q}/\mathbb{Z}$ is well-defined.

Note that the map α_c is an analogue of the map given by the Brauer-Manin pairing. In the following we show that α_c has a classical property of the Brauer-Manin pairing.

Proposition 6.6. *The map $\alpha_c : Ш(K, K') \to \mathbb{Q}/\mathbb{Z}$ is independent of the choice of the local point $x = (x_i^v)$.*

Proof. We use the notation of section 5.1. Let $a \in G$ and $I(a) = (I_0, ..., I_{p^{e_1}-1})$. If $a \in D$, then by Lemma 6.3, we have $\alpha_c(a) = 0$. In the following, we assume that $a \notin D$.

By the definition of G, we have $\Omega(I_0) \cup ... \cup \Omega(I_{p^{e_1}-1}) = \Omega_k$. Given a place $v \in \Omega_k$, there exists $n(v) \in \mathbb{Z}/p^{e_1}\mathbb{Z}$ such that $v \in \Omega(I_{n(v)})$. Set $\delta_i = \delta(n(v), a_i)$ and let $K_i^v = \prod\limits_{w|v} K_i^w$, where K_i^w are field extensions of k_v. Then for all $i \notin I_{n(v)}$, the algebra E_i^v is isomorphic to a products of field extensions of K_i^w of degree at most p^{δ_i}. Set $b_i^v = b_i^v(x)$; by Lemma 6.1, we have $b_i^v \in \frac{1}{p^{\delta_i}}\mathbb{Z}/\mathbb{Z}$. By the definition of δ_i, we have $\pi_{e_i,\delta_i}(a_i) = \pi_{e_1,\delta_i}(n(v))$. Hence for $i \notin I_{n(v)}$, we have

$$a_i b_i^v = \pi_{e_i,\delta_i}(a_i) b_i^v = \pi_{e_1,\delta_i}(n(v)) b_i^v = n(v) b_i^v.$$

Hence for all $v \in \Omega_k$, we have

$$\sum_{i \in \mathcal{I}} a_i b_i^v = n(v) \sum_{i \in \mathcal{I}} b_i^v = n(v) \mathrm{inv}(K, c)_v,$$

which is again independent of the x_i^v's. Therefore, the map α_c is independent of the choice of the local point, and the proposition is proved.

The map $\alpha_c : Ш(K, K') \to \mathbb{Q}/\mathbb{Z}$ will be called the *Brauer-Manin map* for X_c.

Let K_0 be the unique subfield of K such that $[K_0 : k] = p^{e-1}$, and set $L_0 = K_0 \times K'$. If $c \in k^\times$, let X_c^0 be the affine k-variety determined by $N_{L_0/k}(t) = c$. There is a natural map $\rho : X_c \to X_c^0$ defined as $\rho(x_0, ..., x_m) = (N_{K/K_0}(x_0), x_1, ..., x_m)$.

If $X_c^0(k_v) \neq \emptyset$ for all $v \in \Omega_k$, we denote by $\alpha_c^0 : Ш(K_0, K') \to \mathbb{Q}/\mathbb{Z}$ the corresponding Brauer-Manin map.

If $t_i \in K_i^v$, set

$$b_i^v(K, t_i) = \mathrm{inv}(K^v, N_{K_i^v/k_v}(t_i)), \text{ and } b_i^v(K_0, t_i) = \mathrm{inv}(K_0^v, N_{K_i^v/k_v}(t_i)).$$

Recall that a local point of X_c is $x = (x_i^v) \in \prod\limits_{v \in \Omega_k} X_c(k_v)$ such that for each $i \in \mathcal{I}$, we have $b_i^v(K, x_i^v) = 0$ for almost all $v \in \Omega_k$.

The following lemma is an analogue of the functoriality of the Brauer-Manin pairing.

Lemma 6.7. *Assume that $X_c(k_v) \neq \emptyset$ for all $v \in \Omega_k$. Then we have*

(i) $X^0_c(k_v) \neq \emptyset$ *for all* $v \in \Omega_k$.
(ii) $\alpha_c \circ F = \alpha^0_c$.

Proof. If $x^v \in X_c(k_v)$, then $N_{L^v/L^v_0}(x^v) \in X^0_c(k_v)$. This proves (i). Let us check (ii). Let $x = (x^v_i)$ be a local point of X_c. Note that $b^v_i(K_0, x^v_i) = pb^v_i(K, x^v_i)$. Let $a \in Ш(K_0, K')$. Then we have

$$\alpha_c(F(a)) = \sum_{v\in\Omega_k}\sum_{i\in\mathcal{I}} a_i(pb^v_i(K, x^v_i)) = \sum_{v\in\Omega_k}\sum_{i\in\mathcal{I}} a_i b^v_i(K_0, x^v_i) = \alpha^0_c(a).$$

This completes the proof of the lemma.

6.3. Brauer-Manin map - the general case

Recall that K/k is a cyclic extension of degree d, and that $L = K \times K'$, where K' is an étale k-algebra. We keep the notation of 5.3, in particular, $\mathcal{P}$ is the set of prime divisors of d. For all $p \in \mathcal{P}$, we denote by $K(p)$ the largest subfield of K of degree a power of p, and we set $L(p) = K(p) \times K'$. For all $c \in k^\times$ and $p \in \mathcal{P}$, we let $X_c(p)$ be the $T_{L(p)/k}$-torsor defined by

$$N_{L(p)/k}(x) = c.$$

Let $x = (x^v_i) \in \prod_{v\in\Omega_k} X_c(k_v)$ be a local point of X_c, and let us write $x = (x^v_0, x'^{\,v})$ with $x^v_0 \in K^v$ and $x'^{\,v} \in K'^{\,v}$. Then $(N_{K^v/K(p)^v}(x^v_0), x'^{\,v})$ is a local point of $X_c(p)$.

Let $\alpha(p)$ be the Brauer-Manin map of $X_c(p)$, as defined above. By Proposition 6.6 the map $\alpha(p)$ is independent of the choice of the local point. Recall that $Ш(K, K') = \bigoplus_{p\in\mathcal{P}} Ш(K(p), K')$, and let us define $\alpha_c : Ш(K, K') \to \mathbb{Q}/\mathbb{Z}$ by $\alpha_c = \bigoplus_{p\in\mathcal{P}} \alpha_c(p)$. Hence α_c is also independent of the choice of the local point. We call α_c the *Brauer-Manin map* for X_c.

7. Necessary and sufficient condition

We keep the notation of the previous sections. The main theorem is the following:

Theorem 7.1. *The affine k-variety X_c has a k-point if and only if X_c has a k_v-point at each place $v \in \Omega_k$ and α_c is the zero map.*

7.1. The prime power degree case

We suppose that K is cyclic of degree p^e, where p is a prime number and $e \geq 1$. The proof of Theorem 7.1 uses induction on e.

The proof can be divided into three parts. Recall that $\rho : X_c \to X_c^0$ is the map given by $(x_0, x_1, \dots, x_m) \mapsto (\mathrm{N}_{K/K_0}(x_0), x_1, \dots, x_m)$. (See §6.2.) Suppose that X_c has a k_v-point for all $v \in \Omega_k$ and that X_c^0 has a k-point $z = (z_0, ..., z_m)$. In the first part we use the point z to get a system of local solutions $(\tilde{x}_i^v)$ of X_c such that $\sum\limits_{v \in \Omega_k} b_i^v(K, \tilde{x}_i^v) \in \frac{1}{p}\mathbb{Z}/\mathbb{Z}$. (See Lemma 7.3-Lemma 7.5.)

In Lemma 7.6-Lemma 7.9, we show that one can further modify $(\tilde{x}_i^v)$ so that $\sum\limits_{v \in \Omega_k} b_i^v(K, \tilde{x}_i^v) = 0$. In the end we conclude our main theorem by induction on e and Lemma 6.5.

We would like to mention that an alternative way to prove the theorem is to find the generators of the unramified Brauer group of X_c and show that the Brauer-Manin map defined here is the evaluation on the unramified Brauer group. However, here we choose to prove the theorem in a more elementary way and keep the unramified Brauer group for our future work.

We start with some preliminary results.

Recall that $E_i = K \otimes_k K_i$.

Lemma 7.2. *Suppose that K is a cyclic extension of degree p^e, where p is a prime and $e \geq 1$. Let $v \in \Omega_k$ and $i \in \mathcal{I}$ be such that E_i^v is not isomorphic to a product of copies of K_i^v. Then for all $b \in \frac{1}{p}\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$, there exists $x \in K_i^v$ such that* $\mathrm{inv}(K^v, N_{K_i^v/k_v}(x)) = b$.

Proof. Suppose that K^v is isomorphic to a product of copies of a field extension M of k_v, and set $[M : k_v] = p^f$. Since by hypothesis E_i^v is not isomorphic to a product of copies of K_i^v, we have $f \geq 1$. Assume that $K_i^v \simeq \prod\limits_{j \in J} M_{i,j}$, where $M_{i,j}$ is a field extension of k_v for all $j \in J$.

It suffices to prove that $\frac{1}{p}\mathbb{Z}/\mathbb{Z} \subseteq \mathrm{inv}(M, N_{M_{i,j}/k_v}(M_{i,j}^\times))$ for some $j \in J$; hence we may assume that K^v is a field extension of k_v of degree p^e with $e \geq 1$, and that K_i^v is a field.

Let $\mathrm{Br}(K^v/k_v)$ be the subgroup of the Brauer group of k_v split by K^v; this group is isomorphic to $\mathbb{Z}/p^e\mathbb{Z} \simeq k_v^\times/N((K^v)^\times)$. (See [6] Cor. 4.4.10 and [2] Chap. VI §1.1 Thm. 3 Cor. 2.)

For all $i \in \mathcal{I}$, let M_i be a field such that $E_i^v = K \otimes_k K_i^v$ is a product of copies of M_i, and set $[M_i : K_i^v] = p^{e_i^v}$; the hypothesis implies that $e_i^v \geq 1$. The corestriction map $\mathrm{Br}(K_i^v) \to \mathrm{Br}(k_v)$ is an injection and restricts to an injection of $\mathrm{Br}(M_i/K_i^v)$ into $\mathrm{Br}(K^v/k_v)$, the image being the unique subgroup of order $p^{e_i^v}$ of the cyclic group of order p^e. By the projection formula ([6] Prop. 3.4.10), the image consists of cyclic algebras of the type $(K^v, N_{K_i^v/k_v}(z))$ with z an element of K_i^v. Hence $\frac{1}{p}\mathbb{Z}/\mathbb{Z} \subseteq \frac{1}{p^{e_i^v}}\mathbb{Z}/\mathbb{Z} = \mathrm{inv}(K^v, N_{K_i^v/k_v}(K_i^v)^\times)$. This completes the proof of the lemma.

Let K_0 be the unique subfield of K such that $[K_0 : k] = p^{e-1}$.

Recall that we have $K' = \prod_{i \in \mathcal{I}} K_i$, that $E_i = K \otimes K_i$, and that E_i is the product of copies of a cyclic extension of degree p_i^e of K_i. Set $E_i^0 = K_0 \otimes K_i$. Then E_i^0 also splits as a product of copies of a cyclic extension of K_i; let us denote by p_i^f the degree of this extension. Recall that for all $i \in \mathcal{I}$, we have $f_i \leq e_i$. If moreover $e_i \neq 0$, then $e_i = f_i + 1$ (cf. Lemma 5.5). For all $i \in \mathcal{I}$, the map $F_i : \mathbb{Z}/p^{f_i}\mathbb{Z} \to \mathbb{Z}/p^{e_i}\mathbb{Z}$ is the inclusion of the unique subgroup of order p^{f_i} in the group $\mathbb{Z}/p^{e_i}\mathbb{Z}$, and we set $F = \underset{i \in \mathcal{I}}{\oplus} F_i$.

The map $F : \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{f_i}\mathbb{Z} \to \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z}$ induces a homomorphism $F : Ш(K_0, K') \to Ш(K, K')$. Recall that the cokernel of F is isomorphic to the group $Ш(K/K_0, K')$, defined in section 5.

For all $i \in \mathcal{I}$, set $r_i = \min\{1, e_i\}$. For all $c \in \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{r_i}\mathbb{Z}$ and $n \in \mathbb{Z}/p\mathbb{Z}$, set $I_n^1(c) = \{i \in \mathcal{I} \ \ |n \succeq c\}$. If $I_n^1(c) \neq \mathcal{I}$, set $\Omega(I_n^1(c)) = \underset{i \notin I_n^1(c)}{\cap} \Sigma_i$; if $I^n(c) = \mathcal{I}$, set $\Omega(I_n^1(c)) = \Omega_k$. Set

$$G(K/K_0, K') = \{c \in \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{r_i}\mathbb{Z} \ \ | \bigcup_{n \in \mathbb{Z}/p^{r_1}\mathbb{Z}} \Omega(I_n(c)) = \Omega_k\},$$

let $D(K/K_0, K')$ be the diagonal subgroup of $G(K/K_0, K')$, and recall that

$$Ш(K/K_0, K') = G(K/K_0, K')/D(K/K_0, K').$$

Recall that the projection $\pi : \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{e_i}\mathbb{Z} \to \underset{i \in \mathcal{I}}{\oplus} \mathbb{Z}/p^{r_i}\mathbb{Z}$ induces a homomorphism $F : Ш(K, K') \to Ш(K/K_0, K')$ (cf. Lemma 5.9).

If $t_i \in K_i^v$, set $b_i^v(K, t_i) = \operatorname{inv}(K^v, N_{K_i^v/k_v}(t_i))$, and $b_i^v(K_0, t_i) = \operatorname{inv}(K_0^v, N_{K_i^v/k_v}(t_i))$.

Recall that a local point of X_c is $x = (x_i^v) \in \prod_{v \in \Omega_k} X_c(k_v)$ such that for each $i \in \mathcal{I}$, we have $b_i^v(K, x_i^v) = 0$ for almost all $v \in \Omega_k$.

Lemma 7.3. *Let $x = (x_i^v)$ be a local point of X_c, and let $z = (z_i)$ be a global point of X_c^0. Then for all $v \in \Omega_k$, we have*

$$p \sum_{i \in \mathcal{I}} b_i^v(K, x_i^v) = p \sum_{i \in \mathcal{I}} b_i^v(K, z_i).$$

Proof. Since x is a local point of X_c, we have $\sum_{i \in \mathcal{I}} b_i^v(K, x_i^v) = \operatorname{inv}(K^v, c)$ for all $v \in \Omega_k$. Similarly, we have $\sum_{i \in \mathcal{I}} b_i^v(K_0, z_i) = \operatorname{inv}(K_0^v, c)$ for all $v \in \Omega_k$. Note that $\operatorname{inv}(K_0^v, c) = p \operatorname{inv}(K^v, c)$, and $\operatorname{inv}(K_0^v, z_i) = p \operatorname{inv}(K^v, z_i)$ for all $i \in \mathcal{I}$. Hence we have

$$p \sum_{i \in \mathcal{I}} b_i^v(K, x_i^v) = p \operatorname{inv}(K^v, c) = \operatorname{inv}(K_0^v, c) = \sum_{i \in \mathcal{I}} b_i^v(K_0, z_i) = p \sum_{i \in \mathcal{I}} b_i^v(K, z_i),$$

as claimed.

Lemma 7.4. *Let $x = (x_i^v)$ be a local point of X_c, and assume that $X_c^0(k) \neq \emptyset$. Then there exist $\tilde{x}_i^v \in K_i^v$ such that*

(i) *For each $i \in \mathcal{I}$, we have $b_i^v(K, \tilde{x}_i^v) = 0$ for almost all $v \in \Omega_k$.*
(ii) *For all $i \in \mathcal{I}$, we have $\sum\limits_{v \in \Omega_k} b_i^v(K, \tilde{x}_i^v) \in \frac{1}{p}\mathbb{Z}/\mathbb{Z}$.*
(iii) *For all $v \in \Omega_k$, we have*

$$\sum_{i \in \mathcal{I}} b_i^v(K, x_i^v) = \sum_{i \in \mathcal{I}} b_i^v(K, \tilde{x}_i^v).$$

Proof. Let $z = (z_i)$ be a global point of X_c^0. Set $b_i^v = b_i^v(K, x_i^v)$ and $h_i^v = b_i^v(K, z_i)$. By Lemma 7.3, we have $p\sum\limits_{i \in \mathcal{I}} b_i^v = p\sum\limits_{i \in \mathcal{I}} h_i^v$. Since $b_i^v = 0$ and $h_i^v = 0$ for almost all $v \in \Omega_k$, for almost places $v \in \Omega_k$ we have $\sum\limits_{i \in \mathcal{I}} h_i^v = \sum\limits_{i \in \mathcal{I}} b_i^v$. Suppose that there is $v \in \Omega_k$ such that $\sum\limits_{i \in \mathcal{I}} h_i^v \neq \sum\limits_{i \in \mathcal{I}} b_i^v$. If $v \in \bigcap\limits_{i \in \mathcal{I}} \Sigma_i$, then $b_i^v = h_i^v = 0$ for all $i \in \mathcal{I}$, which is a contradiction. Hence there exists $i \in \mathcal{I}$ such that $v \notin \Sigma_i$. Since $p\sum\limits_{j \in \mathcal{I}} b_j^v = p\sum\limits_{j \in \mathcal{I}} h_j^v$ in $\mathbb{Q}/\mathbb{Z}$, we know that $\sum\limits_{j \in \mathcal{I}} b_j^v - \sum\limits_{j \in \mathcal{I}} h_j^v \in \frac{1}{p}\mathbb{Z}/\mathbb{Z}$. By Lemma 7.2, there exists $\tilde{x}_i^v \in K_i^v$ such that $\operatorname{inv}(K^v, N_{K_i^v/k_v}(\tilde{x}_i^v)) = h_i^v - \sum\limits_{j \in \mathcal{I}} (h_j^v - b_j^v)$.

Set $\tilde{h}_i^v = \operatorname{inv}(K^v, N_{K_i^v/k_v}(\tilde{x}_i^v))$; for all $j \neq i$, let $\tilde{x}_j^v = z_j$, $\tilde{h}_j^v = h_j^v = b_j^v(K, z_j)$. Then we have $\sum\limits_{j \in \mathcal{I}} \tilde{h}_j^v = \sum\limits_{j \in \mathcal{I}} b_j^v$; this proves (iii).

Since $\tilde{h}_i^v = h_i^v$ for almost all $v \in \Omega_k$, (i) holds. As $z = (z_i)$ is a global point of X_c^0, we have $\sum\limits_{v \in \Omega_k} b_i^v(K_0, z_i) = 0$, hence $\sum\limits_{v \in \Omega_k} h_i^v \in \frac{1}{p}\mathbb{Z}/\mathbb{Z}$; moreover, $h_i^v - \tilde{h}_i^v \in \frac{1}{p}\mathbb{Z}/\mathbb{Z}$ for all $i \in \mathcal{I}$ and all $v \in \Omega_k$. Therefore we have $\sum\limits_{v \in \Omega_k} \tilde{h}_i^v \in \frac{1}{p}\mathbb{Z}/\mathbb{Z}$, and this proves (ii).

Lemma 7.5. *Assume that $X_c(k_v) \neq \emptyset$ for all $v \in \Omega_k$, and that $X_c^0(k) \neq \emptyset$. Then there exists a local point $\tilde{x} = (\tilde{x}_i^v)$ of X_c such that for all $i \in \mathcal{I}$, we have*

$$\sum_{v \in \Omega_k} b_i^v(K, \tilde{x}_i^v) \in \frac{1}{p}\mathbb{Z}/\mathbb{Z}.$$

Proof. Let $x = (x_i^v)$ be a local point of X_c. By Lemma 7.4, there exist $\tilde{x}_i^v \in K_i^v$ such that $b_i^v(K, \tilde{x}_i^v) = 0$ for almost all $v \in \Omega_k$, that $\sum\limits_{i \in \mathcal{I}} b_i^v(K, x_i^v) = \sum\limits_{i \in \mathcal{I}} b_i^v(K, \tilde{x}_i^v)$, and that for all $i \in \mathcal{I}$, we have $\sum\limits_{v \in \Omega_k} b_i^v(K, \tilde{x}_i^v) \in \frac{1}{p}\mathbb{Z}/\mathbb{Z}$. By Lemma 6.4, for all $v \in \Omega_k$, there exists $\tilde{x}_0^v \in (K^v)^\times$ such that $(\tilde{x}_0^v, \tilde{x}_1^v, ..., \tilde{x}_m^v) \in X_c(k_v)$. This completes the proof of the lemma.

Recall that if $X_c(k_v) \neq \emptyset$ for all $v \in \Omega_k$, and that for all $c \in k^\times$, we have a homomorphism $\alpha_c : Ш(K, K') \to \mathbb{Q}/\mathbb{Z}$. We now show that α_c induces a homomorphism $\overline{\alpha}_c : Ш(K/K_0, K') \to \mathbb{Q}/\mathbb{Z}$ such that $\overline{\alpha}_c \circ \pi = \alpha_c$.

Lemma 7.6. *Assume that $X_c(k_v) \neq \emptyset$ for all $v \in \Omega_k$ and that $X_c^0(k) \neq \emptyset$. Then there exists a homomorphism $\overline{\alpha}_c : Ш(K/K_0, K') \to \mathbb{Q}/\mathbb{Z}$ such that $\overline{\alpha}_c \circ \pi = \alpha_c$.*

Proof. Let $x = (x_i^v)$ be a local point of X_c, and set $b_i^v = \operatorname{inv}(K^v, N_{K_i^v/k_v}(x_i^v))$ for all $i \in \mathcal{I}$ and all $v \in \Omega_k$. Let $a = (a_1, ..., a_m) \in G$. Then by Lemma 5.9 $\pi(a) = (\overline{a}_1, ..., \overline{a}_m) \in G(K/K_0, K') \subseteq \underset{i\in\mathcal{I}}{\oplus} \mathbb{Z}/p^{r_i}\mathbb{Z}$. Note that $r_i = \min\{1, e_i\}$ by definition. If $e_i = 0$, then $e_i = r_i = 0$ and $a_i = \overline{a}_i = 0$. If not, then $r_i = 1$ and $\overline{a}_i = a \pmod p$. By Lemma 7.5, we may assume that $\sum\limits_{v\in\Omega_k} b_i^v \in \frac{1}{p}\mathbb{Z}/\mathbb{Z}$ for all $i \in \mathcal{I}$; hence $a_i(\sum\limits_{v\in\Omega_k} b_i^v) = \overline{a}_i(\sum\limits_{v\in\Omega_k} b_i^v)$. We then have

$$\alpha_c(a_1, ..., a_m) = \sum_{i\in\mathcal{I}} a_i(\sum_{v\in\Omega_k} b_i^v) = \sum_{i\in\mathcal{I}} \overline{a}_i(\sum_{v\in\Omega_k} b_i^v).$$

Hence α_c induces a homomorphism $\overline{\alpha}_c : Ш(K/K_0, K') \to \mathbb{Q}/\mathbb{Z}$, as claimed.

Lemma 7.7. *Let $x = (x_i^v)$ be a local point of X_c, and set $b_i^v = b_i^v(K, x_i^v)$. Assume that $\alpha_c = 0$, and that $X_c^0(k) \neq \emptyset$. Let $(I_0, \dots, I_{p-1}) \in G(K/K_0, K')$. Then we have $\sum\limits_{i\in I_n} \sum\limits_{v\in\Omega_k} b_i^v = 0$ for all $n \in \mathbb{Z}/p\mathbb{Z}$.*

Proof. Let $n \in \mathbb{Z}/p\mathbb{Z}$. The statement is trivial if I_n is empty, and it follows from Lemma 6.3 if $I_n = \mathcal{I}'$. Assume that I_n is not empty, and $I_n \neq \mathcal{I}'$. Let $n' \in \mathbb{Z}/p\mathbb{Z}$ such that $n' \neq n$, and set $J_n = I_n$, $J_{n'} = \underset{r\neq n}{\cup} I_r$, and $J_r = \emptyset$ if $r \neq n, n'$. Then by Lemma 5.15, we have $(J_0, \dots, J_{p-1}) \in G(K/K_0, K')$. Since $X_c^0(k) \neq \emptyset$, by Lemma 7.6 there exists a homomorphism $\overline{\alpha}_c : Ш(K/K_0, K') \to \mathbb{Q}/\mathbb{Z}$ such that $\overline{\alpha}_c \circ \pi = \alpha_c$. By hypothesis α_c is the zero map, hence we have $\overline{\alpha}_c = 0$. Therefore we have

$$\sum_{r\in\mathbb{Z}/p\mathbb{Z}} \sum_{i\in J_r} \sum_{v\in\Omega_k} r b_i^v = \sum_{i\in J_n} \sum_{v\in\Omega_k} n b_i^v + \sum_{i\in J_{n'}} \sum_{v\in\Omega_k} n' b_i^v = 0.$$

By Lemma 6.3 we have $\sum\limits_{i\in\mathcal{I}'} \sum\limits_{v\in\Omega_k} b_i^v = 0$, hence $(n-n') \sum\limits_{i\in J_n} \sum\limits_{v\in\Omega_k} b_i^v = 0$. Recall that $n' \neq n$ by hypothesis, therefore we have $\sum\limits_{i\in J_n} \sum\limits_{v\in\Omega_k} b_i^v = 0$; since $J_n = I_n$, we have $\sum\limits_{i\in I_n} \sum\limits_{v\in\Omega_k} b_i^v = 0$, as claimed.

Lemma 7.8. *Let $x = (x_i^v)$ be a local point of X_c. Assume that $\alpha_c = 0$, and that $X_c^0(k) \neq \emptyset$. Let $(I_0, \dots, I_{p-1}) \in G(K/K_0, K')$, and let $n \in \mathbb{Z}/p\mathbb{Z}$. Then there exists a local point $\tilde{x} = (\tilde{x}_i^v)$ of X_c such that $\tilde{x}_i^v = x_i^v$ if $i \notin I_n$, and that $\sum\limits_{v\in\Omega_k} b_i^v(K, \tilde{x}) = 0$ for all $i \in I_n$.*

Proof. We prove this by induction on the cardinality of I_n. If $|I_n| = 0$ then the claim is trivial; if $|I_n| = 1$, then it follows from Lemma 7.7, since we have $\sum\limits_{v\in\Omega_k} b_i^v(x) = 0$ for all $i \in I_n$. Suppose that the claim is true for $|I_n| < h$. For $|I_n| = h$, suppose that there are nonempty disjoint subsets I_n^0 and I_n^1 of I_n satisfying $I_n^0 \cup I_n^1 = I_n$ and $(\bigcap_{i\in I_n^0} \Sigma_i) \cup (\bigcap_{i\in I_n^1} \Sigma_i) = \Omega_k$. Then consider the element $(J_0, ...J_{p-1})$ where $J_r = I_r$ if $r \neq n, n+1$, $J_n = I_n^0$ and $J_{n+1} = I_n^1 \cup I_{n+1}$. Note that $\Omega(I_r) = \Omega(J_r)$ if $r \neq n, n+1$ and that $\Omega(I_{n+1}) \subset \Omega(J_{n+1})$. Let us prove that $(J_0, ...J_{p-1})$ represents an element of $Ш(K, K')$; for this, we have to check that $\Omega(J_0)\cup\cdots\cup\Omega(J_{p-1}) = \Omega_k$. Since $\Omega(I_r) \subset \Omega(J_r)$ if $r \neq n$ and $\Omega(I_0) \cup \cdots \cup \Omega(I_{p-1}) = \Omega_k$, it suffices to check that if $v \in \Omega(I_n)$, then $v \in \Omega(J_0) \cup \cdots \cup \Omega(J_{p-1})$. If $v \in \bigcap_{i\in I_n^1} \Sigma_i$, then we have $v \in \Omega(J_n)$. Otherwise, we have $v \in \bigcap_{i\in I_n^0} \Sigma_i$ because $(\bigcap_{i\in I_n^0} \Sigma_i)\cup(\bigcap_{i\in I_n^1} \Sigma_i) = \Omega_k$. Hence we have $v \in (\bigcap_{i\notin I_n\cup I_{n+1}} \Sigma_i)\cap(\bigcap_{i\in I_n^0} \Sigma_i) = \Omega(J_{n+1})$. Therefore $(J_0, ...J_{p-1})$ represents an element of $Ш(K, K')$. Since $|J_n| < h$, we can apply the induction hypothesis, and hence there exists a local point $\tilde{x} = (\tilde{x}_i^v)$ such that $\tilde{x}_i^v = x_i^v$ if $i \notin J_n = I_n^1$, and that $\sum_{v\in\Omega} b_i^v(K, \tilde{x}) = 0$ for all $i \in J_n = I_n^1$. The same argument with I_n^0 instead of I_n^1 gives the desired result.

Assume now that I_n does not have any non-trivial subpartitions, in other words, that there are no nonempty disjoint subsets I_n^0 and I_n^1 of I_n satisfying $I_n^0 \cup I_n^1 = I_n$ and $(\bigcap_{i\in I_n^0} \Sigma_i) \cup (\bigcap_{i\in I_n^1} \Sigma_i) = \Omega_k$. Let us consider the graph with vertex set I_n, and edge set $\mathcal{E} = \{(i,j)|\Sigma_i \cup \Sigma_j \neq \Omega_k\}$; since I_n has no non-trivial subpartitions, this graph is connected. Set $b_i^v = b(K, x_i^v)_i^v$, and for all $i \in I_n$, set $d_i = \sum_{v\in\Omega_k} b_i^v$. Let us fix an ordering of I_n, say $I_n = \{i_0, ..., i_t\}$. Since the graph is connected, there exists a loop-free path between i_0 and i_1. Along this path, for any two adjacent vertices i, j, there exists $v \in \Omega_k$ such that $v \notin \Sigma_i \cup \Sigma_j$. By Lemma 7.5 we may assume that $b_i^v \in \frac{1}{p}\mathbb{Z}/\mathbb{Z}$ for all $i \in I_n$. Applying Lemma 7.2, by modifying x_i^v and x_j^v we can modify b_i^v to $b_i^v - d_{i_0}$ and b_j^v to $b_j^v + d_{i_0}$. Note that this modification does not change $\sum_{i\in\mathcal{I}} b_i^v$. Therefore by Lemma 6.4, after changing also x_0^v if necessary, the modified (x_i^v) is still a local point of X_c. After these modifications, we have $\sum_{v\in\Omega_k} b_{i_0}^v = 0$, $\sum_{v\in\Omega_k} b_{i_1}^v = d_{i_1} + d_{i_0}$, and all the other d_i's remain unchanged. We repeat this process along a loop-free path from i_1 to i_2, and we modify each adjacent pair along the path from i_1 to i_2 by $d_{i_0} + d_{i_1}$ and so on. At the end, we modify each adjacent pair along the path from i_{t-1} to i_t by $\sum_{r=0}^{t-1} d_{i_r}$. After this process, we have $\sum_{v\in\Omega_k} b_{i_r}^v = 0$ for $r = 0, ..., t-1$ and $\sum_{v\in\Omega_k} b_{i_t}^v = d_{i_t} + \sum_{r=0}^{t-1} d_{i_r}$. However, by Lemma 7.7, we know that $\sum_{r=0}^{t} d_{i_r} = 0$; hence, we have $\sum_{v\in\Omega_k} b_{i_t}^v = 0$. Moreover, only finitely many b_i^v's are modified, so $b_i^v = 0$ for almost all v; the lemma then follows.

Proposition 7.9. *Let $x = (x_i^v)$ be a local point of X_c. Assume that $\alpha_c = 0$, and that $X_c^0(k) \neq \emptyset$. Then there exists a local point $\tilde{x} = (\tilde{x}_i^v)$ of X_c such that for all $i \in \mathcal{I}$, we have*

$$\sum_{v\in\Omega_k} b_i(K, \tilde{x}_i^v) = 0.$$

Proof. This follows from Lemma 7.8.

Proof of Theorem 7.1 for K of prime power degree. It is clear that if X_c has a k-point, then X_c has a k_v-point for all $v \in \Omega_k$ and $\alpha_c = 0$. Conversely, suppose that X_c has a k_v-point for all $v \in \Omega_k$ and that $\alpha_c = 0$. Let us show that the variety X_c has a k-point. We show our claim by induction on the exponent e. Suppose that $e = 1$. Then $K_0 = k$, and $X_c^0(k) \neq \emptyset$. By Proposition 7.9, there exists a local point $x = (x_i^v)$ of X_c such that for all $i \in \mathcal{I}$, we have $\sum\limits_{v \in \Omega_k} b_i(x_i^v) = 0$. Lemma 6.5 implies that $X_c(k) \neq \emptyset$. Assume now that $e > 1$. Since X_c has a k_v-point for all $v \in \Omega_k$, the variety X_c^0 also has a k_v-point for all $v \in \Omega_k$. As α_c is the zero map, by Lemma 6.7 the Brauer-Manin map α_c^0 for X_c^0 is also the zero map. Therefore X_c^0 has a k-point by induction hypothesis. By Proposition 7.9, there exists a local point $x = (x_i^v)$ of X_c such that for all $i \in \mathcal{I}$, we have $\sum\limits_{v \in \Omega_k} b_i(x_i^v) = 0$. Lemma 6.5 implies that $X_c(k) \neq \emptyset$.

7.2. The general case

Recall that K/k is a cyclic extension of degree d, and that $L = K \times K'$, where K' is an arbitrary étale k-algebra. We keep the notation of 5.3, in particular, $\mathcal{P}$ is the set of prime divisors of d. For all $p \in \mathcal{P}$, we denote by $K(p)$ the largest subfield of K of order a power of p, and $L(p) = K(p) \times K'$. For all $c \in k^\times$ and $p \in \mathcal{P}$, the affine k-variety defined by

$$N_{L(p)/K(p)}(x) = c,$$

is denoted by $X_c(p)$. Recall that there is a natural map from X_c to $X_c(p)$ (§6.3). We denote by $\alpha_c(p)$ be the Brauer-Manin map of $X_c(p)$. Recall that $\text{Ш}(K, K') = \bigoplus\limits_{p \in \mathcal{P}} \text{Ш}(K(p), K')$, and that $\alpha_c : \text{Ш}(K, K') \to \mathbb{Q}/\mathbb{Z}$ is given by $\alpha_c = \bigoplus\limits_{p \in \mathcal{P}} \alpha_c(p)$.

Lemma 7.10. *Let $c \in k^\times$. Then X_c has a k-point if and only if $X_c(p)$ has a k-point for all $p \in \mathcal{P}$.*

Proof. Let $z \in X_c(k)$ be a k-point of X_c, and let us write $z = (x, y)$ with $x \in K$ and $y \in K'$. Then $(N_{K/K(p)}(x), y)$ is a k-point of $X_c(p)$ for all $p \in \mathcal{P}$. Conversely, suppose that for all $p \in \mathcal{P}$, the k-variety $X_c(p)$ has a k-point $(x_p, y_p) \in K(p) \times K'$. For all $p \in \mathcal{P}$, set

$$r_p = \prod_{q \in \mathcal{P}, q \neq p} [K(q) : k],$$

and let $s_p \in \mathbb{Z}$ such that $\sum\limits_{p \in \mathcal{P}} r_p s_p = 1$. Set $x = \prod\limits_{p \in \mathcal{P}} x_p^{s_p}$, and $y = \prod\limits_{p \in \mathcal{P}} y_p^{r_p s_p}$. Then (x, y) is a k-point of X_c.

Remark 7.11. The above lemma is compatible with base change to any field extension l of k.

Proof of Theorem 7.1. Suppose that X_c has a k-point. Then by Lemma 7.10, $X_c(p)$ has a k-point for all $p \in \mathcal{P}$. This implies that $\alpha_c(p) = 0$ for all $p \in \mathcal{P}$, and hence $\alpha_c = 0$. Conversely, suppose that X_c has a k_v-point for all $v \in \Omega_k$ and that $\alpha_c = 0$. Then $X_c(p)$ has a k_v-point for all $v \in \Omega_k$. Since $\alpha_c = 0$, we have $\alpha_c(p) = 0$ for all $p \in \mathcal{P}$. But $K(p)$ is a cyclic extension of prime power degree, hence this implies that $X_c(p)$ has a k-point for all $p \in \mathcal{P}$. Therefore X_c has a k-point by Lemma 7.10.

Corollary 7.12. *Let I_L be the idèle group of L. Then sending $c \in k^\times$ to α_c gives rise to an isomorphism*

$$(k^\times \cap N_{L/k}(I_L))/N_{L/k}(L^\times) \to Ш(L)^*.$$

Proof. It is clear from the definition of α_c that sending $c \in k^\times$ to α_c is a homomorphism; Theorem 7.1 implies that this homomorphism is injective. That it is an isomorphism follows from the fact that $Ш(L)^* \simeq Ш^1(k, T_{L/k})$ (see Corollary 5.17).

Metacyclic extensions

In the following we apply the main theorem to the case where K is a metacyclic extension of k (recall that a metacyclic extension is a Galois extension such that all the Sylow subgroups of its Galois group are cyclic). As before, let X_c be the k-variety defined by the equation (0.1). Assume that K/k is a metacyclic extension of degree $q = \prod_{j=1}^{s} p_j^{e_j}$, where p_j's are distinct primes. Let $q_j = p_j^{e_j}$ and $r_j = q/q_j$. For $1 \leq j \leq s$, let G_j be a p_j-Sylow subgroup of $\mathrm{Gal}(K/k)$ and let F_j be the subfield of K fixed by G_j. Note that $[F_j : k] = r_j$. Let X_c^j be $X_c \otimes_k F_j$. Then the injection $k \to F_j$ induces a natural injection of $X_c(k)$ to $X_c(F_j) = X_c^j(F_j)$.

Suppose that X_c has a k_v-point for all $v \in \Omega_k$. Then X_c^j has a $F_{j,w}$-point for all $w \in \Omega_{F_j}$. Since F_j is a cyclic extension of k, we can define the Brauer-Manin map α_j for X_c^j. The necessary and sufficient condition for the Hasse principle for X_c to hold is the following:

Proposition 7.13. *Assume that K is a metacyclic extension. Then X_c has a k-point if and only if X_c has a k_v-point for all $v \in \Omega_k$ and $\alpha_j = 0$ for $1 \leq j \leq s$.*

Proof. Assume that X_c has a k_v-point for all $v \in \Omega_k$, and that $\alpha_j = 0$ for $1 \leq j \leq s$. Then the variety X_c^j has a $F_{j,w}$-point for all $w \in \Omega_{F_j}$. Since $\alpha_j = 0$ for all $1 \leq j \leq s$, by Theorem 7.1 the variety X_c^j has a F_j-point. Let $(x_{j,i})$ be a F_j-point of X_c^j, where $x_{j,i} \in (F_j \otimes_k K_i)^\times$. Let $b_j \in \mathbb{Z}$ such that $\sum_{j=1}^{s} b_j r_j = 1$, and set $z_i = \prod_{j=1}^{s} N_{F_j \otimes K_i/K_i}(x_{j,i})^{b_j}$; then (z_i) is a point of X_c. The other direction is trivial.

8. Products of cyclic extensions

In this section, we suppose that L is a *product of cyclic extensions*, and we denote by $Ш(L)$ the obstruction group. In the following, we give a simple criterion for the vanishing of $Ш(L)$; in other words, an easy way to decide whether the Hasse principle holds for L.

Assume that $L = \prod\limits_{i\in J} K_i$, where K_i/k is a cyclic extension of degree d_i. Let $\mathcal{P}$ be the set of prime numbers dividing $\prod\limits_{i\in J} d_i$. For all $p \in \mathcal{P}$ and all $i \in J$, let $K_i(p)$ be the largest subfield of K_i such that $[K_i(p) : k]$ is a power of p, and set $L(p) = \prod\limits_{i\in J} K_i(p)$.

For any cyclic field extension K/k of prime power degree, we denote by K_{prim} the unique subfield of K of degree p over k. Set $L(p)_{\mathrm{prim}} = \prod\limits_{i\in J} K_i(p)_{\mathrm{prim}}$.

The aim of this section is to prove the following two results:

Theorem 8.1.

$$Ш(L) = 0 \iff \underset{p\in\mathcal{P}(L)}{\oplus} Ш(L(p)_{\mathrm{prim}}) = 0,$$

where $\mathcal{P}(L)$ is a set of prime numbers, subset of $\mathcal{P}$.

The set $\mathcal{P}(L)$ is determined in Theorem 8.3, see below.

Theorem 8.2.

$$Ш(L(p)_{\mathrm{prim}}) \simeq (\mathbb{Z}/p\mathbb{Z})^{m_p(L)},$$

where $m_p(L)$ is a positive integer.

The value of $m_p(L)$ is given in Theorem 8.3.

We start with the proof of Theorem 8.2, which amounts to treating the case where L is a product of cyclic extensions of prime degree.

Theorem 8.3. *Let p be a prime number, and assume that L is a product of n non-isomorphic cyclic extensions of degree p. Then we have*

(a) *If $n \leq 2$, then* $Ш(L) = 0$.
(b) *If $3 \leq n \leq p+1$, then either* $Ш(L) = 0$, *or* $Ш(L) \simeq (\mathbb{Z}/p\mathbb{Z})^{n-2}$.
(c) *If $n \geq p+2$, then* $Ш(L) = 0$.

Note that Theorem 8.3 implies immediately Theorem 8.2, and gives the value of the integer $m_p(L)$. Note also that the case $n = 1$ is a special case Hasse's cyclic norm theorem, the case $n = 2$ follows from Hürlimann's result [9] Prop. 3.3, (see also Proposition 4.1), and that the case $n = 3$, $p = 3$ is a result of Colliot-Thélène, cf. [3], Théorème 4.1.

In order to prove Theorem 8.3, we need to come back to the definition of $Ш(L) = Ш(K, K')$ in the case where K is cyclic of prime degree, and give a description of this group in terms of partitions.

We keep the notation of 5.1, with $e = 1$. In particular, p is a prime number, and $L = K \times K'$, where K is a cyclic extension of k of degree p. Recall that $E_i = K \otimes K_i$, and note that E_i is either a cyclic field extension of K_i or a product of p copies of K_i. Let J be the subset of $i \in \mathcal{I}$ such that E_i/K_i is a field extension, and let $r = |J|$.

Recall that Σ_i is the set of $v \in \Omega_k$ such that E_i^v is the product of p copies of K_i^v. For all $J' \subset J$ with $J' \neq J$, set $\Omega(J') = \underset{i \notin J'}{\cap} \Sigma_i$, and let $\Omega(J) = \Omega_k$. By Lemma 5.12, the group $G(K, K')$ is in bijection with the set of partitions $(J_0, \dots, J_{p-1})$ of J such that $\underset{n \in \mathbb{Z}/p\mathbb{Z}}{\cup} \Omega(J_n) = \Omega_k$. We identify $G(K, K')$ with the set of these partitions. Note that under this identification, $D(K, K')$ corresponds to the partitions where one of the subsets is J, and all the others are empty; these will be called the trivial partitions of J.

For all $n \in \mathbb{Z}/p\mathbb{Z}$ and all $a \in (\mathbb{Z}/p\mathbb{Z})^r$, set $J_n(a) = \{i \in J \mid a_i = n\}$. Then Lemma 5.12 can be reformulated as follows:

Lemma 8.4. *$G(K, K')$ is in bijection with the set*

$$\{a \in (\mathbb{Z}/p\mathbb{Z})^r \mid \underset{n \in \mathbb{Z}/p\mathbb{Z}}{\cup} \Omega(J_n(a)) = \Omega_k\}.$$

Proof of Theorem 8.3. Note first that (a) follows from Proposition 4.1. From now on, we assume that $n \geq 3$. Theorem 8.3, as well as a precise condition for when $Ш(L) = 0$ in case (b), is a consequence of Proposition 8.5 below.

For any positive integer d, a finite separable extension F of k is said to have *local degrees* $\leq d$ if for all places $v \in \Omega_k$, the étale algebra $F \otimes_k k_v$ is a product of field extensions of k_v with degrees $\leq d$.

Proposition 8.5. *Let p be a prime number, and assume that L is a product of distinct field extensions of degree p of k, at least one of which is cyclic.*

Then $Ш(L) \neq 0 \iff$ the factors of L are distinct subfields of a field extension F/k of degree p^2, and all the local degrees of F are $\leq p$.

Moreover, if $Ш(L) \neq 0$, and if L is a product of n distinct degree p field extensions of k, then $Ш(L) \simeq (\mathbb{Z}/p\mathbb{Z})^{n-2}$.

Proof. Let K be a cyclic factor of L, and let us write $L = K \times K'$, where K' is a product of field extensions of degree p of k. Suppose that $Ш(L) \neq 0$. Then there exists a partition (I_0, I_1) of J such that $\Omega(I_0) \cup \Omega(I_1) = \Omega_k$. Indeed, let $(J_0, \dots, J_{p-1})$ be a non-trivial partition of J such that $\underset{r \in \mathbb{Z}/p\mathbb{Z}}{\cup} \Omega(J_i) = \Omega_k$. Without loss of generality, we can assume that J_0 is not empty. Set $I_0 = J_0$, and let $I_1 = \underset{i \neq 0}{\cup} J_i$; then we have $\Omega(I_0) = \Omega(J_0)$, and $\Omega(J_r) \subset \Omega(I_1)$ for all $r \neq 0$. Therefore $\Omega(I_0) \cup \Omega(I_1) = \Omega_k$, as claimed. Let K_i and K_j be two distinct factors of K', and let K_iK_j be the composite of K_i and K_j. For all $v \in \Sigma_i$, we have

$$K \otimes_k (K_iK_j)^v \simeq K \otimes_k K_i^v \otimes_{K_i^v} (K_iK_j)^v,$$

and, since $v \in \Sigma_i$, this is isomorphic to the product of p copies of $(K_iK_j)^v$.

Let $i \in I_0$ and $j \in I_1$. As we have $\Omega(I_0) \cup \Omega(I_1) = \Omega_k$, the tensor product $K \otimes_k (K_iK_j)^v$ is isomorphic to the product of p copies of $(K_iK_j)^v$ for all $v \in \Omega_k$. This implies that K is a subfield of K_iK_j. Recall that K is cyclic, and that K_i, K_j are not isomorphic; hence we have $K \otimes_k K_i \simeq KK_i \subset K_iK_j$. The degree of K_iK_j is at most p^2, hence we have $KK_i = K_iK_j = KK_j$, and $K_i \otimes_k K_j \simeq K_iK_j$ is of degree p^2 over k.

Let $i \in I_0$, and set $F = KK_i$; we just saw that F is independent of the choice of i, and that $F = K_iK_j$ for all $j \in I_1$. This shows that K_i is a subfield of F for all $i \in J$. Since (I_0, I_1) represents a non-trivial element of $Ш(L)$, for all $v \in \Omega_k$ there exists $i \in J$ such that $F^v \simeq K \otimes_k K_i^v$ is isomorphic to a product of p copies of K_i^v. Therefore all the local degrees of F are $\leq p$.

Conversely, let F be a separable extension of degree p^2 of k such that all the factors of L are distinct subfields of F. It suffices to prove that all non-trivial partitions $(J_0, \dots, J_{p-1})$ of J satisfy $\underset{r \in \mathbb{Z}/p\mathbb{Z}}{\cup} \Omega(J_i) = \Omega_k$. Suppose that this is not the case. Let $(J_0, \dots, J_{p-1})$ be a non-trivial partition of J with $\underset{r \in \mathbb{Z}/p\mathbb{Z}}{\cup} \Omega(J_i) \neq \Omega_k$. Let $v \in \Omega_k$ with $v \notin \underset{r \in \mathbb{Z}/p\mathbb{Z}}{\cup} \Omega(J_i)$. Since $v \notin \Omega(J_0)$, there exists $i \notin J_0$ such that $iv \notin \Sigma_i$. Let $r \in \mathbb{Z}/p\mathbb{Z}$ such that $i \in J_r$; since $v \notin \Omega(J_r)$, there exists $j \notin J_r$ such that $v \notin \Sigma_j$.

Since the degree p extensions K, K_i and K_j are distinct subfields of F, we have $F \simeq K \otimes K_i \simeq K \otimes K_j$. Note that $[K^v : k_v] = p$, because $v \notin \Sigma_i$. Let us write K_i^v as a product of separable extensions of k_v. If one of the factors M_s of K_i^v is such that $1 < [M_s : k_v] < p$, then M_s and K^v are linearly disjoint, and this contradicts the assumption that all the local degrees of F are $\leq p$. Hence K_i^v is either a degree p field extension of k_v, or a product of p copies of k_v. However, if K_i^v and K^v are both fields, then E_i^v is a field extension of degree p^2 of k_v. Since $F^v \simeq E_i^v$, this contradicts the hypothesis that all the local degrees of F are $\leq p$. Therefore K_i^v is a product of p copies of k_v, and hence $F^v \simeq E_i^v$ is a product of p copies of K^v.

Set $d = [K_iK_j : k]$. Since $v \notin \Sigma_j$, the same argument shows that K_j^v is a product of p copies of k_v, hence $(K_iK_j)^v$ is a product of d copies of k_v. Note that $(K_iK_j)^v$ is a subalgebra of F^v, and that F^v is a product of p copies of K^v; hence we have $d \leq p$. As K_i and K_j are distinct subfields of K_iK_j, we have $d = rp$ for some integer $r > 1$, and this leads to a contradiction.

Hence for all non-trivial partitions $(J_0, \dots, J_{p-1})$ of J we have $\underset{r \in \mathbb{Z}/p\mathbb{Z}}{\cup} \Omega(J_i) = \Omega_k$. This shows that $Ш(K, K') = Ш(L) \simeq (\mathbb{Z}/p\mathbb{Z})^{n-2}$.

Proof of Theorem 8.1. Assume now that L is a product of n cyclic extensions, $L = K_1 \times \cdots \times K_n$, where K_i/k is a cyclic extension of degree d_i, and let $J = \{1, \dots, n\}$. Note that $Ш(L) = Ш(K_i, K_i')$ for any $i \in J$, where $L = K_i \times K_i'$. This will be used repeatedly in the sequel.

Let $\mathcal{P}$ be the set of prime numbers dividing $d_1 \dots d_n$. For all $p \in \mathcal{P}$ and all $i \in J$, let $K_i(p)$ be the largest subfield of K_i such that $[K_i(p) : k]$ is a power of p, and set $L(p) = K_1(p) \times \cdots \times K_n(p)$.

Proposition 8.6. *We have*

$$Ш(L) = \bigoplus_{p \in \mathcal{P}(L)} Ш(L(p)).$$

Proof. This follows from Proposition 5.16, and from the fact that L is a product of cyclic extensions.

Lemma 8.7. *Let p be a prime number, and let K_i/k, $i \in J$, be cyclic extensions of degree a power of p of k. For all $i \in J$, let N_i/k be a subextension of K_i/k. Then $Ш(\prod_{i \in J} N_i)$ injects into $Ш(\prod_{i \in J} K_i)$.*

Proof. This follows from Proposition 5.7, and Remark 5.8 following this proposition.

Proof of Theorem 8.1. Assume that $Ш(L) = 0$. By Lemma 8.7 and Proposition 8.6, the group $Ш(L_{\text{prim}})$ injects into $Ш(L)$, hence this implies that $Ш(L_{\text{prim}}) = 0$. Conversely, suppose that $Ш(L_{\text{prim}}) = 0$. By Proposition 8.6, we may assume that L is a product of extensions of degree a power of a prime p. Let us write $L = K \times K'$, for some cyclic field extension K/k; then $L_{\text{prim}} = K_{\text{prim}} \times K'_{\text{prim}}$. Since $Ш(L_{\text{prim}}) = 0$, by Proposition 5.14 we have $Ш(K, K'_{\text{prim}}) = 0$. Permuting K with one of the other cyclic factors and repeating the same procedure, we obtain $Ш(L) = 0$.

Example 8.8. Let p be a prime number, and let F/k be an extension with Galois group $C_p \times C_p$, where C_p denotes the cyclic group of order p. Let $K_1, \dots, K_{p+1}$ be the distinct subfields of degree p of F. Set $L = K_1 \times \cdots \times K_{p+1}$. Then by Proposition 8.5, we have $Ш(L) = 0$ or $Ш(L) = (\mathbb{Z}/p\mathbb{Z})^{p-1}$. Moreover, we have

$$Ш(L) = 0 \iff \text{there exists } v \in \Omega_k \text{ such that } F^v \text{ is a field.}$$

- Assume first that there exists $v \in \Omega_k$ such that F^v is a field. Then $Ш(L) = 0$, hence for all $c \in k^\times$, we have $X_c(k) \neq \emptyset$. In other words, we have

$$N_{L/k}(L^\times) = k^\times$$

  in this case.

- Assume now that all the local degrees of F are $\leq p$. Then by Proposition 8.5 we have $Ш(L) = (\mathbb{Z}/p\mathbb{Z})^{p-1}$.

Let Ω_i be the set of $v \in \Omega_k$ such that K_i^v is split. Note that we have $\Omega_1 \cup \cdots \cup \Omega_{p+1} = \Omega_k$. This implies that $X_c(k_v) \neq \emptyset$ for all $v \in \Omega_k$ and for all $c \in k\times$.

Set $K = K_{p+1}$. For all $c \in k^\times$ and for all $v \in \Omega_k$, let us denote by $[K, c]_v \in \mathbb{Z}/p\mathbb{Z}$ the image of $\mathrm{inv}(K, c)_v$ by the isomorphism $\frac{1}{p}\mathbb{Z}/\mathbb{Z} \simeq p\mathbb{Z}/\mathbb{Z}$. Then the map

$$f : k^\times / N_{L/k}(L^\times) \to (\mathbb{Z}/p\mathbb{Z})^{p-1}$$

given by

$$c \mapsto (\sum_{\Omega_1}[K, c]_v, \ldots, \sum_{\Omega_{p-1}}[K, c]_v),$$

is an isomorphism.

When $p = 2$, we recover a well-known result of Serre and Tate, see [2], Exercise 5.2, page 360; see also [3], Proposition 5.1.

References

[1] T.D. Browning, R. Newton, The proportion of failures of the Hasse norm principle, Mathematika 62 (2016) 337–347.
[2] J.W.S. Cassels, A. Fröhlich, Algebraic Number Theory, Washington, 1967; second corrected edition, L.M.S., 2010.
[3] J.-L. Colliot-Thélène, Groupe de Brauer non ramifié d'espaces homogènes de tores, J. Théor. Nombres Bordeaux 26 (2014) 69–83.
[4] C. Demarche, D. Wei, Hasse principle and weak approximation for multinorm equations, Israel J. Math. 202 (1) (2014) 275–293.
[5] C. Frei, D. Loughran, R. Newton, The Hasse norm principle for abelian extensions, Amer. J. Math. 140 (2018) 1639–1685.
[6] P. Gille, T. Szamuely, Central Simple Algebras and Galois Cohomology, Cambridge University Press, 2006.
[7] H. Hasse, Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol, Nachr. Ges. Wiss., Göttingen, 1931, pp. 64–69.
[8] H. Hasse, Theory of cyclic algebras over an algebraic number field, Trans. Amer. Math. Soc. 34 (1932) 171–214.
[9] W. Hürlimann, On algebraic tori of norm type, Comment. Math. Helv. 59 (1984) 539–549.
[10] J. Oesterlé, Nombres de Tamagawa et groupes unipotents en caractéristique p, Invent. Math. 78 (1984) 13–88.
[11] V. Platonov, A.S. Rapinchuk, Algebraic Groups and Number Theory, Academic Press, 1994.
[12] T. Pollio, On the multinorm principle for finite abelian extensions, Pure Appl. Math. Q. 10 (2014) 547–566.
[13] T. Pollio, A.S. Rapinchuk, The multinorm principle for linearly disjoint Galois extensions, J. Number Theory 133 (2013) 802–821.
[14] G. Prasad, A.S. Rapinchuk, Local-global principles for embedding of fields with involution into simple algebras with involution, Comment. Math. Helv. 85 (2010) 583–645.
[15] J.-J. Sansuc, Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres, J. Reine Angew. Math. 327 (1981) 12–80.