COMPOSITIO MATHEMATICA

Le complémentaire des puissances n-ièmes dans un corps de nombres est un ensemble diophantien

Jean-Louis Colliot-Thélène and Jan Van Geel

Compositio Math. **151** (2015), 1965–1980.

doi:10.1112/S0010437X15007368

Compositio Math. 151 (2015) 1965–1980
doi:10.1112/S0010437X15007368

Le complémentaire des puissances n-ièmes dans un corps de nombres est un ensemble diophantien

Jean-Louis Colliot-Thélène et Jan Van Geel

Abstract

For $n = 2$ the statement in the title is a theorem of B. Poonen (2009). He uses a one-parameter family of varieties together with a theorem of Coray, Sansuc and one of the authors (1980), on the Brauer–Manin obstruction for rational points on these varieties. For $n = p$, p any prime number, A. Várilly-Alvarado and B. Viray (2012) considered analogous families of varieties. Replacing this family by its $(2p+1)$th symmetric power, we prove the statement in the title using a theorem on the Brauer–Manin obstruction for rational points on such symmetric powers. The latter theorem is based on work of one of the authors with Swinnerton-Dyer (1994) and with Skorobogatov and Swinnerton-Dyer (1998), work generalising results of Salberger (1988).

Samenvatting

Voor $n = 2$ is de bewering in de titel een stelling van B. Poonen (2009). Hij gebruikt een één-parameter familie van variëteiten, en een stelling van Coray, Sansuc en één van de auteurs (1980), over de Brauer–Manin obstructie voor de rationale punten van deze variëteiten. Voor $n = p$, p een willekeurig priemgetal, beschouwden A. Várilly-Alvarado en B. Viray (2012) een analoge familie van variëteiten. We bewijzen de bewering in de titel door deze familie te vervangen door de $(2p + 1)$-de symmetrische macht ervan en door een stelling over de Brauer–Manin obstructie voor de rationale punten van zulke symmetrische machten toe te passen. Deze stelling steunt op werk van één van de auteurs met Swinnerton-Dyer (1994) en met Skorobogatov en Swinnerton-Dyer (1998). Dat werk veralgemeent resultaten van Salberger (1988).

1. Introduction

Soient k un corps et $n > 0$ un entier. Un sous-ensemble D de $\mathbf{A}^n(k) = k^n$ est dit diophantien s'il existe une k-variété Z et un k-morphisme $f : Z \to \mathbf{A}^n_k$ tel que $D = f(X(k))$. Dans cette définition, on peut supposer Z affine. On peut même supposer que Z est un sous-schéma fermé de $\mathbf{A}^{m+n}_k$ pour un certain m et que le morphisme f est induit par la projection $\mathbf{A}^{m+n}_k \to \mathbf{A}^n_k$. Une union finie de sous-ensembles diophantiens dans $\mathbf{A}^n(k)$ est un sous-ensemble diophantien. Une intersection finie de sous-ensembles diophantiens dans $\mathbf{A}^n(k)$ est un sous-ensemble diophantien : ceci résulte de l'existence des produits fibrés. Si K/k est une extension finie de corps, et D est diophantien dans $\mathbf{A}^n_K = K^n$, alors $D \cap k^n \subset K^n$ est diophantien dans $\mathbf{A}^n_k = k^n$: ceci résulte de l'existence du foncteur de restriction à la Weil pour les schémas affines sur un corps.

Received 20 January 2014, accepted in final form 20 February 2015, published online 22 June 2015.
2010 Mathematics Subject Classification 14G25 (primary), 11G35, 14C25, 11U99 (secondary).
Keywords: zero-cycles, Brauer–Manin obstruction, diophantine definitions.

Nous montrons (théorème 4.3) :

Pour tout corps de nombres k et tout entier $r > 1$, le complémentaire dans $k^\times$ de l'ensemble $k^{\times r}$ des puissances r-ièmes est un ensemble diophantien.

Pour r une puissance de 2, c'est un théorème de Poonen [Poo09a]. Une démonstration « élémentaire » du cas $r = 2$ sur $k = \mathbb{Q}$ vient d'être donnée par Königsmann [Kön13, proposition 20(b)].

Dans le cas $r = 2$, l'argument de Poonen utilise les surfaces de Châtelet d'équation affine

$$y^2 - az^2 = P(x)$$

avec $a \in k^\times$ et $P(x)$ polynôme séparable produit de deux polynômes $Q(x)$ et $R(x)$ de degré 2. Pour de telles surfaces, il est établi par Colliot-Thélène, Coray et Sansuc [CTCoSa80] que l'obstruction de Brauer–Manin est la seule obstruction au principe de Hasse pour les points rationnels sur de telles surfaces. Ce résultat est généralisé dans [CTSaSD87] à tout polynôme $P(x)$ de degré 4.

Poonen [Poo09a] part d'un contre-exemple au principe de Hasse d'équation $y^2 - bz^2 = Q(x)R(x)$ (il en existe sur tout corps de nombres [Poo09b]), puis considère la famille $\mathbb{U}_u$ à un paramètre $u \in k^\times$ de surfaces U_u d'équation $y^2 - buz^2 = Q(x)R(x)$.

Un point clé est que l'ensemble des $u \in k^\times$ sans obstruction de Brauer–Manin pour l'existence de points rationnels sur $\mathbb{U}_u$ est un ensemble diophantien, car d'après [CTCoSa80], c'est l'image des points k-rationnels de $\mathbb{U}_u$ par le k-morphisme $\mathbb{U}_u \to \mathbb{G}_{m,k}$ donné par la coordonnée u.

Dans le cas $r = p$ avec p premier quelconque, sur un corps de nombres k contenant une racine p-ième de 1, on considère les k-variétés définies par une équation

$$\mathrm{Norm}_{k((bu)^{1/p})/k}(\Xi) = P(x)$$

avec $b \in k^\times$ fixe, u variant dans $k^\times$, et $P(x)$ un polynôme séparable produit de deux polynômes $Q(x)$ et $R(x)$ de degré p. Sous l'hypothèse de Bouniakowsky–Dickson–Schinzel, Colliot-Thélène et Swinnerton-Dyer [CTSD94] montrent que l'obstruction de Brauer–Manin est la seule obstruction au principe de Hasse pour les points rationnels de telles variétés. C'est ce qui a permis à Várilly-Alvarado et Viray [VAV12] d'étendre, de façon conditionnelle, l'argument de Poonen à tout entier r.

L'article [CTSD94] établit aussi un résultat inconditionnel : pour des variétés du type ci-dessus, l'obstruction de Brauer–Manin à l'existence d'un zéro-cycle de degré 1 est la seule obstruction [CTSD94, théorème 5.1]. C'est une généralisation d'un résultat de Salberger [Sal88] sur les surfaces fibrées en coniques.

L'idée nouvelle du présent article est d'utiliser une version « effective » de ce résultat (corollaire 3.2) : Il existe un entier N, premier à p, indépendant de u, avec la propriété suivante. Pour $u \in k^\times$, sur un modèle projectif et lisse convenable $\mathbb{X}_u$ d'une variété ci-dessus, s'il n'y a pas d'obstruction de Brauer–Manin à l'existence d'un point rationnel, alors il existe un zéro-cycle effectif de degré N sur $\mathbb{X}_u$, ce qui se traduit par le fait que le produit symétrique $\mathrm{Sym}^N \mathbb{X}_u$ possède un k-point. Cela permet de montrer que le complémentaire de l'ensemble des points $u \in k^\times$ pour lesquels $\mathbb{X}_u(\mathbf{A}_k) \neq \emptyset$ et $\mathbb{X}_u(\mathbf{A}_k)^{\mathrm{Br}} = \emptyset$ est un ensemble diophantien. Le reste de l'argument (théorème 4.3) est alors comme dans [Poo09a].

Pour établir le résultat d'effectivité, nous reprenons les démonstrations de [CTSD94], dans la version plus souple développée dans [CTSkSD98] (théorème 3.1 et corollaire 3.2). La méthode donne $N = 2p + 1$. Comme nous l'a signalé O. Wittenberg au vu d'une précédente version de notre article, un résultat d'effectivité plus général a déjà été obtenu, comme conséquence aisée de [CTSkSD98], dans son article [Wittenb12].

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

Si l'on utilise un théorème d'effectivité purement algébrique annoncé par Salberger dans sa thèse [Sal85], mais non publié, une utilisation directe des résultats arithmétiques de [CTSD94] ou [CTSkSD98] donne $N = (p-1)^2$. Le résultat de Salberger [Sal85] est décrit au §6, la variante de la démonstration du théorème principal étant exposée au §5.

Rappels et notations

On note $A[n]$ le sous-groupe de n-torsion d'un groupe abélien A.

Soient k un corps et n un entier. On appelle extension cyclique K de k de degré n une k-algèbre étale K munie d'une action de $G = \mathbb{Z}/n$ sur K qui fait de $\operatorname{Spec} K \to \operatorname{Spec} k$ un G-torseur. En particulier, par extension cyclique de corps K/k, on entend dans ce texte une extension cyclique galoisienne de groupe $G = \mathbb{Z}/n$ muni du générateur $1 \in \mathbb{Z}/n$. Ceci définit une classe $\chi_{K/k} \in H^1(k, \mathbb{Z}/n)$. Pour $n \neq 0 \in k$, à tout élément $c \in k^\times$ on associe sa classe dans $k^\times/k^{\times n} \xrightarrow{\simeq} H^1(k, \mu_n)$.

Pour K/k une extension cyclique de degré n premier à la caractéristique de k, et $c \in k^\times$, on dispose de l'algèbre simple centrale cyclique $(K/k, c)$ de degré n, dont on note encore $(K/k, c)$ la classe dans le groupe de Brauer $\operatorname{Br} k$, qui est définie comme le cup-produit via

$$H^1(k, \mathbb{Z}/n) \times H^1(k, \mu_n) \to H^2(k, \mu_n)$$

de la classe $\chi_{K/k}$ et de la classe de c dans $k^\times/k^{\times n}$.

Supposons que k contient une racine primitive n-ième de 1, soit ζ. Le choix d'un isomorphisme $\mathbb{Z}/n \xrightarrow{\simeq} \mu_n$ permet d'identifier $H^1(k, \mathbb{Z}/n) = H^1(k, \mu_n) = k^\times/k^{\times n}$ et $(\operatorname{Br} k)[n] = H^2(k, \mu_n) = H^2(k, \mu_n^{\otimes 2})$. Étant donnés $b, c \in k^\times$, on note alors $(b, c)_\zeta \in (\operatorname{Br} k)[n]$ le cup-produit des classes b et c dans $k^\times/k^{\times n} = H^1(k, \mu_n)$. La k-algèbre $k(b^{1/n}) := k[t]/(t^n - b)$ est alors munie d'une structure d'extension cyclique de degré n, et l'on a $(k(b^{1/n})/k, c) = (b, c)_\zeta \in \operatorname{Br} k$.

La lecture du présent article requiert une certaine familiarité avec les articles [CTSD94, CTSkSD98, Poo09a].

2. Algèbre

Le lemme suivant est bien connu (cf. [GS06, Chapitres 4 et 5]).

Lemme 2.1. *Soit K/k une extension cyclique de corps de degré n premier à la caractéristique de k. Soit $c \in k^\times$.*

(i) *La k-variété affine Y d'équation $\operatorname{Norm}_{K/k}(\Xi) = c$ est un ouvert de la k-variété de Severi–Brauer X d'indice $n-1$ attachée à l'algèbre simple centrale $(K/k, c)$.*

(ii) *La k-variété Y possède un k-point si et seulement si la classe de $(K/k, c)$ est nulle dans $\operatorname{Br} k$.*

(iii) *On a une suite exacte*

$$\mathbb{Z}/n \to \operatorname{Br} k \to \operatorname{Br} X \to 0,$$

où $1 \in \mathbb{Z}/n$ a pour image $(K/k, c) \in \operatorname{Br} k$.

Démonstration. En utilisant [GS06], on établit ce lemme bien connu, à un point près. L'exercice [GS06, exercice 1], où il convient de remplacer bx par bx^n, donne un énoncé d'équivalence birationnelle stable au lieu de (i) ci-dessus. Esquissons comment l'on obtient (i). On a les suites exactes de k-tores

$$1 \to R^1_{K/k}\mathbb{G}_m \to R_{K/k}\mathbb{G}_m \xrightarrow{\operatorname{Norm}_{K/k}} \mathbb{G}_{m,k} \to 1$$

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

et

$$1 \to \mathbb{G}_{m,k} \xrightarrow{x \mapsto x} R_{K/k}\mathbb{G}_m \to R_{K/k}\mathbb{G}_m/\mathbb{G}_{m,k} \to 1.$$

Notons $T_1 = R^1_{K/k}\mathbb{G}_m$ et $T = R_{K/k}\mathbb{G}_m/\mathbb{G}_{m,k}$. Le choix d'un générateur de $\mathrm{Gal}(K/k)$ définit un isomorphisme de k-tores $T_1 \xrightarrow{\simeq} T$. La k-variété Y est un espace principal homogène sous le k-tore T_1. C'est donc aussi un espace principal homogène sous le k-tore T. On a un plongement torique, de $R_{K/k}\mathbb{G}_m$ dans $W := R_{K/k}\mathbb{G}_a\backslash\{0\} \simeq \mathbf{A}^n_k\backslash\{0\}$, qui induit un plongement torique de T dans le quotient de W par l'action diagonale de $\mathbb{G}_{m,k}$, quotient qui s'identifie à l'espace projectif $\mathbf{P}^{n-1}_k$. La k-variété Y est donc un ouvert dans la k-variété $X = Y \times^T \mathbf{P}^{n-1}_k$ quotient de $Y \times \mathbf{P}^{n-1}_k$ par l'action diagonale de T. Cette k-variété X est une forme tordue de l'espace projectif. On a le diagramme commutatif de k-groupes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{G}_{m,k} & \longrightarrow & R_{K/k}\mathbb{G}_m & \longrightarrow & T & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{G}_{m,k} & \longrightarrow & GL_{n,k} & \longrightarrow & PGL_{n,k} & \longrightarrow & 1. \end{array}$$

Ce diagramme induit un diagramme commutatif

$$\begin{array}{ccc} H^1(k,T) & \longrightarrow & \mathrm{Br}\, k \\ \downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ H^1(k,PGL_{n,k}) & \longrightarrow & \mathrm{Br}\, k. \end{array}$$

La flèche $H^1(k,T) \to H^1(k,PGL_{n,k})$ envoie la classe de Y sur la classe de X, et le composé $k^\times/N_{K/k}K^\times \xrightarrow{\simeq} H^1(k,T_1) \xrightarrow{\simeq} H^1(k,T) \to \mathrm{Br}\, k$ envoie la classe de c sur la classe de l'algèbre cyclique $(K/k,c)$ (cf. [GS06, corollaire 4.7.4]). Quant à la flèche $H^1(k,PGL_{n,k}) \to \mathrm{Br}\, k$, elle envoie la classe d'isomorphie d'une variété de Severi–Brauer d'indice $n-1$ sur sa classe dans le groupe de Brauer. □

Proposition 2.2. *Soit k un corps de caractéristique zéro. Soient p un nombre premier et $P(x) \in k[x]$ un polynôme séparable de degré $2p$. Soit K/k une extension galoisienne cyclique, de groupe $G = \mathbb{Z}/p$. Soit U la k-variété définie par*

$$\mathrm{Norm}_{K/k}(\Xi) = P(x) \neq 0.$$

(i) *Il existe une k-compactification lisse X de U, équipée d'un morphisme $\pi : X \to \mathbf{P}^1_k$ étendant l'application $(\Xi, x) \mapsto x$, dont la fibre générique $X_\eta/k(\mathbf{P}^1)$ est une variété de Severi–Brauer de dimension $p-1$, d'algèbre simple centrale associée l'algèbre cyclique $(K/k, P(x))$, telle que pour M point fermé de $\mathbf{P}^1_k$ non zéro de $P(x)$, la fibre X_M est une variété de Severi–Brauer sur le corps résiduel $k(M)$.*

(ii) *Si K n'est pas un corps, alors la k-variété X est k-birationnelle à $\mathbf{P}^p_k$, et $\mathrm{Br}\, k = \mathrm{Br}\, X$.*

(iii) *Supposons que K est un corps, et que $P(x) = Q(x).R(x)$ avec $Q(x)$ et $R(x)$ irréductibles de degré p et sans zéro dans K. Alors les algèbres cycliques $(K/k, Q(x))$ et $(K/k, R(x))$ dans $\mathrm{Br}\, k(x)$ ont une image dans $\mathrm{Br}\, k(X)$ qui appartient à $\mathrm{Br}\, X$, et le quotient de $\mathrm{Br}\, X$ par l'image de $\mathrm{Br}\, k$ est un groupe cyclique d'ordre p engendré par l'image de $(K/k, Q(x))$.*

Démonstration. On considère la k-variété d'équation

$$\mathrm{Norm}_{K/k}(\Xi) = P(x)$$

et $U_1 \subset U$ l'ouvert maximal sur lequel la projection $U_1 \to \mathbf{A}^1_k = \mathrm{Spec}\ k[x]$ définie par x est lisse.

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

Soit V la k-variété V d'équation

$$\mathrm{Norm}_{K/k}(\Theta) = P'(y)$$

avec $P'(y) := y^{2p}P(1/y)$. Soit $V_1 \subset V$ l'ouvert maximal sur lequel le morphisme $V_1 \to \mathbf{A}^1_k = \mathrm{Spec}\ k[y]$ défini par y est lisse.

On recolle la k-variété U_1 et la k-variété V_1 en une k-variété W via $x = 1/y$ et $y^2.\Xi = \Theta$. On dispose donc d'un k-morphisme $W \to \mathbf{P}^1_k$ à fibres lisses, dont toutes les fibres sauf celles au-dessus des points fermés à support dans $P(x) = 0$ sont géométriquement intègres.

Une variante du lemme 2.1 permet alors de construire une k-variété W' lisse équipée d'un morphisme $W' \to \mathbf{P}^1_k$ dont les fibres au-dessus des points fermés autres que ceux supportés dans $P(x) = 0$ sont des variétés de Severi–Brauer, et dont les fibres en les points fermés supportés dans $P(x) = 0$ sont les fibres de $W \to \mathbf{P}^1_k$. En utilisant le théorème d'Hironaka, on obtient alors l'existence d'une k-variété projective lisse X munie d'un k-morphisme $\pi : X \to \mathbf{P}^1_k$, contenant W' comme ouvert, le morphisme π étendant $W' \to \mathbf{P}^1_k$, ce qui établit le point (i). (Après la rédaction de notre article, une construction évitant le recours au théorème d'Hironaka a été donnée [VAV15], complétant ainsi [VAV12].)

L'énoncé (ii) est évident : si K n'est pas un corps, alors $\mathrm{Norm}_{K/k}(\Xi)$ s'écrit comme un produit de variables indépendantes, et la k-variété définie par l'équation

$$Y_1 \dots Y_p = P(x) \neq 0$$

est clairement k-rationnelle.

L'énoncé (iii) est essentiellement démontré dans [CTSD94, §2.2, théorème 2.2.1]. Nous donnons les points principaux de la démonstration, renvoyant le lecteur à [CTSD94, §1 et §2] pour des explications plus détaillées.

On fixe un générateur σ de $\mathrm{Gal}(K/k)$, et on note $(K/k, c) = (K/k, \sigma, c)$.

On a la suite exacte (lemme 2.1)

$$\mathbb{Z}/p.(\alpha) \to \mathrm{Br}\, k(\mathbf{P}^1) \xrightarrow{\pi^*} \mathrm{Br}\, X_\eta \to 0,$$

où $\alpha = (K(x)/k(x), P(x))$, qu'on note $(K/k, P(x))$. Soit $\gamma \in \mathrm{Br}\, X \subset \mathrm{Br}\, X_\eta$. Il existe donc un élément $\beta \in \mathrm{Br}\, k(\mathbf{P}^1)$ tel que $\gamma = \pi^*(\beta)$.

Les fibres de π aux points fermés de $\mathbf{A}^1_k = \mathrm{Spec}\ k[x]$ autres que ceux définis par $Q = 0$ et $R = 0$ sont lisses et géométriquement intègres. La comparaison des résidus de γ et de β entraîne que les résidus de β en tout point fermé de $\mathbf{A}^1_k$ autre que $Q = 0$ et $R = 0$ sont nuls. La comparaison des résidus de γ et de β au-dessus de $Q = 0$, resp. de $R = 0$, sur l'ouvert $U_1 \subset X$, montre aussi que $\mathrm{Res}_Q(\beta) \in H^1(k_Q, \mathbb{Q}/\mathbb{Z})$, resp. $\mathrm{Res}_R(\beta) \in H^1(k_R, \mathbb{Q}/\mathbb{Z})$, où k_Q, resp. k_R, désigne le corps résiduel en $Q = 0$, resp. en $R = 0$, s'annulent par passage à $K \otimes_k k_Q$, resp. $K \otimes_k k_R$. Les groupes $H^1(K \otimes_k k_Q/k_Q, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/p$, et $H^1(K \otimes_k k_R/k_R, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/p$ sont engendrés par l'image d'un générateur χ de $H^1(K/k, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/p$. La k-algèbre $(K/k, Q(x))$ a sur $\mathbf{A}^1_k$ pour seul résidu χ_{k_Q} en $Q = 0$. La k-algèbre $(K/k, R(x))$ a sur $\mathbf{A}^1_k$ pour seul résidu χ_{k_R} en $R = 0$. On voit donc qu'il existe des entiers r et s tels que

$$\beta - (K/k, Q(x)^r) - (K/k, R(x)^s)$$

ait tous ses résidus triviaux sur $\mathbf{A}^1_k$, donc par la suite exacte de Faddeev (cf. [CTSD94, §1.2]) soit dans l'image de $\mathrm{Br}\, k$. Comme la classe $\alpha = (K/k, P(x)) \in \mathrm{Br}\, k(\mathbf{P}^1)$ a une image nulle dans $\mathrm{Br}\, k(X)$, on voit que $\gamma \in \mathrm{Br}\, X \subset \mathrm{Br}\, k(X)$ est la somme d'un multiple de $\pi^*(K/k, Q(x))$ et d'une

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

classe dans $\mathrm{Br}\, k$. Nous renvoyons à [CTSD94, théorème 2.2.1] pour la démonstration du fait que $\pi^*(K/k, Q(x))$ appartient à $\mathrm{Br}\, X$, démonstration qui utilise le fait que le degré de Q est p. Si la classe $\pi^*(K/k, Q(x)) \in \mathrm{Br}\, k(X)$ appartenait à l'image de $\mathrm{Br}\, k$, d'après le lemme 2.1 il existerait un entier r tel que

$$(K/k, Q(x)) - r(K/k, P(x)) = (K/k, Q(x)) - r(K/k, Q(x)R(x)) \in \mathrm{Br}\, k(x)$$

appartienne à $\mathrm{Br}\, k$. Le calcul du résidu d'un tel élément au point fermé $R(x) = 0$ donne $r = 0$. Et le résidu de $(K/k, Q(x))$ en $Q(x) = 0$ n'est pas nul. Ainsi $\mathrm{Br}\, X/\mathrm{Br}\, k$ est d'ordre p, engendré par la classe $\pi^*(K/k, Q(x))$. Le calcul de résidu a utilisé le fait que ni Q ni R n'ont de zéro dans K. □

3. Arithmétique

Soient k un corps de nombres et Ω l'ensemble de ses places. Pour $v \in \Omega$, on note k_v le complété de k en v et pour v non archimédienne, $\mathbb{F}_v$ le corps résiduel en v.

Comme mentionné dans l'introduction, le théorème suivant, avec précisément la même borne $d \geqslant d_0$, est un cas particulier d'un résultat de Wittenberg [Wittenb12, théorème 4.8], résultat qui est une conséquence de [CTSkSD98, théorème 4.1]. Comme nous partons ici d'une hypothèse sur les points rationnels et non sur les zéro-cycles, la démonstration que nous proposons ici est plus courte que celle de [Wittenb12, théorème 4.8] (qui elle-même fait appel sans en répéter les détails à la démonstration de [CTSkSD98, théorème 4.1]).

Théorème 3.1. *Soient k un corps de nombres et X une k-variété projective, lisse, géométriquement intègre, équipée d'un morphisme projectif et plat $\pi : X \to \mathbf{P}^1_k$ à fibre générique géométriquement intègre. Soit d_0 la somme des degrés sur k des points fermés de $\mathbf{P}^1_k$ dont la fibre n'est pas lisse.*

Supposons :

(i) *Pour tout point fermé $M \in \mathbf{P}^1_k$, de corps résiduel $k(M)$, la fibre $X_M/k(M)$ contient une composante irréductible $Z \subset X_M$, de multiplicité 1, telle que la fermeture algébrique de $k(M)$ dans le corps des fonctions de Z est une extension abélienne de $k(M)$.*

(ii) *Il existe un adèle dans $X(\mathbf{A}_k)$ orthogonal au groupe de Brauer vertical de X, c'est-à-dire au sous-groupe de $\mathrm{Br}\, X$ dont l'image dans $\mathrm{Br}\, k(X)$ appartient à $\pi^*(\mathrm{Br}\, k(\mathbf{P}^1))$.*

(iii) *Le principe de Hasse vaut pour les fibres lisses de π au-dessus de tout point fermé de $\mathbf{P}^1_k$.*

Alors, pour tout entier $d \geqslant d_0$, et tout ouvert de Zariski non vide $V \subset \mathbf{P}^1_k$, il existe un point fermé $m \in V$ de degré d sur k, à fibre X_m lisse contenant un $k(m)$-point rationnel.

Démonstration. On peut supposer que la fibre de π au-dessus du point à l'infini de $\mathbf{P}^1_k$ est lisse. Soit $V \subset \mathbf{A}^1_k$ le complémentaire de l'ensemble des points fermés M dont la fibre $X_M/k(M)$ n'est pas lisse. Soit $U = \pi^{-1}(V)$. La projection $\pi : U \to V$ est donc lisse. Soient $\{M_i\}_{i\in I}$ les points fermés de $\mathbf{A}^1_k = \mathrm{Spec}\, k[t]$ non dans V. Notons $k_i = k(M_i)$ le corps résiduel en M_i. Soit e_i un générateur de k_i sur k. D'après l'hypothèse (i), pour chaque point M_i, on peut choisir une composante irréductible Z_i de multiplicité 1 dans la fibre de M_i telle que la fermeture intégrale K_i de k_i dans le corps des fonctions de Z_i soit une extension abélienne de k_i. Écrivons cette extension comme un composé d'extensions cycliques $K_{i,j}/k_i$, $j \in J_i$. Définissons

$$A_{i,j} = \mathrm{Cores}_{k_i/k}(K_{i,j}/k_i, t - e_i) \in \mathrm{Br}\, k(t).$$

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

En appliquant le « lemme formel » d'Harari [Har94, corollaire 2.6.1] à la famille finie des $A_{i,j}$, on déduit de l'hypothèse (ii) l'existence d'un ensemble fini S_1 de places de k, contenant l'ensemble S des places de « mauvaise réduction », et de points $p_v \in U(k_v)$ pour $v \in S_1$, tels que l'on ait

$$\sum_{v\in S_1} A_{i,j}(p_v) = 0 \in \mathbb{Q}/\mathbb{Z}.$$

En utilisant le théorème des fonctions implicites, pour chaque place $v \in S_1$ on peut trouver des $p_{v,l} \in U(k_v)$, $l = 1, \dots, d$, d'images respectives $m_{v,l} = \pi(p_{v,l})$, tous distincts dans $V(k_v)$, tels que $A_{i,j}(p_{v,l}) = A_{i,j}(p_v) \in \operatorname{Br} k_v \subset \mathbb{Q}/\mathbb{Z}$ pour tout l.

Pour chaque $v \in S_1$ on définit le zéro-cycle z_v sur U,

$$z_v = \sum_{l=1}^{d} p_{v,l}.$$

Soit $G_v(t)$ le polynôme unitaire de degré d, de diviseur $\pi(z_v)$ sur $\mathbf{A}^1_{k_v}$. Les fibres lisses au-dessus des racines de G_v ont des points rationnels sur leurs corps de définition.

En utilisant une méthode due à Salberger et explicitée dans [CTSkSD98, théorème 3.1], on construit alors un polynôme unitaire irréductible $G(t) \in k[t]$, de degré d, proche des $G_v(t)$ pour $v \in S_1$, satisfaisant certaines propriétés qui impliquent, par les arguments et calculs dans [CTSkSD98, §4, pp. 20–21] (qui utilisent les égalités $\sum_{v\in S_1} A_{i,j}(p_v) = 0$), que le point fermé $m \in U$ défini par $G(t) = 0$ a une fibre lisse $X_m/k(m)$ qui possède des points dans tous les complétés de $k(m)$. D'après l'hypothèse (iii), cette fibre X_m a donc un $k(m)$-point rationnel. □

Soient k un corps parfait et $\overline{k}$ une clôture séparable de k. Pour $N > 0$ entier, et toute k-variété quasi-projective U, on note $\operatorname{Sym}^N U$ le quotient de l'action du groupe symétrique $\mathfrak{S}_N$ sur le produit U^N. On a une bijection entre les ensembles suivants :

(i) Les k-points de $\operatorname{Sym}^N U$.

(ii) Les zéro-cycles effectifs de degré N sur U.

(iii) Les zéro-cycles effectifs de degré N sur $U \times_k \overline{k}$ qui sont invariants sous l'action de $\operatorname{Gal}(\overline{k}/k)$.

La bijection entre (ii) et (iii) est claire. Pour tout k-point de $\operatorname{Sym}^N U$ on choisit un relèvement $(P_1, \dots, P_N) \in U^N(\overline{k})$. Le zéro-cycle $P_1 + \cdots + P_N$ est invariant sous $\operatorname{Gal}(\overline{k}/k)$. Inversement si $P_1 + \cdots + P_N$ est un zéro-cycle effectif de degré N sur $U \times_k \overline{k}$ invariant sous l'action de $\operatorname{Gal}(\overline{k}/k)$, alors l'image de $(P_1, \dots, P_N) \in U^N(\overline{k})$ dans $(\operatorname{Sym}^N U)(\overline{k})$ est invariante sous $\operatorname{Gal}(\overline{k}/k)$, donc définit un k-point de $\operatorname{Sym}^N U$.

Corollaire 3.2. *Soit k un corps de nombres. Soit K/k une extension finie cyclique de corps, de degré premier p. Soit $P(x) = Q(x)R(x)$ un polynôme séparable de degré $2p$ produit de deux polynômes irréductibles de degré p. Soit $U = U(K/k, P)$ la k-variété affine, lisse, intègre définie par l'équation*

$$\operatorname{Norm}_{K/k}(\Xi) = P(x) \neq 0.$$

Soit X une k-variété projective et lisse, géométriquement intègre, contenant U comme ouvert dense. S'il existe un élément $\{M_v\}$ du produit $\prod_{v\in\Omega} U(k_v)$ orthogonal à $(K/k, Q(x)) \in \operatorname{Br} X$, alors il existe une extension de corps L/k de degré $2p+1$ avec $U(L) \neq \emptyset$. En particulier les k-variétés $\operatorname{Sym}^{2p+1} U$ et $\operatorname{Sym}^{2p+1} X$ possèdent un k-point.

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

Démonstration. D'après la proposition 2.2, il existe un tel modèle X. Les propriétés d'invariance birationnelle du groupe de Brauer montrent que l'énoncé ne dépend pas du choix du modèle. D'après la proposition 2.2, les classes $(K/k, Q(x))_{k(X)}$ et $(K/k, R(x))_{k(X)}$ sont chacune dans $\mathrm{Br}\, X$, leur somme dans $\mathrm{Br}\, k(X)$ est dans l'image de $\mathrm{Br}\, k$, et ce sont des générateurs de $\mathrm{Br}\, X$. Les hypothèses du théorème 3.1 sont clairement satisfaites, avec $d_0 = 2p$. On choisit ici $d = 2p+1$. □

Remarque 3.3. Dans le cadre du corollaire, les seuls $A_{i,j}$ intervenant dans la preuve du théorème 3.1 sont $(K/k, Q(x))_{k(X)}$ et $(K/k, R(x))_{k(X)}$, et ces éléments de $\mathrm{Br}\, k(X)$ sont ici dans $\mathrm{Br}\, X$. On n'a donc pas besoin ici d'invoquer le lemme formel d'Harari, l'hypothèse $X(\mathbf{A}_k)^{\mathrm{Br}} \neq \emptyset$ donne directement des égalités

$$\sum_{v \in S_1} A_{i,j}(M_v) = \sum_{v \in \Omega} A_{i,j}(M_v) = 0 \in \mathbb{Q}/\mathbb{Z},$$

avec M_v comme dans l'énoncé du corollaire, et avec S_1 égal à l'ensemble fini S évident des places de mauvaise réduction.

Si l'on se limite à p premier impair, ce qui suffirait ici, le cas $p = 2$ ayant déjà été traité par Poonen [Poo09a], on peut aussi éviter les difficultés spécifiques aux places réelles (voir à ce sujet [CTSD94, p. 82, l. 6/8] et [CTSkSD98, p. 17, l. 9/11]).

Proposition 3.4. *Soient p un nombre premier et k un corps de nombres contenant une racine primitive p-ième de l'unité ζ. Il existe $d \in k^\times$, $d \notin k^{\times p}$ et un polynôme séparable $P(x) = Q(x)R(x) \in k[x]$ avec $Q(x)$ et $R(x)$ irréductibles de degré p, sans zéro dans $K = k(d^{1/p})$, tels que toute k-variété X projective, lisse, géométriquement connexe k-birationnelle à la k-variété $U = U(K/k, P)$ d'équation affine*

$$\mathrm{Norm}_{K/k}(\Xi) = P(x) \neq 0$$

satisfasse :

(i) *X possède des points rationnels dans tous les complétés k_v de k.*

(ii) *X ne possède pas de zéro-cycle de degré 1. Plus précisément, l'algèbre $A = (K/k, Q(x)) = (d, Q(x))_\zeta \in \mathrm{Br}\, k(X)$ appartient à $\mathrm{Br}\, X$ et, pour toute famille $\{z_v\}$, $v \in \Omega$, de zéro-cycles de degré 1 sur X, on a*

$$\sum_{v \in \Omega} A(z_v) \neq 0 \in \mathbb{Q}/\mathbb{Z}.$$

(iii) *On a $(\mathrm{Sym}^{2p+1} U)(k) = \emptyset$ et $(\mathrm{Sym}^{2p+1} X)(k) = \emptyset$.*

Démonstration. Si une k-variété X satisfait (i) et (ii), toute autre k-variété projective, lisse, géométriquement connexe k-birationnelle à X satisfait (i) et (ii).

L'énoncé (iii) est une conséquence immédiate de l'énoncé (ii). En effet U possède de façon évidente un point dans une extension de degré p.

Poonen [Poo09b, §5, proposition 5.1] (cas $p = 2$) puis de façon semblable Várilly-Alvarado et Viray [VAV12, proposition 4.1] (cas p impair) construisent (au moins birationnellement) une telle variété X avec des points rationnels dans tous les k_v mais telle qu'il y ait obstruction de Brauer–Manin à l'existence d'un point rationnel. Nous allons montrer que leur exemple satisfait aussi l'énoncé analogue pour les zéro-cycles de degré 1, à savoir l'énoncé (ii) de la proposition. Ceci ne résulte pas formellement du cas des points rationnels (cf. [CTSD94, §10]).

Soit $M \in \mathbb{N}$ un entier tel que toute courbe plane projective lisse (et donc géométriquement intègre) de degré p sur un corps fini $\mathbb{F}$ de cardinal au moins M possède au moins $2p+1$ points $\mathbb{F}$-rationnels.

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

En utilisant le théorème de densité de Chebotarev et la théorie du corps de classes, on trouve $a, b, c \in k$ avec les propriétés suivantes :

(1) $b \in O_k$, bO_k idéal premier, $b \equiv 1 \bmod (1-\zeta)^{2p-1}O_k$, $b \gg 0$ et $\#\mathbb{F}_b > M$,

(2) $a \in O_k$, aO_k idéal premier distinct de bO_k, $a \equiv 1 \bmod (1-\zeta)^{2p-1}O_k$, $a \notin k_b^{\times p}$, $a \gg 0$ et $\#\mathbb{F}_a > M$,

(3) $c \in O_k$, $b \mid ac+1$.

Soient $d = ab$ et K le corps $k(d^{1/p})$. Soient $Q(x) = x^p + c$ et $R(x) = ax^p + ac + 1$.

Soit X une k-variété projective, lisse, géométriquement connexe et k-birationnelle à la k-variété U d'équation

$$\mathrm{Norm}_{K/k}(\Xi) = Q(x)R(x) \neq 0.$$

Suivant [Poo09b, lemme 5.3], montrons que l'on a $U(k_v) \neq \emptyset$ pour toute place v.

Comme on a $d \gg 0$, on a $U(k_v) \neq \emptyset$ pour toute place archimédienne.

Soit v une place finie de k différente de $v = v_a$, $v = v_b$ et telle que $v(p) = 0$. L'extension $k(d^{1/p})/k$ est non ramifiée en v. Pour tout $x \in k_v$ avec $v(x) < 0$, on a $v(P(x)) = 2p$, on a donc des points dans $U(k_v)$ avec un tel x.

Soit v une place avec $v(p) > 0$. L'entier d satisfait $d = ab \equiv 1 \bmod (1-\zeta)^{2p-1}O_k$. Soit $h(x) = x^p - d$. Les éléments p et $(1-\zeta)^{p-1}$ diffèrent par une unité dans $\mathbb{Q}(\zeta)$. On en déduit $v(h(1)) > 2v(h'(1))$, où $h'(x) = px^{p-1}$ est le polynôme dérivé de $h(x)$. Le lemme de Hensel assure alors l'existence d'une solution (entière et congrue à 1 modulo v) de $x^p - d = 0$ dans k_v. On a donc $U(k_v) \neq \emptyset$.

Soit $v = v_b$. Alors a et c sont des unités dans k_v. Les hypothèses assurent que la courbe affine lisse $z^p = a(x^p + c) \neq 0$ sur le corps $\mathbb{F}_v$ possède un point $\mathbb{F}_v$-rationnel. Il en est donc de même de la courbe $z^p = (x^p + c)(ax^p + ac + 1) \neq 0$ puisque $v_b(ac+1) > 0$. Par le lemme de Hensel, un tel point se relève en un point de $z^p = (x^p + c)(a(x^p + c) + 1) \neq 0$ dans k_v. Ainsi $U(k_v) \neq \emptyset$.

Soit $v = v_a$. Sur le corps $\mathbb{F}_v$, on trouve une solution de l'équation $z^p = x^p + c \neq 0$, donc une solution de $z^p = (x^p + c)(a(x^p + c) + 1) \neq 0$. Une telle solution se relève en une solution de l'équation $z^p = (x^p + c)(a(x^p + c) + 1) \neq 0$ dans k_v. On a donc $U(k_v) \neq \emptyset$.

D'après la proposition 2.2, l'algèbre cyclique $A = (K/k, Q(x)) = (d, Q(x))_\zeta$ appartient au groupe $\mathrm{Br}\, X$.

Soit v une place de k et soit L/k_v une extension finie de corps, et w l'extension de v à L. L'application $ev_A : X(L) \to \mathrm{Br}\, L \subset \mathbb{Q}/\mathbb{Z}$ obtenue par évaluation de A est continue. Par le théorème des fonctions implicites, son image est la même que l'image de l'évaluation de A sur $U(L)$:

$$ev_A : U(L) \to \mathrm{Br}\, L \subset \mathbb{Q}/\mathbb{Z}, \quad P \mapsto A(P).$$

Si d est une puissance p-ième dans L, l'image de ev_A est clairement nulle. C'est le cas pour v place complexe et aussi pour v une place réelle, puisque l'on a $a \gg 0$ et $b \gg 0$, et donc $d \gg 0$. C'est aussi le cas si $v(p) > 0$.

Soit v une place non archimédienne de k distincte de v_a et de v_b, avec $v(p) = 0$. Si d est une puissance p-ième dans L, l'image de ev_A est nulle. Supposons que d ne soit pas une puissance p-ième dans L. L'extension de corps locaux KL/L est non ramifiée, les normes sont exactement les éléments de valuation divisible par p. Soit $(\Xi, x) \in U(L)$. De l'équation de U on déduit

$$w(Q(x)) + w(R(x)) \equiv 0 \bmod p.$$

Si $w(x) < 0$, alors $w(Q(x)) = w(x^p + c) = pw(x) \equiv 0 \bmod p$. Supposons $w(x) \geqslant 0$. On a

$$(ax^p + ac + 1) - a(x^p + c) = 1.$$

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

On a donc soit $0 = w(ax^p + ac + 1)$ soit $0 = w(a) + w(x^p + c) = w(x^p + c)$. Donc $w(Q(x)) = 0$ ou $w(R(x)) = 0$. Comme on a $w(Q(x)) + w(R(x)) \equiv 0 \bmod p$, on en déduit $w(Q(x)) \equiv 0 \bmod p$. Dans tous les cas, on a donc $w(Q(x)) \equiv 0 \bmod p$, et ceci implique $(d, Q(x))_\zeta = 0$. On voit donc que pour toute place v non archimédienne de k distincte de v_a et de v_b, et toute extension finie L/k_v, l'application $ev_A : U(L) \to \operatorname{Br} L \subset \mathbb{Q}/\mathbb{Z}$ a son image nulle.

Soit $v = v_a$. Si $w(x) < 0$ alors $Q(x) = x^p + c$ est une puissance p-ième dans L, donc $(d, Q(x))_\zeta = 0$. Supposons $w(x) \geqslant 0$. Alors $ax^p + ac + 1 \equiv 1 \bmod a$, ce qui implique que $R(x) = ax^p + ac + 1$ est une puissance p-ième dans L, et donc $(d, Q(x))_\zeta = (d, R(x))_\zeta = 0$.

On voit donc que, pour toute place $v \neq v_b$ et tout zéro-cycle z_v sur X_{k_v}, on a $A(z_v) = 0$.

Soit enfin $v = v_b$. L'équation de U donne

$$(d, Q(x))_\zeta + (d, R(x)_\zeta) = 0 \in \mathbb{Z}/p \subset \mathbb{Q}/\mathbb{Z} = \operatorname{Br} L.$$

Supposons $w(x) \neq 0$. On a $w(ac + 1) > 0$. Ainsi $R(x) = ax^p + ac + 1$ est le produit de a et d'une puissance p-ième dans L. Donc $(d, R(x))_\zeta = (ab, a)_\zeta$, et donc $(d, Q(x))_\zeta = -(ab, a)_\zeta \in \mathbb{Z}/p$. Supposons $w(x) > 0$. De $w(ac + 1) > 0$ on déduit que c est une unité dans L et que $-ac$ est une puissance p-ième dans L. Alors $Q(x) = x^p + c$ est le produit de $-a^{-1}$ et d'une puissance p-ième dans L, donc $(d, Q(x))_\zeta = (ab, -a^{-1})_\zeta = -(ab, -a)_\zeta$. Si p est impair, -1 est une puissance p-ième, donc $-(ab, a)_\zeta = -(ab, -a)_\zeta$. Si $p = 2$, on a encore cette égalité, car $(ab, -1)_{v_b} = 0$ [Poo09b, lemme 5.2]. Ceci est établi en utilisant $(a, -1)_{v_b} = 0$ (facile) et $(b, -1)_{v_b} = 0$ (obtenu via la formule du produit). En conclusion, pour $v = v_b$, toute extension finie L de k_{v_b} et tout point $P \in U(L)$, on a $A(P) = -(ab, -a)_\zeta = (b^{-1}, -a)_\zeta = (b^{-1}, a)_\zeta \in \operatorname{Br} L$.

Pour toute extension finie E/F de corps, le composé $\operatorname{Br} F \to \operatorname{Br} E \to \operatorname{Br} F$ de la restriction et de la corestriction est la multiplication par le degré $[E : F]$. Pour $v = v_b$ et $z_{v_b} = \sum_i n_i P_i$ un zéro-cycle sur X_{k_v}, la valeur prise par A sur ce zéro-cycle est donc

$$\sum n_i [k(P_i) : k](b^{-1}, a)_\zeta \in \operatorname{Br} k_v,$$

soit encore $\deg(z_{v_b})(b^{-1}, a)_\zeta \in \operatorname{Br} k_{v_b}$. Si le zéro-cycle z_{v_b} est de degré 1, la valeur prise est

$$[(b^{-1}, a)_\zeta]_{v_b} \in \operatorname{Br} k_{v_b} \subset \mathbb{Z}/p,$$

et cette classe est non nulle, car l'unité a n'est pas une puissance p-ième dans le corps résiduel de k_{v_b}.

On voit donc que pour toute famille $\{z_v\}, v \in \Omega$, de zéro-cycles de degré 1 sur X, on a

$$\sum_{v \in \Omega} A(z_v) = [(b^{-1}, a)_\zeta]_{v_b} \neq 0 \in \mathbb{Q}/\mathbb{Z}. \qquad \square$$

4. Le théorème

Soient p un nombre premier et k un corps de nombres contenant une racine primitive p-ième ζ de 1, qu'on fixe, déterminant ainsi un isomorphisme $\mathbb{Z}/p \xrightarrow{\sim} \mu_p$ sur k. Soient $a, b, c, d \in k$, puis $Q(x), R(x)$ et $P(x) = Q(x)R(x)$ comme dans la proposition 3.4 et sa démonstration.

Soient $A = k[u, 1/u]$ et $B = k[u, 1/u][v]/(v^p - du)$, avec le plongement évident $A \hookrightarrow B$, qui fait de Spec B un A-schéma fini étale, plus précisément un $\mathbb{Z}/p$-torseur.

Soit $\mathbb{U}$ le R-schéma lisse défini par

$$\operatorname{Norm}_{B/A}(\Xi) = P(x) \neq 0,$$

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

où $\Xi = \sum_{i=0}^{p-1} v^i x_i$. Le schéma $\mathbb{U}$ est affine, car donné par le système

$$\mathrm{Norm}_{B/A}(\Xi) = P(x), \quad P(x)y - 1 = 0.$$

La fibre de $\mathbb{U}/R$ en un point $u \in \mathrm{Spec}\ R$ est notée $\mathbb{U}_u$. Pour u un k-point, $\mathbb{U}_u = U(k((du)^{1/p})/k, P(x))$.

En utilisant le théorème d'Hironaka, on construit un A-schéma intègre $\mathbb{X}$, projectif et lisse sur A, contenant le A-schéma $\mathbb{U}$ comme ouvert, tel que pour tout k-homomorphisme $A \to k$, c'est-à-dire pour tout choix de $u \in k^\times$, le A-schéma $\mathbb{X}$ se spécialise en une k-variété projective, lisse, géométriquement intègre $\mathbb{X}_u = X_{k((du)^{1/p})/k}$ contenant $U(k((du)^{1/p})/k, P(x))$ comme ouvert dense.

LEMME 4.1. *Soit C la k-courbe lisse définie par l'équation*

$$z^p = Q(x)R(x) \neq 0.$$

Il existe un ensemble fini S de places de k, contenant les places archimédiennes, tel que, pour toute place $v \notin S$,

(i) *on a $C(k_v) \neq \emptyset$;*

(ii) *pour tout $u \in k_v^\times$ de valuation v-adique $v(u)$ non nulle modulo p, l'algèbre $(u, Q(x))_\zeta$, quand évaluée sur $C(k_v)$, prend toutes les valeurs dans $\mathbb{Z}/p \subset \mathrm{Br}\, k_v$.*

Démonstration. Soit v une place finie telle que $Q(x)R(x)$ ait ses coefficients dans l'anneau O_v des entiers de k_v, son coefficient dominant une unité dans O_v, et que p soit inversible dans O_v. Soit $\mathbb{F}_v$ le corps résiduel en v. La $\mathbb{F}_v$-courbe C_γ définie par

$$z_1^p = \gamma Q(x) \neq 0, \quad z_2^p = \gamma^{-1} R(x) \neq 0,$$

est lisse et géométriquement intègre. Son modèle projectif évident dans $\mathbf{P}^3$ est une courbe intersection complète lisse D_γ de deux surfaces de degré p, le genre de D_γ est donc $p^3 - 2p^2 + 1$. Sur une clôture algébrique du corps de base, on vérifie immédiatement que le complémentaire de C_γ dans D_γ est formé de $3p^2$ points.

Si le cardinal de $\mathbb{F}_v$ est plus grand qu'une constante dépendant seulement de l'entier p, par les estimations de Weil pour les courbes, pour tout $\gamma \in \mathbb{F}_v^\times$, la $\mathbb{F}_v$-courbe C_γ contient un $\mathbb{F}_v$-point. En associant au point de coordonnées (x, z_1, z_2) le point de coordonnées $(x, z = z_1.z_2)$, on définit un morphisme de C_γ dans la courbe lisse d'équation $z^p = Q(x)R(x) \neq 0$ sur $\mathbb{F}_v$. Par le lemme de Hensel, l'image d'un $\mathbb{F}_v$-point de C_γ dans cette courbe lisse est un $\mathbb{F}_v$-point qui se relève en un O_v-point de la courbe C. Sur un tel O_v-point, l'algèbre $(u, Q(x))_\zeta$ a pour valeur $\gamma^{v(u)} \in \mathbb{F}_v^\times/\mathbb{F}_v^{\times p} \simeq \mathbb{Z}/p$. Comme $\gamma \in \mathbb{F}_v^\times$ est arbitraire, ceci établit le lemme. □

L'énoncé suivant est la généralisation du théorème 1.3 de [Poo09a] (cas $p = 2$). C'est le théorème 5.2 de [VAV12].

PROPOSITION 4.2. *L'ensemble des $u \in k^\times$ tels que que l'on ait à la fois $\mathbb{X}_u(\mathbf{A}_k) \neq \emptyset$ et $\mathbb{X}_u(\mathbf{A}_k)^{\mathrm{Br}} = \emptyset$ forme un nombre fini de classes dans $k^\times/k^{\times p}$.*

Démonstration. Il est clair que chacune des deux propriétés considérées ne dépend que de la classe de u dans $k^\times/k^{\times p}$. Soient C et S comme dans le lemme 4.1. On suppose de plus que S contient les places finies avec $v(d) \neq 0$, c'est-à-dire v_a et v_b. Pour tout $u \in k^\times$, la courbe C est contenue dans $\mathbb{X}_u$. Soit u tel que $\mathbb{X}_u(\mathbf{A}_k) \neq \emptyset$. S'il existe une place $v \notin S$ telle que $v(u) = v(du) \in \mathbb{Z}$ ne soit pas divisible par p, alors, d'après le lemme 4.1, l'algèbre $(du, Q(x))_\zeta$

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

parcourt sur $C(k_v) \subset \mathbb{X}_u(k_v)$ toutes les valeurs dans $\mathbb{Z}/p \subset \mathrm{Br}\, k_v$. D'après la proposition 2.2, la classe de $(du, Q(x))_\zeta$ appartient à $\mathrm{Br}\, \mathbb{X}_u$ et engendre $\mathrm{Br}\, \mathbb{X}_u/\mathrm{Br}\, k$. Il ne saurait donc y avoir obstruction de Brauer–Manin à l'existence d'un k-point, et encore moins d'un zéro-cycle de degré 1 sur $\mathbb{X}_u$. On voit donc que les $u \in k^\times$ tels que $\mathbb{X}_u(\mathbf{A}_k) \neq \emptyset$ et qu'on ait obstruction de Brauer–Manin à l'existence d'un zéro-cycle de degré 1 ont leur image dans le noyau de l'application

$$\mathrm{div} : k^\times/k^{\times p} \to \bigoplus_{v \notin S} \mathbb{Z}/p$$

et ce noyau est fini (finitude du nombre de classes et théorème des unités de Dirichlet). □

Nous pouvons maintenant donner la démonstration du théorème principal.

Théorème 4.3. *Soit k un corps de nombres. Soit $r > 0$ un entier. Le complément de $k^{\times r}$ dans $k^\times$ est un ensemble diophantien : il existe une k-variété Z et un k-morphisme $f : Z \to \mathbf{A}^1_k$ tel que $f(Z(k))$ soit le complémentaire des puissances r-ièmes dans k.*

Démonstration. Pour établir le résultat sur tout corps de nombres k, il suffit de l'établir lorsque r est un nombre premier p, et que de plus k contient une racine primitive p-ième de l'unité, soit ζ. Complétons ici la démonstration donnée dans [Poo09a, corollaire 1.2] et [VAV12, lemme 5.3 et démonstration du corollaire 1.2, p. 133]. Pour $r > 1$ entier, notons $A_r(k) : k^\times \backslash k^{\times r}$. Pour r, s entiers premiers entre eux, on a $A_{rs}(k) = A_r(k) \cup A_s(k)$. On peut donc se limiter au cas où $r = p^n$ est une puissance d'un nombre premier p. Si k ne contient pas une racine primitive p-ième ζ de l'unité, soit $K = k(\zeta)$. L'extension K/k est de degré premier à p. Ainsi $A_{p^n}(k) = k^\times \cap A_{p^n}(K) \subset K$. Si donc $A_{p^n}(K) \subset K$ est diophantien, alors $A_{p^n}(k) \subset k$ est diophantien. On est donc réduit au cas où $r = p^n$ est une puissance d'un nombre premier p et où k contient une racine primitive p-ième ζ de l'unité. On observe alors que l'on a la formule

$$A_{p^{n+1}} = A_p \cup \left[\bigcap_{i=1}^{p} (\zeta^i A_{p^n})\right]^p,$$

pour $n \geqslant 1$, ce qui par récurrence sur n ramène au cas $r = p$, avec k contenant une racine primitive p-ième de l'unité, cas que nous considérons désormais.

Notons $H_v = k^\times \cap k_v^{\times p}$ et N_v le complémentaire de H_v dans $k^\times$. Ce sont des ensembles diophantiens (cf. [Poo09a, théorème 1.5]) stables par multiplication par $k^{\times p}$.

Soit D_1 l'ensemble des $u \in k^\times$ tels que $\mathrm{Sym}^{2p+1}\mathbb{U}_u(k) \neq \emptyset$. C'est un ensemble stable par multiplication par $k^{\times p}$. C'est un ensemble diophantien, car c'est l'image des points k-rationnels de la k-variété $\mathrm{Sym}^{2p+1}_A \mathbb{U}$ par la projection naturelle $\mathrm{Sym}^{2p+1}_A \mathbb{U} \to \mathrm{Spec}\, A = \mathbb{G}_{m,k} \subset \mathbf{A}^1_k$. On a noté ici $\mathrm{Sym}^{2p+1}_A \mathbb{U}$ le quotient du produit fibré de N exemplaires de $\mathbb{U}$ au-dessus de Spec A par l'action de $\mathfrak{S}_N$.

Soit D_2 la réunion de D_1, des N_v pour $v \in S$, avec S comme au lemme 4.1 et des N_v pour v place non archimédienne avec $v(d) \neq 0$. C'est un ensemble diophantien dans $k^\times \subset k$, stable par multiplication par $k^{\times p}$.

Considérons le complément E de D_2 dans $k^\times$. C'est un ensemble stable par multiplication par $k^{\times p}$. Pour tout $u \in E$, on a $\mathbb{X}_u(\mathbf{A}_k) \neq \emptyset$. D'après le corollaire 3.2, l'ensemble E est contenu dans l'ensemble C des $u \in k^\times$ tels que de plus $\mathbb{X}_u(\mathbf{A}_k)^{\mathrm{Br}} = \emptyset$. D'après la proposition 4.2, l'ensemble C est union d'un nombre *fini* d'orbites de $k^{\times p}$ dans $k^\times$. Il en est donc de même de E. D'après la proposition 3.4, l'orbite de 1, soit $k^{\times p}$, n'est pas dans D_2, et elle est dans E.

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

Le complément D_3 de $k^{\times p}$ dans E est une union finie d'orbites de $k^{\times p}$ dans $k^\times$, chacune clairement un ensemble diophantien, donc D_3 est un ensemble diophantien. La réunion de D_2 et de D_3 est un ensemble diophantien D_4 dont le complément dans $k^\times$ est précisément $k^{\times p}$. Ainsi le complément de $k^{\times p}$ dans $k^\times$ est l'ensemble diophantien D_4, ce qui établit le théorème 4.3. □

Remarque 4.4. Dans la démonstration, on peut remplacer l'ensemble diophantien D_1 par l'ensemble diophantien D_1' formé des $u \in k^\times$ tels que $\mathrm{Sym}^{2p+1}\mathbb{X}_u(k) \neq \emptyset$. L'ensemble D_1' est stable par multiplication par $k^{\times p}$. Il contient D_1. On définit D_2' comme la réunion de D_1' et des N_v pour $v \in S$, puis $E' \subset E \subset C$ comme le complément de D_2' dans $k^\times$.

5. Une variante de la démonstration

Dans la démonstration du théorème 4.3, un ingrédient clé est le corollaire 3.2 du théorème 3.1.

En combinant un résultat non publié de Salberger (1985), décrit dans l'appendice ci-après, on peut utiliser directement les théorèmes principaux de [CTSD94] ou [CTSkSD98] sur les zéro-cycles pour donner une variante de la démonstration du théorème 4.3, variante qui évite le corollaire 3.2 du théorème 3.1, et donc aussi ce dernier théorème.

Le corollaire 3.2 du théorème 3.1 établit le résultat suivant :

Soit $u \in k^\times$. Si l'on a $\mathbb{X}_u(\mathbf{A}_k)^{\mathrm{Br}} \neq \emptyset$, alors $\mathrm{Sym}^{2p+1}\mathbb{X}_u(k) \neq \emptyset$.

Voici comment établir directement un substitut de ce résultat. D'après [CTSD94, théorème 5.1] ou encore [CTSkSD98, théorème 4.1], l'hypothèse $\mathbb{X}_u(\mathbf{A}_k)^{\mathrm{Br}} \neq \emptyset$ implique l'existence d'un zéro-cycle de degré 1 sur la k-variété $\mathbb{X}_u$. Le théorème A.2 ci-dessous, avec $s = 2p$, donne alors l'existence d'un zéro-cycle effectif de degré $(p-1)^2$ sur $\mathbb{X}_u$. Ainsi $\mathbb{X}_u(\mathbf{A}_k)^{\mathrm{Br}} \neq \emptyset$ implique que $u \in k^\times$ est dans l'image des points k-rationnels de $\mathrm{Sym}_A^{p^2-2p+1}\mathbb{X}$ via la projection $\mathrm{Sym}_A^{p^2-2p+1}\mathbb{X} \to \mathbb{G}_m$. On procède alors exactement comme dans la démonstration du théorème 4.3, en y remplaçant la projection $\mathrm{Sym}_A^{p+1}\mathbb{U} \to \mathbb{G}_m$ par $\mathrm{Sym}_A^{p^2-2p+1}\mathbb{X} \to \mathbb{G}_m$.

Appendice A. Résultats d'effectivité pour les zéro-cycles sur les familles de variétés de Severi–Brauer

Soit p un nombre premier, k un corps contenant une racine primitive p-ième de 1 et $P(x) \in k[x]$ un polynôme séparable de degré $2p$. Soit K/k une extension cyclique de corps, de groupe $G = \langle\sigma\rangle = \mathbb{Z}/p$.

Soit R_1 la $k[x]$-algèbre

$$R_1 = \bigoplus_{i=0}^{p-1} K[x]\xi^i,$$

avec x central et les relations $\xi^p = P(x)$ et pour $\lambda \in K$, $\xi.\lambda = \sigma(\lambda).\xi$. Alors R_1 est un ordre maximal, et donc en particulier héréditaire, dans l'algèbre simple centrale $(K/k, P(x))$ sur sur le corps $k(x)$.

Notons $P'(y) = y^{2p}P(1/y)$. Soit R_2 la $k[y]$-algèbre

$$R_1 = \bigoplus_{i=0}^{p-1} K[y]\eta^i,$$

avec y central et les relations $\eta^p = P'(y)$ et, pour $\lambda \in K$, $\eta.\lambda = \sigma(\lambda).\eta$. Alors R_2 est un ordre héréditaire sur $k[y]$.

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

Les identifications $y = 1/x$ et $y^2\xi = \eta$ permettent, sur $k[x, x^{-1}]$ et $k[y, y^{-1}]$, de recoller les deux ordres héréditaires en un faisceau $\tilde{R}$ de tels ordres sur la droite projective $\mathbf{P}^1_k$.

D'après Artin [Art82], le foncteur F sur la catégorie des $\mathbf{P}^1_k$-schémas dont les points $F(S)$ sur un $\mathbf{P}^1_k$-schéma affine S sont les idéaux à gauche du faisceau d'algèbres $\tilde{R}_S$ qui sont localement libres de rang p comme faisceaux de O_S-modules, et qui sont localement facteurs directs comme O_S-modules de $\tilde{R}_S$, est représentable par un $\mathbf{P}^1_k$-schéma projectif X'.

Au-dessus de l'ouvert de $\mathbf{P}^1_k$ où l'algèbre $\tilde{R}$ est d'Azumaya, ce schéma X' se restreint en un schéma de Severi–Brauer relatif. Toujours d'après Artin [Art82, théorème (1.4)], la fibre générique du $\mathbf{P}^1_k$-schéma X' est la variété de Severi–Brauer sur le corps $k(\mathbf{P}^1) = k(x)$ associée à la $k(x)$-algèbre simple centrale $(K/k, P(x))$.

Toujours d'après Artin, la composante connexe du schéma X' contenant la fibre générique est un k-schéma régulier $X = X(K/k, P)$, donc lisse sur k si $\mathrm{car}(k) = 0$. Les fibres de $\pi : X \to \mathbf{P}^1_k$ sont géométriquement connexes.

Artin ([Art82], voir aussi [Fro97]), donne une description précise des fibres non lisses du morphisme projectif $X \to \mathbf{P}^1_k$, description dont nous n'aurons pas besoin ici.

Le théorème suivant est annoncé et partiellement démontré par Salberger dans sa thèse [Sal85].

Théorème A.1 [Sal85, corollaire 5.9]. *Soit k un corps de caractéristique nulle. Soit $K = k(\mathbf{P}^1)$. Soit A une algèbre à division sur K d'indice premier p. Soit $\tilde{R}$ un faisceau d'ordres maximaux de A sur $\mathbf{P}^1_k$. Soient $X = X(K/k, P)$ et $\pi : X \to \mathbf{P}^1_k$ comme ci-dessus. Soit s la somme des degrés sur k des points fermés de $\mathbf{P}^1_k$ au voisinage desquels la $O_{\mathbf{P}^1_k}$-algèbre $\tilde{R}$ n'est pas une algèbre d'Azumaya.*

Tout zéro-cycle sur X de degré au moins égal à

$$N_0 = (1/2)(p-1)(s - 2(p+1)/p)$$

est rationnellement équivalent sur X à un zéro-cycle effectif.

Ce théorème généralise un résultat sur les surfaces fibrées en coniques au-dessus de la droite projective [CTCo79]. Salberger donne un énoncé plus général, au-dessus d'une courbe de genre quelconque. Sa démonstration utilise une version de l'inégalité de Riemann pour les idéaux des ordres maximaux sur une courbe due à Witt [Witt34], et reprise en particulier dans [VBVG85].

Corollaire A.2. *Avec les notations et hypothèses ci-dessus, soit $N = N(p, s) \geqslant 1$ le plus petit entier congru à 1 modulo p et au moins égal à $(1/2)(p-1)(s - 2(p+1)/p)$. Les conditions suivantes sont équivalentes :*

(a) *X possède un zéro-cycle de degré 1.*

(b) *X possède un zéro-cycle effectif de degré N.*

(c) *Le produit symétrique $\mathrm{Sym}^N X$ possède un k-point.*

Lemme A.3. *Soit k un corps de caractéristique zéro. Soient X et Y deux k-variétés projectives, lisses, géométriquement intègres, k-birationnellement équivalentes. Si pour un entier $N > 0$ tout zéro-cycle de degré N sur X est rationnellement équivalent sur X à un zéro-cycle effectif sur X, alors le même énoncé vaut pour tout zéro-cycle de degré N sur Y.*

Démonstration. D'après Hironaka, il existe une k-variété projective, lisse, géométriquement intègre Z et des k-morphismes birationnels $f : Z \to X$ et $g : Z \to Y$ tels que de plus f soit obtenu par éclatements successifs de sous k-variétés fermées lisses. Soit $U \subset Y$ un ouvert non vide tel que f induise un isomorphisme entre $V = f^{-1}(U)$ et U. Soit z un zéro-cycle de degré N sur Y.

https://doi.org/10.1112/S0010437X15007368 Published online by Cambridge University Press

Un lemme de déplacement facile [CT05, p. 599] assure que z est rationnellement équivalent, sur Y, à un zéro-cycle z_1, de degré N, dont le support est dans U. Soit z_2 le zéro-cycle de $V \subset Z$, de degré N, tel que $g_*(z_2) = z_1$. Soit $z_3 = f_*(z_2)$ son image sur X par f_*. Ce zéro-cycle a degré N. Par hypothèse, il est rationnellement équivalent, sur X, à un zéro-cycle effectif z_4 de degré N. Comme f est obtenu par composition d'éclatements le long de sous-variétés lisses, et que la fibre d'un point par un tel éclatement est un espace projectif, il existe un zéro-cycle effectif z_5 sur Z tel que $f_*(z_5) = z_4$ sur X. Par ailleurs, l'application induite sur les groupes de Chow de zéro-cycles $f_* : CH_0(Z) \to CH_0(X)$ est un isomorphisme [CTCo79, proposition 6.3]. Ainsi, sur Z, le zéro-cycle z_2 est rationnellement équivalent au zéro-cycle effectif z_5. Donc $z_1 = g_*(z_2)$ est rationnellement équivalent, sur Y, au zéro-cycle effectif $g_*(z_5)$. Et donc z est rationnellement équivalent, sur Y, au zéro-cycle effectif $g_*(z_5)$. □

Ce lemme nous permet de donner une version plus générale de l'énoncé de Salberger.

THÉORÈME A.4. *Soit k un corps de caractéristique zéro. Soit $Y \to \mathbf{P}^1_k$ un k-morphisme de k-variétés projectives et lisses géométriquement intègres dont la fibre générique est $k(\mathbf{P}^1)$-birationnelle à une variété de Severi–Brauer d'indice premier p, d'algèbre associée $A/k(\mathbf{P}^1)$. Soit s la somme des degrés sur k des points fermés de $\mathbf{P}^1_k$ où l'algèbre A a un résidu non trivial. Soit $N = N(p,s) \geqslant 1$ un entier congru à 1 modulo p et au moins égal à*

$$(1/2)(p-1)(s-2(p+1)/p).$$

Les conditions suivantes sont équivalentes :

(a) *Y possède un zéro-cycle de degré 1.*

(b) *Y possède un zéro-cycle effectif de degré N.*

(c) *Le produit symétrique $\mathrm{Sym}^N Y$ possède un k-point.*

Démonstration. Soit $A/K = k(\mathbf{P}^1)$ l'algèbre simple centrale associée à la fibre générique de π. Si A n'est pas une algèbre à division, alors c'est une algèbre de matrices, et la k-variété Y est k-birationnelle à $\mathbf{P}^{p-1}_k \times_k \mathbf{P}^1_k$, donc à $\mathbf{P}^p_k$. Le groupe de Chow $CH_0(Y)$ des zéro-cycles modulo l'équivalence rationnelle sur Y est alors égal à $\mathbb{Z}$, engendré par la classe d'un point k-rationnel, et le théorème est clair.

Supposons que A est une algèbre à division. Soit $\pi : X \to \mathbf{P}^1_k$ un modèle donné par le théorème A.1. Les k-variétés X et Y sont k-birationnellement équivalentes. La considération d'une fibre lisse sur un k-point de $\mathbf{P}^1_k$ montre que X et Y possèdent soit un k-point soit un point fermé de degré p sur k. Ceci établit en particulier que (b) implique (a). Supposons (a). D'après ce qui précède, il existe un zéro-cycle de degré $N(p,s)$ sur Y. Le corollaire A.2 (appliqué au modèle d'Artin X) et le lemme A.3 donnent alors (b). Les énoncés (b) et (c) sont équivalents. □

REFERENCES

Art82 M. Artin, *Left ideals in maximal orders*, in *Brauer groups in ring theory and algebraic geometry*, Lecture Notes in Mathematics, vol. 917 (Springer, Berlin, 1982), 182–193.

CT05 J.-L. Colliot-Thélène, *Un théorème de finitude pour le groupe de Chow des zéro-cycles d'un groupe algébrique linéaire sur un corps p-adique*, Invent. math. **159** (2005), 589–606.

CTCo79 J.-L. Colliot-Thélène and D. Coray, *L'équivalence rationnelle sur les points fermés des surfaces rationnelles fibrées en coniques*, Compositio Math. **39** (1979), 301–322.

CTCoSa80 J.-L. Colliot-Thélène, D. Coray and J.-J. Sansuc, *Descente et principe de Hasse pour certaines variétés rationnelles*, J. reine angew. Math. **320** (1980), 150–191.

CTSaSD87 J.-L. Colliot-Thélène, J.-J. Sansuc and Sir Peter Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces, I, II*, J. reine angew. Math. **373** (1987), 37–107 ; **374** (1987) 72–168.

CTSD94 J.-L. Colliot-Thélène and Sir Peter Swinnerton-Dyer, *Hasse principle and weak approximation for pencils of Severi–Brauer and similar varieties*, J. reine angew. Math. **453** (1994), 49–112.

CTSkSD98 J.-L. Colliot-Thélène, A. N. Skorobogatov and Sir Peter Swinnerton-Dyer, *Rational points and zero-cycles on fibred varieties : Schinzel's hypothesis and Salberger's device*, J. reine angew. Math. **495** (1998), 1–28.

Fro97 E. Frossard, *Fibres dégénérées des schémas de Severi–Brauer d'ordres*, J. Algebra **198** (1997), 362–387.

GS06 P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101 (Cambridge University Press, Cambridge, 2006).

Har94 D. Harari, *Méthode des fibrations et obstruction de Manin*, Duke Math. J. **75** (1994), 221–260.

Kön13 J. Königsmann, *Defining* $\mathbb{Z}$ *in* $\mathbb{Q}$, Preprint (2013), arXiv:1011.3424v2 [math.NT].

Poo09a B. Poonen, *The set of nonsquares in a number field is Diophantine*, Math. Res. Lett. **16**(1) (2009), 165–170 ; version corrigée : http://www-math.mit.edu/∼poonen/papers/nonsquares.pdf.

Poo09b B. Poonen, *Existence of rational points on smooth projective varieties*, J. Eur. Math. Soc. **11** (2009), 529–543.

Sal85 P. Salberger, *Class groups of orders and Chow groups of their Brauer–Severi schemes*, in *K-theory of orders and their Brauer–Severi schemes,* Thèse, Chalmers University of Technology, Göteborg (1985).

Sal88 P. Salberger, *Zero-cycles on rational surfaces over number fields*, Invent. math. **91**(3) (1988), 505–524.

VBVG85 M. Van den Bergh and J. Van Geel, *Algebraic elements in division algebras over function fields of curves*, Israel J. Math. **52** (1985), 33–45.

VAV12 A. Várilly-Alvarado and B. Viray, *Higher dimensional analogues of Châtelet surfaces*, Bull. London Math. Soc. **44**(1) (2012), 125–135.

VAV15 A. Várilly-Alvarado and B. Viray, *Smooth compactifications of certain normic bundles*, European J. Math., to appear. http://math.rice.edu/∼av15/files/compactifications.pdf.

Witt34 E. Witt, *Riemann–Rochscher Satz und Z-Funktion im Hyperkomplexen*, Math. Ann. **110** (1934), 12–28.

Wittenb12 O. Wittenberg, *Zéro-cycles sur les fibrations au-dessus d'une courbe de genre quelconque*, Duke Math. J. **161** (2012), 2113–2166.

Jean-Louis Colliot-Thélène jlct@math.u-psud.fr
CNRS & Université Paris-Sud, Mathématiques, Bâtiment 425,
F-91405 Orsay Cedex, France

Jan Van Geel jvg@cage.ugent.be
Universiteit Gent, Vakgroep Wiskunde, Krijgslaan 281, S22,
B-9000 Gent, Belgium