ACTA ARITHMETICA
XLI (1982)

Sur le principe de Hasse et l'approximation faible, et sur une hypothèse de Schinzel

par

JEAN-LOUIS COLLIOT-THÉLÈNE et JEAN-JACQUES SANSUC (Paris)

1. Introduction. Soit k un corps de nombres. Nous nous intéressons, dans cet article, à la validité du principe de Hasse et de l'approximation faible pour les k-variétés algébriques définies par un système d'équations du type

$$0 \neq P_i(\lambda_1, \ldots, \lambda_n) = Q_i(x_{i,1}, \ldots, x_{i,n_i}), \quad i = 1, \ldots, r, \tag{1}$$

où les P_i sont des polynômes à coefficients dans k en les variables λ_j et les Q_i des formes quadratiques à coefficients dans k en des variables indépendantes $x_{i,h}$, chacune de rang $\geqslant 2$. On connaît bien des exemples de telles variétés qui vérifient le principe de Hasse. Il en est ainsi pour un système du type

$$0 \neq \lambda = Q_1,$$

$$0 \neq \lambda = Q_2$$

où Q_1 et Q_2 désignent deux formes quadratiques à coefficients dans k en des variables indépendantes, la première de rang 2, la seconde de rang $\geqslant 2$, et c'est précisément la considération d'un tel système qui a permis à Hasse ([6], pp. 16, 20, 87) d'établir qu'une forme quadratique de rang $\geqslant 4$ sur k représente non trivialement 0 dans k, dès qu'il en est ainsi dans chaque complété de k. On connaît cependant aussi, parmi les systèmes du type (1), pour $k = \boldsymbol{Q}$, des contre-exemples au principe de Hasse (Iskovskikh [7]):

$$0 \neq (3-\lambda^2)(\lambda^2-2) = x^2+y^2$$

et à l'approximation faible (Swinnerton-Dyer [12]):

$$0 \neq (4\lambda-7)(\lambda^2-2) = x^2+y^2.$$

Dans la première partie de cet article (paragraphes 2-4), nous montrons que les variétés du type (1) satisfont le principe de Hasse et l'approximation faible dans chacun des deux cas suivants:

(α) chaque forme Q_i est de rang $\geqslant 3$,

(β) les polynômes P_i sont tous égaux à un même polynôme en une seule variable λ de degré $\leqslant 1$, autrement dit, le système d'équations est du type

$$0 \neq a\lambda + b = Q_1 = \ldots = Q_r \tag{2}$$

avec a et b dans k et les formes quadratiques Q_i comme en (1).

Les démonstrations reprennent fidèlement les arguments utilisés par Hasse pour les formes quadratiques ([6], loc. cit.), et repris, pour $k = \boldsymbol{Q}$, dans [1] et [11]. En particulier, dans le cas (β), la démonstration du principe de Hasse utilise le théorème de la progression arithmétique généralisé. La seconde partie de cet article (paragraphes 5–6) consiste à traiter, pour $k = \boldsymbol{Q}$, un cas plus large que (β), en s'appuyant sur une extrapolation conjecturale du théorème de Dirichlet, dite hypothèse H de Schinzel, et formulée dans des cas particuliers par Dickson et Bouniakowsky (Schinzel et Sierpiński [10], voir aussi l'introduction du livre d'Halberstam et Richert [4]). Nous obtenons ainsi au paragraphe 5, sous l'hypothèse H, le principe de Hasse et l'approximation faible pour les variétés du type (1) dans le cas suivant:

(γ) $k = \boldsymbol{Q}$, $n = 1$ et P_i *irréductible* pour chaque forme Q_i de rang 2.

On observera que la condition d'irréductibilité n'est pas satisfaite dans les contre-exemples indiqués plus haut. Ceux-ci sont du type particulier

$$0 \neq x^2 - ay^2 = P(\lambda) \tag{3}$$

où $a \in \boldsymbol{Q}^*$ et où $P \in \boldsymbol{Q}[\lambda]$ est un polynôme non nécessairement irréductible. L'objet du paragraphe 6 est d'obtenir, dans le cadre de l'hypothèse H, des renseignements sur les points rationnels des surfaces du type (3), à partir des résultats du paragraphe précédent et malgré la disparition éventuelle du principe de Hasse et de l'approximation faible pour de telles surfaces.

Nous tenons à remercier D. Coray qui a attiré notre attention sur l'hypothèse H et M. Vallino qui a bien voulu traiter sur ordinateur quelques exemples de variétés du type (γ) et nous a ainsi donné des évidences numériques particulièrement frappantes vis-à-vis des conséquences de l'hypothèse H indiquées au paragraphe 5.

2. Préliminaires. Dans les paragraphes 2–4, on désigne par k un corps de nombres quelconque et par Ω l'ensemble de ses places. Pour $v \in \Omega$, on note k_v le complété de k en v et $|\ |_v$ une valeur absolue associée sur k_v, ce qui donne une norme sur l'espace vectoriel k_v^n par la formule $\|(x_i)\|_v = \sup_i(|x_i|_v)$. Si p est un idéal premier de l'anneau des entiers de k, on note $v_\mathfrak{p}$ la place associée et $k_\mathfrak{p}$ le complété correspondant. On désigne

par $\boldsymbol{A}_k^n = \boldsymbol{A}^n$ l'espace affine de dimension n sur k, en tant que k-variété algébrique, par $\boldsymbol{G}_{m,k} = \boldsymbol{G}_m$ l'ouvert de $\boldsymbol{A}_k^1$ complémentaire de 0 et par $\boldsymbol{G}_m^n$ son produit n-uple avec lui-même. Enfin, si X est une k-variété algébrique et K une extension de k, on note $X(K)$ l'ensemble des points K-rationnels de X.

Définition. Etant donnée une famille $\mathscr{C}$ de variétés algébriques, ou de systèmes d'équations, définies sur k, on dit que $\mathscr{C}$ satisfait le principe de Hasse (ou, par abus, que les variétés de $\mathscr{C}$ le satisfont) si, pour une variété X quelconque dans $\mathscr{C}$, les conditions $X(k_v) \neq \emptyset$, pour toutes les places v de k, impliquent $X(k) \neq \emptyset$. On dit que $\mathscr{C}$ satisfait l'approximation faible (ou, par abus, que les variétés de $\mathscr{C}$ la satisfont) si, pour toute variété X de $\mathscr{C}$ possédant un point k-rationnel, l'ensemble $X(k)$ est dense (via le plongement diagonal) dans l'espace topologique produit $\prod_{v\in\Omega} X(k_v)$, chaque ensemble $X(k_v)$ étant muni de la topologie déduite de celle de k_v.

Lemme 1. *Soit, pour chaque entier $i = 1, \ldots, r$, une forme quadratique Q_i à coefficients dans k, en n_i variables, de rang $\geqslant 2$. On pose $N = n_1 + \ldots + n_r$. Soient $\varphi\colon \boldsymbol{A}^N = \boldsymbol{A}^{n_1} \times \ldots \times \boldsymbol{A}^{n_r} \to \boldsymbol{A}^r$ le k-morphisme défini par $(Q_1, \ldots, Q_r)$, puis X une k-variété algébrique, $\varphi\colon X \to \boldsymbol{G}_m^r \hookrightarrow \boldsymbol{A}^r$ un k-morphisme et enfin Y la k-variété algébrique, produit fibré $X \times_{\boldsymbol{A}^r} \boldsymbol{A}^N$ de φ et ψ. On note p_X: $Y \to X$ la projection. On suppose $Y(k_v)$ non vide quelle que soit la place v et on note $E = p_X\big(Y(k)\big)$ et, pour chaque place v, $E_v = p_X\big(Y(k_v)\big)$. Alors, si l'image diagonale de E dans le produit topologique $\prod_{v\in\Omega} X(k_v)$ est dense dans le produit $\prod_{v\in\Omega} E_v$, l'approximation faible vaut pour la variété Y.*

Démonstration. On doit montrer que, pour toute partie finie S de Ω, l'ensemble $Y(k)$ est dense, via le plongement diagonal, dans l'espace topologique produit $\prod_{v\in S} Y(k_v)$. Soient S une telle partie finie, ε un nombre réel > 0 et, pour chaque v dans S, un point (R_v, M_v) de $X(k_v) \times k_v^N$ qui appartienne à $Y(k_v)$; on pose $\xi_v = \varphi(R_v) = \psi(M_v) \in k_v^{*r}$ et on considère enfin un voisinage ouvert U_v de R_v dans $X(k_v)$. L'hypothèse de densité de l'énoncé assure l'existence d'un point R de $X(k)$ qui appartienne à E et qui soit assez proche du point (R_v) dans l'espace topologique produit $\prod_{v\in S} X(k_v)$ pour qu'on ait simultanément, en posant $\xi = \varphi(R) \in k^{*r}$, les propriétés suivantes:

$$[\psi^{-1}(\xi)](k) \neq \emptyset$$

et, pour chaque $v \in S$,

$$R \in U_v, \qquad \xi = \eta_v^2 \xi_v = \psi(\eta_v M_v)$$

où η_v est un certain élément de k_v^{*r} vérifiant l'inégalité

$$\|\eta_v - 1\|_v < \frac{\varepsilon}{2}\|M_v\|_v^{-1}$$

(dans cette inégalité on désigne par 1 l'élément $(1, \ldots, 1)$ de k_v^{*r} et dans l'égalité précédente on fait agir le groupe $\boldsymbol{G}_m^r$ sur $\boldsymbol{A}^{n_1} \times \ldots \times \boldsymbol{A}^{n_r}$ via l'action diagonale naturelle du i-ème facteur $\boldsymbol{G}_m$ de $\boldsymbol{G}_m^r$ sur $\boldsymbol{A}^{n_i}$). Posons $\xi = (\xi_1, \ldots, \xi_r)$. Comme $[\varphi^{-1}(\xi)](k)$ est non vide, chaque quadrique affine d'équation

$$Q_i(x_{i,1}, \ldots, x_{i,n_i}) = \xi_i$$

a un point k-rationnel et, comme chaque Q_i est de rang $\geqslant 2$, chacune de ces variétés vérifie l'approximation faible. On en déduit l'existence d'un point M de k^N tel qu'on ait:

$$\psi(M) = \xi$$

et, pour chaque v dans S,

$$\|M - \eta_v M_v\|_v < \varepsilon/2\,.$$

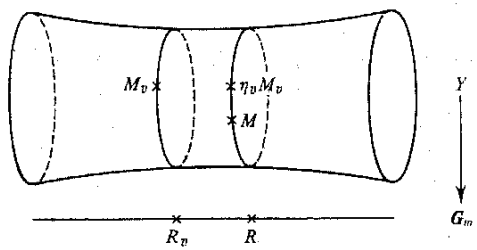
Les inégalités précédentes donnent, pour chaque v dans S, la majoration

$$\|M - M_v\|_v \leqslant \|M - \eta_v M_v\|_v + \|\eta_v - 1\|_v \|M_v\|_v < \varepsilon,$$

ce qui achève la démonstration: le point (R, M) appartient à $Y(k)$ et est aussi proche que voulu, pour chaque $v \in S$, du point (R_v, M_v). Ajoutons deux compléments: d'abord les équations de Y dans $X \times \boldsymbol{A}^N$,

$$0 \neq \varphi_i(R) = Q_i(M_i), \quad i = 1, \ldots, r, \tag{4}$$

qui font apparaître les variétés du type (1) comme un cas particulier, ensuite une illustration de la démonstration dans le cas $X = \boldsymbol{G}_m$, $\varphi = \mathrm{id}_{\boldsymbol{G}_m}$, $r = 1$, $n_1 = 2$, $k = \boldsymbol{Q}$ et $S = \{v_\infty\}$:



Remarque. Ce lemme nous permettra d'établir simultanément le principe de Hasse et l'approximation faible pour les variétés Y considérées par la suite par la simple vérification de l'hypothèse de densité de E: elle implique en effet $E \neq \emptyset$, donc $Y(k) \neq \emptyset$, puis l'approximation faible d'après le lemme.

3. Le cas où chaque forme Q_i est de rang $\geqslant 3$. On donne un énoncé dans un cas un peu plus général que le cas (α) de l'introduction:

Proposition 1. *Soit, pour chaque $i = 1, \ldots, r$, une forme quadratique Q_i à coefficients dans k, en n_i variables, de rang $\geqslant 3$. Soit X une k-variété algébrique ayant un point k-rationnel et vérifiant l'approximation faible. Soient ψ: $\boldsymbol{A}^N = \boldsymbol{A}^{n_1} \times \ldots \times \boldsymbol{A}^{n_r} \to \boldsymbol{A}^r$ le k-morphisme défini par $(Q_1, \ldots, Q_r)$, puis φ: $X \to \boldsymbol{G}_m^r \hookrightarrow \boldsymbol{A}^r$ un k-morphisme et enfin Y la k-variété algébrique $X \times_{\boldsymbol{A}^r} \boldsymbol{A}^N$, produit fibré de φ et ψ. Alors, si Y a des points dans tous les complétés k_v, elle en a un dans k et elle satisfait l'approximation faible.*

Démonstration. Comme chaque forme Q_i est de rang $\geqslant 3$, l'ensemble S_0 des places v, pour lesquelles il existe au moins une forme Q_i ne représentant pas, sur k_v, tout k_v, est un ensemble fini; on notera que, pour $v \notin S_0$, la variété Y a automatiquement un point dans k_v dès que X en a un. Avec les notations du lemme 1, on se propose de montrer que, pour toute partie finie S de Ω, l'ensemble E est dense dans le produit $\prod_{v \in S} E_v$. On peut supposer que S contient S_0. Soit, pour chaque $v \in S$, un point (R_v, M_v) de $X(k_v) \times k_v^N$ qui appartienne à $Y(k_v)$. L'approximation faible pour X, et la continuité des applications induites au niveau v-adique par les morphismes, assurent l'existence d'un point R de $X(k)$ aussi proche qu'on le désire du point (R_v) du produit topologique $\prod_{v \in S} X(k_v)$ et tel que, pour chaque $v \in S$,

$$\varphi(R) = \eta_v^2 \varphi(R_v)$$

pour un certain $\eta_v \in k_v^r$. On en déduit, pour $v \in S$,

$$\varphi(R) = \eta_v^2 \varphi(R_v) = \eta_v^2 \psi(M_v) = \psi(\eta_v M_v).$$

Si l'on pose $\varphi(R) = (\varphi_1(R), \ldots, \varphi_r(R))$, chaque composante $\varphi_i(R) \in k^*$ est donc représentée par la forme Q_i sur chaque corps k_v pour $v \in S$, donc pour tout $v \in \Omega$ d'après le choix de S. Le principe de Hasse pour la forme quadratique Q_i assure que $\varphi_i(R)$ est alors représenté par Q_i sur k. Le point R appartient donc à E et l'hypothèse de densité du lemme 1 est établie, ce qui achève la démonstration.

Corollaire 1. *Les variétés définies par un système d'équations du type* (1), *pour des formes quadratiques Q_i de rang $\geqslant 3$, vérifient le principe de Hasse et l'approximation faible.*

Il suffit en effet de considérer pour X l'ouvert de l'espace affine $\boldsymbol{A}^n$ défini par les conditions $P_i(\lambda_1, \ldots, \lambda_n) \neq 0$ pour $i = 1, \ldots, r$ et pour φ le morphisme $(P_1, \ldots, P_r)$.

Remarque. On ne peut pas, dans la proposition 1, remplacer $\boldsymbol{G}_m^r$ par $\boldsymbol{A}^r$. Par exemple, la $\boldsymbol{Q}$-variété Z définie dans $\boldsymbol{A}^5$ par l'équation

$$(\lambda^2 - 2)^2 = -x_1^2 - x_2^2 - x_3^2 - x_4^2$$

a des points dans $\boldsymbol{R}$ et dans tous les $\boldsymbol{Q}_p$, mais n'a pas de point dans $\boldsymbol{Q}$. Il faut néanmoins remarquer que ce contre-exemple n'est pas vraiment géométrique: si Z a bien des points non singuliers dans chacun des $\boldsymbol{Q}_p$, les seuls points de $Z(\boldsymbol{R})$ sont les deux points $(\pm\sqrt{2}, 0, 0, 0, 0)$ et ils sont *singuliers*; en particulier, l'ouvert Y de Z défini par $\lambda^2-2 \neq 0$ n'a pas de point réel! De fait, on sait que, sur un corps local K, réel ou p-adique, tout ouvert de Zariski d'une K-variété algébrique irréductible Z admet un point dans K si $Z(K)$ contient un point non singulier. D'où l'intérêt d'hypothèses de non-singularité si l'on désire remplacer $\boldsymbol{G}_m^r$ par $\boldsymbol{A}^r$ dans la proposition 1. On a par exemple l'énoncé suivant (où $Z_{\text{rég}}$ désigne l'ouvert de lissité de Z):

Corollaire 2. *Soient, pour $i = 1, \ldots, r$, des formes quadratiques Q_i à coefficients dans k, en des variables indépendantes, chacune de rang $\geqslant 3$, puis P_i des polynômes non nuls en d'autres variables $\lambda_1, \ldots, \lambda_n$. Soit Z la k-variété définie par les équations*

$$P_i(\lambda_1, \ldots, \lambda_n) = Q_i(x_{i,1}, \ldots, x_{i,n_i}), \quad i = 1, \ldots, r. \tag{5}$$

Si Z a, pour chaque place $v \in \Omega$, un point non singulier dans k_v, alors elle a des points, non singuliers, dans k et $Z_{\text{rég}}$ vérifie l'approximation faible.

En effet, Z est une variété irréductible et les remarques ci-dessus montrent que l'ouvert de Zariski Y défini par la condition $P_1 \ldots P_r \neq 0$ a un point dans chaque complété k_v, d'où $Y(k) \neq \emptyset$ par le corollaire précédent.

4. Le cas où tous les P_i sont égaux à un même polynôme linéaire en une variable. C'est le cas (β) de l'introduction. Lorsque $a = 0$, on retrouve le principe de Hasse et l'approximation faible pour les quadriques. Seul nous intéresse donc le cas $a \neq 0$:

Proposition 2. *Soient, pour $i = 1, \ldots, r$, des formes quadratiques Q_i à coefficients dans k, en des variables indépendantes, chacune de rang $\geqslant 2$. Soient λ une nouvelle variable, $a \in k^*$ et $b \in k$. Les équations du type*

$$0 \neq a\lambda + b = Q_1(x_{1,1}, \ldots, x_{1,n_1}) = \ldots = Q_r(x_{r,1}, \ldots, x_{r,n_r}) \tag{2}$$

satisfont le principe de Hasse et l'approximation faible.

Démonstration. Quitte à faire des changements de variables linéaires, on peut supposer les formes Q_i diagonales et se limiter à l'étude d'un système du type

$$0 \neq \lambda = Q_i(x_{i,1}, \ldots, x_{i,n_i}), \quad i = 1, \ldots, r. \tag{2}^*$$

Avec les notations du lemme 1, on se propose de montrer que, pour toute partie finie S de Ω, l'ensemble E est dense dans le produit $\prod_{v \in S} E_v$. Quitte à agrandir S, on peut supposer qu'elle contient toutes les places archimédiennes et les places finies pour lesquelles le nombre 2 ou l'un quelconque des coefficients non nuls de l'une des formes Q_i n'est pas une unité. On se donne en outre, pour chaque $v \in S$, une solution $(\lambda_v, M_v) \in k_v^* \times k_v^N$ du système $(2)^*$, avec $N = n_1 + \ldots + n_r$. L'approximation faible pour $\boldsymbol{G}_m$ assure l'existence d'un élément ϱ de k^* tel que, pour chaque $v \in S$, le quotient ϱ/λ_v soit un carré dans k_v^*. Le système d'équations indépendantes

$$Q_i(x_{i,1}, \ldots, x_{i,n_i}) = \varrho, \quad i = 1, \ldots, r$$

a donc, pour chaque $v \in S$, une solution dans k_v^N. Soit $\mathfrak{r}$ la partie étrangère à S dans la décomposition de l'idéal (ϱ) en produit de puissances d'idéaux premiers. Le théorème de Dirichlet généralisé ([5], §8, théorème 13, [8], chap. VIII, §4, p. 167), appliqué à la classe de l'idéal $\mathfrak{r}$ selon un module convenable de support S, assure, pour tout $\varepsilon > 0$, l'existence d'un élément a de k^* ayant les propriétés suivantes:

(i) $|a-1|_v < \varepsilon$ pour toute place finie $v \in S$,

(ii) a totalement positif,

(iii) il existe au plus, en dehors de S, une place w telle que $w(a\varrho) \neq 0$.

Quitte à choisir ε assez petit, la condition (i) assure que a est un carré dans k_v pour chaque $v \in S$. Posons $\zeta = a\varrho$. Pour $i = 1, \ldots, r$, chaque équation

$$Q_i(x_{i,1}, \ldots, x_{i,n_i}) = \zeta$$

a une solution dans k_v, pour chaque $v \in S$. Le choix initial de S montre qu'il en est encore ainsi pour $v \notin S$ si la forme quadratique Q_i est de rang $\geqslant 3$. Soit Q_i de rang 2. Pour $v \notin S$ et $v \neq w$, le choix initial de S et la condition (iii) assurent que ζ est représenté par Q_i sur k_v; on sait que c'est également vrai pour $v \in S$, donc aussi, par la formule du produit ([2], chap. VII, 9.6, ou exercice 2.9, p. 352), pour la seule place restante w. Ainsi, chaque équation $Q_i = \zeta$ a une solution dans k_v pour tout $v \in \Omega$, donc aussi dans k d'après le principe de Hasse classique pour les formes quadratiques. D'où $\zeta \in E$, ce qui établit le principe de Hasse pour le système $(2)^*$. Les choix ci-dessus assurent, pour tout $v \in S$, l'existence d'un élément β_v de k_v^* tel que:

$$\frac{\zeta}{\lambda_v} = a\frac{\varrho}{\lambda_v} = \beta_v^2.$$

Etant donné $\eta > 0$, l'approximation faible pour $\boldsymbol{G}_m$ implique l'existence d'un élément β de k^* tel que, pour tout $v \in S$,

$$\left|\frac{\beta_v}{\beta} - 1\right|_v < \eta.$$

Soit $\sigma = \zeta\beta^{-2}$. C'est encore un élément de E et, à condition de prendre η assez petit, chaque nombre

$$|\sigma - \lambda_v|_v = |\lambda_v|_v |(\beta_v/\beta)^2 - 1|_v$$

peut être, pour $v \in S$, rendu aussi petit qu'on le désire. Ceci prouve la densité de E dans $\prod_{v\in S} E_v$, d'où l'approximation faible pour le système (2)* par application du lemme 1.

Remarque. La démonstration ci-dessus suit en tout point celle donnée par Hasse ([6], pp. 16, 87) pour la représentation de 0 par une forme quadratique de rang 4 (alors que la démonstration de la proposition 1 reprend celle donnée par Hasse pour les formes de rang $\geqslant 5$, cf. [6], pp. 20, 91): voir aussi [1], chap. I, §7, et [11], chap. IV, §3 (où la démonstration est un peu compliquée par le recours aux symboles de Hilbert). Ces démonstrations établissent le principe de Hasse pour une équation du type $Q_1 = Q_2$ grâce à une réduction à l'étude du système $0 \neq Q_1 = Q_2$: celui-ci a en effet une solution dans un corps K dès que la forme $Q_1 - Q_2$ y a un zéro non trivial —car une forme quadratique qui représente 0 non trivialement dans K représente alors tout élément de K. Or, cette réduction ne vaut plus si l'on considère un système

$$Q_1(x_{1,1}, \ldots, x_{1,n_1}) = \ldots = Q_r(x_{r,1}, \ldots, x_{r,n_r}) \tag{6}$$

faisant intervenir $r \geqslant 3$ formes quadratiques Q_i, chacune de rang $\geqslant 2$. C'est ce que montrent les deux exemples suivants, pour $k = \boldsymbol{Q}$:

$$x^2 - 2y^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 = -y_1^2 - y_2^2 - y_3^2 - y_4^2$$

et (exemple dû à W. Ellison)

$$x^2 + 23y^2 = u^2 - 3v^2 = -w^2 + 3t^2.$$

Le premier système définit une $\boldsymbol{Q}$-variété affine qui a des points non singuliers dans tous les $\boldsymbol{Q}_p$, mais dont les points réels sont tous singuliers et annulent tous les trois formes Q_i figurant dans le système; la seule solution dans $\boldsymbol{Q}$ est la solution triviale. Le second système définit une $\boldsymbol{Q}$-variété affine qui a des points non singuliers dans $\boldsymbol{R}$ et dans tous les $\boldsymbol{Q}_p$ pour $p \neq 2, 3$; elle a des points dans $\boldsymbol{Q}_2$ et $\boldsymbol{Q}_3$, mais ils sont tous singuliers et dans $\boldsymbol{Q}$ il n'y a que la solution triviale. Comme pour le corollaire 2 de la proposition 1, on obtient cependant l'énoncé suivant grâce à des hypothèses de non-singularité:

Corollaire. *Soient, pour $i = 1, \ldots, r$, des formes quadratiques Q_i à coefficients dans k, en des variables indépendantes, chacune de rang $\geqslant 2$. Soit Z la k-variété affine définie par les équations*

$$Q_1(x_{1,1}, \ldots, x_{1,n_1}) = \ldots = Q_r(x_{r,1}, \ldots, x_{r,n_r}). \tag{6}$$

Si, pour chaque place $v \in \Omega$, elle a un point non singulier dans k_v, alors elle a des points, non singuliers, dans k et $Z_{\text{rég}}$ vérifie l'approximation faible.

En effet, Z est une variété irréductible et l'ouvert de Zariski Y défini par $0 \neq Q_1 = \ldots = Q_r$ a un point dans chaque complété k_v, donc dans k d'après la proposition, l'étude de Y se ramenant à celle du système (2)*.

5. Une conséquence de l'hypothèse H de Schinzel. Rappelons l'énoncé de cette hypothèse [10], qui est loin d'être démontrée —même dans les cas les plus simples —, mais qui sert de cadre à de nombreuses recherches d'arithmétique (voir l'introduction de [4]):

Hypothèse H. Soient, pour $i = 1, \ldots, r$, des polynômes $R_i \in \boldsymbol{Z}[t]$, irréductibles et à coefficient dominant > 0, tels qu'il n'existe pas de nombre premier p divisant le produit $R_1(n) \ldots R_r(n)$ quel que soit l'entier n; alors il existe une infinité d'entiers naturels n tels que les entiers $R_1(n), \ldots, R_r(n)$ soient tous premiers.

Théorème. *Soient, pour chaque $i = 1, \ldots, r$, un élément a_i de $\boldsymbol{Q}^*$ et un polynôme irréductible $P_i \in \boldsymbol{Q}[t]$. Soit Y la $\boldsymbol{Q}$-variété définie dans $\boldsymbol{A}^{2r+1}$ par le système d'équations*

$$0 \neq P_i(t) = x_i^2 - a_i y_i^2, \quad i = 1, \ldots, r. \tag{7}$$

On suppose l'hypothèse H vraie. Alors, si Y a un point dans chaque $\boldsymbol{Q}_p$ et dans $\boldsymbol{R}$, elle a un point dans $\boldsymbol{Q}$ et elle vérifie l'approximation faible.

La démonstration utilise les deux lemmes suivants, indépendants de H:

Lemme 2. *Soit $P \in \boldsymbol{Z}[t]$ un polynôme non nul, de contenu 1. Si p est un nombre premier qui divise $P(n)$ pour tout entier naturel n, alors $p \leqslant d^0P$.*

Démonstration. Soit $\overline{P} \in \boldsymbol{F}_p[t]$ la réduction modulo p de P. On a $\overline{P} \neq 0$ car P est de contenu 1. L'hypothèse montre que $\overline{P}$ est divisible par le produit des $(t-n)$ pour $0 \leqslant n < p$, d'où $d^0P \geqslant d^0\overline{P} \geqslant p$.

Lemme 3. *Soit $P \in \boldsymbol{Q}[t]$ un polynôme irréductible de degré n tel que $P(0) \neq 0$. Soient $m \in \boldsymbol{Q}^*$ et Q_m le polynôme de degré $2n$, à coefficients rationnels, défini par*

$$Q_m(t) = t^{2n} \cdot P\left(\frac{m}{t^2}\right).$$

Si, pour une racine a de P, le nombre $\sqrt{m}$ n'appartient pas à $\boldsymbol{Q}(\sqrt{a})$, ce polynôme Q_m est irréductible dans $\boldsymbol{Q}[t]$.

Démonstration. Notons que, si d est le coefficient dominant de P, celui de Q_m est $P(0)$ et son terme constant est dm^n. Le lemme résulte aussitôt des deux assertions suivantes:

(i) si $\Phi \in K[t]$ est un polynôme, à coefficients dans un corps K, irréductible de degré n tel que $\Phi(0) \neq 0$, il en est de même du polynôme Q, de degré n, défini par $Q(t) = t^n\Phi(1/t)$;

(ii) si K est de caractéristique $\neq 2$, si Φ est comme en (i) et si $a \in K^*$, le polynôme Ψ défini par $\Psi(t) = \Phi(at^2)$ est irréductible si et seulement si, pour une racine α de Φ, on a $\sqrt{a/a} \notin K(\alpha)$.

L'assertion (i) est évidente. Prouvons (ii): dire que Ψ est irréductible, c'est dire que, pour une racine β de Ψ, l'extension $K(\beta)/K$ est de degré $2n$, ou encore que $K(\beta)/K(\alpha)$ est quadratique, et on peut justement prendre $\beta = \sqrt{a/a}$. Le lemme s'en déduit ainsi: posons $R(t) = P(mt^2)$; d'après (ii), le polynôme R est irréductible puisque $\sqrt{m} \notin \boldsymbol{Q}(\sqrt{a})$, donc Q est irréductible d'après (i) appliquée à $\Phi = R$.

Démonstration du théorème. Indiquons d'abord le principe de la démonstration. Nous allons démontrer simultanément le principe de Hasse et l'approximation faible pour Y en établissant l'hypothèse de densité du lemme 1 pour les données suivantes: X est l'ouvert de $\boldsymbol{A}^1$ défini par $P_1 \dots P_r \neq 0$, l'application φ est celle définie par $(P_1, \dots, P_r)$ et $Q_i(x_i, y_i) = x_i^2 - a_i y_i^2$. Nous notons ∞ la place réelle de $\boldsymbol{Q}$ et $|\ |_\infty$ la valeur absolue usuelle sur $\boldsymbol{R}$. Pour p premier, la notation v_p sera souvent remplacée, en indice, par la notation p et nous posons $|x|_p = (1/p)^{v_p(x)}$ pour $x \in \boldsymbol{Q}_p$; étant donné un ensemble de nombres premiers, la même notation désignera souvent la partie de Ω associée. Avec les notations du lemme 1, nous devons établir que, pour tout ensemble fini S de nombres premiers, l'ensemble E est dense dans le produit $E_\infty \times \prod_{p \in S} E_p$. Soient donc un tel ensemble fini et, pour chaque $v \in S \cup \{\infty\}$, un point (τ_v, M_v) de $\boldsymbol{Q}_v \times \boldsymbol{Q}_v^{2r}$ qui appartienne à $Y(\boldsymbol{Q}_v)$. Soit ε un nombre réel > 0. On doit trouver $\tau \in \boldsymbol{Q}$ tel que, pour tout i, le nombre $P_i(\tau)$ soit non nul et représenté par la forme Q_i sur $\boldsymbol{Q}$ et tel qu'en outre, pour chaque $v \in S \cup \{\infty\}$, on ait $|\tau - \tau_v|_v < \varepsilon$: un tel τ appartient à E et approche à moins de ε l'élément (τ_v) du produit, pour $v \in S \cup \{\infty\}$, des E_v.

1. Quitte à multiplier les variables x_i, y_i par des éléments convenables de $\boldsymbol{Q}^*$, on peut supposer tous les a_i entiers et tous les P_i à coefficients entiers. Quitte à éliminer certaines équations, on peut en outre supposer qu'aucun a_i n'est un carré et que chaque P_i a un degré $m_i \geqslant 1$: en effet, si a_i est un carré, Q_i représente tout élément de $\boldsymbol{Q}$ et, si $\tau \in \boldsymbol{Q}$ a les propriétés requises pour le système obtenu par suppression de la $i^{\text{ème}}$ équation, il vérifie, pour ε assez petit, $P_i(\tau) \neq 0$ et convient donc pour le système initial; si P_i est un polynôme constant, le principe de Hasse pour les coniques affines permet d'éliminer l'équation correspondante.

2. Posons $d_i = P_i(0)$, pour $i = 1, \dots, r$. Par hypothèse, $P_i(\tau_\infty) \neq 0$ pour chaque i. Quitte à diminuer ε, on peut supposer que, pour $x \in \boldsymbol{R}$, l'inégalité $|x - \tau_\infty|_\infty < \varepsilon$ implique $P_i(x)/P_i(\tau_\infty) > 0$ pour tout i. Considérons alors deux entiers a et b tels que $|a/b - \tau_\infty|_\infty < \varepsilon/2$, puis, pour chaque i, le polynôme $\tilde{P}_i$ défini par $\tilde{P}_i(t) = b^{2m_i} P_i(t + a/b)$ et le système obtenu en remplaçant chaque P_i par $\tilde{P}_i$. Si, pour ce nouveau système, le nombre $\tau \in \boldsymbol{Q}$ a les propriétés requises relativement à $\varepsilon/2$ et aux données locales $(\tilde{\tau}_v)$ avec $\tilde{\tau}_\infty = 0$ et $\tilde{\tau}_p = \tau_p - a/b$ pour $p \in S$, alors le nombre $\tau + a/b$ convient pour le système et les données initiales. On peut donc supposer, avec les notations initiales que nous reprenons désormais, $\tau_\infty = 0$, auquel cas $d_i \neq 0$ pour tout i.

3. Considérons alors l'ensemble fini T des nombres premiers p satisfaisant l'une des propriétés suivantes: $p \leqslant 2(m_1 + \dots + m_r)$, ou p divise l'un des d_i, ou p se ramifie dans l'une des extensions $\boldsymbol{Q}(\sqrt{a_i})/\boldsymbol{Q}$. Soient $\Sigma = S \cup T$ et

$$A = \prod_{p \in \Sigma} p.$$

On se donne en outre, pour chaque p de Σ n'appartenant pas à S, un point (τ_p, M_p) de $\boldsymbol{Q}_p \times \boldsymbol{Q}_p^{2r}$ qui appartienne à $Y(\boldsymbol{Q}_p)$. Nous allons traiter le problème relatif à Σ au lieu de S et aux données locales (τ_v) ainsi fixées. Quitte à diminuer ε, on peut supposer que, pour chaque $v \in \Sigma \cup \{\infty\}$, on a la propriété suivante:

(+) pour $x \in \boldsymbol{Q}_v$, l'inégalité $|x - \tau_v|_v < \varepsilon$ entraîne que chaque $P_i(x)$ est différent de 0 et est représenté par Q_i sur $\boldsymbol{Q}_v$.

4. Par approximation forte, il existe deux entiers u et s $(s > 0)$ tels que tout diviseur premier de s appartienne à Σ et que:

$$(^0) \qquad \left| \frac{u}{s} - \tau_p \right|_p < \varepsilon \quad \text{pour chaque } p \in \Sigma.$$

Considérons alors, pour chaque i, le polynôme R_i, à coefficients entiers, défini par $R_i(t) = s^{2m_i} \cdot P_i(t/s)$. Notons les inégalités $R_i(0) \neq 0$ et $R_i(u) \neq 0$: la première résulte de $d_i \neq 0$ (voir **2**), la seconde des propriétés $(^0)$ et (+) pour $p = 2$ par exemple. L'hypothèse sur s montre que, si p est un nombre premier qui divise l'un des nombres $R_i(0)$, alors $p \in \Sigma$. Par ailleurs, il existe, en raison des inégalités $(^0)$, un entier $N_1 > 0$ et un nombre réel $\eta > 0$ (par exemple $s\varepsilon$) tels que, pour $\lambda \in \boldsymbol{Q}$, les conditions

$$(*) \qquad \begin{gathered} |\lambda|_\infty < \eta, \\ v_p(\lambda - u) \geqslant N_1 \quad \text{pour tout } p \in \Sigma \end{gathered}$$

entraînent, pour le nombre $\tau = \lambda/s$, les inégalités $|\tau|_\infty < \varepsilon$ et $|\tau - \tau_p|_p < \varepsilon$ pour tout $p \in \Sigma$, et a fortiori $R_i(\lambda) \neq 0$ pour tout i (voir **2** ou appliquer (+) pour $x = \tau$ et $v = v_2$). Il nous suffit donc *désormais* de trouver $\lambda \in \boldsymbol{Q}$ vérifiant les conditions $(*)$ et tel que, pour chaque i, le nombre $R_i(\lambda)$ soit représenté par Q_i sur $\boldsymbol{Q}$: le nombre $\tau = \lambda/s$ aura en effet alors les

propriétés requises pour le système initial, vis-à-vis de ε et des données locales $(\tau_v)_{v\in\Sigma\cup\{\infty\}}$, avec $\tau_\infty = 0$. Observons en outre que, si $\lambda \in \boldsymbol{Q}$ vérifie les conditions (*), chaque nombre $R_i(\lambda)$ est représenté par Q_i sur $\boldsymbol{Q}_v$ pour tout $v \in \Sigma\cup\{\infty\}$, ceci en vertu de la propriété (+) pour $x = \lambda/s$ et ces v-là.

5. Choisissons un entier $N > \sup\left(N_1, \sup_i \sup_{p\in\Sigma} v_p(R_i(u))\right)$. Considérons, pour chaque i et pour m un entier non nul, le polynôme $G_i(m, y) \in \boldsymbol{Q}[y]$, défini par

$$G_i(m, y) = y^{2m_i} R_i\left(\frac{m}{y^2}\right),$$

puis, pour n entier tel que $u + nA^N \neq 0$, le polynôme $S_{i,n}$ défini par

$$S_{i,n}(t) = G_i(u + nA^N, 1 + tA^N).$$

D'après le lemme 3 et le fait que l'application $t \mapsto 1 + tA^N$ est une bijection linéaire, ces polynômes $S_{i,n}$ sont, pour n fixé, irréductibles dans $\boldsymbol{Q}[t]$ si le nombre $\sqrt{u+nA^N}$ n'appartient pas au corps engendré sur $\boldsymbol{Q}$ par les racines carrées des racines des polynômes R_i, qui sont comme les P_i des polynômes irréductibles dans $\boldsymbol{Q}[t]$ non multiples de t; comme le corps K engendré sur $\boldsymbol{Q}$ par les nombres $\sqrt{u+nA^N}$, pour n entier quelconque, est une extension infinie de $\boldsymbol{Q}$ (par le théorème de la progression arithmétique il y a une infinité de nombres premiers ramifiés dans K), il y a une infinité d'entiers n tels que les polynômes $S_{1,n}, \ldots, S_{r,n}$ soient irréductibles dans $\boldsymbol{Q}[t]$. Fixons un tel entier n_1 et posons

$$S_i(t) = S_{i,n_1}(t) = (1 + tA^N)^{2m_i} R_i\left(\frac{u + n_1 A^N}{(1 + tA^N)^2}\right),$$

puis

$$T_i(t) = \frac{1}{c_i} S_i(t$$

où c_i désigne le contenu de S_i, affecté du signe de d_i. Les polynômes S_i et T_i sont à coefficients entiers et S_i a les propriétés suivantes:

(a) il est congru, dans $\boldsymbol{Z}[t]$, à la constante $R_i(u)$ modulo $A^N\boldsymbol{Z}[t]$,

(b) son terme dominant est $R_i(0)A^{2Nm_i}t^{2m_i}$.

Etant donnés le choix de N et la définition de A, la propriété (a) implique, pour tout $p \in \Sigma$ et tout $m \in \boldsymbol{Z}$, les égalités

$$v_p(c_i) = v_p\left(R_i(u)\right) = v_p\left(S_i(m)\right)$$

et donc:

(c) $$v_p\left(T_i(m)\right) = 0.$$

Par ailleurs, la propriété (b) montre que le coefficient dominant de T_i est > 0. Elle montre aussi (voir **4**) que, si p est un nombre premier qui divise c_i, alors $p \in \Sigma$. Enfin, le choix de n_1 et la définition de T_i montrent que le polynôme T_i est irréductible dans $\boldsymbol{Z}[t]$. Tout ceci pour $i = 1, \ldots, r$.

6. Le lemme 2 s'applique au polynôme $T_1 \ldots T_r$, à coefficients entiers et de contenu 1. Par suite, si p est un nombre premier divisant, pour tout entier m, le produit $T_1(m) \ldots T_r(m)$, alors $p \leqslant 2(m_1 + \ldots + m_r)$. D'après la définition de Σ (voir **3**), un tel p appartient donc à Σ. Or nous venons de voir (**5** (c)) qu'un nombre premier p appartenant à Σ ne divise aucun des nombres $T_i(m)$ pour $m \in \boldsymbol{Z}$ et $i = 1, \ldots, r$. Il n'y a donc pas de nombre premier qui divise, pour tout entier m, le produit $T_1(m) \ldots T_r(m)$. Ainsi, *les polynômes* T_i, pour $i = 1, \ldots, r$, *satisfont les conditions de l'hypothèse* H. Supposant cette hypothèse juste, nous pouvons donc trouver un entier naturel m ayant les propriétés suivantes:

(d) pour tout i, l'entier $T_i(m)$ est un nombre premier p_i,

(e) $$\left|\frac{u + n_1 A^N}{(1 + mA^N)^2}\right|_\infty < \eta.$$

Pour obtenir (e), il suffit de prendre m assez grand.

7. Posons $\lambda_m = \dfrac{u + n_1 A^N}{(1 + mA^N)^2}$. Compte tenu de (e) et du choix de N, supérieur à N_1, les conditions (*) de **4** sont bien vérifiées pour $\lambda = \lambda_m$:

$$|\lambda_m|_\infty < \eta,$$

$$v_p(\lambda_m - u) \geqslant N_1 \quad \text{quel que soit } p \in \Sigma.$$

Nous aurons donc terminé la démonstration (voir **4**) si nous montrons que, pour chaque i, le nombre $R_i(\lambda_m)$ est représenté sur $\boldsymbol{Q}$ par Q_i. Fixons i. Nous savons déjà (voir **4**) qu'en raison des conditions (*) le nombre $R_i(\lambda_m)$ est représenté par Q_i sur chaque $\boldsymbol{Q}_v$ pour $v \in \Sigma\cup\{\infty\}$. Par ailleurs, on a les égalités (voir **5** et **6** (d)):

$$c_i p_i = S_i(m) = (1 + mA^N)^{2m_i} R_i(\lambda_m)$$

où p_i est premier et où les facteurs premiers de c_i appartiennent à Σ (voir **5**). Ainsi, pour p premier n'appartenant pas à $\Sigma\cup\{p_i\}$, la valuation p-adique de $R_i(\lambda_m)$ est paire et, comme, d'après le choix de Σ (voir **3**), un tel p n'est pas ramifié dans $\boldsymbol{Q}(\sqrt{a_i})$, le nombre $R_i(\lambda_m)$ est encore représenté par Q_i sur $\boldsymbol{Q}_p$. En résumé, $R_i(\lambda_m)$ est représenté par la forme $x_i^2 - a_i y_i^2$ sur chaque complété de $\boldsymbol{Q}$, sauf éventuellement $\boldsymbol{Q}_{p_i}$: la formule du produit assure alors que $R_i(\lambda_m)$ est également représenté par Q_i sur $\boldsymbol{Q}_{p_i}$; il l'est donc sur $\boldsymbol{Q}$ par le principe de Hasse classique. Ceci achève la démonstration du théorème.

Remarque. La démonstration ci-dessus doit son aspect tortueux, tant du point de vue du principe de Hasse que de l'approximation faible, aux difficultés produites par la place réelle: c'est elle qui impose le changement de variable quadratique fait en **5**, et le recours au lemme 3. Au moins pour établir le principe de Hasse, il y a plusieurs cas où l'on peut donner une démonstration plus simple qui éclaire la démonstration générale. Il suffit que le coefficient dominant de P_i soit > 0 pour chaque $a_i < 0$, pour qu'on puisse utiliser au lieu du changement de variable quadratique fait en **5**, un changement de variable bien plus avantageux, du type $t \mapsto u + A^N t$. Voici des exemples qui se ramènent à ce cas: tous les P_i sont de degré pair (on commence alors par un changement de variable $t \mapsto 1/(b-t)$, bien choisi du point de vue réel); tous les P_i égaux entre eux (quitte à changer t en $-t$ pour rendre le coefficient dominant > 0): la démonstration est alors une généralisation, pour $k = \boldsymbol{Q}$, de celle de la proposition 2 — où le cas particulier de l'hypothèse H utilisé n'est autre que le théorème de Dirichlet!

Corollaire. *Soient, pour chaque $i = 1, \ldots, r$, une $\boldsymbol{Q}$-forme quadratique Q_i en n_i variables, de rang $\geqslant 2$, et un polynôme $P_i \in \boldsymbol{Q}[t]$ supposé irréductible si Q_i est de rang 2. Soit Y la $\boldsymbol{Q}$-variété algébrique définie dans $\boldsymbol{A}^1 \times \boldsymbol{A}^{n_1} \times \ldots \times \boldsymbol{A}^{n_r}$ par le système d'équations*

$$0 \neq P_i(t) = Q_i(x_{i,1}, \ldots, x_{i,n_i}), \quad i = 1, \ldots, r. \tag{8}$$

On suppose l'hypothèse H *vraie. Alors, si Y a un point dans chaque $\boldsymbol{Q}_v$ et dans $\boldsymbol{R}$, elle a un point dans $\boldsymbol{Q}$ et elle vérifie l'approximation faible.*

Démonstration. L'énoncé ci-dessus généralise le théorème et constitue le cas (γ) annoncé dans l'introduction. On peut supposer les formes Q_i diagonales et, pour chaque i, le rang de Q_i égal à n_i. On peut supposer que le nombre s des formes Q_i de rang 2 est à la fois $\geqslant 1$ (sinon on applique le corollaire 1 de la proposition 1) et $< r$ (sinon on applique le théorème). On suppose Q_i de rang 2 pour $i = 1, \ldots, s$. Soit X la $\boldsymbol{Q}$-variété définie dans $\boldsymbol{A}^1 \times \boldsymbol{A}^{n_1} \times \ldots \times \boldsymbol{A}^{n_s}$ par le système d'équations

$$0 \neq P_i(t) = Q_i(x_{i,1}, \ldots, x_{i,n_i}), \quad i = 1, \ldots, s.$$

Soit U l'ouvert de Zariski, non vide, de X défini par $P_{s+1}(t) \ldots P_r(t) \neq 0$. On a une projection naturelle $Y \to U$, d'où $U(\boldsymbol{Q}_v) \neq \emptyset$ pour toute place v. Ayant supposé l'hypothèse H vraie, on peut appliquer le théorème à X: ainsi, $X(\boldsymbol{Q}) \neq \emptyset$ et X vérifie l'approximation faible. Par suite, $U(\boldsymbol{Q}) \neq \emptyset$ (un point de $X(\boldsymbol{Q})$ assez proche, dans $X(\boldsymbol{R})$, d'un point de $U(\boldsymbol{R})$ appartient à $U(\boldsymbol{Q})$!) et U vérifie l'approximation faible. Soient $N = n_{s+1} + \ldots + n_r$, puis φ: $U \to \boldsymbol{G}_m^{r-s} \hookrightarrow \boldsymbol{A}^{r-s}$ le morphisme défini par $(P_{s+1}, \ldots, P_r)$ et ψ: $\boldsymbol{A}^N \to \boldsymbol{A}^{r-s}$ celui défini par $(Q_{s+1}, \ldots, Q_r)$. La variété Y n'est autre que le produit fibré de φ et ψ. Comme les formes $Q_{s+1}, \ldots, Q_r$ sont de rang $\geqslant 3$, la proposition 1 s'applique à cette situation: ainsi, $Y(\boldsymbol{Q}) \neq \emptyset$ et Y vérifie l'approximation faible.

Remarque. On peut, à propos du théorème et de son corollaire, donner, comme dans les remarques des paragraphes 3 et 4, des contre-exemples au principe de Hasse si, dans les systèmes (7) et (8), on supprime les inégalités $0 \neq P_i(t)$. Les conclusions subsistent cependant pour les systèmes

$$P_i(t) = Q_i(x_{i,1}, \ldots, x_{i,n_i}), \quad i = 1, \ldots, r \tag{9}$$

qui possèdent des solutions non singulières dans tout complété de $\boldsymbol{Q}$, les hypothèses sur les P_i et Q_i étant celles du corollaire. Mais il est plus important de noter que l'hypothèse d'irréductibilité de P_i pour Q_i de rang 2 est essentielle, comme le montrent les contre-exemples rappelés dans l'introduction. Il est également essentiel de supposer les Q_i de rang $\geqslant 2$, comme le montre le contre-exemple au principe de Hasse dû à Reichardt et Lind:

$$t^4 - 17 = 2x^2.$$

6. Applications à l'étude, conjecturale, des points rationnels de certaines surfaces rationnelles. Plusieurs auteurs ont écrit qu'il n'y avait pas de limite à la liste des conséquences de l'hypothèse H, et il peut sembler vain d'allonger la liste de celles qui ont été publiées. Sans pouvoir dire s'il y a quelque espoir de démontrer, sans passer par H, que les variétés du théorème satisfont le principe de Hasse (rappelons néanmoins qu'on peut établir le principe de Hasse pour les quadriques sans recourir au théorème de Dirichlet, cf. [2], exercice 4.8, p. 359), il semble pour le moins instructif d'expliciter les conséquences du théorème précédent dans l'étude des points $\boldsymbol{Q}$-rationnels des $\boldsymbol{Q}$-surfaces définies dans $\boldsymbol{A}^3$ par

$$0 \neq y^2 - az^2 = P(\lambda) \tag{3}$$

où $a \in \boldsymbol{Q}^*$ n'est pas un carré et où $P \in \boldsymbol{Q}[\lambda]$ est un polynôme non constant qu'on peut supposer sans facteur carré, mais non nécessairement irréductible. Il s'agit là de surfaces rationnelles (une variété algébrique est dite K-rationnelle si elle est définie sur le corps K et K-birationnelle à l'espace affine, elle est dite rationnelle si elle est K-rationnelle sur une extension convenable K du corps de base), fibrées en coniques sur $\boldsymbol{A}^1$, qui ne vérifient pas nécessairement ni le principe de Hasse, ni l'approximation faible. Dans ce qui suit, nous ne traitons pas le cas où P est de degré pair et possède un facteur irréductible de degré impair.

(a) *Le cas où P est de degré impair.* Soit k un corps de caractéristique $\neq 2$. Soient $a \in k^*$ et $P \in k[\lambda]$ un polynôme séparable de degré impair $2m-1$. Soit Q le polynôme défini par $Q(\mu) = \mu^{2m} P(1/\mu)$. Les équations

$$y^2 - az^2 = P(\lambda)t^2$$

et

$$Y^2 - aZ^2 = Q(\mu)T^2$$

définissent respectivement, dans deux copies de $\boldsymbol{P}^2 \times \boldsymbol{A}^1$ deux variétés qu'on peut recoller le long des ouverts $\lambda \neq 0$ et $\mu \neq 0$ via le changement de coordonnées

$$(Y, Z, T; \mu) = (\lambda^{-m} y, \lambda^{-m} z, t; 1/\lambda).$$

On obtient ainsi une k-surface X propre et lisse, fibrée en coniques sur $\boldsymbol{P}^1$ et $k(\sqrt{a})$-rationnelle. Comme $Q(0) = 0$, cette surface X a un point dans k, à savoir le point singulier de la fibre à l'infini, de coordonnées $(Y, Z, T; \mu) = (0, 0, 1; 0)$. Le cas où a est un carré étant trivial, on peut supposer a non carré. Soient $K = k(\sqrt{a})$ et $P = P_1 \dots P_r$ une décomposition de P en facteurs irréductibles P_i qu'on peut supposer unitaires, quitte à faire un changement de variable $\lambda \mapsto c\lambda$. Nous noterons encore P_i, pour $i = 1, \dots, r$, la fonction rationnelle définie sur X par le polynôme P_i. On peut voir que son diviseur est la norme, relativement à K/k, d'un diviseur de $X \times_k K$.

Proposition 3. *Soient $a \in \boldsymbol{Q}^*$ et $P \in \boldsymbol{Q}[\lambda]$ un polynôme de degré impair. On suppose vraie l'hypothèse* H. *Alors, la $\boldsymbol{Q}$-variété V définie dans $\boldsymbol{A}^3$ par*

$$0 \neq y^2 - az^2 = P(\lambda) \tag{3}$$

a des points dans $\boldsymbol{Q}$ et $V(\boldsymbol{Q})$ est Zariski-dense dans V. De plus, étant donné un ensemble fini S de places de $\boldsymbol{Q}$ et M un point du produit $\prod_{v \in S} V(\boldsymbol{Q}_v)$, il existe un processus fini pour déterminer si ce point appartient à l'adhérence de $V(\boldsymbol{Q})$. C'est toujours le cas si S ne rencontre pas un certain ensemble fini S_0 de places.

Démonstration. On conserve les notations et conventions indiquées en préambule, pour $k = \boldsymbol{Q}$, et on pose $N = N_{K/\boldsymbol{Q}}$. On considère l'application

$$\varrho\colon V(\boldsymbol{Q}) \to (\boldsymbol{Q}^*/N K^*)^r$$
$$(y, z, \lambda) \mapsto \big(\text{classe de } P_i(\lambda)\big)_{i=1,\dots,r}$$

et son image E. Elle est contenue dans le noyau de l'homomorphisme produit $\varkappa\colon (\boldsymbol{Q}^*/NK^*)^r \to \boldsymbol{Q}^*/NK^*$. Nous allons voir qu'elle est finie. Comme chaque fonction P_i a pour diviseur, sur la variété propre et lisse X, la norme d'un diviseur de $X \times_{\boldsymbol{Q}} K$, on sait déterminer effectivement ([3], proposition 4.3), à partir de a et P, un ensemble fini S_0 de places de $\boldsymbol{Q}$ tel que, pour toute place $v \notin S_0$, l'image de l'application

$$\varrho_v\colon V(\boldsymbol{Q}_v) \to (\boldsymbol{Q}_v^*/NK_w^*)^r$$
$$(y, z, \lambda) \mapsto \big(\text{classe de } P_i(\lambda)\big)_{i=1,\dots,r}$$

(où w désigne un prolongement de v à K) soit réduite à l'élément $(1, \dots, 1)$. Soit G l'intersection des noyaux de $\varkappa$ et de l'homomorphisme naturel

$$(\boldsymbol{Q}^*/NK^*)^r \to \prod_{v \notin S_0} (\boldsymbol{Q}_v^*/NK_w^*)^r.$$

C'est un sous-groupe fini de $(\boldsymbol{Q}^*/NK^*)^r$ qui contient E et qu'on sait déterminer de façon effective à partir de a et P. Considérons, pour chaque $g \in G$, un représentant $(a_{g,i})_{i=1,\dots,r}$ de g dans $\boldsymbol{Q}^{*r}$, choisi tel que $a_{g,1} \dots a_{g,r} = 1$. On définit alors, dans l'espace affine de coordonnées $(\lambda, u_1, v_1, \dots, u_r, v_r)$, la $\boldsymbol{Q}$-variété W_g par le système

$$0 \neq P_i(\lambda) = a_{g,i}(u_i^2 - a v_i^2), \quad i = 1, \dots, r,$$

puis l'on considère le $\boldsymbol{Q}$-morphisme

$$\pi_g\colon W_g \to V$$

obtenu en identifiant entre elles les „parties réelles", puis les „parties imaginaires" de l'équation $y + z\sqrt{a} = (u_1 + v_1\sqrt{a}) \dots (u_r + v_r\sqrt{a})$. On trouve alors que, pour $W_g(\boldsymbol{Q}) \neq \emptyset$, l'image de l'application $\varrho \circ \pi_g\colon W_g(\boldsymbol{Q}) \to (\boldsymbol{Q}^*/NK^*)^r$ n'est autre que $\{g\}$ et on obtient ainsi une partition de $V(\boldsymbol{Q})$:

$$V(\boldsymbol{Q}) = \bigcup_{g \in G} \pi_g\big(W_g(\boldsymbol{Q})\big).$$

Observons que $W_g(\boldsymbol{Q}) \neq \emptyset$ équivaut à $g \in E$. Pour une meilleure approximation de E, on peut considérer la partie F de G formée des éléments g tels que la variété W_g ait un point dans chaque complété $\boldsymbol{Q}_v$ de $\boldsymbol{Q}$. Cette partie F contient évidemment E et peut se déterminer de façon effective. Si l'on admet l'hypothèse H, on a même l'égalité $E = F$ par application du théorème du paragraphe 5. Par ailleurs, les polynômes P_i ayant été pris unitaires, on vérifie aisément (pour chaque place v, considérer $\lambda_v \in \boldsymbol{Q}_v$ avec $|\lambda_v|_v \geqslant 0$) que F contient l'élément $e = (1, \dots, 1)$: ceci peut également s'expliquer par l'existence, déjà mentionnée, d'un point rationnel dans la fibre à l'infini de X. Ainsi, F est non vide. Si l'on admet l'hypothèse H, le théorème du paragraphe 5 montre donc que E est non vide et, plus précisément, que la variété W_e a des points rationnels et vérifie l'approximation faible: ainsi, $W_e(\boldsymbol{Q})$ est Zariski-dense dans W_e et, comme le morphisme π_e est dominant, $V(\boldsymbol{Q})$ qui contient $\pi_e\big(W_e(\boldsymbol{Q})\big)$ est Zariski-dense dans V. Ceci montre les deux premières assertions. Considérons ensuite un ensemble fini S de places de $\boldsymbol{Q}$ et le diagramme commutatif suivant, où les verticales sont les applications diagonales et où $\varrho_S = (\varrho_v)_{v \in S}$:

$$\begin{array}{ccc} V(\boldsymbol{Q}) & \xrightarrow{\varrho} & (\boldsymbol{Q}^*/NK^*)^r \\ \downarrow i & & \downarrow j \\ \prod_{v \in S} V(\boldsymbol{Q}_v) & \xrightarrow{\varrho_S} & \prod_{v \in S} (\boldsymbol{Q}_v^*/NK_w^*)^r. \end{array}$$

Si M est un point du produit $\prod_{v\in S} V(Q_v)$ qui appartient à l'adhérence de $i(V(Q))$, alors $\varrho_S(M)$ appartient à $j(F)$: ceci vaut sans l'hypothèse H, et c'est ainsi qu'on obtient des contre-exemples à l'approximation faible du type de [12]. Si l'hypothèse H est vraie, on a la réciproque grâce au théorème du paragraphe 5: si $\varrho_S(M) = j(g)$ pour $g \in F$, l'approximation faible pour W_g montre que M appartient à l'adhérence de $i(V(Q))$. Si S ne rencontre pas S_0, l'image de ϱ_S est réduite à l'élément $(1, \ldots, 1)$ et il en est de même de $j(F)$! Ceci achève la démonstration.

Remarque. Supposons de nouveau le corps k quelconque. Dans le cas où $P(\lambda) = (\lambda-e_1)(\lambda-e_2)(\lambda-e_3)$ et où e_1, e_2, e_3 sont trois éléments distincts de k, la surface V définie par (3) n'est autre que celle étudiée initialement par F. Châtelet, et la „descente" décrite ci-dessus est exactement celle faite par cet auteur, et reprise ultérieurement par Manin ([9], chap. VI, §5). La question générale de savoir si, pour k un corps de nombres, les variétés W_g satisfont le principe de Hasse a déjà été posée par Manin ([9], chap. VI, fin de 5.25) dans le cas d'une surface de Châtelet (une réponse positive permettrait alors de calculer effectivement la R-équivalence sur $V(k)$). Cette question de Manin a donc, pour $k = Q$, une réponse affirmative si l'hypothèse H est vraie. Si V est une surface de Châtelet sur un corps k infini (de caractéristique $\neq 2$) quelconque, $V(k)$ est Zariski-dense dans V: en effet, la variété W_e est alors k-rationnelle d'après Châtelet, et V est donc k-unirationnelle. C'est une question ouverte de savoir si une k-surface rationnelle, propre et lisse, possédant un point dans k, est k-unirationnelle. S'il en était ainsi, les deux premières assertions de la proposition 3 vaudraient encore sur un corps k quelconque, au moins en caractéristique 0. On aurait alors le résultat suivant: étant donnés une extension quadratique K/k et un polynôme $P \in k[\lambda]$ de degré impair, il existe une infinité d'éléments $c \in k$ tels que $P(c) \in N_{K/k}(K)$. Nous ne savons pas s'il en existe même un seul! Revenons au cas d'une surface de Châtelet V sur un corps de nombres k: comme W_e est k-rationnelle lisse (donc satisfait l'approximation faible), on obtient alors, sans hypothèse, le dernier résultat de la proposition 3, à savoir l'existence d'un ensemble fini S_0 de places de k en dehors duquel l'approximation faible vaut toujours pour V.

(b) *Le cas où les facteurs irréductibles de P sont de degré pair.* Nous serons brefs en raison des nombreuses analogies avec le cas précédent. Nous renvoyons le lecteur à ([3], §5) pour certains détails. Soient $a \in Q^*$ non carré et $K = Q(\sqrt{a})$. Soit $P = P_1 \ldots P_r$ le produit de r polynômes $P_i \in Q[\lambda]$, irréductibles, tous de degré pair, et deux à deux non proportionnels. On peut encore construire un modèle propre et lisse X de la Q-variété V définie dans A^3 par

$$0 \neq y^2 - az^2 = P(\lambda),$$

de telle sorte que chaque P_i définisse sur X une fonction dont le diviseur soit la norme d'un diviseur de $X \times_Q K$ (c'est là qu'intervient la parité des degrés des P_i). Il n'y a cependant pas cette fois-ci de point évident dans $X(Q)$; de fait, on écrit facilement des exemples de telles surfaces sans point réel!

Proposition 4. *Soient $a \in Q^*$ et $P \in Q[\lambda]$ un polynôme dont tous les facteurs irréductibles sont de degré pair. Soit V la Q-variété définie dans A^3 par*

$$0 \neq y^2 - az^2 = P(\lambda). \tag{3}$$

On suppose vraie l'hypothèse H. *Il existe alors un processus fini, et effectif pour déterminer si V a un point dans Q. Si c'est le cas, $V(Q)$ est Zariski-dense dans V. De plus, étant donnés un ensemble fini S de places de Q et un point M de $\prod_{v\in S} V(Q_v)$, il existe, pour $V(Q) \neq \emptyset$, un processus fini pour déterminer si M appartient à l'adhérence de $V(Q)$; c'est toujours le cas si S ne rencontre pas un certain ensemble fini S_0 de places.*

La démonstration est strictement analogue à la précédente. La seule différence à signaler est la suivante: l'ensemble fini F formé des $g \in G$ tels que la variété W_g ait un point dans chaque complété Q_v de Q peut être vide; ceci peut arriver même si $V(Q_v)$ est non vide pour toute place v de Q, et c'est d'ailleurs ainsi qu'on fabrique des contre-exemples au principe de Hasse du type de [7].

Un exemple. Soient d un entier $\geqslant 3$ et V la Q-variété définie dans A^3 par

$$0 \neq y^2 + z^2 = (d-x^2)(x^2-d+1)(x^2-d+2). \tag{10}$$

Soient A l'ensemble des points de $V(Q)$ vérifiant $0 < x^2 < d-2$ et B l'ensemble des points de $V(Q)$ vérifiant $d-1 < x^2 < d$. Dans cet exemple, on voit aisément qu'on a

$$A = \pi_\alpha(W_\alpha(Q)) \quad \text{et} \quad B = \pi_\beta(W_\beta(Q))$$

pour $\alpha = (1, -1, -1)$ et $\beta = (1, 1, 1)$. Les variétés W_α et W_β ont pour équations:

$$W_\alpha \begin{cases} 0 \neq u_1^2 + v_1^2 = d - x^2, \\ 0 \neq u_2^2 + v_2^2 = d - 1 - x^2, \\ 0 \neq u_3^2 + v_3^2 = d - 2 - x^2; \end{cases} \qquad W_\beta \begin{cases} 0 \neq u_1^2 + v_1^2 = d - x^2, \\ 0 \neq u_2^2 + v_2^2 = x^2 - d + 1, \\ 0 \neq u_3^2 + v_3^2 = x^2 - d + 2. \end{cases}$$

Elles ont des points dans chaque complété de Q, sauf éventuellement dans Q_2.

L'analyse ci-dessus du cas (b) s'applique ici, sauf dans le cas où l'un des nombres d, $d-1$ ou $d-2$ est un carré (on fait alors appel à l'analyse du cas (a) après un changement de variable convenable en x dans les équations de W_α et W_β). On obtient ainsi, sous l'hypothèse H, les équi-

valences

$$A \neq \emptyset \Leftrightarrow W_a(\boldsymbol{Q}_2) \neq \emptyset,$$
$$B \neq \emptyset \Leftrightarrow W_\beta(\boldsymbol{Q}_2) \neq \emptyset,$$

ce qui donne les résultats suivants:

$d \equiv 0 \bmod 4$				
$d = 4^m(8n+7)$	avec	$m \geqslant 1,\ n \geqslant 0,$	$A = \emptyset,$	$B = \emptyset,$
$d \neq 4^m(8n+7)$	avec	$m \geqslant 1,\ n \geqslant 0,$	$A = \emptyset,$	$B \neq \emptyset,$
$d \equiv 1 \bmod 4$			$A = \emptyset,$	$B \neq \emptyset,$
$d \equiv 2 \bmod 4$				
$d-2 = 4^m(8n+7)$	avec	$m \geqslant 1,\ n \geqslant 0,$	$A = \emptyset,$	$B \neq \emptyset,$
$d-2 \neq 4^m(8n+7)$	avec	$m \geqslant 1,\ n \geqslant 0,$	$A \neq \emptyset,$	$B \neq \emptyset,$
$d \equiv 3 \bmod 4$				
$d \equiv 7 \bmod 8$			$A = \emptyset,$	$B = \emptyset,$
$d \equiv 3 \bmod 8$			$A \neq \emptyset,$	$B = \emptyset.$

En résumé,

$$V(\boldsymbol{Q}) = \emptyset \quad \text{pour } d = 4^m(8n+7) \text{ avec } m,\ n \geqslant 0$$

(et V est alors toujours un contre-exemple au principe de Hasse, car on vérifie $V(\boldsymbol{Q}_2) \neq \emptyset$) et, inversement, si l'hypothèse H est vraie,

$$V(\boldsymbol{Q}) \neq \emptyset \quad \text{pour les autres valeurs de } d.$$

Les résultats soumis à l'hypothèse H, à savoir $W_a(\boldsymbol{Q}) \neq \emptyset$ ou $W_\beta(\boldsymbol{Q}) \neq \emptyset$ pour telle ou telle valeur de d, ont été effectivement vérifiés sur ordinateur par M. Vallino pour $d < 32768$.

Remarque. C'est uniquement la partie „principe de Hasse" du théorème du paragraphe 5 qui sert à établir la première assertion de la proposition 4. Dans l'article [3], D. Coray et les auteurs démontrent (sans hypothèse) que, pour k un corps de nombres, $a \in k^*$ et $P_1, P_2 \in k[\lambda]$ deux polynômes du second degré irréductibles, tout k-modèle propre et lisse de la k-variété définie dans $\boldsymbol{A}^5$ par le système

$$0 \neq P_i(\lambda) = u_i^2 - av_i^2, \quad i = 1, 2,$$

a un point dans k dès qu'il en a dans chaque complété de k ([3], théorème 3.2). Ce résultat est, pour $k = \boldsymbol{Q}$, un cas très particulier de ce que prédit le théorème du paragraphe 5. Il nous permet de décider, par un processus

fini, si un k-modèle propre et lisse d'une équation du type

$$0 \neq y^2 - az^2 = P_1(\lambda)P_2(\lambda)$$

avec a, P_1 et P_2 comme ci-dessus, possède un point dans k ([3], §5).

Bibliographie

[1] Z. I. Borevič, I. R. Šafarevič, *Théorie des nombres* (en russe), Nauka, Moscou 1964 (trad. franç.: Gauthier-Villars, Paris 1967).

[2] J. W. S. Cassels, A. Fröhlich (editors), *Algebraic Number Theory*, Academic Press, Londres 1967.

[3] J.-L. Colliot-Thélène, D. Coray, J.-J. Sansuc, *Descente et principe de Hasse pour certaines variétés rationnelles*, J. Reine Angew. Math. 320 (1980), pp. 150–191.

[4] H. Halberstam, H.-E. Richert, *Sieve Methods*, Academic Press, Londres 1974.

[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I, Jahresbericht d. DMV 35 (1926), pp. 1–55.

[6] — *Mathematische Abhandlungen*, Bd. 1, de Gruyter, Berlin 1975.

[7] V. A. Iskovskikh, *Un contre-exemple au principe de Hasse pour les couples de formes quadratiques en cinq variables* (en russe), Mat. Zametki 10 (1971), pp. 253–257 (trad. angl.: Math. Notes 10 (1971), pp. 575–577).

[8] S. Lang, *Algebraic Number Theory*, Addison Wesley, Reading 1970.

[9] Y. I. Manin, *Formes cubiques* (en russe), Nauka, Moscou 1972 (trad. angl.: North-Holland, Amsterdam 1974).

[10] A. Schinzel, W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), pp. 185–208; Errat. ibid. 5 (1959), p. 259.

[11] J.-P. Serre, *Cours d'arithmétique*, P. U. F., Paris 1970.

[12] H. P. F. Swinnerton-Dyer, *Two special cubic surfaces*, Mathematika 9 (1962), pp. 54–56.

Reçu le 13. 11. 1979 (1183)