LES GRANDS THÈMES DE FRANÇOIS CHÂTELET

Autor(en): **Colliot-Thélène, Jean-Louis**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **34 (1988)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-56605

L'Enseignement Mathématique, t. 34 (1988), p. 387-405

LES GRANDS THÈMES DE FRANÇOIS CHÂTELET [1])

par Jean-Louis COLLIOT-THÉLÈNE

Les travaux mathématiques de F. Châtelet ont porté principalement sur la géométrie diophantienne, et il a contribué de façon significative et très originale à l'arithmétique de trois classes de variétés algébriques: les variétés de Severi-Brauer, les courbes de genre 1 et les surfaces cubiques. Il s'est aussi intéressé aux points exceptionnels (points de torsion) sur les courbes elliptiques, ainsi qu'aux quadriques et hyperquadriques.

Pour rendre compte de ces travaux, j'utiliserai quelques notations usuelles en géométrie algébrique. Etant donnée X/k une variété algébrique définie sur un corps k (i.e. définie par un système d'équations à coefficients dans k) on note $X(k)$ l'ensemble des points k-rationnels de X (solutions à coefficients dans k). Si L est un surcorps de k, on note X_L la variété X considérée sur L et $X(L)$ les points L-rationnels de X. Etant donnée $\bar{k}$ une clôture séparable de k, on note $\bar{X} = X_{\bar{k}}$. On note $\mathbf{P}^n_k$ l'espace projectif de dimension n sur le corps k.

1. VARIÉTÉS DE SEVERI-BRAUER

1.1. AVANT CHÂTELET.

Les variétés de Severi-Brauer sont des généralisations en dimension supérieure des coniques. Voici quelques propriétés bien connues des coniques. Une conique $C \subset \mathbf{P}^2_k$ qui possède un point rationnel est k-isomorphe à $\mathbf{P}^1_k$ (Diophante; c'est la paramétrisation par les droites passant par un point). Si une conique possède un point rationnel dans une extension de degré impair de k, elle possède un point k-rationnel. Si k est un corps fini, toute conique possède un point rationnel. Si k est le corps $\mathbf{R}$ des réels,

[1]) François Châtelet, professeur à l'Université de Besançon depuis 1949, est décédé le 19 avril 1987 dans sa 75e année. Il faisait partie de la rédaction de *L'Enseignement Mathématique* depuis 1960. Le présent exposé a été fait à Besançon, le 28 septembre 1987, lors de la réunion à la mémoire de F. Châtelet.

toute conique est $\mathbf{R}$-isomorphe soit à $\mathbf{P}^1_{\mathbf{R}}$ soit à $x^2 + y^2 + z^2 = 0$. Si k est le corps $\mathbf{Q}$ des rationnels, les conditions de congruence (et la condition réelle) suffisent à assurer l'existence d'un point $\mathbf{Q}$-rationnel (Legendre). Plus généralement, si k est un corps de nombres, la condition $C(k_v) \neq \emptyset$ pour chaque complété k_v de k en une place v assure $C(k) \neq \emptyset$ (principe de Hasse).

Comme toute courbe (projective et lisse) définie sur k et de genre 0, c'est-à-dire isomorphe, sur $\bar{k}$, à $\mathbf{P}^1_{\bar{k}}$ est k-isomorphe à une conique (Max Noether 1884, Hilbert/Hurwitz 1884, Poincaré 1901), toute telle courbe C satisfait les propriétés ci-dessus. En outre, il existe une extension au plus quadratique K de k telle que $C(K)$ soit non vide. Notons enfin la propriété, qu'on peut attribuer à Hasse (1924): si deux courbes de genre zéro C et D définies sur un corps de nombres k sont isomorphes sur tous les complétés k_v de k, elles sont isomorphes sur k.

D'un point de vue géométrique, les courbes mentionnées ci-dessus admettent deux extensions naturelles en dimension plus grande que 1: les quadriques et les variétés de Severi-Brauer. Pour les quadriques, l'analogue de la plupart des propriétés ci-dessus, et tout spécialement le principe de Hasse, furent établis par Hasse dans ses mémoires sur les formes quadratiques (1923/1924).

Définition. Une variété X de dimension d définie sur le corps k est dite de Severi-Brauer si $\bar{X}$ est *isomorphe* à $\mathbf{P}^d_{\bar{k}}$ (isomorphe sans exceptions).

C'est dans la thèse de François Châtelet que furent développées systématiquement les propriétés de ces variétés. Néanmoins, comme le note B. Segre en 1949, cette notion apparaît pour la première fois chez Severi (1932) qui donne une démonstration géométrique du théorème: si $X(k)$ est non vide, alors X est k-isomorphe à $\mathbf{P}^d_k$. Par ailleurs, dans le cas $d = 1$, Witt (1934) et Hasse (1935) notent la correspondance entre coniques et algèbres de quaternions. Les algèbres de quaternions (Hamilton, Frobenius) sont un cas spécial des algèbres centrales simples (Dickson, Wedderburn, 1905), qui sont les k-algèbres A telles qu'il existe un isomorphisme de $\bar{k}$-algèbres $A \otimes_k \bar{k} \simeq M_n(\bar{k})$ ($M_n(\bar{k})$ est l'algèbre des matrices (n, n) sur le corps $\bar{k}$). Les propriétés des algèbres centrales simples (« systèmes hypercomplexes ») furent dégagées par Brauer, Hasse, E. Noether et Albert entre 1927 et 1934, et Deuring leur consacra son livre *Algebren* en 1935.

Rappelons ici les propriétés principales. Une k-algèbre simple centrale A est k-isomorphe à une k-algèbre $M_r(D)$ où D est un corps gauche de centre k, le degré $[D : k]$ étant un carré i^2. On appelle i l'index de A. Pour $k = \mathbf{R}$, les seuls corps gauches de dimension finie sur leur centre $\mathbf{R}$ sont $\mathbf{R}$

lui-même et **H** l'algèbre des quaternions de Hamilton (Frobenius). Si k est un corps fini, toute algèbre simple centrale sur k est de la forme $M_r(k)$ (Wedderburn). Enfin, si k est un corps de nombres, et si $A \otimes_k k_v \simeq M_n(k_v)$ pour toute place v de k, alors $A \simeq M_n(k)$ comme k-algèbre (Brauer/Hasse/Noether, Albert). Par ailleurs, Skolem et Noether identifièrent le groupe des automorphismes d'une k-algèbre simple centrale A au quotient A^*/k^* (le groupe des unités A^* agissant par conjugaison intérieure). De son côté, Brauer organisa les classes d'algèbres simples centrales sur k en un groupe, dit depuis groupe de Brauer de k, via le produit tensoriel des algèbres, les algèbres « déployées » $M_n(k)$ étant considérées comme triviales. Ceci l'amena à introduire les « systèmes de facteurs », qui sont l'un des ancêtres de la cohomologie des groupes.

1.2. La contribution de F. Châtelet [1943*a*] [1943*b*] [1944].

Dans sa thèse [1944], François Châtelet généralisa aux variétés de Severi-Brauer tous les résultats connus pour les coniques:

Théorème. *Soient X et Y deux variétés de Severi-Brauer de dimension d sur le corps k.*

1) *Si $X(k)$ est non vide, alors X est k-isomorphe à $\mathbf{P}^d_k$.*

2) *Il existe un corps K contenant k et de degré $[K:k]$ divisant $(d+1)$ tel que $X(K)$ soit non vide.*

3) *Si L est une extension finie de k, $X(L)$ non vide et $[L:k]$ premier à $(d+1)$, alors X possède un k-point rationnel.*

4) *Si k est fini, X est k-isomorphe à $\mathbf{P}^d_k$.*

5) *Si k est un corps de nombres, et $X_{k_v} \simeq Y_{k_v}$ pour toute place v de k, alors X est k-isomorphe à Y.*

En particulier, si $X(k_v)$ est non vide pour chaque place v de k, alors X possède un k-point rationnel.

Quelle est la méthode de Châtelet? Pour reprendre le langage de sa thèse, il considère une extension galoisienne finie K/k de groupe G et une variété de (Severi-)Brauer de dimension d « admettant K comme corps de représentation » (les groupes profinis n'avaient pas encore fait leur apparition). A une telle variété est attaché un « système de matrices associées » (« Algèbre de Brauer de degré $d+1$ »). Enfin à une telle algèbre est attaché un « système de scalaires associés ».

En termes d'aujourd'hui, Châtelet s'intéresse aux classes d'isomorphismes de k-variétés X qui deviennent isomorphes à $\mathbf{P}^d_K$ sur K. Un calcul depuis bien connu (chez Châtelet, la relation caractérisant les 1-cocycles apparaît sous le nom de « relation de compatibilité ») associe à une telle k-variété une classe dans l'ensemble de cohomologie $H^1(G, \mathrm{Aut}_K(\mathbf{P}^d_K))$, et montre que deux telles k-variétés X et Y sont k-isomorphes si et seulement si elles ont même classe de cohomologie. En fait, comme $\mathbf{P}^d_k$ est une variété raisonnable, on sait que toute classe de cohomologie provient d'une variété de Severi-Brauer, ce que Châtelet semble avoir vu et qui fut plus tard démontré par Weil (1956).

Ce qui permet alors à Châtelet d'obtenir le théorème ci-dessus, c'est le double isomorphisme:

$\mathrm{Aut}_K(\mathbf{P}^d_K) \simeq PGL_{d+1}(K)$ (tout automorphisme de l'espace projectif est donné par une homographie)

$\mathrm{Aut}_K(M_{d+1}(K)) \simeq PGL_{d+1}(K)$ (Skolem-Noether).

Les « systèmes de matrices associés » ne sont autres que les 1-cocycles à valeurs dans $PGL_{d+1}(K)$; quant aux « systèmes de scalaires associés » à un tel 1-cocycle, c'est un 2-cocycle dont la classe de cohomologie dans le sous-groupe $H^2(G, K^*)$ du groupe de Brauer de k est obtenue à partir du 1-cocycle via la suite exacte G-équivariante de groupes:

$$1 \to K^* \to GL_{d+1}(K) \to PGL_{d+1}(K) \to 1 .$$

Le même principe général que plus haut, et dont, rappelons-le, Châtelet fut l'un des principaux inventeurs, dit que l'ensemble $H^1(G, PGL_{d+1}(K))$ classifie aussi les k-algèbres simples centrales de degré $d+1$ qui sont déployées par passage au corps K. Châtelet obtient ainsi tous les résultats sur les variétés de Severi-Brauer à partir des résultats connus sur les algèbres centrales simples.

Le mémoire de 1944 contient un autre résultat, oublié jusqu'à sa remise au goût du jour par M. Artin en 1982: F. Châtelet appelle « sous-variété normale » Y d'une variété de Severi-Brauer X une sous-variété fermée telle que $\bar{Y} \subset \bar{X} \simeq \mathbf{P}^n_{\bar{k}}$ soit un espace linéaire (ce qui ne dépend pas de l'isomorphisme choisi). Définissant $i(X)$ comme étant le plus petit des entiers r tels qu'il existe une sous-variété normale $Y \subset X$ de dimension $(r-1)$, Châtelet montre que $i(X)$ coïncide avec l'index (de la classe) d'une algèbre simple centrale associée à X par la correspondance ci-dessus (ceci généralise le point 1) du théorème).

Glissons ici un mot sur les articles de Châtelet consacrés à l'arithmétique des (hyper)quadriques (1948). Châtelet y examine d'un point de vue géomé-

trique les transformations qui permettent de passer d'une quadrique non-singulière X de $\mathbf{P}^3$ à une conique de $\mathbf{P}^2$ définie sur l'extension discriminant et ainsi en particulier d'obtenir le principe de Hasse pour ces quadriques.

1.3. Après les travaux de Châtelet.

En 1949, B. Segre tout en rendant hommage au travail de Châtelet rappelle l'existence du travail de Severi (1932) qui avait échappé à l'attention de Châtelet, et indique en particulier que Severi par ses méthodes avait obtenu $(d+1)^d$ au point 2) du théorème ci-dessus. C'est dans cet article que Segre transforme les « variétés de Brauer » de Châtelet en « variétés de Severi-Brauer ». Convenons qu'il eut été plus juste de les appeler variétés de Severi-Châtelet.

Alors que la théorie de Châtelet insiste de façon très moderne sur l'isomorphie sans exceptions, Amitsur en 1955 refait la théorie d'un point de vue plus birationnel (corps de décomposition « générique » d'une algèbre centrale simple) et redémontre l'énoncé 2) du théorème ci-dessus. Il établit le résultat intéressant suivant: si X et Y sont deux k-variétés de Severi-Brauer k-birationnellement équivalentes, les classes $a(X)$ et $a(Y)$ qui leurs sont associées dans le groupe de Brauer de k engendrent le même sous-groupe. On ignore si la réciproque vaut. Le point de vue de l'ensemble de cohomologie $H^1(\mathrm{Gal}(K/k), PGL_{d+1}(K))$ réapparaît dans un article de Roquette (1963). Signalons aussi un article d'Amitsur (1981).

Le point de vue moderne sur les variétés de Severi-Brauer qui a été esquissé plus haut fut dégagé par Serre dans ses livres *Corps locaux* (1962) et *Cohomologie galoisienne* (1965). Après l'introduction des algèbres d'Azumaya, qui généralisent les algèbres simples centrales, le corps de base étant remplacé par un anneau commutatif (Azumaya 1951, Auslander/Goldman 1960), Grothendieck (1965) dans une série magistrale d'exposés sur le groupe de Brauer d'un schéma étudie les schémas de Severi-Brauer relatifs.

1.4. Importance des variétés de Severi-Brauer.

En arithmétique, les variétés de Severi-Brauer servent de référence dans l'étude des variétés rationnelles plus générales (une variété X est dite rationnelle si elle devient birationnellement équivalente (mais non nécessairement isomorphe) à l'espace projectif sur une extension finie de son corps de base.) Pour $d > 1$, aucune des propriétés du théorème ci-dessus ne vaut en général, mais on peut essayer de trouver des substituts. Nous reviendrons là-dessus au paragraphe 3.

En géométrie, i.e. dans l'étude des variétés définies sur le corps des nombres complexes, les variétés de Severi-Brauer jouent un grand rôle comme fibre générique de morphismes $X \to Y$, dans l'étude des variétés qui sont « proches d'être rationnelles »: variétés unirationnelles de divers types. Ainsi, le fameux contre-exemple d'Artin/Mumford (1972) au problème de Lüroth en dimension 3 (une variété qui est dominée par une variété rationnelle n'est pas nécessairement rationnelle) est-il fourni par une telle variété X fibrée au-dessus d'une surface rationnelle Y, la fibre générique étant une conique sans point rationnel. D'autres variétés de Severi-Brauer apparaissent dans l'étude des corps d'invariants d'actions linéaires presque libres de groupes linéaires connexes.

Mais là où les variétés de Severi-Brauer ont sans conteste joué le rôle le plus important, c'est dans la démonstration des théorèmes de Merkur'ev et Suslin (1982) sur le groupe K_2 des corps, ceci via le calcul de Quillen (1973) de la K-théorie des schémas de Severi-Brauer. Ces théorèmes ont eu des applications tant aux algèbres simples centrales sur un corps arbitraire qu'à l'étude des groupes de Chow des variétés algébriques (classes de cycles pour l'équivalence rationnelle).

2. Courbes de genre 1

2.1. Avant Châtelet.

En 1901, Poincaré montre qu'une courbe C de genre 1 définie sur un corps k et qui possède un point k-rationnel est isomorphe sur son corps de définition à une courbe elliptique E de Weierstrass:

$$(E) \qquad y^2 = x^3 + ax + b\,,$$

laquelle admet naturellement une loi de groupe avec élément neutre le point à l'infini. Cette loi de groupe en induit une sur l'ensemble $E(k)$ des points rationnels. Poincaré formule l'hypothèse que pour k le corps $\mathbf{Q}$ des rationnels, le groupe $E(\mathbf{Q})$ est engendré par un nombre fini d'éléments. Ceci fut démontré par Mordell en 1922 et généralisé par Weil en 1928 au cas où k est un corps de nombres, et où E est la jacobienne d'une courbe de genre quelconque. Weil donna aussi une méthode « élémentaire », qui passe par des « factorisations ». On montre ainsi que pour E donnée par

$$y^2 = (x-e_1)(x-e_2)(x-e_3)$$

on dispose d'une injection

$$E(k)/2E(k) \to (k^*/k^{*2})^2$$
$$(x, y) \mapsto (x-e_1, x-e_2),$$

qui est d'image finie si k est un corps de nombres (théorème de Mordell-Weil faible). Nous verrons au paragraphe 3 comment ceci inspira Châtelet dans un autre contexte.

2.2. La contribution de Châtelet [1938] [1941] [1946a] [1947a].

La motivation initiale de Châtelet était de déterminer quand une courbe C de genre 1 définie sur un corps k a un point rationnel. Il s'agissait là d'un projet bien ambitieux: à ce jour on ne possède, dans le cas $k = \mathbf{Q}$, d'aucun algorithme sûr pour ce faire. Voici les résultats que Châtelet obtint (le corps k est simplement supposé parfait).

1) *Pour C de genre 1 définie sur k, il existe une courbe elliptique E définie sur k (i.e. E de genre 1, et $E(k) \neq \emptyset$) et un isomorphisme, défini sur $\bar{k}$,*

$$f : \bar{E} \simeq \bar{C}.$$

2) *A un tel isomorphisme on associe un 1-cocycle*

$$a_\sigma = {}^\sigma f \circ f^{-1} \in Z^1(G, \mathrm{Aut}(\bar{E})), \quad \text{où} \quad G = \mathrm{Gal}(\bar{k}/k).$$

3) *On dispose d'une suite exacte de G-groupes:*

$$1 \to E(\bar{k}) \to \mathrm{Aut}(\bar{E}) \to F \to 1,$$

où F est un groupe fini, en général égal à $\{\pm 1\}$. Quitte à changer de courbe de référence E en 1), on peut assurer que a_σ vient de $Z^1(G, E(\bar{k}))$. Cette condition détermine la courbe elliptique E (qui n'est autre alors que la jacobienne de E).

4) *Deux courbes C et D de genre 1 définies sur k sont isomorphes sur k si et seulement si d'une part elles ont même jacobienne E, d'autre part il existe $b \in E(\bar{k})$ tel que $a_\sigma(C) - a_\sigma(D) = {}^\sigma b - b$ pour tout $\sigma \in G$.*

5) *$C(k)$ est non vide si et seulement si il existe $b \in E(\bar{k})$ tel que $a_\sigma = {}^\sigma b - b$ pour tout $\sigma \in G$.*

En termes modernes, 3) dit que C est un espace principal homogène sous la courbe elliptique E, et 4) dit que l'ensemble des classes d'isomorphisme

d'espaces principaux homogènes sous E se plonge dans le groupe (abélien) de cohomologie $H^1(G, E(\bar{k}))$.

Ce fut Weil qui, en 1955, montra que ce plongement est en fait une bijection, si bien que les classes d'isomorphisme d'espaces principaux homogènes sous E forment un groupe abélien. C'est ce groupe qui fut nommé en 1957 groupe de Weil-Châtelet WC(E) par Tate, lequel considéra plus généralement le groupe $H^1(G, A(\bar{k}))$ pour A une variété abélienne définie sur k.

Les résultats de Châtelet lui permirent de retrouver des résultats antérieurs de façon entièrement algébrique:

Il établit d'une part ([1939], [1947*c*]) le théorème de F. K. Schmidt (1931) selon lequel toute courbe de genre 1 sur un corps fini F possède un point rationnel en montrant que les groupes $H^1(\mathrm{Gal}(F_r/F), E(F_r))$ et $E(F)/NE(F_r)$, où N est la norme correspondant à l'extension de corps finis F_r/F, ont même cardinal et que le dernier groupe est nul, en utilisant le théorème de Riemann-Roch.

Il retrouva d'autre part ([1949*a*]) les résultats de Klein, Weichold, Witt (1934) sur la classification des courbes de genre 1 sur le corps $\mathbf{R}$: si C et D sont deux courbes de genre 1 sur $\mathbf{R}$ de jacobienne E, elles sont isomorphes à E si $E(\mathbf{R})$ est connexe; si $E(\mathbf{R})$ est disconnexe et ni C ni D n'ont de point réel, elles sont isomorphes entre elles. Le point ici est l'isomorphisme $H^1(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), E(\mathbf{C})) \simeq E(\mathbf{R})/N_{\mathbf{C}/\mathbf{R}}(E(\mathbf{C})) = 0$ ou $\mathbf{Z}/2$.

Enfin, F. Châtelet a fait quelques pas dans la direction de la suite exacte de cohomologie (dégagée par Lang et Tate en 1958)

$$0 \to E(k)/nE(k) \to H^1(G, {}_nE(\bar{k})) \to {}_nH^1(G, E(\bar{k})) \to 0$$

déduite de la suite de G-modules

$$0 \to {}_nE(\bar{k}) \to E(\bar{k}) \xrightarrow{n} E(\bar{k}) \to 0\,.$$

Dans des cas particuliers [1941], il a vu la structure de groupe sur le terme médian $H^1(G, {}_nE(\bar{k}))$, d'où une composition des « n-revêtements ». Mais il semble bien que ce soit Weil qui ait établi la structure de groupe de l'ensemble des classes d'isomorphisme d'espaces principaux homogènes sous E.

Il est intéressant de noter que dans ses articles, Châtelet insiste sur le fait que son analyse permet de ramener la question de l'existence d'un point rationnel sur C à la connaissance du groupe de Mordell-Weil $E(k)$ de la courbe jacobienne E associée. Si les deux problèmes sont en fait essentiellement équivalents, l'approche cohomologique que F. Châtelet a contribué à introduire a servi de fondement à tous les développements ultérieurs.

2.3. Après Châtelet.

On a vu plus haut les développements directs que constituèrent les articles de Weil (1955) et de Lang-Tate (1958). En 1956, Lang établit que pour un groupe algébrique connexe quelconque A défini sur un corps fini F, l'ensemble de cohomologie $H^1(G, A(\bar{F}))$ est trivial: tout espace principal homogène sous A est isomorphe à A, ce qui généralise l'approche de Châtelet du théorème de F. K. Schmidt. En 1957, un exposé fameux de Tate au séminaire Bourbaki, intitulé « WC-groups over $\mathfrak{p}$-adic fields », établit, pour k un corps $\mathfrak{p}$-adique et A une variété abélienne définie sur k, des théorèmes de dualité entre $A(k)$ et $H^1(G, A(\bar{k}))$ qui sont les analogues des théorèmes de Witt (1934) dans le cas réel.

La théorie des courbes de genre 1 a depuis connu de tels développements qu'il serait impossible de les évoquer ici. Mentionnons cependant les travaux de Selmer (1951-1956) et Cassels (1959-1966), et l'introduction du groupe de Tate-Shafarevitch

$$Ш^1(k, E) = \mathrm{Ker}\,[WC(E) \to \Pi_v WC(E_v)]\,,$$

où v parcourt les places du corps de nombres k et où E_v est la courbe E considérée sur le complété k_v de k. Ce groupe mesure le défaut du principe de Hasse pour les espaces principaux homogènes sous E. Sa finitude est conjecturée et vient seulement d'être établie pour certaines courbes (Rubin, 1986).

2.4. Points de torsion.

Châtelet a aussi consacré plusieurs articles ([1940*a*], [1940*b*], [1947*b*], [1950*a*]) aux « points exceptionnels » des cubiques planes. La tangente en un point rationnel P d'une cubique plane E recoupe E en un troisième point rationnel, on prend la tangente en ce nouveau point et l'on recommence: le point P est dit exceptionnel si après un nombre fini d'itérations on retrouve le point P. Dans le cas d'une cubique de Weierstrass, ceci revient à dire que le point P est un point de torsion du groupe $E(k)$. Lorsque k est un corps de nombres, ce groupe est fini. Pour $k = \mathbf{Q}$ et E sous forme de Weierstrass

$$y^2 = x^3 + ax + b$$

avec a et b dans $\mathbf{Z}$, Nagell établit en 1935 que si $(x, y) \in E(\mathbf{Q})$ est un point exceptionnel, alors x et y sont dans $\mathbf{Z}$ et y est nul ou divise $4a^3 + 27b^2$, ce qui permet une détermination *effective* des points de torsion. Une méthode

générale fut développée par E. Lutz (1937) et A. Weil (1936), qui étudièrent la structure du groupe topologique $E(k)$ lorsque k est un corps p-adique (ce qu'on peut transcrire aujourd'hui au moyen des groupes formels et des modèles de Néron). Châtelet attira l'attention sur le fait que la méthode d'E. Lutz permet la détermination effective des points exceptionnels lorsque le corps de base k est un corps de nombres quelconque. Dans une note de 1940, Châtelet observe que les résultats de Lutz permettent de borner uniformément la torsion des courbes elliptiques définies sur un corps de nombres k et d'invariant j fixé (il suffit de se placer sur une complétion p-adique de k; à k-isomorphisme près, il n'y a alors qu'un nombre fini de courbes elliptiques d'invariant j donné, et pour chacune d'elles le groupe de torsion est fini). C'est un problème ouvert de savoir si la condition sur j peut être omise (dans le cas $k = \mathbf{Q}$, c'est un théorème de Mazur que l'ordre du groupe de torsion est au plus 16).

3. Surfaces cubiques

C'est la partie de l'œuvre de Châtelet qui a joué un grand rôle dans mes recherches personnelles.

Sauf mention du contraire, les surfaces cubiques ici considérées sont supposées absolument irréductibles et non coniques. Le corps de base k est pris de caractéristique zéro.

3.1. Avant Châtelet.

De 1940 à 1944, Mordell et B. Segre s'intéressent aux surfaces cubiques. Ils montrent que si une telle surface X définie sur k possède un point rationnel non singulier, alors il existe une application rationnelle dominante définie sur k d'un plan projectif sur X. En particulier les points rationnels sont denses pour la topologie de Zariski. B. Segre montre en 1944 qu'une surface cubique singulière X qui possède un point rationnel non singulier est k-rationnelle (k-birationnelle au plan projectif) sauf si X possède exactement deux points singuliers conjugués. En 1951, ce même Segre étudie les surfaces cubiques non singulières. On dit qu'une telle surface contient un S_n si elle contient un ensemble globalement défini sur k de n droites gauches deux à deux. Segre montre que si X est k-rationnelle, alors X contient nécessairement un S_1, un S_2, un S_3 ou un S_6 (comme le montrèrent indépendamment en 1970 Swinnerton-Dyer et Iskovskih, X contient en fait un S_2, un S_3 ou un S_6). En 1951, Segre donne aussi les premiers exemples

de surfaces cubiques X qui possèdent un point rationnel non-singulier mais qui ne sont pas k-rationnelles. En 1953, Selmer établit le principe de Hasse pour les surfaces cubiques diagonales

$$ax^3 + by^3 + cz^3 + dt^3 = 0\,, \qquad ab/cd \in k^{*3}\,.$$

En 1955, Skolem établit le principe de Hasse pour les surfaces cubiques singulières.

3.2. La contribution de Châtelet [1953] [1954*a*] [1954*b*] [1958] [1959*b*] [1966].

Tout d'abord, Châtelet montra qu'une surface cubique non singulière qui contient un S_3 ou un S_6 satisfait le principe de Hasse. Ce résultat généralise le résultat de Selmer mentionné ci-dessus. La clé de la démonstration est que si X contient un S_6, alors X est k-birationnelle à une surface de Severi-Brauer. Les notes de 1953 et 1954 contiennent des équations concrètes pour des surfaces satisfaisant les dites conditions.

Dans [1954*b*], Châtelet se demande comment décrire l'ensemble $X(k)$ des points rationnels d'une surface cubique X lorsque k est un corps de nombres et que X n'est pas k-rationnelle, ce qui exclut une représentation paramétrique essentiellement biunivoque. On pourrait a priori chercher un nombre fini de paramétrisations multivoques $\varphi_i : X_i \to X$ avec $X(k) = \bigcup_i \varphi_i(X_i(k))$ et chaque X_i k-birationnel au plan projectif $\mathbf{P}^2_k$. Châtelet remarque que cela semble très difficile (en 1967, Manin montrera que c'est en général impossible). Aussi Châtelet fait-il la suggestion très originale suivante: chercher de telles paramétrisations, mais avec X_i k-birationnel à $\mathbf{P}^n_k$ pour un entier $n > 2$. Il prend alors comme exemple la surface X d'équation

$$N_{K/k}(x + \omega y + \omega^2 z) = 1$$

avec $K = k(\omega)$ extension cubique non cyclique du corps de nombres k. Ici $X(k) = K^{*1}$ est le groupe des éléments de K^* de norme 1. Si L/k est la clôture galoisienne de K/k, $G = \mathrm{Gal}\,(L/k) = \langle s, t \rangle$ avec $s^3 = t^2 = 1$, Châtelet montre que l'application

$$\varphi : L^* \to K^{*1}$$
$$x \mapsto (s(x)/x) \cdot (t(s(x))/x))$$

a un conoyau fini. La démonstration utilise des factorisations fort réminiscentes de la démonstration du théorème de Mordell-Weil faible. En

fait, l'application φ est, pour des raisons algébriques, surjective quel que soit le corps k. Mais la méthode inspira des travaux ultérieurs (voir 3.3).

En 1958, Châtelet s'intéressa à des surfaces cubiques avec deux points singuliers conjugués :

$$y^2 - az^2 = (x-e_1)(x-e_2)(x-e_3) \qquad (X).$$

Les résultats qu'il obtint et que je vais maintenant décrire eurent une grande influence sur les recherches ultérieures.

Pour ces surfaces, appelées depuis surfaces de Châtelet, il établit ([1959*b*], [1966]), lorsque k est un corps de nombres, l'existence d'un nombre fini de paramétrisations pour les points rationnels, du type suggéré plus haut (les X_i sont ici k-birationnels à $\mathbf{P}^4_k$). Ici, une seule paramétrisation ne suffit en général pas à couvrir les points rationnels d'une telle surface.

La méthode est directement inspirée de la démonstration de Weil du théorème de Mordell-Weil faible. Si K est l'extension quadratique $k(\sqrt{a})$ de k et N désigne la norme de K à k, Châtelet considère l'application :

$$f : X(k) \to (k^*/NK^*)^2$$
$$(x, y, z) \mapsto (x-e_1, x-e_2)$$

et montre qu'elle a une image finie. Par ailleurs, il montre que le noyau de f est constitué des points de $X(k)$ qui sont obtenus à partir de $X(K)$ par l'application p qui à un point $P \in X(K)$ associe le troisième point d'intersection avec X de la droite passant par P et par le conjugué de P (composition de P et de son conjugué). Cette application peut être vue comme l'application $\varphi_1 : X_1(k) \to X(k)$ induite par une application rationnelle définie sur k de la k-variété algébrique $X_1 = R_{K/k}(X_K)$ vers X. Ici $R_{K/k}$ est le foncteur de descente « à la Weil » qui transforme une variété définie sur K en variété définie sur k, en multipliant la dimension par le degré de K sur k. Soit S le k-tore algébrique défini par $u_1^2 - av_1^2 = 1$, $u_2^2 - av_2^2 = 1$, et soit $\mathscr{T}$ l'espace principal homogène sur X sous S défini par les équations

$$x - e_1 = u_1^2 - av_1^2, \quad x - e_2 = u_2^2 - av_2^2.$$

Ce que Châtelet établit plus précisément, c'est d'une part que l'application rationnelle $R_{K/k}(X_K) \to X$ définie par la « composition » se factorise par une application $i : R_{K/k}(X_K) \to \mathscr{T}$, d'autre part, par un calcul explicite et qui à ce jour n'a pas encore perdu tout son mystère, que l'application i est k-birationnelle. Ce calcul est analogue à la présentation de la multiplication par 2 sur une courbe de Weierstrass E comme espace principal homogène sur E sous le groupe $\mu_2 \times \mu_2$ donné par les équations $x - e_1 = u_1^2$, $x - e_2 = u_2^2$.

Comme X_K est évidemment une surface K-rationnelle, la k-variété $X_1 = R_{K/k}(X_K)$ est k-rationnelle, si bien que l'on a paramétré les points du noyau de f. Pour paramétrer les points de $X(k)$ d'image non triviale par f, Châtelet observe par un calcul fort instructif que pour tout $\alpha = f(P_0)$, les points M de $f^{-1}(\alpha) \subset X(k)$ sont obtenus à partir des points de $\varphi_1(X_1(k))$ en appliquant la « symétrie » par rapport au point P_0.

3.3. Après Châtelet.

Les travaux consécutifs à ceux de Châtelet se sont en général placés dans la perspective plus large de l'étude des surfaces rationnelles et aussi de certaines variétés rationnelles de dimension plus grande. Comme ces travaux ont fait récemment l'objet d'exposés généraux (Manin/Tsfasman 1986, l'auteur 1986), on se contentera ici de décrire les développements ayant trait directement aux recherches de Châtelet.

Manin et Iskovskih, généralisant des résultats d'Enriques (1897) ont établi une classification k-birationnelle des surfaces rationnelles. Dans cette classification, les surfaces de Châtelet généralisées:

$$y^2 - az^2 = P(x), \quad \deg P \leqslant 4$$

apparaissent comme les surfaces arithmétiquement non-triviales les plus simples. Elles ont servi de banc d'essai pour toutes les conjectures concernant les variétés rationnelles, conjectures dont on a quelques raisons d'espérer qu'elles s'insèrent dans un ensemble bien plus vaste, sortant du cadre des variétés rationnelles.

Pour la commodité de l'exposé, disons que l'on s'est intéressé aux trois thèmes suivants:

k-rationalité. Si X est une surface (variété) rationnelle avec un k-point non singulier, qu'est-ce qui empêche X d'être k-rationnelle, ou du moins k-stablement rationnelle ($X \times \mathbf{P}^r_k$ k-birationnel à $\mathbf{P}^s_k$), et y a-t-il une différence entre ces deux notions (problème de Zariski, mentionné par B. Segre en 1950)?

Principe de Hasse. Si k est un corps de nombres, décrire l'obstruction à la validité du principe de Hasse.

Description des points rationnels. Si k est un corps de nombres, et $X(k) \neq \emptyset$, obtenir des paramétrisations finies du type de Châtelet pour d'autres classes de variétés. A défaut, décrire des relations d'équivalence sur $X(k)$ approchant la décomposition en classes de paramétrisation.

Manin et Voskresenskii dégagèrent le rôle important du module galoisien $\mathrm{Pic}(\bar{X})$ (X variété rationnelle projective et lisse) dans l'étude de la k-rationalité (stable). Ainsi, au moins en caractéristique zéro, le groupe $H^1(G, \mathrm{Pic}(\bar{X}))$ est un invariant k-birationnel qui est essentiellement équivalent à un autre invariant, le groupe de Brauer-Grothendieck de X. Ces invariants permettent souvent de reconnaître qu'une k-variété rationnelle n'est pas k-rationnelle, ce bien qu'elle possède un point rationnel.

Swinnerton-Dyer donna dès 1962 des contre-exemples au principe de Hasse pour les surfaces cubiques lisses, et d'autres suivirent pour d'autres types de surfaces rationnelles. Manin (1970) mit de l'ordre dans ces contre-exemples, en les interprétant au moyen du groupe de Brauer-Grothendieck.

Dans son livre sur les formes cubiques (1970), Manin donne aussi son point de vue sur la paramétrisation des points rationnels des surfaces de Châtelet. Il introduit d'une part la notion de R-équivalence sur les points (être liés par une chaîne de courbes de genre zéro), d'autre part l'équivalence de Brauer, via l'accouplement naturel $X(k) \times \mathrm{Br}\, X \to \mathrm{Br}\, k$. Il se trouve que pour les surfaces de Châtelet ces deux notions coïncident, mais il n'en est plus ainsi pour les surfaces de Châtelet généralisées.

En 1970, je passai une année à Cambridge (Angleterre) et P. Swinnerton-Dyer me suggéra de comprendre en profondeur les calculs assez mystérieux de Châtelet, ce afin de généraliser les résultats à d'autres variétés. En 1974, je pus ainsi interpréter une partie des calculs de Châtelet grâce à l'utilisation de torseurs sous des tores particuliers (ainsi le calcul fort instructif mentionné à la fin de 3.2 peut être interprété au moyen d'une généralisation de la loi de réciprocité d'A. Weil).

En 1976, Sansuc et moi-même, inspirés par les articles de Châtelet de 1954 et 1959 d'une part et par les travaux de Manin et Voskresenskii d'autre part, établîmes pour les points rationnels des tores algébriques l'analogue du résultat de paramétrisation finie de Châtelet. Ce résultat peut s'interpréter dans la perspective de la « descente » sur les points rationnels d'une variété rationnelle X. Comme Châtelet, on utilise des torseurs sur X sous des tores, plutôt que le groupe de Brauer-Grothendieck (de tels torseurs donnent une meilleure approximation de la R-équivalence sur $X(k)$). En 1984, Sansuc, Swinnerton-Dyer et moi-même pûmes compléter le programme de la descente pour toutes les surfaces de Châtelet généralisées. Ainsi, si une telle surface X possède un k-point et si l'invariant $\mathrm{Pic}(\bar{X})$ est « trivial », alors X est stablement k-rationnelle. Comme d'autres invariants, non stables, permettent parfois de montrer que X n'est pas k-rationnelle, ceci mena à une réponse négative au problème de Zariski, tant pour les surfaces sur $\mathbf{Q}$

(exemple: $y^2+3z^2=x^3-2$) que pour les variétés de dimension 3 sur $\mathbf{C}$ (résultat obtenu en collaboration avec Beauville). Par ailleurs, l'obstruction de Manin au principe de Hasse (donnée par le groupe de Brauer-Grothendieck) est ici la seule, et ceci permet de déterminer effectivement si une telle surface a un point rationnel. Enfin, les points rationnels d'une telle surface peuvent être décrits au moyen d'un nombre fini de paramétrisations par des variétés k-rationnelles.

Dans ses recherches, François Châtelet ne s'est jamais enlisé dans un formalisme gratuit. Les idées qu'il a lancées sont encore fécondes aujourd'hui, et j'aimerais en conclusion redire combien elles m'ont marqué.

ARTICLES DE FRANÇOIS CHÂTELET

[1938] Points rationnels et classification des courbes de genre un. *C. R. Acad. Sc. Paris 206* (1938), 1532.

[1939] Classification des courbes de genre un, dans le corps des restes, module *p*. *C. R. Acad. Sc. Paris 208* (1939), 487-489.

[1940*a*] Points exceptionnels d'une cubique de Weierstrass. *C. R. Acad. Sc. Paris 210* (1940), 90-92.

[1940*b*] Groupe exceptionnel d'une classe de cubiques. *C. R. Acad. Sc. Paris 210* (1940), 200-202.

[1941] Courbes réduites dans les classes de courbes de genre 1. *C. R. Acad. Sc. Paris 212* (1941), 320-322.

[1943*a*] Sur la notion d'équivalence due à Poincaré. *C. R. Acad. Sc. Paris 216* (1943), 142-144.

[1943*b*] Equivalence de certaines variétés unicursales. *C. R. Acad. Sc. Paris 216* (1943), 189-191.

[1944] Variations sur un thème de Poincaré. *Annales E.N.S., 3^e série, 61* (1944), 249-300.

[1945] Les êtres géométriques d'un corps abstrait. *Annales de l'Université de Lyon, 3^e série, Section A, VIII* (1945), 5-28.

[1946*a*] Méthode galoisienne et courbes de genre un. *Annales de l'Université de Lyon, 3^e série, Section A, IX* (1946), 40-49.

[1946*b*] Introduction géométrique à l'étude arithmétique des cubiques. *Revue Scientifique 84* (1946), 3-6.

[1946*c*] Eléments de géométrie galoisienne. *Bulletin de la S.M.F. 74* (1946), 69-86.

[1946*d*] Les correspondances birationnelles à coefficients rationnels sur une courbe. *C. R. Acad. Sc. Paris 222* (1946), 351-353.

[1947*a*] Sur l'arithmétique des courbes de genre un. *Annales de l'Université de Grenoble (nouvelle série), XXII, Année 1946* (1947), 153-165.

[1947*b*] Utilisation des congruences en analyse indéterminée. *Annales de l'Université de Lyon, 3^e série, Section A, X* (1947), 5-22.

[1947c] Les courbes de genre 1 dans un champ de Galois. *C. R. Acad. Sc. Paris 224* (1947), 1616-1618.

[1947d] Intérêt et signification de l'analyse indéterminée. *Rev. Gén. Sci. Pures et Appl., nouvelle série, 54* (1947), 199-201.

[1947e] Sur la réalité des courbes unicursales. *Revue Sci. 85* (1947), 709-715.

[1947f] Une méthode galoisienne en théorie des nombres. *Suppl. au fasc. 9 de l'Interm. des Rech. Math.* (1947), 49-53.

[1948a] Relations entre l'arithmétique et la géométrie sur une quadrique. *Bulletin de la S.M.F. 76* (1948), 108-113.

[1948b] Formes quadratiques dans un corps arbitraire. *C. R. Acad. Sci. Paris 226* (1948), 1233-1235.

[1948c] Hyperquadriques dans un corps arbitraire. *C. R. Acad. Sci. Paris 226* (1948), 1578-1580.

[1949a] Sur la réalité des courbes de genre un. *Annales de la Faculté des Sciences de l'Université de Toulouse (4) XI, Année 1947* (1949), 75-92.

[1949b] Sur les points multiples des courbes algébriques planes. *Cahiers Rhodaniens I* (1949), 9 p.

[1950a] Points exceptionnels des cubiques. In *Algèbre et théorie des nombres*, Coll. intern. du C.N.R.S. n° 24, 71-72. C.N.R.S., Paris, 1950.

[1950b] Représentations des courbes par radicaux. In *Algèbre et théorie des nombres*, Coll. intern. du C.N.R.S. n° 24, 73-76. C.N.R.S., Paris, 1950.

[1950c] Application des idées de Galois à la géométrie algébrique. *Colloque de géométrie algébrique*, Liège, 1949, 91-103. Georges Thone, Liège ; Masson et Cie, Paris, 1950.

[1953] Sur un exemple de M. B. Segre. *C. R. Acad. Sc. Paris 236* (1953), 268-269.

[1954a] Exemples de surfaces de Brauer. *C. R. Acad. Sci. Paris 239* (1954), 1578-1579.

[1954b] Points rationnels sur les surfaces cubiques. (20 Février 1954), *Séminaire d'algèbre et de théorie des nombres de Paris* (A. Châtelet/P. Dubreil) 1953/1954, exposé n° 8. Secrétariat mathématique, Paris, 1956.

[1955] Géométrie diophantienne et théorie des algèbres. *Séminaire d'algèbre et de théorie des nombres de Paris* (A. Châtelet/P. Dubreil) 1954/1955, exposé n° 17. Secrétariat mathématique, Paris, 195?.

[1957] Quelques propriétés arithmétiques des courbes algébriques. *Séminaire Dubreil-Pisot*, 1956/1957, Exposé n° 16.

[1958] Courte communication au congrès international d'Edimbourg (1958).

[1959a] Points rationnels sur certaines surfaces cubiques. *Séminaire Dubreil, Dubreil-Jacotin, Pisot*, 1958/1959, Exposé n° 12.

[1959b] Points rationnels sur certaines courbes et surfaces cubiques. *Ens. Math. 5* (1959), 153-170.

[1960] Introduction à l'analyse diophantienne. *Ens. Math. 6* (1960), 3-17.

[1961] L'arithmétique des corps quadratiques. *Séminaire Dubreil, Dubreil-Jacotin, Pisot*, 1960/1961, Exposé n° 14 (1963), 2 p.

[1964] Les idéaux de l'anneau des polynômes d'une variable à coefficients entiers. In *Algebraische Zahlentheorie*, Oberwolfach 1964, Bibliographisches Institut, Mannheim 1966, 43-51.

[1966] Points rationnels sur certaines surfaces cubiques. In *Les tendances géométriques en algèbre et théorie des nombres*, Clermont-Ferrand (1964). Editions du C.N.R.S. (1966), 67-75.

[1967] (avec S. Thouvenot). Au sujet des congruences de degré supérieur à deux. *Ens. Math. 13* (1967), 89-98.

[1973] Construction d'algèbres normales simples et de variétés de Severi-Brauer. *Séminaire de théorie des nombres de Besançon*, 19 et 26 Octobre 1973.

[1975*a*] Construction d'algèbres simples. *J. für die reine und ang. Math. 274/275* (1975), 258-262.

[1975*b*] Sur l'équivalence finie des polyèdres. *Ens. Math. 21* (1975), 115-121.

BIBLIOGRAPHIE

AMITSUR, S. A. Generic splitting fields of central simple algebras. *Ann. of Math. 62* (1955), 8-43.

—— Some results on central simple algebras. *Ann. of Math. 63* (1956), 285-293.

—— Generic splitting fields. In *Brauer groups in ring theory and algebraic geometry*, Springer L.N.M. 917 (1982), ed. F. van Oystaeyen and A. Verschoren, 1-24.

ARTIN, M. Brauer-Severi varieties (notes by A. Verschoren). In *Brauer groups in ring theory and algebraic geometry*, Springer L.N.M. 917 (1982), ed. F. van Oystaeyen and A. Verschoren, 194-210.

ARTIN, M. and D. MUMFORD. Some elementary examples of unirational varieties which are not rational. *Proc. London Math. Soc. (3) 25* (1972), 75-95.

BEAUVILLE, A., J.-L. COLLIOT-THÉLÈNE, J.-J. SANSUC et Sir Peter SWINNERTON-DYER. Variétés stablement rationnelles non rationnelles. *Ann. of Math. 121* (1985), 283-318.

CASSELS, J. W. S. Diophantine equations with special reference to elliptic curves. *Journal London Math. Soc. 41* (1966), 193-291.

COLLIOT-THÉLÈNE, J.-L. Arithmétique des variétés rationnelles et problèmes birationnels. *Proc. Intern. Congr. Math., Berkeley*, 1986.

COLLIOT-THÉLÈNE, J.-L. et J.-J. SANSUC. La *R*-équivalence sur les tores. *Ann. Sci. Ecole Norm. Sup. 10* (1977), 175-229.

COLLIOT-THÉLÈNE, J.-L. et J.-J. SANSUC. La descente sur les variétés rationnelles II. *Duke Math. J. 54* (1987), 375-492.

COLLIOT-THÉLÈNE, J.-L., J.-J. SANSUC and Sir Peter SWINNERTON-DYER. Intersections of two quadrics and Châtelet surfaces. *J. für die reine und angew. Math. 373* (1987), 37-107; *374* (1987), 72-168.

DEURING, M. *Algebren.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer Verlag, Berlin 1935 zweite Auflage 1968.

GROTHENDIECK, A. Le groupe de Brauer I, II, III. In *Dix exposés sur la cohomologie des schémas*, North Holland, Amsterdam (1968), 46-188.

LANG, S. Algebraic groups over finite fields. *Amer. J. of Math. 78* (1956), 555-563.

LANG, S. and J. TATE. Principal homogeneous spaces over abelian varieties. *Amer. J. of Math. 80* (1958), 659-684.

LUTZ, E. Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques. *J. reine und ang. Math. 177* (1937), 237-247.

MERKUR'EV, A. S. and A. A. SUSLIN. *K*-cohomology of Severi-Brauer varieties and the norm residue homomorphism. *Izv. Akad. Nauk SSSR Ser. Mat. 46* (1982), 1011-1046 = *Math. USSR Izv. 21* (1983), 307-340.

MANIN, Yu. I. Le groupe de Brauer-Grothendieck en géométrie diophantienne. In *Actes Congrès Intern. Math. (Nice 1970)*, Gauthiers-Villars, Paris 1971, Tome 1, 401-411.

—— *Cubic forms.* Nauka, Moscou 1972, Traduction: North Holland, Amsterdam-London, 1974, second revised edition 1986.

MANIN, Yu. I. and M. A. TSFASMAN. Rational varieties: algebra, geometry and arithmetic. *Uspekhi Mat. Nauk 41* (1986), 43-94 = *Russian Math. Surveys 41* (1986), 51-116.

NOETHER, M. Über Flächen, welche Schaaren rationaler Curven besitzen. *Math. Ann. 3* (1871), 161-227.

—— Rationale Ausführung der Operationen in der Theorie der algebraischen Functionen. *Math. Ann. 23* (1884), 311-358.

POINCARÉ, H. Sur les propriétés arithmétiques des courbes algébriques. *J. Math. Pures et Appl., 5^e série, 7* (1901), 161-234 = *Oeuvres*, t. V, 483-550 (1950).

QUILLEN, D. Higher algebraic *K*-theory, I. In *Algebraic K-theory I, Higher K-theories*, Springer L.N.M. 341 (1973), 85-147.

ROQUETTE, P. On the Galois cohomology of the projective group and its applications to the construction of splitting fields of algebras. *Math. Ann. 150* (1963), 411-439.

—— Isomorphisms of generic splitting fields of simple algebras. *Journal für die reine und ang. Math. 214/215* (1964), 207-226.

SCHMIDT, F. K. Analytische Zahlentheorie in Körpern der Charakteristik *p*. *Math. Zeit. 33* (1931), 1-31.

SEGRE, B. Questions arithmétiques sur les variétés algébriques. In *Colloque International d'Algèbre et de Théorie des Nombres* (Paris 1949), 83-91, C.N.R.S., Paris 1950.

—— The rational solutions of homogeneous cubic equations in four variables. *Math. Notae (Rosario, Argentina) 11* (1951), 1-68.

—— *Arithmetical questions on algebraic varieties.* Univ. of London, Athlone Press, London 1951.

—— Sull'esistenza, sia nel campo razionale che nel campo reale, di involuzioni piane non birazionali. *Atti Accad. Naz. Lincei, Rend. Cl. Sci. fis. mat. e nat. 10* (1951), 94-97.

SELMER, E. Sufficient congruence conditions for the existence of rational points on certain cubic surfaces. *Math. Scand. 1* (1953), 113-119.

SERRE, J.-P. *Groupes algébriques et corps de classes.* Hermann, Paris, 1959.

—— *Cohomologie galoisienne.* L.N.M. 5, Springer-Verlag, Berlin, 1965.

—— *Corps locaux.* Hermann, Paris, 1968.

SEVERI, F. Un nuovo campo di richerche nella geometria sopra una superficie e sopra una varietà algebrica. *Mem. della Acc. R. d'Italia 3* (1932), 1-52 = *Opere matematiche, vol. terzo*, 541-586, Acc. Naz. Lincei, Roma 1977.

SKOLEM, T. Einige Bemerkungen über die Auffindung der rationalen Punkte auf gewissen algebraischen Gebilden. *Math. Z. 63* (1955), 295-312.

SUSLIN, A. A. Algebraic *K*-theory and the norm residue homomorphism. *Journal of Soviet Mathematics 30* (1985), 2556-2611.

TATE, J. T. *WC*-groups over p-adic fields. *Séminaire Bourbaki 156* (1957-1958).

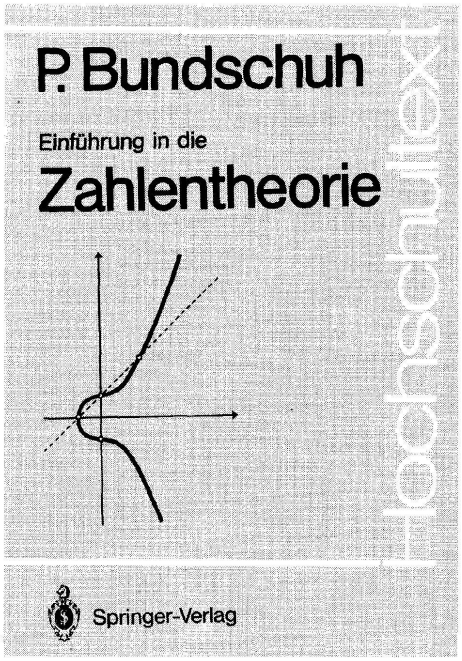
—— The arithmetic of elliptic curves. *Inventiones math. 23* (1974), 179-206.

WEIL, A. Sur les fonctions elliptiques p-adiques. *C. R. Acad. Sc. Paris 203* (1936), 22-24.
—— On algebraic groups and homogeneous spaces. *American J. of Math. 77* (1955), 493-512.
—— The field of definition of a variety. *Amer. J. of Math. 78* (1956), 509-524.
WITT, E. Über ein Gegenbeispiel zum Normensatz. *Math. Z. 39* (1934), 462-467.
—— Zerlegung reeller algebraischer Functionen in Quadrate. Schiefkörper über reellem Functionenkörper. *J. für die reine und angew. Math. 171* (1934), 4-11.

(Reçu le 31 mars 1988)

Jean-Louis Colliot-Thélène

Mathématique — Bâtiment 425
Université de Paris-Sud
F-91405 ORSAY Cedex (France)



P. Bundschuh

Einführung in die Zahlentheorie

1988. 7 Abbildungen. XIV, 332 Seiten. Broschiert DM 78,-.
ISBN 3-540-15305-5

Inhaltsübersicht: Teilbarkeit. - Kongruenzen. - Potenzreste, insbesondere quadratische Reste. - Additive Probleme und diophantische Gleichungen. - Verschiedene Entwicklungen reeller Zahlen. - Transzendenz. - Primzahlen. - Literaturverzeichnis. - Namen- und Sachverzeichnis.

Das Buch gibt eine umfassende Darstellung der wichtigsten Grundlagen der elementaren Zahlentheorie; dabei wird die historische Entwicklung in stärkerem Maße als üblich berücksichtigt. Behandelt wird in den ersten fünf Kapiteln (Teilbarkeit, Kongruenzen, Potenzreste und quadratische Reste, additive Probleme und diophantische Gleichungen, verschiedene Entwicklungen reeller Zahlen) etwa der Stoff einer einsemestrigen Einführungsvorlesung. Dabei ergeben sich schon früh neue Probleme, die in späteren Kapiteln wieder aufgegriffen werden. So kommen bereits im ersten Kapitel arithmetische und Primzahlfragen zur Sprache, die in den beiden letzten (Transzendenz, Primzahlen) erheblich vertieft werden. In diesen Kapiteln soll der Leser beispielhaft lernen, wie sich die Zahlentheorie zur Lösung ihrer Probleme bisweilen anderer mathematischer Disziplinen bedient: Beide Kapitel zeigen die Leistungsfähigkeit analytischer Methoden bei zahlentheoretischen Fragestellungen.

N. Koblitz

A Course in Number Theory and Cryptography

1987. 5 figures. VII, 208 pages. (Graduate Texts in Mathematics, Volume 114). Hard cover DM 74,-.
ISBN 3-540-96576-9

Contents: Some Topics in Elementary Number Theory. - Finite Fields and Quadratic Residues. - Cryptography. - Public Key. - Primality and Factoring. - Elliptic Curves. - Answers to Exercises. - Index.

Springer-Verlag
Berlin Heidelberg New York
London Paris
Tokyo Hong Kong

Heidelberger Platz 3, D-1000 Berlin 33 · 175 Fifth Ave., New York, NY 10010, USA · 28, Lurke Street, Bedford MK40 3HU, England · 26, rue des Carmes, F-75005 Paris · 37-3, Hongo 3-chome, Bunkyo-ku, Tokyo 113, Japan · Citicorp Centre, Room 1603, 18 Whitfield Road, Causeway Bay, Hong Kong

Springer