

**Zeitschrift:** L'Enseignement Mathématique  
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique  
**Band:** 19 (1973)  
**Heft:** 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** ÉQUATIONS ET VARIÉTÉS ALGÈBRIQUES SUR UN CORPS FINI  
**Autor:** Joly, Jean-René

**Bibliographie**  
**DOI:** <https://doi.org/10.5169/seals-46287>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 28.04.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

variétés algébriques a été établie par Grothendieck (1964, b); voir également Dwork (1966, b). Pour l'application de ce résultat à l'étude des sommes exponentielles, voir notamment Bombieri (1966).

§ 5: les exemples de ce paragraphe sont empruntés essentiellement à Davenport-Hasse (1934) et à Weil (1949). Signalons que le lemme 1 (sect. 5.2) peut aussi se démontrer à l'aide de la proposition 9, (ii) (chap. 5), et du résultat suivant, dû à Stickelberger (1890): si  $\chi$  est un caractère multiplicatif de  $\mathbf{F}_{p^2}$ , et si  $\theta$  est un élément primitif de  $\mathbf{F}_{p^2}/\mathbf{F}_p$ , on a  $\tau(\chi | \beta) = \chi(\theta) p$ , si  $p \neq 2$ , et  $\tau(\chi | \beta) = p$  si  $p = 2$ ; pour une démonstration de ce dernier énoncé, voir aussi Carlitz (1956, a).

Pour  $V = V_1$  et  $q \equiv -1 \pmod{6}$ , ou  $V = V_2^*$  et  $q \equiv -1 \pmod{4}$ , ou  $V = V_3^*$  et  $q \equiv -1 \pmod{3}$ , on a trouvé la même expression

$$Z(V; t) = (1 + qt^2)/(1 - t)(1 - qt);$$

ceci résulte (1) du fait que, dans les trois cas, on a  $N_1 = q + 1$ , et (2) de la relation  $Z(V; t) = (1 + (N_1 - q - 1)t + qt^2)/(1 - t)(1 - qt)$ , valable pour toute courbe  $V$  (projective, non singulière) de genre 1, définie sur  $k$  et ayant  $N_1$  points rationnels sur  $k$  (cette relation se déduit facilement du théorème 3 et du théorème 2, corollaire 1 et remarque). En fait, si deux courbes de genre 1, définies sur  $k$ , ont même nombre  $N_1$  de points rationnels sur  $k$ , alors, elles ont le même nombre  $N_m$  de points rationnels sur  $k_m$  pour tout  $m$ , puisqu'elles ont même fonction zêta (appliquer la formule ci-dessus !): on peut prouver que ceci se produit si et seulement si les deux courbes sont isogènes sur  $k$  (voir [4], p. 242, pour la partie « si », et Tate (1966), pour la partie « seulement si ».)

## BIBLIOGRAPHIE

### 1. Ouvrages généraux, monographies.

- [1] ARTIN, E. *Geometric Algebra*, Interscience Publishers (1957).
- [2] ——— *Algebraic Numbers and Algebraic Functions*, Gordon and Breach (1967).
- [3] BOREVICH, Z. I. and I. R. SHAFAREVICH. *Number Theory*, Academic Press (1966).
- [4] CASSELS, J. W. S. *Diophantine equations with special reference to elliptic curves* (survey article), J. London Math. Soc., 41 (1966), pp. 193-291.
- [5] EICHLER, M. *Introduction to the theory of algebraic numbers and functions*, Academic Press (1966).
- [6] GEL'FAND, A. et I. LINNIK. *Méthodes élémentaires dans la théorie analytique des nombres*, Gauthier-Villars (1965).
- [7] GREENBERG, M. J. *Lectures on forms in many variables*, Benjamin (1969).

- [8] HASSE, H. *Vorlesungen über Zahlentheorie*, Springer (1950).
- [9] LANG, S. *Abelian Varieties*, Interscience Publishers (1959).
- [10] ——— *Algebra*, Addison-Wesley (1965).
- [11] ——— *Algebraic Number Theory*, Addison-Wesley (1970).
- [12] ——— *Introduction to Algebraic Geometry*, Interscience Publishers (1958).
- [13] LEVEQUE, W. J. (editor). *Studies in Number Theory*, MAA Studies, vol. 6 (1969).
- [14] MORDELL, L. J. *Diophantine Equations*, Academic Press (1969).
- [15] SAMUEL, P. *Méthodes d'algèbre abstraite en géométrie algébrique*, Springer (1967).
- [16] SCHILLING, O. F. G. (editor). *Arithmetical Algebraic Geometry*, Harper & Row (1965).
- [17] SERRE, J. P. *Cours d'arithmétique*, Presses Universitaires de France (1970).
- [18] SKOLEM, T. *Diophantische Gleichungen*, Springer (1938).
- [19] WEIL, A. *Basic Number Theory*, Springer (1967).
- [20] ——— *Courbes algébriques et variétés abéliennes*, Hermann (1970).

## 2. Articles, mémoires.

- ARTIN, E. (1924). Quadratische Körper im Gebiet der höheren Kongruenzen, I, II, *Math. Z.*, **19**, pp. 153-206, 207-246.
- AX, J. (1964). Zeroes of polynomials over finite fields, *Amer. J. Math.*, **86**, pp. 255-261.
- (1965, a). A field of cohomological dimension 1 which is not  $(C_1)$ , *Bull. Amer. Math. Soc.*, **71**, p. 717.
- (1965, b). Proof of some conjectures in cohomological dimension, *Proc. Amer. Math. Soc.*, **16**, pp. 1214-1221.
- (1968). The elementary theory of finite fields, *Ann. of Math.*, **88**, pp. 239-271.
- BATEMAN, P. T. and R. M. STEMLER (1962). Waring's problem for algebraic number fields and primes of the form  $(p^r - 1)/(p^d - 1)$ , *Illinois J. Math.*, **6**, pp. 142-156.
- BIRCH, B. J. and H. P. F. SWINNERTON-DYER (1965). Notes on elliptic curves, II, *J. reine angew. Math.*, **218**, pp. 79-108.
- BOMBIERI, E. (1966). On exponential sums in finite fields, *Amer. J. Math.*, **88**, pp. 71-105.
- BOREL, E. (1894). Sur une application d'un théorème de M. Hadamard, *Bull. Sci. Math.*, **18**, pp. 22-25.
- CARLITZ, L. (1953). Invariantive theory of equations in a finite field, *Trans. Amer. Math. Soc.*, **75**, pp. 405-427.
- (1954). Invariant theory of systems of equations in a finite field, *J. Analyse Math.*, **3**, pp. 382-413.
- (1956, a). The number of solutions of a particular equation in a finite field, *Publ. Math. Debrecen*, **4**, pp. 379-383.
- (1956, b). Solvability of certain equations in a finite field, *Quart. J. Math. (Oxford)*, **7**, pp. 3-4.
- CASSELS, J. W. S. (1970). On Kummer sums, *Proc. London Math. Soc.*, **21**, pp. 19-27.
- CHEVALLEY, C. (1935). Démonstration d'une hypothèse de M. Artin, *Abh. Math. Sem. Hamburg*, **11**, pp. 73-75.
- CHOWLA, S. (1961). On the congruence  $\sum a_i x_i^k \equiv 0 \pmod{p}$ , *J. Indian Math. Soc.*, **25**, pp. 47-48.
- H. B. MANN and E. G. STRAUS (1959). On diagonal forms over finite fields, *Norske Vid. Selsk. Forh. (Trondheim)*, **32**, pp. 74-80.
- COHEN, E. (1956). Congruences in algebraic number fields involving sums of similar powers, *Trans. Amer. Math. Soc.*, **83**, pp. 547-556.
- DAVENPORT, H. und H. HASSE (1934). Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, *J. reine angew. Math.*, **172**, pp. 151-182.
- and D. J. LEWIS (1963). Homogeneous additive equations, *Proc. Royal Soc. (London)*, **274**, pp. 443-460.

- DEDEKIND, R. (1857). Abriss einer Theorie der höheren Kongruenzen in Bezug auf einer reellen Primzahl-Modulus, *J. reine angew. Math.*, **54**, pp. 1-26.
- DEMAZURE, M. (1969). Motifs des variétés algébriques, Séminaire Bourbaki, 1969/70, exposé n° 365.
- DEMYANOV, V. B. (1956). Sur la représentation de zéro par des formes du type  $\sum a_i X_i^n$  (en russe), *Dokl. Akad. Nauk SSSR*, **105**, pp. 203-205.
- DEURING, M. (1941). Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hamburg*, **14**, pp. 197-272.
- DICKSON, L. E. (1909). Sets of solutions of  $x^e + y^e + z^e \equiv 0 \pmod{p}$ , *J. reine angew. Math.*, **135**, pp. 181-188.
- DWORK, B. (1960). On the rationality of the zeta function of an algebraic variety, *Amer. J. Math.*, **82**, pp. 631-648.
- (1962). On the zeta function of a hypersurface, I, Inst. Hautes Etudes Sci., *Publ. Math.* n° 12, pp. 5-68.
- (1964). On the zeta function of a hypersurface, II, *Ann. of Math.*, **80**, pp. 227-299.
- (1966, a). On the zeta function of a hypersurface, III, *Ann. of Math.*, **83**, pp. 457-519.
- (1966, b). On the rationality of the zeta functions and  $L$  series, Proceedings of a Conference on Local Fields (Driebergen, 1966), Springer Verlag (1967).
- EULER, L. (1760). Demonstratio circa residua ex divisione potestatum per numeros primos resultantia, *Novi Comm. Acad. Petrop.*, 1760, pp. 74-104.
- FATOU, P. (1906). Etude de la série de Taylor sur son cercle de convergence, *Acta Math.*, **30**, pp. 364-400.
- GALOIS, E. (1830). Sur la théorie des nombres, *Bull. Sci. Math. Férussac*, XIII, § 218.
- GRAY, J. F. (1960). Diagonal forms of odd degree over a finite field, *Michigan Math. J.*, **7**, pp. 297-301.
- GROTHENDIECK, A. (1964, a). Cohomologie  $l$ -adique et fonctions  $L$ , Séminaire de Géométrie Algébrique, 1964/65, Inst. Hautes Etudes Sci., Bures-sur-Yvette.
- (1964, b). Formule de Lefschetz et rationalité des fonctions  $L$ , Séminaire Bourbaki, 1964/65, exposé n° 279.
- HARDY, G. H. and J. E. LITTLEWOOD (1922). Some problems of Partitio Numerorum, IV, *Math. Z.*, **12**, pp. 161-188.
- HASSE, H. (1933). Beweis des Analogons der Riemannschen Vermutung..., *Nachr. Ges. Wiss. Göttingen, Math. Phys. Kl.*, 1933, pp. 253-262.
- (1934). Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörper, *Abh. Math. Sem. Hamburg*, **10**, pp. 325-348.
- (1936). Zur Theorie der abstrakten elliptischen Funktionenkörper, I, II, III, *J. reine angew. Math.*, **175**, pp. 55-62, 69-88, 193-208.
- HUA, L. K. and H. S. VANDIVER (1948). On the existence of solutions of certain equations in finite fields, *Proc. Nat. Acad. Sci. USA*, **34**, pp. 258-263.
- (1949, a). Characters over certain types of rings, with applications to the theory of equations in a finite field, *Proc. Nat. Acad. Sci. USA*, **35**, pp. 94-99.
- (1949, b). On the nature of the solutions of certain equations in a finite field, *Proc. Nat. Acad. Sci. USA*, **35**, pp. 481-487.
- HURWITZ, A. (1909). Über die Kongruenz  $ax^e + by^e + cz^e \equiv 0 \pmod{p}$ , *J. reine angew. Math.*, **136**, pp. 272-292.
- IGUSA, J. (1949). On the theory of algebraic correspondences and its application to the Riemann hypothesis in function fields, *J. Math. Soc. Japan*, **1**, pp. 147-201.
- JACOBSTHAL, E. (1907). Über die Darstellung der Primzahlen der Form  $4n + 1$  als Summe zweier Quadrate, *J. reine angew. Math.*, **132**, pp. 238-245.
- JOLY, J. R. (1968). Sommes de puissances  $m$ -ièmes dans les anneaux  $P$ -adiques et les anneaux d'entiers algébriques, *Enseign. Math.*, **14**, pp. 197-204.

- (1971). Nombre de solutions de certaines équations diagonales sur un corps fini, *C. R. Acad. Sci. Paris*, **272**, pp. 1549-1552.
- KATZ, N. M. (1971). On a theorem of Ax, *Amer. J. Math.*, **93**, pp. 485-499.
- (1972). Travaux de Dwork, Séminaire Bourbaki, 1971/72, exposé n° 409.
- LANG, S. (1952). On quasi-algebraic closure, *Ann. of Math.*, **55**, pp. 373-390.
- (1956). Algebraic groups over finite fields, *Amer. J. Math.*, **78**, pp. 555-563.
- and A. WEIL (1954). Number of points of varieties in finite fields, *Amer. J. Math.*, **76**, pp. 819-827.
- LEBESGUE, V. A. (1837). Recherches sur les nombres, I, *J. Math. Pures Appl.*, **2**, pp. 253-292.
- (1838). Recherches sur les nombres, II, III, *J. Math. Pures Appl.*, **3**, pp. 113-131, 132-144.
- LEWIS, D. J. (1960). Diagonal forms over finite fields, *Norske Vid. Selsk. Forh. (Trondheim)*, **33**, pp. 61-65.
- LIBRI, G. (1832). Mémoire sur la théorie des nombres, *J. reine angew. Math.*, **9**, pp. 261-276.
- LUBKIN, S. (1967). On a conjecture of A. Weil, *Amer. J. Math.*, **89**, pp. 443-548.
- (1968). A  $p$ -adic proof of Weil's conjectures, *Ann. of Math.*, **87**, pp. 105-255.
- MANIN, I. (1956). Sur les congruences cubiques selon un module premier (en russe), *Izv. Akad. Nauk SSSR*, **20**, pp. 673-678.
- MORDELL, L. J. (1922). Three lectures on Fermat's last theorem, London Univ. Press.
- MORLAYE, B. (1971). Equations diagonales non homogènes sur un corps fini, *C. R. Acad. Sci. Paris*, **272**, pp. 1545-1548.
- (1972). Démonstration élémentaire d'un théorème de Davenport et Hasse, *Enseign. Math.*, à paraître.
- NAGATA, M. (1957). Note on a paper of Lang concerning quasi-algebraic closure, *Mem. Univ. Kyoto*, **30**, pp. 237-241.
- NISNEVICH, L. (1954). Sur le nombre de points d'une variété algébrique sur un corps fini premier (en russe), *Dokl. Akad. Nauk SSSR*, **99**, pp. 17-20.
- PORTER, A. D. (1966). Special equations in a finite field, *Math. Nachr.*, **32**, pp. 277-279.
- RAJWADE, A. R. (1970). A note on the number  $N_p$  of solutions of the congruence  $y^2 \equiv x^3 - Dx \pmod{p}$ , *Proc. Cambridge Philos. Soc.*, **67**, pp. 603-605.
- REDEI, L. (1846). Zur Theorie der Gleichungen in endlichen Körpern, *Acta Univ. Szeged*, **11**, pp. 63-70.
- ROQUETTE, P. (1953). Arithmétique Beweis der Riemannschen Vermutung, *J. reine angew. Math.*, **191**, pp. 199-252.
- SAMUEL, P. (1967). Courbes algébriques, *Enseign. Math.*, **13**, pp. 305-311.
- SCHMIDT, F. K. (1931). Analytische Zahlentheorie in Körpern der Charakteristik  $p$ , *Math. Z.*, **33**, pp. 1-32.
- SCHUR, I. (1916). Über die Kongruenz  $ax^e + by^e + cz^e \equiv 0 \pmod{p}$ , *Jahresbericht DMW*, **25**, pp. 114-120.
- SCHWARZ, S. (1948, a). On Waring's problem for finite fields, *Quart. J. Math. (Oxford)*, **19**, pp. 123-128.
- (1948, b). On the equation  $a_1x_1^k + a_2x_2^k + \dots + a_kx_k^k = 0$  in finite fields, *Quart. J. Math. (Oxford)*, **19**, pp. 160-163.
- (1950). On universal forms in finite fields, *Casopis Pest. Mat. Fys.*, **75**, pp. 45-50.
- (1956). On a type of universal forms in discretely normed fields, *Acta Univ. Szeged*, **17**, pp. 5-19.
- SERRE, J. P. (1959). Rationalité des fonctions  $\zeta$  des variétés algébriques (d'après Dwork), Séminaire Bourbaki, 1959/60, exposé n° 198.
- STICKELBERGER, L. (1890). Über eine Verallgemeinerung von der Kreistheilung, *Math. Annalen*, **37**, pp. 321-367.
- TATE, J. (1966). Endomorphisms of abelian varieties over finite fields, *Inventiones Math.*, **2**, pp. 134-144.

- TERJANIAN, G. (1966). Sur les corps finis, *C. R. Acad. Sci. Paris*, **262**, pp. 167-169.
- (1972). Dimension arithmétique d'un corps, à paraître.
- TIETÄVÄINEN, A. (1968). On diagonal forms over finite fields, *Ann. Univ. Turku, Ser. A I*, n° 118, 10 p.
- TORNHEIM, L. (1938). Sums of  $n$ -th powers in fields of prime characteristic, *Duke Math. J.*, **4**, pp. 359-362.
- TSEN, C. C. (1933). Divisionsalgebren über Funktionenkörpern, *Nachr. Ges. Wiss. Göttingen*, 1933, pp. 335-339.
- WARNING, E. (1935). Bemerkung zur vorstehenden Arbeit von Herrn Chevalley, *Abh. Math. Sem. Hamburg*, **11**, pp. 76-83.
- WATERHOUSE, W. C. (1969). Abelian varieties over finite fields, *Ann. Sci. Ec. Norm. Sup., Sér. 4*, **2**, pp. 521-560.
- (MACLAGLAN-) WEDDERBURN, J. H. (1905). A theorem on finite algebras, *Trans. Amer. Math. Soc.*, **6**, pp. 349-352.
- WEIL, A. (1940). Sur les corps de fonctions algébriques à corps de constantes fini, *C. R. Acad. Sci. Paris*, **210**, pp. 592-594.
- (1948, a). Sur les courbes algébriques et les variétés qui s'en déduisent, *Actual. Sci. Ind.*, n° 1041, Hermann, Paris (= [20], 1<sup>re</sup> partie).
- (1948, b). On some exponential sums, *Proc. Nat. Acad. Sci. USA*, **34**, pp. 204-207.
- (1949). Number of solutions of equations in finite fields, *Bull. Amer. Math. Soc.*, **55**, pp. 497-504.
- (1954). Abstract versus classical algebraic geometry. *Proc. Intern. Cong. Math.* (Amsterdam), vol. III, pp. 550-558.
- WITT, E. (1931). Über die Kommutativität endlicher Schiefkörper, *Abh. Math. Sem. Hamburg*, **8**, p. 413.
- YAMAMOTO, K. (1959). The Artin-Hasse-Shafarevich function, *Japan J. Math.*, **29**, pp. 165-172.

( Reçu le 25 septembre 1972 )

Jean-René Joly

Université Scientifique et Médicale de Grenoble  
Institut de Mathématiques Pures  
B. P. 116  
F-38 — Saint Martin d'Hères

**Vide-leer-empty**