Introduction

ÉQUATIONS ET VARIÉTÉS ALGÉBRIQUES SUR UN CORPS FINI

par Jean-René JOLY

INTRODUCTION

Cet article passe en revue les propriétés diophantiennes classiques des corps finis. Ces propriétés peuvent se grouper en quatre catégories:

(1) Le théorème de Chevalley, et ses variantes ou améliorations: théorèmes de Chevalley-Warning, Warning, Ax, Katz, Terjanian, ... Indiquons (ou rappelons) que le théorème de Chevalley (pour *un* polynôme à n variables $F(X_1, ..., X_n)$ sur un corps fini k) est l'énoncé suivant: si F est sans terme constant, et si $\deg(F) < n$, alors l'équation $F(X_1, ..., X_n) = 0$ admet sur k une solution autre que la solution « triviale » $(0, 0, ..., 0)$. Ces divers théorèmes sont étudiés aux chapitres 3 et 7.

(2) Les résultats de Hasse, Weil, Lang-Weil, Nisnevich, ..., concernant l'« hypothèse de Riemann » en caractéristique p. Le théorème de Lang-Weil, par exemple, peut s'énoncer grosso modo de la façon suivante: si V est une variété absolument irréductible de dimension r définie sur un corps fini k à q éléments, le nombre de points de V rationnels sur k est voisin de q^r, avec un « terme d'erreur » de l'ordre de grandeur de $q^{r-(1/2)}$. Les propriétés de ce type sont étudiées au chapitre 8.

(3) Les résultats relatifs aux fonctions zêta des variétés algébriques sut un corps fini, et notamment le théorème de rationalité de Dwork: si V esf une variété algébrique définie sur un corps fini k; si, pour tout entier positi- m, N_m désigne le nombre de points de V rationnels sur k_m (l'unique extenr sion de degré m de k); et si t désigne une variable, alors il existe une fraction rationnelle en t, à coefficients rationnels, soit $Z(V; t)$ (c'est la « fonction zêta » de V), telle qu'on ait $\sum_{m \geqq 1} N_m t^m/m = \log Z(V; t)$; la connaissance de la famille *finie* des coefficients de $Z(V; t)$ est alors équivalente à celle de la suite *infinie* $(N_m)_{m \geqq 1}$. Les propriétés des fonctions zêta sont exposées au chapitre 9.

(4) Enfin, les résultats spécifiques relatifs aux équations diagonales, c'est-à-dire aux équations de la forme $a_1 X_1^{d1} + \ldots + a_n X_n^{dn} = b$. L'étude de ces équations (sur un corps fini, spécialement sur un corps de restes modulo p) est traditionnelle, et remonte à Gauss et Jacobi. Les équations diagonales se prêtent à un calcul exact du nombre de leurs solutions, et ont été utilisées de ce fait (notamment par Davenport-Hasse et Weil) pour vérifier sur des cas particuliers, et avant leur démonstration par Dwork et Weil, la rationalité des fonctions zêta et l'hypothèse de Riemann; elles ont permis plus généralement d'étayer les « conjectures de Weil » relatives à la forme exacte des fonctions zêta. Les équations diagonales sont étudiées aux chapitres 4 et 6.

Naturellement, ces diverses catégories de résultats ne sont pas indépendantes: en particulier, les contenus des chapitres 8 et 9 sont étroitement liés, et ce découpage en deux chapitres n'a été pratiqué que pour la commodité de l'exposition. Indiquons d'autre part que les chapitres 1, 2 et 5, non mentionnés ci-dessus, sont consacrés respectivement à un rappel des propriétés générales des corps finis, à l'étude des polynômes sur un corps fini, et à l'étude des sommes de Gauss et de Jacobi attachées à un corps fini. Voir d'ailleurs la table des matières.

* * *

Les chapitres 1 à 6 de cet article sont tout à fait élémentaires, et ne supposent connus que les rudiments de la théorie des groupes finis et de la théorie des corps: ce qui est largement couvert par les chapitres II, IV, V et VII du Van der Waerden, par exemple; le chapitre 7 utilise (mais avec tous les rappels nécessaires) quelques propriétés très simples des corps cyclotomiques. Les chapitres 8 et 9 sont plus techniques, et supposent connu un minimum de géométrie algébrique: toutefois, le langage employé étant le langage classique des variétés affines ou projectives, l'intuition devrait pouvoir suppléer le plus souvent à d'éventuelles lacunes en ce domaine. Ainsi, la quasi totalité des neuf chapitres est en principe accessible à tout lecteur (et notamment à tout débutant en théorie des nombres) ayant un niveau équivalent au deuxième cycle des universités françaises. Cet article a d'ailleurs pour origine lointaine un cours de première année de troisième cycle: « propriétés diophantiennes des corps finis », Grenoble, novembre/décembre 1969.

* * *

Les notations employées sont celles de Bourbaki, ou, plus simplement, celles de l'« Algebra » de Lang; rappelons seulement que **Z**, **Q**, **R**, **C**, $\mathbf{F}_p$ désignent respectivement l'anneau des entiers rationnels, le corps des nombres rationnels, celui des nombres réels, celui des nombres complexes, celui des restes modulo p; et que, si a et b sont deux entiers non nuls, (a, b) représente leur p.g.c.d.

La bibliographie (en fin d'article) comporte deux parties: la première est la liste des ouvrages généraux auxquels il est fait référence dans le texte (par numéro entre crochets); la seconde est la liste des articles cités, qui sont classés (et auxquels il est fait référence) par nom(s) d'auteur(s) et année de publication. La première liste mentionne plusieurs monographies relatives aux « vraies » équations diophantiennes (sur les corps locaux et globaux): [**4**], [**14**], [**18**], ainsi que [**3**] (chap. 1, 2 et 4), [**7**] (chap. 7) et [**13**] (chap. 1 et 2): pour l'application à ces équations des résultats examinés dans le présent article, voir [**4**], 1re partie (notamment pp. 204-205), [**13**], chap. 2 (notamment p. 29), et aussi [**3**], chap. 1, sect. 5 et 6.

TABLE DES MATIÈRES