Variétés algébriques et corps de fonctions sur un corps fini

Yves Aubry

Université de la Méditerranée

Aix-Marseille II - Faculté des Sciences de Luminy

Habilitation à Diriger des Recherches

Discipline : Mathématiques

Variétés algébriques et corps de fonctions sur un corps fini

Yves Aubry

Soutenue le 13 décembre 2002

Membres du Jury

Gerhard Frey (Rapporteur)

Gerard van der Geer (Rapporteur)

Gilles Lachaud

Eric Reyssat

Philippe Satgé

Mikhaïl Tsfasman

Serge Vlăduţ (Rapporteur)

Remerciements

Je profite de l'opportunité qui m'est donnée à l'occasion de cette habilitation pour rendre hommage à Gilles Lachaud pour ses qualités scientifiques et humaines et pour lui dire le grand plaisir que j'ai eu à évoluer dans son équipe "Arithmétique et Théorie de l'Information" du C.N.R.S..

Gerhard Frey, Gerard van der Geer et Serge Vlăduţ m'ont fait le grand honneur d'accepter le rôle de rapporteur : je les en remercie vivement.

Mes remerciements vont également à Mikhaïl Tsfasman qui me gratifie de sa présence dans mon jury.

J'ai beaucoup appris dans le séminaire-groupe de travail de Géométrie Algébrique de l'Université de Caen animé avec brio par Philippe Satgé : je lui en suis très reconnaissant et suis ravi qu'il siège parmi mon jury.

J'ai également profité de la grande qualité scientifique du séminaire de Théorie des Nombres de l'Université de Caen, et notamment de celle d'Eric Reyssat que j'ai eu le privilège de cotoyer : je suis heureux de le compter parmi les membres de mon jury.

Pour les nombreuses discussions que j'ai pu avoir avec Yves Hellegouarch, John Boxall et Jean Cougnard, je leur adresse mes sincères salutations, et à travers eux, je tiens à dire toute l'estime que je porte aux mathématiciens de l'Université de Caen que j'ai cotoyés au laboratoire "Structures Discrètes et Analyse Diophantienne" et maintenant au "Laboratoire de Mathématiques Nicolas Oresme".

J'ai bénéficié de l'influence scientifique stimulante de Stéphane Louboutin avec qui, quotidiennement, nous avons échangé nos points de vue : je lui en sais gré.

Je n'oublie pas les nombreux échanges que j'ai pu avoir avec Michel Laurent, Robert Rolland et François Rodier et c'est l'ensemble de l'Institut de Mathématiques de Luminy à Marseille que je remercie de m'avoir accueilli en son sein lors de ma délégation C.N.R.S..

Je remercie également Dominique Le Brigand, un de mes co-auteur, notamment pour l'accueil qu'elle a su m'offrir lors de mon séjour parisien.

Je terminerais ces remerciements par mon second co-auteur, Marc Perret, à qui je voudrais dire tout le bien que je pense de lui.

Table des matières

Introduction

Les variétés algébriques sur un corps fini apparaissent de façon naturelle dans bien des situations. Par exemple lors de la résolution d'équations diophantiennes, où l'existence de solutions modulo un nombre premier est une condition nécessaire à celle de solutions entières. Elles apparaissent également directement dans la construction de différents objets de Mathématiques discrètes ou de géométrie finie.

André Weil a formulé des conjectures concernant leur fonction zêta (rationalité, équation fonctionnelle, Hypothèse de Riemann), qu'il a lui-même démontrées dans le cas des courbes et des variétés abéliennes et qui le furent par la suite par Pierre Deligne dans le cas général. Elles concernent le nombre de points rationnels de ces variétés qui forme le cœur de nos recherches en Géométrie Algébrique.

Les corps de fonctions à une variable sur un corps fini représentent la facette Arithmétique des courbes sur un corps fini. Etudiés par Emil Artin dans sa thèse, ils admettent, comme les corps de nombres, des anneaux d'entiers (relatifs à un ensemble fini de places) et des groupes de classes d'idéaux fractionnaires. Ils constituent l'objet de nos recherches en Théorie des Nombres.

Voici en quelques lignes un survol chronologique de nos travaux. Ils seront détaillés, peu ou prou, dans les chapitres suivants.

Nous nous sommes tout d'abord intéressés au nombre de points rationnels sur un corps fini des hypersurfaces quadriques (pouvant être dégénérées) et plus particulièrement à leurs sections hyperplanes ainsi qu'à leurs intersections entre elles (voir [1]) ; ceci s'appliquant à la détermination des paramètres de codes correcteurs d'erreurs associés à ces variétés.

La construction par Goppa de codes géométriques algébriques à partir d'une courbe algébrique a permis d'établir un résultat théorique remarquable en théorie des Codes. Nous avons donné une construction de codes géométriques algébriques à partir d'une surface algébrique, et donné des estimations de ses paramètres fondamentaux (voir [2]).

Lesquels paramètres sont intimement liés à des nombres de points rationnels d'intersections de variétés projectives. Dans le cas où celles-ci sont des courbes, elles n'ont aucune raison *a priori* d'être lisses ou irréductibles.

C'est pourquoi, par la suite, nous avons étudié les courbes singulières, et, avec la collaboration de Marc Perret, nous avons généralisé la borne de Weil portant sur l'estimation du nombre de points rationnels sur un corps fini d'une courbe algébrique projective absolument irréductible lisse au cas de telles courbes non nécessairement lisses (voir [3]).

Nous avons ensuite établi, toujours avec Marc Perret, un résultat généralisant à la fois celui de [3] et celui connu dans le cas lisse, portant sur la différence des nombres de points rationnels dans un revêtements de courbes non nécessairement lisses (voir [4]).

Nous nous sommes alors tournés vers les corps de fonctions à une variable

sur un corps fini. Nous avons établi un théorème de finitude en ce qui concerne les extensions totalement imaginaires d'extensions totalement réelles de corps de fonctions dont le nombre de classes d'idéaux du corps imaginaire est fixé (voir [5]).

Dans le cas où ces extensions sont quadratiques, nous donnons une formule du nombre de classes relatif en terme de fonction L, ainsi qu'une formule liant cette fonction L à une somme de caractères de type Legendre dans le cas du nombre de classe 1 (voir [6]).

Si l'on suppose de plus que le groupe de Galois d'une telle extension est isomorphe au groupe de Klein, via la théorie du corps de classes ainsi que des factorisations de fonctions zêta et des estimations de régulateurs, nous déterminons ces corps en caractéristique impaire (voir [7]) ainsi qu'en caractéristique paire, cette fois en collaboration avec Dominique Le Brigand, via les extensions d'Artin-Schreier et des calculs de nombres de points de jacobiennes (voir [8]).

A l'issu de ce travail, nous nous sommes à nouveau penchés sur le comportement des fonctions zêta des courbes dans un revêtement (plat) de courbes algébriques projectives absolument irréductibles. Nous avons montré, à nouveau avec Marc Perret, la divisibilité de ces fonctions zêta dans la situation précédente (voir [9]) ainsi que dans le cas plus général de courbes supposées seulement connexes (voir [10]), que l'on peut interpréter comme un analogue de la conjecture d'holomorphie d'Artin sur les fonctions zêta de Dedekind des corps de nombres. Nous avons ensuite déterminé explicitement les polynômes caractéristiques de l'endomorphisme de Frobenius sur les groupes de cohomologie étale ℓ-adiques de courbes projectives connexes, qui, combinée à une forme plus générale que la divisibilité de [10], permet de donner une estimation de la différence du nombre de points rationnels dans un revêtement de courbes connexes (voir [11]).

Les résultats jusqu'au paragraphe 1.3.2. correspondent à ma première thèse et seront donc développés de manière très succinte.

1 Nombre de points des variétés algébriques

1.1 Quadriques

Nous nous sommes intéressé dans [1] au nombre de points des hypersurfaces quadriques projectives dégénérées, puis à celui de leurs sections hyperplanes et enfin à celui de l'intersection de deux quadriques (ce dernier résultat a d'ailleurs été amélioré depuis par D. Leep et L. Schueller ("Zeros of a pair of quadratic forms defined over a finite field", Finite Fields Appl. 5 (1999), no. 2, 157-176)). Ces estimations de nombre de points nous permettaient d'estimer les paramètres fondamentaux de codes de Reed-Muller projectifs généralisés construits sur les quadriques.

1.2 Surfaces algébriques

La construction par Goppa de codes géométriques algébriques à partir de courbes a permis d'établir l'existence de familles de codes dépassant la fameuse borne de Varshamov-Gilbert (Y. Ihara : "Some remarks on the number of rational points of algebraic curves over finite fields", J. Fac. Sci. Univ. Tokyo Sect. IA Math 28 (1981), no. 3, 721–724 (1982) et M. Tsfasman, S. Vladut, Th. Zink : "Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound", Math. Nachr. 109 (1982), 21-28). Nous proposons dans [2] une construction de codes géométriques algébriques sur des variétés de dimension quelconque à partir également d'espaces $L(D)$ pour un diviseur sur notre variété. Cette construction redonne celle de Goppa dans le cas où la variété est une courbe. Nous nous intéressons alors au cas des surfaces et plus particulièrement à celui des surfaces réglées.

Depuis, et, dans le même esprit, S. Hansen a proposé également une construction de codes sur des variétés de dimension > 1 et estimé leurs paramètres (cf "Error-correcting codes from higher-dimensional varieties", Finite Fields Appl. 7, (2001), no. 4, 531-552).

1.3 Nombre de points des courbes et fonctions zêta

1.3.1 Courbes non lisses

En 1948, André Weil a montré que (cf A. Weil : "Sur les courbes algébriques et les variétés qui s'en déduisent", Hermann, Paris 1948) si X est une courbe algébrique projective définie sur un corps fini $k = \mathbf{F}_q$, absolument irréductible et lisse, alors son nombre de points rationnels sur k vérifie :

$$\mid \sharp X(\mathbf{F}_q) - (q+1) \mid \leq 2g\sqrt{q} \tag{1}$$

où g est son genre géométrique.

Dans [3], nous nous affranchissons de l'hypothèse de lissité et donnons la forme de la fonction zêta d'une telle courbe éventuellement singulière. On en déduit en particulier le théorème suivant :

Théorème 1 *Soit X une courbe algébrique projective absolument irréductible définie sur le corps fini $k = \mathbf{F}_q$. Alors*

$$| \sharp X(\mathbf{F}_q) - (q+1) | \leq 2g\sqrt{q} + \Delta_X \leq 2g\sqrt{q} + \pi - g \leq 2\pi\sqrt{q},$$

où π est le genre arithmétique de X, où $\Delta_X = \sharp\widetilde{X}(\overline{k}) - \sharp X(\overline{k})$ et où $\widetilde{X}$ est la normalisée de X.

Dans le cas particulier d'une courbe plane de degré d, son genre arithmétique étant $\frac{(d-1)(d-2)}{2}$, on trouve alors $(d-1)(d-2)\sqrt{q}$ pour majorant. Cette dernière borne concernant les courbes planes a été également établie, simultanément et indépendamment par D. Leep et C. Yoemans dans "The number of points on a singular curve over a finite field", Arch. Math., 63, (1994), 420-426. Par la suite, E. Bach a également publié essentiellement le même résultat dans "Weil bounds for singular curves", Appl. Algebra Engrg. Comm. Comput., 7, (1996), no. 4, 289-298.

Afin d'étudier l'aspect asymptotique du nombre de points des courbes, Y. Ihara a introduit la quantité suivante : $A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}$, avec $N_q(g) = \max_X \sharp X(\mathbf{F}_q)$ où X décrit l'ensemble des courbes (algébriques projectives absolument irréductibles) lisses définies sur $\mathbf{F}_q$ de genre (géométrique) g. Il en a donné (pour q carré), ainsi que J.-P. Serre (pour q quelconque), des minorations. D'autre part, V. G. Drinfeld et S. Vladut (cf "Sur le nombre de points d'une courbe algébrique", Anal. Fonct. Appl. 17 (1983), 68-69) ont donné la majoration suivante : $A(q) \leq \sqrt{q} - 1$, pour tout q. Nous introduisons dans [3] un analogue de cette quantité. On définit $A'(q)$ par :

$$A'(q) = \limsup_{\pi\to\infty} \frac{N_q(\pi)}{\pi}$$

avec $N_q(\pi) = \max_X \sharp X(\mathbf{F}_q)$ où X décrit l'ensemble des courbes (algébriques projectives absolument irréductibles) non nécessairement lisses définies sur $\mathbf{F}_q$ de genre arithmétique π. On a trivialement $A(q) \leq A'(q)$ et nos résultats entraînent que $A'(q) \leq A(q) + 1$. On démontre dans [3] que l'on a également :

Proposition 2 *Pour tout q :*

$$A'(q) \leq \sqrt{q} - 1.$$

Ce résultat a été également publié (avec une preuve ne marchant pas dans le cas général, voir le rapport de Constantin Manoil dans Math. Reviews) ultérieurement par Galindo Zúniga dans "Number of rational points of a singular curve", Proc. Amer. Math. Soc. 126 (1998), no. 9, 2549-2556.

Une question reste ouverte : a-t-on $A'(q) = A(q)$?

1.3.2 Revêtements plats

La borne de Weil (1) peut s'interpréter de la façon suivante. Tout courbe est un revêtement (morphisme fini) de la droite projective $\mathbf{P}^1$. Celle-ci admet $q+1$ points rationnels sur $\mathbf{F}_q$ et est de genre zéro. La borne de Weil se réécrit donc :

$$| \sharp X(\mathbf{F}_q) - \sharp \mathbf{P}^1(\mathbf{F}_q) | \leq 2(\pi_X - \pi_{\mathbf{P}^1})\sqrt{q}.$$

Nous montrons dans [4] que cette borne se généralise à tout revêtement plat :

Théorème 3 *Soit $f : Y \longrightarrow X$ un morphisme fini et plat entre deux courbes algébriques projectives absolument irréductibles X et Y définies sur $\mathbf{F}_q$, de genres arithmétiques respectifs π_X et π_Y. Alors :*

$$| \sharp Y(\mathbf{F}_q) - \sharp X(\mathbf{F}_q) | \leq 2(\pi_Y - \pi_X)\sqrt{q}.$$

Le résultat généralise celui de Gilles Lachaud concernant les extensions d'Artin-Schreier (cf "Artin-Schreier curves, exponentiel sums and the Carlitz-Uchiyama bound for geometric codes", J. Numb. Th. 39, 18-40 (1991)) ainsi que celui de Marc Perret concernant les extensions de Kummer (cf "Multiplicative character sums and Kummer coverings", Acta Arithmetica, LIX. 3, 279-290 (1991)). Remarquons qu'il est faux sans hypothèse sur le morphisme comme le montre l'exemple du morphisme de normalisation d'une courbe à singularité nodale.

1.3.3 Polynômes caractéristiques du Frobenius

Si X est une variété définie sur un corps fini k, on définit sa fonction zêta, notée $Z_{k,X}(T)$ ou plus simplement $Z_X(T)$, par :

$$Z_X(T) = \exp\left(\sum_{n=1}^{\infty} \sharp X(k_n)\frac{T^n}{n}\right),$$

où k_n désigne l'extension de degré n de k. La formule de Grothendieck-Lefschetz donne une interprétation de cette fonction zêta en termes des polynômes (réciproques des polynômes) caractéristiques de l'endomorphisme de Frobenius F induit sur les groupes de cohomologie étale ℓ-adique à support compact de $\overline{X} = X \times_k \overline{k}$ (où $\overline{k}$ est une clôture algébrique de k et ℓ un nombre premier différent de sa caractéristique) :

$$Z_X(T) = \frac{\det(1 - FT \mid H_c^1(\overline{X}, \mathbf{Q}_\ell))}{\det(1 - FT \mid H_c^0(\overline{X}, \mathbf{Q}_\ell))\ \det(1 - FT \mid H_c^2(\overline{X}, \mathbf{Q}_\ell))}.$$

Si X est une variété sur un corps k, nous noterons $|X|$ l'ensemble de ses points fermés, $k(P)$ le corps résiduel d'un point $P \in |X|$, $d_P = [k(P) : k]$ le degré de P sur k et $\nu_X : \widetilde{X} \longrightarrow X$ le morphisme de normalisation de X. Pour simplifier, nous noterons $H^i(X)$ le groupe $H_c^i(\overline{X}, \mathbf{Q}_\ell)$ et $P_{k,H^i(X)}(T)$ le polynôme $\det(1 - FT \mid H_c^i(\overline{X}, \mathbf{Q}_\ell))$. Le corps k sera le corps fini à q éléments.

La conjecture d'holomorphie d'Artin, prouvée indépendamment par Aramata et Brauer dans le cas galoisien, prédit que, pour toute extension de corps de nombres, le quotient de leurs fonctions zêta de Dedekind est une fonction

entière. Par analogie, on peut se demander si, pour tout morphisme surjectif fini $f : Y \longrightarrow X$ entre deux variétés algébriques projectives définies sur un corps fini k, le polynômes $P_{k,H^i(X)}(T)$ divise $P_{k,H^i(Y)}(T)$. Lorsque Y et X sont des variétés lisses, c'est un résultat de Kleiman (S. L. Kleiman : "Algebraic cycles and the Weil conjectures", Dix exposés sur la cohomologie des schémas, North-Holland, Amsterdam (1968), 359-386.). Lorsque X et Y sont des courbes lisses, en voici une démonstration (voir [9]) :

Proposition 4 *Si $f : Y \longrightarrow X$ est un morphisme fini entre deux courbes algébriques projectives absolument irréductibles et lisses X et Y définies sur un corps fini k, alors $P_{k,H^1(X)}(T)$ divise $P_{k,H^1(Y)}(T)$ dans $\mathbf{Z}[T]$.*

Démonstration. Pour tout ℓ distinct de la caractéristique de k, considérons le $\mathbf{Q}_\ell$-espace vectoriel $T_\ell(J_X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ de dimension $2g_X$, où $T_\ell(J_X)$ est le module de Tate de la jacobienne J_X de X et g_X le genre (géométrique) de X. Le polynôme $P_{k,H^1(X)}(T)$ n'est rien d'autre que le polynôme (réciproque du polynôme) caractéristique de l'endomorphisme de Frobenius sur $T_\ell(J_X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. L'application $f^* : J_X \longrightarrow J_Y$ induite par f sur les jacobiennes a un noyau fini et envoie les points de ℓ^n-torsion de J_X sur ceux de J_Y. En tensorisant par $\mathbf{Q}_\ell$, on obtient alors un morphisme injectif de $\mathbf{Q}_\ell$-espaces vectoriels

$$T_\ell(J_X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell \stackrel{f^* \otimes 1}{\longrightarrow} T_\ell(J_Y) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell.$$

Le morphisme de Frobenius sur $T_\ell(J_Y) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ laisse fixe le sous-espace $T_\ell(J_X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$, donc son polynôme caractéristique sur celui-ci divise son polynôme caractéristique sur celui-là dans $\mathbf{Q}_\ell[T]$, donc dans $\mathbf{Z}[T]$ puisque ces polynômes sont à coefficients entiers et ont un terme constant égal à 1. □

Dans [9], nous montrons le résultat de manière élémentaire sans l'hypothèse de lissité :

Théorème 5 *La proposition 4 est encore vraie sans supposer la lissité des courbes.*

Ce résultat admet un corollaire en ce qui concerne les variétés semi-abéliennes. Introduisons tout d'abord certaines choses.

On a montré dans [3] que, pour une courbe X algébrique projective absolument irréductible et définie sur k, le polynôme $P_{k,H^1(X)}(T)$ s'écrivait

$$P_{k,H^1(X)}(T) = P_{k,H^1(\tilde{X})}(T) P_{X/\tilde{X}}(T)$$

où $P_{X/\tilde{X}}$ est un polynôme dont les racines sont de module 1 (i.e. de poids zéro dans la terminologie de Deligne (cf P. Deligne : "La conjecture de Weil, II", Publ. Math. IHES, **52** (1980), 137-252)).

On note J_X la jacobienne de X. On a la suite exacte de schémas en groupes commutatifs connexes lisses sur k (cf S. Bosch, W. Lütkebohmert and M. Raynaud : "Néron Models", Springer-Verlag Ergebnisse der Math. **21** (1990)) :

$$0 \longrightarrow L_X \longrightarrow J_X \longrightarrow J_{\tilde{X}} \longrightarrow 0 \qquad (*)$$

où L_X est un groupe algébrique linéaire connexe lisse qui peut s'écrire $L_X = U_X \times T_X$ avec U_X un groupe unipotent et T_X un tore.

Puisque $\tilde{X}$ est lisse et propre sur k, $J_{\tilde{X}}$ est une variété abélienne et donc la jacobienne J_X est une variété semi-abélienne i.e. une extension d'une variété abélienne par un groupe linéaire. Nous montrons alors (cf [9]) que pour tout ℓ différent de la caractéristique de k,

$$P_{k,H^1(X)}(T) = \det(1 - TF \mid T_\ell(J_X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell)$$

On en déduit que (cf [9]) :

$$P_{X/\tilde{X}}(T) = \det(1 - TF \mid T_\ell(T_X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell)$$

On a alors le résultat suivant :

Proposition 6 *Soit*

$$f : Y \longrightarrow X$$

un morphisme fini plat entre courbes algébriques projectives réduites absolument irréductibles sur un corps fini k. Alors la jacobienne J_X de X est k-isogène à une sous-variété semi-abélienne définie sur k de la jacobienne J_Y de Y.

Démonstration. Une extension d'une variété abélienne par le group multiplicatif $\mathbf{G}_m$ est paramétrisé par un point du dual de la variété abélienne (voir J.-P. Serre : "Groupes algébriques et corps de classes", Hermann, Paris (1959)). Sur un corps fini, un tel point est un point de torsion, donc l'extension est isogène à l'extension triviale. D'où, pour une extension J_X de $J_{\tilde{X}}$ par un tore T_X, il y a une isogénie entre J_X et $J_{\tilde{X}} \times T_X$ qui induit un isomorphisme Galois-équivariant entre $T_\ell(J_X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ et $T_\ell(J_{\tilde{X}} \times T_X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell \simeq (T_\ell(J_{\tilde{X}}) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell) \times (T_\ell(T_X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell)$. Puisque l'endomorphisme de Frobenius agit semi-simplement sur les variétés abéliennes ainsi que sur les tores, on en déduit qu'il agit semi-simplement sur les variétés semi-abéliennes aussi et donc sur $T_\ell(J_X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ et $T_\ell(J_Y) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. De plus, on a vu plus haut que leurs polynômes caractéristiques étaient les polynômes $P_{k,H^1(X)}(T)$ et $P_{k,H^1(Y)}(T)$. Par le théorème 5, celui-là divise celui-ci, et on en déduit donc que $T_\ell(J_X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ est $\mathrm{Gal}(\bar{k}/k)$-isomorphe à un $\mathrm{Gal}(\bar{k}/k)$-sous espace de $T_\ell(J_Y) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$.

De plus, le théorème de Tate sur les variétés abéliennes (cf J. Tate : "Endomorphisms of abelian varieties over finite fields", Inventiones Math., **2**, 134-144, (1966)) reste vrai pour les variétés semi-abéliennes : en effet, Jannsen (cf U. Jannsen : "Mixed motives, motivic cohomology and Ext-groups", Proceedings of the International Congress of Mathematicians, Zürich, Switzerland 1994, Birkhäuser Verlag (1995)) a prouvé que pour toute variété semi-abélienne A définie sur un corps fini k, on a :

$$\mathrm{End}_k(A) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell \simeq \mathrm{End}_{\mathrm{Gal}(\bar{k}/k)}(T_\ell(A) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell).$$

En imitant la preuve de Tate (cf J. Tate : "Endomorphisms of abelian varieties over finite fields", Inventiones Math., **2**, 134-144, (1966)), on obtient le résultat recherché. □

Revenons à la divisibilité des polynômes caractéristiques. Nous avons par la suite donné dans [10] une preuve, également élémentaire, du théorème 5 sans hypothèse d'irréductibilité des courbes. Celle-ci étant plus longue et moins générale que celle dont nous allons parler maintenant, nous ne la détaillerons donc pas. En effet, nous avons le résultat suivant, dont la preuve utilise les propriétés de l'application Trace (cf Exposé XVIII, Théorème 2.9 de A. Grothendieck (avec M. Artin et J.-L. Verdier), SGA-4 : Théorie des topos et cohomologie étale des schémas, Lectures Notes in Math. 269, 270, 305, Springer-Verlag, Heidelberg (1972-73)), et qui nous a été communiquée par N. Katz :

Proposition 7 *Soient $f : Y \longrightarrow X$ un morphisme fini plat entre variétés algébriques définies sur k et G un $\mathbf{Q}_\ell$-faisceau constructible sur X. Alors le groupe $H^i_c(\overline{X}, G)$ est facteur direct de $H^i_c(\overline{Y}, f^*(G))$ pour tout $i \geq 0$.*

En prenant pour G le faisceau constant $\mathbf{Q}_\ell$, on obtient :

Corollaire 8 *Soit $f : Y \longrightarrow X$ un morphisme fini plat entre variétés algébriques quasi-projectives définies sur k. Alors, pour tout $i \geq 0$, le polynôme $P_{k,H^i_c(X)}(T)$ divise le polynôme $P_{k,H^i_c(X)}(T)$ dans l'anneau $\mathbf{Z}[T]$.*

On se place maintenant dans le cadre le plus général parmi les courbes algébriques projectives, à savoir celui des courbes algébriques projectives, non nécessairement lisses, non nécessairement absolument irréductibles et non nécessairement irréductibles sur un corps fini. On cherche à déterminer les polynômes caractéristiques de l'endomorphisme de Frobenius sur les groupes de cohomologie ℓ-adiques sur de telles courbes. On obtiendra en corollaire des résultats sur les nombres de points rationnels de telles courbes et également sur la différence des nombres de points dans un revêtement plat entre telles courbes. Ce qui suit retrace essentiellement, sans les démonstrations, l'article [11].

Puisque les groupes de cohomologie d'une variété algébrique sont la somme des groupes de cohomologie de ses composantes connexes, les polynômes caractéristiques du Frobenius sont les produits des polynômes caractéristiques sur les composantes. Nous n'allons donc considérer que des courbes projectives *connexes*.

L'exemple de la courbe projective plane d'équation $x^2+y^2=0$ sur k montre l'importance à accorder à la différence entre l'irréductibilité sur k et celle sur $\overline{k}$. En effet, si $q \equiv 1 \pmod 4$, le nombre de points rationnels de cette courbe sur k_n est $2q^n+1$ ce qui nous donne pour fonction zêta $\frac{1}{(1-T)(1-qT)^2}$. Si, en revanche, $q \equiv 3 \pmod 4$, son nombre de points rationnels est donné par $q^n+(-q)^n+1$ et sa fonction zêta est alors $\frac{1}{(1-T)(1-q^2T^2)}$.

Nous nous contenterons de donner la preuve uniquement du deuxième des deux lemmes suivants qui seront d'une grande utilité pour la suite.

Lemme 9 *Soient X une courbe projective définie sur k et $Z \subset X$ une sous-variété non vide de dimension zéro définie sur k. On a alors :*

$$P_{k,H_c^1(X-Z)}(T) = P_{k,H^1(X)}(T)\frac{P_{k,H^0(Z)}(T)}{P_{k,H^0(X)}(T)}.$$

Lemme 10 *Soit V une variété irréductible (resp. connexe) définie sur k qui s'écrit, après extension des scalaires à $\overline{k}$, comme réunion disjointe*

$$\overline{V} = \overline{V}_1 \cup \ldots \cup \overline{V}_m$$

de sous-variétés absolument irréductibles (resp. absolument connexes). Alors les sous-variétés $\overline{V}_1, \ldots, \overline{V}_m$ sont définies sur k_m, conjuguées sous l'action du groupe de Galois $Gal(k_m/k)$ et

$$P_{k,H_c^i(V)}(T) = P_{k_m,H_c^i(V_1)}(T^m).$$

Démonstration. Soit k_n la plus petite extension de k sur laquelle chaque V_i, $1 \leq i \leq m$, soit définie. Alors $\mathrm{Gal}(k_n/k)$ agit sur l'ensemble $\{V_1, \cdots, V_m\}$. La réunion des V_i apparaissant dans une orbite pour cette action est définie sur k et est irréductible (resp. connexe) sur k. Puisque V est irréductible (resp. connexe) par hypothèse, cette action est transitive et on a alors $n \geq m$. D'autre part, chaque V_i est défini sur le corps fixe de k_n par le stabilisateur commun.

Par minimalité de n, ce stabilisateur est trivial et donc $n = m$ ce qui prouve les deux premières assertions du lemme.

La suite exacte de Mayer-Vietoris entraîne que :

$$H_c^i(V) = H_c^i(V_1) \oplus \ldots \oplus H_c^i(V_m)$$

en tant qu'espaces vectoriels. A un renumérotage près, on peut supposer que F permute de manière cyclique $V_1, \ldots, V_m$. Soit $\mathcal{B}_1 = \{e_1, \cdots, e_b\}$ une base de $H_c^i(V_1)$, ce qui entraîne que $\mathcal{B}_k = \{F^{k-1}(e_1), \cdots, F^{k-1}(e_b)\}$ est une base de $H_c^i(V_k)$. Dans la base $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_m$ de $H_c^i(V)$, la matrice de F est donc

$$Mat_{\mathcal{B}}(F \mid H_c^i(V)) = \begin{pmatrix} 0 & 0 & \cdots & \cdots & A \\ I & 0 & \cdots & \cdots & 0 \\ 0 & I & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & I & 0 \end{pmatrix}$$

pour une certaine matrice $A \in M_b(\mathbf{Q}_\ell)$. D'où,

$$Mat_{\mathcal{B}}(\varphi_{q^m} \mid H_c^i(V)) = Mat_{\mathcal{B}}(F \mid H_c^i(V))^m = \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A \end{pmatrix};$$

mais la matrice $Mat_{\mathcal{B}}(\varphi_{q^m} \mid H_c^i(V))$ vaut également

$$\begin{pmatrix} Mat_{\mathcal{B}_1}(\varphi_{q^m} \mid H_c^i(V_1)) & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & Mat_{\mathcal{B}_m}(\varphi_{q^m} \mid H_c^i(V_m)) \end{pmatrix},$$

ce qui implique que $A = Mat_{\mathcal{B}_1}(\varphi_{q^m} \mid H_c^i(V_1))$. Le lemme découle alors de la simple remarque que, si $A \in \mathcal{M}_b(\mathbf{Q}_\ell)$ et I est la matrice identité dans $\mathcal{M}_b(\mathbf{Q}_\ell)$ alors

$$\det \begin{pmatrix} I & 0 & \cdots & 0 & -TA \\ -TI & I & \ddots & & 0 \\ 0 & -TI & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & I & 0 \\ 0 & \cdots & 0 & -TI & I \end{pmatrix} = \det(I - T^m A).$$

□

Proposition 11 *Soit X une courbe algébrique projective connexe définie sur k et soit $\overline{X} = \overline{\mathcal{X}}_1 \cup \cdots \cup \overline{\mathcal{X}}_{\overline{c}}$ sa décomposition, après extension à $\overline{k}$, en composantes absolument connexes.*

(i) Les $\overline{\mathcal{X}}_i$ sont définis sur $k_{\overline{c}}$, conjugués sous l'action de $Gal(k_{\overline{c}}/k)$ et

$$P_{k,H^0(X)}(T) = 1 - T^{\overline{c}}.$$

(ii) Soient $\mathcal{X}_1 = X_1 \cup \ldots \cup X_r$ la décomposition de $\mathcal{X}_1$ en composantes $k_{\overline{c}}$-irréductibles et $\overline{r}_i$ le nombre de composantes absolument irréductibles de X_i. Alors

$$P_{k,H^2(X)}(T) = \prod_{i=1}^{r} (1 - (qT)^{\overline{c}.\overline{r}_i}).$$

Si Z est un ensemble algébrique de dimension 0 défini sur k, le lemme 9 nous donne immédiatement :

$$P_{k,H^0(Z)}(T) = \prod_{P \in |Z|} (1 - T^{d_P}).$$

On traite alors le cas du H^1 par dévissage : tout d'abord pour les courbes absolument irréductible (déjà traitées dans [1]), puis seulement réductible sur le corps de base et absolument connexe pour terminer avec le cas connexe.

Théorème 12 *Soit X une courbe algébrique projective définie sur k.*

(i) Si X est absolument irréductible, alors

$$P_{k,H^1(X)}(T) = P_{k,H^1(\widetilde{X})}(T) \prod_{P \in |X|} \frac{\prod_{\nu_X(\widetilde{P})=P} (1 - T^{d_{\widetilde{P}}})}{(1 - T^{d_P})}.$$

(ii) Si X est irréductible sur k et absolument connexe, soit $\overline{X} = \overline{X}_1 \cup \ldots \cup \overline{X}_{\overline{r}}$ sa décomposition, après extension à $\overline{k}$, en composantes absolument irréductibles. Soit l'ensemble algébrique $\overline{Z} = \bigcup_{i \neq j} \overline{X}_i \cap \overline{X}_j$, et $\overline{Z}_i = \overline{Z} \cap \overline{X}_i$. Alors les $\overline{X}_i$ sont définies sur $k_{\overline{r}}$ et sont conjuguées sous l'action de $Gal(k_{\overline{r}}/k)$; $\overline{Z}$ est défini sur k ; les $\overline{Z}_i$ sont définies sur $k_{\overline{r}}$, et

$$P_{k,H^1(X)}(T) = P_{k_{\overline{r}},H^1(X_1)}(T^{\overline{r}}) \frac{P_{k_{\overline{r}},H^0(Z_1)}(T^{\overline{r}}) \big/ P_{k,H^0(Z)}(T)}{(1 - T^{\overline{r}}) \big/ (1 - T)}.$$

(iii) Si X est connexe, on pose, comme dans la proposition 11, $\overline{X} = \overline{\mathcal{X}}_1 \cup \cdots \cup \overline{\mathcal{X}}_{\overline{c}}$ la décomposition de $\overline{X}$ en composantes absolument connexes et $\mathcal{X}_1 = X_1 \cup \ldots \cup X_r$ la décomposition de $\mathcal{X}_1$ en composantes $k_{\overline{c}}$-irréductibles et on note $\overline{c}_i$ le nombre de composantes absolument connexes de X_i. Soit l'ensemble algébrique $Z = \bigcup_{i \neq j} (X_i \cap X_j)$ et $Z_i = Z \cap X_i$. Alors Z et Z_i sont définies sur $k_{\overline{c}}$ et

$$P_{k,H^1(X)}(T) = \prod_{i=1}^{r} P_{k_{\overline{c}},H^1(X_i)}(T^{\overline{c}}) \times \frac{\prod_{i=1}^{r} P_{k_{\overline{c}},H^0(Z_i)}(T^{\overline{c}})}{P_{k_{\overline{c}},H^0(Z)}(T^{\overline{c}})} \times \frac{(1 - T^{\overline{c}})}{\prod_{i=1}^{r} (1 - T^{\overline{c}.\overline{c}_i})}.$$

On peut alors bien entendu écrire, en combinant la proposition 11 et le théorème 12, une formule du nombre de points pour une courbe algébrique projective faisant apparaître les éventuels facteurs communs au numérateur et au dénominateur de la fonction zêta avant simplification.

Une approche élémentaire, basée sur la formule d'inclusion-exclusion, permet d'établir le résultat suivant.

Théorème 13 *Soient X une courbe algébrique projective connexe définie sur k et $X = \overline{X}_1 \cup \cdots \cup \overline{X}_{\overline{r}}$ sa décomposition en courbes projectives $\overline{k}$-irréductibles. Soient g_{X_i} le genre géométrique de $\overline{X}_i$ et $\Delta_X = \sharp\widetilde{X}(\overline{k}) - \sharp X(\overline{k})$.*

Le nombre de points de X rationnels sur k_n est alors donné par :

$$\sharp X(k_n) = \sum_{i=1}^{\overline{r}} \rho_i^n - \sum_{i=1}^{\overline{r}} \sum_{j=1}^{2g_{X_i}} \omega_{i_j}^n - \sum_{i=1}^{\Delta_X - \overline{r}} \beta_i^n$$

où les ρ_{i_j} sont des entiers algébriques de module q, les $\omega_{i,j}$ sont des entiers algébriques de module $\sqrt{q}$ et les β_i sont des racines de l'unité dans $\mathbf{C}$.

Lemme 14 *Soit X une courbe projective connexe définie sur k de genre arithmétique π_X, et $\overline{X} = \overline{X}_1 \cup \cdots \cup \overline{X}_{\overline{r}}$ sa décomposition en composantes $\overline{k}$-irréductibles. Soit $\overline{c}$ le nombre de composantes absolument connexes de $\overline{X}$ et $\Delta_X = \sharp\widetilde{X}(\overline{k}) - \sharp X(\overline{k})$. Alors, on a :*

$$\Delta_X \leq \pi_X - \sum_{i=1}^{\overline{r}} g_{X_i} + \overline{r} - \overline{c}.$$

On en déduit par exemple le corollaire suivant :

Corollaire 15 *Soit X une courbe algébrique projective absolument connexe définie sur k de genre arithmétique π_X, possédant r composantes k-irréductibles supposées absolument irréductibles et de genre géométrique $g_1, \ldots, g_r$. Alors :*

$$|\sharp X(k) - (rq+1)| \leq 2\sum_{i=1}^{r} g_i\sqrt{q} + \Delta_X - r + 1 \leq 2\pi_X\sqrt{q}.$$

Remarquons que l'on peut, de la même manière que J.-P. Serre (cf "Sur le nombre de points rationnels d'une courbe algébrique sur un corps fini", *C. R. Acad. Sci. Paris,* 296, *série I*, (1983), 397–402), améliorer cette borne en remplaçant $2\sqrt{q}$ par sa partie entière.

En combinant les théorèmes 11 et 12 avec le corollaire 8, on obtient :

Théorème 16 *Pour tout morphisme surjectif fini et plat $f : Y \longrightarrow X$ entre courbes algébriques projectives absolument connexes Y and X définies sur k ayant respectivement $\overline{r}_Y$ et $\overline{r}_X$ composantes $\overline{k}$-irréductibles $\overline{Y}_i$ et $\overline{X}_i$ de genres géométriques g_{Y_i} et g_{X_i}, on a :*

$$|\sharp Y(k) - \sharp X(k)| \leq (\overline{r}_Y - \overline{r}_X)q + 2(\sum_{i=1}^{\overline{r}_{Y_i}} g_{Y_i} - \sum_{i=1}^{\overline{r}_{X_i}} g_{X_i})\sqrt{q} + \Delta_Y - \Delta_X - (\overline{r}_{\overline{Y}} - \overline{r}_{\overline{X}}).$$

Dans le cas où $X = \mathbf{P}^1$, et si on suppose que Y est lisse et absolument irréductible, on retrouve la borne de Weil (l'hypothèse de platitude étant alors automatiquement vérifiée). Si l'on supprime l'hypothèse de lissité sur Y, on retrouve la borne sur les courbes singulières donnée dans [1] (et donc aussi dans D. Leep et C. Yeomans : "The number of points on a singular curve over a finite field", *Arch. Math.*, 63, (1994), 420-426 et dans E. Bach : "Weil bounds for singular curves", *Appl. Algebra Engrg. Comm. Comput.,* 7, (1996), no. 4, 289-298 et aussi dans G. Zúniga : "Number of rational points of a singular curve", *Proc. Amer. Math. Soc.* 126 (1998), no. 9, 2549-2556). Lorsque X et Y sont singulières absolument irréductibles, on retrouve alors la borne de [3].

2 Nombre de classes dans les corps de fonctions

2.1 Finitude du nombre de corps de fonctions de type C.M. de nombre de classes donné

Les extensions quadratiques imaginaires des corps $\mathbf{F}_q(X)$ de nombre de classes d'idéaux égal à 1 sont bien connu : ils sont au nombre de 4 (cf R. E. MacRae : "On unique factorization in certain rings of algebraic functions", J. Algebra **17** (1971), 243-261). Le cas des extensions quadratiques réelles est bien différent puisqu'il y a une infinité de tels corps principaux (cf T. A. Schmidt : "Infinitely many real quadratic fields of class number one", J. of Number Theory **54**, 203-205 (1995)). Remarquons que l'on est bien loin de la conjecture de Gauss qui énonce le même résultat mais avec q fixé. Nous nous intéressons ici aux extensions totalement imaginaires d'extensions totalement réelles des corps de fonctions rationnelles $\mathbf{F}_q(X)$. Nous montrons dans [5] la finitude du nombre de telles extensions de nombre de classes fixé.

Pour ce faire, nous montrons tout d'abord que le quotient des régulateurs dans une telle extension est essentiellement l'indice des unités de leurs anneaux d'entiers. Nous montrons ensuite, dans le cas général, la divisibilité des nombres de classes de diviseurs dans une extension séparable finie de corps de fonctions.

Soit K un corps de fonctions algébriques à une variable de corps des constantes $\mathbf{F}_q$.

Soient $S_\infty(K) = \{P_1, \ldots, P_{s_\infty}\}$ un ensemble non vide de places de K et A l'anneau des éléments de K dont les pôles sont dans $S_\infty(K)$ (c'est un anneau de Dedekind). On note $\mathrm{Cl}(A)$ le groupe des classes d'idéaux de A et h_A son ordre. Le nombre h_A est fini et est appelé le nombre de classes d'idéaux de A.
L'analogue du théorème de Dirichlet affirme que le groupe des unités A^* de A (modulo les constantes) est libre et de type fini et de rang $s_\infty - 1$ où $s_\infty = \sharp S_\infty(K)$:

$$A^*/\mathbf{F}_q^* \simeq \mathbf{Z}^{s_\infty - 1}.$$

On considère $\mathcal{D}$ le groupe des diviseurs de K, $\mathcal{D}^0$ celui des diviseurs de degré zéro de K, $\mathcal{P}$ celui des diviseurs principaux de K, $C = \mathcal{D}/\mathcal{P}$ le groupe des classes de diviseurs, $J = \mathcal{D}^0/\mathcal{P}$ celui des classes de diviseurs de degré zéro et δ_K le plus grand commun diviseur de $\{\deg P_1, \ldots, \deg P_{s_\infty}\}$.

Rappelons que l'on a un isomorphisme de C/N sur $\mathrm{Cl}(A)$ où N est le sous-groupe de C engendré par les classes des places de $S_\infty(K)$. Remarquons aussi que J est isomorphe au groupe des points rationnels sur $\mathbf{F}_q$ de la jacobienne de la courbe projective non singulière qui a K pour corps des fonctions. Donc, l'ordre h_K de J, appelé nombre de classes de diviseurs, est aussi l'évaluation en 1 du polynôme numérateur de la fonction zêta de K.
Soient $\mathcal{D}_\infty$ l'ensemble des diviseurs à support dans $S_\infty(K)$, $\mathcal{D}_\infty^0 = \mathcal{D}_\infty \cap \mathcal{D}^0$, $\mathcal{P}_\infty$ l'ensemble des diviseurs principaux à support dans $S_\infty(K)$ et $r_A = [\mathcal{D}_\infty^0 : \mathcal{P}_\infty]$. On a des suites exactes :

$$0 \longrightarrow \mathbf{F}_q^* \longrightarrow A^* \longrightarrow \mathcal{P}_\infty \longrightarrow 0$$

et

$$0 \longrightarrow \mathcal{D}^0_\infty/\mathcal{P}_\infty \longrightarrow J \longrightarrow \mathrm{Cl}(A) \longrightarrow \mathbf{Z}/\delta_K\mathbf{Z} \longrightarrow 0$$

qui nous donnent l'isomorphisme $\mathcal{P}_\infty \simeq A^*/\mathbf{F}_q^*$ et la relation

$$\delta_K h_K = r_A h_A.$$

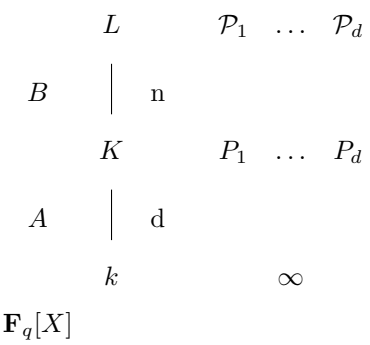
Si P est une place de K, on note v_P la valuation associée à P. Considérons la matrice à s_∞ lignes et $(s_\infty - 1)$ colonnes dont l'élément à la i-ème ligne et j-ème colonne est $-\deg P_i v_{P_i}(\varepsilon_j)$ où $\{\varepsilon_1, \ldots, \varepsilon_{d-1}\}$ est un système fondamental d'unités de A^*. Le régulateur R_A de A est défini comme étant la valeur absolue commune du déterminant de chacun des $(s_\infty - 1) \times (s_\infty - 1)$ mineur de cette matrice. On montre facilement que :

$$r_A = \frac{\delta_K R_A}{\prod_{i=1}^{s_\infty} \deg P_i}.$$

On pose $k = \mathbf{F}_q(X)$ et ∞ la place à l'infini de k. Toutes nos extensions seront contenues dans une clôture séparable de k et admettront $\mathbf{F}_q$ pour corps des constantes.

Considérons une extension totalement imaginaire L de degré n d'une extension totalement réelle K de degré d de k. Cela signifie que la place ∞ de k est totalement décomposée dans K et que les places à l'infini de K ont uniquement une place au-dessus d'elles dans L.

Soit A la clôture intégrale de $\mathbf{F}_q[X]$ dans K et B celle de A dans L.



Par le théorème de Dirichlet, les groupes des unités de L et K sont de rang $d-1$, et on a :

$$[\mathcal{P}_\infty(L) : \mathcal{P}_\infty(K)] = [B^* : A^*]$$

On montre alors (voir [5]) que l'indice $Q := [B^* : A^*]$ divise n^{d-1} et que le quotient des régulateurs s'écrit :

$$\frac{R_B}{R_A} = \frac{n^{d-1}}{Q}.$$

On montre de plus la divisibilité des nombres de classes de diviseurs dans toute extension finie et séparable de corps de fonctions. On s'attache alors à établir une minoration du nombre de classes de diviseurs relatif $h_L^- = \frac{h_L}{h_K}$:

$$h_L^- \geq (\sqrt{q}-1)^{2(n-1)(g_K-1)+\mathcal{R}}$$

où $\mathcal{R}$ est le degré de la différente de L/K.

En montrant qu'à isomorphisme près, il n'y a qu'un nombre fini de courbes algébriques projectives lisses définies sur $\mathbf{F}_q$ de genre borné, où q est borné, nous sommes alors en mesure, dans [5], de démontrer le théorème :

Théorème 17 *Soient K/k un corps de fonctions totalement réel de degré fixé et L/K une extension totalement imaginaire de degré fixé > 1. Soit B la clôture intégrale de $\mathbf{F}_q[X]$ dans L et supposons que le nombre de classes d'idéaux de B est fixé. Alors, à isomorphisme près, il n'y a qu'un nombre fini de telles extensions L/K.*

2.2 Une formule du nombre de classes

Soit $\mathbf{F}_q$ un corps fini à q éléments avec q une puissance d'un premier impair. Pour tout corps de fonctions algébriques M à une variable contenu dans une clôture séparable de $k = \mathbf{F}_q(x)$ et de corps des constantes $\mathbf{F}_q$, on considère l'ensemble S_M de ses places au-dessus de la place à l'infini de k et son anneau de S_M-entiers $\mathcal{O}_M$. On note $h_{\mathcal{O}_M}$ le nombre de classes d'idéaux de $\mathcal{O}_M$.

Soient K une extension quadratique réelle de k et L une extension quadratique imaginaire de K. Nous montrons que le nombre de classes d'idéaux relatif d'une telle extension est reliée à une fonction L dont la valeur en 1 peut s'écrire comme une somme finie de caractères sur des idéaux de l'anneau des entiers de K.

Pour tout corps de fonctions M, soit $\zeta_{\mathcal{O}_M}$ la fonction zêta de l'anneau $\mathcal{O}_M$ définie par :

$$\zeta_{\mathcal{O}_M} = \sum_I \frac{1}{N(I)^s} = \prod_P (1 - N(P)^{-s})^{-1}$$

où $s \in \mathbf{C}$, la somme étant sur tous les idéaux non nuls I de $\mathcal{O}_M$, où $N(I)$ désigne la norme de l'idéal I i.e. le cardinal de l'anneau quotient $\mathcal{O}_M/I$ et où le produit se fait sur les idéaux premiers non nuls de $\mathcal{O}_M$.

On peut alors écrire :

$$\zeta_{\mathcal{O}_L}(s) = \zeta_{\mathcal{O}_K}(s) L_{\mathcal{O}_K}(s, \chi)$$

où

$$L_{\mathcal{O}_K}(s,\chi) = \prod_P \Big(1 - \frac{\chi(P)}{N(P)^s}\Big)^{-1} = \sum_I \frac{\chi(I)}{N(I)^s}$$

où le produit se fait sur les idéaux premiers non nuls de $\mathcal{O}_K$, avec $\chi(P) = -1$, 0 ou 1 selon que P soit inerte, ramifié ou décomposé dans L/K et où χ est étendu multiplicativement à tous les idéaux non nuls de $\mathcal{O}_K$.

En reliant la fonction zêta d'un corps de fonction à celle de la courbe algébrique projective lisse qui lui est associée, on peut établir la relation :

$$h_{\mathcal{O}_L} R_{\mathcal{O}_L} = h_{\mathcal{O}_K} R_{\mathcal{O}_K} L_{\mathcal{O}_K}(0, \chi)$$

où $R_{\mathcal{O}_L}$ et $R_{\mathcal{O}_K}$ désignent les régulateurs de $\mathcal{O}_L$ et $\mathcal{O}_K$. De plus, le quotient $R_{\mathcal{O}_L}/R_{\mathcal{O}_K}$ des régulateurs est égal à $2/Q$ où Q est l'indice des unités $[\mathcal{O}_L^* : \mathcal{O}_K^*]$ qui lui même vaut 1 ou 2.

De plus, on peut montrer que pour toute extension finie séparable totalement imaginaire L/K de corps de fonctions, le nombre de classes d'idéaux de K divise celui de L. Notre preuve (non publiée), contrairement à celle donnée par M. Rosen (cf "The Hilbert class field in function fields", Expo. Math. 5 (1987), 365-378), ne suppose pas l'existence d'une place de l'anneau des entiers $\mathcal{O}_K$ de K qui soit totalement ramifiée dans $\mathcal{O}_L$. La voici en quelques lignes.

En effet, soit $K^{\mathcal{O}_K}$ le corps de classe de Hilbert de K associé à $\mathcal{O}_K$. Il s'agit de l'extension abélienne non ramifiée maximale de K dans une clôture séparable de K dans laquelle toutes les places à l'infini de K se décomposent totalement. Puisque l'extension $K^{\mathcal{O}_K}/K$ est abélienne et non ramifiée, l'extension du compositum $LK^{\mathcal{O}_K}/L$ l'est également. Le corps $LK^{\mathcal{O}_K}$ est donc contenu dans le corps de classes de Hilbert $L^{\mathcal{O}_L}$ de L et on a alors $[LK^{\mathcal{O}_K} : L]$ qui divise $[L^{\mathcal{O}_L} : L]$. Ce dernier est précisément le nombre de classes d'idéaux de $\mathcal{O}_L$, le symbole d'Artin $(\ , L^{\mathcal{O}_L}/L)$ induisant un isomorphisme entre le groupe des classes d'idéaux $\mathrm{Cl}(\mathcal{O}_L)$ et le groupe de Galois $\mathrm{Gal}(L^{\mathcal{O}_L}/L)$.

L'isomorphisme donné par la restriction

$$\mathrm{Gal}(LK^{\mathcal{O}_K}/L) \longrightarrow \mathrm{Gal}(K^{\mathcal{O}_K}/L \cap K^{\mathcal{O}_K})$$

défini par $\sigma \longmapsto \sigma|_{K^{\mathcal{O}_K}}$ nous donne $[LK^{\mathcal{O}_K} : L] = [K^{\mathcal{O}_K}/L \cap K^{\mathcal{O}_K}]$. Finalement, on a $L \cap K^{\mathcal{O}_K} = K$ puisque, d'une part, les places à l'infini de K se décomposent totalement dans $K^{\mathcal{O}_K}$ et donc dans $L \cap K^{\mathcal{O}_K}$, et d'autre part, elles sont ramifiées ou inertes dans L et donc dans $L \cap K^{\mathcal{O}_K}$. D'où, $[LK^{\mathcal{O}_K} : L] = [K^{\mathcal{O}_K} : K] = h_{\mathcal{O}_K}$ divise $[L^{\mathcal{O}_L} : L] = h_{\mathcal{O}_L}$.

On obtient donc, en notant $h^-_{\mathcal{O}_L} = h_{\mathcal{O}_L}/h_{\mathcal{O}_K}$ le nombre de classes relatif :

$$\frac{2}{Q} h^-_{\mathcal{O}_L} = L_{\mathcal{O}_K}(0, \chi).$$

Pour tout corps de fonctions M, on peut définir sa fonction zêta ζ_M par :

$$\zeta_M(s) = \prod_P \Big(1 - \frac{1}{N(P)^s}\Big)^{-1}$$

où P décrit les places de K. On peut alors écrire :

$$\zeta_M(s) = \zeta_{\mathcal{O}_M}(s) \prod_{P \in S_M} \Big(1 - \frac{1}{N(P)^s}\Big)^{-1} = Z_M(q^{-s}) = \frac{P_M(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}$$

où $Z_M(t)$ est la fonction zêta de la courbe lisse associée à M et P_M est un polynôme de degré $2g_M$ où g_M est le genre de cette courbe.

Nous avons montré que pour toute extension L/K, le quotient $\zeta_L(s)/\zeta_K(s)$ est un polynôme en q^{-s} de degré $2(g_L - g_K)$ où g_L et g_K sont les genres des courbes lisses associées à L et K.

Proposition 18 *$L_{\mathcal{O}_K}(s,\chi)$ est un polynôme en q^{-s} de degré*

$$d = 2(g_L - g_K) + j$$

avec j égal à 0, 1 ou 2 selon que les degrés des places à l'infini de L soient égaux à 1, soient différents ou soient égaux à 2.

Si I est un idéal non nul de $\mathcal{O}_K$, on définit le degré de I par $N(I) = q^{\deg I}$. Pour tout entier i, considérons la somme

$$S_i(\chi) = \sum_{\deg I = i} \chi(I)$$

portant sur tous les idéaux non nuls I de $\mathcal{O}_K$ de degré i. Remarquons que l'on a $S_0(\chi) = 1$. On montre alors dans [6] :

Théorème 19 *Soit d l'entier défini dans la proposition précédente. On a :*

$$\frac{2}{Q} h^-_{\mathcal{O}_L} = L_{\mathcal{O}_K}(0,\chi) = \sum_{i=0}^{d} S_i(\chi)$$

La somme intervenant dans le théorème est bien finie. En effet, il n'y a qu'un nombre fini d'idéaux de $\mathcal{O}_K$ de degré donné.

2.3 Corps de fonctions biquadratiques principaux

L'objet de [7] et [8] consiste respectivement en la détermination de tous les corps de fonctions de degré 4 sur $\mathbf{F}_q(X)$, galoisien à groupe de Galois $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, de nombre de classes d'idéaux égal à 1, dans le cas de la caractéristique respectivement impaire et paire. Après l'acceptation pour publication au *Journal of Number Theory* de [7], il est apparu que le résultat était déjà publié dans l'union des trois articles suivants : X.-K. Zhang : "Ambiguous classes and 2-rank of class group of quadratic function field", J. China Univ. Sci. Technol. **17**, n. 4 (1987), 425-431, puis dans X.-K. Zhang : "Algebraic function fields of type $(2, 2, \cdots, 2)$", Scientia Sinica A **31**, n. 5 (1988), 521-530 et enfin dans X.-K. Zhang : "Determination of algebraic function fields of type $(2, 2, .., 2)$ with class number one", Scientia Sinica A **31**, n. 8 (1988), 908-915. Nous ne détaillerons donc pas plus ce travail.

Dans le cas de la caractéristique paire (cf [8]), nous établissons le résultat suivant :

Proposition 20 *Soient L une extension biquadratique bicyclique imaginaire de $\mathbf{F}_q(X)$ et K_1, K_2 and K_3 les trois corps intermédiaires de L/k. On a alors :*

$$\zeta_{\mathcal{O}_L}(s)/\zeta_{\mathcal{O}_k}(s) = \prod_{i=1}^{3} \left(\zeta_{\mathcal{O}_{K_i}}(s)/\zeta_{\mathcal{O}_k}(s)\right) .$$

Cela nous permet de factoriser les nombres de classes d'idéaux en jeu. Une étude minutieuse des extensions d'Artin-Schreier ainsi que du 2-rang du groupe des classes d'idéaux nous permet alors de démontrer le théorème (cf [8]) :

Théorème 21 *Soit L une extension biquadratique bicyclique imaginaire de $k = \mathbf{F}_q(X)$ et soient K_i, $i = 1, 2, 3$, les trois corps intermédiaires. Les extensions L/k de nombre de classes d'idéaux égal à 1 sont exactement les suivants (à isomorphisme laissant fixe la place à l'infini de k près et où α est un générateur de $\mathbf{F}_4^*$) : $L = k(y, z)$, où*

1. *$k = \mathbf{F}_{2^e}(x)$, $y^2 + y = f(x)$, $z^2 + z = g(x)$, où f et g sont des polynômes de degré 1 de $\mathbf{F}_{2^e}[x]$ indépendant sur $\mathbf{F}_{2^e}$ et on a alors $g_L = 0$.*
2. *$k = \mathbf{F}_4(x)$, $y^2 + y = x^3 + \alpha$, $z^2 + z = ax + b$, $(a, b) \in \mathbf{F}_4^* \times \mathbf{F}_4$, et on a alors $g_L = 2$.*
3. *$k = \mathbf{F}_4(x)$, $y^2 + y = x + \frac{\alpha}{x}$ et $z^2 + z = x$ et on a alors $g_L = 1$.*
4. *$k = \mathbf{F}_2(x)$, $y^2 + y = x + 1 + \frac{1}{x}$ and $z^2 + z = x + 1$ et on a alors $g_L = 1$.*
5. *$k = \mathbf{F}_2(x)$, $y^2 + y = x + 1 + \frac{x}{x^2+x+1}$ and $z^2 + z = x + 1$ et on a alors $g_L = 3$.*
6. *$k = \mathbf{F}_2(x)$, $y^2 + y = x + 1 + \frac{1}{x^3}$, $z^2 + z = x + 1$ et on a alors $g_L = 3$.*
7. *$k = \mathbf{F}_2(x)$, $y^2 + y = x + 1 + \frac{x}{x^3+x+1}$ and $z^2 + z = x + 1$ et on a alors $g_L = 5$.*

C'est l'analogue du résultat montré par E. Brown et C. J. Parry dans le cas des corps de nombres (cf "The imaginary bicyclic biquadratic fields with class number 1", *J. Reine Angew. Math.* 266 (1974), 118-120).

Références

[1] Y. Aubry. Reed-Muller codes associated to projective algebraic varieties, Lecture Notes in Mathematics **1518**, *Coding Theory and Algebraic Geometry*, 4-17 (1991).

[2] Y. Aubry. Algebraic geometric codes on surfaces, Conférence à Eurocode, Udine (Italie), (1992), in *Thèse de l'Université d'Aix-Marseille II* (1993).

[3] Y. Aubry, M. Perret. A Weil theorem for singular curves, *Arithmetic, Geometry and Coding Theory - 1993*, Walter de Gruyter, Berlin-New York, 1-7 (1996).

[4] Y. Aubry, M. Perret. Coverings of singular curves over finite fields, *Manuscripta Math.* **88**, 467-478 (1995).

[5] Y. Aubry. Class number in totally imaginary extensions of totally real function fields, *Proceedings of the Third International Conference on Finite fields and Applications*, Lecture Note Series of the London Mathematical Society, Cambridge University Press, 23-29 (1996).

[6] Y. Aubry. Une formule de nombres de classes, *Rapport de Recherche S.D.A.D. - C.N.R.S. ESA 6081*, (1998-3).

[7] Y. Aubry. Principal imaginary bicyclic function fields, *Rapport de Recherche S.D.A.D. - C.N.R.S. ESA 6081*, (1998-4).

[8] Y. Aubry, D. Le Brigand. Imaginary bicyclic biquadratic functions fields in characteristic two, *J. Number Theory* **77**, 36-50 (1999).

[9] Y. Aubry, M. Perret. Divisibility of zeta functions of curves in a covering, *Prétirage de l'Institut de Mathématiques de Luminy no. 2001-34*, soumis, (10 pages), (juillet 2001).

[10] Y. Aubry, M. Perret. An analogue of an Artin conjecture for zeta function of algebraic curves, *Prétirage de l'Institut de Mathématiques de Luminy no. 2002-25*, (14 pages), (2002).

[11] Y. Aubry, M. Perret. On the characteristic polynomials of the Frobenius endomorphism for projective curves over finite fields, soumis (18 pages), (octobre 2002).

[12] E. Bach. Weil bounds for singular curves, *Appl. Algebra Engrg. Comm. Comput.*, 7, (1996), no. 4, 289-298.

[13] S. Bosch, W. Lütkebohmert, M. Raynaud. *Néron Models*, Springer-Verlag Ergebnisse der Math. **21** (1990).

[14] E. Brown, C. Parry. The imaginary bicyclic biquadratic fields with class number 1, *J. Reine Angew. Math.* **266** (1974), 118-120.

[15] P. Deligne. La conjecture de Weil, II, *Publ. Math. IHES*, **52** (1980), 137-252.

[16] V. G. Drinfeld et S. Vladut. Sur le nombre de points d'une courbe algébrique, *Anal. Fonct. Appl.* 17 (1983), 68-69)

[17] A. Grothendieck (avec M. Artin et J.-L. Verdier). SGA-4 : *Théorie des topos et cohomologie étale des schémas*, Lectures Notes in Math. 269, 270, 305, Springer-Verlag, Heidelberg (1972-73).

[18] S. Hansen. Error-correcting codes from higher-dimensional varieties, *Finite Fields Appl.* 7, (2001), no. 4, 531-552).

[19] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo Sect. IA Math 28* (1981), no. 3, 721–724 (1982)

[20] U. Jannsen. Mixed motives, motivic cohomology and Ext-groups, *Proceedings of the International Congress of Mathematicians*, Zürich, Switzerland 1994, Birkhäuser Verlag (1995).

[21] S. L. Kleiman. Algebraic cycles and the Weil conjectures, in *Dix exposés sur la cohomologie des schémas*, North-Holland, Amsterdam (1968), 359-386.

[22] G. Lachaud. Artin-Schreier curves, exponentiel sums and the Carlitz-Uchiyama bound for geometric codes, *J. Number Theory* 39, 18-40 (1991).

[23] D. Leep, C. Yeomans. The number of points on a singular curve over a finite field, *Arch. Math.*, 63, (1994), 420-426.

[24] D. Leep, L. Schueller. Zeros of a pair of quadratic forms defined over a finite field, *Finite Fields Appl. 5* (1999), no. 2, 157-176.

[25] M. Perret. Multiplicative character sums and Kummer coverings, *Acta Arithmetica*, LIX. 3, 279-290 (1991).

[26] R. E. MacRae. On unique factorization in certain rings of algebraic functions, *J. Algebra 17* (1971), 243-261.

[27] M. Rosen. The Hilbert class field in function fields, *Expo. Math.* 5 (1987), 365-378)

[28] T. A. Schmidt. Infinitely many real quadratic fields of class number one, *J. of Number Theory* **54**, 203-205 (1995).

[29] J.-P. Serre. *Groupes algébriques et corps de classes*, Hermann, Paris 1959.

[30] J.-P. Serre. Sur le nombre de points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris*, **296**, *série I*, (1983), 397–402.

[31] J. Tate. Endomorphisms of abelian varieties over finite fields, *Inventiones Math.*, **2**, 134-144, (1966).

[32] M. Tsfasman, S. Vladut, Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* 109 (1982), 21-28.

[33] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, Paris 1948.

[34] X.-K. Zhang. Determination of algebraic function fields of type $(2, 2, .., 2)$ with class number one, *Scientia Sinica A* **31**, n. 8 (1988), 908-915.

[35] X.-K. Zhang. Algebraic function fields of type $(2, 2, \cdots, 2)$, *Scientia Sinica A* **31**, n. 5 (1988), 521-530.

[36] X.-K. Zhang. Ambiguous classes and 2-rank of class group of quadratic function field, *J. China Univ. Sci. Technol.* **17**, n. 4 (1987), 425-431.

[37] G. Zúniga. Number of rational points of a singular curve, *Proc. Amer. Math. Soc.* 126 (1998), no. 9, 2549-2556.