Journées mathématiques X-UPS

Année 1993

Codes géométriques algébriques et arithmétique sur les corps finis

Michel RAYNAUD

Courbes algébriques

Journées mathématiques X-UPS (1993), p. 45-62.
https://doi.org/10.5802/xups.1993-03

Les Éditions de l'École polytechnique
Route de Saclay
F-91128 PALAISEAU CEDEX
https://www.editions.polytechnique.fr

Centre de mathématiques Laurent Schwartz
CMLS, École polytechnique, CNRS,
Institut polytechnique de Paris
F-91128 PALAISEAU CEDEX
https://portail.polytechnique.edu/cmls/

Publication membre du
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org

Journées mathématiques X-UPS
1993, p. 45–62 doi: 10.5802/xups.1993-03

COURBES ALGÉBRIQUES

par

Michel Raynaud

Table des matières

Sur le corps des complexes $\mathbb{C}$, une surface de Riemann X est définie par un atlas de cartes à valeurs dans des ouverts de $\mathbb{C}$, avec des changements de cartes holomorphes. Lorsque X est compacte, X est algébrique, c'est-à-dire peut être définie par des équations polynomiales homogènes, dans un espace projectif convenable. Le passage des équations polynomiales à un atlas résulte alors du théorème des fonctions implicites. Il utilise la topologie de $\mathbb{C}$ et les fonctions analytiques. Nous allons voir comment on peut contourner cette difficulté sur un corps commutatif k quelconque.

Désormais k désigne un corps commutatif, de caractéristique $p \geqslant 0$. Notons d'abord que le calcul différentiel algébrique garde un sens : un polynôme à coefficients dans k, en les variables $x_1, \ldots, x_n$, admet des

Publication originelle dans Journées X-UPS 1993. Codes géométriques algébriques et arithmétique sur les corps finis. Prépublication du Centre de mathématique de l'École polytechnique, 1993.

dérivées partielles par rapport aux x_j, de définition purement algébrique. Si A est une k-algèbre de type fini, quotient de $k[x_1, \cdots, x_n]$ par un idéal I, le A-module des k-différentielles $\Omega^1_{A/k}$ de A est le quotient du A-module libre de base les dx_j, par les relations $df = 0$, où f parcourt un système de générateurs de I. Notons que si $p > 0$ et si g est une puissance p-ème d'un élément de A, on a automatiquement $dg = 0$.

1. Courbes lisses, affines ou projectives

Carte étale. Considérons une variété algébrique affine X, de k-algèbre $A = k[x_1, \ldots, x_n]/I$. Les points rationnels de X correspondent aux n-uples $a = (a_1, \ldots, a_n)$ dans k^n qui annulent les polynômes de I. En un tel point, l'évaluation des fonctions en a définit un morphisme de k-algèbre $A \to k$. Son noyau est donc un idéal maximal m. On obtient ainsi une bijection entre les points de X dans k^n et les idéaux maximaux m de A, tels que A/m soit k-isomorphe à k. Mais il y a lieu d'élargir la notion de point de X, en considérant tous les *idéaux maximaux* de A. Si m est un tel idéal maximal, le quotient A/m est un corps extension de k. Comme c'est aussi une k-algèbre de type fini, cette extension est automatiquement de degré fini sur k. Ainsi un point a de X correspond à un idéal maximal m_a de A et admet un corps résiduel $k(a) = A/m_a$, de degré fini sur k. Un tel point devient rationnel si on étend le corps de définition de k à $k(a)$.

Supposons que l'idéal I soit engendré par $f_1, \ldots, f_{n-1}$ et que le mineur Δ des dérivées partielles des f_j par rapport à $x_1, \ldots, x_{n-1}$ soit inversible dans A. Lorsque $k = \mathbb{C}$, le théorème des *fonctions implicites* nous dit alors que x_n est une coordonnée locale sur X, vue comme surface de Riemann. Sur un corps k général, il n'y a plus de théorème des fonctions implicites. Notons toutefois qu'avec les hypothèses faites, dx_n est une base du A-module $\Omega^1_{A/k}$. La projection $X \to \mathcal{A}$ sur la droite affine, qui envoie $(x_1, \ldots, x_n)$ sur x_n est appelée un *morphisme étale*. Ainsi un morphisme étale correspond à un isomorphisme local sur les complexes.

Sous les hypothèses ci-dessus, nous dirons que X est *une courbe affine lisse*, de coordonnée étale x_n. Une coordonnée étale ne correspond plus en général à un morphisme injectif dans la droite affine,

mais du point de vue du calcul différentiel, elle conduit au même confort qu'une carte holomorphe sur les complexes.

Courbe affine. Une variété affine X d'anneau $A = k[x_1, \ldots, x_n]/I$ est une courbe lisse, si localement pour la topologie de Zariski, elle admet une coordonnée étale au sens précédent. De façon précise, si a est un point de X, on demande qu'il existe un polynôme g dans $k[x_1, \ldots, x_n]$, non nul en a, tel que dans le localisé $k[x_1, \ldots, x_n][g^{-1}]$, l'image de I soit engendrée par $n-1$ éléments $f_1, \ldots, f_{n-1}$ de $k[x_1, \ldots, x_n]$, avec un mineur d'ordre $n-1$ de la matrice jacobienne inversible en a.

Courbe projective. On définit de même une courbe lisse projective, dans l'espace projectif $\mathbb{P}^n$, de coordonnées homogènes $U_0, \ldots, U_n$, en considérant cette fois un idéal I d'équations homogènes, qui localement est engendré par $n-1$ équations, dont la matrice jacobienne admet un mineur d'ordre $n-1$ inversible.

Exemple. Considérons l'application de la droite projective $\mathbb{P}$, de coordonnées homogènes (λ, μ), dans l'espace projectif $\mathbb{P}^3$, de coordonnées homogènes (U, V, W, T), donnée par les formules :

$$U = \lambda^3, \quad V = \lambda^2\mu, \quad W = \lambda\mu^2, \quad T = \mu^3.$$

Alors, l'image est une courbe lisse définie comme l'intersection des trois quadriques :

$$UT - VW = UW - V^2 = VT - W^2 = 0.$$

Corps des fractions et anneaux locaux. On considère désormais une courbe lisse X, affine ou projective, et on suppose qu'elle est connexe, c'est-à-dire qu'il n'y a pas sur X de fonction algébrique idempotente non triviale. Alors X admet un corps des fractions rationnelles $F = F(X)$ qui est une extension de type fini de k, de degré de transcendance 1. Dans le cas affine, d'anneau $A = k[x_1, \ldots, x_n]/I$, A est alors intègre et F n'est autre que le corps des fractions de A. Dans le cas projectif, de coordonnées homogènes U_j et lorsque la courbe X n'est pas contenue dans un hyperplan de coordonnées, F est engendré par les fonctions induites sur la courbe par les U_i/U_j.

Considérons, dans l'espace affine de coordonnées $x_1, \ldots, x_n$, une courbe affine X, passant par l'origine o et admettant x_n pour coordonnée étale. Si on complète $k[x_1, \ldots, x_n]$ pour la topologie définie par l'idéal maximal $(x_1, \ldots, x_n)$, on obtient l'anneau de séries formelles $k[\![x_1, \ldots, x_n]\!]$ et dans ce contexte formel, on dispose à nouveau d'un théorème des fonctions implicites : les x_i s'expriment comme séries formelles en x_n sans terme constant. En particulier le complété de l'anneau local de X en o est $k[\![x_n]\!]$, donc est un anneau de valuation discrète. Rappelons qu'un *anneau de valuation discrète* R est un anneau local principal intègre qui n'est pas un corps. Son unique idéal maximal m est alors engendré par un élément non nul et R/m est le corps résiduel. Les idéaux non nuls de R sont les puissances de m. Par exemple, l'anneau des germes de fonctions holomorphes au voisinage de 0 dans $\mathbb{C}$ est un anneau de valuation discrète. Il en est de même des localisés en les idéaux maximaux d'un anneau d'entiers de corps de nombres.

Revenons à notre courbe X passant par l'origine o. L'anneau local de X en o est un anneau de valuation discrète, puisqu'il en est ainsi de son complété. Plus généralement, en tout point z d'une courbe lisse X, l'anneau local des germes de fonctions algébriques en z est un anneau de valuation discrète $\mathcal{O}_{X,z}$, de corps des fractions $F = F(X)$, de corps résiduel $k(z)$, extension finie de k. Si X est affine d'algèbre A et si z correspond à l'idéal maximal m de A, l'anneau local $\mathcal{O}_{X,z}$ se déduit de A par localisation par les éléments de $A - m$.

Rappelons qu'un corps est *parfait* s'il est de caractéristique zéro ou bien s'il est de caractéristique $p > 0$ et si tout élément est une puissance p-ème. En particulier les corps finis et les corps algébriquement clos sont parfaits.

Lorsque le corps de base est parfait, le corps résiduel $k(z)$ au point z d'une courbe lisse X se relève canoniquement dans le complété de l'anneau local en z, qui se trouve donc être isomorphe à l'anneau de séries formelles $k(z)[\![t]\!]$.

Ainsi lorsque X est une courbe lisse affine connexe, son anneau A est un anneau noethérien intègre dont les localisés aux divers idéaux maximaux sont des anneaux de valuation discrète. Un tel anneau est

un *anneau de Dedekind*. À côté des anneaux des courbes affines lisses, les anneaux de Dedekind les plus utiles sont les anneaux d'entiers d'un corps de nombres. Un tel anneau est presqu'aussi confortable qu'un anneau principal : tout idéal est localement principal et tout idéal I non nul s'écrit de manière unique comme produit d'un nombre fini d'idéaux maximaux.

Soit X une k-courbe lisse connexe de corps des fractions F et soit k' la fermeture intégrale de k dans F. Alors k' est une extension finie séparable de k et X est en fait une courbe sur k'. Il y a intérêt à remplacer le corps des constantes k par k', ce qui assure que la courbe X reste connexe après toute extension de corps. On dit alors que X est *géométriquement connexe*.

Une courbe X est munie de la *topologie de Zariski* pour laquelle les ouverts non vides sont les complémentaires des ensembles finis de points. Cette topologie n'est pas séparée mais elle assure que si $f \in F(X)$, f est définie sur un ouvert de X et l'ensemble des zéros et des pôles de f sont des fermés.

Courbes projectives et places. Sur le corps des complexes une courbe projective, munie de la topologie héritée de celle de $\mathbb{C}$, est *compacte*. Nous allons donner une caractérisation des courbes projectives sur un corps quelconque.

Soit X une k-courbe lisse, connexe, de corps des fractions F.

Définition. Une *k-place* de F est un anneau de valuation discrète V contenant k, et de corps des fractions F.

Nous avons vu qu'à tout point z de X, correspond une k-place de F : l'anneau local $\mathcal{O}_{X,z}$.

Proposition. *Si X est une courbe lisse projective, connexe, les k-places de $F(X)$ sont en bijection avec les points de X.*

Ainsi, on obtient une caractérisation des points d'une courbe projective et lisse en terme du corps des fractions $F(X)$ et du corps des constantes k. Elle est indépendante du plongement projectif. On dit qu'une courbe projective est *complète*, par opposition aux courbes

affines pour lesquelles il manque un nombre fini de points qui apparaîtront « à l'infini », si l'on plonge l'espace affine dans l'espace projectif.

Proposition. *Supposons le corps k* parfait. *L'application $X \mapsto F(X)$, réalise une bijection entre les courbes lisses, complètes, connexes et les corps F, extension de type fini de k, de degré de transcendance* 1.

Pour construire la courbe X à partir de F, on procède comme suit. On choisit un élément x de F transcendant sur k. Alors $[F : k(x)] = d$ est fini. Soit A_1 (resp. A_2) la clôture intégrale de $k[x]$ (resp. $k[x^{-1}]$) dans F. C'est une k-algèbre de type fini, qui est l'algèbre d'une courbe affine lisse X_1 (resp. X_2) (c'est ici que sert k parfait). Par recollement de X_1 et X_2 au-dessus de $k[x, x^{-1}]$, on obtient une courbe complète X, lisse, de corps des fractions F, réalisée comme revêtement (ramifié) de degré d, de la droite projective de coordonnée x.

Remarque. Une courbe lisse complète se réalise de multiples façons comme courbe projective. Si de plus k est infini, on peut toujours la réaliser comme courbe gauche dans $\mathbb{P}^3$. Les plus accessibles de ces courbes gauches sont celles qui sont intersection complète de deux surfaces de degrés d_1 et d_2. En dehors de ce cas très exceptionnel, et de celui encore plus exceptionnel des courbes planes, les équations explicites de la courbe plongée sont difficiles à utiliser. On va plutôt s'intéresser à des propriétés intrinsèques de la courbe, indépendantes de tout plongement projectif.

2. Diviseurs et faisceaux inversibles

Soit X une courbe lisse, connexe, définie sur le corps k et de corps des fractions F. On note $\mathrm{Div}(X)$ le groupe libre commutatif, de base les points de X. Un diviseur est donc donné par une combinaison formelle $D = \sum_z n_z z$, où z parcourt les points de X et où les n_z sont des entiers presque tous nuls. Le diviseur D est dit $\geqslant 0$ si $n_z \geqslant 0$, pour tout z. Si f est un élément non nul de F, on lui associe son diviseur $(f) = \sum_z v_z(f)z$, où v_z est la valuation de l'anneau local $\mathcal{O}_{X,z}$, qui vaut 1 sur un générateur de l'idéal maximal. Les diviseurs

de la forme (f) sont les diviseurs principaux. Deux diviseurs sont linéairement équivalents s'ils différent par un diviseur principal.

Un faisceau inversible $\mathcal{L}$ sur X est un faisceau localement isomorphe au faisceau structural $\mathcal{O}_X$, pour la topologie de Zariski. On peut toujours recouvrir X par deux ouverts affines U et U', tels que $\mathcal{L}_{|U}$ (resp. $\mathcal{L}_{|U'}$) soit engendré par une base s (resp. s'). Alors sur $U \cap U'$, on a $s' = us$, où u est une fonction inversible. Le faisceau des 1-formes différentielles $\omega = \Omega^1_X$ est un faisceau inversible localement engendré par la différentielle dx d'une coordonnée étale ; on l'appelle le *faisceau canonique*.

À tout diviseur D, on associe classiquement un faisceau inversible noté $\mathcal{O}_X(D)$ qui est un sous-faisceau du faisceau constant $\underline{F}$ des fonctions rationnelles sur X. Pour tout ouvert U de X, les sections de $\mathcal{O}_X(D)$ sur U, sont les fonctions rationnelles f sur U, telle que $[(f) + D]_{|U} \geqslant 0$. Pour U assez petit, un générateur de $\mathcal{O}_X(D)_{|U}$ est une fonction f de F telle que $[(f) + D]_{|U} = 0$. En particulier, les sections globales de $\mathcal{O}_X(D)$ sont les fonctions rationnelles f telles que $(f) + D \geqslant 0$.

Réciproquement, si on part d'un faisceau inversible $\mathcal{L}$ sur X, le faisceau $\mathcal{L} \otimes_{\mathcal{O}_X} \underline{F}$ est isomorphe à $\underline{F}$. Le choix d'une section non nulle de $\mathcal{L} \otimes_{\mathcal{O}_X} \underline{F}$ permet d'identifier $\mathcal{L}$ à un sous-faisceau de $\underline{F}$, de la forme $\mathcal{O}_X(D)$, pour un diviseur D convenable. Changer de section, revient à remplacer D par un diviseur linéairement équivalent. On obtient ainsi un dictionnaire entre classes d'isomorphismes de faisceaux inversibles et classes de diviseurs.

Supposons de plus la courbe X *complète*. On définit alors le degré d'un diviseur $D = \sum_z n_z z$, par la formule :

$$\text{degré}(D) = \sum_z n_z [k(z) : k],$$

où $[k(z) : k]$ désigne le degré sur k de l'extension résiduelle $k(z)$. Alors tout diviseur principal (f) est de degré 0 (i.e., le degré du diviseur des zéros est égal à celui des pôles). En particulier, on peut parler du degré d'une classe de diviseurs, et si $\mathcal{L}$ est un faisceau inversible, isomorphe à $\mathcal{O}_X(D)$, on définit le degré de $\mathcal{L}$ comme étant celui de D. Toujours dans le cas où X est complète, le k-espace vectoriel $H^0(X, \mathcal{L})$, des sections globales de $\mathcal{L}$, est de dimension finie. Chaque

section non nulle s de $\mathcal{L} \approx \mathcal{O}_X(D)$ admet un ensemble de zéros qui est un diviseur $\Delta \geqslant 0$, linéairement équivalent à D. Si X est géométriquement connexe, les seuls éléments non nuls de F, de diviseur nul, sont les éléments non nuls de k. On obtient ainsi une bijection entre l'espace projectif des droites du k-vectoriel $H^0(X, \mathcal{L})$, où $\mathcal{L} = \mathcal{O}_X(D)$, et l'ensemble des diviseurs $\Delta \geqslant 0$, linéairement équivalents à D. En particulier, si $\mathcal{L}$ est degré $< 0, H^0(X, \mathcal{L}) = 0$.

3. Le genre

Sur les complexes, une surface de Riemann X compacte connexe a un genre g, défini par sa topologie : comme espace topologique X est un tore à g trous. Mais g est aussi la dimension sur $\mathbb{C}$ de l'espace des formes différentielles holomorphes sur X. C'est cette dernière définition qui va pouvoir s'adapter au cas d'un corps quelconque.

Définition. Soit X une k-courbe lisse complète géométriquement connexe. Le genre g de X est la dimension sur k du k-espace vectoriel $H^0(X, \omega)$, espace des formes différentielles algébriques sur X.

Remarque. On peut aussi déterminer le genre g de X, à partir du degré de ω qui est $2g - 2$.

Exemple. Rappelons que sur l'espace projectif $Q = \mathbb{P}^n$ et pour tout entier m, on note $\mathcal{O}_Q(m)$ le faisceau inversible des « fonctions » homogènes de degré m. Si X est une courbe plane, lisse de degré d, dans le plan projectif $Q = \mathbb{P}^2$, le faisceau ω_X est isomorphe à $\mathcal{O}_Q(d-3)_{|X}$ et le genre de X est $(d-1)(d-2)/2$.

Soit $\pi : Y \to X$ un morphisme fini de degré d entre courbes lisses, complètes géométriquement connexes. Supposons que le corps des fractions $F(Y)$ de Y soit une extension séparable de $F(X)$. Alors ω_Y contient $\pi^*(\omega_X)$, l'image réciproque par π du faisceau ω_X, de sorte qu'il existe un faisceau d'idéaux $\mathcal{V}_{Y/X}$ sur Y, tel que $\omega_Y = \pi^*(\omega_X)[\mathcal{V}_{Y/X}]^{-1}$. Le faisceau $\mathcal{V}_{Y/X}$ est la *différente* de Y par rapport à X et correspond à un diviseur $\geqslant 0$ sur Y : $\sum_y n_y y$, avec $n_y \geqslant 0$. De plus, $n_y > 0$ si et seulement si π est ramifié en y.

En comparant les degrés on trouve la *formule de Hurwitz* :

$$2\text{genre}(Y) - 2 = d[2\text{genre}(X) - 2] + \deg \mathcal{V}_{Y/X}.$$

L'avantage de cette formule est que le calcul du degré de la différente se ramène à un calcul local en chacun des points de ramification de π : si y est un point de Y au-dessus du point x de X et si t (resp. τ) sont des coordonnées étales centrées en x (resp. y), on a $dt = u\tau^{n_y} d\tau$, où u est une unité en y.

- En un point y de Y où l'indice de ramification e_y de π est d'ordre premier à p (on dit alors que la ramification est modérée), l'exposant n_y de y dans la différente est $e_y - 1$, comme dans le cas complexe.
- Par contre, en un point y où l'indice de ramification géométrique est multiple de p (on dit qu'il y a ramification sauvage), l'exposant n_y de y peut être arbitrairement élevé, indépendamment du degré d.

Exemple. Plaçons nous en caractéristique $p > 0$. Considérons la droite affine de coordonnée x et le revêtement galoisien de groupe $\mathbb{Z}/p\mathbb{Z}$, d'équation :

$$U^p - U = H(x),$$

où $H(x)$ est un polynôme en x, de degré $m > 0$ premier à p. Ce revêtement de la droite affine est non ramifié et s'étend en un revêtement Y de la droite projective $\mathbb{P}$, totalement ramifié au-dessus de l'infini. Notons ∞' l'unique point de Y au-dessus du point ∞ de $\mathbb{P}$ et calculons l'exposant de ∞' dans la différente $\mathcal{V}_{Y/\mathbb{P}}$.

Soit τ une coordonnée étale centrée en ∞' et $t = 1/x$ la coordonnée sur $\mathbb{P}$ centrée en ∞. La fonction rationnelle U admet en ∞' un pôle d'ordre m et donc, puisque $(m, p) = 1$, dU admet en ∞' un pôle d'ordre $m + 1$. D'où, à des unités locales près, : $d\tau/\tau^{m+1} \approx dU = -dH \approx dt/t^{m+1}$. Donc $dt \approx (t/\tau)^{m+1} d\tau$. L'exposant dans la différente au point ∞' est donc $(p-1)(m+1)$, et par suite le genre de Y est $g = (m-1)(p-1)/2$.

4. Courbes de petit genre

Soit X une courbe complète lisse sur k, géométriquement connexe, de genre g.

• Si $g = 0$, X est canoniquement une *conique* dans le plan projectif. Si de plus elle possède un point rationnel, (en particulier si k est fini), X est isomorphe à la droite projective. Par contre sur $\mathbb{R}$, la conique « imaginaire » d'équation $U^2+V^2+W^2 = 0$, n'a pas de points rationnels. Sur un corps algébriquement clos de caractéristique 2, une conique projective lisse admet pour équation $UV + W^2 = 0$. Le fait que la dérivée par rapport à W soit nulle, entraîne que toutes les tangentes à la conique passent par le point $(0, 0, 1)$.

• Lorsque $g = 1$, X est une courbe *elliptique*. Si X possède un point rationnel (ce qui est le cas en particulier si k est fini), X se réalise comme cubique dans le plan projectif. En coordonnées homogènes U, V, W, l'équation de la cubique peut être mise sous le forme :

$$V^2W + a_1UVW + a_3VW^2 = U^3 + a_2U^2W + a_4UW^2 + a_6W^3,$$

avec un discriminant $\Delta \neq 0$.

Lorsque la caractéristique p est différente de 2 et 3, on se ramène, par translations, à la forme de Weierstrass habituelle :

$$V^2W = U^3 + a_4UW^2 + a_6W^3,$$

avec $\Delta = -(4a_4^3 + 27a_6^2)$.

• Lorsque $g = 2$, X ne se réalise pas comme courbe plane ou comme courbe gauche intersection complète. Par contre, X est hyperelliptique, c'est-à-dire est canoniquement un revêtement séparable de degré 2 de la droite projective $\mathbb{P}$.

Pour $p \neq 2$, ce revêtement est ramifié en 6 points géométriques et X est la complétion projective d'une courbe affine d'équation $y^2 = P_6(x)$, où P_6 est un polynôme de degré 6, sans racines multiples. Si l'un des points de ramification est rationnel et choisi à l'infini, X est la complétion d'une courbe affine d'équation $y^2 = H(x)$, où H est polynôme unitaire en x de degré 5, sans racines multiples.

Si $p = 2$, le revêtement de la droite projective peut être ramifié en 3, 2, ou 1 point géométrique et X est la complétion projective d'une courbe affine d'équation du type : $y^2 + P_3(x)y + P_6(x) = 0$, où P_i est un polynôme de degré $\leqslant i$. Par exemple, l'équation $y^2 - y = x^5$, conduit à une courbe de genre 2, ramifiée uniquement au-dessus de $x = \infty$.

• Une courbe de genre 3, se réalise canoniquement comme quartique dans le plan projectif, sauf si elle est hyperelliptique. Parmi les quartiques, on trouve celle de Klein d'équation :

$$U^3V + V^3W + W^3U = 0.$$

Sur les complexes, cette courbe admet un groupe G d'automorphismes qui est le deuxième groupe fini simple : $G \approx PSL(\mathbb{F}_7)$ à 168 éléments. En caractéristique 3, le groupe d'automorphismes gonfle jusqu'à devenir le groupe projectif $PU(3,3)$ à 6048 éléments.

5. Formule de Riemann-Roch et dualité

Soit toujours X une k-courbe lisse, complète, géométriquement connexe de genre g.

Si $\mathcal{F}$ est un faisceau en groupes commutatifs sur X pour la topologie de Zariski, on dispose de ses groupes de cohomologie $H^i(X,\mathcal{F})$, qui sont nuls pour $i \neq 0, 1$. Si $\mathcal{F}$ est un faisceau inversible $\mathcal{L}$, les groupes $H^i(X,\mathcal{L})$ sont des k-vectoriels de dimension finie. On note $H^i(\mathcal{L})$ la dimension sur k de $H^i(X,\mathcal{L})$. Si $\mathcal{L}$ est un faisceau inversible, $\mathcal{L}^*$ désigne le faisceau inversible dual. Lorsque $\mathcal{L} = \mathcal{O}_X(D)$, $\mathcal{L}^* = \mathcal{O}_X(-D)$.

La compréhension de la cohomologie des faisceaux inversibles est régie par celle du faisceau dualisant ω.

Théorème

(1) *$H^1(X,\omega)$ est canoniquement isomorphe au corps k.*

(2) *Pour tout faisceau inversible $\mathcal{L}$ sur X, et tout entier i, l'accouplement*

$$H^i(X,\mathcal{L}) \times H^{1-i}(X,\omega \otimes \mathcal{L}^*) \longrightarrow H^1(X,\omega) = k,$$

donné par le cup-produit, est une dualité parfaite.

Rappelons que pour calculer la cohomologie d'un faisceau $\mathcal{F}$ sur X, on considère une résolution de $\mathcal{F}$:

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{F}^1 \longrightarrow \mathcal{F}^2 \longrightarrow \cdots,$$

où les $\mathcal{F}^i$ sont acycliques, c'est-à-dire ont des groupes de cohomologie $H^i(X,\mathcal{F}^i)$ nuls pour $j > 0$. Le groupe $H^j(X,\mathcal{F})$ est alors le j-ème

groupe de cohomologie du complexe :

$$H^0(X, \mathcal{F}^1) \longrightarrow H^0(X, \mathcal{F}^2) \longrightarrow \cdots$$

Parmi les faisceaux acycliques, on trouve les faisceaux flasques $\mathcal{G}$, c'est-à-dire ceux pour lesquels, pour tout couple d'ouverts U, V avec $V \supset U$, toute section de $\mathcal{G}$ sur U s'étend en une section de $\mathcal{G}$ sur V.

Pour calculer $H^1(X, \omega)$, on dispose d'une résolution acyclique naturelle de ω. En effet, ω se plonge dans le faisceau constant $\omega \otimes_{\mathcal{O}_X} \underline{F}$ des formes différentielles rationnelles. Le conoyau est le faisceau M des parties polaires de différentielles. On obtient ainsi une résolution flasque canonique de ω, qui permet de calculer la cohomologie. En particulier, on a :

$$H^1(X, \omega) = \mathrm{coker}[H^0(X, \omega \otimes_{\mathcal{O}_X} \underline{F}) \longrightarrow H^0(X, M)].$$

Notons qu'en chaque point x de X, une section μ de M admet un *résidu* $\mathrm{Res}_X(\mu)$ qui est un élément du corps résiduel $k(x)$. Si x est un point rationnel et si t est une coordonnée étale centrée en x, μ s'écrit $(\sum_{-1}^{-n} a_i t^i)dt$ et le résidu est le coefficient a_{-1}. On doit bien sûr vérifier qu'il est indépendant du choix de t. Si μ est une section de M, on peut, grâce à l'opération de trace, définir la « somme » des résidus $\sum_x \mathrm{Tr}_{k(x)/k}\mathrm{Res}_x(\mu)$, qui est un élément de k. L'assertion (1) du théorème équivaut alors à la conjonction des deux propriétés suivantes :

(1) Pour toute forme différentielle rationnelle τ, on a

$$\sum_x \mathrm{Tr}_{k(x)/k}\mathrm{Res}_x(\tau) = 0.$$

(2) Toute section μ de M, telle $\sum_x \mathrm{Tr}_{k(x)/k}\mathrm{Res}_x(\mu) = 0$, est la partie polaire d'une différentielle rationnelle τ sur X.

On trouvera dans [3] une démonstration accessible du théorème ci-dessus, du moins lorsque le corps k est algébriquement clos.

Corollaire. *On a* $g = h^1(\mathcal{O}_X)$.

Pour tout faisceau inversible $\mathcal{L}$ sur X, on définit la caractéristique d'Euler-Poincaré de $\mathcal{L}$, par $\chi(\mathcal{L}) = h^0(\mathcal{L}) - h^1(\mathcal{L})$.

On connaît $\chi(\omega) = g - 1$. On en déduit facilement le corollaire suivant :

Corollaire. *Pour tout faisceau inversible $\mathcal{L}$ sur X, on a :*

$$\chi(\mathcal{L}) = 1 - g + \text{degré}(\mathcal{L}).$$

Ainsi la caractéristique d'Euler-Poincaré se calcule au moyen d'invariants numériques, par contre les dimensions des espaces de cohomologie $h^i(\mathcal{L})$ peuvent être plus difficiles à déterminer.

En combinant avec la formule de dualité on obtient :

***Corollaire* (théorème de Riemann-Roch).** *Pour tout faisceau inversible $\mathcal{L}$ sur X, on a*

$$h^0(\mathcal{L}) - h^0(\omega \otimes (\mathcal{L}^*)) = 1 - g + \text{degré}(\mathcal{L}).$$

Cet énoncé a l'avantage de ne plus faire intervenir que des espaces de cohomologie en degré zéro. Si l'on choisit un diviseur K dans la classe canonique, il se reformule :

$$h^0(\mathcal{O}_X(D)) - h^0(\mathcal{O}_X(K - D)) = 1 - g + \text{degré}(D).$$

Corollaire. *Pour* $\text{degré}(\mathcal{L}) < 0$*, on a* $h^0(\mathcal{L}) = 0$*. Pour* $\text{degré}(\mathcal{L}) > 2g - 2$*, on a* $h^1(\mathcal{L}) = 0$ *et* $h^0(\mathcal{L}) = 1 - g + \text{degré}(\mathcal{L})$.

Remarque. Sur la droite projective, le théorème de décomposition des fractions rationnelles en éléments simples, nous dit qu'étant donnée une partie polaire arbitraire, on peut trouver une fonction rationnelle globale, définie à l'addition près d'une constante, qui admet précisément la donnée comme partie polaire. Il n'en va plus de même en genre $g > 0$. Ainsi le corollaire précédent nous dit que si on se donne un diviseur positif D de degré $> 2g - 2$, $h^0(\mathcal{O}_X(D))$ a pour dimension seulement $1 - g + \text{degré}(D)$, qui est strictement plus petit que $1 + \text{degré}(D)$ pour $g > 0$.

6. Courbes sur les corps finis

Désormais k désigne un corps fini $\mathbb{F}_q$, à q éléments. On choisit une clôture algébrique $\overline{k}$ de k. Pour tout entier $m \geqslant 1$, k_m désigne l'extension de degré m de k contenue dans $\overline{k}$. On note $X \otimes_k k_m$ la

courbe déduite de X par extension du corps de base k à k_m et $\overline{X}$ la courbe $X \otimes_k \overline{k}$. Pour tout entier $m > 0$, $X(k_m)$ est l'ensemble fini des points rationnels de $X \otimes_k k_m$.

On note :

- A_m le nombre de diviseurs $\geqslant 0$ sur X, de degré m,
- M_m le nombre de points de X de corps résiduel k_m,
- N_m le nombre de points rationnels de $X \otimes_k k_m$.

Rappelons que pour s complexe avec $\mathrm{Re}(s) > 1$, on définit la fonction zêta de Riemann par la formule :

$$\zeta(s) = \sum \frac{1}{n^s} = \prod \frac{1}{(1 - 1/p^s)},$$

où p parcourt l'ensemble des nombres premiers, c'est-à-dire encore le spectre maximal de $\mathbb{Z}$. Cette expression admet un analogue pour la courbe X, qui est la fonction zêta de la courbe X :

$$\zeta_X(s) = \prod_X \frac{1}{(1 - 1/(\#k(x))^s)},$$

où $\#k(x)$ désigne le cardinal du corps résiduel $k(x)$. Or, en un point x où $[k(x) : k] = m$, on a $\#k(x) = q^m$. Par suite, si on pose $T = 1/q^s$ et

$$(*) \qquad Z_X(T) = \prod_{x \in X} \frac{1}{(1 - T^{\deg(x)})},$$

on a $\zeta_X(s) = Z_X(q^{-s})$.

Proposition. *Les trois séries formelles suivantes sont égales, et coïncident avec $Z_X(T)$:*

(a) $\displaystyle\sum_0^\infty A_m T^m$,

(b) $\displaystyle\prod_1^\infty (1 - T^m)^{-M_m}$,

(c) $\displaystyle\exp\Big(\sum_1^\infty N_m T^m/m\Big)$.

L'expression (b) résulte de $(*)$ en regroupant les termes qui correspondent à un degré m donné.

L'égalité de (a) et (b) provient du fait que tout diviseur positif s'écrit de manière unique comme somme de points de X à coefficients entiers $\geqslant 0$.

L'égalité de (b) et (c), résulte, en prenant les dérivées logarithmiques, de la relation $N_m = \sum_{d|m} dM_d$.

Corollaire. *On a* $TZ'_X/Z_X = \sum_1^\infty N_m T^m$.

Faisons l'observation suivante. Supposons avoir écrit Z_X sous la forme P/Q, où P et Q sont des polynômes en T de terme constant 1. Écrivons dans $\mathbb{C}[T]$:

$$P = \prod_i (1 - \alpha_i T), \quad Q = \prod_j (1 - \beta_j T).$$

Alors

$$TZ'_X/Z_X = -\sum_i \alpha_i T/(1 - \alpha_i T) + \sum_j \beta_j T/(1 - \beta_j T).$$

Par suite on a :

$$N_m = \sum_j \beta_j^m - \sum_i \alpha_i^m.$$

Théorème **(André Weil)**

(1) *Il existe un polynôme de* $\mathbb{Z}[T]$ *de degré* $2g$: $P_1 = 1 + \cdots + q^g T^{2g}$, *tel que* $Z_X(T) = P_1(T)/(1 - T)(1 - qT)$, *en particulier* Z_X *est une fraction rationnelle en* T.

(2) *On a* $P_1(T) = \prod_{i=1}^{2g}(1 - \alpha_i T)$, *où les* α_i *sont des entiers algébriques, qui, dans tout plongement dans* $\mathbb{C}$ *ont pour module* $\sqrt{q}$. *De plus l'application* $\alpha \mapsto q/\alpha$ *induit une permutation des* α_i.

Notons que toutes les propriétés ci-dessus, à l'exception du module des α_i, se déduisent formellement du théorème de Riemann-Roch. Quant au fait que les α_i aient pour module $\sqrt{q}$, il équivaut au fait que les zéros de la fonction $\zeta_X(s)$ ont pour partie réelle $1/2$, un analogue de l'hypothèse de Riemann.

Corollaire. *Pour tout entier* $m > 0$ *on a* $N_m = 1 + q^m - \sum_{i=1}^{2g} \alpha_i^m$. *En particulier,*

$$|N_m - (1 + q^m)| \leqslant 2gq^{m/2}.$$

Corollaire. *Le nombre h de classes de diviseurs de degré 0 sur X est fini, égal $P_1(1)$.*

Cela résulte du fait que pour un degré $m > 2g-2$, chaque classe de diviseurs compte $(q^{m+1-g}-1)/(q-1)$ éléments, et par suite $A_m = h(q^{m+1-g}-1)/(q-1)$.

Remarques

(1) On note que $1+q^m$ est le nombre de points rationnels de la droite projective sur k_m. En particulier, quand m tend vers l'infini, N_m est équivalent à $1+q^m$.

(2) On retrouve que pour $g = 0$ ou 1, X a toujours un point rationnel. Sur le corps $k = \mathbb{F}_4$, la courbe elliptique d'équation $y^2 - y = x^3 + j$, où j est une racine primitive troisième de l'unité, a pour seul point rationnel le point à l'infini, et la borne inférieure de Weil est atteinte.

(3) Considérons sur le corps $\mathbb{F}_3$, la courbe de genre 2 d'équation : $y^2 = P_6(x)$, avec $P_6 = x^6 + x^4 + x^2 + 1$. Elle admet le maximum de points rationnels possible pour une courbe hyperelliptique, à savoir 8. Par contre la courbe $y^2 = -P_6(x)$ n'a pas de points rationnels. C'est aussi le cas de la courbe $U^{p-1} + V^{p-1} + W^{p-1} = 0$ sur le corps à p éléments pour $p \geqslant 5$.

Corollaire. *Pour connaître $Z_X(T)$, et donc tous les N_m, il suffit de connaître les g premiers. En particulier, pour connaître la fonction zêta d'une courbe elliptique, il suffit de connaître N_1.*

La démonstration de Weil [4] utilise les propriétés d'intersection du morphisme de Frobenius sur la jacobienne de X. On trouvera dans [2] une démonstration liée à la théorie des intersections sur les surfaces. Une démonstration élémentaire, à partir de Riemann-Roch a été donnée ultérieurement par Stepanov [1].

La justification la plus conceptuelle de l'expression de la fonction zêta vaut en fait pour une variété algébrique lisse projective quelconque et a été pressentie par Weil, lorsqu'il a formulé ses célèbres conjectures sur les corps finis.

On commence par définir l'endomorphisme de Frobenius Φ sur X, qui consiste à élever les fonctions à la puissance q. Soit $\overline{\Phi}$ l'extension de Φ à $\overline{X}$. Alors les N_m points rationnels de X dans k_m sont les N_m points fixes de $\overline{\Phi}^m$.

Si l'on était sur les complexes, on pourrait utiliser la cohomologie transcendante $H^i(X_{\text{top}}, \mathbb{Q})$ et la formule de Lefschetz, qui exprime le nombre de points fixes d'un endomorphisme, et plus généralement d'une correspondance, comme somme alternée de ses traces sur la cohomologie. Weil a suggéré qu'il devait exister une cohomologie de $\overline{X}$ à valeur dans un corps (?) de caractéristique zéro, qui conduise à une formule des traces de Lefschetz :

$$N_m = \sum (-1)^i \text{Tr}(\overline{\Phi}^m, H^i(\overline{X}, ?)).$$

Dans les années 60, Grothendieck a défini la cohomologie en question, puis Grothendieck et Deligne ont démontré les conjectures de Weil en toute dimension.

Choisissons un nombre premier ℓ, distinct de la caractéristique p. À l'aide de la *topologie étale*, on définit pour chaque entier $n > 0$, les groupes de cohomologie $H^i(\overline{X}, \mathbb{Z}/\ell^n\mathbb{Z})$ qui sont des $\mathbb{Z}/\ell^n\mathbb{Z}$-modules de type fini. Pour n variable, ces cohomologies forment un système projectif, et par définition, on pose :

$$H^i(\overline{X}, \mathbb{Z}_\ell) = \varprojlim_n H^i(\overline{X}, \mathbb{Z}/\ell^n\mathbb{Z})$$

qui est un $\mathbb{Z}$-module de type fini, et $H^i(\overline{X}, \mathbb{Q}_\ell) = H^i(\overline{X}, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, qui est un $\mathbb{Q}_\ell$-espace vectoriel.

Lorsque $k = \mathbb{C}$, les espaces de cohomologie $H^i(\overline{X}, \mathbb{Q}_\ell)$ sont canoniquement isomorphes aux espaces de cohomologie $H^i(X_{\text{top}}, \mathbb{Q}_\ell)$ associés à la variété topologique X_{top} sous-jacente à X.

Pour une courbe propre et lisse, de genre g, sur un corps k algébriquement clos, $H^0(X, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$, $H^1(X, \mathbb{Q}_\ell)$ est de dimension $2g$, $H^2(X, \mathbb{Q}_\ell)$ est de dimension 1.

Pour une variété algébrique propre et lisse, de dimension d, sur un corps k fini, le Frobenius $\overline{\Phi}$ agit par fonctorialité sur les espaces $H^i(\overline{X}, \mathbb{Q}_\ell)$, et

$$P_i(T) = \det(1 - T\overline{\Phi} | H^i(\overline{X}, \mathbb{Q}_\ell))$$

est un polynôme à coefficients entiers, indépendant de ℓ, qui dans $\mathbb{C}[T]$, s'écrit $\prod(1-\alpha_j T)$, où les α_j sont des nombres complexes de module $q^{i/2}$. L'expression de la fonction zêta de X, par rapport à la variable $T = q^{-s}$, est alors :

$$Z_X(T) = \frac{P_1(T)\cdots P_{2d-1}(T)}{P_0(T)\cdots P_{2d}(T)}.$$

Références

[1] E. Bombieri – « Counting points on curves over finite fields (d'après S. A. Stepanov) », in *Séminaire Bourbaki, (1972/1973)*, Lect. Notes in Math., vol. 383, Springer, Berlin, 1974, Exp. no. 430, p. 234–241.

[2] P. Monsky – *p-adic analysis and zeta functions*, Lect. Notes in Math., vol. 4, Kinokuniya Book Store Co., Ltd., Tokyo, 1970.

[3] J.-P. Serre – *Groupes algébriques et corps de classes*, 2e éd., Publ. Inst. Math. Univ. Nancago, vol. 7, Hermann, Paris, 1984.

[4] A. Weil – *Sur les courbes algébriques et les variétés qui s'en déduisent*, Publ. Inst. Math. Univ. Strasbourg, vol. 7, Hermann, Paris, 1948.

Michel Raynaud, Département de Mathématiques, Université de Paris XI, 91405 Orsay Cedex, France