LA PREUVE PAR ANDRÉ WEIL DE L'HYPOTHÈSE DE RIEMANN POUR UNE COURBE SUR UN CORPS FINI

par

Marc Hindry

La démonstration par André Weil, dans les années quarante, de l'hypothèse de Riemann pour une courbe sur un corps fini est un moment mathématique assez extraordinaire pour de multiples raisons : le contexte dramatique durant lequel ce travail a été produit et rédigé par Weil, la polémique avec le mathématicien Helmut Hasse qui a suivi, l'histoire des développements qui l'ont précédé avec notamment les contributions de E. Artin, H. Hasse, F. K. Schmidt et bien sûr B. Riemann, et enfin les prodigieux développements qui l'ont suivi, d'une part dans le cadre des mathématiques appliquées (théorie des codes correcteurs linéaires) et d'autre part dans le cœur des mathématiques pures avec les fameuses « conjectures de Weil », qui ont guidé et stimulé le développement spectaculaire de la géométrie algébrique durant les décennies suivantes, culminant avec leur preuve par Grothendieck et Deligne.

Le contexte. En 1940, nous sommes en pleine seconde guerre mondiale et André Weil, à la suite de péripéties qu'il narre dans ses « souvenirs d'apprentissage » [**We1991**], est enfermé pour insoumission dans la prison « Bonne Nouvelle » à Rouen. Il y séjournera quelques mois, y travaille intensément ses mathématiques, correspond avec Henri Cartan [**Aud2011**], sa sœur Simone Weil [**Wei1940a**] et... démontre la fameuse « *hypothèse de Riemann pour une courbe sur un corps fini* », travail qu'il résume dans une note [**Wei1940b**] de trois pages aux Comptes rendus de l'Académie, présentée, *via* Élie Cartan, lors de la séance du 22 avril 1940. Le résumé glisse sous le tapis un énoncé

(« *Voici un lemme important* ») dont il ne fournit pas la preuve. Libéré de prison et ayant réussi à rallier les États-Unis, André Weil publie une deuxième note [**Wei1941**] aux Proceedings of the National Academy of Sciences où il simplifie sa preuve... mais toujours en laissant un point capital sans élément de preuve (« *as in Severi* »). La note américaine se termine par l'annonce « *A detailed account of this theory* [...] *and of the "transcendental" theory as outlined in my previous note is being prepared for publication.* » En fait Weil publiera en 1946 « *Foundations of Algebraic Geometry* » et en 1948 deux livres sur les courbes algébriques et les variétés abéliennes qui complètent ce programme, ce qui est ainsi résumé par Jean-Pierre Serre « *Après huit années, et plus de 500 pages, sa Note de 1940 est enfin justifiée* ! » [**Ser1999**].

La polémique. Hasse, qui avait réussi quelques années auparavant à démontrer la dite hypothèse de Riemann [**Has1934, Has1936**] pour les courbes de genre 1, a été outré de l'attitude de Weil. Ce dernier a d'ailleurs explicitement décrit ses motivations et la rivalité avec Hasse dans une lettre à Henri Cartan, datée du 8 avril 1940 [**Aud2011**] « *J'ai expédié la note sans avoir démontré le lemme fondamental ; mais j'y vois assez clair sur ces questions à présent pour en prendre le risque. Jamais je n'ai rien écrit, et je n'ai presque jamais rien vu, qui atteigne un aussi haut degré de concentration que cette note. Hasse n'a plus qu'à se pendre, car j'y résous (sous réserve de mon lemme)* tous *les principaux problèmes de la théorie : 1) hypothèse de Riemann pour les fonctions ζ de ces corps (démontrée par Hasse pour le genre* 1*) 2) les séries L d'Artin relatives aux caractères des extensions algébriques de ces corps sont des polynômes, dont je détermine le degré* ». Il s'en est suivi un échange indirect d'amabilités dont je citerai deux extraits : « *Avez-vous une idée d'un "profiteur de guerre spirituel" ? il me semble que notre "ami" André Weil soit un tel . [...] C'est ce que j'appelle une manière typiquement juive !* » (Lettre de Hasse à Gaston Julia, 14 septembre 1941) et, de nombreuses années plus tard, dans les commentaires de ses œuvres, Weil écrit « *Faut-il en conclure que l'esprit de ceux-ci [des algébristes allemands] avait été quelque peu grisé par les succès de leurs généraux ?* »

La genèse. Les analogies entre corps de nombres (le corps $\mathbb{Q}$ et ses extensions finies) et les corps de fonctions sur un corps fini (le corps $\mathbb{F}_p(X)$ et ses extensions finies) ou encore entre arithmétique et géométrie ont exercé une fascination sur de nombreux mathématiciens, le premier étant peut-être Kronecker. Weil lui-même était presque obsédé par cette idée, lui adjoignant en plus un lien avec la topologie riemannienne, il parlait de « texte trilingue » [**Wei1940a**]. L'article de Riemann [**Rie1859**] sur la répartition des nombres premiers est son unique texte traitant de théorie des nombres, il y développe les propriétés de la fonction zêta $\zeta(s) = \sum_{n\geqslant 1} n^{-s}$ et démontre le théorème des nombres premiers en admettant au passage plusieurs résultats dont ce qui est aujourd'hui appelé l'hypothèse de Riemann. Emil Artin a introduit l'analogue des fonctions zêta pour les corps de fonctions sur $\mathbb{F}_q$ et la théorie a été développée par l'école allemande, notamment Deuring, Hasse et Schmidt [**Sch1931, Has1934, Has1936**], établissant la rationalité (analogue du prolongement analytique), l'équation fonctionnelle et, pour les courbes de genre 1, l'hypothèse de Riemann. L'avancée capitale et par bien des aspects l'idée centrale, féconde et novatrice de Weil est de sortir le problème du cadre algébrique et de le placer dans un contexte géométrique.

Les développements ultérieurs. En 1949 André Weil publie un article [**Wei1949**] sur le nombre de points d'une variété algébrique sur un corps fini. Cette article propose une série de conjectures qui généralisent aux variétés de dimensions quelconques les propriétés de la fonction zêta d'une courbe. Cet article visionnaire va, pendant trois décennies, catalyser et susciter la plupart des développements de la géométrie algébrique abstraite, développements pilotés par Grothendieck et complétés plus tard par Deligne : schémas, faisceaux, cycles algébriques et théorie de l'intersection, cohomologie étale, etc.

L'hypothèse de Riemann sur les corps finis s'avèrera également importante pour des questions de télécommunications et théorie de l'information à travers les « codes de Goppa » [**Gop1970**] où la borne dite de Hasse-Weil joue un rôle important. Il s'agit de construire explicitement des bons codes (linéaires) correcteurs d'erreurs ; la découverte de Goppa est que certains systèmes linéaires sur les courbes sur

un corps fini fournissent de tels codes. Un des paramètres importants est le nombre de points rationnels de la courbe, qui doit être aussi grand que possible, c'est-à-dire en pratique approchant autant que possible la borne supérieure fournie par le théorème dit de Hasse-Weil !

Nous commençons bien sûr par expliquer dans le paragraphe suivant l'énoncé de l'hypothèse de Riemann et la définition de la fonction zêta d'une courbe, donnons ensuite des exemples avant de décrire brièvement les conjectures de Weil et allusivement quelques applications. Les trois paragraphes suivants présentent les mathématiques impliquées : d'abord le théorème de Riemann-Roch (hélas sans preuve) qui permet de montrer rationalité et équation fonctionnelle de la fonction zêta d'une courbe, puis la preuve de Weil de l'hypothèse de Riemann et enfin une preuve peut-être moins éclairante mais plus élémentaire découverte trente ans plus tard par Stepanov.

Nous avons repoussé en appendice quelques définitions, notions et exemples concernant corps finis, courbes algébriques et diviseurs sur celles-ci, en estimant que nombre des lecteurs seraient déjà familiers avec ces objets mais que quelques rappels pourrait être utiles à d'autres. Les notions de géométrie algébrique abordées ou évoquées peuvent toutes être étudiées par exemple dans [**Har1977**] et le monde plus élémentaire des courbes algébriques dans [**Gol2002**]. Enfin nous avons tenté d'émailler le texte d'exemples, l'hypothèse de Riemann sur les corps finis étant un énoncé très concret se prêtant bien aux illustrations et expérimentations élémentaires.

1. Corps de fonctions, courbes algébriques et fonctions zêta

La formulation la plus simple de l'hypothèse de Riemann pour les courbes sur un corps fini est la suivante :

Théorème 1.1. *Soit $f(x, y)$ un polynôme irréductible à coefficient entiers. Pour chaque nombre premier p, notons $N_p(f)$ le nombre de solutions des congruences $f(x, y) \equiv 0 \bmod p$. Il existe un entier A ne dépendant que de f tel que*

$$|N_p(f) - p| \leqslant A\sqrt{p}.$$

Notons que cet énoncé implique en particulier que pour p assez grand (ici $p > A^2$ suffit) on aura une solution $f(x, y) \equiv 0 \bmod p$. Le véritable énoncé précis demande un peu plus de vocabulaire ; on pourra trouver en appendice une description des notions assez intuitives de « courbe algébrique » ainsi que celle de ses qualités éventuelles « lisse » ou « projective » et une brève présentation de la théorie des « diviseurs » sur une courbe algébrique.

Théorème 1.2 **(Hypothèse de Riemann pour les courbes sur les corps finis)**

Soit C une courbe algébrique lisse et projective, définie sur un corps fini $\mathbb{F}_q$. Il existe un entier $g \geqslant 0$ appelé le genre *de C et des entiers algébriques $\alpha_1, \ldots, \alpha_{2g}$ de module $|\alpha_i| = \sqrt{q}$ tels que, pour tout entier $m \geqslant 1$,*

$$\#C(\mathbb{F}_{q^m}) = q^m + 1 - \left(\alpha_1^m + \cdots + \alpha_{2g}^m\right).$$

En particulier, on a l'inégalité

$$|\#C(\mathbb{F}_{q^m}) - q^m - 1| \leqslant 2gq^{m/2}.$$

L'énoncé dit d'une certaine façon que le nombre de points rationnels d'une courbe algébrique sur $\mathbb{F}_q$ est proche du nombre de points de la droite projective sur $\mathbb{F}_q$, c'est-à-dire $q + 1$. Le lien avec l'énoncé précédent est le suivant : toute courbe algébrique, comme par exemple la courbe définie par $f(x, y) = 0$, est comparable à une courbe lisse et projective et la différence entre leurs nombres de points rationnels est bornée par une constante ne dépendant que de la géométrie. Il nous reste à expliquer pourquoi cet énoncé s'appelle « hypothèse de Riemann ».

La fonction zêta de Riemann est définie dans le demi-plan $\mathrm{Ré}\, s > 1$ par une série de Dirichlet ou un produit eulérien

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s} = \prod_p (1 - p^{-s})^{-1}.$$

L'égalité entre la série et le produit (où p parcourt l'ensemble des nombres premiers) est une version analytique de l'unicité de la décomposition en facteurs premiers.

Pour énoncer le théorème suivant on utilise la fonction $\Gamma(s)$ d'Euler, qui est définie pour $\mathrm{Ré}(s) > 0$ par l'intégrale

$$\Gamma(s) := \int_0^\infty e^{-t} t^{s-1} dt$$

et prolongée au plan complexe via l'identité $\Gamma(s+1) = s\Gamma(s)$.

***Théorème 1.3* (Riemann).** *Les principales propriétés de la fonction $\zeta(s)$ (dont la dernière est conjecturale) sont :*

(1) *(Prolongement analytique) La fonction $\zeta(s)$ se prolonge en une fonction méromorphe sur le plan complexe ayant un unique pôle simple en $s = 1$, de résidu égal à 1.*

(2) *(Équation fonctionnelle) Introduisons la fonction zêta « complétée » : $\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$, elle vérifie l'équation fonctionnelle :*

$$\xi(1-s) = \xi(s).$$

(3) *(Hypothèse de Riemann) Les zéros de $\xi(s)$ sont situés sur la droite $\mathrm{Ré}(s) = 1/2$.*

Notons que la fonction $\zeta(s)$ ne s'annule pas dans le demi-plan de convergence du produit eulérien $\mathrm{Ré}\, s > 1$ et, au vu de l'équation fonctionnelle et des pôles de la fonction $\Gamma(s)$, possède comme uniques zéros dans le demi-plan $\mathrm{Ré}\, s < 0$ des zéros simples en $-2n$ (pour $n \geqslant 1$ entier). Les zéros situés dans la bande critique $0 \leqslant \mathrm{Ré}\, s \leqslant 1$ sont les mêmes que ceux de $\xi(s)$ et sont situés symétriquement par rapport à la droite critique $\mathrm{Ré}\, s = 1/2$. Rappelons que l'hypothèse de Riemann est considérée comme l'un des problèmes ouverts majeurs en mathématiques. Le succès de la fonction zêta de Riemann, notamment dans l'étude de la répartition des nombres premiers (voir à ce sujet [**Bos2003**]) a stimulé les mathématiciens pour introduire d'autres fonctions zêta dans d'autres contextes.

L'analogue pour une courbe C définie sur $\mathbb{F}_q$ s'écrit en introduisant l'ensemble des points *fermés* $|C|$, c'est-à-dire les classes de conjugaison sous le groupe de Galois des points de $C(\overline{\mathbb{F}}_q)$. Pour un point fermé $x \in |C|$, son corps résiduel $\kappa(x)$ est le corps engendré par les coordonnées d'un de ses représentants et on note $N(x) := \#\kappa(x)$. On pose alors

$$\zeta_C(s) = \prod_{x \in |C|} (1 - N(x)^{-s})^{-1}.$$

On montre (c'est un calcul essentiellement formel donné ci-dessous) que

$$\zeta_C(s) = Z(C, q^{-s}),$$

où la série formelle $Z(C,T)$ peut être décrite par

$$\begin{aligned} Z(C/\mathbb{F}_q, T) &= \prod_D (1 - T^{\deg D})^{-1} \\ &= \exp\Big(\sum_{m=1}^{\infty} \frac{\#C(\mathbb{F}_{q^m})}{m} T^m \Big) = \sum_{n=0}^{\infty} A_n T^n, \end{aligned}$$

où D parcourt l'ensemble des diviseurs effectifs irréductibles sur $\mathbb{F}_q$ et A_n désigne le nombres de diviseurs effectifs de degré n définis sur $\mathbb{F}_q$.

Pour vérifier ces formules, introduisons les notations suivantes : $N_m := \#C(\mathbb{F}_{q^m})$ et Φ_m désigne le nombre de diviseurs définis sur $\mathbb{F}_q$, irréductibles de degré m. On a alors

$$Z(C,T) = \prod_{m=1}^{\infty} (1 - T^m)^{-\Phi_m}.$$

En écrivant une partition de l'ensemble $C(\mathbb{F}_{q^m})$ suivant le degré du corps engendré sur $\mathbb{F}_q$ par un point et en remarquant que ce degré doit diviser m, on obtient la formule

$$N_m = \sum_{n \,|\, m} n\Phi_n.$$

On en déduit la deuxième expression de $Z(C,T)$:

$$\begin{aligned} \log Z(C,T) &= \sum_{n=1}^{\infty} \Phi_n \Big(\sum_{h=1}^{\infty} \frac{T^{nh}}{h} \Big) \\ &= \sum_{m=1}^{\infty} \Big(\sum_{n \,|\, m} n\Phi_n \Big) \frac{T^m}{m} = \sum_{m=1}^{\infty} \frac{N_m}{m} T^m \end{aligned}$$

Ensuite, si l'on développe le produit on obtient la dernière formule :

$$\begin{aligned} \prod_D (1 - T^{\deg D})^{-1} &= \prod_D \Big(\sum_{m=0}^{\infty} T^{m \deg D} \Big) \\ &= \sum_{n=0}^{\infty} \Big(\sum_{m_1 \deg D_1 + \cdots + m_r \deg D_r = n} 1 \Big) T^n = \sum_{n=1}^{\infty} A_n T^n. \end{aligned}$$

Exemples 1.4. Dans le cas $C = \mathbb{P}^1$ on vérifie aisément que

$$\#\mathbb{P}^1(\mathbb{F}_{q^m}) = \frac{q^{2m}-1}{q^m-1} = q^m + 1$$

et donc :

$$Z(\mathbb{P}^1/\mathbb{F}_q, T) = \exp\Big(\sum_{m=1}^{\infty}(q^m+1)\frac{T^m}{m}\Big) = \frac{1}{(1-T)(1-qT)}.$$

On utilise pour cela la formule élémentaire

$$\exp\Big(\sum_{m=1}^{\infty}\frac{T^m}{m}\Big) = \frac{1}{1-T}.$$

Dans le cas d'une courbe elliptique (c'est-à-dire quand $g(C) = 1$), Hasse a montré que la fonction zêta prend la forme

$$Z(C/\mathbb{F}_q, T) = \frac{1-aT+qT^2}{(1-T)(1-qT)},$$

où a est un entier vérifiant $|a| \leqslant 2\sqrt{q}$. Plus précisément $1-aT+qT^2 = (1-\alpha T)(1-\overline{\alpha}T)$ avec $|\alpha| = \sqrt{q}$. La contribution de Weil est la démonstration de l'analogue de ces énoncés pour une courbe de genre $g \geqslant 2$.

Observons que, si $g = 1$, on a

$$\#C(\mathbb{F}_q) \geqslant q + 1 - 2\sqrt{q} = (\sqrt{q}-1)^2 > 0,$$

donc une courbe de genre 0 ou 1 possède toujours un point $\mathbb{F}_q$-rationnel.

Cependant l'existence d'un diviseur de degré 1 n'implique pas l'existence d'un point rationnel de degré 1 lorsque $g \geqslant 2$. L'inégalité de Weil

$$\#C(\mathbb{F}_q) \geqslant q + 1 - 2g\sqrt{q}$$

garantit l'existence d'un point $\mathbb{F}_q$-rationnel si q est assez grand, par exemple si $q \geqslant 4g^2 - 1$. Donnons des exemples de courbes de genre 2 ne possédant aucun point $\mathbb{F}_q$-rationnel. Quand la caractéristique p n'est pas égale à 2, on peut choisir une courbe définie par l'équation affine $y^2 = f(x) = f_6x^6 + \cdots + f_0$. La courbe possède deux points à l'infini ; ils sont $\mathbb{F}_q$-rationnels si et seulement si f_6 est un carré. Soit a un non carré et soit

$$f(x) = a(x^6 + \cdots + xa_1) + a = ag(x) + a,$$

où g est tel que pour tout $x \in \mathbb{F}_q$ on ait $g(x) = 0$ (loisible pour $q = 3$ ou 5). Alors la courbe $y^2 = f(x)$ n'a aucun point rationnel.

Pour $q = 7$, considérons

$$y^2 = 3(1 - (x^2 - 1)(x^2 - 2)(x^2 - 4)) = f(x).$$

Puisque $f(x) = 3 \notin \mathbb{F}_7^{*2}$ (ensemble des carrés dans le groupe multiplicatif du corps $\mathbb{F}_7$) pour $x \neq 0$ et $f(0) = 6 \notin \mathbb{F}_7^{*2}$, on voit que $C(\mathbb{F}_7) = \varnothing$.

On peut construire un exemple similaire pour $q = 9$ en choisissant $f(x)$ unitaire de degré 6 tel que $f(x) \in \mathbb{F}_9^{*2}$ pour $x \in \mathbb{F}_9$, et on considère alors la courbe d'équation $ay^2 = f(x)$ avec a non carré. Choisissons α tel que $\alpha^2 = -1 \in \mathbb{F}_3$. On a alors $\mathbb{F}_9 = \{0, \pm 1, \pm\alpha, \pm\alpha \pm 1\}$ et $\mathbb{F}_9^{*2} = \{\pm 1, \pm\alpha\}$, et si on choisit $f(x) = x^6 - x^4 + x^2 + 1$ on a $f(\pm 1) = -1$, $f(\pm\alpha) = 1$ et $f(\pm\alpha \pm 1) = -1$, donc la courbe $y^2 = (\alpha + 1)f(x)$ n'a aucun point rationnel sur $\mathbb{F}_9$.

Dans le cas de caractéristique 2, il faut procéder un peu différemment. Considérons la courbe affine $f_4(x, y) + f_3(x, y) + f_2(x, y) = 0$ avec f_i homogène de degré i ; le point $P_0 = (0, 0)$ est singulier double ordinaire et les deux tangentes ne sont rationnelles que si $f_2(x, y)$ se factorise sur $\mathbb{F}_q$; les points à l'infini sont donnés par $Z = 0$, $f_4(X, Y) = 0$ avec $(X, Y) \neq (0, 0)$). Si P_0 est le seul point singulier, alors $g = 2$. Par exemple

$$X^4 + YX^3 + Y^4 + Z(X^3 + YX^2 + Y^3) + Z^2(X^2 + XY + Y^2) = 0,$$

correspond à une courbe de genre 2 avec $C(\mathbb{F}_2) = \varnothing$.

Remarque 1.5. Pour illustrer la différence entre l'existence d'un point $\mathbb{F}_q$-rationnel, garantie seulement si q est assez grand par rapport à g, et l'existence d'un diviseur de degré 1 défini sur $\mathbb{F}_q$, considérons la courbe de genre 2 sur $\mathbb{F}_3$ d'équation affine $y^2 = -(x^3 - x)^2 - 1$. Cette courbe n'a aucun point rationnel sur $\mathbb{F}_3$; néanmoins, si α_1, α_2 désignent les racines de $y^2 = -1$, le diviseur $D_1 := (0, \alpha_1) + (0, \alpha_2)$ est défini sur $\mathbb{F}_3$ tandis que, si β_1, β_2, β_3 désignent les racines de $x^3 - x = -1$, le diviseur $D_2 := (\beta_1, 1) + (\beta_2, 1) + (\beta_3, 1)$ est défini sur $\mathbb{F}_3$. Ainsi $D := D_2 - D_1$ est un diviseur de degré 1 défini sur $\mathbb{F}_3$.

On peut reformuler l'hypothèse de Riemann en terme de la fonction $Z(C/\mathbb{F}_q, T)$ ainsi :

Théorème 1.6 **(Hypothèse de Riemann pour les courbes sur les corps finis)**

Soit C une courbe algébrique lisse et projective, définie sur un corps fini $\mathbb{F}_q$. Il existe un entier $g \geqslant 0$ appelé le genre *de C et des entiers algébriques $\alpha_1, \ldots, \alpha_{2g}$ de module $|\alpha_i| = \sqrt{q}$ tels que*

$$Z(C/\mathbb{F}_q, T) = \frac{(1-\alpha_1 T)\ldots(1-\alpha_{2g}T)}{(1-T)(1-qT)}.$$

De plus la fonction zêta vérifie l'équation fonctionnelle :

$$Z(C/\mathbb{F}_q, T) = q^{g-1}\, T^{2g-2}\, Z\Big(C/\mathbb{F}_q, \frac{1}{qT}\Big). \tag{1}$$

Si l'on revient à la définition initiale de la fonction $\zeta_C(s)$, on voit que l'énoncé donne un prolongement méromorphe au plan complexe (avec des pôles simples en $s = 2i\pi/\log q$ et $s = 1 + 2i\pi/\log q$, une équation fonctionnelle $\zeta_C(s) = q^{(2g-2)(s-1/2)}\zeta_C(1-s)$ et l'affirmation sur le module des nombres α_i équivaut à dire que $\zeta_C(s) = 0$ implique $\mathrm{Ré}\, s = 1/2$, ce qui est bien l'analogue de l'hypothèse de Riemann.

Remarque 1.7. Si l'on sait déjà que $|\alpha_j|^2 = \alpha_j \overline{\alpha}_j = q$, on peut en déduire que, si α est une racine réciproque du numérateur de la fonction zêta, alors q/α également. Si l'on ne connait pas encore l'hypothèse de Riemann, l'équation fonctionnelle de la fonction zêta permet de retrouver que la transformation $\alpha \mapsto q/\alpha$ échange les racines réciproques.

Remarque 1.8. Soit $\alpha_1, \ldots, \alpha_{2g}$ les entiers algébriques associés à la courbe C par le théorème 1.2 ou 1.6 ; introduisons les polynômes symétriques $\sigma_i = \sigma_i(\alpha_1, \ldots, \alpha_{2g})$ et les sommes $S_i = \alpha_1^i + \cdots + \alpha_{2g}^i$. Posons en outre $N_i := \#C(\mathbb{F}_q)$; la connaissance de $N_1, \ldots, N_g$ équivaut à celle de $S_1, \ldots, S_g$ et, par les formules de Newton, à celle de $\sigma_1, \ldots, \sigma_g$ qui, par l'équation fonctionnelle, donne celle de $\sigma_1, \ldots, \sigma_{2g}$. Ainsi pour calculer $Z(C/\mathbb{F}_q, T)$ on a seulement besoin de connaître $N_1, \ldots, N_g$.

2. Variantes et exemples

Il est traditionnel d'appeler borne de Hasse-Weil l'inégalité :

$$\left|\#C(\mathbb{F}_q) - \#\mathbb{P}^1(\mathbb{F}_q)\right| \leqslant [2g\sqrt{q}\,], \tag{2}$$

On peut, dans certains cas, légèrement l'améliorer : tout d'abord le lemme ci-dessous montre qu'on peut écrire :

$$\left|\#C(\mathbb{F}_q) - \#\mathbb{P}^1(\mathbb{F}_q)\right| \leqslant g\,[2\sqrt{q}\,], \tag{3}$$

Cette inégalité parfois appelée borne de Hasse-Weil-Serre [**Ser1983**] améliore l'inégalité (2) lorsque q n'est pas un carré.

Lemme 2.1. *Soit $S = \{\alpha_1, \ldots, \alpha_s\}$ un ensemble d'entiers algébriques stable par action du groupe de Galois sur $\mathbb{Q}$ et tels que α_i vérifie $|\alpha_i| = p^{w/2}$ avec w impair. Alors s est pair et*

$$|\alpha_1 + \cdots + \alpha_s| \leqslant \frac{s}{2}\left[2p^{w/2}\right].$$

Démonstration. Si α_i est réel alors $\alpha_i = \pm p^{w/2}$ et $-\alpha_i$ est conjugué avec α_i qui appartient donc à S, les autres éléments peuvent être groupés deux par deux avec leurs conjugués complexes, donc s est pair, disons $s = 2t$. Puisque $p^{w/2}$ et $-p^{w/2}$ ont une somme nulle, on peut supposer qu'aucun α_i n'est réel et écrire $S = T \cup \overline{T}$ avec $T = \{\alpha_1, \ldots, \alpha_t\}$. Posons $m := [2p^{w/2}]$ et $x_i := m + 1 + \alpha_i + \overline{\alpha}_i$, alors les x_i sont des entiers algébriques réels positifs et forment un ensemble stable sous Galois donc le produit $x_1 \cdots x_t$ est un entier positif donc $\geqslant 1$. En utilisant l'inégalité de la moyenne arithmétique-géométrique on obtient

$$\frac{1}{t}\sum_{i=1}^{t} x_i \geqslant \sqrt[t]{x_1 \ldots x_t} \geqslant 1,$$

et donc $tm + \sum_{i=1}^{s} \alpha_i \geqslant 0$. En remplaçant α_i par $-\alpha_i$ on obtient deux inégalités qui prouvent le lemme. □

Une autre technique est celle dite des « formules explicites ». Écrivons

$$L(C,T) = \prod_{j=1}^{g}(1 - \sqrt{q}\,e^{i\theta_j}T)(1 - \sqrt{q}\,e^{-i\theta_j}T).$$

Pour un polynôme trigonométrique $f(\theta) = 1 + 2\sum_{n\geqslant 1} c_n \cos(n\theta)$, posons $\psi_d(t) = \psi_{f,d}(t) = \sum_{n\geqslant 1} c_{dn} t^{dn}$. À partir de

$$2\sum_{j=1}^{g} \cos(m\theta_j) = \sum_{j=1}^{2g} \alpha_j^m q^{-m/2} = -N_m q^{-m/2} + q^{-m/2} + q^{m/2}$$
$$= -\sum_{d\,|\,m} d\Phi_d q^{-m/2} + q^{-m/2} + q^{m/2},$$

qu'on multiplie par c_m, on obtient en sommant la formule explicite suivante :

$$\sum_{j=1}^{g} f(\theta_j) + \sum_{d\geqslant 1} d\,\Phi_d\,\psi_d(q^{-1/2}) = g + \psi_1(q^{-1/2}) + \psi_1(q^{1/2}).$$

Si on choisit f de sorte que $c_n \geqslant 0$ et $f(\theta) \geqslant 0$, on peut minorer le membre de gauche par $N_1\psi_1(q^{-1/2}) = \Phi_1\psi(q^{-1/2})$ et en tirer

$$N_1 \leqslant 1 + \frac{g + \psi_1(q^{1/2})}{\psi_1(q^{-1/2})}.$$

Ainsi, par exemple en choisissant

$$f(\theta) = 1 + \sqrt{2}\cos(\theta) + \frac{\cos(2\theta)}{2} = \frac{(1+\sqrt{2}\cos\theta)^2}{2},$$

c'est-à-dire

$$c_1 = \frac{1}{\sqrt{2}}, \quad c_2 = \frac{1}{4} \quad \text{et} \quad \psi_1(t) = \frac{t}{\sqrt{2}} + \frac{t^2}{4},$$

on obtient, lorsque $g \leqslant q^{3/2} - q^{1/2}/\sqrt{2}$, l'inégalité

$$N \leqslant q^2 + 1,$$

qui bien sûr n'améliore l'inégalité de Weil que si

$$\frac{q^{3/2} - q^{1/2}}{2} < g \leqslant \frac{q^{3/2} - q^{1/2}}{\sqrt{2}},$$

c'est-à -dire quand g est grand devant q mais pas trop.

Exemple 2.2. Pour $g = 6$ et $q = 5$,

- l'inégalité de Weil donne $N_1 \leqslant 5 + 1 + [12\sqrt{5}\,] = 32$,
- l'inégalité de Weil améliorée donne $N_1 \leqslant 5 + 1 + 6[2\sqrt{5}\,] = 30$
- et la formule explicite précédente donne $N_1 \leqslant 5^2 + 1 = 26$.

Exemple 2.3. Supposons $p \neq 3$ et $a_1a_2a_3 \neq 0$. Considérons la cubique plane C sur $\mathbb{F}_p$ d'équation :

$$a_1X^3 + a_2Y^3 + a_3Z^3 = 0.$$

C'est une courbe elliptique : elle est de genre 1 et, comme nous l'avons vu, elle possède nécessairement un point $\mathbb{F}_p$-rationnel. Lorsque $p \equiv 2 \bmod 3$, l'application $x \mapsto x^3$ est une bijection de $\mathbb{F}_p$ donc $\#C(\mathbb{F}_p) = \#\mathbb{P}^1(\mathbb{F}_p) = p+1$ et l'on peut conclure

$$Z(C/\mathbb{F}_p, T) = \frac{1+pT^2}{(1-T)(1-pT)}.$$

Le cas $p \equiv 1 \bmod 3$ est plus subtil mais peut être décrit explicitement ainsi (voir par exemple [**Hin2008, Gol2002**]). Pour $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$ un caractère de Dirichlet, on définit une *somme de Gauss*

$$G(\chi) = \sum_{u \in \mathbb{F}_p} \chi(u) \exp(2\pi i u/p)$$

et une *somme de Jacobi*

$$J(\chi) = \sum_{u \in \mathbb{F}_p} \chi(u)\chi(1-u).$$

Proposition 2.4. *Soit χ un caractère d'ordre 3. La somme de Jacobi $J(\chi)$ est un entier algébrique de module $\sqrt{p}$. On a*

$$Z(C/\mathbb{F}_p, T) = \frac{1-aT+pT^2}{(1-T)(1-pT)},$$

avec

$$a := -\overline{\chi}(a_1a_2a_3)J(\chi) - \chi(a_1a_2a_3)J(\overline{\chi}).$$

Posons $D := a_1a_2a_3$, pour $p = 7$ on trouve

$$Z(C/\mathbb{F}_7, T) = \frac{1-aT+7T^2}{(1-T)(1-7T)} = \frac{(1-\alpha T)(1-\overline{\alpha}T)}{(1-T)(1-7T)},$$

avec

$$a := \begin{cases} 1 & \text{si } D = \pm 1 \\ -4 & \text{si } D = \pm 3 \\ 5 & \text{si } D = \pm 2 \end{cases} \quad \text{et, respectivement,} \quad \alpha = \begin{cases} \dfrac{1+i3\sqrt{3}}{2} \\ -2+i\sqrt{3} \\ \dfrac{5+i\sqrt{3}}{2} \end{cases}$$

Exemple 2.5. Considérons la courbe d'équation affine $y^q + y = x^{q+1}$ sur $\mathbb{F}_q$ ou encore comme courbe plane projective

$$C := \left\{(X, Y, Z) \in \mathbb{P}^2 \mid ZY^q + Z^qY - X^{q+1} = 0\right\}.$$

Le genre de C est $g = q(q-1)/2$ et il y a un unique point à l'infini, de coordonnées homogènes $(0, 1, 0)$. Pour les points sur $\mathbb{F}_q$ on observe que $x^q = x$ et $y^q = y$, donc il y a q points sur la courbe affine. Pour les points sur $\mathbb{F}_{q^2}$ notons que l'application trace de $\mathbb{F}_{q^2}$ vers $\mathbb{F}_q$ est $\mathbb{F}_q$-linéaire surjective et définie par $T(y) = y^q + y$, tandis que l'application norme de $\mathbb{F}_{q^2}^*$ vers $\mathbb{F}_q^*$ est un homomorphisme surjectif de groupes et définie par $N(y) = x^{q+1}$. L'ensemble des points de $C(\mathbb{F}_{q^2})$ est donné par le point à l'infini, les points $(0, y)$ tels que $y^q + q = 0$ (soit q points) et enfin la réunion, pour $t \in \mathbb{F}_q^*$, des ensembles $\{(x, y) \mid x^{q+1} = t = y^q + y\}$, soit $(q-1)(q+1)q$ points, et on peut conclure :

$$N_1 = q + 1 \quad \text{et} \quad N_2 = q^3 + 1.$$

Remarquons que la borne de Hasse-Weil s'écrit $N_2 \leqslant q^2 + 1 + 2gq = q^3 + 1$, donc la courbe est maximale sur $\mathbb{F}_{q^2}$.

Exemple 2.6. Considérons la quartique de Klein sur $\mathbb{F}_2$:

$$C := \left\{(X, Y, Z) \in \mathbb{P}^2 \mid ZY^3 + Z^3X + X^3Y = 0\right\}.$$

Le genre de C est $g = 3$. On voit aisément que

$$C(\mathbb{F}_2) = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\};$$

considérant l'automorphisme $\sigma(X, Y, Z) = (Y, Z, X)$ d'ordre 3, on voit qu'il possède deux points fixes $(j, j^2, 1)$, où $j^2 + j + 1 = 0$, tous deux rationnels sur $\mathbb{F}_4$; on a donc $N_2 \geqslant 5$ et $N_2 \equiv 2 \bmod 3$. Soit maintenant $\mu \in \mathbb{F}_8^*$ un générateur (une racine 7-ième de l'unité), l'automorphisme $\phi(X, Y, Z) = (X, \mu^3 Y, \mu Z)$ est d'ordre 7 et possède comme points fixes les trois points de $C(\mathbb{F}_2)$ donc $N_3 \equiv 3 \bmod 7$. Ces remarques aident à déterminer :

$$N_1 = 3, \quad N_2 = 5 \quad \text{et} \quad N_3 = 24$$

et, après calculs :

$$Z(C/\mathbb{F}_2, T) = \frac{1 + 5T^3 + 8T^6}{(1 - T)(1 - 2T)}.$$

Remarquons que la borne de Hasse-Weil s'écrit $N_3 \leqslant 8+1+[6\sqrt{8}\,] = 25$, tandis que la borne de Hasse-Weil-Serre s'écrit $N_3 \leqslant 8+1+3[2\sqrt{8}\,] = 24$, donc la courbe est maximale sur $\mathbb{F}_8$.

3. Généralisations et applications

Les conjectures de Weil [**Wei1949**] décrivent une vaste généralisation du théorème 1.6 pour les variétés de dimension quelconque, mais toujours projective et lisse ; leur démonstration, achevée dans les années soixante-dix a occupé pendant trente ans les géomètres. On pose ainsi pour une variété algébrique définie sur $\mathbb{F}_q$:

$$Z(V/\mathbb{F}_q, T) := \exp\Big(\sum_{m=1}^{\infty} \frac{\#V(\mathbb{F}_{q^m})}{m} T^m\Big).$$

Théorème 3.1 **(Conjectures de Weil, théorème de Grothendieck-Deligne)**

Soit V une variété algébrique projective et lisse de dimension n.

(1) *La série formelle $Z(V/\mathbb{F}_q, T)$ est une fraction rationnelle.*

(2) *La fonction $Z(V/\mathbb{F}_q, T)$ vérifie l'équation fonctionnelle suivante où $\varepsilon = \varepsilon_V = \pm 1$ et $\chi = \chi_V$ est un entier :*

$$Z\Big(V/\mathbb{F}_q, \frac{1}{q^n T}\Big) = \varepsilon\, q^{n\chi/2}\, T^{\chi}\, Z(V/\mathbb{F}_q, T)$$

(3) *(Hypothèse de Riemann) On peut écrire*

$$Z(V/\mathbb{F}_q, T) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)\cdots P_{2n}(T)},$$

avec $P_0(T) = 1 - T$ et $P_{2n}(T) = 1 - q^n T$ et

$$P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{i,j} T) \quad \text{et} \quad |\alpha_{i,j}| = q^{i/2}.$$

(4) *Les degrés b_i des polynômes P_i peuvent être calculés purement « topologiquement » de même que $\chi = \sum_{i=0}^{2n} (-1)^i b_i$.*

Remarque 3.2. En utilisant l'égalité

$$Z'(T)/Z(T) = \sum_{m \geqslant 1} \#V(\mathbb{F}_{q^m}) T^{m-1},$$

on peut traduire ces formules en une formule pour $\#V(\mathbb{F}_{q^m})$:

$$\#V(\mathbb{F}_{q^m}) = \sum_{i=0}^{2n}\sum_{j=1}^{b_i}(-1)^i\alpha_{i,j}^m = q^{nm} + \sum_{i=0}^{2n-1}(-1)^i\sum_{j=1}^{b_i}\alpha_{i,j}^m.$$

On voit en particulier que pour b_i fixés (ou bornés), la variété V possède un point $\mathbb{F}_q$-rationnel dès que q est assez grand.

Remarque 3.3. Dans le cas $V = \mathbb{P}^n$ on voit que

$$\#V(\mathbb{F}_{q^m}) = q^{mn} + q^{m(n-1)} + \cdots + q^m + 1$$

et

$$Z(\mathbb{P}^n/\mathbb{F}_q, T) = \frac{1}{(1-T)(1-qT)\dots(1-q^nT)}.$$

Ainsi on peut directement vérifier l'équation fonctionnelle avec $\varepsilon = (-1)^{n+1}$ et $\chi = n+1$. Dans le cas d'une courbe de genre g, notons que $\varepsilon = +1$ et $\chi = 2-2g$; on peut trouver d'autres exemples élémentaires dans [**Hin2008**].

Remarque 3.4. La signification du dernier point du théorème 3.1 est une généralisation de la notion de genre (voir [**Pop2012**] pour un bel historique et un panorama de la notion de genre). Du point de vue de la topologie, une courbe lisse projective sur $\mathbb{C}$ est une surface (sic) de Riemann et son genre est le nombre de trous de la surface de Riemann. En dimension supérieure, on peut associer à une variété lisse projective V de dimension n sur $\mathbb{C}$, l'espace topologique $V(\mathbb{C})$ et ses « nombres de Betti » $B_i(V(\mathbb{C}))$, qui généralisent le genre, par exemple pour une courbe $B_1 = 2g$, ainsi que sa « caractéristique d'Euler-Poincaré » $\chi(V(\mathbb{C})) := \sum_{i=0}(-1)^i B_i(V(\mathbb{C}))$. Le point 4 du théorème 3.1 signifie que les b_i obtenus en caractéristique p sont égaux aux B_i issus de la topologie. On est ainsi témoin d'une grandiose unification de l'arithmétique, de la géométrie et de la topologie, à laquelle Weil rêvait souvent. La topologie est en effet sous-jacente à la preuve des conjectures de Weil, via notamment la formule de Lefschetz comptant le nombre de points fixes d'une application (ici le « Frobenius »), la dualité de Poincaré (qui explique l'équation fonctionnelle), la formule de Künneth, etc.

L'hypothèse de Riemann originale est intimement liée à la distribution des nombres premiers et implique notamment des inégalités

comme

$$\Big|\sum_{p\leqslant x}\log p - x\Big| \leqslant c\,\sqrt{x}\,(\log x)^2.$$

Une des applications les plus fréquentes à la théorie analytique des nombres de l'hypothèse de Riemann sur les corps finis est la majoration de sommes d'exponentielles de la forme, pour un polynôme F dans $\mathbb{Z}[X_1,\dots,X_n]$ ou $\mathbb{F}[X_1,\dots,X_n]$,

$$S := \sum_{x\in\mathbb{F}_p^n} \exp\Big(\frac{2\pi i F(x)}{p}\Big).$$

On peut majorer trivialement cette somme par $|S| \leqslant p^n$, mais le caractère oscillatoire des termes de la somme suggère que des majorations beaucoup plus précises doivent être possibles. L'exemple historiquement et théoriquement très important est celui de la somme de Gauss :

$$S(a) := \sum_{x\in\mathbb{F}_p} \exp\Big(\frac{2\pi i a x^2}{p}\Big).$$

On montre en effet classiquement que pour $a \not\equiv 0 \bmod p$ on a $|S(a)| = \sqrt{p}$. L'hypothèse de Riemann pour les courbes permet de montrer par exemple que, pour $f(x)$ séparable de degré d, on a

$$\Big|\sum_{x\in\mathbb{F}_p} \exp\Big(\frac{2\pi i f(x)}{p}\Big)\Big| \leqslant C_d\sqrt{p}.$$

L'étude des bornes pour les sommes d'exponentielles est encore aujourd'hui source de recherches très actives.

Les codes correcteurs (linéaires) ont été développés pour résoudre un problème très concret : lors de la transmission d'informations, de messages par téléphone, onde ou voie électronique, il peut arriver qu'une partie du message soit altéré (interférences, bruits, etc), on souhaite donc développer des techniques permettant de reconstituer autant que faire ce peut le message original. Les codes correcteurs linéaires sont parmi les plus utilisés et performants, ils sont par exemple utilisés dans la technique du compact disc. On écrit les messages avec un alphabet (en bijection avec) $\mathbb{F}_q$, c'est-à-dire des mots de disons $\mathbb{F}_q^k$; un « code linéaire » est un sous-espace vectoriel $\mathscr{C}$ de $\mathbb{F}_q^n$ muni d'un isomorphisme $\lambda : \mathbb{F}_q^k \cong \mathscr{C} \subset \mathbb{F}_q^n$. Au lieu d'envoyer $x \in \mathbb{F}_q^k$, on envoie $\lambda(x) \in \mathbb{F}_q^n$. Si l'on reçoit un message $x' \notin \mathscr{C}$ on sait qu'il

a été altéré et le procédé le plus simple pour le reconstituer est de remplacer x' par le mot $x \in \mathscr{C}$ le plus proche. Pour donner un sens précis à cela on définit la « distance de Hamming » et le « poids » (*weight* en anglais) d'un élément :

$$d(x,y) := \#\{i \in [1,n] \mid x_i \neq y_i\} \quad \text{et} \quad w(x) := d(x,0).$$

La distance minimale d'un code est définie par

$$d(\mathscr{C}) := \min\{d(x,y) \mid x \neq y \in \mathscr{C}\} = \min\{w(x) \mid 0 \neq x \in \mathscr{C}\}.$$

On voit facilement que si disons $d = d(\mathscr{C})$ est impair, il sera possible de repérer $d-1$ erreurs et d'en corriger $(d-1)/2$. Une première évaluation (naïve mais efficace) montre que les paramètres les plus importants d'un code sont n, k, d et que la qualité d'un code peut s'apprécier en ce que le rapport $1 < n/k$ ne soit pas trop grand et d soit le plus grand possible.

Les codes de Goppa sont des codes linéaires liés aux courbes algébriques sur les corps finis ; ils peuvent être décrits succinctement, selon [**Gop1970, Sti1993**], en anticipant un peu sur des définitions données dans le paragraphe suivant. On choisit n points rationnels distincts $P_1, \ldots, P_n$ dans $C(\mathbb{F}_q)$, on notera $D = P_1 + \cdots + P_n$ le diviseur somme de ces points ; on choisit également G un diviseur défini sur $\mathbb{F}_q$ de support disjoint de D, on considère l'espace vectoriel $L(D)$ des fonctions ayant au plus des pôles en G et on pose

$$\mathscr{C} := \{(x(P_1), \ldots, x(P_n)) \mid x \in L(G)\}.$$

On démontre alors que $k := \dim \mathscr{C} = \dim L(G) - \dim L(G-D)$ et $d \geqslant n - \deg G$. Ce recours à la géométrie algébrique a permis de construire plusieurs des meilleures familles de codes connus. On notera que la taille du code, l'entier n, est bornée par le nombre de points dans $C(\mathbb{F}_q)$ donc par la borne de Hasse-Weil ; cette observation a stimulé un grand nombre de travaux à la recherche de courbes maximales (c'est-à-dire ayant le plus grand nombre de points pour un genre donné). C'est un bel exemple d'interaction fructueuse entre théorie et applications.

4. Le théorème de Riemann-Roch pour les courbes

Nous renvoyons à l'appendice pour les notions élémentaires sur les courbes et les corps finis.

Soit C une courbe (lisse et projective) sur un corps K. À toute fonction rationnelle f non nulle on peut associer son *diviseur* qui est la somme formelle de ses zéros (comptés avec multiplicité positive) et pôles (comptés avec multiplicité négative). Si $D = \sum n_P[P]$ est un diviseur sur la courbe on définit l'ensemble

$$L(D) := \{f \in K(C) \mid \operatorname{div}(f) + D \geqslant 0\} \cup \{0\}.$$

En utilisant la relation sur l'ordre des zéros et pôles

$$\operatorname{ord}_P(f_1 + f_2) \geqslant \min\left(\operatorname{ord}_P f_1, \operatorname{ord}_P f_2\right),$$

on voit que $L(D)$ est un espace vectoriel. On notera $\ell(D) = \dim L(D)$. Par ailleurs comme $\operatorname{div}(f_1 f_2) = \operatorname{div}(f_1) + \operatorname{div}(f_2)$, on voit que, si $D' = D + \operatorname{div}(f)$, la multiplication par f induit une bijection de $L(D')$ sur $L(D)$; en particulier $\ell(D') = \ell(D)$.

La première forme du théorème de Riemann-Roch (celle démontrée par Riemann sur le corps des nombres complexes) s'énonce ainsi :

Théorème 4.1 **(Riemann-Roch, forme « faible »).** *Soit C une courbe lisse et projective. Il existe un entier positif g, appelé le* genre *de la courbe et une constante c_1 tels que*

(1) *pour tout diviseur D, on a*

$$\ell(D) \geqslant \deg D - g + 1;$$

(2) *de plus, si $\deg D \geqslant c_1$, on a l'égalité*

$$\ell(D) = \deg D - g + 1.$$

La forme complète du théorème de Riemann-Roch s'énonce ainsi

Théorème 4.2 **(Riemann-Roch).** *Soit C une courbe lisse et projective. Il existe un entier positif g, appelé le* genre *de la courbe et un diviseur K_C appelé le* diviseur canonique *tels que pour tout diviseur D, on a*

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

Remarque 4.3. En prenant $D = 0$ dans l'énoncé, on voit que $\ell(K_C) = g$; en prenant ensuite $D = K_C$, on voit que $\deg K_C = 2g-2$. En particulier, comme $\ell(D) = 0$ lorsque $\deg D < 0$, on voit que, si

$\deg D \geqslant 2g-1$, alors $\ell(K_c - D) = 0$ et on conclut que la constante c_1 dans le théorème 4.1 peut être prise égale à $2g-1$.

Remarque 4.4. On peut décrire la classe de diviseur K_C comme la classe du diviseur d'une 1-forme différentielle sur la courbe. Par exemple la forme différentielle $\omega = dx$ n'a aucun zéro ou pôle sur l'ouvert $\mathbb{P}^1 \setminus \{\infty\}$ et quand on effectue le changement de variable $t = 1/x$, on voit $\omega = dx = -dt/t^2$ donc ω a un pôle d'ordre 2 au point ∞ et on a donc

$$\operatorname{div}(\omega) = -2[\infty].$$

On retrouve ainsi que le genre de $\mathbb{P}^1$ est zéro.

Si on considère la courbe elliptique d'équation affine $y^2 = x^3 + ax + b$ avec $\Delta = 4a^3 + 27b^2 \neq 0$, on peut introduire la 1-forme

$$\omega = \frac{dx}{2y} = \frac{dy}{3x^2 + a}$$

qui n'a ni zéro ni pôle dans la partie affine ; un calcul montre qu'elle n'a pas non plus de zéro ou pôle en le point à l'infini, autrement dit $\operatorname{div}(\omega) = 0$ et on retrouve que $g = 1$.

Exemple 4.5. Nous n'allons pas donner la démonstration générale mais vérifier le théorème de Riemann-Roch sur un exemple. Considérons la courbe d'équation affine $y^2 = h(x)$, où h est un polynôme séparable de degré $2g+1$; elle possède un unique point à l'infini que nous notons ∞. L'algèbre des fonctions ayant comme unique pôle le point ∞ est l'algèbre des polynômes en x, y ; on a $\operatorname{div}(x)_\infty = 2[\infty]$ et $\operatorname{div}(y)_\infty = (2g+1)[\infty]$; on en déduit qu'une base de $L(m(\infty))$ est donnée par :

$$\{x^i \mid 0 \leqslant i \leqslant m/2\} \cup \{yx^j \mid 0 \leqslant j \leqslant (m-2g-1)/2\}.$$

On vérifie directement que, lorsque $m \geqslant 2g-1$, on a $\ell(m(\infty)) = m + 1 - g$. Par ailleurs la forme différentielle dx/y n'a ni zéro ni pôle hors de ∞ et un calcul local montre qu'elle a un zéro d'ordre $2g-2$ en ∞ donc $K_C = (2g-2)[\infty]$ et on vérifie directement la formule de Riemann-Roch, c'est-à-dire que, pour $m \in [0, 2g-2]$, on a $\ell(m(\infty)) - \ell((2g-2-m)\infty) = m - g + 1$.

Le théorème de Riemann-Roch permet de démontrer que la fonction zêta est une fraction rationnelle (la forme faible suffit) et vérifie

l'équation fonctionnelle annoncée (la forme complète étant utilisée). On partira de l'expression

$$Z(T) = Z(C/\mathbb{F}_q, T) = \sum_{n=0}^{\infty} A_n T^n$$

avec $A_n := \#\{D \geqslant 0,\ D/\mathbb{F}_q,\ \deg D = n\}$. Notons h le nombre de classes de diviseurs de degré zéro[(1)] et récrivons la formule de Riemann-Roch pour une classe de diviseur c :

$$\ell(c) - \ell(K_C - c) = \deg(c) + 1 - g,$$

où K_C désigne la classe canonique.

Supposons qu'il existe une classe de diviseurs c_1 de degré 1 sur $C/\mathbb{F}_q$ (on peut montrer que ceci est toujours réalisé), alors l'ensemble des classes de diviseurs de degré n est en bijection avec l'ensemble des classes de diviseurs de degré 0 par l'application $c \mapsto c - nc_1$.

$$\begin{aligned} A_n = \sum_{\deg(c)=n} \frac{q^{\ell(c)} - 1}{q-1} &= \frac{1}{q-1}\left\{ \sum_{\deg(c)=n} q^{\ell(c)} - \sum_{\deg(c)=n} 1 \right\} \\ &= \frac{1}{q-1}\left\{ \sum_{\deg(c)=n} q^{\ell(c)} - h \right\}. \end{aligned}$$

De plus, si $\deg(c) > 2g-2$ on a

$$\sum_{\deg(c)=n} q^{\ell(c)} = q^{n+1-g} h$$

et donc

$$\begin{aligned} &Z(T) = Z(C/\mathbb{F}_q, T) \\ &= \frac{1}{q-1}\left\{ \sum_{\deg(c)\leqslant 2g-2} q^{\ell(c)} T^{\deg(c)} + h \sum_{n=2g-1}^{\infty} q^{n+1-g} T^n - h \sum_{n=0}^{\infty} T^n \right\}. \end{aligned}$$

Ainsi, si l'on pose

$$A(T) := \sum_{\deg(c)\leqslant 2g-2} q^{\ell(c)} T^{\deg(c)} \quad \text{et} \quad B(T) = \frac{q^g T^{2g-1}}{1-qT} - \frac{1}{1-T}$$

(1) Le nombre de classes est un invariant très intéressant ; il s'interprète comme le nombre de points rationnels de la *jacobienne* de la courbe.

on peut récrire

$$Z(T) = \frac{1}{q-1}\left\{A(T) + hB(T)\right\}.$$

Noter que $B(T)$ ne dépend que du genre. En particulier, on voit qu'il existe un polynôme $L(T) = L(C/\mathbb{F}_q, T) \in \mathbb{Z}[T]$ tel que

$$Z(T) = \frac{L(T)}{(1-T)(1-qT)}$$

avec $L(1) = h$ et $L(1/q) = hq^{-g+1}$. Utilisons la symétrie $c \leftrightarrow K_C - c$ en notant $c' := K_C - c$ de sorte que

$$\begin{aligned} \deg(c) &= 2g - 2 - \deg(c'), \\ \ell(c) &= \ell(c') + \deg(c) + 1 - g = \ell(c') - \deg(c') - 1 + g \end{aligned}$$

et remarquons que $c \mapsto c'$ est une bijection sur les classes qui satisfont à $0 \leqslant \deg(c) \leqslant 2g-2$; on obtient

$$A(T) = q^{g-1}T^{2g-2}A(1/qT). \tag{4}$$

Un calcul direct donne

$$B(T) = q^{g-1}T^{2g-2}B(1/qT). \tag{5}$$

En combinant les équations (4) et (5) on obtient l'équation fonctionnelle de $Z(T)$:

$$Z(T) = q^{g-1}T^{2g-2}Z(1/qT).$$

On tire aisément de cette équation fonctionnelle que $\deg(L(T)) = 2g$ et on peut écrire :

$$L(C/\mathbb{F}_q, T) = \prod_{j=1}^{2g}(1 - \beta_j T).$$

avec la propriété que la transformation $\beta \mapsto q/\beta$ induit une bijection sur $\beta_1, \ldots, \beta_{2g}$. On peut traduire cela en la formule :

$$\#C(\mathbb{F}_{q^m}) = q^m + 1 - \sum_{j=1}^{2g}\beta_j^m.$$

Ces résultats ont été prouvés par Artin et Schmidt. Il reste à prouver l'hypothèse de Riemann, c'est-à-dire que les β_j sont tous de module $\sqrt{q}$, ce qui a été fait par Hasse lorsque $g = 1$ puis par Weil

quand $g \geqslant 2$. Remarquons qu'il suffit de prouver pour tout j l'inégalité $|\beta_j| \leqslant \sqrt{q}$ car elle entraîne l'inégalité $|q/\beta_j| \leqslant \sqrt{q}$ et donc $|\beta_j| \geqslant \sqrt{q}$.

5. La preuve originale de Weil

Note historique. Comme nous l'avons rappelé en introduction, la preuve de Weil ([**Wei1940b, Wei1941**]) a suscité des polémiques puisqu'elle reposait sur un « lemme-clef » que Weil n'avait pas, à ce moment-là, démontré ; voir à ce propos la correspondance avec Henri Cartan [**Aud2011**]. Les deux notes reposent sur un énoncé de positivité en géométrie algébrique sur un corps fini dont l'analogue était connu de Weil sur le corps des complexes, mais dont la démonstration était de nature « transcendante », utilisant analyse holomorphe et topologie et donc non applicable directement. Nous présentons en fait la preuve de la note de 1941, basée sur l'inégalité de Castelnuovo.

La preuve de Weil requiert de travailler sur des variétés algébriques de dimension supérieure. La première version (la note de 1940) utilisait une variété de dimension g appelée *jacobienne* de la courbe, la deuxième version (la note de 1941) requiert seulement de travailler sur la surface $C \times C$. On définit un « diviseur » sur une surface comme une somme formelle à coefficients entiers de courbes ; le diviseur d'une fonction est la somme de ses zéros (comptés positivement) et de ses pôles (comptés négativement) ; on dit que deux diviseurs sont linéairement équivalents si leur différence est le diviseur d'une fonction.

Dans le plan projectif deux droites distinctes se rencontrent toujours en un point. Cet énoncé élémentaire peut être largement généralisé, tout d'abord avec le résultat suivant.

Théorème 5.1 **(Bézout).** *Soit C_1 et C_2 deux courbes (non nécessairement irréductibles) dans $\mathbb{P}^2$ de degré d_1 et d_2, n'ayant aucune composante commune, alors $C_1 \cap C_2$ est fini et le nombre de points de cette intersection, comptés avec multiplicité, est $d_1 d_2$.*

On peut ainsi définir une forme bilinéaire sur les paires de courbes de $\mathbb{P}^2$ qui à deux courbes C_1 et C_2 associe $C_1 \cdot C_2 := d_1 d_2$ et qui, quand

les courbes se coupent proprement, compte le nombre de points dans l'intersection ; notons que l'on doit donc définir $C \cdot C = (\deg C)^2$.

On peut généraliser ce procédé à toute surface S (lisse, projective) et associer à toute paire de diviseurs (courbes) D_1, D_2 leur « nombre d'intersection » $D_1 \cdot D_2$. Ces nombres sont invariants par déformation des diviseurs et, en particulier par équivalence linéaire, c'est-à-dire que pour toute fonction f et diviseur D sur la surface $D \cdot \mathrm{div}(f) = 0$; si D_1 et D_2 se coupent proprement, ils sont égaux au nombre de points d'intersection. Plongeons la surface S dans un espace projectif $\mathbb{P}^n$ et considérons l'intersection D de S avec un hyperplan de $\mathbb{P}^n$: il s'agit d'un diviseur qui a la particularité de rencontrer toutes les courbes tracées sur S ; un tel diviseur est appelé une section hyperplane ou diviseur très ample, un diviseur ample est tel qu'un multiple positif est très ample.

Lemme 5.2. *Soit H une section hyperplane sur une surface S. Lorsque D est un diviseur tel que $D \cdot H > 0$ et $D^2 > 0$, alors un multiple de D est linéairement équivalent à un diviseur positif.*

La preuve repose sur un théorème de Riemann-Roch pour les surfaces.

***Lemme 5.3* (Inégalité de Hodge).** *Soit H une section hyperplane et D un diviseur sur une surface S. Supposons $D \cdot H = 0$, alors on a*

$$D \cdot D = D^2 \leqslant 0. \tag{6}$$

Démonstration. Supposons que $D^2 > 0$. Introduisons $H_m := D + mH$, de sorte que, pour m assez grand le diviseur H_m est ample et l'on a $D \cdot H_m = D^2 > 0$ donc, d'après le lemme 5.2, un multiple de D est positif et en particulier $D \cdot H > 0$, ce qui contredit l'hypothèse. □

Remarque. Si D est un diviseur quelconque, posons

$$D_1 = (H^2)D - (D \cdot H)H.$$

On a clairement $D_1 \cdot H = 0$ et donc $D_1^2 \leqslant 0$, d'où l'on tire aisément l'inégalité en apparence plus générale

$$(D^2)(H^2) \leqslant (D \cdot H)^2.$$

Voici maintenant l'inégalité-clef utilisée par Weil.

***Lemme 5.4* (Inégalité de Castelnuovo).** *Soit C une courbe lisse projective et D un diviseur sur $C \times C$. Soit P un point de C, notons $F_1 := C \times \{P\}$ et $F_2 := \{P\} \times C$. Notons $d_1 := D \cdot F_1$ et $d_2 := D \cdot F_2$. On a alors*

$$D^2 = D \cdot D \leqslant 2d_1d_2. \tag{7}$$

Démonstration. Ce lemme se déduit du lemme 5.3. Commençons par observer que $F_1 \cdot F_2 = 1$ alors que $F_1 \cdot F_1 = F_2 \cdot F_2 = 0$. Dans le cas $S = C \times C$, on peut prendre $H = F_1 + F_2$. Introduisons $D_1 := D - d_2F_1 - d_1F_2$ alors on vérifie que

$$D_1 \cdot H = (D - d_2F_1 - d_1F_2) \cdot (F_1 + F_2) = 0.$$

On obtient donc

$$0 \geqslant D_1^2 = D^2 - 2d_2(D \cdot F_1) - 2d_1(D \cdot F_2) + 2d_1d_2(F_1 \cdot F_2) = D^2 - 2d_1d_2.$$

C'est exactement l'inégalité de Castelnuovo. □

Le nombre de points rationnels sur $\mathbb{F}_q$ d'une courbe C apparaît géométriquement comme le nombre de points fixes du Frobenius (voir le lemme 7.3 en appendice).

***Lemme 5.5* (Calcul de nombres d'intersection).** *Soit Γ le graphe du Frobenius $C \to C$ défini par « $x \mapsto x^q$ », soit Δ la diagonale de $C \times C$ et soit $N := \#C(\mathbb{F}_q)$ le nombre de points fixes du Frobenius et g le genre de C. On a les formules suivantes*

$$\begin{gathered} \Gamma \cdot \Delta = N, \quad \Delta^2 = 2 - 2g, \quad \Gamma^2 = q(2 - 2g), \\ \Gamma \cdot F_1 = q \quad \text{et} \quad \Gamma \cdot F_2 = 1. \end{gathered} \tag{8}$$

Démonstration. L'intersection du graphe Γ avec Δ est égale au nombre de points fixes du morphisme Frobenius donc au nombre de points définis sur $\mathbb{F}_q$. Comme Γ est un graphe, son nombre d'intersection avec F_2 est égal à 1 ; enfin le Frobenius est de degré q (le nombre d'antécédents d'un point est en général q) donc son nombre d'intersection avec F_1 est égal à q. Le calcul de l'auto-intersection de la diagonale est plus délicat, nous proposons de faire le calcul sur un exemple concret, la courbe hyperelliptique C d'équation affine $y^2 = h(x)$, où h est un polynôme séparable degré impair $2g + 1$.

L'entier g est bien le genre et la courbe possède un unique point à l'infini noté ∞ et, si l'on pose

$$Q_1 = (0, \sqrt{h(0)}), \quad Q_2 = (0, -\sqrt{h(0)}) \quad \text{et} \quad P_j = (a_j, 0)$$

(où a_j parcourt les zéros de h), on vérifie que

$$\operatorname{div}(x) = (Q_1) + (Q_2) - 2(\infty)$$

et surtout que, en posant $f(P,Q) = x(P) - x(Q)$, on a

$$\operatorname{div}(f) = \Delta + \Delta^- - 2(\infty) \times C - 2C \times (\infty),$$

où Δ^- est le graphe de l'involution $\iota(x,y) = (x,-y)$. On en tire

$$0 = \Delta \cdot \Delta + \Delta^- \cdot \Delta - 2\,((\infty) \times C) \cdot \Delta - 2\,(C \times (\infty)) \cdot \Delta.$$

Le nombre d'intersection de Δ et Δ^- est égal au nombre de points fixes de ι, c'est-à-dire $2g+2$ (les $2g+1$ points P_j et le point ∞),d'où le calcul $\Delta \cdot \Delta = 2 \cdot 2 + 2 \cdot 2 - (2g+2) = 2 - 2g$. Enfin on peut écrire le graphe Γ comme l'image réciproque de la diagonale par l'application $\Phi \times \mathrm{Id}_C : C \times C \to C \times C$ et on en déduit que

$$\Gamma \cdot \Gamma = \deg(\Phi \times \mathrm{Id}_C)\, \Delta \cdot \Delta = q\, \Delta \cdot \Delta = q(2-2g). \qquad \square$$

Appliquons ces formules au diviseur $D = r\Gamma + s\Delta$. On obtient :

$$d_1 = D \cdot F_1 = rq + s \quad \text{et} \quad d_2 = D \cdot F_2 = r + s.$$

L'inégalité de Castelnuovo s'écrit donc

$$D \cdot D = D^2 = r^2 q(2-2g) + 2rsN + s^2(2-2g) \leqslant 2(rq+s)(r+s),$$

d'où l'on tire

$$gqr^2 + (q+1-N)rs + gs^2 \geqslant 0.$$

Si l'on écrit que le discriminant de l'équation en r, s doit être négatif on obtient l'inégalité voulue :

$$|q+1-N| \leqslant 2g\sqrt{q}.$$

6. Une autre preuve en restant dans le monde des courbes

Vers la fin des années soixante, Stepanov [**Ste1969**] a introduit une méthode « élémentaire » (c'est-à-dire n'utilisant que le théorème de Riemann-Roch sur la courbe) aboutissant à une preuve de l'hypothèse de Riemann. La preuve a été simplifiée et complétée par Bombieri

[**Bom1973**] et nous allons présenter sa version. En préliminaire, remarquons que si C est définie sur $\mathbb{F}_q$ avec des nombres $\beta_1, \dots, \beta_{2g}$ associés, la courbe C' obtenue en étendant les scalaires à $\mathbb{F}_{q^r}$ est associée à $\beta'_j = \beta_j^r$ et $|\beta'_j| = q^{r/2}$ équivaut à $|\beta_j| = \sqrt{q}$. Ainsi on peut sans dommage remplacer $\mathbb{F}_q$ par $\mathbb{F}_{q^r}$ et en particulier supposer que q est grand.

Proposition 6.1. *Supposons que q soit un carré et soit suffisamment grand, par exemple $q > (g+1)^4$, alors*

$$\#C(\mathbb{F}_q) \leqslant q + 1 + (2g+1)\sqrt{q}.$$

Démonstration. Posons $N := \#C(\mathbb{F}_q)$ et $q = q_0^2$. On peut supposer que l'on a un point $Q \in C(\mathbb{F}_q)$. L'idée est de construire une fonction ayant un unique pôle d'ordre au plus H en $Q \in C(\mathbb{F}_q)$ et s'annulant à l'ordre disons T en chaque point de $C(\mathbb{F}_q) \smallsetminus \{x_0\}$; on aura alors $T(N-1) \leqslant H$ ou encore $N \leqslant 1 + H/T$.

Choisissons deux paramètres $m, n \geqslant 1$, que l'on optimisera ultérieurement, et posons

$$T := \{i \in [0, m] \mid \text{il existe } u_i \text{ avec } \operatorname{div}(u_i)_\infty = iQ\}$$

De plus, pour chaque $i \in T$ on choisit une fonction u_i.

Lemme 6.2. *L'ensemble $\{u_i \mid i \in T\}$ forme une base de $L(mQ)$. En particulier $\#T = \ell(mQ)$.*

Pour voir cela observons que $L((i-1)Q) \subset L(iQ)$ et que, ou bien on a égalité, ou bien il existe $u = u_i \in L(iQ)$ ayant un pôle d'ordre exactement i en Q et alors $L(iQ) = L((i-1)Q) \oplus \langle u_i \rangle$.

On introduit maintenant l'espace vectoriel

$$\begin{aligned} L &:= L(mQ) \cdot L(nQ)^{q_0} \\ &= \left\{ y = \sum_j x_j y_j^{q_0} \mid x_j \in L(mQ),\ y_j \in L(nQ) \right\}. \end{aligned}$$

Lemme 6.3. *L'espace L est un sous-espace vectoriel de $L\left((m + nq_0)Q\right)$. Si l'on suppose $m < q_0$, tout élément de $y \in L$ s'écrit de manière unique sous la forme*

$$y = \sum_{i \in T} u_i z_i^{q_0}$$

avec $z_i \in L(nQ)$. En particulier

$$\dim L = \#T \cdot \ell(nQ) = \ell(mQ) \cdot \ell(nQ).$$

Démonstration. La première partie est claire, de même que l'existence de l'écriture de y. Pour l'unicité, notons que, si l'on avait $0 = \sum_{i\in T} u_i z_i^{q_0}$ avec au moins un des $z_i \neq 0$, on en déduirait $\operatorname{ord}_Q(u_i z_i^{q_0}) = -i + q_0 \operatorname{ord}_Q(z_i) \equiv -i \bmod q_0$, mais comme tous ces ordres sont distincts on obtient une contradiction. Le calcul de la dimension s'ensuit. □

Le lemme permet de définir l'application suivante :

$$\Phi : L \longrightarrow L((q_0 m + n)Q)$$
$$\sum_{i\in T} u_i z_i^{q_0} \longmapsto \sum_{i\in T} u_i^{q_0} z_i.$$

Lemme 6.4. *L'application Φ vérifie les propriétés suivantes :*

(1) *L'application est additive et même semi-linéaire, c'est-à dire :*

$$\Phi(x+y) = \Phi(x) + \Phi(y) \quad \text{et} \quad \Phi(\lambda^{q_0} x) = \lambda \Phi(x).$$

(2) *Posons $m = q_0 - \varepsilon$ et $n = q_0 + \gamma$ et supposons la condition numérique suivante réalisée :*

$$q_0 > \frac{(\gamma + 1 - g)(g + \varepsilon)}{\gamma + 1 - 2g}\,. \tag{9}$$

Alors le noyau de Φ est non trivial.

Démonstration. Le premier point est immédiat et pour prouver le second il suffit de savoir que $\dim L > \ell((q_0 m + n)Q)$. Pour calculer ou estimer ces dimensions, on a recours au théorème de Riemann-Roch qui indique dans ce contexte que

$$\dim L = \ell(mQ) \cdot \ell(nQ) \geqslant (m + 1 - g)(n + 1 - g)$$

et, comme $q_0 m + n \geqslant 2g - 1$:

$$\ell((q_0 m + n)Q = m q_0 + n + 1 - g.$$

L'inégalité $(m+1-g)(n+1-g) > q_0+n+1-g$ se traduit exactement (après calcul) en la condition (9). □

Nous ferons les choix suivants : $\varepsilon = 1$ et $\gamma = 2g$ de sorte que l'inégalité (9) se traduit par $q_0 > (g+1)^2$.

Lemme 6.5. *Soit x une fonction non nulle de* $\operatorname{Ker}\Phi$*, alors pour tout point $P \in C(\mathbb{F}_q) \smallsetminus \{Q\}$ on a $x(P) = 0$.*

Démonstration. On exploite le fait que $q_0^2 = q$ et donc si $a \in \mathbb{F}_q$ on aura $a^{q_0^2} = a$. On écrit la décomposition $x = \sum_{i\in T} u_i z_i^{q_0}$ et on calcule :

$$\begin{aligned} x(P)^{q_0} &= \Big(\sum_{i\in T} u_i(P) z_i(P)^{q_0}\Big)^{q_0} = \sum_{i\in T} u_i^{q_0}(P) z_i(P) \\ &= \Big(\sum_{i\in T} u_i^{q_0} z_i\Big)(P) = (\Phi(x))\,(P) = 0. \end{aligned}$$ □

On termine la démonstration en écrivant

$$\#\left(C(\mathbb{F}_q) \smallsetminus \{Q\}\right) \leqslant \deg \operatorname{div}(x)_0 = \deg \operatorname{div}(x)_\infty \leqslant m + nq_0$$

d'où l'on tire en tenant compte du choix des paramètres :

$$\#C(\mathbb{F}_q) \leqslant q_0 - \varepsilon + q_0(q_0 + \gamma) + 1 = q + 1 + (2g+1)\sqrt{q}.$$ □

Nous allons maintenant donner, pour une famille particulière de courbes, un argument permettant de déduire de la *majoration* 6.1 une minoration du nombre de points rationnels (le cas général suit la même idée mais est plus sophistiqué). Les courbes particulières sont les courbes de la forme $y^d = f(x)$ avec $f(x)$ séparable de degré e et d premier avec pe ; on supposera également que les racines d-ièmes de l'unité sont dans $\mathbb{F}_q$. Il y a dans ce cas un unique point à l'infini que nous notons Q_0. Notons par ailleurs $a_1 = 1, a_2, \ldots, a_d$ des représentants de $\mathbb{F}_q^*/\mathbb{F}_q^{*d}$ (le quotient du groupe multiplicatif $\mathbb{F}_q^*$ par le sous-groupe formé des éléments qui sont des puissances d-ièmes) c'est-à-dire des éléments tels que $\mathbb{F}_q^* = \cup_i a_i \mathbb{F}_q^{*d}$ (union disjointe). Pour $a \in \mathbb{F}_q^*$, on note C_a la courbe affine

$$ay^d = f(x).$$

Ces courbes ont le même genre $g = (d-1)(e-1)/2$ que C, en fait $C_1 = C_{a_1} = C \smallsetminus \{Q_0\}$ et possède aussi un unique point l'infini qui est donc rationnel. On peut leur appliquer la majoration donnée par la proposition 6.1 :

$$C_a(\mathbb{F}_q) \leqslant q + (2g+1)\sqrt{q}.$$

Notons $\mathscr{Z}_0 := \{x \in \mathbb{F}_q \mid f(x) = 0\}$ et $\mathscr{Z} = \mathscr{Z}_0 \times \{0\}$ et $r = \#\mathscr{Z}$; les courbes C_a contiennent chacune l'ensemble $\mathscr{Z}$. Si $x \in \mathbb{F}_q \smallsetminus \mathscr{Z}_0$ on

a $f(x) \in a_i \mathbb{F}_q^{*d}$ pour un seul des a_i et l'équation $a_i y^d = f(x)$ possède d solutions en y. On en tire l'égalité

$$d(q-r) = \sum_{i=1}^{d} \#\left\{C_{a_i}(\mathbb{F}_q) \smallsetminus \mathscr{Z}\right\},$$

ou encore

$$\#C(\mathbb{F}_q) - 1 = \#C_1(\mathbb{F}_q) = dq - \sum_{i=2}^{d} \#C_{a_i}(\mathbb{F}_q).$$

En insérant la majoration de $\#C_a(\mathbb{F}_q)$ obtenue dans la proposition 6.1, on obtient la minoration

$$\#C(\mathbb{F}_q) \geqslant q + 1 - (d-1)(2g+1)\sqrt{q}.$$

Ces arguments permettent ainsi de démontrer une inégalité du type

$$\left|\#C(\mathbb{F}_q^m) - q^m - 1\right| \leqslant cq^{m/2}.$$

D'où l'on tire l'inégalité de Stepanov

$$\left|\sum_{j=1}^{2g} \beta_j^m\right| \leqslant cq^{m/2}.$$

La série entière $S(z) = \sum_{m=0}^{\infty} (\beta_1^m + \cdots + \beta_{2g}^m) z^m$ est égale à la somme des $(1-\beta_j z)^{-1}$ et son rayon de convergence est $R = (\max |\beta_j|)^{-1}$. L'inégalité de Stepanov montre que le rayon de convergence est supérieur ou égal à $q^{-1/2}$; on en tire donc bien l'inégalité $\max_j |\beta_j| \leqslant \sqrt{q}$. Si l'on se souvient que la transformation $\beta \mapsto q/\beta$ laisse stable l'ensemble des β_j on obtient bien l'égalité voulue : $|\beta_j| = \sqrt{q}$.

7. Appendice : Corps finis et courbes algébriques

7.a. Corps finis. Le premier exemple de corps fini est bien sûr $\mathbb{Z}/p\mathbb{Z}$ muni de l'addition et multiplication, que l'on note $\mathbb{F}_p$. Un corps fini K est nécessairement de caractéristique finie égale à un nombre premier p (l'homomorphisme $\mathbb{Z} \to K$ donné par $m \mapsto m \cdot 1_K$ ne peut être injectif) et contient donc $\mathbb{F}_p$; c'est donc un espace vectoriel de dimension finie, disons n, sur $\mathbb{F}_p$ et donc le cardinal de K est p^n.

Théorème 7.1. *Soit K un corps fini de cardinal $q = p^n$. Le groupe K^* est cyclique de cardinal $q-1$. On dispose de la factorisation*

$$X^q - X = \prod_{a \in K} (X - a).$$

L'application $\Phi : x \mapsto x^p$ est un automorphisme de K dont les points fixes sont les éléments de $\mathbb{F}_p \subset K$.

Cet énoncé permet aussi de construire un corps de cardinal p^m : il suffit de construire un corps K' extension de $\mathbb{F}_p$ tel que le polynôme $X^{p^m} - X \in \mathbb{F}_p[X]$ ait toutes ses racines dans K' ; on définit alors K comme l'ensemble de ces racines et on vérifie aisément que c'est un corps (si x et y sont des racines de $X^{p^m} - X = 0$ alors $x \pm y$, xy, x^{-1} également). On arrive ainsi a l'énoncé fondamental.

Théorème 7.2. *Soit p un nombre premier et $m \geqslant 1$. Il existe un corps, unique à isomorphisme près, de cardinal p^m. On le note $\mathbb{F}_{p^m}$. Si l'on plonge tous ces corps dans une clôture algébrique $\overline{\mathbb{F}}_p$ on peut identifier $\mathbb{F}_{p^m}$ comme l'ensemble des points fixes de Φ^m (où $\Phi(x) = x^p$ désigne le Frobenius).*

Pour construire « concrètement » un tel corps une solution est de trouver un polynôme de de degré m et irréductible dans $\mathbb{F}_p[X]$; par exemple

$$\begin{aligned}
\mathbb{F}_4 &= \mathbb{F}_2[X]/(X^2 + X + 1)\mathbb{F}_2[X], \\
\mathbb{F}_8 &= \mathbb{F}_2[X]/(X^3 + X + 1)\mathbb{F}_2[X], \\
\mathbb{F}_9 &= \mathbb{F}_3[X]/(X^2 + 1)\mathbb{F}_3[X].
\end{aligned}$$

7.b. Courbes algébriques et diviseurs. Une courbe affine est un sous-ensemble algébrique, c'est-à-dire l'ensemble des zéros communs de polynômes, qui de plus est de dimension 1, par exemple

$$C := \{(x, y) \in \mathbb{A}^2 \mid f(x, y) = 0\}.$$

Si f est à coefficients dans $\mathbb{F}_q$, on dit que la courbe C est définie sur $\mathbb{F}_q$, ce qu'on indique par $C/\mathbb{F}_q$, et $C(\mathbb{F}_q)$ désigne l'ensemble des couples $(x, y) \in \mathbb{F}_q^2$ solutions de $f(x, y) = 0$: ce sont les *points rationnels de $C/\mathbb{F}_q$*. Pour toute extension $\mathbb{F}$ de $\mathbb{F}_q$ ($\mathbb{F}_{q^m}$ ou $\overline{\mathbb{F}}_q$ par exemple), $C(\mathbb{F})$ désigne l'ensemble des solutions de $f(x, y) = 0$ dans $\mathbb{F}^2$.

On est souvent amené à considérer les courbes projectives : les sous-ensembles algébriques de dimension 1 d'un espace projectif, c'est-à-dire l'ensemble des zéros communs de polynômes homogènes. Par exemple si on pose

$$F(X,Y,Z) = Z^{\deg(f)} f(XZ^{-1}, YZ^{-1})$$

alors

$$\overline{C} := \{(X,Y,Z) \in \mathbb{P}^2 \mid F(X,Y,Z) = 0\}$$

est une courbe projective qui est la fermeture de la courbe affine C précédente (ce procédé est l'analogue algébrique de la compactification topologique). Un *diviseur* sur une courbe est une somme formelle de points à coefficients entiers $D = \sum_{P \in C} n_P P$, son degré est l'entier $\deg D = \sum_{P \in C} n_P$. Si f est une fonction rationnelle sur la courbe, on définit son diviseur $\mathrm{div}(f)$ comme la somme de ses zéros moins la somme de ses pôles (comptés avec multiplicités), ce que l'on peut noter $\mathrm{div}(f) = \sum_P \mathrm{ord}_P(f)[P]$. Si C est projective, on a toujours $\deg \mathrm{div}(f) = 0$.

Ces notions sont définies sur la clôture algébrique disons de $\mathbb{F}_q$, mais on peut parler de courbes, diviseurs *définis* sur $\mathbb{F}_q$: ce sont les objets définis à l'aide de polynômes à coefficients dans $\mathbb{F}_q$ ou encore invariants sous le groupe de Galois de $\overline{\mathbb{F}}_q$ sur $\mathbb{F}_q$.

Sur une courbe affine $f(x,y) = 0$ un point *singulier* est un point $P = (x_0, y_0)$ tel que

$$f(x_0,y_0) = \frac{\partial f}{\partial x}(x_0,y_0) = \frac{\partial f}{\partial y}(x_0,y_0) = 0$$

(intuitivement c'est un point où il n'y a pas de tangente bien définie). On dit qu'une courbe est *lisse* si elle ne possède aucun point singulier. On peut montrer que toute courbe est birationnelle à une unique courbe lisse projective.

Il est facile d'expliciter sur l'exemple de la droite projective le diviseur d'une fonction. Le corps des fonctions est le corps des fonctions rationnelles en x et on peut écrire

$$f = a \prod_{i=1}^{r} (x - a_i)^{m_i},$$

avec des a_i distincts et $m_i \in \mathbb{Z}$. Le support de $\mathrm{div}(f)$ contient naturellement les points $P_i = (a_i, 1)$ et (éventuellement) le point à l'infini

$\infty = (1,0) \in \mathbb{P}^1$ dont la multiplicité est $-\deg f = -\sum_i m_i$ en effet si on pose $t = 1/x$ alors t est un paramètre local en ∞ et

$$f = a\prod_{i=1}^{r}(t^{-1} - a_i)^{m_i} = at^{-\deg f}\prod_{i=1}^{r}(1 - a_i t)^{m_i}.$$

On vérifie donc bien l'égalité

$$\deg \operatorname{div}(f) = \deg\Big(\sum_{i=1}^{r} m_i[P_i] - \deg(f)[\infty]\Big) = \sum_i m_i - \deg f = 0.$$

On peut aussi explicitement calculer l'espace

$$L(m[\infty]) := \{f \in K(x) \mid \operatorname{div}(f) + m[\infty] \geqslant 0\}.$$

Lorsque $m \geqslant 0$, il s'agit des polynômes de degré $\leqslant m$, on retrouve ainsi $\ell(m[\infty]) = m + 1$ et donc $g = 0$ dans le théorème de Riemann-Roch. Plus généralement $\ell(D) = 0$ si $\deg(D) < 0$ et comme on peut toujours écrire

$$\begin{aligned} D = \sum_i m_i[P_i] &= \sum_i m_i[P_i] - \Big(\sum_i m_i\Big)[\infty] + \Big(\sum_i m_i\Big)[\infty] \\ &= \operatorname{div}(f) + \deg(D)[\infty], \end{aligned}$$

un diviseur D est équivalent à $\deg D[\infty]$ et donc

$$\ell(D) = \deg D + 1, \quad \text{si } \deg D \geqslant 0.$$

Le *genre* d'une courbe algébrique est son invariant le plus important, la première définition vient de la topologie : si C est une « courbe » algébrique définie sur le corps des complexes et si la courbe est lisse, l'ensemble de ses points complexes forme (sic) une « surface de Riemann » et si la courbe est projective, la surface de Riemann associée est compacte. La topologie nous apprend qu'une surface compacte a la forme d'un « tore à g trous », l'invariant g est bien le « genre » (voir [**Pop2012**]). Le théorème de Riemann-Roch permet de donner une définition purement algébrique du genre.

Par exemple, le genre d'une courbe plane lisse de degré d est

$$g = \frac{(d-1)(d-2)}{2};$$

si l'on considère une courbe plane projective quelconque, l'ensemble S de ses points singuliers est fini et on peut attacher à chaque point

$P \in S$ une mesure de sa singularité $\delta(P) \geqslant 1$ telles que

$$g = \frac{(d-1)(d-2)}{2} - \sum_{P \in S} \delta(P).$$

Par exemple le genre d'une courbe $y^d = f(x)$ avec f séparable de degré e et $\operatorname{pgcd}(d, pe) = 1$ est $g = (d-1)(e-1)/2$. Ainsi pour une courbe d'équation affine $y^2 = f(x)$ avec $p \neq 2$ et f un polynôme séparable de degré impair d, on trouve $g = (d-1)/2$. L'équation homogène est $Z^{d-2}Y^2 = Z^d f(X/Z)$ et il y a un seul point à l'infini $\infty = (0, 1, 0)$. Pour $d = 3$ le point à l'infini est lisse et le genre égal à 1 ; pour $d > 3$, le point ∞ est singulier et $\delta(\infty) = (d-1)(d-3)/2$.

7.c. Le Frobenius. Le « Frobenius » $x \mapsto x^q$ peut être étendu en un morphisme $\Phi : \mathbb{P}^n \to \mathbb{P}^n$, encore appelé Frobenius, défini par $\Phi(x_0, \ldots, x_n) := (x_0^q, \ldots, x_n^q)$. Le calcul simple suivant est essentiel dans la preuve du lemme ci-dessous. Si $F = \sum_i a_i x^i \in \mathbb{F}_q[X_0, \ldots, X_n]$ est un polynôme à coefficients dans $\mathbb{F}_q$ alors

$$F(x_0, \ldots, x_n)^q := \Big(\sum_i a_i x^i \Big)^q = \sum_i a_i^q x^{iq} = \sum_i a_i x^{iq} = F(x_0^q, \ldots, x_n^q).$$

Lemme 7.3. *Soit V une sous-variété de $\mathbb{P}^n$ définie sur $\mathbb{F}_q$. Alors Φ induit un endomorphisme de V, noté $\Phi_V : V \to V$. De plus, l'ensemble des points $\mathbb{F}_q$-rationnels est l'ensemble des points fixes du Frobenius Φ_V, c'est-à-dire*

$$V(\mathbb{F}_q) = \left\{ x \in V(\overline{F}_q) \mid \Phi_V(x) = x \right\}.$$

En effet si $F_1(x) = \cdots = F_t(x) = 0$ est un ensemble d'équations à coefficients dans $\mathbb{F}_q$ définissant V, on a, pour tout $P = (x_0, \ldots, x_n) \in V(\overline{F}_q)$, l'égalité $F_i(\Phi(P)) = F_i(x_0, \ldots, x_n)^q = 0$ donc $\Phi(P) \in V$. Pour la deuxième affirmation, on peut choisir une coordonnée égale à 1 et l'assertion découle de la propriété des corps finis rappelée : $x^q = x$ équivaut à $x \in \mathbb{F}_q$. Si $P \in V$, on a donc $\Phi(P) = P$ si et seulement si $P \in V(\mathbb{F}_q)$ ou plus généralement $\Phi^m(P) = P$ si et seument si $P \in V(\mathbb{F}_{q^m})$.

Références

[Aud2011] Audin M., *Correspondance entre Henri Cartan et André Weil (1928–1991)*, Documents mathématiques, Soc. Math. France, 2011.
[Voir notamment les lettres du 17 mars 1940, p. 65–66 ; 26 mars 1940, p. 69–70 ; 30 mars 1940, p. 72 ; 5 avril 1940, p. 76–77 ; 8 avril 1940, p. 78–80 ; 2 mai 1940, p. 83]

[Bom1973] Bombieri, E., *Counting points on curves over finite fields (d'après S.A.. Stepanov)*, Séminaire Bourbaki, 25e année (1972/73), Exp. no 430, p. 234–241. Lecture Notes in Math., Vol. 383, Springer, Berlin, 1974, `http://www.numdam.org/numdam-bin/fitem?id=SB_1972-1973__15__234_0`.

[Bos2003] Bost, J.-B., *Le théorème des nombres premiers et la transformation de Fourier*. In La fonction zêta, Journées X-UPS 2002, p. 1-35, Éd. École Polytechnique, Palaiseau, 2003.

[Gol2002] Goldschmidt, D., *Algebraic functions and projective curves*. GTM 215, Springer 2002.

[Gop1970] Гоппа Б. Д., новый класс пинейных корректирующих кодов проблемы передачи информаций 6 (1970), no. 3, p. 24–30. [Goppa, V. D., *A new class of linear correcting codes*. Problemy Peredachi Informatsii 6 (1970), no. 3, p. 24–30.]

[Har1977] Hartshorne R., *Algebraic Geometry*. GTM 52, Springer 1977.

[Has1934] Hasse H., *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichen Konstantenkörper*, J. Reine Angew. Math. 172 (1934), p. 37–54.

[Has1936] Hasse H., *Über die Riemannsche Vermuntung in Funktionenkörper*, in *Congrès international des mathématiciens*, Oslo, 1936, p. 183–206.

[Hin2008] Hindry M., *Arithmétique*. Calvage & Mounet, 2008.

[Pop2012] Popescu-Pampu P., *Qu'est-ce-que le genre ?* In Histoires de mathématiques, Journées X-UPS 2011, Éd. École Polytechnique, Palaiseau, 2012.

[Rie1859] Riemann, B., *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*. Monatsberichte der Berliner Akademie, 1859.

[Sch1931] Schmidt, F. K., *Analytische Zahlentheorie in Körpern der Characteristik p*, Math. Zeitschr. 33 (1931).

[Ser1983] Serre J-P., *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C.R.A.S. 296, (1983), p. 397–402.

[Ser1999] Serre J-P., *La vie et l'œuvre d'André Weil*. Enseign. Math. 45 (1999), no. 1-2, p. 5–16.

[Ste1969] Степанов ц. а., О числе точек гиперэллиптической кривой над простым конечым полем, известия академии наук ссср 33 (1969), p. 1103–1114. [Stepanov, S. A.,

On the number of points of a hyperelliptic curve over a finite prime field, Izv. Akad. Nauk SSSR, Ser. Math. 33 (1969), p. 1103–1114.]

[Sti1993] Stichtenoth, H., *Algebraic function fields and codes.* Universitext, Springer 1993.

[Wei1940a] Weil, A., *Une lettre et un extrait de lettre à Simone Weil.* In Œuvres scientifiques [1940a], Springer 1979.

[Wei1940b] Weil, A., *Sur les fonctions algébriques à corps de constantes fini.* C. R. Acad. Sci. Paris 210 (1940), p. 592–594.

[Wei1941] Weil, A., *On the Riemann hypothesis in function fields.* Proc. Nat. Acad. Sci. U. S. A. 27 (1941), p. 345–347.

[Wei1949] Weil, A., *Numbers of solutions of equations in finite fields.* Bull. Amer. Math. Soc. 55 (1949), p. 497–508.

[We1991] Weil, A., *Souvenirs d'apprentissage.* Vita Mathematica, 6. Birkhäuser Verlag, Basel, 1991.

Marc Hindry, Institut mathématique de Mathématiques de Jussieu, Université Denis Diderot Paris 7, Case Postale 7012, 2, place Jussieu, 75251 Paris Cedex 05 • *E-mail :* hindry@math.jussieu.fr
Url : http://www.math.jussieu.fr/~hindry/