Journées mathématiques X-UPS

Année 1993

Codes géométriques algébriques et arithmétique sur les corps finis

Christian HOUZEL

Nombre de points d'une variété algébrique sur un corps fini

Journées mathématiques X-UPS (1993), p. 63-80.
https://doi.org/10.5802/xups.1993-04

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. 63–80 doi: 10.5802/xups.1993-04

NOMBRE DE POINTS D'UNE VARIÉTÉ ALGÉBRIQUE SUR UN CORPS FINI

par

Christian Houzel

Table des matières

En 1949, A. Weil a associé à toute variété algébrique sur un corps fini k une *fonction zêta* liée au nombre de points de la variété dans les diverses extensions finies de k et il a formulé des conjectures célèbres au sujet de cette fonction. Les conjectures de Weil ont été un des principaux stimulants pour le développement de la géométrie algébrique abstraite, en particulier dans l'œuvre d'A. Grothendieck ; elles ont été finalement démontrées par P. Deligne en 1973 en utilisant les outils élaborés par Grothendieck.

Dans cet exposé, nous allons essayer d'expliquer l'histoire qui précède la formulation des conjectures de Weil et de montrer comment on a pu arriver à les concevoir.

La fonction zêta classique, celle de Riemann, donne des informations sur la distribution des *nombres premiers* dans l'anneau $\mathbb{Z}$ des entiers. Sa définition a été étendue par Dedekind au cas d'un *corps de nombres algébriques* K (extension finie de $\mathbb{Q}$) ; la fonction zêta de Dedekind est liée à la distribution des *idéaux premiers* dans l'anneau des entiers de K et elle informe aussi sur le nombre des classes d'idéaux de K.

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.

1. E. Artin

Dans sa thèse (1921, publiée en 1924), E. Artin a développé, sur le modèle de la théorie des corps quadratiques, une théorie arithmétique des extensions quadratiques $\Omega = K(\sqrt{D})$ du corps des fractions rationnelles $K = \mathbb{F}_p(t)$ à coefficients dans un corps fini $\mathbb{F}_p$ (p nombre premier impair) ; une telle extension est engendrée par la racine carrée d'un polynôme D (sans facteur carré) à coefficients dans $\mathbb{F}_p$. Artin y définit l'anneau des entiers, les idéaux de cet anneau, qui se décomposent d'une manière unique en produits d'idéaux *premiers* et se partagent en un nombre fini de *classes modulo* les idéaux principaux ; le nombre h de ces classes est 1 si D est de degré 0 ou 1 et 2 si D est de degré 2. En vue d'évaluer h dans les autres cas, Artin associe une fonction zêta au corps Ω sur le modèle de celle de Dedekind en théorie des nombres :

$$\mathbb{Z}(s) = \mathbb{Z}_D(s) = \sum_{\mathfrak{a}} \frac{1}{|N\mathfrak{a}|^s};$$

dans cette formule $\mathfrak{a}$ parcourt l'ensemble des idéaux non nuls, $N\mathfrak{a}$ est la *norme* de l'idéal $\mathfrak{a}$, c'est-à-dire le polynôme unitaire qui engendre le produit $\mathfrak{a}\mathfrak{a}'$ de $\mathfrak{a}$ par son *conjugué* $\mathfrak{a}'$ (obtenu par l'automorphisme de Ω qui change $\sqrt{D}$ en $-\sqrt{D}$; le produit est automatiquement un idéal principal) et, pour chaque polynôme $F \in \mathbb{F}_p[t]$ de degré n on pose $|F| = p^n$ (on notera que $|N\mathfrak{a}|$ est le nombre d'éléments de l'anneau résiduel $\bmod \mathfrak{a}$). La variable s est complexe et la série converge pour $\mathrm{Re}(s) > 1$; comme dans le cas des corps de nombres, on peut écrire $\mathbb{Z}(s)$ sous forme d'un produit étendu à tous les *idéaux premiers* :

$$\mathbb{Z}(s) = \prod_{\mathfrak{p}} \frac{1}{1 - |N\mathfrak{p}|^{-s}}.$$

Artin regroupe dans ce produit les $\mathfrak{p}$ qui divisent un même polynôme irréductible $P \in \mathbb{F}_p[t]$, puis en transformant à nouveau le produit en série il trouve

$$\mathbb{Z}(s) = \frac{1}{1 - p^{-(s-1)}} \sum_{F} \left[\frac{D}{F}\right] \frac{1}{|F|^s}$$

où F parcourt l'ensemble des polynômes unitaires à coefficients dans $\mathbb{F}_p$ et où $\left[\frac{D}{F}\right] = \pm 1$ est un symbole analogue à celui de Jacobi en

théorie des nombres. Ce symbole fait l'objet d'une *loi de réciprocité*, établie par Artin, qui permet de montrer que la somme

$$\sigma_\nu = \sum_{|F|=p^\nu} \left[\frac{D}{F}\right]$$

est nulle pour $\nu \geqslant n = \deg D$ lorsque $n \geqslant 1$; ainsi, pour D non constant,

$$\mathbb{Z}_D(s) = \frac{1}{1-p^{-(s-1)}} \sum_{\nu-0}^{n-1} \frac{\sigma_\nu}{p^{\nu s}}.$$

Lorsque D est constant, on peut supposer que c'est une racine primitive $g \mod p$ et on trouve que

$$\mathbb{Z}_g(s) = \frac{1}{1-p^{-(s-1)}} \cdot \frac{1}{1+p^{-(s-1)}};$$

dans tous les cas $\mathbb{Z}(s)$ est rationnelle en p^{-s}.

Pour relier la fonction zêta au nombre h des classes d'idéaux, Artin étudie, pour chaque classe d'idéaux $\mathbb{K}$ la somme partielle $\mathbb{Z}(s, \mathbb{K})$ de la série obtenue en prenant $\mathfrak{a} \in \mathbb{K}$. Dans le « cas imaginaire » (D de degré impair ou bien de degré pair avec un coefficient dominant non carré dans $\mathbb{F}_p$), ils trouve que $\mathbb{Z}(0, \mathbb{K}) = 1/w$ indépendamment de la classe $\mathbb{K}$, où w est le nombre des *unités* de Ω (éléments inversibles de l'anneau des entiers) ; ainsi

$$h = \begin{cases} -w\mathbb{Z}(0) = 1 & \text{si } D = g, \\ \sigma_0 + \sigma_1 + \cdots + \sigma_{n-1} & \text{si } \deg D = n \geqslant 1. \end{cases}$$

Le cas « réel » (D de degré pair avec un coefficient dominant carré) est un peu plus compliqué : on a $\sigma_0+\sigma_1+\cdots+\sigma_{n-1} = 0$ comme conséquence de la loi de réciprocité et on n'atteint pas h en considérant $\mathbb{Z}$ en 0 ; mais on a, indépendamment de $\mathbb{K}$,

$$\lim_{s\to 1}(s-1)\mathbb{Z}(s, \mathbb{K}) = \frac{(p-1)R}{|\sqrt{D}| \log p},$$

où le nombre R est défini de manière que $|\varepsilon_0| = p^R$, ε_0 étant une « unité fondamentale » de Ω. Ainsi

$$h = \frac{|\sqrt{D}|}{(p-1)R} \sum_{\nu-0}^{n-1} \frac{\sigma_\nu}{p^\nu}$$

et le résidu de $\mathbb{Z}(s)$ en son pôle $s = 1$ est $h/\kappa \log p$, où $\kappa = |\sqrt{D}|/(p-1)R$. On trouve une forme analogue pour ce résidu dans le cas imaginaire grâce à l'*équation fonctionnelle* de la fonction zêta, qui se démontre sur les fonctions partielles $\mathbb{Z}(s, \mathbb{K})$:

$$\mathbb{Z}(1-s) = \begin{cases} \dfrac{1-p^{-(s-1)}}{1-p^s}\left(\sqrt{|D|/p}\right)^{2s-1} \cdot \mathbb{Z}(s) & \text{pour } n \text{ impair} \\ \dfrac{1-p^{-(s-1)}}{1-p^{2s}}\left(\sqrt{|D|}\right)^{2s-1} \cdot \mathbb{Z}(s) & \text{pour } n \text{ pair} \end{cases}$$

et D de coefficient dominant g ; les valeurs κ correspondantes sont respectivement $\sqrt{|D|/p}$ et $2\sqrt{|D|}/p + 1$. Il y a aussi une équation fonctionnelle dans le cas réel ; Artin l'obtient à partir des précédentes grâce à l'identité facile

$$(*) \qquad \mathbb{Z}_D(s + \frac{\pi i}{\log p}) = \frac{1-p^{-(s-1)}}{1+p^{-(s-1)}} \cdot \mathbb{Z}_{gD}(s)$$

et elle s'écrit

$$\mathbb{Z}(1-s) = \Big(\frac{1-p^{-(s-1)}}{1+p^s}\Big)^2 \left(\sqrt{|D|}\right)^{2s-1} \mathbb{Z}(s).$$

L'équation fonctionnelle se traduit par des relations entre les coefficients σ_ν :

$$\sigma_{2m-\nu} = p^{m-\nu_{\sigma_\nu}} \quad \text{si } \deg D = 2m+1 \text{ est impair}$$

$$\text{et} \quad \sigma_{2m-\nu} \pm p\sigma_{m\nu-1} = p^{m-\nu}(\sigma_\nu \pm p\sigma_{\nu-1}) \quad \text{si } \deg D = 2m \text{ est pair}$$

($\pm = +$ dans le cas imaginaire et $-$ dans le cas réel). À l'aide de ces relations, le calcul des σ_ν et de h devient facile pour les petites valeurs de p et de m et Artin donne des tables de ces nombres pour $\deg D = 3, p = 3, 5$ et 7 et pour $\deg D = 4, p = 3$.

Par ailleurs $(*)$ montre que $\mathbb{Z}_D\big(1 + \pi i/\log p\big)$ n'est pas nul puisque le résidu de $\mathbb{Z}_{gD}$ en $s = 1$ n'est pas nul ; comme $\mathbb{Z}$ est une fonction périodique de s (de période $2\pi i/\log p$), elle ne s'annule en aucun des points $1 + (2n+1)\pi i/\log p$ et Artin en déduit qu'elle ne s'annule pas sur la droite $\mathrm{Re}(s) = 1$.

Dans les cas correspondant à ses tables numériques, Artin va plus loin en établissant l'analogue de l'*hypothèse de Riemann* ; les zéros

(non triviaux) de $\mathbb{Z}$ sont sur la droite $\mathrm{Re}(s) = 1/2$. Ceci signifie encore que les racines $z = \beta_\nu \neq \pm 1$ de l'équation algébrique $z^{n-1} + \sigma_1 z^{n-2} + \cdots + \sigma_{n-1} = 0$ sont toutes de valeur absolue $p^{1/2}$. Pour $n = 3$, cette équation se réduit à $z^2 + \sigma_1 z + p = 0$ et l'hypothèse de Riemann signifie donc que les racines de cette équation sont imaginaires conjuguées ou encore que $|\sigma_1| < 2\sqrt{p}$; les tables donnent $|\sigma_1| \leqslant 3$ pour $p = 3$, $|\sigma_1| \leqslant 4$ pour $p = 5$ et $|\sigma_1| \leqslant 5$ pour $p = 7$, d'où l'hypothèse de Riemann. Pour $n = 4$ l'équation $z^3 + \sigma_1 z^2 + \sigma_2 z + p = 0$ avec $\sigma_2 = p - 1 + \sigma_1$ (racine triviale -1) ; ses racines non triviales sont celles de l'équation $z^2 + (\sigma_1 - 1)z + p = 0$ et l'hypothèse de Riemann s'écrit dans ce cas $|\sigma_1 - 1| < 2\sqrt{p}$ qu'Artin vérifie pour $p = 3$ ou 5.

Le nombre h de classes d'idéaux s'exprime au moyen de $\mathbb{Z}(0)$ (cas imaginaire) ou de $\mathbb{Z}'(0)$ (cas réel) et par conséquent au moyen des racines β_ν :

$$h = \begin{cases} \displaystyle\prod_{\nu=1}^{n-1} (\beta_\nu - 1) & \text{pour } n = \deg D \text{ impair,} \\ \displaystyle 2 \prod_{\nu=1}^{n-1} (\beta_\nu - 1) & \text{pour } n = \deg D \text{ pair dans le cas imaginaire,} \\ \displaystyle \frac{1}{R} \prod_{v=1}^{n-2} (\beta_\nu - 1) & \text{pour } n = \deg D \text{ pair dans le cas réel.} \end{cases}$$

En utilisant l'hypothèse de Riemann, Artin en déduit des encadrements pour h et il trouve ainsi qu'il n'y a qu'un nombre fini de corps $K(\sqrt{D})$ avec un nombre de classes h donné ; par exemple, si $p > 5$ et $n > 3$, le nombre de classes est $\geqslant 2$.

La fonction $\mathbb{Z}$ donne aussi une estimation asymptotique du nombre $\pi(x)$ d'idéaux premiers $\mathfrak{p}$ tels que $|N\mathfrak{p}| = x$; on a

$$\pi(p^\nu) = \frac{p^\nu}{\nu} + O(p^{\theta\nu}/\nu)$$

en notant θ la borne supérieure des parties réelles des zéros de $\mathbb{Z}$ (si l'hypothèse de Riemann est vraie, $\theta = 1/2$).

2. F. K. Schmidt

La théorie d'Artin a été étendue par F. K. Schmidt (1925, 1931) au cas des extensions finies K (non nécessairement quadratiques) d'un corps de fonctions rationnelles $k(z)$ à coefficients dans un corps fini k. Pour définir et étudier la fonction zêta dans ce cas plus général, Schmidt a été amené à changer de point de vue et à remplacer le modèle des corps de nombres algébriques par celui des corps de fonctions algébriques d'une variable. Dedekind et Weber (1882) avaient en effet développé, en s'inspirant de la théorie des nombres algébriques, une théorie purement algébrique des extensions finies K du corps $\mathbb{C}(z)$ des fonctions rationnelles à coefficients complexes ; une telle extension est formée des fonctions rationnelles en deux variables z et u liées par une relation algébrique $F(z,u)=0$. Le but de Dedekind et Weber était d'obtenir une définition générale et rigoureuse des points de la surface de Riemann associée à la fonction algébrique u de z. Un point correspond à une *place* P de K, sous-anneau de valuation de K formé des fonctions régulières au point considéré ; un tel anneau possède un unique idéal maximal $\mathfrak{p}$, formé des fonctions nulles au point et l'homomorphisme $\mathrm{P} \to \mathrm{P}/\mathfrak{p} \cong \mathbb{C}$ correspond à l'évaluation d'une fonction au point.

Dans le cas de Schmidt, $\mathbb{C}$ est remplacé par un corps fini k (de caractéristique p_0), mais on peut encore définir les places P de K (ce sont les sous-anneaux intégralement clos de K admettant K comme corps des fractions) et ceci d'une manière indépendante du choix de la variable z ; si $z \in \mathrm{P}$ cette place contient la fermeture entière $\mathfrak{I}$ de $k[z]$ dans K, $\mathfrak{I} \cap \mathfrak{p} = \widetilde{\mathfrak{p}}$ est un idéal *premier* de $\mathfrak{I}$ et P est le localisé correspondant. Les places qui ne contiennent pas z s'interprètent comme des points à l'infini relativement à la variable z et on obtient toutes les places en localisant les fermetures intégrales des deux anneaux $k[z]$ et $k[1/z]$. Au lieu de travailler, comme Artin, avec un anneau d'entiers $\mathfrak{I}$ et ses idéaux, Schmidt travaille avec les *diviseurs* de K, qui sont des expressions formelles $\mathfrak{c} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_s^{e_s}$ où les $\mathfrak{p}_i$ sont des idéaux maximaux de places P_i et les exposants e_i sont des entiers (non nécessairement positifs) ; ces diviseurs forment un

groupe multiplicatif (commutatif) $\mathbb{D}$ engendré librement par les diviseurs *premiers* $\mathfrak{c} = \mathfrak{p}$. Un diviseur est dit *entier* si tous ses exposants sont $\geqslant 0$ et un diviseur $\mathfrak{c}'$ est *multiple* de $\mathfrak{c}''$ si $\mathfrak{c}'/\mathfrak{c}''$ est entier. À un élément z non nul de K on associe le diviseur $(z) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_s^{e_s}$ où les $\mathfrak{p}_i$ sont tels que $\mathrm{P}_i z \neq \mathrm{P}_i$ et les e_i sont déterminés par $\mathrm{P}_i z = \mathfrak{p}_i^{e_i}$; si $\widetilde{\mathfrak{c}} = \widetilde{\mathfrak{p}}_1^{e_1}\widetilde{\mathfrak{p}}_2^{e_2}\cdots\widetilde{\mathfrak{p}}_s^{e_s}$ est un idéal d'un sous-anneau de Dedekind R de K avec sa décomposition en produit d'idéaux premiers, on lui associe le diviseur $\mathfrak{c} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_s^{e_s}$ où, pour chaque i, $\mathfrak{p}_i$ est l'idéal maximal de la place $R_{\widetilde{\mathfrak{p}}_i}$.

L'*ordre* est un homomorphisme du groupe $\mathbb{D}$ dans le groupe $\mathbb{Z}$ des entiers ; pour un diviseur premier $\mathfrak{p}$, c'est le degré de l'extension résiduelle $\mathrm{P}/\mathfrak{p}$ relativement à $(\mathrm{P}\cap k[z])/(\mathfrak{p}\cap k[z])$; les diviseurs d'éléments de K sont d'ordre 0, donc tous les diviseurs d'une même classe *modulo* le sous-groupe $\mathbb{H}$ des diviseurs d'éléments de K ont le même ordre. Si z appartient à K mais pas à k et que K est séparable sur $k(z)$, Schmidt associe à l'extension $K/k(z)$ un diviseur *différente* ∂_z dont l'ordre est l'indice de *ramification* w_z de K sur $k(z)$; le *genre* de K est défini par

$$g = \frac{w_z}{2} - m_z + 1$$

où $m_z = [K : k(z)]$ et il est indépendant du choix de z.

Le point central de la théorie de Schmidt est l'analogue du théorème de *Riemann-Roch* dans le théorie classique des fonctions algébriques d'une variable, il permet d'évaluer le nombre des diviseurs entiers qui appartiennent à une classe donnée de diviseurs $\mathbb{C} \in \mathbb{D}/\mathbb{H}$. Si $\mathfrak{c}$ est un diviseur donné, les diviseurs entiers équivalents sont de la forme $(\alpha)\mathfrak{c}$ où $\alpha \in K$ est choisi tel que (α) soit multiple de $\mathfrak{e}/\mathfrak{c}$ ($\mathfrak{e}$ note le diviseur neutre). Un premier résultat (difficile) est que les $\alpha \in K$ tels que (α) soit multiple d'un diviseur donné forment un sous-k-espace vectoriel de rang fini ; Schmidt établit ensuite que ce rang r ne dépend que de la classe $\mathbb{C}$ de $\mathfrak{c}$ dans le cas où le diviseur donné est $\mathfrak{e}/\mathfrak{c}$ et il l'appelle la *dimension* $\{\mathbb{C}\} = r$ de $\mathbb{C}$. Si k a p éléments, le nombre de diviseurs entiers dans $\mathbb{C}$ est $(p^r - 1)/(p - 1)$. Le théorème de Riemann-Roch s'énonce par la relation

$$\{\mathbb{C}\} = \left\{\frac{\mathbb{W}}{\mathbb{C}}\right\} + q - g + 1$$

où q est l'ordre de la classe $\mathbb{C}$ et $\mathbb{W}$ est la *classe différentielle* de K, c'est-à-dire celle des diviseurs ∂_z/n_z^2 où z est un élément de K non dans k, de dénominateur n_z ; on en tire (en faisant successivement $\mathbb{C} = \mathbb{H}$ et $\mathbb{C} = \mathbb{W}$) que $\mathbb{W}$ est d'ordre $2g-2$, donc la classe *complémentaire* $\mathbb{C}' = \mathbb{W}/\mathbb{C}$ de $\mathbb{C}$ est d'ordre $q' = 2g-2-q$. Ceci permet de donner au théorème une forme symétrique

$$\{\mathbb{C}\} - \frac{q}{2} = \{\mathbb{C}'\} - \frac{q'}{2};$$

lorsque $q \geqslant 2g-2, q' \leqslant 0$ donc

$$\{\mathbb{C}'\} = 0 \quad \text{et} \quad \{\mathbb{C}\} = q - g + 1 \ (> 0 \text{ si } q > 0).$$

La fonction zêta associée par Schmidt au corps K est définie par le produit infini

$$\mathbb{Z}(s) = \prod_{\mathfrak{p}} \frac{1}{1 - |\mathfrak{p}|^{-s}}$$

étendu à tous les diviseurs premiers de K et dans lequel $|\mathfrak{p}| = p^f$ si $\mathfrak{p}$ est d'ordre f ; le produit converge pour $\mathrm{Re}(s) > 1$ et il est égal à la somme de la série $\sum_{\mathfrak{c}} 1/|\mathfrak{c}|^s$ (où $\mathfrak{c}$ parcourt l'ensemble des diviseurs entiers). Schmidt somme cette série réunissant les $\mathfrak{c}$ d'une même classe ; il n'y a qu'un nombre fini de $\mathfrak{c}$ avec un ordre $< q_0 = 2g-2$ et, pour les autres, le nombre d'éléments de la classe est donné explicitement par le théorème de Riemann-Roch ; il démontre en même temps que le p.g.c.d. des ordres des diviseurs premiers est 1 et il trouve finalement

$$\mathbb{Z}(s) = \frac{1}{p-1} \sum_{q=1}^{q_0-1} \sum_{i=1}^{h} \frac{p^{\{\mathbb{C}_q^{(i)}\}}}{p^{qs}} + \frac{hp^{-(g-1)}}{p-1} \cdot \frac{p^{(2g-2)(1-s)}}{1-p^{1-s}} + \frac{h}{p-1} \cdot \frac{1}{1-p^s}$$

où h est le nombre (fini) des classes de diviseurs d'ordre 0. Cette formule et le théorème de Riemann-Roch donnent l'équation fonctionnelle

$$\mathbb{Z}(1-s) = p^{(g-1)(2s-1)} \mathbb{Z}(s).$$

Schmidt compare sa fonction zêta à celle qu'on obtiendrait en considérant les idéaux d'un anneau $\mathfrak{I}$ à la manière d'Artin et il retrouve les résultats d'Artin dans le cas particulier des extensions quadratiques.

3. H. Hasse

H. Hasse a pu démontrer l'hypothèse de Riemann pour la fonction zêta de Schmidt dans le cas où le genre g est 1 ; il a exposé ce résultat au Congrès international d'Oslo en 1936. Partant d'un polynôme irréductible à deux variables $f(X,Y) \in \mathbb{F}_p[X,Y]$ (p premier), il considère un facteur irréductible f_0 de f sur la clôture algébrique k de $\mathbb{F}_p$ et le corps k_0 engendré par les coefficients de f_0 ; le corps K_0 est alors l'extension de k_0 engendrée par X et Y liés par $f_0(X,Y) = 0$. Si $q = p^f$ est le nombre d'éléments de k_0, la fonction zêta s'écrit

$$\mathbb{Z}(s) = \prod_{\mathfrak{p}} \frac{1}{1-(N\mathfrak{p})^{-s}} = \prod_{n\geqslant 1} \left(\frac{1}{1-q^{-ns}}\right)^{N_n} = 1 + \frac{N_1}{q^s} + \cdots$$

où N_n est le nombre de diviseurs premiers de *degré* n (on dit désormais *degré* au lieu d'*ordre* comme Schmidt) ; Hasse la décompose en $\mathbb{Z}_0(s)L(s)$ avec

$$\mathbb{Z}_0(s) = \frac{1}{1-1/q^s} \cdot \frac{1}{1-q/q^s} = 1 + \frac{q+1}{q^s} + \cdots$$

(fonction zêta de $k_0(X)$) et

$$L(s) = 1 + \frac{N_1-(q+1)}{q^s} + \cdots + \frac{q^s}{q^{2gs}} = \prod_{i=1}^{g} (1-\omega_i/q^s)$$

où g est le genre de K_0.

Avec ces notations

$$N_1 - (q+1) = \sum_{i=1}^{2g} \omega_i$$

et l'hypothèse de Riemann, qui s'écrit $|\omega_i| = q^{1/2}$ pour $1 \leqslant i \leqslant 2g$, implique l'inégalité

$$|N_1 - (q+1)| \leqslant 2g\sqrt{q}.$$

Dans le cas où $g = 1$, on a

$$L(s) = 1 + \frac{N_1-(q+1)}{q^s} + \frac{q}{q^{2s}}$$

et l'hypothèse de Riemann signifie que les racines ω_1 et ω_2 sont imaginaires conjuguées c'est-à-dire que

$$|N_1 - (q+1)| \leqslant 2\sqrt{q};$$

des inégalités moins précises avaient été obtenues par Davenport et par Mordell dans le cas d'une équation

$$Y^2 = f(X),$$

f polynôme de degré 3 à coefficients dans $\mathbb{F}_p$ (avec des exposants 3/4 ou 2/3 au lieu de 1/2).

Pour démontrer l'hypothèse de Riemann, Hasse étudie la structure de l'ensemble $\mathbb{A}$ des « points » de $K = k(X, Y)$ (ce sont, par définition, les diviseurs premiers de degré 1) ; parmi ces points, les N_1 diviseurs premiers de degré 1 de K_0 sont caractérisés par leur invariance relativement à l'opération de *Frobenius* π, qui provient de l'élévation à la puissance q de X et de Y. D'une manière précise, $\pi : \varphi(X, Y) \mapsto \varphi(X^q, Y^q)$ est un isomorphisme de K sur un sous-corps $K\pi = k(X^q, Y^q)$ et on pose, pour tout diviseur premier $\mathfrak{p}$ de K,

$$\pi\mathfrak{p} = (N_{K/K\pi}\mathfrak{p})^{\pi^{-1}}.$$

Hasse dit qu'un isomorphisme μ de K sur un sous-corps $K\mu$ est un *méromorphisme* de K et il le fait opérer sur $\mathbb{A}$ en posant

$$\mu\mathfrak{p} = (N_{K/K\mu}\mathfrak{p})^{\mu^{-1}}.$$

Lorsqu'on choisit une origine $\mathfrak{o}$ dans $\mathbb{A}$ on établit une correspondance bijective $\mathfrak{p} \mapsto \mathfrak{p}/\mathfrak{o}$ de $\mathbb{A}$ sur le groupe $\mathbb{D}_0/\mathbb{H}$ des classes de diviseurs de degré 0, d'où une loi de groupe commutatif sur $\mathbb{A}$; l'ensemble M des méromorphismes de $\mathbb{A}$ qui laissent $\mathfrak{o}$ invariant a alors une structure d'*anneau* (non nécessairement commutatif) qui contient $\mathbb{Z}$. La *norme*

$$\mu \mapsto N(\mu) = [K : K\mu] \quad (\mu \in M)$$

est multiplicative et c'est une fonction quadratique de μ, d'où on déduit l'inégalité (de Cauchy-Schwarz)

$$(N(\mu \pm \nu) - N(\mu) - N(\nu))^2 \leqslant 4N(\mu)N(\nu)$$

et le fait que tout méromorphisme μ vérifie une équation du second degré $\mu^2 + \ell\mu + m = 0$ avec

$$\ell = N(\mu - 1) - N(\mu) - 1 = \mu + \overline{\mu} \quad \text{et} \quad m = N(\mu) = \mu\overline{\mu}$$

($\overline{\mu}$ « conjugué » de μ) ; l'inégalité précédente montre que $\ell^2 \leqslant 4m$. Dans le cas du méromorphisme π de Frobenius, $m = N(\pi) = q$ et $N(\pi - 1) = N_1$ (nombre de points fixe par π) donc

$$\ell = N(\pi - 1) - N(\pi) - 1 = N_1 - (q + 1);$$

l'inégalité trouvée est précisément celle qui exprime l'hypothèse de Riemann.

Hasse termine son travail en indiquant une voie, suggérée par Deuring, pour étendre cette théorie aux corps du genre g quelconque. Pour $g \geqslant 2$ il n'y a plus de loi de groupe sur $\mathbb{A}$ ni d'anneau des méromorphismes, mais on peut construire un anneau des *correspondances* sur le modèle de la théorie développée par Hurwitz en 1886 pour les surfaces de Riemann (une correspondance (m, n) associe un n-uple de points à un m-uple de points).

4. A. Weil

C'est cette voie qu'A. Weil (1940) a suivie pour démontrer l'hypothèse de Riemann dans le cas d'un genre g quelconque. Mais pour développer sa méthode, Weil a de nouveau déplacé le cadre théorique : au lieu de la théorie des fonctions algébriques d'une variable, il prend pour modèle celui de la *géométrie* des courbes algébriques. Ceci l'a amené à développer la géométrie algébrique sur un corps de base (commutatif) arbitraire (Weil 1946) ou géométrie algébrique abstraite. Sur un corps de base k parfait (par exemple fini ou algébriquement clos ou de caractéristique 0), un corps K de fonctions algébriques d'une variable peut s'interpréter comme le corps Ω_k des fonctions sur une courbe algébrique complète Γ sans point multiple qui admettent k comme corps de définition ; les diviseurs de K correspondent aux *diviseurs* sur Γ rationnels par rapport à k, qui sont des combinaisons linéaires de points de Γ à coefficients entiers. En géométrie, on note additivement la loi du groupe des diviseurs. Si le

corps de base k est fini, à q éléments, on définit la fonction zêta de Γ par

$$Z(u) = \sum_{\mathfrak{a}} u^{\deg(\mathfrak{a})} = \prod_{\mathfrak{p}} \left(1 - u^{\deg(\mathfrak{p})}\right)^{-1}$$

où la somme est étendue à tous les diviseurs positifs rationnels par rapport à k et le produit à tous les diviseurs premiers rationnels par rapport à k ; la variable u remplace q^{-s} et la convergence a lieu pour $|u| < 1/q$. Weil établit que Z est une fonction *rationnelle*, de la forme

$$\frac{P(u)}{(1-u)(1-qu)}$$

où P est un polynôme de degré $2g$ où g est le *genre* de la courbe Γ et que l'on a une équation fonctionnelle

$$Z\left(1/qu\right) = q^{1-g}u^{2-2g}Z(u);$$

ceci résulte, comme dans la théorie de Schmidt, du théorème de Riemann-Roch qui permet d'évaluer le rang $\ell(\mathfrak{a})$ (sur le corps des constantes) de l'espace vectoriel des diviseurs positifs équivalents à un diviseur $\mathfrak{a}$ donné : $\ell(\mathfrak{a}) = \deg(\mathfrak{a}) - g + 1 + r(\mathfrak{a})$ où le genre g est défini comme la valeur maximum de $\deg(\mathfrak{a}) - \ell(\mathfrak{a}) + 1$ lorsque $\mathfrak{a}$ varie et $r(\mathfrak{a}) = \ell(\mathfrak{k} - \mathfrak{a})$ en notant $\mathfrak{k}$ (k gothique) un diviseur *canonique*, c'est-à-dire la projection sur Γ d'un cycle d'intersection $\Delta \cdot [(\theta) - \Delta]$ (Δ désigne la diagonale du produit $\Gamma \times \Gamma$ et θ une fonction sur ce produit s'annulant à l'ordre 1 le long de Δ et admettant k comme corps de définition ; la classe $\omega = \{\theta\}$ de θ *modulo* les θ' qui s'annulent le long de Δ à un ordre > 1 est appelée une *différentielle* et le diviseur $\mathfrak{k} = (\omega)$ ne dépend que de ω). Tous les diviseurs canoniques sont équivalents et de degré $2g - 2$; on a $\ell(\mathfrak{k}) = g$ et $r(\mathfrak{k}) = 1$.

On a

$$d(\log Z(u)) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \deg(\mathfrak{p}) u^{m \deg(\mathfrak{p})} \frac{du}{u} = \sum_{n=1}^{\infty} \nu_n u^n \frac{du}{u}$$

où $\nu_n = \sum_{\deg(\mathfrak{p})|n} \deg(\mathfrak{p})$ s'interprète comme le nombre de points P de Γ dont le corps de définition $k(\mathrm{P})$ est contenu dans l'extension k_n

de degré n de k (unique sous-corps à q^n éléments dans la clôture algébrique de k). Ainsi ν_n est le nombre de points fixes de la *correspondance* de Frobenius itérée I_n définie par l'élévation des coordonnées à la puissance q^n-ième.

Une correspondance X sur Γ est, par définition, un diviseur sur le produit $\Gamma \times \Gamma$ (combinaison linéaire formelle à coefficients entiers de courbes). On fait opérer X sur les diviseurs de Γ de la manière suivante ; si $X = X_0 + \mathfrak{a} \times \Gamma$ où X_0 n'a pas de composante de la forme $\mathrm{A} \times \Gamma$ (A point de Γ) et $\mathfrak{a}$ est un diviseur de Γ, $X(\mathfrak{b})$ est la deuxième projection de l'intersection $X_0(\mathfrak{b} \times \Gamma)$ ($\mathfrak{b}$ diviseur quelconque de Γ). Le groupe additif des correspondances est muni d'une forme bilinéaire $(X, Y) \mapsto I(X, Y)$ (à valeurs entières) telle que $I(X, Y) = \deg(X \cdot Y)$ lorsque le produit d'intersection $X \cdot Y$ est défini et d'une relation d'équivalence $\equiv$ telle que $X \equiv 0$ équivaille au fait que X transforme tout diviseur $\mathfrak{m}$ de degré 0 en le diviseur $X(\mathfrak{m})$ d'une fonction sur Γ. Les correspondances se composent de manière que $X \circ Y$ transforme $\mathfrak{b}$ en $X(Y(\mathfrak{b}))$ et cette loi de composition est compatible avec la relation d'équivalence ; l'ensemble des *classes de correspondances* est ainsi muni d'une structure d'*anneau* (non commutatif) dont l'élément unité est la classe δ de la diagonale Δ. Cet anneau A possède une anti-involution $\xi \mapsto \xi'$ qui provient de la symétrie $P \times Q \mapsto Q \times P$ de $\Gamma \times \Gamma$ et une *trace* $\sigma : A \to \mathbb{Z}$ (forme linéaire) telle que $\sigma(\xi') = \sigma(\xi)$ et $\sigma(\xi \cdot \eta) = \sigma(\eta \cdot \xi)$. La trace $\sigma(\xi)$ d'une classe de correspondances ξ est définie comme dans la théorie de Hurwitz : si X est une correspondance de classe ξ, on lui associe des entiers $d(X)$ et $d'(X)$ de manière que les deux projections de X sur Γ soient $d(X)\Gamma$ et $d'(X)\Gamma$, puis on pose $S(X) = d(X) + d'(X) - I(X \cdot \Delta) = \sigma(\xi)$ (cela ne dépend que de ξ). La trace de δ est $2g$ où g est le genre.

La clef de la démonstration de Weil est l'analogue abstrait d'un théorème démontré par Castelnuovo et Severi (1926) pour la géométrie algébrique complexe : pour toute classe de correspondances $\xi \neq 0$, $\sigma(\xi \cdot \xi') > 0$. Si le genre est 1, on a $\xi \cdot \xi' = N\delta$ avec un entier $N > 0$, d'où $\sigma(\xi \cdot \xi') = 2N > 0$; pour les genres supérieurs, Weil le démontre en travaillant dans la variété $\Omega = \Gamma \times \Gamma \times \cdots \times \Gamma$ produit de $d(X)$ facteurs égaux à Γ. On en déduit (Cauchy-Schwarz)

que $(\sigma(\xi \cdot \eta'))^2 \leqslant \sigma(\xi \cdot \xi')\sigma(\eta \cdot \eta')$. Dans le cas de la correspondance de Frobenius itérée I_n, on a

$$I_n \circ I'_n = q^n\Delta, \quad d(I_n) = 1, \quad d'(I_n) = q^n, \quad \deg(I_n \cdot \Delta) = \nu_n$$

donc

$$S(I_n) = 1 + q^n - \nu_n = \sigma(\iota^n)$$

en notant ι la classe de la correspondance de Frobenius I_1 ; l'inégalité de Cauchy-Schwarz appliquée à $\xi = \iota^n$ et $\eta = \delta$ s'écrit donc

$$(**) \qquad |\sigma(\iota^n)| = |1 + q^n - \nu_n| \leqslant 2gq^{n/2}$$

Le numérateur $P(u) = (1-u)(1-qu)Z(u)$ de la fonction zêta a pour dérivée logarithmique

$$d(\log P(u)) = -\sum_{n=1}^{\infty} \sigma(\iota^n)u^n \frac{du}{u}$$

et l'inégalité $(**)$ montre que cette série converge pour $|u| < q^{-1/2}$; ainsi P n'a ni zéro ni pôle dans ce disque et Z n'y a donc pas de zéro et pas d'autre pôle que $u = 1/q$.

L'équation fonctionnelle permet alors d'en déduire que $Z(u)$ ne s'annule pas non plus pour $|u| > q^{-1/2}$ et que son seul pôle dans ce domaine est $u = 1$; on a ainsi établi l'hypothèse de Riemann selon laquelle les zéros de $Z(u)$ ont tous $q^{-1/2}$ pour valeur absolue.

Weil a poursuivi son travail en interprétant le polynôme P comme un polynôme caractéristique au moyen de la théorie des *jacobiennes* de courbes (1948). À une courbe Γ de genre g est associée une *variété abélienne* J de dimension g, birationnellement équivalente au produit symétrique de g facteurs égaux à Γ, ainsi qu'une fonction $\varphi : \Gamma \to J$ définie à une constante additive près ; rappelons qu'une variété abélienne est, par définition, une variété de groupe qui est complète et que sa loi de groupe est automatiquement commutative. Le groupe des points J est isomorphe au groupe des classes de diviseurs de degré 0 sur Γ et l'anneau A des classes de correspondances sur Γ s'identifie à l'anneau des endomorphismes de J. Si ℓ est un nombre premier $\neq p$, le groupe $\mathfrak{g}_\ell(J)$ des points de J dont l'ordre est une puissance de ℓ est isomorphe à $\mathbb{Q}_\ell^{2g}/\mathbb{Z}_\ell^{2g}$; à la classe de Frobenius ι est associé un endomorphisme de J qui opère sur ce groupe et que l'on peut représenter par une matrice carrée $M_\ell(\iota)$ d'ordre $2g$ à coefficients entiers ℓ-adiques. Alors P est le polynôme caractéristique de cette matrice.

Weil a ensuite essayé d'étendre sa théorie à des variétés algébriques X_0 de dimension quelconque définies sur un corps fini k à q éléments : en notant encore ν_n le nombre des points P de X_0 tels que $k(\mathrm{P})$ soit contenu dans le corps k_m à q^m éléments, il définit la fonction zêta de X_0 par les conditions $Z(0) = 1$ et

$$t\frac{d}{dt}\log Z(t) = \sum_{m=1}^{\infty} \nu_m t^m.$$

Pour des exemples simples, il est facile de calculer les ν_m et de déterminer explicitement $Z(t)$; par exemple pour l'espace affine de dimension r on $\nu_m = q^{mr}$ donc

$$t\frac{d}{dt}\log Z(t) = \frac{q^r t}{1-q^r t} \quad \text{et} \quad Z(t) = \frac{1}{1-q^r t}.$$

De même, pour l'espace projectif de dimension r, $\nu_m = 1 + q^m + \cdots + q^{mr}$ donc

$$t\frac{d}{dt}\log Z(t) = \frac{t}{1-t} + \frac{qt}{1-qt} + \cdots + \frac{q^r t}{1-q^r t}$$

ce qui donne

$$Z(t) = \frac{1}{(1-t)(1-qt)\cdots(1-q^r t)}.$$

Le cas de la *grassmannienne* des sous-espaces de dimension r dans $\mathbb{P}_n$ est aussi calculé par Weil : on a

$$\nu_m = \frac{q^{m(n+1)}-1}{q^m-1}\cdots\frac{q^{m(n+1)}-q^{mr}}{q^{m(r+1)}-q^{mr}} = 1 + b_1 q^m + \cdots + b_d q^{dm}$$

où $d = (n-r)(r+1)$ est la dimension de la grassmannienne et les coefficients b_i sont des entiers. Ainsi

$$t\frac{d}{dt}\log Z(t) = \frac{t}{1-t} + b_1\frac{qt}{1-qt} + \cdots + b_d\frac{q^d t}{1-q^d t},$$

ce qui donne

$$Z(t) = \frac{1}{(1-t)(1-qt)^{b_1}\cdots(1-q^d t)^{b_d}};$$

sur le corps des complexes, la grassmannienne correspondante a pour nombre de Betti b_i en dimension $2i$.

Weil formule enfin ses conjectures générales à la fin d'un article de 1949 consacré au cas des *hypersurfaces monomiales*, c'est-à-dire des variétés d'équation

$$a_0x_0^{n_0} + a_1x_1^{n_1} + \cdots + a_rx_r^{n_r} = b$$

dans l'espace affine de dimension $r+1$. Il fait le décompte des points au moyen d'une méthode déjà mise en œuvre par Hardy et Littlewood (1922) dans leur étude du problème de Waring et reprise par Hasse et Davenport (1935) à propos de l'équation $ax^m + by^n + cz^r = 0$; cette méthode utilise les *sommes de Gauss* bien connues en théorie des nombres et elle permet d'établir, pour le nombre N des points de l'hypersurface avec $b = 0$, l'inégalité

$$|N - q^r| \leqslant M(q-1)q^{(r-1)/2}$$

où M est une constante dépendant seulement des exposants n_i. Le calcul peut être mené à terme avec b quelconque en supposant que tous les n_i sont égaux à un même nombre n ; Weil trouve que

$$Z(U) = \frac{P_{r-1}(U)^{(-1)^r}}{(1-U)(1-qU)\cdots(1-q^{r-1}U)}$$

où P_{r-1} est un polynôme de degré M dont tous les zéros sont de valeur absolue $q^{-\frac{r-1}{2}}$. Or une variété algébrique *complexe* définie par une équation du même type a des nombres de Betti $B_{r-1} = M$ et, pour $h < r-1, B_h = 1$ ou 0 selon que h est pair ou impair.

Ces résultats conduisent Weil à formuler les conjectures suivantes :

(1) La fonction zêta d'une variété algébrique X_0 de dimension n sur k est *rationnelle*.

(2) Elle satisfait une *équation fonctionnelle*

$$Z\left(1/q^n t\right) = \pm q^{n\chi/2}t^{\chi}Z(t)$$

où $\chi = (\Delta\cdot\Delta)$ joue le rôle de la *caractéristique d'Euler-Poincaré* de X_0.

(3) On a

$$Z(t) = \frac{P_1(t)P_3(t)\cdots P_{2n-1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)}$$

où $P_0(t) = 1-t$, $P_{2n}(t) = 1-q^nt$ et, pour $1 \leqslant h \leqslant 2n-1$, $P_h(t)$ est un polynôme dont les racines sont des entiers algébriques de valeur absolue $q^{-h/2}$.

(4) En définissant le *nombre de Betti* B_h de X_0 en dimension h comme le degré de P_h, on a $\chi = \sum_{h=0}^{2n}(-1)^h B_h$. De plus, si X est une variété algébrique sans point multiple sur un corps de nombres algébriques K, les nombres de Betti classiques de X coïncident pour presque tout idéal premier $\mathfrak{p}$ de K avec ceux de la réduction $X_\mathfrak{p}$ de X mod $\mathfrak{p}$.

A. Weil indique de plus un programme pour démontrer ces conjectures : il s'agit de construire, pour les variétés algébriques X (sans point multiple) sur un corps fini k, une théorie cohomologique convenable ; cette théorie doit faire correspondre à chaque X une suite d'espaces vectoriels $H^i(X)$ sur un corps K de *caractéristique* 0 et ceci d'une manière fonctorielle et avec les propriétés suivantes :

(1) *Dualité de Poincaré* : si X est de dimension n, $h^i(X) = 0$ sauf pour $0 \leqslant i \leqslant 2n$, $H^{2n}(X) \approx K$ et on a un accouplement bilinéaire $H^i(X) \times H^{2n-i}(X) \to H^{2n}(X)$ permettant d'identifier $H^{2n-i}(X)$ au dual de $H^i(X)$.

(2) *Formule de Künneth* : $H^*(X) \otimes_K H^*(Y) \approx H^*(X \times Y)$.

(3) *Classe d'un cycle* : il y a un homomorphisme γ_X, fonctoriel et compatible avec la multiplication, du groupe $C^i(X)$ des classes de cycles (pour l'équivalence numérique) de codimension i dans $H^{2i}(X)$.

(4) *Théorème de Lefschetz* pour les sections hyperplanes.

Une telle théorie dispose d'une *formule de Lefschetz* qui permet de calculer le nombre de points fixes d'une correspondance $f \in H^0(X \times X)$ sous la forme

$$\langle f \cdot \Delta \rangle = \sum_{i=0}^{2n}(-1)^i \mathrm{Tr}(f_i)$$

où f_i est l'endomorphisme de $H^i(X)$ induit par f ; cette formule est l'extension, en dimension quelconque, de la formule de Hurwitz pour les courbes (pour lesquelles la jacobienne jouait d'ailleurs le rôle de H^1). En notant F la correspondance de Frobenius, on a

$$\nu_m = \sum_{i=0}^{2n}(-1)^i \mathrm{Tr} F_i^m$$

d'où

$$t\frac{d}{dt}\log Z(t) = \sum_{i=0}^{2n}(-1)^i \sum_m \mathrm{Tr}(F_i^m)t^m$$
$$= \sum_{i=0}^{2n}(-1)^{i+1} t\frac{d}{dt}\log\det(1-tF_i)$$

et, finalement

$$Z(t) = \prod_{i=0}^{2n}\det(1-tF_i)^{(-1)^{i+1}}$$

ce qui donne la première conjecture (rationalité) ; la dualité de Poincaré donne l'équation fonctionnelle (conjecture 2) et on déduit l'hypothèse de Riemann (conjecture 3) des théorèmes de Lefschetz sur les sections hyperplanes, qui permettent de raisonner par récurrence sur la dimension.

Weil (1954) a lui-même démontré ses conjectures dans certains cas particuliers autres que ceux déjà indiqués, comme les intersections de deux quadriques ou les surfaces cubiques. La première démonstration de la conjecture 1 est due à Dwork (1959) ; elle n'utilise pas de cohomologie mais une évaluation directe des ν_m à l'aide de sommes de Gauss grâce à une technique de relèvements p-adiques et des développements d'analyse p-adique. La méthode de Dwork a reçu par la suite une interprétation cohomologique. Entre temps A. Grothendieck a pu construire une théorie cohomologique répondant aux exigences de Weil et démontrer une partie des conjectures ; P. Deligne a établi les théorèmes de Lefschetz pour la cohomologie de Grothendieck et il a terminé la démonstration des conjectures.

Cette histoire est exemplaire des rapports entre l'arithmétique, l'algèbre et la géométrie au vingtième siècle. Elle montre la fécondité de la démarche qui consiste à transporter des idées et des méthodes du cadre qui les a suscitées dans un cadre différent. Mais l'hypothèse de Riemann classique, concernant la fonction zêta du corps des rationnels n'est toujours pas démontrée et il est peu probable qu'on l'atteigne par le genre de méthode dont nous avons parlé.

Christian Houzel, Département de Mathématiques,Université de Paris VII, 2, place Jussieu, 75230 Paris cedex 05, France