Les conjectures de Weil

> Quant à l'influence de A. Weil, qu'il nous suffise de dire que c'est la nécessité de développer l'outillage nécessaire pour formuler avec toute la généralité voulue la définition de la « cohomologie de Weil » et pour aborder la démonstration de toutes les propriétés formelles nécessaires pour établir ses célèbres conjectures en Géométrie diophantienne, qui a été une des principales motivations de la rédaction du présent Traité (...).
> — EGA, Introduction.

André Weil, en menant des calculs assez élémentaires sur le nombre de solutions de certains systèmes d'équations algébriques dans les corps finis, a été conduit à formuler en 1949 une série de remarquables conjectures qui relient, pour une variété algébrique X définie sur un corps de nombres, le nombre de points de X sur un corps fini et ses extensions d'une part, et des propriétés plutôt topologiques de la variété analytique $X(\mathbf{C})$ d'autre part. En établissant ainsi une relation entre une information de nature arithmétique sur X et la topologie, Weil a inauguré tout un programme qui a servi de guide aux fondateurs de la géométrie algébrique moderne, et qui consiste schématiquement à exprimer, dans un langage purement algébrique valable sur une large classe de corps ou d'anneaux, les constructions que la géométrie et la topologie différentielles fournissent sur $\mathbf{C}$.

Après quelques indications heuristiques et historiques sur les conjectures de Weil dans le cas général, on en démontrera une partie dans le cas des courbes, qui était déjà bien connu de Weil lui-même. Enfin, on tentera de montrer comment, dans le cas très particulier et concret des courbes elliptiques, on peut construire à la main une sorte de cohomologie ad hoc ayant des propriétés formelles suffisantes pour en déduire les conjectures. L'exposé de ces cas particuliers n'a pas, bien sûr, l'envergure grandiose et la profondeur de la dimension quelconque, mais il illustre déjà, on l'espère, certains objets et certaines idées qui interviennent dans les développements plus ambitieux, tout en restant relativement élémentaire.

1 Énoncé et origine des conjectures

1.1 Fonction zêta d'une variété algébrique

Soit k un corps[1] quelconque. On appellera ici variété algébrique (projective) X définie sur k la donnée, pour un certain entier $n \geq 1$, d'une famille quelconque de polynômes homogènes P_i de $k[X_0, \ldots, X_n]$. Pour tout surcorps K de k, on définit alors l'ensemble $X(K)$ des points de X sur K comme l'ensembles des points $(x_0 : \ldots : x_n)$ de l'espace projectif $\mathbf{P}^n(K)$ vérifiant $P_i(x_0, \ldots, x_n) = 0$ pour tout i.

Étant donnée une variété algébrique X définie sur le corps $k = \mathbf{F}_q$ à q éléments, on peut donc s'intéresser à l'ensemble des points de X sur les corps $k_m = \mathbf{F}_{q^m}$. Or, pour chaque m, $\mathbf{P}^n(k_m)$ est fini :

$$|\mathbf{P}^n(k_m)| = \frac{q^{m(n+1)} - 1}{q^m - 1} = 1 + q^m + q^{2m} + \cdots + q^{nm}$$

1. On ne parle ici que de corps et d'anneaux *commutatifs*. Cette partie s'inspire du premier chapitre du cours de Katz [Kat74] et de l'appendice C de Hartshorne [Har77]. Pour les notes historiques, le panorama dressé par Dieudonné [Die75] et l'exposé introductif de Katz [Kat76] ont été d'un grand secours.

donc il en est a fortiori de même pour $X(k_m)$, et on a la majoration $|X(k_m)| \leq |\mathbf{P}^n(k_m)|$. Ce dont vont parler les conjectures de Weil, c'est précisément de ces nombres de points, que F.K. Schmidt a eu l'idée de rassembler en une série formelle appelée fonction zêta.

Définition 1.1 Si X est une variété algébrique définie sur $k = \mathbf{F}_q$, et N_m le nombre de points de X sur $k_m = \mathbf{F}_{q^m}$, on appelle fonction zêta de X la série :

$$Z_X(T) = \exp\left(\sum_{m=1}^{+\infty} N_m \frac{T^m}{m}\right)$$

Exemple 1.1 On peut facilement calculer la fonction zêta de $\mathbf{P}^n$. Elle s'écrit :

$$\begin{aligned}
\log Z_{\mathbf{P}^n}(T) &= \sum_{m=1}^{+\infty} (1 + q^m + \cdots + q^{nm}) \frac{T^m}{m} \\
\log Z_{\mathbf{P}^n}(T) &= \sum_{k=0}^{n} \sum_{m=1}^{+\infty} \frac{(q^k T)^m}{m} \\
\log Z_{\mathbf{P}^n}(T) &= \sum_{k=0}^{n} -\log(1 - q^k T) \\
Z_{\mathbf{P}^n}(T) &= \frac{1}{(1-T)(1-qT)\cdots(1-q^nT)}
\end{aligned}$$

On peut noter, et l'observation n'est bien sûr pas innocente, que l'on obtient ainsi une fraction rationnelle, ce qui est tout de même remarquable au regard de la définition de la fonction zêta.

On va essayer d'esquisser une motivation un peu plus forte de cette définition que l'allure agréable de l'exemple précédent, et en particulier tenter de justifier le nom de « fonction zêta ». Pour cela, on va considérer l'ensemble $X(K)$ des points de X sur une clôture algébrique $\bar{k}$ de k, qui n'est rien d'autre que la réunion des $X(k_m)$. Alors $G = \mathrm{Gal}(\bar{k}/k)$ opère sur $X(\bar{k})$ coordonnée par coordonnée.

On appellera place de X toute G-orbite de points de $X(\bar{k})$. Une place est ainsi une sous-variété non vide définie sur k et minimale. C'est un ensemble fini. Si $\mathfrak{p}$ est une place de X, on note $\deg \mathfrak{p}$ son cardinal, encore appelé degré, et l'on appelle norme de $\mathfrak{p}$ l'entier $N\mathfrak{p} = q^{\deg \mathfrak{p}}$.

Le résultat suivant fait alors apparaître le lien avec les fonctions zêta que l'on rencontre en théorie des nombres.

Proposition 1 *La fonction zêta de X s'écrit sous la forme d'un produit infini étendu à toutes les places de X :*

$$Z_X(T) = \prod_{\mathfrak{p}} \frac{1}{1 - T^{\deg \mathfrak{p}}}$$

Si l'on introduit la fonction $\zeta_X(s) = Z_X(q^{-s})$, cette relation devient :

$$\zeta_X(s) = \prod_{\mathfrak{p}} \frac{1}{1 - (N\mathfrak{p})^{-s}}$$

Démonstration. On note P_r l'ensemble des places de X de degré r. Alors pour tout m, $X(k_m)$ est la réunion des P_r pour r divisant m. Il suffit pour cela de voir qu'un élément quelconque de $\bar{k}$ est dans k_m si et seulement si le cardinal de sa G-orbite divise m.

Cela étant, les P_r sont des ensembles finis, et si l'on note $B_r = |P_r|$, on a :

$$N_m = \sum_{r|m} r B_r$$

de sorte que :

$$\begin{aligned}
\sum_{m=1}^{\infty} N_m \frac{T^m}{m} &= \sum_{m=1}^{\infty} \frac{T^m}{m} \sum_{r|m} rB_r \\
\sum_{m=1}^{\infty} N_m \frac{T^m}{m} &= \sum_{r=1}^{\infty} rB_r \sum_{k=1}^{\infty} \frac{T^{rk}}{rk} \\
\sum_{m=1}^{\infty} N_m \frac{T^m}{m} &= \sum_{r=1}^{\infty} -B_r \log(1-T^r) \\
Z_X(T) &= \prod_{r=1}^{\infty} (1-T^r)^{-B_r} = \prod_{\mathfrak{p}} (1-T^{\deg \mathfrak{p}})^{-1}
\end{aligned}$$

□

Ce résultat est évidemment à rapprocher de l'expression sous forme de produit infini de la fonction zêta de Riemann :

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$$

ou mieux, des fonctions zêta de Dedekind. En fait, il y a plus qu'une analogie formelle entre ces fonctions. Dans un formalisme adéquat (le langage des schémas), on peut donner une définition générale des fonctions zêta qui englobe entre autres tous ces cas.

1.2 Les conjectures de Weil

On peut alors énoncer effectivement les conjectures. Soit X une variété algébrique (projective) définie sur $k = \mathbf{F}_q$ et de dimension [2] n que l'on suppose absolument irréductible et non-singulière (moralement, une variété connexe et lisse). Alors Weil a formulé les conjectures suivantes sur la fonction zêta $Z(T)$ de X.

Rationalité. $Z(T)$ est une fraction rationnelle. Plus précisément, il existe des polynômes $P_0, \ldots, P_{2n}$ à à coefficients entiers, de termes constants égaux à 1, tels que :

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

De plus, $P_0(T) = 1 - T$ et $P_{2n}(T) = 1 - q^n T$.

Hypothèse de Riemann. On peut choisir (et ce, bien sûr, d'une seule manière) les polynômes précédents de telle sorte que les racines de P_i soient toutes de module $q^{-i/2}$.

Équation fonctionnelle. Soit $\chi = \sum_i (-1)^i \deg P_i$. On appelle χ la caractéristique d'Euler de X. Alors pour un certain signe $\varepsilon = \pm 1$, $Z(T)$ vérifie l'équation fonctionnelle :

$$Z\left(\frac{1}{q^n T}\right) = \varepsilon q^{n\chi/2} T^{\chi} Z(T)$$

2. On ne cherchera pas à donner des définitions précises des notions de géométrie algébrique qui interviennent dans ces énoncés si elles ne servent pas pour les quelques démonstrations des parties suivantes.

Interprétation « topologique ». Supposons que X provienne, par bonne réduction modulo un idéal premier, d'une variété $\tilde{X}$ (projective, non-singulière, absolument irréductible) définie sur un anneau d'entiers algébriques. Alors on peut voir $M = \tilde{X}(\mathbf{C})$ comme variété analytique réelle connexe de dimension $2n$, et l'on peut en particulier parler de sa cohomologie (de De Rham, disons). Alors pour tout i, $\deg P_i = \dim H^i(M)$. Autrement dit, la cohomologie de M se lit entièrement sur la fonction zêta de X.

Notons que l'hypothèse de Riemann est bien analogue à l'énoncé bien connu sur les corps de nombres. En effet, elle signifie que la fonction méromorphe $\zeta_X(s) = Z(q^{-s})$ a ses poles sur les droites $\Re s = 0, 1, \ldots, n$, et ses zéros sur les droites $\Re s = 1/2, 3/2, \ldots, (2n-1)/2$. De même, réécrite en termes de ζ_X, l'équation fonctionnelle a un certain air de famille. Elle relie les valeurs de ζ_X aux points s et $n - s$.

Exemple 1.2 On peut vérifier les conjectures de Weil pour les espaces projectifs. La fonction zêta $Z_{\mathbf{P}^n}$ que l'on a calculé au paragraphe précédent est bien une fraction rationnelle de la forme souhaitée, avec $P_{2k}(T) = 1 - q^k T$ et $P_{2k+1}(T) = 1$. En particulier, l'hypothèse de Riemann est satisfaite. D'autre part, on a :

$$\begin{aligned} Z_{\mathbf{P}^n}\left(\frac{1}{q^n T}\right) &= \prod_{k=0}^{n} \frac{1}{1 - \frac{1}{q^{n-k}T}} \\ Z_{\mathbf{P}^n}\left(\frac{1}{q^n T}\right) &= \prod_{k=0}^{n} \frac{-q^{n-k}T}{1 - q^{n-k}T} \\ Z_{\mathbf{P}^n}\left(\frac{1}{q^n T}\right) &= (-1)^n q^{n(n+1)/2} T^n Z_{\mathbf{P}^n}(T) \end{aligned}$$

ce qui est bien la relation attendue, puisque $\chi = n + 1$. Enfin, si l'on calcule la cohomologie de $\mathbf{P}^n(\mathbf{C})$ (ce que Godbillon [God71] fait par exemple assez rapidement par récurrence sur n en écrivant des suites exactes de cohomologie à support compact), on vérifie qu'elle est bien $\mathbf{R}$ en dimension paire et 0 en dimension impaire.

1.3 Histoire et perspectives

Une partie des conjectures était connue avant Weil dans certains cas particuliers (qui sont précisément ceux dans lesquels on proposera de donner effectivement des preuves dans les parties suivantes). L'idée d'un analogue de la fonction zêta pour les corps de fonctions remonte à la thèse d'E. Artin. Il prouve, en 1923, la rationalité et l'équation fonctionnelle pour les corps de fonctions des courbes hyperelliptiques, et vérifie l'hypothèse de Riemann sur un certain nombre d'exemples. Un peu plus tard, en 1931, F.K. Schmidt introduit le point de vue géométrique qui est celui du présent article, et montre comment, pour toutes les courbes, la rationalité et l'équation fonctionnelle résultent du théorème de Riemann-Roch. Hasse, à la même époque, démontre l'hypothèse de Riemann pour les courbes elliptiques.

Weil lui-même établit l'hypothèse de Riemann pour les courbes, et a besoin pour cela de retrouver, dans le cas d'un corps de base quelconque, des résultats que la géométrie algébrique classique obtenait sur $\mathbf{C}$ par des méthodes transcendantes. Il montre également les résultats analogues pour les variétés abéliennes et certaines classes d'hypersurfaces, et quitte ainsi la dimension 1. C'est à l'occasion de son travail sur les hypersurfaces diagonales qu'il formule les conjectures qui précèdent, et en particulier qu'il fait le lien avec la topologie. Il suggère que si l'on disposait, pour les variétés algébriques, d'une théorie cohomologique ayant de bonnes propriétés, analogues à celles qui peuvent exister en géométrie différentielles, on pouvait espérer

en déduire les conjectures (à l'exception de l'hypothèse de Riemann, dont l'interprétation est moins immédiate).

Ainsi débute, parmi les géomètres algébristes, la quête d'une « cohomologie de Weil ». Une des bonnes propriétés requises pour une telle cohomologie est de prendre ses valeurs dans un corps de caractéristique nulle, afin de pouvoir « compter » (par exemple, en exprimant la dimension d'un espace de cohomologie comme la trace de l'identité, et d'autres manipulations similaires). Cette condition rendait inadaptées certaines cohomologies naturelles qui intervenaient dans la construction de la géométrie algébrique abstraite mais prenaient leurs valeurs dans le corps de bases. C'est en particulier le cas de la cohomologie de Serre des faisceaux cohérents, ou de la cohomologie de De Rham algébrique. La première construction d'une cohomologie de Weil est due à Grothendieck et M. Artin : c'est la cohomologie étale ℓ-adique, qui a apporté en 1962 une preuve des conjectures de Weil à l'exception de l'hypothèse de Riemann. Grothendieck a formulé ensuite une série de conjectures très difficiles, dites conjectures standard, qui permettraient de montrer également de montrer l'hypothèse de Riemann en cohomologie étale. Malheureusement, elles restent presque toutes ouvertes à l'heure actuelle.

La résolution des conjectures est donc plusieurs fois passée par des voies « non canoniques », qui ont beaucoup surpris les mathématiciens. La première occasion est celle de la preuve de Dwork de la rationalité de la fonction zêta (sans supposer la variété non-singulière), dès 1960, par des méthodes d'analyse p-adiques. La seconde surprise est la démonstration par Deligne de l'hypothèse de Riemann, en 1973 : il utilisait de manière essentielle la cohomologie étale, mais ne passait pas par les conjectures standard, et au contraire déduisait l'une d'elles des résultats qu'il établissait. Ces travaux lui ont valu la médaille Fields. On peut également citer, à la même époque, même si l'importance historique en est sans doute moindre, la preuve originale et élémentaire qui a été donnée par Stepanov et Bombieri de l'hypothèse de Riemann pour les courbes et qui, contrairement aux preuves de Weil, ne requiert pas de géométrie en dimension supérieure. [3]

Par la suite, d'autres cohomologies de Weil ont été construites, comme la cohomologie cristalline et la cohomologie rigide de Berthelot, qui ont récemment permis d'établir l'ensemble des conjectures par des méthodes p-adiques. De manière plus générale, on suppose qu'il existe une sorte de cohomologie de Weil universelle dont toutes les théories cohomologiques usuelles seraient des réalisations particulières : la cohomologie motivique. Il semble que les conjectures de Weil soient importantes en particulier en ce qu'elles sont un des premiers énoncés abstraits à propos des motifs, encore que j'ignore si cette affirmation a même un sens précis. [4]

1.4 Propriétés d'une cohomologie de Weil

On peut donner un exposé axiomatique précis des propriétés que devraient vérifier une cohomologie de Weil. On se contentera ici des propriétés qui servent effectivement à aborder les conjectures de Weil.

3. Si bien qu'on aurait pu l'utiliser dans le présent article. On a préféré privilégier, pour l'hypothèse de Riemann, le cas particulier des courbes elliptiques, car il met un peu scène les manipulations que l'on peut faire dans le « premier groupe d'homologie » que constitue de le module de Tate (et qui se généralisent naturellement aux variétés abéliennes).

4. Après avoir lu, à propos de la fonction zêta d'une variété X sur un corps fini un certain nombre de remarques du type de celle de Katz dans [Kat76] : "It contains all of the diophantine information that X has to offer", j'avais demandé sur `<news:fr.sci.maths>` quelle était précisément le genre d'informations donné par la fonction zêta. On vérifie en effet facilement qu'elle ne caractérise pas une variété à isomorphisme près. Pierre Bernard m'a signalé que, pour les variétés abéliennes, le théorème de Tate montrait que c'est la classe d'isogénie qui est caractérisée par la fonction zêta. De même, pour une courbe, c'est la classe d'isogénie de la jacobienne. Dans ces cas-ci, on peut donc dire que la fonction zêta caractérise complètement le motif associé à X, si je comprends bien une explication de Serre dans [Ser91]. Je ne sais pas ce qu'il en est dans le cas général, mais c'est peut-être déjà une indication de la signification « motivique » des conjectures de Weil.

Soit k un corps fini et $\bar{k}$ une clôture algébrique. On appellera donc ici cohomologie de Weil la donnée d'une famille de foncteurs contravariants $H^i(-, K)$, $i \geq 0$, des variétés projectives irréductibles et non-singulières définies sur $\bar{k}$ dans les espaces vectoriels de dimension finie sur un certain corps K qui se plonge dans $\mathbf{C}$. Soit de plus X une variété projective irréductible non singulière de dimension n sur $\bar{k}$. On demande que ces foncteurs vérifient de plus les propriétés suivantes.

Nullité. $H^i(X, K) = 0$ pour $i > 2n$.

Dualité de Poincaré. $H^{2n}(X, K)$ est de dimension 1. De plus, pour $0 \leq i \leq 2n$, il existe une forme bilinéaire non-dégénérée $H^i(X, K) \times H^{2n-i}(X, K) \to H^{2n}(X, K)$, et cette forme bilinéaire est fonctorielle en X. Plus précisément, si $f : Y \to X$ est un morphisme, on a, pour $(v, w) \in H^i(X, K) \times H^{2n-i}(X, K)$:

$$\langle f^* u, f^* v \rangle = f^* \langle u, v \rangle$$

Formule de Lefschetz. Soit $f : X \to X$ un morphisme dont tous les points fixes sont simples (i.e. en chaque point fixe, l'endomorphisme $1 - df$ de l'espace tangent est injectif). Alors f a un nombre fini $L(f, X)$ de points fixes, donné par :

$$L(f, X) = \sum (-1)^i \operatorname{Tr}(f_i^*)$$

où f_i^* est l'endomorphisme de $H^i(X, K)$ déduit de f par fonctorialité.

Comparaison. Si X provient par bonne réduction modulo un idéal premier d'une variété $\tilde{X}$ définie sur un anneau d'entiers algébriques, alors pour tout i, on a $\dim_K H^i(X, K) = \dim_{\mathbf{R}} H^i(\tilde{X}(\mathbf{C}))$.

Montrons comment une partie des conjectures se déduit de l'existence d'une cohomologie présentant ces propriétés formelles. Soit $X \subset \mathbf{P}^r$ une variété projective non-singulière absolument irréductible définie sur k, et $\bar{X}$ la variété qui s'en déduit par extension des scalaires à $\bar{k}$. On considère le morphisme de Frobenius, $F : \bar{X} \to \bar{X}$, obtenu par restriction du morphisme :

$$(x_0 : \ldots : x_r) \mapsto (x_0^q : \ldots : x_r^q)$$

de $\mathbf{P}^r$. Un point x de $\mathbf{P}^r(\bar{k})$ est dans $\mathbf{P}^r(k_m)$ si et seulement si $F^m(x) = x$, donc le nombre N_m de points de X sur k_m s'écrit :

$$N_m = L(F^m, \bar{X})$$

Or en tout point, $dF = 0$, donc tous les points fixes de F sont simples, et l'on peut appliquer la formule de Lefschetz pour déterminer N_m :

$$N_m = \sum (-1)^i \operatorname{Tr}((F_i^m)^*) = \sum (-1)^i \operatorname{Tr}((F_i^*)^m)$$

où F_i^* est l'endomorphisme de $H^i(\bar{X}, K)$ induit par F. Le lemme élémentaire suivant va alors donner la rationalité.

Lemme 1 *Soit u un endomorphisme d'un K-espace vectoriel E. Alors on a l'égalité suivante de séries formelles en T sur K :*

$$\exp\left(\sum_{m=1}^{\infty} \operatorname{Tr}(u^m) \frac{T^m}{m}\right) = \det(1 - Tu)^{-1}$$

Démonstration. Comme K se plonge dans $\mathbf{C}$, on peut supposer sans perte de généralité que $K = \mathbf{C}$, et que u est triangulaire supérieure, avec pour valeurs propres $\lambda_1, \ldots, \lambda_r$. Alors le membre de droite s'écrit :

$$\begin{vmatrix} 1-\lambda_1 T & & * \\ & \ddots & \\ 0 & & 1-\lambda_r T \end{vmatrix}^{-1} = \frac{1}{(1-\lambda_1 T)\ldots(1-\lambda_r T)}$$

Et par ailleurs, on a :

$$\begin{aligned} \sum_{m=1}^{\infty} \mathrm{Tr}(u^m)\frac{T^m}{m} &= \sum_{k=1}^{r}\sum_{m=1}^{\infty}\frac{(\lambda_k T)^m}{m} \\ \sum_{m=1}^{\infty} \mathrm{Tr}(u^m)\frac{T^m}{m} &= \sum_{k=1}^{r} -\log(1-\lambda_k T) \end{aligned}$$

d'où le résultat. □

Par conséquent, la fonction zêta de X vérifie :

$$\begin{aligned} \log Z_X(T) &= \sum_{m=1}^{\infty}\sum_{i=0}^{2n}(-1)^i \mathrm{Tr}((F_i^*)^m)\frac{T^m}{m} \\ Z_X(T) &= \prod_{i=0}^{2n}\exp\left(\sum_{m=1}^{\infty}\mathrm{Tr}((F_i^*)^m)\frac{T^m}{m}\right)^{(-1)^i} \\ Z_X(T) &= \prod_{i=0}^{2n}\det(1-(F_i^*)T)^{(-1)^{i+1}} \end{aligned}$$

Si l'on pose $P_i(T) = \det(1-(F_i^*)T)$ pour $0 \leq i \leq 2n$, les P_i sont des polynômes de coefficient constant 1 et de degrés $\dim_K H^i(\bar{X}, K)$ tels que :

$$Z_X(T) = \frac{P_1(T)\ldots P_{2n-1}(T)}{P_0(T)\ldots P_{2n}(T)}$$

ce qui démontre bien que $Z_X(T)$ est une fraction rationnelle dont la forme ressemble beaucoup à celle escomptée. Néanmoins, sans information supplémentaire sur la cohomologie ainsi utilisée, on ne peut pas affirmer que les P_i soit à coefficients entiers (on sait seulement qu'ils sont dans $K[X]$), ni qu'ils sont précisément les polynômes prévus par l'hypothèse de Riemann. Si ce sont bien les polynômes attendus, cependant, la propriété de comparaison pour notre cohomologie montre immédiatement que l'interprétation topologique est également vérifiée.

En supposant toujours que les P_i sont bien les polynômes attendus, on peut déduire l'équation fonctionnelle de la dualité de Poincaré et d'une autre propriété (qui est conséquence formelle d'autres hypothèses plus techniques sur une cohomologie Weil) selon laquelle l'endomorphisme F_{2n}^* induit par F sur l'espace de dimension 1 $H^{2n}(\bar{X}, K)$ est la multiplication par q^n. Notons que cette propriété assure alors que $P_{2n}(T) = 1 - q^n T$, comme on l'attend. On aura besoin du lemme suivant.

Lemme 2 *Soit V, W deux K-espaces vectoriels munis d'une forme bilinéaire non-dégénérée $V \times W \to K$. On suppose donnés des endomorphismes $\varphi : V \to V$ et $\psi : W \to W$, et un élément λ de K^* tels que, pour tout $(v, w) \in V \times W$:*

$$\langle \varphi v, \psi w \rangle = \lambda \langle v, w \rangle$$

Alors, si l'on note $r = \dim_K V$, il vient :

$$\det(1-\psi T) = \frac{(-1)^r \lambda^r T^r}{\det \varphi} \det(1-\varphi/\lambda T) \quad et \quad \det \psi = \frac{\lambda^r}{\det \varphi}$$

Démonstration. La forme bilinéaire non-dégénérée fournit un isomorphisme $\Phi : V \tilde{\to} W^*$, $\langle v, w\rangle = \Phi(v)(w)$. En particulier, V et W ont même dimension. L'hypothèse s'écrit alors :

$$^t\psi \circ \Phi \circ \varphi = \lambda \Phi$$

En particulier, φ est inversible, et l'on a encore :

$$^t\psi = \Phi(\lambda \varphi^{-1})\Phi^{-1}$$

La deuxième relation annoncée en résulte immédiatement. Par ailleurs, on peut écrire :

$$\det(1-\psi T) = \det(1-\lambda\varphi^{-1}T) = \frac{\det(\varphi - \lambda T)}{\det \varphi} = \frac{(-1)^r\lambda^r T^r}{\det\varphi}\det(1-\varphi/\lambda T)$$

ce qui conclut la démonstration. □

Notons alors $B_i = \dim_K H^i(\bar{X}, K)$ pour tout i, et $\chi = \sum(-1)^i B_i$. La dualité de Poincaré permet d'appliquer le lemme précédent avec $V = H^i(\bar{X}, K)$, $W = H^{2n-i}(\bar{X}, K)$, $\varphi = F_i^*$ et $\psi = F_{2n-i}^*$. Comme F agit sur $H^{2n}(\bar{X}, K)$ par multiplication par q^n, on a ainsi $\lambda = q^n$, et donc :

$$P_{2n-i}(T) = \frac{(-1)^{B_i} q^{nB_i} T^{B_i}}{\det F_i^*} P_i\left(\frac{1}{q^n T}\right)$$

En effectuant le produit alterné des relations précédentes (en élevant la relation i à la puissance $(-1)^{i+1}$), on obtient donc :

$$Z_X(T) = (-1)^{-\chi} q^{-n\chi} T^{-\chi} \alpha Z_X\left(\frac{1}{q^n T}\right) \quad \text{avec } \alpha = \prod (\det F_i^*)^{(-1)^i}$$

Or la deuxième relation du lemme précédent donne $(\det F_i^*)(\det F_{2n-i}^*) = q^{nB_i}$, soit en effectuant le produit alterné, $\alpha^2 = q^{n\chi}$. On a donc $\alpha = \pm q^{n\chi/2}$, et l'équation fonctionnelle en résulte :

$$Z_X\left(\frac{1}{q^n T}\right) = \pm q^{n\chi/2} T^\chi Z_X(T)$$

2 Théorème de Riemann-Roch et conjectures de Weil pour les courbes

2.1 Corps de fonctions des courbes algébriques

Soit $X \subset \mathbf{P}^r$ une variété projective non-singulière irréductible définie sur un corps (parfait) k, et soit $\bar{k}$ une clôture algébrique de k. Un polynôme homogène $R \in k[X_0, \ldots, X_r]$ est dit nul sur X si pour tout $x \in X(\bar{k})$, $R(x) = 0$ (relation qui ne dépend pas de la famille de coordonnées homogènes choisie pour x). On appelle alors corps de fonctions de X le corps $k(X)$ formé par les quotients R/S de polynômes homogènes de même degré avec S non nul sur X, et où l'on identifie R_1/S_1 et R_2/S_2 lorsque $(R_1S_2 - S_1R_2)$ est nul sur X. On dit de plus que X est une *courbe* si $k(X)$ est de degré de transcendance 1 sur k, i.e., s'il existe un élément $f \in k(X)$ transcendant sur k tel que l'extension $k(X)/k(f)$ soit algébrique. Par définition, on a clairement $k(X) \cap \bar{k} = k$, donc tout élément $f \in k(X)$ qui n'est pas dans k convient alors.

Soit alors X une courbe sur k. On définit de manière évidente $\bar{k}(X)$, et pour tout point $x \in X(\bar{k})$, on définit l'anneau local de X en x comme étant le sous-anneau $\mathcal{O}_x$ de $\bar{k}(X)$ formé des quotients R/S de polynômes homogènes de même degré sur $\bar{k}$ avec $S(x) \neq 0$. On peut montrer alors[5] que $\mathcal{O}_x$ a un unique idéal premier non nul $\mathfrak{m}_x$, et qu'il est principal. On peut alors définir la valuation ord_x en x par $\mathrm{ord}_x(f) = \max_n\{f \in \mathfrak{m}_x^n\}$ pour tout $f \in \mathcal{O}_x$ non nul. On peut étendre cette valuation au corps des fractions de $\mathcal{O}_x$, qui est évidemment $\bar{k}(X)$, en posant $\mathrm{ord}_x(f/g) = \mathrm{ord}_x(f) - \mathrm{ord}_x(g)$. On dit que $f \in \bar{k}(X)$ a un zéro (resp. un pôle) en x lorsque $\mathrm{ord}_x(f) > 0$ (resp. < 0). On montre qu'une fonction donnée n'a de zéros et de pôles qu'en un nombre fini de points, et qu'une fonction qui n'a aucun pôle est constante (i.e. élément de $\bar{k}$).

On appelle groupes des $\bar{k}$-diviseurs de X le groupe abélien libre $\mathrm{Div}_{\bar{k}}(X)$ engendré par les points de X sur $\bar{k}$. On appelle degré d'un $\bar{k}$-diviseur $D = \sum_x n_x x$ l'entier $\deg D = \sum n_x$. Par ailleurs, la remarque précédente montre que pour toute fonction $f \in \bar{k}(X)^*$, on définit un $\bar{k}$-diviseur (f) en posant :

$$(f) = \sum_x \mathrm{ord}_x(f)x$$

Comme $\mathrm{ord}_x(fg) = \mathrm{ord}_x(f) + \mathrm{ord}_x(g)$, $f \mapsto (f)$ est un morphisme de groupes $\bar{k}(X)^* \to \mathrm{Div}_{\bar{k}}(X)$. Son noyau est $\bar{k}^*$. Une propriété essentielle (qui n'est vraie que parce que l'on travaille avec des courbes projectives) est en outre que pour tout $f \in \bar{k}(X)$, $\deg(f) = 0$.

Soit $G = \mathrm{Gal}(\bar{k}/k)$ le groupe de Galois de k. G agit naturellement, comme on l'a vu, sur $X(\bar{k})$, et donc sur $\mathrm{Div}_{\bar{k}}(X)$. Les $\bar{k}$-diviseurs invariants par l'action de G forment alors exactement le sous-groupe abélien libre engendré par les places de X. Ce sous-groupe sera appelé groupe des diviseurs de X et noté simplement $\mathrm{Div}(X)$. Le degré définit par restriction un morphisme $\mathrm{Div}(X) \to \mathbf{Z}$, et le degré d'une place en ce sens coïncide bien avec son cardinal, conformément à la définition donnée au 1.1.

D'autre part, G agit sur les polynômes homogènes, donc sur $\bar{k}(X)$, et l'on a $\bar{k}(X)^G = k(X)$. De plus, pour tout $\sigma \in G$, $x \in X(\bar{k})$ et $f \in \bar{k}(X)^*$, $\mathrm{ord}_{x^\sigma}(f^\sigma) = \mathrm{ord}_x(f)$, et par conséquent :

$$(f^\sigma) = \sum_x \mathrm{ord}_x(f^\sigma)x = \sum_x \mathrm{ord}_{x^\sigma}(f^\sigma)x^\sigma = \sum_x \mathrm{ord}_x(f)x^\sigma = (f)^\sigma$$

En particulier, pour tout $f \in k(X)^*$, on a bien $f \in \mathrm{Div}(X)$. On dit enfin que deux diviseurs D et D' de X sont linéairement équivalents lorsqu'il existe $f \in k(X)$ telle que $D - D' = (f)$.

Le groupe $\mathrm{Div}(X)$ est partiellement ordonné par la relation $\sum_\mathfrak{p} n_\mathfrak{p}\mathfrak{p} \geq 0$ si et seulement si tous les $n_\mathfrak{p}$ sont positifs. Un diviseur $D \geq 0$ est dit positif (ou effectif). Étant donné $D \in \mathrm{Div}(X)$ quelconque, on appelle série linéaire définie par D l'ensemble :

$$L(D) = \{f \in k(X)^* \ / \ (f) + D \geq 0\} \cup \{0\}$$

D'après les propriétés des valuations, $L(D)$ est un espace vectoriel sur k. On montre qu'il est de dimension finie. Soit $\ell(D)$ sa dimension. Le théorème fondamental de la théorie des courbes algébriques est alors le suivant.[6]

Théorème 1 (Riemann-Roch) *Soit X une courbe algébrique sur k. Il existe un entier $g \geq 0$, appelé* genre *de X, et un diviseur $K \in \mathrm{Div}(X)$ de degré $2g - 2$, tels que pour tout diviseur $D \in \mathrm{Div}(X)$, on ait la relation :*

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

5. La référence de tout ce qui suit en matière de théorie des courbes algébriques est le bel exposé qu'en donne Silverman dans [Sil86], ch. II, en prélude à l'étude des courbes elliptiques. On a également puisé avec profit dans la présentation de Serre dans [Ser59].

6. Je n'ai trouvé le théorème de Riemann-Roch énoncé sous cette forme (et sans démonstration) que dans [Kat76] et [Vol01]. Dans mes autres références, il n'est énoncé que dans le cas d'un corps de base algébriquement clos. J'ai confiance en la justesse de cette formulation, d'autant que P. Samuel donne dans [Sam63] la preuve d'un résultat très analgue dans le langage des valuations, mais je ne sais pas la démontrer.

2.2 Conjectures de Weil pour les courbes

Soit k un corps fini, q son cardinal, et X une courbe de genre g sur k. On va montrer la rationalité de $Z_X(T)$ ainsi que l'équation fonctionnelle sous réserve que les polynômes qui interviennent dans la décomposition soient bien ceux qu'impose l'hypothèse de Riemann. La présentation est empruntée au chapitre 2 du cours de Katz [Kat74].

On veut en fait exprimer la fonction zêta de façon à pouvoir appliquer le seul résultat de « structure » dont on dispose ici sur les courbes, à savoir le théorème de Riemann-Roch. Pour cela, on commence par remarquer que si l'on développe l'expression en produit infini de $Z_X(T)$, on obtient une somme sur les diviseurs positifs :

$$Z_X(T) = \prod_{\mathfrak{p}} (1 - T^{\deg \mathfrak{p}})^{-1} = \prod_{\mathfrak{p}} \sum_{n=0}^{\infty} T^{\deg n\mathfrak{p}} = \sum_{D \geq 0} T^{\deg D}$$

En particulier, il n'y a qu'un nombre fini e_n de diviseurs positifs de degré n pour tout n, et l'on a $Z_X(T) = \sum_{n=0}^{\infty} e_n T^n$.

Notons $\mathrm{Div}^n(X)$ l'ensemble des diviseurs (positifs ou non) de degré n sur X. Comme deux diviseurs linéairement équivalents ont même degré, l'équivalence linéaire définit bien une relation d'équivalence sur $\mathrm{Div}^n(X)$. On note $\mathrm{Pic}^n(X)$ l'ensemble quotient, et $D \mapsto \bar{D}$ la surjection canonique. Soit alors $D \in \mathrm{Div}^n(X)$ un diviseur quelconque. Par définition de $L(D)$, les diviseurs positifs équivalents à D sont exactement ceux de la forme $D + (f)$ avec $f \in L(D) - \{0\}$. De plus, $D + (f)$ et $D + (g)$ sont égaux si et seulement si $f/g \in k^*$. Par conséquent, l'ensemble des diviseurs positifs équivalents à D est en bijection avec l'ensemble des droites du k-espace vectoriel $L(D)$, donc de cardinal $(q^{\ell(D)} - 1)/(q - 1)$. On peut donc écrire :

$$e_n = \sum_{\bar{D} \in \mathrm{Pic}^n(X)} \frac{q^{\ell(D)} - 1}{q - 1}$$

Si $n > 2g - 2$, le théorème de Riemann-Roch donne $\ell(D) = n + 1 - g$ pour tout $D \in \mathrm{Pic}^n$, et l'expression précédente devient :

$$e_n = \frac{q^{n+1-g} - 1}{q - 1} |\,\mathrm{Pic}^n(X)|$$

et en particulier, $\mathrm{Pic}^n(X)$ est fini. On va voir qu'en fait, son cardinal de dépend pas de n.

Le degré définit un morphisme du groupe $\mathrm{Div}(X)$ dans $\mathbf{Z}$. Ce morphisme est non nul (la place engendrée par un point quelconque de $X(\bar{k})$ est de degré ≥ 1), donc il existe $d \geq 1$ tel que $\mathrm{Im}(\deg) = d\mathbf{Z}$. Soit D un diviseur de degré d. Alors l'addition de D induit une bijection $\mathrm{Div}^n(X) \to \mathrm{Div}^{n+d}(X)$ pour tout $n \in Z$, et cette bijection est compatible avec l'équivalence linéaire, donc par passage au quotient, on en déduit une bijection $\mathrm{Pic}^n(X) \to \mathrm{Pic}^{n+d}(X)$ pour tout $n \in \mathbf{Z}$. Puisque $\mathrm{Pic}^n(X)$ est fini pour n assez grand, il est donc fini pour tout n et ainsi, si l'on pose $h = |\,\mathrm{Pic}^0(X)| = |\,\mathrm{Pic}^d(X)| \in \mathbf{N}^*$:

$$|\,\mathrm{Pic}^n(X)| = \begin{cases} h & \text{si } d|n \\ 0 & \text{sinon} \end{cases}$$

Comme il existe sur X un diviseur de degré $2g-2$ (dans la classe canonique), on peut écrire : [7]

$$\begin{aligned} Z_X(T) &= \sum_{\substack{0\leq n\leq 2g-2 \\ d|n}} e_n T^n + \sum_{\substack{n\geq 2g-2+d \\ d|n}} h\frac{q^{n+1-g}-1}{q-1}T^n \\ Z_X(T) &= Q(T) + \frac{h}{q-1}T^{2g-2+d}\sum_{m\geq 0}(q^{g-1+d+md}-1)T^{md} \\ Z_X(T) &= Q(T) + \frac{h}{q-1}T^{2g-2+d}\left[\frac{q^{g-1+d}}{1-(qT)^d} - \frac{1}{1-T^d}\right] \end{aligned}$$

avec $Q(T)$ le polynôme en T^d formé par les termes de degré inférieur à $2g-2$. On obtient ainsi déjà que $Z_X(T)$ est une fraction rationnelle, et même une fraction rationnelle en T^d. De plus, on voit que pour tout m, $Z_X(T^m)$ a un pôle *simple* en 1. Cette remarque va nous permettre de montrer que $d=1$, d'où la forme voulue de la rationalité se déduira facilement.

En effet, soit X_d la courbe sur le corps k_d à q^d éléments obtenue à partir de X par extension des scalaires. D'après la remarque précédente, $Z_{X_d}(T^d)$ a un pôle simple en 1. Or on a $Z_{X_d}(T^d) = \prod_{\omega^d=1} Z_X(\omega T)$. En effet, les logarithmes de ces séries formelles sont égaux, puisque l'on a, en notant $N_m = |X(k_m)|$:

$$\begin{aligned} \sum_{\omega^d=1}\sum_{m\geq 0}\frac{N_m}{m}(\omega T)^m &= \sum_{m\geq 0}\left(\sum_{\omega^d=1}\omega^m\right)\frac{N_m}{m}T^m \\ \sum_{\omega^d=1}\sum_{m\geq 0}\frac{N_m}{m}(\omega T)^m &= \sum_{d|m} d\frac{N_m}{m}T^m \\ \sum_{\omega^d=1}\sum_{m\geq 0}\frac{N_m}{m}(\omega T)^m &= \sum_{s\geq 0}\frac{N_{sd}}{s}T^{sd} \end{aligned}$$

Or, comme $Z_X(T)$ est une fraction rationnelle en T^d, $Z_X(\omega T) = Z_X(T)$ pour toute racine d-ième de l'unité, et par conséquent, on a $Z_{X_d}(T^d) = Z_X(T)^d$. Or la seconde fraction rationnelle possède un pôle d'ordre d en 1. Il en résulte bien que $d=1$.

On peut alors terminer la simplification de $Z_X(T)$:

$$\begin{aligned} Z_X(T) &= Q(T) + \frac{h}{q-1}T^{2g-1}\left[\frac{q^g}{1-qT} - \frac{1}{1-T}\right] \\ Z_X(T) &= \frac{(1-T)(1-qT)Q(T) + \frac{h}{q-1}T^{2g-1}(q^g - q^gT - 1 + qT)}{(1-T)(1-qT)} \\ Z_X(T) &= \frac{P(T)}{(1-T)(1-qT)} \end{aligned}$$

où $P(T)$ est le polynôme de degré $2g$ au plus donné par :

$$P(T) = (1-T)(1-qT)\sum_{n=0}^{2g-2} e_n T^n + h\frac{q^g-1}{q-1}T^{2g-1} - h\frac{q^g-q}{q-1}T^{2g}$$

En particulier, $P(T)$ est à coefficients entiers, et comme $Z_X(0)=1$ par définition de la fonction zêta, on a $P(0)=1$. Par conséquent, la décomposition précédente est exactement de la forme suggérée par les conjectures de Weil.

7. Dans tout ce qui suit, on mène les calculs pour $g \geq 1$. Néanmoins, le même argument fonctionne en genre 0, et montre que la fonction zêta d'une courbe de genre 0 est nécessairement de la forme $\frac{h}{(1-T)(1-qT)}$, et donc forcément égale à $\frac{1}{(1-T)(1-qT)}$, puisqu'elle doit valoir 1 en 0. Cela montre en particulier qu'une courbe de genre 0 sur un corps fini a exactement autant de points que la droite projective, ce qui n'a rien d'évident a priori.

On va maintenant montrer à la fois que $P(T)$ est de degré précisément $2g$, de sorte que $\chi = 2-2g$, et que $Z_X(T)$ satisfait à l'équation fonctionnelle prescrite :

$$Z_X\left(\frac{1}{qT}\right) = q^{1-g}T^{2-2g}Z_X(T)$$

On reprend pour cela la fonction zêta sous la forme :

$$\begin{aligned}
(q-1)Z_X(T) &= \sum_{n=0}^{2g-2}\left(\sum_{\bar{D}\in\mathrm{Pic}^n(X)} q^{\ell(D)}-1\right)T^n + \sum_{n\geq 2g-1} h(q^{n+1-g}-1)T^n \\
(q-1)Z_X(T) &= \sum_{n=0}^{2g-2}\left(\sum_{\bar{D}\in\mathrm{Pic}^n(X)} q^{\ell(D)}\right)T^n + \left[\frac{hq^gT^{2g-1}}{1-qT} - \frac{h}{1-T}\right] \\
(q-1)Z_X(T) &= R(T)+F(T)
\end{aligned}$$

On va montrer que le polynôme $R(T)$ et la fraction rationnelle $F(T)$ satisfont tous les deux à l'équation fonctionnelle. Pour $F(T)$ c'est un calcul facile :

$$\begin{aligned}
F\left(\frac{1}{qT}\right) &= hq^g\frac{q^{1-2g}T^{1-2g}}{1-\frac{1}{T}} - \frac{h}{1-\frac{1}{qT}} \\
F\left(\frac{1}{qT}\right) &= -h\frac{q^{1-g}T^{2-2g}}{1-T} + \frac{hqT}{1-qT} \\
F\left(\frac{1}{qT}\right) &= q^{1-g}T^{2-2g}F(T)
\end{aligned}$$

Par ailleurs, on a $R(T)=\sum_{n=0}^{2g-2}a_nT^n$, avec $a_n=\sum_{\bar{D}\in\mathrm{Pic}^n(X)}q^{\ell(D)}$. Or, d'après le théorème de Riemann-Roch, $\ell(D)=n+1-g+\ell(K-D)$ pour tout D de degré n. Comme $D\mapsto K-D$ induit une bijection $\mathrm{Div}^n(X)\to\mathrm{Div}^{2g-2-n}(X)$ compatible avec l'équivalence linéaire, il en résulte que :

$$a_n = \sum_{\bar{D}\in\mathrm{Pic}^n(X)} q^{n+1-g}q^{\ell(K-D)} = q^{n+1-g}\sum_{\bar{D}'\in\mathrm{Pic}^{2g-2-n}(X)} q^{\ell(D')} = q^{n+1-g}a_{2g-2-n}$$

Par conséquent :

$$\begin{aligned}
R\left(\frac{1}{qT}\right) &= q^{1-g}T^{2-2g}\sum_{n=0}^{2g-2} a_nq^{-n-1+g}T^{2g-2-n} \\
R\left(\frac{1}{qT}\right) &= q^{1-g}T^{2-2g}\sum_{n=0}^{2g-2} a_{2g-2-n}T^{2g-2-n} \\
R\left(\frac{1}{qT}\right) &= q^{1-g}T^{2-2g}R(T)
\end{aligned}$$

Il en résulte que $Z_X(T)$ vérifie bien l'équation fonctionnelle. Voyons de plus que $P(T)$ est de degré $2g$. On a $e_0=P(0)=1$, et d'autre part :

$$e_0 = \sum_{\bar{D}\in\mathrm{Pic}^n(X)}\frac{q^{\ell(D)}-1}{q-1} = \frac{a_0-h}{q-1} = \frac{q^{1-g}a_{2g-2}-h}{q-1}$$

Par conséquent :

$$e_{2g-2} = \frac{a_{2g-2}-h}{q-1} = \frac{(q-1+h)q^{g-1}-h}{q-1} = q^{g-1}+h\frac{q^{g-1}-1}{q-1}$$

Et ainsi, le terme de degré $2n$ de $P(T)$ vaut :

$$qe_{2g-2} - h\frac{q^g - q}{q-1} = q^g \neq 0$$

ce qui conclut. On a donc bien obtenu tout une partie des conjectures de Weil pour les courbes, et l'on a un peu plus précisément l'allure de la fonction zêta :

$$Z_X(T) = \frac{1 + \cdots + q^g T^{2g}}{(1-T)(1-qT)}$$

On peut noter que l'interprétation topologique s'applique également puisque, si X provient par bonne réduction d'une courbe $\tilde{X}$ définie sur un anneau d'entiers algébriques, $\tilde{X}(\mathbf{C})$ est une surface de Riemann compacte connexe de genre g, c'est-à-dire une sphère à g poignées. Son homologie est clairement 1 en dimensions 0 et 2, et les $2g$ cycles obtenus en parcourant l'intérieur et le pourtour de chacune des poignées forment une base de l'homologie en dimension 1.

3 Conjectures de Weil pour les courbes elliptiques

3.1 Isogénies des courbes elliptiques

Les courbes elliptiques sont les courbes les plus simples (après les courbes rationnelles, si l'on veut). Elles sont naturellement munies d'une loi de groupe algébrique qui rend leur manipulation particulièrement pratique. En fait, elles sont à la fois des cas particuliers de courbes et de variétés abéliennes, ce qui va permettre d'aborder dessus les conjectures de Weil par des méthodes « à la Weil ». Donnons d'abord les définition de base, d'après Silverman [Sil86].

On appelle courbe elliptique sur un corps k la donnée d'une courbe E de genre 1 sur k, et d'un point O de $E(k)$ (en particulier, on suppose $E(k)$ non vide). On se place dans la suite dans le cas où k est un corps fini, de caractéristique p et de cardinal q. On peut noter à ce propos qu'une courbe E de genre 0 sur un tel corps a toujours un point rationnel. En effet, on a montré qu'il existait au moins un diviseur D de degré 1 sur E, et l'on a alors, puisque $1 > 2g - 2 = 0$, $\ell(D) = 1 + 1 - 1 = 1$. Il existe donc $f \in k(E)^*$ tel que $(f) + D$ soit un diviseur positif de degré 1, c'est-à-dire un point rationnel.

Voyons de quelle manière (E, O) est munie d'une loi de groupe. Soit K une extension algébrique de k (contenue dans $\bar{k}$). Pour tout K-diviseur $D \in \mathrm{Div}^0_K(E)$, il existe un unique point $P \in E(K)$ tel que D soit équivalent à $(P) - (O)$. En effet, $L_K(D + (O))$ est de dimension 1 d'après le théorème de Riemann-Roch (appliqué à la courbe obtenue par extension des scalaires à K, si l'on veut), donc il existe $P \in E(K)$ tel que $D \sim (P) - (O)$. D'autre part, si $P' \in E(K)$ vérifie également cette propriété, (P') est positif et linéairement équivalent à (P) sur K, donc il existe $f \in L_K((P))$ tel que $(P') = (f) + (P)$. Or $L_K((P))$ est de dimension 1 et contient les constantes, donc f est necessairement constante, et ainsi $(f) = 0$ et $(P) = (P')$.

Par conséquent, l'application $E(K) \to \mathrm{Pic}^0_K(E)$ définie par $P \mapsto \overline{(P) - (O)}$ est bijective pour tout K. Comme $\mathrm{Pic}^0_K(E)$ est naturellement muni d'une loi de groupe, on peut munir $E(K)$ de la loi de groupe correspondante par cette identification. Comme pour toute inclusion $K \to K'$ on a un morphisme naturel $\mathrm{Pic}^0_K(E) \to \mathrm{Pic}^0_{K'}(E)$, l'association qui à toute extension algébrique K de k associe le groupe $E(K)$ est fonctorielle. On montre en fait que cette association provient d'une loi de groupe algébrique, i.e. qu'il existe des morphismes algébriques $+ : E \times E \to E$ et $- : E \to E$ (obtenus en fait par le procédé classique de la corde et de la tangente) définis sur k et qui induisent sur $E(K)$ les opérations $P, P' \mapsto P + P'$ et $P \mapsto -P$ du groupe défini précédemment.

On rappelle qu'un morphisme de courbes $\phi : X \to Y \subset \mathbf{P}^r$ sur k est la donnée de fonctions $f_0, \ldots, f_r$ de $k(X)$ non toutes nulles telles que pour tout $x \in X(\bar{k})$ où aucune des f_i n'a de pôle,

on a $(f_0(x) : \ldots : f_r(x)) \in Y(\bar{k})$. On montre alors que tout point x de $X(K)$, quitte à multiplier les f_i par une même fonction $g_x \in k(X)^*$, a une image bien définie $\phi(x)$ dans $Y(K)$ pour toute extension K de k. De plus, l'application $X(\bar{k}) \to Y(\bar{k})$ induite par ϕ est constante ou surjective. Dans ce dernier cas, la relation $f \mapsto f \circ \phi$ définit un morphisme de corps $\phi^* : k(Y) \to k(X)$, et l'extension $k(X)/\phi^* k(Y)$ est finie. Son degré $\deg \phi$ est appelé degré de ϕ. La fibre $\phi^{-1}(y)$ en tout $y \in Y(\bar{k})$ est finie, et l'on peut écrire, en notant t un générateur de $\mathfrak{m}_y$:

$$\deg \phi = \sum_{x \in \phi^{-1}(y)} e_\phi(x) \quad \text{avec } e_\phi(x) = \mathrm{ord}_x(\phi^* t)$$

Si de plus l'extension $k(X)/\phi^* k(Y)$ est séparable, on dit que ϕ est séparable, et alors pour tout $y \in Y(\bar{k})$ sauf peut-être un nombre fini, la fibre $\phi^{-1}(y)$ contient $\deg \phi$ points. Par convention, un morphisme constant a pour degré 0, ce qui donne pour tous morphismes $\phi : X \to Y$, $\psi : Y \to Z$, $\deg(\psi\phi) = \deg \psi \cdot \deg \phi$.

Soit alors deux courbes elliptiques E_1, E_2 sur k. Une isogénie $\phi : E_1 \to E_2$ est un morphisme vérifiant $\phi(O) = O$. Un tel morphisme est toujours un morphisme de groupes. En effet, pour toute extension K de k dans $\bar{k}$, ϕ définit un morphisme $\phi_* : \mathrm{Pic}^0_K(E_1) \to \mathrm{Pic}^0_K(E_2)$ par $\phi_* \sum_x n_x x = \sum_x n_x \phi(x)$, et alors l'application induite par ϕ sur $E(K)$ est la composée :

$$E_1(K) \xrightarrow{\sim} \mathrm{Pic}^0_K(E_1) \xrightarrow{\phi_*} \mathrm{Pic}^0_K(E_2) \xrightarrow{\sim} E_2(K)$$

où toutes les flèches sont des morphismes de groupes. Les isogénies d'une courbe elliptique E dans elle-même s'appellent endomorphismes de E. Elles forment un anneau $\mathrm{End}(E)$ pour l'addition donnée par $(\phi + \psi)(x) = \phi(x) + \psi(x)$ et pour la composition. Une famille importante d'endomorphismes de E est celle des « multiplication par un entier » : pour $m \in \mathbf{N}$ on note $[m]$ l'endomorphisme de E donné par $[m]x = x + \cdots + x$ (m fois) sur $E(\bar{k})$. De même, on pose $[-m]x = (- \circ [m])(x) = -(x + \cdots + x)$. $[\cdot]$ est alors clairement un morphisme d'anneaux $\mathbf{Z} \to \mathrm{End}(E)$. Un autre endomorphisme important est le Frobenius F correspondant à l'élévation de toutes les coordonées à la puissance $q = |k|$. C'est bien une isogénie car, comme $O \in E(k)$, on a bien $F(O) = O$.

On voit, en composant par des translations $x \mapsto x + x_0$ (qui sont non-ramifiées), que l'indice de ramification $e_\phi(x)$ d'une isogénie ϕ est le même en tout point x. En particulier, une isogénie *séparable* est non-ramifiée, donc sa fibre en tout point a pour cardinal son degré. En particulier, le noyau $E[\phi]$ de ϕ vue comme morphisme de groupe $E(\bar{k}) \to E(\bar{k})$ est de cardinal $\deg \phi$. On montre que l'isogénie $(a + bF)$, a et b entiers, est séparable dès que p ne divise pas a, et non nulle si $(a, b) \neq (0, 0)$.

L'anneau $\mathrm{End}(E)$ est muni d'une importante anti-involution définie de la façon suivante. Soit $\phi : E \to E$ une isogénie non constante de degré m. ϕ définit un morphisme de groupes $\phi^* : \mathrm{Pic}^0_k(E) \to \mathrm{Pic}^0_k(E)$ par $\phi^* y = \sum_{x \in \phi^{-1}(y)} e_\phi(x) x$ (et en prolongeant par linéarité). On a clairement $\phi^* \phi_* = \phi_* \phi^* = \deg \phi$. On peut alors montrer que ϕ^* provient bien d'une isogénie. Il existe une unique isogénie $\hat{\phi} \in \mathrm{End}(E)$ dont l'action sur les points soit la composée :

$$E(K) \xrightarrow{\sim} \mathrm{Pic}^0_K(E) \xrightarrow{\phi^*} \mathrm{Pic}^0_K(E) \xrightarrow{\sim} E(K)$$

On l'appelle isogénie duale de ϕ. On a en particulier $\phi\hat{\phi} = \hat{\phi}\phi = [m]$, et $\hat{\phi}$ est caractérisée par cette propriété. Il vient alors sans difficulté que $\phi \mapsto \hat{\phi}$ est une anti-involution de l'anneau. On voit en particulier que le degré, $\phi \mapsto \hat{\phi}\phi$, est une forme forme quadratique définie positive $\mathrm{End}(E) \to \mathbf{Z}$. On a notamment $\deg[m] = m^2$ pour tout m.

Lorsque m est premier à p, on a vu que $[m]$ était séparable. La dernière remarque montre donc que l'ensemble $E[m]$ des points d'ordre m de $E(\bar{k})$ est d'ordre m^2. En appliquant ce résultat pour les diviseurs de m, on en déduit la structure de $E[m]$:

$$E[m] \cong (\mathbf{Z}/m\mathbf{Z})^2$$

Choisissons alors un nombre premier $\ell \neq p$. Pour tout n, $E[\ell^n] \cong (\mathbf{Z}/\ell^n\mathbf{Z})^2$, et la multiplication par ℓ donne des morphismes surjectifs $E[\ell^{n+1}] \to E[\ell^n]$. En passant à la limite projective, on obtient donc $\varprojlim E[\ell^n] = \mathbf{Z}_\ell^2$. Cette limite projective $T_\ell(E)$, vue comme $\mathbf{Z}_\ell$-module libre de rang 2, s'appelle module de Tate de E (d'indice ℓ). Toute isogénie de E laisse stable $E[\ell^n]$, donc induit un endomorphisme de $T_\ell(E)$. C'est cet espace qui va nous servir de « groupe de cohomologie ».

3.2 Cohomologie de Weil des courbes elliptiques

Plus précisément, comme le suggère Serre dans [Ser60] §5, on fabrique, sur les courbes elliptiques sur k, des foncteurs contravariants $H^0(-, \mathbf{Q}_\ell)$, $H^1(-, \mathbf{Q}_\ell)$ et $H^2(-, \mathbf{Q}_\ell)$ vers les espaces vectoriels de dimension finie sur $\mathbf{Q}_\ell$ de la façon suivante. Pour toute courbe E, on pose $H^0(E, \mathbf{Q}_\ell) = H^2(E, \mathbf{Q}_\ell) = \mathbf{Q}_\ell$, et $H^1(E, \mathbf{Q}_\ell) = T_\ell(E) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell \cong \mathbf{Q}_\ell^2$. De plus, si $\phi : E_1 \to E_2$ est une isogénie, $H^0(\phi, \mathbf{Q}_\ell)$ est l'identité, $H^1(\phi, \mathbf{Q}_\ell)$ est le morphisme induit par $\hat{\phi}$ sur $T_\ell(E)$, et $H^2(\phi, \mathbf{Q}_\ell)$ est la multiplication par $\deg \phi = \deg \hat{\phi}$. Par ailleurs, toute translation opère sur ces espaces par l'identité, ce qui permet bien de définir les $H^i(\phi, \mathbf{Q}_\ell)$ pour tout morphisme.

Les $H^i(-, \mathbf{Q}_\ell)$ sont alors des foncteurs contravariants bien définis. Ils vérifient l'axiome de nullité évoqué au 1.4, et on a facilement aussi la dualité de Poincaré entre H^0 et H^2 : c'est simplement la multiplication, qui est alors clairement compatible avec les morphismes. De plus, l'hypothèse supplémentaire selon laquelle le Frobenius opère sur H^2 par multiplication par q, dont on a eu besoin dans la preuve générale de l'équation fonctionnelle, est également vérifiée, car $\deg F = q$ ([Sil86] II.2.11.c). On peut mentionner en outre que l'interprétation topologique est vérifiée, pour la même raison que dans le cas général des courbes.

On aura donc les propriétés du 1.4 si l'on peut construire une dualité de Poincaré convenable $H^1 \times H^1 \to H^2$, et si l'on peut montrer la formule de Lefschetz. Commençons par la dualité de Poincaré. Pour cela, on va construire pour tout n un accouplement bilinéaire $e_{\ell^n} : E[\ell^n] \times E[\ell^n] \to \mu_{\ell^n}$ appelé accouplement de Weil. On procède de la façon suivante. Soit m premier à p quelconque.

Remarquons que l'application composée $\mathrm{Div}_K^0(E) \twoheadrightarrow \mathrm{Pic}_K^0(E) \xrightarrow{\sim} E(K)$ est simplement donnée par $\sum_x n_x x \mapsto \sum_x [n_x]x$. En particulier, un diviseur $\sum_x n_x x$ est principal si et seulement si, au sens de l'addition sur la courbe, $\sum_x [n_x]x = O$. Soit alors $T \in E[m]$. Il existe $f \in \bar{k}(E)$ telle que $(f) = m(T) - m(O)$. Choisissons en outre $T' \in E(\bar{k})$ tel que $mT' = T$. Il existe également une fonction $g \in \bar{k}(E)$ telle que :

$$(g) = \sum_{R \in E[m]} (T' + R) - (R)$$

Les fonctions $f \circ [m]$ et g^m ont alors même diviseur associé, donc quitte à multiplier f par une constante, on peut supposer $f \circ [m] = g^m$. Soit alors $S \in E[m]$ quelconque. Pour tout $P \in E(\bar{k})$, on a :

$$g(P+S)^m = f([m]P + [m]S) = f([m]P) = g(P)^m$$

donc si l'on note g_S la fonction donnée par $g_S(P) = g(P+S)$, on voit que $(g_S/g)^m = 1$, donc g_S/g est un élément de μ_m. On pose alors $e_m(S,T) = g_S/g$. Notons que g est déterminé par T à une constante près, donc $e_m(S,T)$ est bien défini. On montre alors ([Sil86] III.8) que e_m est un accouplement bilinéaire alterné non-dégénéré. De plus, si ϕ est une isogénie, $\hat{\phi}$ est son adjoint dans cette accouplement, au sens où pour tout S, T, $e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T)$. Enfin, les accouplements e_{ℓ^n} pour les n successifs se « comportent bien » vis-à-vis du système projectif des $E[\ell^n]$, au sens où, pour S, T dans $E[\ell^{n+1}]$, $e_{\ell^n}([\ell]S, [\ell]T) = e_{\ell^{n+1}}(S,T)^\ell$, donc le diagramme évident entre les $E[\ell^n]$ et les μ_{ℓ^n} commute. Ceci permet de passer les e_{ℓ^n} à la limite projective, et obtenir un accouplement bilinéaire alterné non dégénéré :

$$e : T_\ell(E) \times T_\ell(E) \to \varprojlim \mu_{\ell^n} \cong \mathbf{Z}_\ell$$

pour lequel l'adjoint d'une isogénie est son isogénie duale.

En étendant les scalaires à $\mathbf{Q}_\ell$, on obtient ainsi un accouplement bilinéaire non-dégénéré $\langle , \rangle : H^1(E, \mathbf{Q}_\ell) \times H^1(E, \mathbf{Q}_\ell) \to H^2(E, \mathbf{Q}_\ell)$. De plus, la propriété d'adjonction précédente assure qu'il est bien fonctoriel. En effet, si $\phi : E_1 \to E_2$ est une isogénie et ϕ_ℓ le morphisme induit sur le module de Tate, alors pour tous $(u, v) \in H^1(E_2, \mathbf{Q}_\ell)^2$, il vient :

$$\langle \phi^* u, \phi^* v \rangle = \langle (\hat{\phi})_\ell(u), (\hat{\phi})_\ell(v) \rangle = \langle (\phi\hat{\phi})_\ell(u), v \rangle = (\deg \phi)\langle u, v \rangle$$

On va utiliser cet accouplement pour montrer la formule de Lefschetz. Soit (u, v) une base du $\mathbf{Q}_\ell$-espace vectoriel $H^1(E, \mathbf{Q}_\ell)$, ϕ un endomorphisme de E. Écrivons la matrice de $\phi^* = (\hat{\phi})_\ell$ dans la base (u, v) :

$$\phi^* = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

Il vient alors :

$$(\deg \phi)\langle u, v \rangle = \langle \phi^* u, \phi^* v \rangle = \langle au + bv, cu + dv \rangle = (\det \phi^*)\langle u, v \rangle$$

puisque l'accouplement $\langle , \rangle$ est alterné. Comme il est non dégénéré, on en déduit que $\det \phi^* = \deg \phi$.

Or, pour toute matrice A de taille 2×2, en écrivant :

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

il vient :

$$\det(A) - \det(1 - A) = ad - bc - (1 - a)(1 - d) + bc = a + d - 1 = \mathrm{Tr}(A) - 1$$

donc $\mathrm{Tr}(\phi^*) = 1 + \deg \phi - \deg(1 - \phi)$. Le nombre de Lefschetz de ϕ dans cette « cohomologie » est donc :

$$L(\phi, E) = \mathrm{Tr}(\mathrm{id}_{\mathbf{Q}_\ell}) - \mathrm{Tr}(\phi^*) + \mathrm{Tr}(\deg \phi \cdot \mathrm{id}_{\mathbf{Q}_\ell}) = \deg(1 - \phi)$$

En particulier, dès que $1 - \phi$ est non-ramifié en tout point de son noyau (ce qui revient à demander que ϕ de n'ait que des points fixes simples), on obtient bien que ϕ a $L(\phi, E)$ points fixes, et la formule de Lefschetz est donc vérifiée.

En outre, le polynôme caractéristique de ϕ^* est unitaire à coefficients entiers, d'après l'expression de la trace et du déterminant, donc on obtient en plus des résultats du 1.4 l'intégralité des polynômes qui interviennent dans la fonction zêta. En fait, on a exactement :

$$Z_E(T) = \frac{\det(1 - T\phi^*)}{(1 - T)(1 - qT)} = \frac{1 - \mathrm{Tr}(\phi^*)T + \det(\phi^*)T^2}{(1 - T)(1 - qT)}$$

Or, pour tout rationnel a/b, on a $\det(1 - (a/b)\phi^*) = \det(b - a\phi^*)/b^2 = \deg(b - a\phi^*)/b^2 \geq 0$. Le polynôme $P(T) = \det(1 - T\phi^*)$ ne peut donc pas avoir deux racines réelles distinctes (sans quoi il prendrait des valeurs strictement négatives en certains rationnels). Ses racines sont donc égales ou conjugées, et on en tout cas même module. Comme leur produit est $1/q$, elles ont donc pour module $q^{-1/2}$, ce qui est exactement l'hypothèse de Riemann.

Références

[Die75] J. Dieudonné, *On the history of the Weil conjectures*, The Mathematical Intelligencer **10** (1975).

[God71] C. Godbillon, *Éléments de topologie algébrique*, Méthodes, Hermann, 1971.

[Har77] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer Verlag, 1977.

[Kat74] N. M. Katz, *Lectures on Deligne's proof of the Riemann Hypothesis for varieties over finite fields*, disponible sous forme numérisée sur `<http://modular.fas.harvard.edu/scans/>`, 1974, notes manuscrites d'un cours donné à Princeton en 1973–1974, prises par S. Bloch.

[Kat76] N. M. Katz, *An overview of Deligne's proof of the Riemann Hypothethis over finite fields*, Amer. Math. Soc. Proc. Symp. Pure Math., vol. 28, 1976.

[Sam63] P. Samuel, *Corps de fonctions algébriques*, Notas de matemática, vol. 28, Instituto de matemática pura e aplicada, Rio de Janeiro, 1963, notes d'un cours donné à Clermont-Ferrand en 1961–1962, rédigées par A. Micali.

[Ser59] J.-P. Serre, *Groupes algébriques et corps de classes*, Publications de l'Institut de mathématiques de Nancago, vol. VII, Hermann, 1959.

[Ser60] J.-P. Serre, *Sur la rationalité des représentations d'Artin*, Ann. of Math **72** (1960), 405–420.

[Ser91] J.-P. Serre, *Motifs*, Astérisque, vol. 198–200, 1991, pp. 333–349.

[Sil86] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer Verlag, 1986.

[Vol01] F. Voloch, *Topics in algebra: equations over finite fields*, disponible sous forme électronique sur `<http://www.ma.utexas.edu/users/voloch/des01.html>`, 2001, notes d'un cours donné à l'Université du Texas en 2001, rédigées par B. van der Ven.