DE L'HYPOTHÈSE DE RIEMANN AUX CONJECTURES STANDARDS

F. DÉGLISE

Table des matières

Conventions

Tous les schémas sont noéthériens.

1. Rappels de théorie de l'intersection

1.1. Cycles algébriques.

Définition 1.1. Soit X un schéma. Si x est un point de X – on entendra simplement un élément de l'ensemble sous-jacent à X – on note $Z(x)$ l'adhérence de $\{x\}$ dans X.

Etant donné un élément $p \in \mathbb{N} \cup \{\infty\}$, on définit deux sous-ensembles de l'ensemble des points de X :

$$X^{(p)} = \{x \in X \mid \operatorname{codim}_X(Z(x)) = p\},$$
$$X_{(p)} = \{x \in X \mid \dim(Z(x)) = p\}.$$

Remark 1.2. La graduation la plus naturelle sur les points de X est celle par la codimension. En effet, dans le cas de la graduation par la dimension, il est souvent plus naturel de remplacer la fonction $\dim(Z(x))$ par d'autres fonctions que l'on appelle simplement *fonction de dimension*.

Définition 1.3. Soit X un schéma. Le groupe de cycles algébriques de X est le groupe abélien libre engendré par l'ensemble des points de X :

$$Z(X) := \langle X \rangle.$$

Date: 3 octobre 2012.

Ce groupe admet deux graduations :

$$Z^p(X) := \langle X^{(p)} \rangle,$$
$$Z_p(X) := \langle X_{(p)} \rangle.$$

A tout sous-schéma fermé noethérien Z de X, on associe un cycle :

$$\langle Z \rangle_X = \sum_{x \in Z^{(0)}} \lg \mathcal{O}_{X,x}.x;$$

l'entier $\lg \mathcal{O}_{X,x}$, longueur de l'anneau artinien $\mathcal{O}_{X,x}$, est appelé la *multiplicité géométrique de x dans X*.

1.4. Soit X un schéma intègre, de corps des fonctions K. Considérons un point $x \in X^{(1)}$ d'anneau local A. On définit l'ordre de tout élément non nul $a \in A$ au point x comme l'entier :

$$\mathrm{ord}_x(a) = \lg \big(A/(a)\big).$$

Notons en effet que $A/(a)$ est bien un anneau artinien (donc de longueur finie) – car a n'est pas diviseur de 0. Notons que K est encore le corps des fractions de A. Ainsi tout élément $f \in K^\times$ s'écrit $f = a/b$ pour des éléments non nuls $a, b \in A$. On vérifie facilement que l'entier :

$$\mathrm{ord}_x(f) := \mathrm{ord}_x(a) - \mathrm{ord}_x(b)$$

est bien définit et induit un morphisme $\mathrm{ord}_x : K^\times \to \mathbb{Z}$.

Avec les notations qui précèdent, on pose pour tout élément $f \in K^\times$.

$$\mathrm{div}(f) = \sum_{x \in X^{(1)}} \mathrm{ord}_x(f).x;$$

en effet la somme est finie.

Nous appellerons un élément $f \in K^\times$ une fonction méromorphe sur X.

Définition 1.5. Un cycle α de X est *rationellement équivalent à* 0 si il existe des sous-schéma fermés intègres $W_1, ..., W_n$ de X et pour chaque entier $i \in [1, n]$ une fonction méromorphe f_i sur W_i tels que :

$$\alpha = \sum_i \mathrm{div}(f_i)$$

où l'on voit le cycle $\mathrm{div}(f_i)$ de W_i comme un cycle de X. On note simplement :

$$\alpha \sim 0.$$

La relation $(\beta - \alpha) \sim 0$, que l'on note encore $\alpha \sim \beta$, définit une relation d'équivalence sur le groupe abélien $Z(X)$.

On pose :

$$\mathrm{CH}(X) = Z(X)/\sim .$$

Si X est caténaire (par exemple de type fini sur un corps), ce groupe est gradué par la codimension. [1]

1.6. Rappelons quelques unes des propriétés des groupes de Chow :

(1) Le foncteur CH^* est contravariant par rapport au morphismes plats f et covariant par rapport aux morphismes propres p (p_* change les degrés codimensionnels).
formule de projection : $f^* p_* = p'_* f'^*$.
formule du degré : f plat fini de degré constant d : $f_* f^*(\alpha) = d.\alpha$.

1. En effet, dans le cas où X est caténaire, le diviseur associé à une fonction méromorphe sur un sous-schéma de codimension n est bien un cycle de codimension $n + 1$.

(2) Si on restreint CH^* aux k-schémas lisses, il devient un foncteur contravariant à valeurs dans les anneaux.
formule de projection (produit) : f propre entre lisses : $f_*(\alpha.f^*(\beta)) = f_*(\alpha).\beta$.

Remark 1.7. Dans le point (2), il suffit de restreindre CH^* aux schémas réguliers d'égales caractéristiques pour avoir les propriétés énumérées. Mais c'est une question ouverte dans le cas des schémas réguliers quelconques. Dans cette voie, Grothendieck, dans [SGA6], a montré que quitte à tuer la torsion dans le groupe de Chow, on obtient toutes les propriétés énumérées dans (2) pour les schémas réguliers quelconques.

1.8. Rappelons pour terminer qu'on associe à tout k-schéma projectif $p : X \to \mathrm{Spec}(k)$ une application degré :

$$\deg = p_* : \mathrm{CH}_0(X) \to \mathrm{CH}_0(\mathrm{Spec}(k)) = \mathbb{Z}.$$

Explicitement, pour un 0-cycle $\alpha = \sum_i n_i.x_i$, on a :

$$\deg(\alpha) = \sum_i n_i.[\kappa(x_i) : k]$$

où $\kappa(x_i)$ est le corps résiduel du point x_i de X.

1.2. **Correspondances.** Dans toute cette section, on fixe un corps de base k.

Définition 1.9. Pour tous k-schémas projectifs lisses X et Y, une correspondance de X vers Y est un élément de

$$C(X,Y) := \bigoplus_{i\in I} CH^{d_i}(X_i \times_k Y)$$

où $(X_i)_{i\in I}$ est la famille des composantes connexes de X, $d_i = \dim(X_i)$.

1.10. Rappelons comment les correspondances se composent : considérons X, Y, Z des k-schémas projectifs lisses, et $(\alpha,\beta) \in C(X,Y) \times C(Y,Z)$. On considère les projections canoniques :

$$p_1 : XYZ \to XY, p_2 : XYZ \to XZ, p_3 : XYZ \to YZ$$

(on a omis le symbole $\times_k$ pour plus de concision). Alors, on pose :

$$\beta \circ \alpha = p_{2*}(p_1^*(\alpha).p_3^*(\beta))$$

qui définit bien un élément de $C(X,Z)$. On vérifie facilement que ce produit est associatif, et définit un produit de composition sur les k-schémas projectifs lisses (en utilisant les propriétés de la théorie de l'intersection rappelées dans le paragraphe 1.6).

Définition 1.11. On note $\mathscr{P}^{cor}(k)$ la catégorie dont les objets sont les k-schémas projectifs lisses et les morphismes sont les correspondances.

Précisons que l'identité de X, en tant que correspondance, est donné par le cycle $\langle\Delta_X\rangle$ associé à la diagonale de X/k. D'ailleurs, à tout morphisme $f : X \to Y$, on associe une correspondance de Y vers X :

$$\gamma_f := \langle\Gamma_f\rangle_{YX}$$

où Γ_f est le graphe de Y dans X, vu à travers l'isomorphisme de permutation des facteurs $XY \simeq YX$. On vérifie que l'on a ainsi définit un foncteur contravariant :

$$\mathscr{P}(k) \to \mathscr{P}^{cor}(k).$$

Remark 1.12. On notera que c'est l'indexe codimensionnel choisit dans la définition des correspondances qui fait que le foncteur précédent est contravariant. Pour cette raison, on parle encore de *correspondances cohomologiques*.

2. Hypothèse de Riemann pour les courbes : la preuve de Weil

Dans toute cette section, on fixe un corps fini k à q éléments, une cloture algébrique $\bar{k}$ de k. Pour tout entier $r > 0$, on note $k_r \subset k$ l'unique sous-extension de corps de k sde degré q^r.

Nous exposons la preuve de l'hypothèse de Riemann à partir du livre [Wei48] de Weil.

2.1. **Fonctions zêta de Hasse-Weil.**

2.1. Si X est un k-schéma projectif lisse de dimension n, on introduit suivant Weil le produit formel :

$$Z_X(t) = \prod_{x \in X_{(0)}} \frac{1}{1 - t^{\delta_x}}$$

où l'on a posé pour tout point fermé x de X : $\delta_x = [\kappa(x) : k]$, degré du corps résiduel de x dans X. Ce produit infini a une importante signification arithmétique, donnée par l'expression suivante :

$$\frac{d}{dt} \log Z_X(t) = \sum_{r>0} N_r . t^{r-1} \tag{2.1.a}$$

où N_r est le nombre de points fermés de X à valeurs dans k_r. On la déduit en effet aisément du fait que

$$N_r = \sum_{x \in X_{(0)}, \delta_x | r} \delta_x.$$

Dans l'article [Wei49], d'une importance historique capitale, Weil énonce les conjectures suivantes sur la fonction zêta qui porte maintenant son nom :

(W1) *Rationalité.–* $Z_X(t)$ est une fonction rationnelle en t.

(W2) *Équation fonctionnelle.–* Si e désigne la multiplicité d'auto-intersection de la diagonale, [2]

$$Z_X\left(q^{-n}.t^{-1}\right) = \pm q^{ne/2} t^e Z_X(t).$$

(W3) Il existe des polynômes $P_i(t) \in \mathbb{Z}[t]$ pour $i = 0, ..., 2n$ tels que :

- (a) $$Z_X(t) = \frac{P_1(t)...P_{2n-1}(t)}{P_0(t)...P_{2n}(t)}.$$
- (b) $P_0(t) = 1 - t$.
- (c) $P_{2n}(t) = 1 - q^n t$.
- (d) *Hypothèse de Riemann.–* $\forall r \in [1, 2n-1]$, les racines complexes de $P_r(t)$ sont toutes de valeur absolue $q^{r/2}$.

Remark 2.2. La *fonction zêta de Hasse-Weil* associée à X est la fonction de s définie par la relation :

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

Dans le cas où X est une courbe, on interprète (W3) comme l'écriture :

$$Z(X, t) = \frac{P_1(t)}{(1-t)(1-q.t)} \tag{2.2.a}$$

---

2. En terme de l'anneau de Chow de $X \times_k X$,

$$e = \deg(\langle\Delta\rangle.\langle\Delta\rangle)$$

où deg est l'application degré de $X \times_k X$ et le produit est pris dans $CH^*(X \times_k X)$. Si X est une courbe de genre g, on obtient donc : $e = 2 - 2g$.

où $P_1(t)$ est un polynôme à coefficients entiers. La propriété (W3)(d) revient alors à demander que les zéros de la fonction ζ_X ont pour partie réelle $\frac{1}{2}$, ce qui est bien l'analogue de l'hypothèse de Riemann (la fonction zêta de Riemann est associée à $\mathrm{Spec}(\mathbb{Z})$ qui est un schéma de dimension 1).

2.3. On peut tracer les étapes suivantes autour des conjectures de Weil :

(1919) H. Kornblum introduit la fonction zêta de $k[x]$ – et même ses variantes obtenues en considérant un caractère, les fonctions L.

(1921) E. Artin dans sa thèse introduit la fonction zêta d'une extension quadratique de l'extension transcendante $k(t)$ de k – et ses variantes, fonction L attachée à un caractère. Il vérifie dans plusieurs cas l'intégralité des conjectures de Weil, y compris l'hypothèse de Riemann – mais il ne formule pas de conjectures sur ce sujet.

(1926) F.K. Schmidt introduit la fonction zêta d'un corps de fonctions (d'une variable) sur k.

(1931) F.K. Schmidt prouve le théorème de Riemann-Roch sur les corps finis,en déduit la rationalité de la fonction zêta attachée à un corps de fonctions sur k – y compris le point (W3)(a) dans ce cas – et l'équation fonctionelle. Notons au passage qu'il prouve que tout corps de fonctions d'une variable sur un corps fini admet un diviseur positif de degré 1.

(1934) H. Hasse publie une preuve de l'hypothèse de Riemann pour les courbes elliptiques. Il s'agit de sa deuxième preuve, la première utilisait la méthode de relèvement d'une courbe sur k en caractéristique 0 avec multiplication complexe, mais elle devait exclure certains cas.

A cette époque, l'hypothèse de Riemann pour les de fonctions d'une variable sur les corps finis est bien acquise, et il est clair qu'Artin est le père de cette conjecture. On peut d'ailleurs citer une lettre de Noether à Hasse de mars 1933 (traduction de P. Roquette, [Roq04a, p. 63]) :

> First of all my congratulation to the "Riemann hypothesis". You have done unbelievably many things lately ! I assume that now you will be able to get at the general Artin-Schmidt zeta function since you already use general class field theory...

(1940) A. Weil annonce une preuve de l'hypothèse de Riemann dans une note aux C.R.A.S. pour les courbes de genre arbitraire. La preuve complète ne sera publiée que 8 ans plus tard après un énorme travail théorique.

(1949) A. Weil introduit la fonction zêta d'une variété algébrique sur k et formule les conjectures ci-dessus.

Cet historique est partiellement construit sur les articles de P. Roquette [Roq04b] et [Roq04a].

2.4. Dans la suite, nous présentons la preuve de Weil de l'hypothèse de Riemann pour les courbes. Rappelons qu'à l'époque de Weil, Schmidt avait démontré les propriétés (W1), (W2) et $(W3)(a)(b)(c)$ pour la fonction zêta associée à une courbe, Hasse avait démontré l'hypothèse de Riemann pour les courbes elliptiques.

2.2. Théorème de Riemann-Roch et méthode de Schmidt.

2.5. Soit X une courbe projectives lisses sur k de genre $g = \dim_k H^1(X, \mathcal{O}_X)$.

Rappelons les points suivants :

- Un diviseur (de Weil) sur X est un cycle $\alpha \in Z^1(X)$. Un diviseur α est positif ou effectif si tous ses coefficients sont positifs. On note $\alpha \geq 0$.
- Les diviseur modulo équivalence rationelle (encore appelée parfois *équivalence linéaire*) forment un groupe en bijection avec le groupe de Picard de X :

$$\mathrm{CH}^1(X) \simeq \mathrm{Pic}(X), \alpha \mapsto \mathcal{L}(\alpha).$$

Puisque X est lisse, le faisceau des formes différentielles de degré 1 est inversible. On note K_X la classe de diviseur correspondante par l'isomorphisme précédent. Par abus de langage, on l'appelle le *diviseur canonique sur X*. [3]

On associé à tout diviseur α de X un entier :

$$l(\alpha) := \dim_k H^0(X, \mathcal{L}(\alpha)).$$

Rappelons que $l(\alpha)$ est encore le cardinal de l'ensemble des diviseurs effectifs rationellement équivalents à α – cet ensemble est classiquement appelé le *système linéaire complet* associé à α.

La formule de Riemann-Roch pour les courbes s'énonce classiquement sous la forme [4] :

Théorème 2.6 (Riemann-Roch)**.** *Sous les hypothèses ci-dessus, la relation suivante est vérifiée :*

$$l(\alpha) - l(K_X - \alpha) = \deg(\alpha) + 1 - g.$$

Cette formule appliquée à K_X donne $\deg(K_X) = 2g - 2$ – en effet, $l(K_X) = g$. Ainsi, lorsque $\deg(\alpha) > 2g - 2$, on obtient :

$$l(\alpha) = \deg(\alpha) + 1 - g$$

puisque $K_X - \alpha$ est alors de degré négatif. [5]

2.7. Décrivons la méthode de Schmidt pour obtenir la rationalité de la fonction Z_X à partir de la formule de Riemann. A nouveau X est une courbe de genre g. Pour tout entier $n \geq 0$, on note ν_n le cardinal de l'ensemble fini suivant :

$$\big\{\alpha \in Z^1(X) \mid \alpha \geq 0, \deg(\alpha) = n\big\}.$$

Suivant la méthode de Dedekind, on peut écrire :

$$\begin{aligned} Z_X(t) &= \prod_{x \in X_{(0)}} \sum_{n=0}^{\infty} t^{(n\delta_x)} = \sum_{\alpha \in Z^1(X), \alpha \geq 0} t^{\deg(\alpha)} \\ &= \sum_{n=0}^{\infty} \nu_n . t^n. \end{aligned}$$

Proposition 2.8. *Pour toute courbe X projective lisse de genre g, il existe un entier $h > 0$ tel qu'on peut écrire :*

$$Z_X(t) = \sum_{n=0}^{2g-2} \nu_n . t^n + \frac{h}{q-1} \cdot \left[\frac{q^{1-g}}{1-qt} - \frac{1}{1-t}\right] \cdot t^{2g-1}.$$

Démonstration. On donne la preuve en admettant qu'il existe un diviseur sur X de degré 1 – cf Corollaire 2.23

Le démonstration repose sur le lemme suivant :

Lemme 2.9. *Il existe un entier $h > 0$ tel que pour tout entier m supérieur à $2g-1$,*

$$\nu_m = \frac{h}{q-1} \cdot (q^{m-g+1} - 1).$$

3. Dans la littérature, on choisit un cycle explicite qui représente la classe de K_X et on appelle ce cycle "diviseur canonique". Toutefois, il est inutile de faire un tel choix puisque l'on peut travailler directement avec la classe de cycles K_X.
4. De nos jours, on la retrouve comme corollaire du théorème de Grothendieck-Riemann-Roch.
5. Cette égalité est parfois appelée *formule de Riemann.*

Pour prouver le lemme, on fixe un entier ν tel que $\nu > 2g-2$ et un ensemble maximal de diviseurs $\alpha_1, ..., \alpha_h$ non rationellement équivalents deux à deux et de degré ν. Ceci définit l'entier $h > 0$ dans l'énoncé du lemme.

Notons que si α est un diviseur de degré ν, la formule de Riemann donne $l(\alpha) = \nu - g + 1 > 0$ et on en déduit que α est rationellement équivalent à l'un des α_i et un seul.

Un calcul simple montre que pour tout diviseur α, le cardinal de l'ensemble des diviseurs positifs rationellement équivalents à α est :

$$\frac{q^{l(\alpha)}-1}{q-1}. \tag{2.9.a}$$

Fixons un entier m satisfaisant l'hypothèse du lemme, et un diviseur α de degré m. Alors, d'après ce qui précède, il existe un unique le diviseur $\alpha - (m-\nu)\alpha_0$, de degré ν, est équivalent à exactement l'un des α_i pour un $i \in \{1, \dots, n\}$:

$$\alpha \sim \alpha_i + (m-\nu)\alpha_0.$$

Or l'ensemble des diviseurs positifs équivalents à $\alpha_i + (m-\nu)\alpha_0$ est, d'après (2.9.a) et la formule de Riemann, de cardinal $\frac{q^{m-g+1}-1}{q-1}$. Le lemme en résulte.

On déduit donc du lemme l'expression suivante :

$$Z_X(t) = \sum_{n=0}^{2g-2} \nu_n . t^n + \sum_{n>2g-2} \frac{h}{q-1} \cdot (q^{n-g+1}-1).t^{n\delta}$$

qui implique facilement le corollaire. □

2.3. **Correspondances.** Dans toute cette section, on fixe une courbe X projective lisse connexe sur un corps fini k de cardinal q.

Définition 2.10. Suivant Weil, on définit l'anneau des correspondances de X comme le groupe abélien :

$$C(X) := \mathrm{CH}^1(X \times_k X)$$

la multiplication étant induite par le produit de composition des correspondances (Paragraphe 1.10).

Cet anneau est muni d'une involution : si l'on considère l'isomorphisme de permutation des facteurs :

$$\epsilon : XX \to XX, (x,y) \mapsto (y,x)$$

on définit la *transposée* d'une correspondance $\alpha \in C(X)$ comme le cycle :

$$\alpha' = \epsilon^*(\alpha).$$

On a ainsi définit un anti-automorphisme de $C(X)$ d'ordre 2 :
- $(\beta \circ \alpha)' = \alpha' \circ \beta'$,
- $(\alpha')' = \alpha$.

2.11. Soit $p_1, p_2 : XX \to X$ les projections canoniques repsectivement sur le premier et le deuxième facteur.

Notons que le morphism projectif p_1 induit en utilisant le pushout sur les cycles un morphisme :

$$p_{1*} : C(X) = \mathrm{CH}^1(XX) \to \mathrm{CH}^0(X) = \mathbb{Z},$$

le dernière identification résultant du fait que X est connexe.

Définition 2.12. Avec les notations qui précèdent, on définit l'indice d'une correspondance α de X comme l'entier

$$d(\alpha) = p_{1*}(\alpha).$$

On définit le coindice de α comme l'entier $d'(\alpha) = d(\alpha')$.

Dans la littérature, étant donnés deux entiers a, b on trouve la terminologie (a, b)-*correspondance* pour désigner une correspondance α telle que $d(\alpha) = a$, $d'(\alpha) = b$ – cf [Ful98, XVI].

Notons la formule suivante :

$$d(\alpha \circ \beta) = d(\alpha)d(\beta). \tag{2.12.a}$$

Ainsi, d est une morphisme d'anneau :

$$d : C(X) \to \mathbb{Z}.$$

Remark 2.13. Rappelons que la variété jacobienne de X est définie comme le groupe abélien $CH^1(X)_0$ des diviseurs de X de degré 0, muni de la structure appropriée de variété algébrique.

Il est facile de voir que toute correspondance α agit sur $\mathrm{CH}^1(X)_0$ par la formule

$$\alpha_*(a) = p_{1*}(\alpha.p_2^*(a)).$$

Cette action, sur les diviseurs de degré 0, est justifiée par la formule :

$$\deg(\alpha_*(a)) = d(\alpha). \deg(a).$$

On en déduit donc un morphisme canonique :

$$C(X) \to \mathrm{End}(J(X)).$$

Un théorème de Weil montre que ce morphisme est surjectif et a pour noyau le groupe des *correspondances dégénérées* (ie de la forme $p_1^*(a)+p_2^*(b)$ pour des divieurs a et b de X).

Etudier les classes de correspondances modulo les correspondances dégénérées revient donc à étudier les endomorphismes de la jacobienne de X.

Définition 2.14. Soit α une correspondance sur X, et δ_X la classe de la diagonale de X. On définit le nombre de points fixes virtuels de X comme l'entier :

$$\deg(\alpha.\delta_X)$$

On définit suivant Weil l'opérateur :

$$\sigma(\alpha) = d(\alpha) + d'(\alpha) - \deg(\alpha.\delta_X).$$

On obtient les relations suivantes :
- $\sigma(\alpha') = \sigma(\alpha)$,
- $\sigma(\alpha \circ \beta) = \sigma(\beta \circ \alpha)$.

Notons en effet pour le dernier point la formule :

$$\deg\big((\beta \circ \alpha).\delta_X\big) = \deg(\alpha.\beta'), \tag{2.14.a}$$

le deuxième membre étant symétrique en α et β (utiliser la formule de projection).[6]

Autrement dit, l'opérateur σ se comporte comme une trace sur l'anneau des correspondances, invariant par transposition.

6. Notons au passage que cet entier est encore appelé le *nombre virtuel des coincidences* de α et β'.

Exemple 2.15. Supposons que X soit birationnelle à $\mathbb{P}^1_k$. Alors le principe de correspondance de Chasles, signifie en langage moderne que pour toute correspondance α,

$$\deg(\alpha.\delta_X) = d(\alpha) + d'(\alpha)$$

autrement dit $\sigma = 0$.

Remark 2.16. Weil considère plutôt cet opérateur sur l'anneau des classes de cycles modulo les correspondances dégénérées (cf Remarque 2.13). Il utilise cela dans la preuve du théorème suivant.

Le point clé de la preuve de Weil est le résultat suivant :

Théorème 2.17 (Weil). *Si X est une courbe de genre $g > 0$, pour toute correspondance α de X,*

$$\sigma(\alpha \circ \alpha') \geq 0$$

et $\sigma(\alpha \circ \alpha') = 0$ si et seulement si α est dégénérée.

Mattuck et Tate ont montré que la positivité de σ est une conséquence du théorème de Riemann-Roch (cf [MT58] et [Gro58] pour une simplification). Notons d'ailleurs qu'ils baptisent cette inégalité de *Castelnuovo-Severi*.

Suivant Fulton, on donne la preuve de cette positivité dans le cas où $\alpha = \gamma_f$ est le graphe d'un endomorphisme $f : X \to X$, cas suffisant pour la preuve de l'hypothèse de Riemann. On suppose que X est connexe ; on définit le degré de f comme l'élément $f_*(1)$ de $\mathrm{CH}^0(X)$, identifié à $\mathbb{Z}$.

Par définition, on obtient :

$$d(\gamma_f) = \deg(f), d'(\gamma_f) = 1.$$

Considérons le carré cartésien

$$\begin{tikzcd} X \arrow[r, "\nu"] \arrow[d, "f"'] & XX \arrow[d, "1\times f"] \\ X \arrow[r, "d"] & XX \end{tikzcd}$$

où d est le morphisme diagonal de X/k, et donc ν est l'immersion du graphe de f – on a identifié Γ_f à X au moyen de l'isomorphisme évident. On en déduit la relation entre fibrés vectoriels :

$$N_\nu = f^{-1}(T_X)$$

où N_ν est le fibré normal de l'immersion fermée ν et T_X est le fibré tangent de X (*i.e.* fibré normal de d).

Alors, d'après le formule d'excès d'intersection,

$$\gamma_f.\gamma_f = \nu_*\nu^*\nu_*(1) = \nu_* f^*(c_1(T_X)).$$

On en déduit

$$\begin{aligned} \deg(\gamma_f.\gamma_f) &= \deg(f^*(c_1(T_X)) = \deg(f_*(1).c_1(T_X)) \\ &= \deg(f). \deg(c_1(T_X)) = (2-2g). \deg(f) \end{aligned}$$

La dernière égalité résulte du fait que $c_1(T_X)$ est l'opposé du diviseur canonique sur X, dont le degré est $2g-2$ d'après la formule de Riemann-Roch.

On a finalement obtenu :

$$\sigma(\gamma_f \gamma'_f) = 2\deg(f) - (2-2g). \deg(f) = 2g \deg(f) \qquad (2.17.a)$$

ce qui prouve le théorème dans le cas de γ_f – ou de toute combinaison linéaire de graphes d'endomorphismes.

Remark 2.18. Weil utilise son théorème pour étudier l'anneau, noté $\mathfrak{A}$ des correspondances finies modulo les correspondances dégénérées – soit les endomorphismes de la jacobienne d'après la remarque 2.13.

Tout d'abord, $\mathfrak{A}$ est sans torsion. Weil démontre de plus, grâce à l'étude des variétés abéliennes, que $\mathfrak{A}$ est de type fini sur $\mathbb{Z}$, de rang inférieur à $4g^2$ – cette borne est d'après lui optimale, en particulier dans le cas $g = 1$. La $\mathbb{Q}$-algèbre $\mathfrak{A}_\mathbb{Q}$ est semi-simple, la $\mathbb{C}$-algèbre $\mathfrak{A}_\mathbb{C}$ est une algèbre de type S.

2.4. **Fin de la preuve.**

2.19. Le principe, découvert par Weil, est d'utiliser l'endomorphisme de Frobenius du k-schéma X :

$$f : X \to X$$

donné par l'identité sur l'ensemble X et par le morphisme de faisceaux d'anneaux :

$$\mathcal{O}_X(U) \to \mathcal{O}_X(U), u \mapsto u^q.$$

On considère f comme une correspondance ι, égale à la classe de cycles associées au graphe de f. Notons en particulier que ι est une $(1, q)$-correspondance :

$$d(\iota) = 1, d'(\iota) = \deg f = q. \tag{2.19.a}$$

L'observation clée est la suivante :

Lemme 2.20. *Considérons les notations qui précèdent. Alors, pour tout entier $r > 0$, le nombre virtuel de points fixes de ι^r (ou f^r) est :*

$$\deg\left(\iota^r \cdot \delta_X\right) = N_r$$

où $N_r = \sharp X(k_r)$ – nombre de points fermés de X à valeur dans l'extension k_r/k de degré q^r.

Démonstration. Si $\bar{X}$ désigne l'extension de X/k à la cloture algébrique $\bar{k}/k$ (fixée en tête de cette section), et que l'on pose $\bar{f} = f \otimes_k \bar{k}$, les points fixes de $\bar{f}^r$ sont exactement les points de $X(k_r)$. Du fait que ι^r est transverse à δ_X, on déduit :

$$\iota_r.\delta_X = \sum_{x \in X(k_r)/G} x$$

où $G = Gal(k_r/k) \simeq \mathbb{Z}/r\mathbb{Z}$. On en déduit la relation attendue. □

Notons que $d(\iota) = 1$ et $d'(\iota) = \deg(f) = q$. Compte tenu de la formule (2.17.a), du lemme précédent et des relations (2.19.a), on obtient la proposition suivante :

Proposition 2.21. *Ayant fixé un entier $r > 0$, les relations suivantes sont vérifiées :*

$$\sigma(\iota^r) = 1 + q^r - N_r, \tag{2.21.a}$$

$$\sigma(\iota^r \gamma_f'^r) = 2gq^r. \tag{2.21.b}$$

On peut d'ailleurs étendre ces relations au cas où $r = 0$ en posant $N_0 = 2g$, puisque $\sigma(\delta_X) = 2g$ – en utilisant par exemple d'après la formule (2.17.a).

On en déduit l'inégalité suivante (que certains auteurs appellent abusivement à mon sens l'hypothèse de Riemann) :

Corollaire 2.22. *Pour tout entier $r > 0$, on a :*

$$|\sigma(\iota^r)| = |1 + q^r - N_r| \leq 2g.q^{r/2}.$$

Démonstration. Pour tout couple d'entiers (x, y), si on applique le théorème 2.17 à la correspondance $\sigma = x.\delta_X + y.\iota^r$ et que l'on tient compte des calculs donnés par la proposition précédente, on obtient l'ingalité suivante :

$$2g.x^2 + 2(1 + q^r - N_r).xy + 2gq^n.y^2 \geq 0$$

Le membre de gauche de cette égalité est donc une forme bilinéaire quadratique semi-définie positive. Son discriminant est donc positif, ce qui est précisément l'inégalité voulue. □

On déduit de l'inégalité précédente le fait suivant, prouvé par Schmidt :

Corollaire 2.23. *Toute courbe projective lisse admet un diviseur de degré positif.*

Démonstration. On déduit du corollaire précédent la minoration suivante :

$$N_r \geq 1 + q^r - 2q.q^{r/2}$$

En particulier, il existe un entier $R > 0$ tel que pour tout $r > R$, $N_r \geq 1$. Soit a et b deux nombres premiers distincts plus grand que R. Alors, X admet un point fermé x dans k_a (resp. y dans k_b). De plus, il existe des entiers $s, t \in \mathbb{Z}$ tels que $sa + tb = 1$. Le diviseur $s.x + t.y$ est alors de degré 1 comme attendu. □

Rappelons qu'on s'est placé à la suite des résultats de Schmidt. La série $Z_X(t)$ s'écrit donc :

$$Z_X(t) = \frac{P_1(t)}{(1-t)(1-qt)}$$

où $P_1(t)$ est un polynôme à coefficients entiers de degré inférieur à $2g$. On déduit d'ailleurs de cette expression que $Z_X(t)$ définie une fontion complexe sur le disque ouvert de rayon $1/q$, et se prolonge en une fonction méromorphe avec pour deux pôles simples, en 1 et $1/q$.

Notons aussi que l'équation fonctionelle (W2) pour $Z_X(t)$ se traduit par l'équation fonctionelle suivante pour $P_1(t)$:

$$P_1(t) = q^g.t^{2g}.P(1/qt). \tag{2.23.a}$$

Théorème 2.24 (Hypothèse de Riemann)**.** *Pour toute courbe X sur un corps fini k, les zéros de la fonction $Z_X(t)$ sont sur le cercle $|t| = q^{-1/2}$.*

Démonstration. Compte tenu de la formule précédant l'énoncé du théorème, on peut écrire :

$$P_1(t) = Z_X(t)(1-t)(1-qt).$$

Dès lors, utilisant les formules (2.1.a) et (2.21.a), on obtient :

$$\frac{d}{dt}\log P_1(t) = -\sum_{r>0} \sigma(\iota^r).t^r.$$

On déduit du corollaire précédent que cette série converge pour $|t| < q^{-1/2}$. Donc $P_1(t)$ est non nulle pour $|t[< q^{-1/2}$. L'équation fonctionelle (2.23.a) montre réciproquement que $P_1(t)$ est non nulle pour $|t| > q^{-1/2}$ d'où le résultat. □

3. L'interprétation topologique de Serre

3.1. **Cohomologie de Weil.** Dans son article [Wei49], Weil énonce une conjecture supplémentaire à celles listées dans le paragraphe 2.1, savoir que le degré b_i du polynôme $P_i(t)$ se comporte comme un nombre de Betti.

D'une part, la somme alternée

$$\sum_{i=0}^{2n} (-1)^i.b_i$$

est égale à l'entier $e = \deg(\delta_X.\delta_X)$, appelée *caractéristique d'Euler-Poincaré de X* par Weil. Les b_i jouent donc le rôle de dimension de groupes de cohomologie.

Par ailleurs, Weil, indique que certains évidences suggèrent que si X admet un relèvement X' en caractéristique 0, le degré de $P_i(t)$ coincide avec le i-ème nombre de Betti de $X'(\mathbb{C})$. Il donne l'exemple des Grasmaniennes pour supporter cette conjecture.

Weil ne parle donc pas de groupe de cohomologie du schéma X, mais il suggère le fait que la cohomologie d'un relevé de X a un rôle à jouer.

3.2. **Théorie de Hodge et valeurs propres.** L'idée de Serre consiste à utiliser la théorie de Hodge en caractéristique 0 pour produire les opérateurs $'$ et σ obtenus sur les correspondances, analogues des opérateurs utilisés par Weil.

3.1. Soit X un schéma projectif lisse sur $\mathbb{C}$ de dimension n – on peut encore utiliser une variété kahlerienne.

On note $H^*(X)$ la cohomologie de Betti à coefficients complexes de X. Cette cohomologie vérifie les propriétés fondamentales suivantes :

– *Formule de Künneth.–*
– *Dualité de Poincaré.–*
– *Théorème de Lefschetz difficile.–* Il existe pour tout $i \leq n$ un isomorphisme :

$$L_X^{n-i} : H^i(X) \to H^{2n-i}(X)$$

donné par le produit avec la classe fondamentale u_X d'une section hyperplane lisse – ou, ce qui revient au même, d'un diviseur ample. On dit encore que X est *polarisée*, la classe u_X étant la polarisation.

On peut alors décomposer la cohomologie de X en parties primitives (décomposition de Lefschetz).

– *Théorème de l'indice de Hodge.–* On déduit du premier point un opérateur C, dit *opérateur de Weil*, tel que le produit :

$$T_X : (a, b) \mapsto \langle a, Cb \rangle \tag{3.1.a}$$

est une forme hermitienne définie positive sur les classes de cohomologie réelle de type (r, r).

A partir de là, on introduit les définitions suivantes :

Définition 3.2. Soit X et Y deux schémas projectifs lisses sur $\mathbb{C}$.

Une correspondance cohomologique de X vers Y est un morphisme $\mathbb{C}$-linéaire

$$a : H(X) \to H(Y)$$

homogène de degré 0.

On dit que a est H-compatible si de plus a est homogène de bidegré $(0, 0)$ par rapport à la décomposition de Hodge et commute à la conjugaison complexe.

D'après la formule de Künneth et la dualité de Poincaré :

$$\mathrm{Hom}(H(X), H(Y)) = H(X)^\vee \otimes H(Y) \simeq H(X) \otimes H(Y) \simeq H(X \times Y)$$

et à travers cet isomorphisme, a correspond à un élément noté $\tilde{a}$ de $H^{2n}(X \times Y)$ – plus généralement, un morphisme homologène par rapport aux degrés cohomologiques de degré d correspond à une classe de $H^{2n+d}(X \times Y)$.

Dire que a est homogène de bidegré $(0, 0)$ par rapport à la bigraduation de Hodge revient à demander que $\tilde{a}$ est de type de Hodge (n, n). Le fait que a commute à la conjugaison revient à demander que $\tilde{a}$ se relève en une classe de cohomologie à coefficients réels – on dit aussi que c'est un *opérateur réel*.

Exemple 3.3. Soit X et Y des $\mathbb{C}$-schémas projectifs lisses.

– Si $f : X \to Y$ est un morphisme de $\mathbb{C}$-schémas , f^* est une correspondance cohomologique H-compatible.
– Si $\alpha \in C(X \times Y)$ est une correspondance, la classe de cohomologie qui lui est associé
$$\gamma(\sigma) \in H^{2n}(X \times Y)$$
est une correspondance cohomologique H-compatible. L'exemple précédent est un cas particulier de celui-ci puisque f^* correspond à la classe de cohomologie associé au graphe de f.

Une correspondance cohomologique de cette forme est dite *algébrique.*

Définition 3.4. Soit X, Y deux schémas projectifs lisses sur $\mathbb{C}$, munis de polarisations L_X et L_Y.

On dit qu'une correspondance cohomologique a de X vers Y est L-compatible si a respecte les décompositions primitives vis à vis de L_X et L_Y. Il revient au même de demander :
$$\forall r, s \geq 0, a(L_X^r(\mathrm{Ker}(L_X^s)) \subset L_Y^r(\mathrm{Ker}(L_Y^s))$$

Toute correspondance algébrique est L, H-compatible.

Remark 3.5. La conjecture de Hodge peut être reformulée en l'assertion suivante : toute correspondance cohomologique de degré quelconque (et pas seulement les correspondances de degré 0 comme ci-dessus) L, H-compatible et rationelle (*i.e.* provenant de la cohomologie à coefficients rationnels) est algébrique.

Théorème 3.6 (Serre)**.** *Soit a une correspondance cohomologique de X vers Y qui est L, H-compatible.*

Soit $a_r : H^r(X) \to H^r(Y)$ la correspondance induite par restriction. On pose :
$$a'_r = (L_X^{r-n})^{-1} \circ {}^{\mathrm{t}}(a_r) \circ L_Y^{n-r}.$$
Alors, si $a_r \neq 0$,
$$tr(a_r \circ a'_r) > 0$$

Démonstration. Notons que a_r et ${}^{\mathrm{t}}\, a_r$ sont par définition adjoints l'un de l'autre par le corchet de dualité de Poincaré relativement à X et Y. Il résulte des définitions choisies que a_r et ${}^{\mathrm{t}}\, a_r$ sont adjoints l'un de l'autre par rapport à la forme (3.1.a) :
$$T_Y(a_r(x), y) = T_X(x, a'_r(y)).$$
Du fait que T_X et T_Y sont définies positives sur les classes de type (r, r), on déduit la formule :
$$tr(a_r a'_r) = N(a_r)^2$$
où N est la norme vis à vis des formes hermitiennes T_X et T_Y. □

3.7. On a donc obtenu :
– Une involution sur les correspondances cohomologiques L, H-compatibles, $a \mapsto a'$.
– Une forme bilinéaire sur les correspondances cohomologiques, la trace, tel que $tr(a - ra'_r)$ est positive.

Suivant la méthode de Weil, on en déduit le corollaire suivant :

Corollaire 3.8. *Soit a une correspondance cohomologique L, H-compatible de X dans X telle que $a_2(u) = q.u$ pour un entier $q > 0$ où u est la polarisation de X.*

Alors a_r est semi-simple et a pour valeur absolue $q^{-r/2}$.

En fait, on a dans ce cas une preuve plus courte que celle utilisant la fonction zêta attachée à a :
$$Z_a(t) = \prod_{i=0}^{2n} \det(1 - a_i.t)^{(-1)^{i+1}}.$$

En effet, si l'on $b_r = q^{-r/2}.a_r$, on obtient une correspondance réelle g telle que $g(u) = u$. On en déduit $g(u^n) = u^n$, ce qui implique que g respecte la classe fondamentale de X et donc la dualité de Poincaré. Il s'en suit que g respecte la forme hermitienne T_X :

$$T_X(g(x), y) = T_X(x, g(y)).$$

Ainsi, g est un opérateur unitaire. Le corollaire en résulte.

Remark 3.9. Les conjectures standards ainsi que la théorie des motifs naissent de la volonté de transporter à la fois la démonstration de Weil et son interprétation complexe par Serre pour les schémas projectifs lisses sur un corps arbitraire.

Références

[Ful98] William Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 1998.

[Gro58] A. Grothendieck. Sur une note de Mattuck-Tate. *J. Reine Angew. Math.*, 200 :208–215, 1958.

[MT58] Arthur Mattuck and John Tate. On the inequality of Castelnuovo-Severi. *Abh. Math. Sem. Univ. Hamburg*, 22 :295–299, 1958.

[Roq04a] P. Roquette. July 3, 2003 the riemann hypothesis in characteristic p, its origin and development. part 2. the first steps by davenport and hasse. (version of july 17, 2003). mitteilungen der mathematischen gesellschaft in hamburg (2004) 5-74. `http://www.rzuser.uni-heidelberg.de/~ci3/rv2.pdf`, 2004.

[Roq04b] P. Roquette. The riemann hypothesis in characteristic p, its origin and development. part 1. the formation of the zeta functions of artin and f.k. schmidt. `http://www.rzuser.uni-heidelberg.de/~ci3/rv.pdf`, 2004.

[SGA6] P. Berthelot, A. Grothendieck, and L. Illusie. *Théorie des intersections et théorème de Riemann-Roch*, volume 225 of *Lecture Notes in Mathematics*. Springer-Verlag, 1971. Séminaire de Géométrie Algébrique du Bois–Marie 1966–67 (SGA 6).

[Wei48] André Weil. *Variétés abéliennes et courbes algébriques*. Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.

[Wei49] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55 :497–508, 1949.