Les conjectures de Weil sur les courbes

Ce travail a été effectué sous la direction de Bernard Le Stum.

Pierre Martinez

24 septembre 2019

Résumé

Cette rédaction est en grande partie basée sur un cours [1] que Paul Monsky a donné au Japon en 1970. Nous commençons par introduire les conjectures de Weil en posant le problème et en discutant du plan d'attaque dans le cas des courbes algébriques, situation dans laquelle on se place à partir de la deuxième section. Puis, on démontre la première des conjectures par des méthodes analytiques en s'appuyant sur le théorème de Riemann-Roch. Enfin, on prouve la troisième conjecture à l'aide de résultats sur la géométrie des surfaces algébriques et de théorie de l'intersection.

1. Voir [Mon70].

Introduction aux conjectures de Weil

On pose $k \coloneqq \mathbb{F}_q$ et $k_s \coloneqq \mathbb{F}_{q^s}$ et on se donne m polynômes $P_1,P_2,\ldots,P_m \in k[X_1,X_2,\ldots,X_n]$. Notons alors $\mathcal{N}_s$ le nombre de solutions dans k_s du système suivant :

$$\begin{cases} P_1(x_1,\, x_2,\ldots,\, x_n) = 0 \\ P_2(x_1,\, x_2,\ldots,\, x_n) = 0 \\ \vdots \\ P_m(x_1,\, x_2,\ldots,\, x_n) = 0 \end{cases}$$

La question qui se pose est la suivante : quelle est la dépendance de $\mathcal{N}_s$ vis-à-vis de s ?
Lorsque l'ensemble des P_i est vide ou lorsque l'on considère l'espace projectif $\mathbb{P}^n_{k_s}$ tout entier la réponse n'est pas très difficile à trouver : on dénombre respectivement q^{ns} et $\frac{q^{s(n+1)}-1}{q^s-1}$ solutions. Mais dans le cas général cela revient à compter le nombre de points dans [2] k_s d'une variété algébrique définie sur k, ce qui est nettement moins facile.

C'est ce problème qui, en 1949, conduisit André Weil à énoncer les conjectures suivantes qui portent aujourd'hui son nom [3] :

1. (Rationalité) Pour n'importe quelle variété algébrique V définie sur k, le nombre de points dans k_s de V vaut $\mathcal{N}_s(V) = \sum_i \alpha_i^s - \sum_j \beta_j^s$ avec α_i et β_j des entiers algébriques.

2. (Equation fonctionnelle) Si V est propre et lisse de dimension n alors l'application $\gamma \longmapsto \frac{q^n}{\gamma}$ induit une permutation des α_i et une permutation des β_j.

3. (Pureté) Si V est propre et lisse alors chaque α_i a pour valeur absolue archimédienne une puissance paire de $\sqrt{q}$ et chaque β_j a pour valeur absolue archimédienne une puissance impaire de $\sqrt{q}$.

4. (Cohomologie) Plus généralement, il existe une théorie cohomologique pour les variétés définies sur des corps arbitraires. Sur le corps des complexes, celle-ci coïncide avec la cohomologie classique, de plus elle se comporte bien vis-à-vis de la réduction. Pour les variétés propres et lisses, celle-ci vérifie des résultats du type dualité de Poincaré et formule du point fixe de Lefschetz. Si de plus V est définie sur $\mathbb{F}_q$ et φ est le morphisme de Frobenius alors les valeurs propres du morphisme induit en cohomologie sont des entiers algébriques de valeur absolue archimédienne $q^{\frac{i}{2}}$.

Anticipons un peu et introduisons la fonction zêta associée à une variété algébrique V définie par $\zeta_V(t) \coloneqq \exp \sum_{s=1}^{\infty} \frac{\mathcal{N}_s}{s} t^s$. Weil a montré [4], et c'est précisément cette idée qui lui a permis de résoudre le problème dans le cas des courbes, que l'on pouvait traduire ses conjectures en termes de propriétés de la fonction zêta. Autrement dit les conjectures précédentes sont équivalentes à celles-ci :

1*. (Rationalité) La fonction ζ_V est une fonction rationnelle de t, c'est-à-dire un quotient de deux polynômes à coefficients rationnels.

2. C'est un abus de langage, on y revient un peu plus bas.
3. Et qui sont devenues des théorèmes dans les années 70.
4. Voir [Wei49].

2*. (Equation fonctionnelle) Notons E le nombre d'auto-intersections de la diagonale Δ de $V \times V$ (c'est-à-dire sa caractéristique d'Euler-Poincaré). Alors ζ_V satisfait à l'équation fonctionnelle suivante :

$$\zeta_V(\tfrac{1}{q^n t}) = \pm q^{\frac{nE}{2}} t^E \zeta_V(t)$$

3*. (Analogue à l'hypothèse de Riemann) On peut écrire la fonction ζ_V comme ci-dessous :

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

avec $P_0(t) = 1 - t$, $P_{2n}(t) = 1 - q^n t$ et pour chaque $1 \leq i \leq 2n-1$, $P_i(t)$ est un polynôme à coefficients entiers que l'on peut écrire comme $P_i(t) = \prod_j (1 - \alpha_{ij} t)$ avec les α_{ij} des entiers algébriques de valeur absolue archimédienne $q^{\frac{i}{2}}$.

4*. (Nombres de Betti) Supposons que l'analogue à l'hypothèse de Riemann soit vérifiée, alors on peut définir le $i$ème nombre de Betti $B_i = B_i(V)$ comme le degré du $i$ème polynôme P_i. Alors $E = \sum_i (-1)^i B_i$. Supposons que V soit obtenue à partir d'une variété W définie sur un anneau de nombres algébriques R par réduction modulo un idéal premier $\mathfrak{p}$ de R. Alors $B_i(V)$ est égal au $i$ème nombre de Betti de l'espace topologique $W_h = (W \times_R \mathbb{C})_h$. Autrement dit, le $i$ème nombre de Betti est le rang du groupe de cohomologie classique $H^i(Y_h, \mathbb{Z})$.

Il sera ici question de démontrer l'équivalence entre **1.** et **1*.** et de donner une preuve de **1.** et **3.** que l'on doit à Grothendieck [5] et Weil [6] dans le cas d'une courbe, i.e d'une variété de dimension 1, propre et lisse de genre g. Quant aux idées de démonstration de **1.**, **2.**, **3.** et **4.** dans leur cadre général et à l'historique des conjectures de Weil on pourra se référer à [Har77] et [Mon70].

5. Voir [Gro58].
6. Voir [Wei71].

Rationalité pour les courbes algébriques

Dans toute la suite, on supposera connues certaines notions de théorie de Galois[7]. Supposons que V soit une variété définie sur un corps parfait k de clôture algébrique $\overline{k}$ et identifions V avec l'ensemble de ses points $\overline{k}$-rationnels[8].

Définitions 1 (0-cycle)**.**

- Un 0-cycle D sur V est une combinaison linéaire $\sum_i n_i P_i$ de points P_i de V avec les $n_i \in \mathbb{Z}$. Le degré d'un 0-cycle D, noté $\deg(D)$, est l'entier $\sum_i n_i [k(P_i) : k]$[9] où $k(P_i)$ est le corps résiduel de P_i sur V. On dit que le 0-cycle est *effectif* si chacun des n_i est positif.
- On dit d'un 0-cycle D qu'il est *k-rationnel* s'il est invariant sous l'action naturelle du groupe de Galois $\mathrm{Gal}(\overline{k}/k)$ sur V.
- Donnons-nous un point P de V et regardons $\{P_i\}$ l'orbite de P, alors on dit que $\sum_i P_i$ est un 0-cycle *premier*.

Supposons maintenant que $k = \mathbb{F}_q$ et posons $k_s \coloneqq \mathbb{F}_{q^s}$, on va définir trois quantités qui interviendront souvent dans tout ce qui va suivre.

Définitions 2.

- $\mathcal{A}_s$ est le nombre de 0-cycles effectifs k-rationnels de degré s sur V.
- $\mathcal{M}_s$ est le nombre de 0-cycles premiers de degré s sur V.
- $\mathcal{N}_s$ est le nombre de points k_s-rationnels de V.

Introduisons à présent notre principal objet d'étude.

Théorème - Définition 1 (Fonction zêta attachée à une variété algébrique)**.**
Les trois séries formelles suivantes sont égales :

(i). $\displaystyle\sum_{s=0}^{\infty} \mathcal{A}_s t^s$

(ii). $\displaystyle\prod_{s=1}^{\infty} (1 - t^s)^{-\mathcal{M}_s}$

(iii). $\displaystyle\exp \sum_{s=1}^{\infty} \frac{\mathcal{N}_s}{s} t^s$

On dit que c'est la fonction zêta attachée à V et on la note ζ_V.

Démonstration.

– (i). = (ii).

Il est à noter que les 0-cycles k-rationnels forment un groupe abélien libre sur les 0-cycles premiers. En effet, on montre sans difficulté que l'application

$$\begin{aligned} \mathbb{Z}[V]^{\mathrm{Gal}(\overline{k}/k)} &\longrightarrow \mathbb{Z}\left[V/\mathrm{Gal}(\overline{k}/k)\right] \\ \sum_i n_i P_i &\longmapsto \sum_i n_i \overline{P_i} \end{aligned}$$

7. Le lecteur pourra consulter [LH12].
8. Quand la variété est définie à partir d'un système d'équations polynomiales ce sont exactement les solutions de ce système dans $\overline{k}$.
9. Cette extension est bien finie d'après le lemme de Zariski.

est un isomorphisme. Donnons ensuite une réécriture (il n'y a rien à démontrer, c'est simplement une autre façon de l'écrire) de (ii). :

$$\prod_{s=1}^{\infty}(1-t^s)^{-\mathcal{M}_s}=\prod_{D\in\mathcal{D}}\left(1-t^{\deg(D)}\right)^{-1}.$$

$\mathcal{D}$ étant ici l'ensemble des 0-cycles premiers sans restriction sur le degré. Il ne reste alors plus qu'à développer cette nouvelle expression :

$$\prod_{D\in\mathcal{D}}\left(1-t^{\deg(D)}\right)^{-1}=\prod_{D\in\mathcal{D}}\sum_{n=0}^{\infty}\left(t^{\deg(D)}\right)^n=\sum_{s=0}^{\infty}\sum_{n_1\deg(D_1)+\ldots+n_r\deg(D_r)=s}t^s=\sum_{s=0}^{\infty}\mathcal{A}_s t^s.$$

Dans l'avant-dernière égalité on somme sur les n_i et les D_i et la liberté conclut.

– (ii). = (iii).

Notons P_d l'ensemble des 0-cycles premiers de degré d sur V. On peut montrer [10] que, pour tout s, l'ensemble des points dans k_s de V est la réunion des P_d pour d divisant s. Ainsi, pour tout s, $\mathcal{N}_s=\sum_{d|s}d\mathcal{M}_d$. Passons au logarithme dans (iii). et développons :

$$\log\left((\text{iii})\,.\right)=\sum_{s=1}^{\infty}\frac{\mathcal{N}_s}{s}t^s=\sum_{s=1}^{\infty}\frac{t^s}{s}\sum_{d|s}d\mathcal{M}_d=\sum_{d=1}^{\infty}d\mathcal{M}_d\sum_{k=1}^{\infty}\frac{t^{kd}}{kd}=\sum_{d=1}^{\infty}\mathcal{M}_d.-\log\left(1-t^d\right).$$

On termine la preuve en passant à l'exponentielle. □

On peut d'ores et déjà démontrer l'équivalence entre **1.** et **1*.**.

Théorème 1 (Weil)**.**

Pour n'importe quelle variété algébrique V définie sur k, $\mathcal{N}_s(V)=\sum_i\alpha_i^s-\sum_j\beta_j^s$ si et seulement si la fonction ζ_V est une fonction rationnelle.

Démonstration.

Commençons par remarquer, par exemple avec (i)., que la fonction ζ_V a pour coefficients des entiers positifs et pour terme constant 1. Supposons donc qu'il existe des nombres complexes α_i et β_j tels que $\mathcal{N}_s(V)=\sum_i\alpha_i^s-\sum_j\beta_j^s$. En se servant de (iii). on obtient :

$$\log(\zeta_V(t))=\sum_{s=1}^{\infty}\frac{\mathcal{N}_s}{s}t^s=\sum_{s=1}^{\infty}\frac{\sum_i\alpha_i^s-\sum_j\beta_j^s}{s}t^s=\sum_{s=1}^{\infty}\sum_i\frac{(\alpha_i t)^s}{s}-\sum_{s=1}^{\infty}\sum_j\frac{(\beta_j t)^s}{s}=\sum_i-\log(1-\alpha_i t)+\sum_j\log(1-\beta_j t)$$

Et en passant à l'exponentielle :

$$\zeta_V(t)=\frac{\prod_j(1-\beta_j t)}{\prod_i(1-\alpha_i t)}.$$

Réciproquement, mettons qu'il existe deux polynômes P et Q dans $\mathbb{C}[t]$ tels que $\zeta_V=\frac{P}{Q}$. Alors on peut supposer que P et Q ont tous deux pour coefficient constant 1 et que $P=\sum_j(1-\beta_j t)$, $Q=\sum_i(1-\alpha_i t)$ avec les α_i, β_j dans $\mathbb{C}$. En utilisant à nouveau (iii). et en regardant la dérivée logarithmique formelle de chaque côté de l'équation $\zeta_V=\frac{P}{Q}$ on trouve $\sum_{s=1}^{\infty}\mathcal{N}_s t^s=\sum_i\frac{\alpha_i t}{1-\alpha_i t}-\sum_j\frac{\beta_j t}{1-\beta_j t}$. Reste à identifier les coefficients devant chacun des t^s pour obtenir $\mathcal{N}_s(V)=\sum_i\alpha_i^s-\sum_j\beta_j^s$. □

A partir de maintenant, nous allons restreindre notre étude aux courbes algébriques. Plus précisément, considérons C une courbe projective, lisse, de genre g sur k. On utilisera désormais le mot « diviseur » pour parler de 0-cycle. Chaque élément f non nul du corps des fonctions de C sur $\overline{k}$, noté $\overline{k}(C)$, définit un diviseur, noté (f), de

10. C'est un résultat de théorie de Galois.

degré 0. Si D est un diviseur sur C on peut s'intéresser à $L(D) \coloneqq \{f \in \overline{k}(C) \mid f = 0 \text{ ou } (f) + D > 0\}$ qui est un espace vectoriel sur $\overline{k}$ de dimension finie $l(D)$.

Définition 1 (Equivalence pour les diviseurs)**.**
On dit que deux diviseurs D et D' sont linéairement équivalents s'il existe f dans $\overline{k}(C)$ tel que $D - D' = (f)$.
Les classes d'équivalence associées à cette relation sont appelées classes de diviseurs.

Avant de donner des résultats sur les diviseurs énonçons des faits [11] dont nous aurons besoin plus tard.

Faits 1.

- Le théorème de Riemann-Roch pour les courbes nous permet d'affirmer ceci :
  - Si $\deg(D) > 2g - 2$ alors $l(D) = \deg(D) - g + 1$.
  - Il existe un diviseur canonique W sur C tel que $\deg(W) = 2g - 2$ et $l(W) = g$.
  - N'importe quel diviseur D de degré $2g-2$ qui n'est pas linéairement équivalent à W vérifie $l(D) = g - 1$.
- Quelques résultats sur la rationalité :
  - Le groupe de Galois $\mathrm{Gal}(\overline{k}/k)$ agit sur $\overline{k}(C)$.
  - On dit d'un élément de $\overline{k}(C)$ qu'il est k-rationnel s'il est invariant sous l'action de $\mathrm{Gal}(\overline{k}/k)$.
  - Si f est k-rationnelle, (f) l'est aussi.
  - Si D est un diviseur k-rationnel alors il existe une base de $L(D)$ dont les éléments sont des fonctions k-rationnelles.
  - Si un diviseur k-rationnel est le diviseur d'une fonction, c'est le diviseur d'une fonction k-rationnelle.
  - Le diviseur canonique W peut être choisi k-rationnel.

On va pouvoir se servir de ceux-ci pour démontrer les théorèmes qui suivent.

Théorème 2.

Donnons-nous D un diviseur k-rationnel. Le nombre de diviseurs *effectifs* k-rationnels linéairement équivalents à D est $\frac{q^{l(D)}-1}{q-1}$.

Démonstration.
Soient $\left(f_1, \ldots, f_{l(D)}\right)$ une base de fonctions k-rationnelles de $L(D)$ et D' un diviseur effectif k-rationnel linéairement équivalent à D. Par définition D' est de la forme $\left(\sum_{i=1}^{l(D)} \alpha_i f_i\right) + D$ avec les $\alpha_i \in k$ non tous nuls. Or, deux $l(D)$-uplets $\left(\alpha_1, \ldots, \alpha_{l(D)}\right)$ et $\left(\alpha'_1, \ldots, \alpha'_{l(D)}\right)$ donnent le même diviseur si et seulement si chaque α'_i vérifie $\alpha'_i = \gamma\alpha_i$ avec γ non nul dans k. Il ne reste plus qu'à compter. □

Théorème 3.

Donnons-nous s un entier. Il n'y a qu'un nombre fini de classes de diviseurs de degré s qui contiennent des diviseurs k-rationnels.

Démonstration.

Si $s \geq 2g$ et $\deg(D) = s$ alors $l(D) = s - g + 1 \geq g + 1 > 0$. Donc si D est linéairement équivalent à un diviseur

11. On renvoie le lecteur à [Har77] et [Per95].

k-rationnel il est équivalent à un diviseur effectif k-rationnel. Or, il n'y a qu'un nombre fini de tels diviseurs de degré s. Dans le cas contraire, il suffit de choisir un diviseur k-rationnel D' de degré suffisamment grand et de considérer l'application qui à D associe $D + D'$. □

Définition 2 (Nombre de classes)**.**
Le nombre de classes de la courbe C sur k, noté h, est le nombre de classes de diviseurs de degré 0 qui contiennent des diviseurs k-rationnels.

On dispose maintenant d'assez de résultats pour pouvoir démontrer la première des conjectures de Weil.

Théorème 4 (Weil)**.**
Donnons-nous C une courbe projective, lisse, de genre g sur $k = \mathbb{F}_q$. Alors $\zeta_C(t) = \prod_{i=1}^{2g} \frac{1-\alpha_i t}{(1-t)(1-qt)}$ avec les α_i des entiers algébriques tels que $\prod_{i=1}^{2g} \alpha_i = q^g$.

Démonstration.
Appelons m le plus petit entier positif tel qu'il existe un diviseur k-rationnel de degré m. On va montrer que $m = 1$. On commence par remarquer que si m ne divise pas s alors $\mathcal{A}_s = 0$. En effet, si ce n'était pas le cas, il existerait un diviseur effectif k-rationnel de degré s et en faisant la division euclidienne de s par m on se rend compte que l'on peut trouver un diviseur k-rationnel de degré plus petit que m. Par contre, si m divise s et si $s > 2g - 2$, alors $\mathcal{A}_s = h(\frac{q^{s-g+1}-1}{q-1})$, ceci découle des faits 1 et du théorème 2.
Ainsi, $\zeta_C(t) = \sum_{s=0}^{\infty} \mathcal{A}_s t^s = $ (polynôme en t^m) $+\frac{h}{q-1} \sum_{s=0}^{\infty} (q^{ms-g+1}-1)t^{ms} = $ (polynôme en t^m) $+\frac{h}{q-1}(\frac{q^{1-g}}{1-q^m t^m} - \frac{1}{1-t^m})$ et en mettant tout au même dénominateur on en conclut que $\zeta_C(t)$ est un quotient de deux polynômes en t^m. Profitons-en pour observer que $\zeta_C(t)$ a un pôle simple en $t = 1$. Posons ensuite $f(t) \coloneqq \prod_{s=1}^{\infty} (1 - t^s)^{-\mathcal{M}_{ms}}$, alors $\zeta_C(t) = f(t^m)$ et f peut s'écrire comme quotient de deux polynômes. Notons $\zeta_C^\dagger(t)$ la fonction zêta attachée à C sur k_m. Alors $\zeta_C^\dagger(t) = \prod_{s=1}^{\infty} (1 - t^s)^{-\mathcal{M}_s^\dagger}$ où $\mathcal{M}_s^\dagger$ joue le même rôle que $\mathcal{M}_s$ sur k_m. Puis, si on se donne un point P de la courbe C vue sur k_m celui-ci définit un diviseur effectif k-rationnel. $\mathcal{A}_{\deg(P)}$ est de ce fait non nul donc $\deg(P) = [k(P) : k_m]$ est divisible par m et en appliquant la multiplicativité du degré à la suite d'extensions $k(P) \supset k_m \supset k$ on obtient $[k(P) : k] = m.[k(P) : k_m]$ et $\mathcal{M}_s^\dagger = m.\mathcal{M}_{ms}$. Ainsi $\zeta_C^\dagger(t) = f(t)^m$. Or, de même que $\zeta_C(t)$, $\zeta_C^\dagger(t)$ a un pôle simple en $t = 1$, nécessairement $m = 1$.

Par conséquent, $\zeta_C(t) = \frac{P(t)}{(1-t)(1-qt)}$ avec P à coefficients entiers et de coefficient constant égal à 1. Supposons $g = 0$, alors, pour tout s positif, $\mathcal{A}_s = h(\frac{q^{s+1}-1}{q-1})$ et en évaluant en $s = 0$ on obtient $h = \mathcal{A}_0 = 1$.
Donc $\zeta_C(t) = \sum_{s=0}^{\infty} (\frac{q^{s+1}-1}{q-1})t^s = \frac{1}{(1-t)(1-qt)}$ et $P = 1$. Supposons maintenant $g > 0$ et posons $\tilde{\mathcal{A}}_s \coloneqq \frac{h}{q-1}(q^{s-g+1} - 1)$. Si $s > 2g - 2$, $\mathcal{A}_s = \tilde{\mathcal{A}}_s$. D'après les faits 1 et le théorème 2 on compte $\frac{q^g-1}{q-1}$ diviseurs effectifs k-rationnels dans la classe des diviseurs qui contient le diviseur canonique alors que dans les autres classes de diviseurs de degré $2g - 2$ on en dénombre $\frac{q^{g-1}-1}{q-1}$. Ainsi, $\mathcal{A}_s = \tilde{\mathcal{A}}_s + q^{g-1}$ pour $s = 2g - 2$ et $\sum_{s=0}^{\infty} \tilde{\mathcal{A}}_s t^s = \frac{h}{q-1}(\frac{q^{1-g}}{1-qt} - \frac{1}{1-t})$ que l'on peut écrire sous la forme $\frac{a+bt}{(1-t)(1-qt)}$. Enfin, $\zeta_C(t) = \sum_{s=0}^{2g-2} (\mathcal{A}_s - \tilde{\mathcal{A}}_s)t^s + \sum_{s=0}^{\infty} \tilde{\mathcal{A}}_s t^s = (q^{g-1}t^{2g-2} + \ldots) + \frac{a+bt}{(1-t)(1-qt)}$. Il s'ensuit immédiatement que $P(t) = q^g t^{2g} + \ldots$. Reste à écrire P sous la forme $P = \prod_{i=1}^{2g} (1 - \alpha_i t)$ et comme les coefficients de P sont des entiers, les α_i sont des entiers algébriques. Enfin, la relation entre coefficients et racines de P nous dit que $\prod_{i=1}^{2g} \frac{1}{\alpha_i} = (-1)^{2g} \frac{1}{q^g}$ donc $\prod_{i=1}^{2g} \alpha_i = q^g$. □

On termine en traduisant le résultat précédent via le théorème 1 pour obtenir $\mathcal{N}_s(C) = q^s + 1 - \sum_{i=1}^{2g} \alpha_i^s$.

Pureté pour les courbes algébriques

Dans ce qui va suivre on supposera connus certains résultats sur la géométrie des surfaces algébriques [12]. On va énoncer deux lemmes puis un théorème sur lequel se base la démonstration que l'on donne de la troisième conjecture de Weil.

Lemme 1.

Donnons-nous $z_1, \ldots, z_n$ des nombres complexes tous de module 1. Alors il existe une infinité d'entiers m strictement positifs tels que chaque z_k^m est proche de 1.

Démonstration.

Pour tout $1 \leq k \leq n$, on écrit $z_k = e^{i\theta_k}$ et par densité de $\mathbb{Q}$ dans $\mathbb{R}$ il existe (p_k, q_k) dans $\mathbb{Z} \times \mathbb{N}^*$ tel que pour tout $\varepsilon > 0$, $|\theta_k q_k - 2\pi p_k| < \varepsilon$. Reste à poser $m \coloneqq \prod_{k=1}^{n} q_k$ et à le multiplier par n'importe quel entier. □

Lemme 2.

Donnons-nous $z_1, \ldots, z_n$ des nombres complexes. Alors il existe une infinité d'entiers $m > 0$ tels que $|z_1|^m \leq |\sum_{i=1}^{n} z_i^m|$.

Démonstration.

Supposons pour commencer que $z_1 = 1$, dans ce cas on souhaite montrer qu'il existe une infinité de m tels que $|1 + \sum_{i=2}^{n} z_i^m| \geq 1$. Le lemme précédent nous dit qu'il en existe une infinité tels que les $(\frac{z_i}{|z_i|})^m$ sont proches de 1 et donc que les parties réelles des z_i^m sont toutes strictement positives. Ainsi,

$$|1 + \sum_{i=2}^{n} z_i^m| = \sqrt{\left(1 + \mathfrak{Re}(z_2^m) + \ldots + \mathfrak{Re}(z_n^m)\right)^2 + \left(\mathfrak{Im}(z_2^m) + \ldots + \mathfrak{Im}(z_n^m)\right)^2} \geq 1.$$

Si $z_1 \neq 1$ et $z_1 \neq 0$ (si ce n'était pas le cas le résultat serait immédiat) alors il suffit de voir que l'inégalité du lemme est équivalente à $\frac{|z_1|^m}{|z_1|^m} \leq |1 + \sum_{i=2}^{n} \left(\frac{z_i}{z_1}\right)^m|$. □

Théorème 5.

Les assertions suivantes sont équivalentes :

(i). Pour tout i, $|\alpha_i| = \sqrt{q}$.

(ii). Il existe une constante non nulle c telle que pour tout s, $|\mathcal{N}_s(C) - q^s - 1| \leq c.q^{\frac{s}{2}}$.

Démonstration.

Si, pour tout i, $|\alpha_i| = \sqrt{q}$ alors, d'après la rationalité de la fonction zêta,

$$|\mathcal{N}_s(C) - q^s - 1| = |\sum_{i=1}^{2g} \alpha_i^s| \leq \sum_{i=1}^{2g} |\alpha_i|^s \leq 2g.q^{\frac{s}{s}}.$$

Réciproquement, d'après le lemme 2 il existe une infinité de $s > 0$ tels que $|\alpha_1|^s \leq |\sum_{i=1}^{2g} \alpha_i^s| = |\mathcal{N}_s - q^s - 1| \leq c.q^{\frac{s}{2}}$. Ainsi, $|\alpha_1| \leq \sqrt{q}$. Comme ce lemme est aussi valable pour n'importe lequel des α_i, on mène le même raisonnement pour montrer que $|\alpha_i| \leq \sqrt{q}$. Enfin, $\prod_{i=1}^{2g} \alpha_i = q^g$ entraîne $|\alpha_i| = \sqrt{q}$ pour tout i. □

12. Le lecteur est invité à consulter [Mum66].

Quittons maintenant le monde des courbes pour penser en termes de surfaces. On va donner des définitions mais surtout des faits[13] indispensables à la preuve de la pureté des courbes.

Définition 3 (Diviseur sur une surface)**.**
Un diviseur D sur une surface S est une combinaison linéaire $\sum_i n_i C_i$ où les C_i sont des courbes irréductibles et les n_i sont dans $\mathbb{Z}$.

Faits 2.

- On peut définir une forme bilinéaire symétrique sur les diviseurs à valeurs dans $\mathbb{Z}$ appelée produit d'intersection. Pour deux diviseurs D et D' on note $(D.D')$ leur produit d'intersection.
- Si on se donne D un diviseur et si on note $\mathcal{F}(D)$ le faisceau inversible attaché à D et $h^i(D) \coloneqq \dim H^i(S, \mathcal{F}(D))$ alors le théorème de Riemann-Roch pour S nous affirme que $h^0(D) - h^1(D) + h^2(D) = \frac{1}{2}(D.D - K) + c$ où K est un diviseur canonique fixé sur S et c une constante.
- La dualité de Serre nous dit que $h^2(D) = h^0(K - D)$ et en notant $l(D) \coloneqq h^0(D)$ on obtient $l(D) + l(K - D) \geq \frac{1}{2}(D.D - K) + c$.

Considérons un plongement projectif $S \subseteq \mathbb{P}^n$ et H une section hyperplane de S. Si D est un diviseur sur S on pose $\deg(D) \coloneqq (D.H)$. On va présenter quelques lemmes sur les diviseurs.

Lemme 3.
Donnons-nous $\{D_i\}$ un ensemble de diviseurs sur S. Si l'ensemble des degrés $\{deg(D_i)\}$ est majoré alors l'ensemble des dimensions $\{l(D_i)\}$ l'est aussi.

Démonstration.
La preuve étant trop sophistiquée pour être exposée ici on se limite à dire qu'elle repose sur la notion de variété de Chow. □

Lemme 4 (Inégalité de Hodge)**.**
Soit D un diviseur sur S. Si $\deg(D) = 0$ alors le produit d'intersection $(D.D) \leq 0$.

Démonstration.
Le lemme précédent nous dit que les ensembles $\{l(nD)\}$ et $\{l(K - nD)\}$ sont majorés pour tout n dans $\mathbb{Z}$. Donc d'après les faits 2, pour tout n dans $\mathbb{Z}$, $(nD.nD - K)$ est majoré et par bilinéarité du produit d'intersection $(D.D) \leq 0$. □

Supposons maintenant que $S = C \times C'$ avec C et C' des courbes projectives, lisses.

Définition 4.
Donnons-nous D un diviseur sur S. On définit deux nouvelles quantités à partir du produit d'intersection : $d_1(D) \coloneqq (D.P \times C')$ et $d_2(D) \coloneqq (D.C \times P')$ avec P et P' des points sur C et C'.

La définition précédente ne dépend bien entendu pas du choix de P et P'.

Lemme 5 (Inégalité de Castelnuovo)**.**
Donnons-nous D un diviseur sur S. Alors $(D.D) \leq 2.d_1(D).d_2(D)$.

13. A nouveau, on renvoie le lecteur à [Har77] et [Per95].

Démonstration.

Notons V l'espace vectoriel de dimension 3 sur $\mathbb{Q}$ engendré par les diviseurs $P \times C'$, $C \times P'$ et D. La matrice du produit d'intersection dans cette base est la suivante :

$$M \coloneqq \begin{pmatrix} 0 & 1 & d_1(D) \\ 1 & 0 & d_2(D) \\ d_1(D) & d_2(D) & (D.D) \end{pmatrix}$$

Supposons que $\det(M) = 2.d_1(D).d_2(D) - (D.D) < 0$, choisissons une base orthogonale (E_1,E_2,E_3) de V et posons $a_i \coloneqq (E_i.E_i)$. Le fait que la matrice de la forme quadratique associée au produit d'intersection est diagonale dans cette nouvelle base implique que $a_1a_2a_3 < 0$ et on peut par exemple supposer $a_1 > 0$, $a_2 > 0$ et $a_3 < 0$. En effet, si les a_i étaient tous strictement négatifs la forme quadratique le serait aussi, or elle est indéfinie sur V. On peut donc construire un diviseur E qui est une combinaison linéaire de E_1 et E_2, de degré nul et tel que $(E.E) > 0$. Ce qui rentre en contradiction avec l'inégalité de Hodge. □

Donnons-nous C une courbe projective, lisse et $\varphi : C \longrightarrow C$ un morphisme. Notons Γ_φ et Δ les graphes respectifs de φ et de l'application identité sur C vus sur la surface $S \coloneqq C \times C$. On arrive à la dernière étape avant la preuve de la pureté.

Théorème 6.

Soit φ de degré d. Alors $|(\Gamma_\varphi.\Delta) - 1 - d| \leq (2 - (\Delta.\Delta)).\sqrt{d}$.

Démonstration.

De même que pour le lemme 3 on se borne à dire que l'idée est d'appliquer l'inégalité de Cauchy-Schwarz à une nouvelle forme bilinéaire symétrique puis d'utiliser le fait que le produit d'intersection commute avec une application bien choisie dans un anneau de Chow. □

Théorème 7 (Weil)**.**

Donnons-nous C une courbe projective, lisse, de genre g sur $k = \mathbb{F}_q$. Alors $\mathcal{N}_s(C) = q^s + 1 - \sum_{i=1}^{2g} \alpha_i^s$ avec, pour tout i, $|\alpha_i| = \sqrt{q}$.

Démonstration.

Regardons $\varphi : C \longrightarrow C$ le morphisme de Frobenius. Alors $\deg(\varphi^s) = q^s$ et le théorème précédent nous permet d'affirmer que $|(\Gamma_{\varphi^s}.\Delta) - q^s - 1| \leq (2 - (\Delta.\Delta)).q^{\frac{s}{2}}$. Or, Γ_{φ^s} et Δ s'intersectent précisément aux points de C dans k_s, de plus ils se rencontrent toujours avec multiplicité d'intersection égale à 1. Ainsi, $(\Gamma_{\varphi^s}.\Delta) = \mathcal{N}_s$ et il ne reste plus qu'à appliquer le théorème 5. □

Références

[Wei49] André Weil. "Numbers of solutions of equations in finite fields". In: *Bull. Amer. Math. Soc.* 5 (1949), pp. 497–508.

[Gro58] Alexandre Grothendieck. "Sur une note de Mattuck-Tate". In: *J. Reine u. Angew. Math.* 200 (1958), pp. 208–215.

[Mum66] David Mumford. *Lectures on Curves on an Algebraic Surface*. Annals of Mathematics Studies. Princeton University Press, 1966.

[Mon70] Paul Monsky. *p-Adic Analysis and Zeta Functions*. Lectures in Mathematics. Kinokuniya Book-store Company, 1970.

[Wei71] André Weil. *Courbes Algébriques et Variétés Abéliennes*. Hermann, 1971.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer-Verlag, 1977.

[Per95] Daniel Perrin. *Géométrie algébrique*. Savoirs Actuels. InterEditions / CNRS Editions, 1995.

[LH12] Yves Laszlo and David Hernandez. *Introduction à la théorie de Galois*. Mathématiques et Applications. Ecole Polytechnique, 2012.