Nombre de solutions d'équations dans les corps finis : l'article fondateur de Weil

Rodolphe LAMPE
TER encadré par Jérôme Germoni

7 juin 2007

Table des matières

Cet article vise à exposer et détailler l'article d'André Weil : Numbers of solutions of equations in finite fields qui est une introduction aux conjectures de Weil.
Dans un premier temps on énoncera les conjectures de Weil (partie 1) puis on étudiera un peu d'analyse harmonique sur les groupes finis (partie 2), les corps finis et le théorème de Hasse-Davenport (partie 3) pour pouvoir attaquer l'article de Weil. Nous verrons le cas des variétés diagonales affines (partie 4) puis une interprétation des conjectures de Weil par l'étude de la fonction zeta des variétés diagonales homogènes projectives (partie 5). Pour finir, un petit historique des développements sur les conjectures de Weil (partie 6).

Soit $r \in \mathbb{N}^*, n_0, \ldots, n_r \in \mathbb{N}^*, a_0, \ldots, a_r \in \mathbb{F}_q^\times$ et on cherche à compter le nombre de solutions des équations du type :

$$a_0 x_0^{n_0} + \ldots + a_r x_r^{n_r} = b,$$

où les x_i sont dans le corps fini $\mathbb{F}_q$. On suppose les a_i tous non nuls. On note N le nombre de solutions de l'équation.

1 Les conjectures de Weil

En 1949, André Weil énonça ses fameuses conjectures sur le nombre de solutions des équations à coefficients dans les corps finis. Ces conjectures lient fortement l'arithmétique de variétés algébriques sur les corps finis et la topologie de variété algébrique définis sur les complexes.

1.1 Enoncé des conjectures

Soit X une variété algébrique sur $\mathbb{F}_q$. Par exemple, l'ensemble des solutions dans l'espace affine ou projectif d'un nombre fini d'équations polynomiales à coefficients dans $\mathbb{F}_q$. Pour chaque entier $\nu \geq 1$, on peut définir le nombre N_ν de points rationnels de X sur l'extension $\mathbb{F}_{q^r}$. Les nombres N_i sont d'une grande importance dans l'étude des propriétés arithmétiques de X. Pour les étudier, on définit la fonction zeta de X :

$$Z(X,t) = \exp\left(\sum_{\nu=1}^{+\infty} N_\nu \frac{t^\nu}{\nu}\right).$$

On peut maintenant énoncer les conjectures de Weil :

Théorème 1.1 (Théorème de Weil)
Soit X une variété sans points singuliers de dimension n définie sur le corps $\mathbb{F}_q$. Soit N_ν le nombre de points rationnels de X sur l'extension $\mathbb{F}_q^\nu$. Alors :

$$\sum_{\nu \geq 1} N_\nu U^{\nu-1} = \frac{d}{dU} \log(Z(U)),$$

où $Z(U)$ est une fraction rationelle en U, vérifiant l'équation fonctionelle :

$$Z\Big(\frac{1}{q^n U}\Big) = \pm q^{n\chi/2} U^\chi Z(U),$$

où χ est la caractéristique d'Euler-Poincaré de X (nombre d'intersections de la diagonale avec elle-même sur le produit $X \times X$). De plus :

$$Z(U) = \frac{P_1(U) \cdots P_{2n-1}(U)}{P_0(U) \cdots P_{2n}(U)},$$

avec $P_0(U) = 1 - U, P_{2n}(U) = 1 - q^n U$*, et, pour* $1 \leq h \leq 2n-1$:

$$P_h(U) = \prod_{i=1}^{B_h}(1 - \alpha_{h_i} U),$$

où les α_{h_i} *sont des entiers algébriques de module* $q^{h/2}$*.*

Les degrées B_h des polynômes P_h sont appellés nombres de Betti de la variété X. La caractéristique d'Euler-Poincaré χ est définie par la formule :

$$\chi = \sum_h (-1)^h B_h.$$

1.2 Cas faciles : les espaces projectifs

On calcule facilement la fonction zeta de l'espace projectif $\mathbb{P}^n$ pour tout $n \geq 1$. En effet, pour tout $\nu \geq 1$, le nombre de points dans l'extension de degré ν de $\mathbb{P}^n$ est :

$$N_\nu = 1 + q^\nu + \cdots + q^{n\nu}.$$

Ainsi :

$$\begin{aligned}
\log(Z(\mathbb{P}^n, T)) &= \sum_{\nu=1}^{+\infty}(1 + q^\nu + \cdots + q^{n\nu})\frac{T^\nu}{\nu} \\
&= \sum_{k=0}^{n}\sum_{\nu=1}^{+\infty}\frac{(q^k T)^\nu}{\nu} \\
&= \sum_{k=0}^{n} -\log(1 - q^k T).
\end{aligned}$$

Ainsi la fonction zeta de l'espace projectif $\mathbb{P}^n$ est la fraction rationnelle :

$$Z(\mathbb{P}^n, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^n T)}.$$

On voit sans difficulté que cette fonction satisfait les conjectures de Weil.

Remarque 1.2
On a l'analogie entre le calcul du nombre de points pour les espaces projectifs sur les corps finis $(1 + q + \cdots + q^n)$ *et la décomposition cellulaire :*

$$\begin{aligned}
\mathbb{P}^n(\mathfrak{K}) &= \mathfrak{K}^n \cup \mathbb{P}^{n-1}(\mathfrak{K}) \\
&= \mathfrak{K}^n \cup \mathfrak{K}^{n-1} \cup \ldots \cup \mathfrak{K} \cup \infty.
\end{aligned}$$

Si $\mathfrak{K}$ *est un corps fini, on obtient immédiatement le nombre de points. Si* $\mathfrak{K}$ *est le corps des complexes, on peut calculer l'homologie singulière de* $\mathbb{P}^n(\mathfrak{K})$*.*

2 Analyse harmonique des groupes abéliens finis

2.1 Caractères des groupes abéliens finis

Soit G un groupe abélien fini. On note $n = \text{card } G$.

Définition 2.1
On appelle caractère de G *tout homomorphisme de* G *dans le groupe multiplicatif* $\mathbb{C}^\times$ *des nombres complexes.*

Les caractères de G forment naturellement un groupe $\mathrm{Hom}(G, \mathbb{C}^\times)$ que l'on note $\widehat{G}$ et que l'on appelle le dual de G.

Le cas G cyclique nous intéresse tout particulièrement car nous regarderons les caractères du groupe multiplicatif d'un corps fini $\mathbb{F}_q$. Soit donc G cyclique d'ordre n et on fixe w un générateur de G. Puisque w est d'ordre n, son image par tout caractère est une racine n-ème de l'unité. Inversement, si $\alpha \in \{0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}\}$, il existe un unique caractère χ_α tel que

$$\chi_\alpha(w) = e^{2i\pi\alpha}.$$

En effet, χ_α est défini par $\chi_\alpha(w^k) = e^{2i\pi\alpha k}$ pour $k \in \mathbb{Z}$. Comme w engendre G, χ_α est bien défini sur G. On a montré :

Proposition 2.2
Soit G cyclique d'ordre n et w un générateur. Alors l'application

$$\begin{array}{ccc} \{0, \frac{1}{n}, \ldots, \frac{n-1}{n}\} & \to & \widehat{G} \\ \alpha & \mapsto & \chi_\alpha \end{array}$$

où $\chi_\alpha(w) = e^{2i\pi\alpha}$ est une bijection.

Remarque : En fait, $\chi_\alpha\chi_{\alpha'} = \chi_\beta$ où β est l'unique élément de $\{0, \frac{1}{n}, \ldots, \frac{n-1}{n}\}$ tel que $\alpha+\alpha' \equiv \beta[1]$ si bien que $\widehat{G}$ est cyclique, engendré par $\chi_{1/n}$ et isomorphe à G.

Proposition 2.3
Soit G un groupe abélien fini, alors $\widehat{G}$ est isomorphe à G.

On sait que G est un produit de groupes cycliques. Or, si G et H sont deux groupes abéliens finis, on établit facilement l'isomorphisme $\widehat{G \times H} \simeq \widehat{G} \times \widehat{H}$. La proposition 2.3 découle donc de la proposition 2.2.

2.2 Relations d'orthogonalité

Proposition 2.4 (Relations d'orthogonalité)
Soit $\chi \in \widehat{G}$, on a :

$$\sum_{x\in G} \chi(x) = \begin{cases} n & si\ \chi = \mathbf{1}, \\ 0 & si\ \chi \neq \mathbf{1}. \end{cases}$$

Dualement, si $x \in G$ alors :

$$\sum_{\chi\in\widehat{G}} \chi(x) = \begin{cases} n & si\ x = 1, \\ 0 & si\ x \neq 1. \end{cases}$$

En effet, pour la première relation d'orthogonalité, soit $\chi \in \widehat{G}$ non trivial et $y \in G$ tel que $\chi(y) \neq 1$. Alors

$$\sum_{x\in G} \chi(x) = \sum_{x\in G} \chi(y)\chi(y^{-1}x) = \chi(y) \sum_{x\in G} \chi(y^{-1}x) = \chi(y) \sum_{z\in G} \chi(z) = \chi(y) \sum_{x\in G} \chi(x).$$

La relation est prouvée pour tout χ non trivial et elle est triviale pour $\chi = \mathbf{1}$.
Pour la seconde relation d'orthogonalité, il suffit d'appliquer la première relation pour le groupe $H = \widehat{G}$ et le caractère $\widehat{x} \in \widehat{H} = \widehat{\widehat{G}}$ défini, pour $\chi \in \widehat{G}$, par $\widehat{x}(\chi) = \chi(x)$.

Définition 2.5
On définit un produit scalaire hermitien sur $\mathbb{C}^G$:

$$\forall f, f' \in \mathbb{C}^G,\ \langle f, f' \rangle = \frac{1}{n} \sum_{x\in G} \overline{f(x)} f'(x).$$

Proposition 2.6
On a :

$$\forall \chi, \chi' \in \widehat{G},\ \langle \chi, \chi' \rangle = \begin{cases} 1 \text{ si } \chi = \chi' \\ 0 \text{ si } \chi \neq \chi' \end{cases}$$

En effet, cela découle immédiatement des relations d'orthogonalité.

Proposition 2.7
L'ensemble $\widehat{G}$ est une base orthonormée de $\mathbb{C}^G$ muni de $\langle ., . \rangle$.

2.3 Sommes de Gauss

Les sommes de Gauss lient un caractère multiplicatif et un caractère additif. Elles sont très utiles et elles ont de nombreuses applications. Une grande partie de l'article de Weil utilise de telles sommes. L'introduction des sommes de Gauss par Weil est l'une des grandes astuces utilisées pour répondre au problème.

Soit ψ un caractère additif fixé non trivial de $\mathbb{F}_q$. On définit la somme de Gauss $g(\chi)$ où χ est un caractère multiplicatif non trivial de $\mathbb{F}_q$ (χ est un caractère de $\mathbb{F}_q^\times$ que l'on a prolongé en 0 : 1 si χ est trivial et 0 sinon) :

$$g(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x).$$

Proposition 2.8
Pour tout caractère χ non trivial de $\mathbb{F}_q$, la somme de Gauss $g(\chi)$ vérifie :

$$g(\chi)\overline{g(\chi)} = q.$$

Remarque : Si χ est trivial alors $g(\chi) = 0$ d'après les relations d'orthogonalité pour $(\mathbb{F}_q, \psi)$.

Comme χ est supposé non trivial, $\chi(0) = 0$ donc :

$$g(\chi)\overline{g(\chi)} = \Big(\sum_{x \neq 0} \chi(x)\psi(x) \Big) \Big(\sum_{y \neq 0} \chi(y^{-1})\psi(-y) \Big) = \sum_{y \neq 0} \sum_{x \neq 0} \chi(xy^{-1})\psi(x-y).$$

Si l'on effectue le changement de variable $x \leftarrow xy$, dans la somme sur x, on obtient :

$$\begin{aligned} g(\chi)\overline{g(\chi)} &= \sum_{y \neq 0} \sum_{x \neq 0} \chi(x)\psi((x-1)y) \\ &= \sum_{x \neq 0} \chi(x) \sum_{y \neq 0} \psi((x-1)y). \end{aligned}$$

Si $x \neq 1$ alors, ψ étant non trivial, on a d'après les relations d'orthogonalité :

$$\sum_{y \neq 0} \psi((x-1)y) = -\psi((x-1) \times 0) = -1,$$

et si $x = 1$ alors :

$$\sum_{y \neq 0} \psi((x-1)y) = q - 1.$$

Ainsi :

$$g(\chi)\overline{g(\chi)} = q - \sum_{x \neq 0} \chi(x).$$

On a choisi χ non trivial, donc la seconde somme est nulle, et donc :

$$g(\chi)\overline{g(\chi)} = q.$$

2.4 Transformée de Fourier

On définit la transformée de Fourier $\mathcal{F}$ l'application qui à toute fonction f sur $\mathbb{F}_q$, à valeurs dans $\mathbb{C}$, associe $\mathcal{F}\phi$:

$$\forall y \in \mathbb{F}_q, (\mathcal{F}f)(y) = \sum_{x \in \mathbb{F}_q} f(x)\psi(xy).$$

Proposition 2.9
Pour toute fonction f sur $\mathbb{F}_q$, à valeurs dans $\mathbb{C}$, on a :

$$\forall z \in \mathbb{F}_q, (\mathcal{F}^2 f)(z) = qf(-z).$$

En effet, soit $z \in \mathbb{F}_q$ alors :

$$\begin{aligned}
(\mathcal{F}^2 f)(z) &= \sum_x \sum_y f(x)\psi(xy)\psi(yz) \\
&= \sum_x f(x) \sum_y \psi(y(x+z)) \\
&= \sum_x f(x-z) \sum_y \psi(xy) \\
&= qf(-z)
\end{aligned}$$

Pour la dernière égalité, quand $x \neq 0$ alors la relation d'orthogonalité implique $\sum_y \psi(xy) = 0$ et quand $x = 0$ alors $\sum_y \psi(xy) = q$.

Proposition 2.10
Pour tout caractère χ non trivial et tout $y \in \mathbb{F}_q^\times$, $(\mathcal{F}\chi)(y) = g(\chi)\chi^{-1}(y)$.

En effet, $(\mathcal{F}\chi)(y) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(xy)$ et si l'on remplace x par ty^{-1} on obtient :

$$(\mathcal{F}\chi)(y) = \sum_{t \in \mathbb{F}_q} \chi(ty^{-1})\psi(t) = \chi(y^{-1})g(\chi)$$

Proposition 2.11
Pour tout caractère χ non trivial et tout $y \in \mathbb{F}_q^\times$, on a l'égalité, appelé développement de Fourier de χ en y :

$$\chi(y) = \frac{g(\chi)}{q}\,\overline{(\mathcal{F}\chi)(y)} = \frac{g(\chi)}{q} \sum_{t \in \mathbb{F}_q} \overline{\chi(t)\psi(ty)}.$$

En effet, d'après la section sur les sommes de Gauss on sait que $g(\chi)\overline{g(\chi)} = q$. Il suffit donc de montrer que $\overline{g(\chi)}\chi(y) = \overline{(\mathcal{F}\chi)(y)}$ ce qui évident d'après la proposition 2.10.

2.5 Somme de Jacobi

Pour prouver la loi de réciprocité quadratique, nous avons besoin de savoir multiplier deux sommes de Gauss. Pour cela, on introduit les sommes de Jacobi qui vont également être utiles pour la suite de l'article.

Soit χ_{α_1} et χ_{α_2} deux caractères multiplicatifs non triviaux de $\mathbb{F}_q$. Calculons $g(\chi_{\alpha_1})g(\chi_{\alpha_2})$:

$$\begin{aligned} g(\chi_{\alpha_1})g(\chi_{\alpha_2}) &= \left(\sum_{x\in\mathbb{F}_q}\chi_{\alpha_1}(x)\psi(x)\right)\left(\sum_{y\in\mathbb{F}_q}\chi_{\alpha_2}(y)\psi(y)\right) \\ &= \sum_{x,y\in\mathbb{F}_q}\chi_{\alpha_1}(x)\chi_{\alpha_2}(y)\psi(x+y) \\ &= \sum_{x,y\in\mathbb{F}_q}\chi_{\alpha_1}(x)\chi_{\alpha_2}(y-x)\psi(y) \\ &= \sum_{x\in\mathbb{F}_q,y\in\mathbb{F}_q^\times}\chi_{\alpha_1}(x)\chi_{\alpha_2}(y-x)\psi(y)+\sum_{x\in\mathbb{F}_q}\chi_{\alpha_1}(x)\chi_{\alpha_2}(-x). \end{aligned}$$

La seconde somme est égale à

$$\sum_{x\in\mathbb{F}_q}\chi_{\alpha_1}(x)\chi_{\alpha_2}(-x)=\chi_{\alpha_2}(-1)\sum_{x\in\mathbb{F}_q}\chi_{\alpha_1}(x)\chi_{\alpha_2}(x)=\chi_{\alpha_2}(-1)\sum_{x\in\mathbb{F}_q}(\chi_{\alpha_1}\chi_{\alpha_2})(x).$$

La relation d'orthogonalité entre les caractères implique que la seconde somme vaut 0 si $\chi_{\alpha_1}\chi_{\alpha_2}\neq 1$ et $q\chi_{\alpha_2}(-1)$ sinon (cette dernière expression est bien symétrique en α_1 et α_2).

Pour le calcul de la première somme, on remplace x par yt :

$$\begin{aligned} \sum_{x\in\mathbb{F}_q,y\in\mathbb{F}_q^\times}\chi_{\alpha_1}(x)\chi_{\alpha_2}(y-x)\psi(y) &= \sum_{t\in\mathbb{F}_q,y\in\mathbb{F}_q^\times}\chi_{\alpha_1}(yt)\chi_{\alpha_2}(y-yt)\psi(y) \\ &= \sum_{y\in\mathbb{F}_q^\times}(\chi_{\alpha_1}\chi_{\alpha_2})(y)\sum_{t\in\mathbb{F}_q}\chi_{\alpha_1}(t)\chi_{\alpha_2}(1-t). \end{aligned}$$

On est conduit à la définition suivante :

Définition 2.12
Soit $\chi_{\alpha_0},\chi_{\alpha_1},\ldots,\chi_{\alpha_r}$ des caractères. On appelle somme de Jacobi de $\chi_{\alpha_0},\chi_{\alpha_1},\ldots,\chi_{\alpha_r}$ et l'on note $J(\chi_{\alpha_0},\chi_{\alpha_1},\ldots,\chi_{\alpha_r})$ la convolée de $\chi_{\alpha_0},\chi_{\alpha_1},\ldots,\chi_{\alpha_r}$ évaluée en 1 :

$$J(\chi_{\alpha_0},\ldots,\chi_{\alpha_r})=(\chi_{\alpha_0}*\chi_{\alpha_1}*\cdots\chi_{\alpha_r})(1).$$

Proposition 2.13
Soit χ_{α_1} et χ_{α_2} deux caractères de $\mathbb{F}_q$ non triviaux et $\chi_{\alpha_1}\chi_{\alpha_2}\neq 1$, alors

$$g(\chi_{\alpha_1})g(\chi_{\alpha_2})=g(\chi_{\alpha_1}\chi_{\alpha_2})J(\chi_{\alpha_1},\chi_{\alpha_2}).$$

En effet, cela découle du calcul précédent de $g(\chi_{\alpha_1})g(\chi_{\alpha_2})$.

Proposition 2.14
Soit $\chi_{\alpha_1},\ldots,\chi_{\alpha_r}$ des caractères. La somme de Jacobi $J(\chi_{\alpha_1},\ldots,\chi_{\alpha_r})$ est de module $q^{\frac{r-1}{2}}$.

En effet, posons

$$\alpha_0=-\alpha_1-\cdots-\alpha_r \qquad \text{et} \qquad S(\alpha)=\sum_{\sum u_i=0}\chi_{\alpha_0}(u_0)\chi_{\alpha_1}(u_1)\cdots\chi_{\alpha_r}(u_r).$$

En utilisant le développement de Fourier de χ_{α_i} (Proposition 2.11), on a :

$$\begin{aligned} S(\alpha) &= \sum_{\sum u_i=0} \left(\frac{g(\chi_{\alpha_0})}{q} \sum_{t_0} \overline{\chi}(t_0)\overline{\psi}(t_0u_0) \right) \cdots \left(\frac{g(\chi_{\alpha_r})}{q} \sum_{t_r} \overline{\chi}(t_r)\overline{\psi}(t_ru_r) \right) \\ &= q^{-r-1} g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_r}) \sum_{t_0,\ldots,t_r} \overline{\chi}_{\alpha_0}(t_0) \cdots \overline{\chi}_{\alpha_r}(t_r) \sum_{\sum u_i=0} \overline{\psi}\Big(\sum_i t_i u_i \Big). \end{aligned}$$

Le groupe $\{u = (u_0, \ldots, u_r), \sum_i u_i = 0\}$ est un groupe d'ordre q^r sur lequel $u \to \overline{\psi}(\sum_i t_i u_i)$ est un caractère. La somme de toutes les valeurs de ce caractère sur ce groupe vaut q^r si le caractère est trivial et 0 sinon. C'est-à-dire q^r si les t_i sont égaux et 0 sinon. Ainsi :

$$S(\alpha) = \frac{1}{q} g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_r}) \sum_t \overline{\chi}_{\alpha_0}(t) \cdots \overline{\chi}_{\alpha_r}(t).$$

Les α_i vérifient $\sum_i \alpha_i \in \mathbb{Z}$ donc si $t \neq 0$ alors $\overline{\chi}_{\alpha_0}(t) \cdots \overline{\chi}_{\alpha_r}(t) = 1$, et si $t = 0$ le produit est nul. Finalement :

$$S(\alpha) = \frac{q-1}{q} g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_r}).$$

Donc $S(\alpha)\overline{S(\alpha)} = (q-1)^2 q^{r-1}$ et donc $S(\alpha)$ est de module $(q-1)q^{\frac{r-1}{2}}$.
Maintenant, on remarque si u_0 est nul alors le produit des $\chi_{\alpha_i}(u_i)$ est nul. Ainsi on peut faire le changement de variable $v_i = -\frac{u_i}{u_0}$. Ainsi :

$$\begin{aligned} S(\alpha) &= \sum_{u_0 \neq 0,\ v_1+\cdots+v_r=1} \chi_{\alpha_0}(u_0) \prod_{i=1}^{r} \chi_{\alpha_i}(-u_0 v_i) \\ &= \chi_{\alpha_1+\cdots+\alpha_r}(-1) \sum_{v_1+\cdots+v_r=1} \chi_{\alpha_1}(v_1) \cdots \chi_{\alpha_r}(v_r) \sum_{u_0 \neq 0} \chi_{\alpha_0+\cdots+\alpha_r}(u_0) \\ &= (q-1)\chi_{\alpha_1+\cdots+\alpha_r}(-1) J(\chi_{\alpha_1}, \ldots, \chi_{\alpha_r}). \end{aligned}$$

Ainsi $J(\chi_{\alpha_1}, \ldots, \chi_{\alpha_r})$ est de module $q^{\frac{r-1}{2}}$.

2.6 Analogie avec les fonctions Gamma et Beta en analyse complexe

Il est intéressant de remarquer quelques analogies avec les fonctions Gamma et Beta très utilisées en analyse complexe :

– En effet, on fait l'analogie entre la somme et l'intégrale, $\chi(t)$ et t^x, $\psi(t)$ et e^{-t}. La mesure $\frac{dt}{t}$ est invariante par translation tout comme l'ensemble sur lequel la somme porte.

$$G(\chi) = \sum_{t \in \mathbb{F}_q^\times} \chi(t)\psi(t) \qquad \leftrightarrow \qquad \Gamma(x) = \int_0^{+\infty} t^x e^{-t} \frac{dt}{t}.$$

– On reconnaît des deux côtés une convolution.

$$J(\chi, \chi') = \sum_{t \in \mathbb{F}_q^\times} \chi(t)\chi'(1-t) \qquad \leftrightarrow \qquad B(x, x') = \int_0^1 t^{x-1}(1-t)^{x'-1} dt.$$

– L'analogie est claire ici :

$$G(\chi)G(\chi') = G(\chi\chi')J(\chi, \chi') \qquad \leftrightarrow \qquad \Gamma(x)\Gamma(x') = \Gamma(x+x')B(x, x').$$

– Moins clair mais on peut tout de même y voir une analogie :

$$G(\chi)G(\chi^{-1}) = \chi(-1)q \qquad \leftrightarrow \qquad \Gamma(x)\Gamma(1-x) = \frac{\pi}{\sin(\pi x)}.$$

3 Extensions de corps finis

3.1 Corps finis, norme et trace

Soit $\nu \in \mathbb{N}^\times$, on considère l'extension de corps $\mathbb{F}_{q^\nu}/\mathbb{F}_q$ où q est une puissance d'un nombre premier.

Définition 3.1
La norme (resp. la trace) est l'application qui à tout $x \in \mathbb{F}_{q^\nu}$ associe le déterminant (resp. la trace) de l'application

$$m_x : \left\{ \begin{array}{ccc} \mathbb{F}_{q^\nu} & \to & \mathbb{F}_{q^\nu} \\ y & \mapsto & yx. \end{array} \right.$$

On note $N(.)$ (resp. $Tr(.)$) la norme (resp. la trace).

On rappelle qu'on a fixé w un générateur de $\mathbb{F}_q^\times$ fixé.

Proposition 3.2
Il existe un générateur z de $\mathbb{F}_{q^\nu}^\times$ tel que $N(z) = w$.

En effet, la norme de z est :

$$N(z) = z^{1+q+\ldots+q^{\nu-1}} = z^{\frac{q^\nu-1}{q-1}}.$$

La norme $N(z)$ est d'ordre $q-1$ donc il existe $\alpha \in \mathbb{N}$ premier avec $q-1$ tel que $w = N(z)^\alpha = N(z^\alpha)$. On vérifie facilement que le noyau de N est l'ensemble des $z^{\lambda(q-1)}$ où λ parcourt $\mathbb{Z}$. On cherche donc $\lambda \in \mathbb{Z}$ tel que $z^{\alpha+\lambda(q-1)}$ soit générateur de $\mathbb{F}_{q^\nu}^\times$, c'est-à-dire $\alpha+\lambda(q-1)$ est premier avec $q^\nu - 1$. On vérifie que

$$\lambda = \prod_{p \in \mathbb{P}, p | q^\nu - 1, p \nmid \alpha} p$$

convient.
En effet, si p est un diviseur premier de $\alpha + \lambda(q-1)$ et $q^\nu - 1$ alors :
– si p divise α c'est que p ne divise pas λ par construction et donc p divise $q-1$ ce qui est absurde car α est premier avec $q-1$.
– si p ne divise pas α, par construction p divise λ mais c'est impossible car alors p diviserait $(\alpha + \lambda(q-1)) - \lambda(q-1) = \alpha$.
Ainsi $\alpha + \lambda(q-1)$ est premier avec $q^\nu - 1$.

Proposition 3.3
La norme et la trace sont surjectives.

On vient de voir dans la proposition précédente qu'il existe un élément $z \in \mathbb{F}_q^\nu$ s'envoyant sur un générateur de $\mathbb{F}_q$. C'est donc que la norme est surjective.
Soient $\sigma_1, \ldots, \sigma_n$ les n $\mathbb{F}_q$-plongements. Supposons que pour tout $x \in \mathbb{F}_{q^\nu}, Tr(x) = 0$. Par definition de la trace,on obtiendrait

$$\sigma_1 + \ldots + \sigma_n = 0,$$

ce qui contredit le lemme d'independance lineaire de Dedekind. Donc, il existe $x_0 \in \mathbb{F}_{q^\nu}$ tel que $Tr(x_0) = \lambda_0 \neq 0$. Pour conclure quant a la surjectivité, il suffit de remarquer que pour tout $\lambda \in \mathbb{F}_q$, on a

$$\lambda = Tr(\frac{\lambda}{\lambda_0} x_0).$$

Proposition 3.4
Tout polynôme irréductible sur $\mathbb{F}_q$ se factorise sur $\mathbb{F}_{q^\nu}$ en produit de polynômes de même degré.

En effet, notons sa factorisation en produit de facteurs irréductibles sur $\mathbb{F}_{q^\nu}$:

$$P = P_1 \dots P_r.$$

On note :

$$G = \mathrm{Gal}(\mathbb{F}_{q^\nu}/\mathbb{F}_q) \quad \text{et} \quad \mathrm{Fix}_G(P_1) = \{\sigma \in G : \ {}^\sigma P_1 = P_1\}.$$

Soit Q définie par :

$$Q = \prod_{\overline{\sigma} \in G/\mathrm{Fix}_G(P_1)} {}^\sigma P_1,$$

où le produit porte sur un système de représentants de $G/\mathrm{Fix}_G(P_1)$.
Montrons alors que $Q = P$ en montrant qu'ils se divisent l'un l'autre.
D'une part, par construction, Q est le produit des polynômes qui sont dans l'orbite de P_1 sous G, donc Q est invariant par G et ainsi $Q \in \mathbb{F}_q[X]$. Comme P est le polyôme minimal d'une des racines de P_1 sur $\mathbb{F}_q$, et Q annule cette racine, on en déduit $P|Q$.
D'autre part, deux facteurs de Q sont premiers entre eux car irréductibles sur $\mathbb{F}_{q^\nu}$ et distincts. De plus, P_1 divise P donc pour tout $\sigma \in G$:

$${}^\sigma P_1 | {}^\sigma P = P,$$

si bien que le produit des ${}^\sigma P_1$ divise P : $Q|P$.
Ainsi $Q = P$ et P se factorise sur $\mathbb{F}_{q^\nu}$ en produit de polynômes de même degré.

3.2 Théorème de Hasse-Davenport

La preuve que nous donnons de ce théorème est celle que donne l'article de Weil.
Soit $\nu \in \mathbb{N}^\times$, on considère l'extension de corps $\mathbb{F}_{q^\nu}/\mathbb{F}_q$ où q est une puissance d'un nombre premier. D'après la proposition 3.2, il existe un générateur z de $\mathbb{F}_{q^\nu}^\times$ tel que $N(z) = w$. On définit alors χ'_α le caractère multiplicatif de $\mathbb{F}_{q^\nu}$ qui vérifie $\chi'_\alpha(z) = e^{2i\pi\alpha}$, α vérifiant $\alpha(q^\nu - 1) \equiv 0[1]$. Si α est tel que $\alpha(q-1) \equiv 0[1]$ alors pour tout $y \in \mathbb{F}_{q^\nu}, \chi'_\alpha(y) = \chi_\alpha[N(y)]$. De même, on définit ψ' le caractère additif de $\mathbb{F}_{q^\nu}$ vérifiant pour tout $y \in \mathbb{F}_{q^\nu}, \psi'(y) = \psi[T(y)]$. Ce caractère est non trivial car on sait d'après la proposition 3.3 que la trace envoie $\mathbb{F}_{q^\nu}$ sur $\mathbb{F}_q$. On définit maintenant $g'(\chi'_\alpha)$ la somme de Gauss sur $\mathbb{F}_{q^\nu}$:

$$g'(\chi'_\alpha) = \sum_{y \in \mathbb{F}_{q^\nu}} \chi'_\alpha(y)\psi'(y).$$

Nous allons démontrer le théorème suivant :

Théorème 3.5 (Hasse-Davenport)
Les sommes de Gauss $g'(\chi'_\alpha)$ et $g(\chi_\alpha)$ vérifient :

$$-g'(\chi'_\alpha) = [-g(\chi_\alpha)]^\nu.$$

Pour prouver ce théorème, on considère les polynômes unitaire de $\mathbb{F}_q[X]$:

$$F(X) = X^n + c_1 X^{n-1} + \dots + c_n,$$

où $n \in \mathbb{N}^\times$. On définit alors le nombre $\lambda(F)$:

$$\lambda(F) = \chi_\alpha(c_n)\psi(c_1).$$

Proposition 3.6
Soit deux polynômes unitaires de $\mathbb{F}_q[X]$: F_1 et F_2, on a la relation

$$\lambda(F_1F_2) = \lambda(F_1)\lambda(F_2).$$

En effet :

$$\begin{aligned} F_1F_2 &= (X^n + c_1X^{n-1} + \ldots + c_n)(X^m + d_1X^{m-1} + \ldots + d_m) \\ &= X^{n+m} + (d_1 + c_1)X^{n+m-1} + \ldots + c_nd_m. \end{aligned}$$

Donc $\lambda(F_1F_2) = \chi_\alpha(c_nd_m)\psi(c_1 + d_1) = \chi_\alpha(c_n)\chi_\alpha(d_m)\psi(c_1)\psi(d_1) = \lambda(F_1)\lambda(F_2)$.

Proposition 3.7
Pour tout polynôme F de $\mathbb{F}_q[X]$, on note $n(F)$ le degré du polynôme F et U une indéterminée, alors on a l'identité formelle :

$$1 + \sum_F \lambda(F)U^{n(F)} = \prod_P [1 - \lambda(P)U^{n(P)}]^{-1},$$

où la somme porte sur tous les polynômes F unitaires de $\mathbb{F}_q[X]$ et le produit porte sur tous les polynômes P irréductibles unitaires de $\mathbb{F}_q[X]$.

Cette identité provient du fait que chaque polynôme F s'exprime comme un unique produit de polynômes irréductibles et λ est complètement multiplicatif.
En fait, on peut nettement améliorer la proposition précédente, en effet :

Proposition 3.8
La somme $\sum_F \lambda(F)U^{n(F)}$ ne contient qu'un seul terme :

$$1 + g(\chi_\alpha)U = \prod_P [1 - \lambda(P)U^{n(P)}]^{-1}.$$

On remarque que les $F \in \mathbb{F}_q[X]$ unitaires de degré 1 sont les polynômes $X + c$ où c parcourt $\mathbb{F}_q$. Ainsi :

$$\sum_{F,\ n(F)=1} \lambda(F)U^{n(F)} = \sum_{c \in \mathbb{F}_q} \chi_\alpha(c)\psi(c)U = g(\chi_\alpha)U.$$

Pour les polynômes F de degré $n \geq 2$, F est de la forme $X^n + c_1X^{n-1} + \ldots + c_n$ donc :

$$\begin{aligned} \sum_{F, n(F)=n} \lambda(F)U^{n(F)} &= \sum_{(c_1,\ldots,c_n) \in \mathbb{F}_q^n} \chi_\alpha(c_n)\psi(c_1)U^n \\ &= q^{n-2} \sum_{(c_1,c_n) \in \mathbb{F}_q^2} \chi_\alpha(c_n)\psi(c_1)U^n \\ &= q^{n-2} \sum_{c_n \in \mathbb{F}_q} \chi_\alpha(c_n) \sum_{c_1 \in \mathbb{F}_q} \psi(c_1)U^n \\ &= 0. \end{aligned}$$

La dernière égalité provient des relations d'orthogonalité.

De même, si $F'(X) = X^n + d_1X^{n-1} + \cdots + d_n$ est un polynôme sur $\mathbb{F}_{q^\nu}$, on pose :

$$\lambda'(F') = \chi'_\alpha(d_n)\psi'(d_1).$$

On obtient de même, en prenant une autre indéterminée, l'identité formelle :

$$1 + g'(\chi'_\alpha)U' = \prod_{P'} [1 - \lambda'(P')U'^{n(P')}]^{-1},$$

où le produit porte sur tout les polynômes unitaires irréductibles de $\mathbb{F}_{q^\nu}$.

Proposition 3.9
Soit P un polynôme unitaire irréductible sur $\mathbb{F}_q$ de degré n, P' un des facteurs irréductibles de P sur $\mathbb{F}_{q^\nu}$ et $d = (n, \nu)$. Alors :

$$\lambda'(P') = \lambda(P)^{\nu/d}.$$

En effet, soit P un polynôme unitaire irréductible sur $\mathbb{F}_q$ de degré n, P' un des facteurs irréductibles de P sur $\mathbb{F}_{q^\nu}$ de degré n' et $d = (n, \nu)$. Soit $-\xi$ une racine de P'. Alors $\mathbb{F}_q(\xi)/\mathbb{F}_q$ est une extension de degré n et $\mathbb{F}_{q^\nu}(\xi)/\mathbb{F}_{q^\nu}$ est une extension de degré n'.
L'extension $\mathbb{F}_{q^\nu}(\xi)/\mathbb{F}_q$ est de degré $n\nu/d$ le ppcm de n et ν car $\mathbb{F}_{q^\nu}(\xi)$ est le compositum de $\mathbb{F}_{q^\nu}$ et $\mathbb{F}_q(\xi)$ qui sont respectivement de degré ν et n sur $\mathbb{F}_q$. De plus, l'extension $\mathbb{F}_{q^\nu}(\xi)/\mathbb{F}_q$ est de degré $n'\nu$ car $[\mathbb{F}_{q^\nu}(\xi) : \mathbb{F}_q] = [\mathbb{F}_{q^\nu}(\xi) : \mathbb{F}_{q^\nu}].[\mathbb{F}_{q^\nu} : \mathbb{F}_q] = n'.\nu$.
Ainsi $n' = n/d$ et P possède d facteurs irréductibles sur $\mathbb{F}_{q^\nu}$ tout de degré n/d. De plus, si $a = N_{\mathbb{F}_q(\xi)/\mathbb{F}_q}(\xi)$ et $b = T_{\mathbb{F}_q(\xi)/\mathbb{F}_q}(\xi)$ sont respectivement la norme et la trace de ξ relatives à l'extension $\mathbb{F}_q(\xi)/\mathbb{F}_q$ alors :

$$P(X) = X^n + bX^{n-1} + \cdots + a.$$

Ainsi :

$$\lambda(P) = \chi_\alpha(a)\psi(b).$$

De même, si $a' = N_{\mathbb{F}_{q^\nu}(\xi)/\mathbb{F}_{q^\nu}}(\xi)$ et $b' = T_{\mathbb{F}_{q^\nu}(\xi)/\mathbb{F}_{q^\nu}}(\xi)$ sont la norme et la trace de ξ relatives à l'extension $\mathbb{F}_{q^\nu}(\xi)/\mathbb{F}_{q^\nu}$ alors :

$$\lambda'(P') = \chi'_\alpha(a')\psi'(b') = \chi_\alpha(N_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(a'))\psi(T_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(b')).$$

On a :

$$\begin{aligned} N_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(a') &= N_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(N_{\mathbb{F}_{q^\nu}(\xi)/\mathbb{F}_{q^\nu}}(\xi)) \\ &= N_{\mathbb{F}_{q^\nu}(\xi)/\mathbb{F}_q}(\xi) \\ &= N_{\mathbb{F}_q(\xi)/\mathbb{F}_q}(N_{\mathbb{F}_{q^\nu}(\xi)/\mathbb{F}_q(\xi)}(\xi)) \\ &= N_{\mathbb{F}_q(\xi)/\mathbb{F}_q}(\xi^{\nu/d}) \\ &= a^{\nu/d}. \end{aligned}$$

Et, de même, $T_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(b') = (\nu/d)b$.
Ainsi :

$$\lambda'(P') = \lambda(P)^{\nu/d}.$$

La proposition est démontrée et on peut maintenant terminer la démonstration du théorème de Hasse-Davenport :
On sait que :

$$1 + g'(\chi'_\alpha)U' = \prod_P{}' [1 - \lambda'(P')U'^{n(P')}]^{-1}.$$

En réunissant les facteurs irréductibles de P sur $\mathbb{F}_{q^\nu}$ et en remplaçant U' par U^ν, on a :

$$1 + g'(\chi'_\alpha)U^\nu = \prod_P \prod_{P', P'|P} [1 - \lambda'(P')(U^\nu)^{n'}]^{-1}.$$

En utilisant la proposition précédente, si $P'|P$ et $P''|P$ alors $\lambda'(P') = \lambda'(P'') = \lambda(P)^{\nu/d}$ et $n' = n''$ donc $[1 - \lambda'(P')(U^\nu)^{n'}]^{-1} = [1 - \lambda'(P'')(U^\nu)^{n''}]^{-1} = [1 - \lambda(P)^{\nu/d}U^{\nu n/d}]^{-1}$. Ainsi :

$$1 + g'(\chi'_\alpha)U^\nu = \prod_P [1 - \lambda(P)^{\nu/d}U^{\nu n/d}]^{-d}.$$

Soit ζ une racine primitive νième de l'unité, alors :

$$\prod_{i=0}^{\nu-1} (1 - \lambda(P)(\zeta^i U)^n) = (1 - \lambda(P)^{\nu/d}U^{n\nu/d})^d.$$

En effet, il faut prouver $\prod_{i=0}^{\nu-1}(1-X\zeta^{in}) = (1-X^{\nu/d})^d$. Il suffit de regarder les racines de ces deux polynômes. Soit x_0 une racine fixé de $X^{\nu/d}-1=0$, il y a exactement d valeurs de i tels que $\zeta^{in}=x_0$. En effet, d est le pgcd n et ν et x_0 est de la forme ζ^{dk}. Ainsi :

$$\begin{aligned}
1+g'(\chi'_\alpha)U^\nu &= \prod_P\prod_{i=0}^{\nu-1}(1-\lambda(P)(\zeta^iU)^n)^{-1} \\
&= \prod_{i=0}^{\nu-1}\prod_P(1-\lambda(P)(\zeta^iU)^n)^{-1} \\
&= \prod_{i=0}^{\nu-1}(1+g(\chi_\alpha)\zeta^iU) \\
&= 1+(-1)^{\nu+1}g(\chi_\alpha)^\nu U^\nu.
\end{aligned}$$

Le théorème est démontré.

4 Nombre de points dans les variétés diagonales affines

Soit $r\in\mathbb{N}^*, n_0,\ldots,n_r\in\mathbb{N}^*, a_0,\ldots,a_r\in\mathbb{F}_q^\times$ et on cherche à compter le nombre de solutions des équations du type :

$$a_0x_0^{n_0}+\ldots+a_rx_r^{n_r}=b,$$

où les x_i sont dans le corps fini $\mathbb{F}_q$. On suppose les a_i tous non nuls. On note N le nombre de solutions de l'équation.

4.1 Premier cas : une inconnue

Soit n un entier fixé, on pose $d=(n,q-1)$ le pgcd de n et $q-1$. On étudie le nombre de solutions de l'équation $x^n=u$ en fonction de u.

Proposition 4.1
On a :

$$\#\{x:x^n=u\}=\begin{cases}1 & \text{si } u=0,\\ d & \text{si } u\neq 0 \text{ et } u \text{ est une puissance dième},\\ 0 & \text{si } u\neq 0 \text{ et } u \text{ n'est pas une puissance dième.}\end{cases}$$

Preuve
– Si u est nul, il est clair qu'il n'y a qu'une solution.
– Si u est non nul et u est une puissance $d-ième$ alors $\#\{x:x^n=u\}=d$. En effet, soit $f:\mathbb{F}_q^\times\to\mathbb{F}_q^\times, u\mapsto u^n$ et $g:\mathbb{F}_q^\times\to\mathbb{F}_q^\times, u\mapsto u^d$. Démontrons que $\mathrm{Im}(f)=\mathrm{Im}(g)$. Comme d divise n, on a $\mathrm{Im}(f)\subset\mathrm{Im}(g)$. On rappelle que w est un générateur de $\mathbb{F}_q^\times$ alors

$$\mathrm{Im}(f)=\{(w^k)^n,k\in\mathbb{Z}\}=\{(w^n)^k,k\in\mathbb{Z}\}=\ \langle w^n\rangle.$$

Ainsi $\mathrm{Im}(f)$ a pour cardinal l'ordre de w^n c'est à dire $(q-1)/d$. De même, $\mathrm{Im}(g)$ a pour cardinal l'ordre de w^d c'est à dire $(q-1)/d$. Ainsi $\mathrm{Im}(f)=\mathrm{Im}(g)$.
Il y a donc exactement autant de racines $d$ième que de racines $n$ièmes. On sait qu'il y a moins de d racines $d$ièmes car le polynôme X^d-u ne peut avoir plus de d racines. Il possède une racine x par hypothèse, et on peut trouver toutes les autres racines en multipliant x par les racines $d$ièmes de l'unité. Ainsi $\#\{x:x^n=u\}=d$.

– Si u est non nul et n'est pas une puissance $d$ième alors il n'y a aucune solution. En effet, par contraposée, si x était une solution alors on a $x^n = u$ c'est-à-dire $\left(x^{n/d}\right)^d = u$.

Proposition 4.2
On peut calculer $\#\{x : x^n = u\}$ à l'aide des sommes de Gauss :

$$\#\{x : x^n = u\} = \sum_{\alpha} \chi_\alpha(u),$$

où la somme porte sur les α vérifiant $\alpha d \equiv 0[1]$ et $0 \leqslant \alpha < 1$.

En effet, si $u = 0$ alors la somme vaut 1 car $\chi_0(0) = 1$. Sinon, on peut écrire $u = w^l$ pour un certain $l \in \mathbb{N}$ donc :

$$\sum_{\alpha} \chi_\alpha(u) = \sum_{j=0}^{d-1} e^{2i\pi.lj/d}.$$

Si u est une puissance $d$ième alors $\frac{lj}{d}$ est entier donc la somme vaut d.
Si u n'est pas une puissance $d$ième alors la somme est nulle (c'est la somme de toutes les racines $d$ièmes de l'unité).

4.2 Le cas-clé : r inconnues et second membre nul

On cherche ici à résoudre l'équation $a_0 x_0^{n_0} + \ldots + a_r x_r^{n_r} = 0$ où les x_i sont dans le corps fini $\mathbb{F}_q$. La première étape consiste à partitionner l'ensemble solution S. Le nombre de solutions final sera la somme du nombre de solutions sur les ensembles de la partition.
On note par la suite $N_i(u)$ le nombre de solutions de l'équation $x^{n_i} = u$ et N le nombre de solutions de $a_0 x_0^{n_0} + \ldots + a_r x_r^{n_r} = 0$.

4.2.1 Partition de l'ensemble solution

On note $L : \mathbb{F}_q^{r+1} \to \mathbb{F}_q$ la forme linéaire définie par

$$\forall u = (u_0, \ldots, u_r) \in {\mathbb{F}_q}^{r+1}, \quad L(u) = \sum_{i=0}^{r} a_i u_i.$$

On définit p et f par :

$$\begin{array}{rccc} p : & \mathbb{F}_q^{r+1} & \to & \mathbb{F}_q^{r+1} \\ & (x_i)_{i=0,\ldots,r} & \mapsto & (x_i^{n_i})_{i=0,\ldots,r} \end{array} \qquad f = L \circ p.$$

Alors $f((x_i)_i) = 0$ si et seulement si $u = p((x_i)_i) \in L^{-1}(0)$. Ainsi :

$$N = \operatorname{card}(f^{-1}(0)) = \sum_{u \in L^{-1}(0)} \operatorname{card}(p^{-1}(u)) = \sum_{u \in \operatorname{Ker} L} N_0(u_0) \cdots N_r(u_r).$$

Et donc on a la

Proposition 4.3
Soit N le nombre de solutions de l'équation $\sum_{i=0}^{r} a_i x_i^{n_i} = 0$, alors :

$$N = \sum_{u \in L^{-1}(0)} N_0(u_0) \cdots N_r(u_r),$$

la somme portant sur les $u \in {\mathbb{F}_q}^{r+1}$ appartenant au sous-espace vectoriel $\operatorname{Ker} L = L^{-1}(0)$ de dimension r (L est une forme linéaire non nulle).

4.2.2 Utilisation des sommes de Gauss

En utilisant les propositions 4.2 et 4.3, on obtient la

Proposition 4.4
On peut calculer N à l'aide des sommes de Gauss :

$$N = \sum_{u \in L^{-1}(0)} \sum_{\alpha \in X} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r),$$

où l'on a noté α le multi-indice $(\alpha_0, \ldots, \alpha_r) \in [0;1[^{r+1}$ et X est l'ensemble des α qui vérifient $\alpha_0 d_0 \equiv 0[1], \ldots, \alpha_r d_r \equiv 0[1]$.

Pour u quelconque et $\alpha = (0, \ldots, 0)$ on a :

$$\prod_{j=0}^{r} \chi_{\alpha_j}(u_j) = \prod_{j=0}^{r} \chi_0(u_j) = \prod_{j=0}^{r} 1 = 1.$$

Ainsi :

$$\begin{aligned} N &= \sum_{u \in \operatorname{Ker} L} 1 + \sum_{u \in L^{-1}(0)} \sum_{\alpha \in X \setminus \{(0,\ldots,0)\}} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r) \\ &= q^r + \sum_{\alpha \in X \setminus \{(0,\ldots,0)\}} \sum_{u \in L^{-1}(0)} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r). \end{aligned}$$

Le multi-indice $(0, \ldots, 0)$ fait donc apparaître un q^r. Parmi les autres multi-indices beaucoup ne contribuent pas. En effet, on a le lemme suivant :

Lemme 4.5
Soit $\alpha \in X \setminus \{0, \ldots, 0\}$ tel que $\alpha_j = 0$ pour un certain $j \in \{0, \ldots, r\}$. Alors

$$\sum_{u \in L^{-1}(0)} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r) = 0.$$

Quitte à permuter les indices, on suppose qu'il existe $s \in \{1, \ldots, r\}$ tel que $\alpha_s = \ldots = \alpha_r = 0$ et les $\alpha_0, \ldots, \alpha_{s-1}$ sont non nuls. On a :

$$\begin{aligned} A &= \sum_{u \in L^{-1}(0)} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r) \\ &= \sum_{u \in L^{-1}(0)} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_{s-1}}(u_{s-1}) \times 1 \times \cdots \times 1 \\ &= \sum_{(u_s,\ldots,u_r) \in \mathbb{F}_q^{r-s+1}} \sum_{(u_0,\ldots,u_{s-1}) \in \mathbb{F}_q^s} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_{s-1}}(u_{s-1}) \\ &= q^{r-s+1} \sum_{(u_0,\ldots,u_{s-1}) \in \mathbb{F}_q^s} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_{s-1}}(u_{s-1}) \\ &= q^{r-s+1} \prod_{i=0}^{s-1} \sum_{u_i \in \mathbb{F}_q} \chi_{\alpha_i}(u_i) \end{aligned}$$

Or, comme $\alpha_0, \ldots, \alpha_{s-1}$ sont tous non nuls, chacun des facteurs, à savoir chaque somme $\sum_{u_i \in \mathbb{F}_q} \chi_{\alpha_i}(u_i)$, est nul (on reconnait la relation d'orthogonalité avec le caractère trivial) . Finalement, A est nul et le lemme est démontré.

Proposition 4.6
On a :

$$N = q^r + \sum_{u,\alpha} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r),$$

où u parcourt $L^{-1}(0)$ et les $\alpha = (\alpha_0, \ldots, \alpha_r)$ vérifient $\alpha_i d_i \equiv 0[1]$ et $\alpha_i \notin \mathbb{Z}$ (ce qui revient à dire que χ_{α_i} n'est pas le caractère trivial).

4.2.3 Changement de variable et apparition des sommes de Jacobi

On va maintenant faire apparaître les a_i pour sommer sur un ensemble plus simple à l'aide d'un changement de variable. Puis, après quelques calculs, nous reconnaitrons une somme de Jacobi et des propriétés en découleront.

Comme les caractères sont des morphismes, pour tout $i \in \{0, \ldots, r\}$ et $u_i \in \mathbb{F}_q$, on a $\chi_{\alpha_i}(u_i) = \chi_{\alpha_i}(a_i^{-1})\chi_{\alpha_i}(a_i u_i)$ (les a_i sont non nuls par hypothèse) et donc :

$$N = q^r + \sum_{u,\alpha} \Big(\chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1})\Big)\Big(\chi_{\alpha_0}(a_0 u_0) \cdots \chi_{\alpha_r}(a_r u_r)\Big).$$

Comme le premier facteur dans chaque terme de la somme ne dépend pas de u on peut écrire :

$$N = q^r + \sum_{\alpha} \left[\Big(\chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1})\Big) \sum_{u} \Big(\chi_{\alpha_0}(a_0 u_0) \cdots \chi_{\alpha_r}(a_r u_r)\Big)\right].$$

La somme porte sur les u appartenant à $\operatorname{Ker} L$, c'est à dire les u qui vérifient $\sum_{i=0}^{r} a_i u_i = 0$. Si on fait le changement de variable $u'_i = a_i u_i$ alors :

$$N = q^r + \sum_{\alpha} \left[\Big(\chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1})\Big) \sum_{u'_0 + \ldots + u'_r = 0} \Big(\chi_{\alpha_0}(u'_0) \cdots \chi_{\alpha_r}(u'_r)\Big)\right].$$

Abandonnons les ' et notons, pour $\alpha = (\alpha_0, \ldots, \alpha_r)$ un $(r+1)$-uple de caractères non triviaux :

$$S(\alpha) = \sum_{u_0 + \ldots + u_r = 0} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r).$$

Dans $S(\alpha)$, si $u_0 = 0$ alors le produit des $\chi_{\alpha_i}(u_i)$ est nul donc on peut se restreindre à prendre la somme sur les u tel que $u_0 + \ldots + u_r = 0$ et $u_0 \neq 0$. Ainsi on peut poser $v_i = \dfrac{u_i}{u_0} (1 \leqslant i \leqslant r)$. On a :

$$\begin{aligned} S(\alpha) &= \sum_{u_0 \neq 0, 1 + v_1 + \ldots + v_r = 0} \chi_{\alpha_0}(u_0) \cdot \chi_{\alpha_1}(u_0)\chi_{\alpha_1}(v_1) \cdots \chi_{\alpha_r}(u_0)\chi_{\alpha_r}(v_r) \\ &= \sum_{1 + v_1 + \ldots + v_r = 0} \chi_{\alpha_1}(v_1) \cdots \chi_{\alpha_r}(v_r) \sum_{u_0 \neq 0} \chi_{\beta}(u_0), \end{aligned}$$

où $\beta = \alpha_0 + \ldots + \alpha_r$. Si β est entier alors χ_β est trivial et la somme sur les $u_0 \neq 0$ des $\chi_\beta(u_0)$ est égale à $q - 1$. Si β n'est pas entier alors cette somme est nulle.

4.2.4 Somme de Jacobi

Dans l'article, André Weil appelle somme de Jacobi pour le corps $\mathbb{F}_q$ le complexe $j(\alpha)$ défini par $j(\alpha) = S(\alpha)/(q-1)$. On a :

$$j(\alpha) = \sum_{1 + v_1 + \ldots + v_r = 0} \chi_{\alpha_1}(v_1) \cdots \chi_{\alpha_r}(v_r).$$

$j(\alpha)$ est en fait presque une somme de Jacobi comme on l'a définit plus tôt :

$$j(\alpha) = \chi_{\alpha_1+\cdots+\alpha_r}(-1)J(\chi_{\alpha_1},\ldots,\chi_{\alpha_r}).$$

On obtient l'expression pour N :

$$\begin{aligned} N &= q^r + \sum_{\alpha} \chi_{\alpha_0}(a_0^{-1})\cdots\chi_{\alpha_r}(a_r^{-1})S(\alpha) \\ &= q^r + (q-1)\sum_{\alpha} \chi_{\alpha_0}(a_0^{-1})\cdots\chi_{\alpha_r}(a_r^{-1})j(\alpha), \end{aligned}$$

où la somme porte sur les α vérifiant $d_i\alpha_i \in \mathbb{Z}$ et $0 < \alpha_i < 1$ pour tout i et la nouvelle condition $\sum_{i=0}^{r} \alpha_i \in \mathbb{Z}$.

4.2.5 Estimation de N

On sait que :

$$N - q^r = (q-1)\sum_{\alpha} \chi_{\alpha_0}(a_0^{-1})\cdots\chi_{\alpha_r}(a_r^{-1})j(\alpha),$$

on obtient ainsi l'encadrement pour N :

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

où M est le nombre de $(r+1)$-uplets $(\alpha_0,\ldots,\alpha_r)$ vérifiant

$$\forall i \in \{0,\ldots,r\} : 0 < \alpha_i < 1, d_i\alpha_i \in \mathbb{Z},\ \sum_i \alpha_i \in \mathbb{Z}.$$

L'entier M dépend uniquement des d_i. On obtient un encadrement pour N qui ne dépend pas des coefficients a_i de l'équation.

4.3 Le cas r inconnues et second membre non nul

On peut maintenant calculer N_1 le nombre de solutions de l'équation

$$\sum_{i=0}^{r} a_i x_i^{n_i} + 1 = 0.$$

En effet, si N est le nombre de solutions de l'équation $\sum_{i=0}^{r} a_i x_i^{n_i} = 0$ et N' le nombre de solutions de l'équation $\sum_{i=0}^{r} a_i x_i^{n_i} + x_{r+1}^{q-1} = 0$ alors, comme x_{r+1}^{q-1} vaut 1 sauf en 0, on a :

$$N' = (q-1)N_1 + N.$$

On peut obtenir une expression plus explicite de N_1 en prolongeant j :

Soit $\alpha = (\alpha_1,\ldots,\alpha_s,\alpha_{s+1},\ldots,\alpha_{s'})$ tel que :
– $\forall i \in \{0,\ldots,s'\} : d_i\alpha_i \in \mathbb{Z}, \sum_i \alpha_i \in \mathbb{Z}$.

– $\forall i \in \{0,\dots,s\}, 0 < \alpha_i < 1$.
– $\forall i \in \{s+1,\dots,s'\}, \alpha_i = 0$.
Alors on prolonge j en α par :

$$j(\alpha_0,\dots,\alpha_{s'}) = (-1)^{s'-s} j(\alpha_0,\dots,\alpha_s).$$

On sait que :

$$N = q^r + (q-1) \sum_{\alpha=(\alpha_0,\dots,\alpha_r)} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) j(\alpha)$$

et

$$N' = q^{r+1} + (q-1) \sum_{\alpha=(\alpha_0,\dots,\alpha_{r+1})} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) \chi_{\alpha_{r+1}}(1) j(\alpha)$$

Ainsi :

$$\begin{aligned} N_1 &= \frac{N'-N}{q-1} \\ &= \frac{1}{q-1}\Bigg[q^{r+1} - (q-1) \sum_{\alpha=(\alpha_0,\dots,\alpha_{r+1})} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) \chi_{\alpha_{r+1}}(1) j(\alpha) \\ &\quad -q^r + (q-1) \sum_{\alpha=(\alpha_0,\dots,\alpha_r)} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) j(\alpha)\Bigg] \\ &= q^r + \sum_{\alpha} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) j\Big(\alpha_0,\dots,\alpha_r, -\sum_{i=0}^{r} \alpha_i\Big). \end{aligned}$$

La dernière somme porte sur les $\alpha = (\alpha_0,\dots,\alpha_{r+1})$ où $\forall i \in \{0,\dots,r+1\}, d_i\alpha_i \in \mathbb{Z}, \sum_i \alpha_i \in \mathbb{Z}$ et $\forall i \in \{0,\dots,r\}, 0 < \alpha_i < 1$ et α_{r+1} peut être nul.
Comme α est à $r+2$ composantes, le module de $j(\alpha)$ est plus grand : $j(\alpha)\overline{j}(\alpha) = q^r$. On obtient alors l'encadrement pour N_1 :

$$|N_1 - q^r| \leqslant M_1 q^{r/2},$$

où M_1 est donné par

$$M_1 = (d_0-1)\cdots(d_r-1) < n_0 \cdots n_r.$$

5 Fonction Zéta des variétés diagonales homogènes projectives

Soit N_ν le nombre de solutions dans $\mathbb{F}_{q^\nu}$ d'une équation de type $\sum_{i=0}^{r} a_i x_i^{n_i} = b$ où les a_i et b sont dans $\mathbb{F}_q$. La série formelle génératrice des N_ν : $\sum_{\nu=1}^{+\infty} N_\nu U^\nu$ est le développement en série d'une fraction rationelle bien particulière. C'est ce que nous allons étudier en considèrant l'équation homogène :

$$a_0 x_0^n + \cdots + a_r x_r^n = 0,$$

consideré comme l'équation d'une variété (sans points singuliers) dans l'espace projectif $\mathbb{P}^r$ de dimension r sur $\mathbb{F}_q$. Le nombre $\overline{N}$ de points rationnels sur $\mathbb{F}_q$ de cette variété est lié au nombre N de solutions de la même équation dans l'espace affine par la relation : $N = 1 + (q-1)\overline{N}$. En effet, N compte le point 0 et le nombre d'antécédents pour chaque point dans le projectif $(q-1)$ multiplié par le nombre de solutions dans l'espace projectif $(\overline{N})$. Ainsi, en posant $d = (n, q-1)$,

d'après les résultats précédents :

$$\begin{aligned}\overline{N} &= \frac{N-1}{q-1} \\ &= \frac{q^r-1}{q-1} + \sum_{\alpha} \overline{\chi}_{\alpha_0}(a_0)\cdots\overline{\chi}_{\alpha_r}(a_r)\cdot j(\alpha).\end{aligned}$$

La somme porte sur les α vérifiant : $\forall i, d\alpha_i \in \mathbb{Z}$ et $\alpha_i \notin \mathbb{Z}, \sum_i \alpha_i \in \mathbb{Z}$.

Calculons la série

$$\sum_{\nu\geq 1} \overline{N_\nu} U^{\nu-1}.$$

Pour tout $\nu \in \mathbb{N}^*$, on a :

$$\overline{N_\nu} = \frac{(q^\nu)^r-1}{q^\nu-1} + \sum_{\alpha\in\mathcal{A}_\nu} \overline{\chi_{\alpha_0}^{(\nu)}}(a_0)\cdots\overline{\chi_{\alpha_r}^{(\nu)}}(a_r)\cdot j^{(\nu)}(\alpha).$$

L'ensemble $\mathcal{A}_\nu$ est l'ensemble :

$$\mathcal{A}_\nu = \{(\alpha_0,\ldots,\alpha_r) \in]0;1[^{r+1} \text{ tels que pour tout i } :(n, q^\nu-1).\alpha_i \in \mathbb{Z}, \sum_{i=0}^{r} \alpha_i \in \mathbb{Z}\}.$$

L'exposant $^{(\nu)}$ signifie que l'on considère un caractère ou une somme de Jacobi dans l'extension $\mathbb{F}_{q^\nu}$.
Ainsi :

$$\sum_{\nu\geq 1} \overline{N_\nu} U^{\nu-1} = \sum_{\nu\geq 1} \frac{(q^\nu)^r-1}{q^\nu-1} U^{\nu-1} + \sum_{\nu\geq 1}\sum_{\alpha\in\mathcal{A}_\nu} \overline{\chi_{\alpha_0}^{(\nu)}}(a_0)\cdots\overline{\chi_{\alpha_r}^{(\nu)}}(a_r)\cdot j^{(\nu)}(\alpha)U^{\nu-1}.$$

On peut écrire la première somme en termes de dérivées logarithmiques :

$$\begin{aligned}\sum_{\nu\geq 1} \frac{(q^\nu)^r-1}{q^\nu-1} U^{\nu-1} &= \sum_{\nu\geq 1}\sum_{h=0}^{r-1} q^{\nu h} U^{\nu-1} \\ &= \sum_{h=0}^{r-1}\sum_{\nu\geq 1} q^{\nu h} U^{\nu-1} \\ &= \sum_{h=0}^{r-1} \frac{q^h}{1-q^hU} \\ &= \sum_{h=0}^{r-1} -\frac{d}{du}\log(1-q^hU).\end{aligned}$$

Nous allons faire la même chose pour la seconde somme.

On sait d'après le théorème de Hasse-Davenport que $g^{(\nu)}(\chi^{(\nu)}) = (-1)^{\nu-1} g(\chi)^\nu$ et, de plus, $j(\alpha) = \frac{1}{q} g(\chi_{\alpha_0})\cdots g(\chi_{\alpha_r})$ donc $j^{(\nu)}(\alpha) = (-1)^{(\nu-1)(r-1)} j(\alpha)^\nu$.
Notons :

$$R(\alpha,\nu) = \overline{\chi_{\alpha_0}^{(\nu)}}(a_0)\cdots\overline{\chi_{\alpha_r}^{(\nu)}}(a_r)\cdot j^{(\nu)}(\alpha), \qquad \alpha \in \mathcal{A}_\nu.$$

On a ainsi :

$$\sum_{\nu\geq 1}\overline{N_\nu}U^{\nu-1}=-\sum_{h=0}^{r-1}\frac{d}{du}\log(1-q^hU)+\sum_{\nu\geq 1}\sum_{\alpha\in\mathcal{A}_\nu}R(\alpha,\nu)U^{\nu-1}.$$

Remarquons que, pour tout $\nu\in\mathbb{N}^*$, $\mathcal{A}_\nu$ est inclus dans l'ensemble

$$\mathcal{A}=\{(\alpha_0,\ldots,\alpha_r)\in]0;1[^{r+1}\text{ tels que pour tout i }:n.\alpha_i\in\mathbb{Z},\sum_{i=0}^{r}\alpha_i\in\mathbb{Z}\}.$$

Ainsi, en permutant les sommes, on a :

$$\sum_{\nu\geq 1}\overline{N_\nu}U^{\nu-1}=-\sum_{h=0}^{r-1}\frac{d}{du}\log(1-q^hU)+\sum_{\alpha\in\mathcal{A}}\sum_{\nu\geq 1}R(\alpha,\nu)U^{\nu-1}.$$

Nous allons permuter les deux sommes à l'aide de la proposition suivante.

Proposition 5.1
Pour tout $\alpha\in\mathcal{A}$, il existe un entier $\mu(\alpha)$ tel que l'ensemble des ν tels que $\alpha\in\mathcal{A}_\nu$ est exactement l'ensemble des multiples de $\mu(\alpha)$.

Soit $\alpha\in\mathcal{A}$ et β le ppcm des dénominateurs des α_i. La proposition $(n,q^\nu-1).\alpha_i\in\mathbb{Z}$ pour tout $i\in\{0,\ldots,r\}$ est équivalente à : $q^\nu\equiv 1(\beta)$. Ainsi la constante $\mu(\alpha)$ est simplement l'ordre de q modulo β. Ainsi :

$$\sum_{\nu\geq 1}\overline{N_\nu}U^{\nu-1}=-\sum_{h=0}^{r-1}\frac{d}{du}\log(1-q^hU)+\sum_{\alpha\in\mathcal{A}}\sum_{\nu\geq 1}R(\alpha,\mu(\alpha)\nu)U^{\mu(\alpha)\nu-1}.$$

Calculons $R(\alpha,\mu(\alpha)\nu)$:

$$\begin{aligned}
R(\alpha,\mu(\alpha)\nu) &= \overline{\chi_{\alpha_0}^{(\mu(\alpha)\nu)}}(a_0)\cdots\overline{\chi_{\alpha_r}^{(\mu(\alpha)\nu)}}(a_r)\cdot j^{(\mu(\alpha)\nu)}(\alpha)\\
&= \overline{\chi_{\alpha_0}}(a_0)^{\mu(\alpha)\nu}\cdots\overline{\chi_{\alpha_r}}(a_r)^{\mu(\alpha)\nu}\cdot j(\alpha)^{\mu(\alpha)\nu}(-1)^{(\nu\mu(\alpha)-1)(r-1)}\\
&= \left(\overline{\chi_{\alpha_0}}(a_0)^{\mu(\alpha)}\cdots\overline{\chi_{\alpha_r}}(a_r)^{\mu(\alpha)}\cdot j(\alpha)^{\mu(\alpha)}(-1)^{\mu(\alpha)(r-1)}\right)^\nu(-1)^{r-1}
\end{aligned}$$

Soit $C(\alpha)$ défini par :

$$C(\alpha)=\overline{\chi_{\alpha_0}}(a_0)^{\mu(\alpha)}\cdots\overline{\chi_{\alpha_r}}(a_r)^{\mu(\alpha)}\cdot j(\alpha)^{\mu(\alpha)}(-1)^{\mu(\alpha)(r-1)}.$$

Donc :

$$R(\alpha,\mu(\alpha)\nu)=(-1)^{r-1}C(\alpha)^\nu.$$

Ainsi :

$$\begin{aligned}
\sum_{\nu\geq 1}\overline{N_\nu}U^{\nu-1} &= -\sum_{h=0}^{r-1}\frac{d}{du}\log(1-q^hU)+(-1)^{r-1}\sum_{\alpha\in\mathcal{A}}\sum_{\nu\geq 1}C(\alpha)^\nu U^{\nu\mu(\alpha)-1}\\
&= -\sum_{h=0}^{r-1}\frac{d}{du}\log(1-q^hU)+(-1)^{r-1}\sum_{\alpha\in\mathcal{A}}\frac{C(\alpha)U^{\mu(\alpha)-1}}{1-C(\alpha)U^{\mu(\alpha)}}\\
&= -\sum_{h=0}^{r-1}\frac{d}{du}\log(1-q^hU)+(-1)^{r-1}\sum_{\alpha\in\mathcal{A}}\frac{-1}{\mu(\alpha)}\frac{-\mu(\alpha)C(\alpha)U^{\mu(\alpha)-1}}{1-C(\alpha)U^{\mu(\alpha)}}\\
&= -\sum_{h=0}^{r-1}\frac{d}{du}\log(1-q^hU)+(-1)^{r-1}\sum_{\alpha\in\mathcal{A}}\frac{-1}{\mu(\alpha)}\frac{d}{du}\log(1-C(\alpha)U^{\mu(\alpha)})\\
&= -\sum_{h=0}^{r-1}\frac{d}{du}\log(1-q^hU)+(-1)^{r}\sum_{\alpha\in\mathcal{A}}\frac{1}{\mu(\alpha)}\frac{d}{du}\log(1-C(\alpha)U^{\mu(\alpha)}).
\end{aligned}$$

De plus, on remarque que $C(q\alpha)=C(\alpha)$ pour tout α car $x\to x^q$ est un automorphisme de $\mathbb{F}_{q^{\mu(\alpha)}}$ qui laisse invariant les a_i. Ainsi, dans la seconde somme, les $\mu(\alpha)$ termes correspondant aux ensembles $\alpha, q\alpha, \ldots, q^{\mu(\alpha)-1}\alpha$ sont égaux. En les réunissant, on supprime le dénominateur $\mu(\alpha)$ et alors :

$$\sum_{\nu\geq 1}\overline{N_\nu}U^{\nu-1}=\frac{d}{du}\log(Z(u)),$$

où $Z(U)$ est la fonction zeta associée à la variété diagonale homogène projective.

6 Historique des développements sur les conjectures de Weil

Weil a été guidé vers ses conjectures par l'étude de fonctions zeta de certaines variétés. Il s'est intéressé au cas des courbes et a prouvé ses conjectures pour celle-ci. La rationalité et l'équation fonctionnelle de la fonction zeta proviennent du théorème de Riemann-Roch. La dernière propriété analogue à l'hypothèse de Riemann a été plus compliqué à prouvé. Weil l'a déduite d'une inégalité de Castelnuovo et Severi sur les correspondances sur les courbes. On a trouvé par la suite une preuve plus simple (Mattuck, Tate et Grothendieck). Weil donna également une autre preuve utilisant la représentation l-adic du Frobenius sur une variété abélienne. Récemment une preuve totalement élémentaire a été découverte par Stepanov, Schmidt et Bombieri.
La plupart des travaux sur les conjectures de Weil a consisté à chercher une bonne cohomologie. Une cohomologie qui donnerait de bons nombres de Betti. Serre et Grothendieck ont beaucoup participés à ce travail. Grothendieck créa la cohomologie étale qui permit d'obtenir une autre preuve de la rationalité et de l'équation fonctionnelle vérifiée par la fonction zeta. La cohomologie cristalline de Grothendieck et Berthelot donna une interprétation cohomologique des conjectures de Weil.
Jusqu'a la preuve de Deligne de l'analogue général de l'hypothèse de Riemann, seulement quelques cas étaient connus : courbes, variétés rationnelles par Manin, surfaces K3 par Deligne.

7 Bibliographie

Weil André. *Number of solutions of equations over finite fields*, Bull. Amer. Math. Soc. 55 (1949), 497-508.
Hartshorne Robin. *Algebraic Geometry*. Appendice C The Weil Conjectures 449-458.
Tibouchi Mehdi. *Conjectures de Weil*. http ://www.eleves.ens.fr/home/tibouchi/tipe2.pdf