COURS DE L'INSTITUT FOURIER

JEAN-RENÉ JOLY

# Chapitre 9 Fonction zêta d'une variété algébrique

*Cours de l'institut Fourier*, tome 4 (1971), p. 1-30

<http://www.numdam.org/item?id=CIF_1971__4__A9_0>

# Chapitre 9

## Fonction zêta d'une variété algébrique

### (9.1). Paragraphe préliminaire: quelques conséquences du Nullstellensatz.

Soit $K$ un corps fini à $q$ éléments, et soit

$$(\Sigma) \quad \begin{cases} F_1(X_1 , \dots , X_n) = 0 \\ \dots\dots \\ F_r(X_1 , \dots , X_n) = 0 \end{cases}$$

un système de $r$ équations polynomiales à $n$ inconnues et à coefficients dans $K$. On peut associer à ce système plusieurs objets:

(I) L'ensemble algébrique affine des zéros de $(\Sigma)$ dans $\bar{K}^n$, $\bar{K}$ désignant la cloture algébrique de $K$ ; cet ensemble sera noté $V$ ; un point $x = (x_1 , \dots , x_n)$ de $V$ est tout simplement une solution commune dans $\bar{K}^n$ (et non plus nécessairement dans $K^n$, comme aux chapitres précédents) des $r$ équations $F_1(X) = 0 , \dots , F_r(X) = 0$.

(II) L'idéal $J$ de $K[X]$ engendré par les $r$ polynômes $F_1 , \dots , F_r$.

(III) L'idéal $I$ de $K[X]$ formé des polynômes $G$ tels que $G(x) = 0$ en tout point $x$ de $V$.

(IV) L'anneau (ou plus précisément la $K$-algèbre) $A = K[X]/I$ : c'est l'"anneau de coordonnées de $V$ ", généralement noté $K[V]$.

Des considérations algébriques élémentaires, plus les deux formes classiques du théorème des zéros (= Nullstellensatz) de Hilbert (voir par exemple

[La] , chapitre X, paragraphes 2 et 3, ou [Jo] , chapitre I) permettent d'affirmer ceci:

(i) L'idéal $I$ est la racine de l'idéal $J$ , c'est-à-dire l'intersection des idéaux premiers de $K[X]$ contenant $J$ , ou encore l'ensemble des éléments de $K[X]$ qui sont nilpotents modulo $J$ (Nullstellensatz, première forme).

(ii) $A = K[V]$ est donc une algèbre réduite, c'est-à-dire dépourvue d'éléments nilpotents; en outre, elle est de type fini sur $K$ : si $\xi_1 , \dots , \xi_n$ sont les images canoniques de $X_1 , \dots , X_n$ dans $A$ , on a évidemment $A = K[\xi_1 , \dots , \xi_n]$ .

(iii) Si $x = (x_1 , \dots , x_n)$ est un point de $V$ , on a

$$K[x_1 , \dots , x_n] = K(x_1 , \dots , x_n)$$

(en abrégé, $K[x] = K(x)$ ), puisque le point $x$ est algébrique sur $K$ (ses coordonnées $x_i$ sont par hypothèse dans la cloture algébrique $K$ de $K$ ). L'homomorphisme canonique $K[X] \longrightarrow K[x]$ (laissant $K$ invariant élément par élément, et appliquant chaque $X_i$ sur la composante $x_i$ correspondante) a donc pour image un corps, et pour noyau un idéal maximal $M$ ; en outre, par définition de $V$ , $J \subset M$ , donc $I \subset M$ , et $M$ donne par passage au quotient selon $I$ un idéal maximal $\mathfrak{m}$ de $A$ , parfaitement déterminé par $x \in V$ , et qu'on dira associé à $V$ ; naturellement,

$$(1) \qquad A/\mathfrak{m} \simeq K[X]/M \simeq K[x] = K(x) ,$$

et l'isomorphisme composé $A/\mathfrak{m} \xrightarrow{\sim} K(x)$ est entièrement défini par le fait que, pour chaque $i$ , il applique $\xi_i \pmod{\mathfrak{m}}$ sur la $i^{\text{ème}}$ composante $x_i$ de $x$ (et que d'autre part c'est un $K$-isomorphisme...)

(iv) Inversement, si $\mathfrak{m}$ est un idéal maximal de $A$ (correspondant de façon unique à un idéal maximal $M$ de $K[X]$ contenant $I$), il existe au moins un $K$-isomorphisme $\varphi : A \longrightarrow \overline{K}$ ayant exactement pour noyau $\mathfrak{m}$, ce qui équivaut à dire que le corps $A/\mathfrak{m}$ est une extension algébrique (de type fini, donc de degré fini) de $K$ (Nullstellensatz, deuxième forme); si alors on pose $x_i = \varphi(\xi_i)$ et $x = (x_1, \dots, x_n)$, on a évidemment

$$A/\mathfrak{m} \simeq K[x] = K(x), \tag{2}$$

l'idéal de $K[X]$ formé des $G$ tels que $G(x) = 0$ est $M \supset I \supset J$, et $x$ est un point de $V$ ($J$ est engendré par les $F_j$ ...)

(v) Ainsi, à tout point $x$ de $V$ correspond exactement un idéal maximal $\mathfrak{m}$ de $A$, et tout idéal maximal de $A$ peut être obtenu par ce procédé. Problème: étant donné $\mathfrak{m}$, idéal maximal de $A$, combien y a-t-il dans $V$ de points $x$ tels que $\mathfrak{m}$ soit l'idéal maximal associé à $x$ ? ou encore, combien de points de $V$ le procédé décrit en (iv) fait-il correspondre à $\mathfrak{m}$ ? Réponse: exactement $m = [A/\mathfrak{m} : K]$. En effet, posons $\xi'_i$ = la classe de $\xi_i$ (mod $\mathfrak{m}$), et, pour chaque $K$-homomorphisme $\varphi : A \longrightarrow \overline{K}$ ayant pour noyau $\mathfrak{m}$, désignons par $\varphi'$ le $K$-isomorphisme de $L = A/\mathfrak{m}$ dans $\overline{K}$ déduit de $\varphi$ par passage au quotient. Comme

$$(x_1, \dots, x_n) = (\varphi'(\xi'_1), \dots, \varphi'(\xi'_n)), \tag{3}$$

il s'agit en fait de compter le nombre de $K$-isomorphismes $\varphi'$ de $L$ dans la cloture algébrique $\overline{K}$ de $K$ ; et il y en a bien $m = [L : K]$, puisque l'extension $L/K$ est séparable. Ces "plongements" de $L$ dans $\overline{K}$ sont d'ailleurs évidemment conjugués les uns des autres par le groupe de Galois de $\overline{K}/K$, c'est-à-dire en réalité de $F_{q^m}/F_q$, $L$ s'identifiant nécessairement à

$F_{q^m}$ et $K$ à $F_q$ . Finalement, on a ce résultat très précis:

si $L = A/\mathfrak{m}$ et si $m = [L : K]$ ; si d'autre part $x = (x_1, \dots, x_n)$ est un point de $V$ correspondant à $\mathfrak{m}$ , il y a sur $V$ exactement $m$ points correspondant à $\mathfrak{m}$ , qui sont explicitement $x$ , $x^q$ , $x^{q^2}$ , ... , $x^{q^{m-1}}$ (avec la notation évidente $x^{q^j} = (x_1^{q^j}, \dots, x_n^{q^j}) \dots$)

(vi) Convenons de dire que deux points $x$ et $y$ de $V$ sont <u>conjugués sur</u> $K$ s'il existe un entier $j$ tel que $y = x^{q^j}$ : la conjugaison est évidemment une relation d'équivalence dans $V$ . Si $x \in V$ et si $[K(x) : K] = m$ , la classe de conjugaison de $x$ contient exactement $m$ points: $x$ , $x^q$ , $x^{q^2}$ , ... , $x^{q^{m-1}}$ , et les alinéas (iii), (iv) et (v) permettent en particulier d'affirmer ceci:

<u>Proposition 1</u>. - Soit $\mathfrak{M}$ l'ensemble de tous les idéaux maximaux (le "spectre maximal" Spm(A) ) de l'anneau de coordonnées $A = K[V]$ ; pour tout $\mathfrak{m} \in \mathfrak{M}$ , posons $\deg(\mathfrak{m}) = [A/\mathfrak{m} : K]$ et $N\mathfrak{m} = q^{\deg(\mathfrak{m})}$ ( $N\mathfrak{m}$ est donc égal au nombre d'éléments du corps résiduel $A/\mathfrak{m}$ ). Alors les correspondances $x \mapsto \mathfrak{m}$ et $\mathfrak{m} \longmapsto x$ définies en (iii) et en (iv) établissent une bijection entre l'ensemble des classes de conjugaison de points de $V$ et l'ensemble $\mathfrak{M}$ ; si la classe $C_x$ de $x \in V$ correspond à $\mathfrak{m} \in \mathfrak{M}$ , on a

$$K(x) \simeq A/\mathfrak{m} , \quad \operatorname{card}(K(x)) = N\mathfrak{m} , \quad \text{et} \tag{4}$$

$$\operatorname{card}(C_x) = [K(x) : K] = [A/\mathfrak{m} : K] = \deg(\mathfrak{m}) . \tag{5}$$

(vii) La proposition 1 permet d'indexer bijectivement les classes de conjugaison de points de $V$ à l'aide des $\mathfrak{m} \in \mathfrak{M}$ ; si $U_{\mathfrak{m}}$ = la classe

correspondant à $\mathfrak{m}$ , la famille $(U_{\mathfrak{m}})_{\mathfrak{m} \in \mathfrak{M}}$ est alors une partition de $V$ , et l'"ensemble partitionné" $(V, (U_{\mathfrak{m}})_{\mathfrak{m} \in \mathfrak{M}})$ possède alors les trois propriétés suivantes:

(EPF1) L'ensemble de base $V$ est dénombrable.

(EPF2) Chaque $U_{\mathfrak{m}}$ $(\mathfrak{m} \in \mathfrak{M})$ est un ensemble fini.

(EPF3) Pour tout entier positif $m$ , l'ensemble des $\mathfrak{m} \in \mathfrak{M}$ tels que $\mathrm{card}(U_{\mathfrak{m}}) = m$ est également fini.

(9.2). Fonctions zêta: définitions.

Un rappel pour commencer: soient $F$ un corps de nombres algébriques, $O_F$ l'anneau des entiers de $F$ et $s$ une variable complexe. On sait (voir par exemple [BS] , chapitre 5) que la fonction zêta correspondante peut être définie par

$$\zeta_F(s) = \prod_{\mathfrak{m}} 1 / (1 - N\mathfrak{m}^{-s})$$

où, dans le membre de droite, $\mathfrak{m}$ parcourt l'ensemble des idéaux maximaux de $O_F$ , et où $N\mathfrak{m} = \mathrm{card}(O_F / \mathfrak{m})$ ; le produit infini converge uniformément sur tout compact dans le demi-plan $\mathrm{Re}(s) > 1$ , et la fonction $\zeta_F$ ainsi définie est a priori une fonction holomorphe dans ce demi-plan.

Soient maintenant $K$ un corps fini à $q$ éléments, $A = K[\xi_1, \ldots, \xi_n]$ une algèbre de type fini sur $K$ et $\mathfrak{M}$ l'ensemble des idéaux maximaux de $A$ . Si $\mathfrak{m} \in \mathfrak{M}$ , $A / \mathfrak{m}$ est une extension algébrique de degré fini de $K$ (voir [La] , chapitre X, paragraphe 2), donc un corps fini: nous poserons

(6) $\quad [A / \mathfrak{m} : K] = \deg(\mathfrak{m})$ ; $\mathrm{card}(A / \mathfrak{m}) = q^{\deg(\mathfrak{m})} = N\mathfrak{m}$ ,

ce qui correspond aux notations du paragraphe précédent. Considérons alors le produit

$$(7) \qquad \prod_{\mathfrak{m} \in \mathfrak{M}} 1 / (1 - N\mathfrak{m}^{-s})$$

où $s$ désigne toujours une variable complexe. On vérifie assez facilement qu'il est absolument et uniformément convergent sur tout compact du demi-plan $\mathrm{Re}(s) > n$ : pour le voir, on se ramène d'abord au cas où $A$ = l'anneau de polynomes $K[X_1, \ldots, X_n]$, puis, par récurrence, au cas où $n = 1$, c'est-à-dire où $A = K[X_1]$ = un anneau principal; et on procède alors comme pour l'anneau $Z$ des entiers relatifs (auquel correspond la fonction zêta de Riemann) en transformant le produit (7) en série de Dirichlet par l'astuce "eulérienne" bien connue. Ceci justifie la définition suivante:

Définition 0. - Conservons les notations de l'alinéa précédent. On appelle fonction $\zeta$ (= zêta minuscule) de l'algèbre $A$ la fonction d'une variable complexe $s$, holomorphe dans le demi-plan $\mathrm{Re}(s) > n$ (au moins...) et définie dans ce demi-plan par

$$(8) \qquad \zeta_A(s) = \prod_{\mathfrak{m} \in \mathfrak{M}} 1 / (1 - N\mathfrak{m}^{-s}) .$$

Les produits infinis étant peu maniables, nous allons immédiatement transformer cette définition en faisant le changement de variable

$$(9) \qquad t = q^{-s}$$

qui donne évidemment $N\mathfrak{m}^{-s} = q^{-s \deg(\mathfrak{m})} = t^{\deg(\mathfrak{m})}$ ; d'où

Définition 1. - Mêmes notations. On appelle fonction $Z$ (= zêta majuscule) de $A$ la fonction d'une variable complexe $t$, holomorphe dans le disque

$|t| < q^{-n}$ (au moins...) et définie dans ce disque par

$$(10) \qquad Z_A(t) = \prod_{m \in \mathfrak{M}} 1 / (1 - t^{\deg(m)}) .$$

La relation $N m^{-s} = t^{\deg(m)}$ et le fait que

$$1 / (1 - t^m) = 1 + t^m + t^{2m} + \ldots\ldots$$

permettent alors d'énoncer

Proposition 2. - (i) Les coefficients du développement de Taylor de $Z_A(t)$ au voisinage de 0 sont des entiers positifs.

(ii) Les deux fonctions $\zeta_A$ et $Z_A$ sont liées par la relation

$$(11) \qquad \zeta_A(s) = Z_A(q^{-s}) .$$

Dans ce qui suit, nous nous occuperons surtout de $Z_A$, et nous laisserons de côté les questions de convergence (à ce propos, et pour ce qui concerne la définition la plus générale de la notion de fonction zêta, voir [Sf], [Br], chapitre III (3ème Partie), et surtout [Sg]). Nous considérerons donc essentiellement $Z_A(t)$ comme série formelle en $t$ à coefficients dans l'anneau $Z$ des entiers relatifs (ou dans le corps $Q$ des nombres rationnels).

*

Prenons en particulier pour $A$ l'algèbre $K[V]$ associée à l'ensemble $V$ des solutions de $(\Sigma)$ algébriques sur $K$ (voir paragraphe 1). Pour tout $m \geq 1$, posons $K_m = F_{q^m}$, considéré comme l'unique extension de degré $m$ de $K$ contenue dans $\overline{K}$, et désignons par $N_m$ le nombre de points de $V$ rationnels sur $K_m$, c'est-à-dire à composantes dans $K_m$ (de façon précise,

$$(12) \qquad N_m = \mathrm{card}(V \cap (K_m)^n) .$$

On a alors le résultat suivant:

Proposition 3. - Dans l'anneau de séries formelles $Q[[t]]$, on a

$$\log Z_A(t) = \sum_{m \geqslant 1} \frac{N_m}{m} t^m . \tag{13}$$

Démonstration. Par définition,

$$\log Z_A(t) = \sum_{\mathfrak{m} \in \mathfrak{M}} \log 1 / (1 - t^{\deg(\mathfrak{m})})$$

ou, plus explicitement,

$$\log Z_A(t) = \sum_{\mathfrak{m} \in \mathfrak{M}} (t^{\deg(\mathfrak{m})} + t^{2 \deg(\mathfrak{m})}/2 + \dots) . \tag{14}$$

Pour tout $j \geqslant 1$, désignons par $D_j$ le nombre (fini, d'après les résultats du paragraphe 1) de $\mathfrak{m} \in \mathfrak{M}$ tels que $\deg(\mathfrak{m}) = j$ ; la formule (14) donne immédiatement

$$\log Z_A(t) = \sum_{m \geqslant 1} \frac{\sum jD_j}{m} t^m , \tag{15}$$

la "somme intérieure" $\sum jD_j$ étant étendue à l'ensemble des diviseurs positifs $j$ de $m$ ; mais $jD_j$ est égal au nombre de points $x$ de $V$ tels que $[K(x) : K] = j$, puisque, d'après la proposition 1, ces points se répartissent en $D_j$ classes de conjugaison dont chacune contient $j$ points. Comme l'assertion $[K(x) : K] = j$ équivaut à l'assertion $K(x) = K_j$, d'une part, et que d'autre part l'assertion $x \in (K_m)^n$ équivaut à l'assertion $K(x) \subset K_m$, elle-même équivalente à l'assertion "il existe $j \mid m$ tel que $K(x) = K_j$" (voir chapitre 1, paragraphe 5, remarque 3), on constate finalement que $\sum_{j|m} jD_j = N_m$, et l'égalité (15) démontre directement la proposition 3.

Cette proposition mène à une nouvelle définition:

Définition 2. - Soit $V$ un ensemble algébrique quelconque (disons, affine

ou projectif...) défini sur $K$, corps fini à $q$ éléments, et, pour tout $m \geqslant 1$, soit $N_m$ le nombre de points de $V$ rationnels sur $K_m = F_{q^m}$. On appelle fonction $Z$ de $V$ la série formelle en $t$ à coefficients rationnels définie par

$$Z_V(t) = \exp\left\{ \sum_{m \geqslant 1} \frac{N_m}{m} t^m \right\} . \tag{16}$$

*

Encore une définition. Soient $W$ un ensemble et $(U_\mathfrak{y})_{\mathfrak{y} \in \mathfrak{P}}$ une partition de $W$, le tout possédant les trois propriétés suivantes:

(EPF1) L'ensemble $W$ est dénombrable.

(EPF2) Chaque $U_\mathfrak{y}$ $(\mathfrak{y} \in \mathfrak{P})$ est un ensemble fini.

(EPF3) Pour tout entier $m \geqslant 1$, l'ensemble des $\mathfrak{y} \in \mathfrak{P}$ tels que $\mathrm{card}(U_\mathfrak{y}) = m$ est également fini.

Si alors, pour tout $\mathfrak{y} \in \mathfrak{P}$, on pose $\mathrm{card}(U_\mathfrak{y}) = \deg(\mathfrak{y})$, on peut décréter

Définition 3. - On appelle fonction $Z$ de l'"ensemble partitionné" $W$ la série formelle en $t$ à coefficients entiers définie par

$$Z_W(t) = \prod_{\mathfrak{y} \in \mathfrak{P}} 1 / (1 - t^{\deg(\mathfrak{y})}) \tag{17}$$

(la convergence du produit dans $Z[[t]]$ étant assurée par les propriétés (EPF1, 2, 3)).

Dans le cas particulier où $W$ = un ensemble algébrique affine $V$ défini sur un corps fini et où la partition de $W$ est formée des classes de conjugaison, on retombe évidemment sur ses pieds: $Z_W(t) = Z_V(t)$.

Proposition 4. - Soient $W$ et $(U_\mathfrak{y})_{\mathfrak{y} \in \mathfrak{P}}$ comme ci-dessus. Pour tout

entier $m \geqslant 1$ , notons $N_m$ le nombre d'éléments $x$ de $W$ ayant la propriété suivante:

si $\varphi(x) =$ le $\varphi \in \Phi$ tel que $x \in U_\varphi$ , alors $\deg(\varphi(x))$ (c'est-à-dire $\operatorname{card}(U_{\varphi(x)})$) divise $m$ .

Alors

$$\log Z_W(t) = \sum_{m \geqslant 1} \frac{N_m}{m} t^m . \tag{18}$$

Démonstration. La même que celle de la proposition 3.

La proposition 4 implique ceci, qui n'est pas visible immédiatement sur la définition 2:

Théorème 1. - Quel que soit l'ensemble algébrique $V$ , $Z_V(t)$ est une série formelle à coefficients entiers.

Démonstration. Faire $W = V$ , prendre pour partition de $W$ les orbites (= trajectoires) pour l'action naturelle sur les points de $V$ du groupe de Galois de $\overline{K}/K$ , et appliquer la proposition 4 (en vérifiant la cohérence des notations, ce qui est immédiat).

(9.3). Propriétés classiques des fonctions zêta des ensembles algébriques.

Les principales propriétés des fonctions $Z_V(t)$ sont données par les théorèmes suivants:

Théorème 2 (Dwork). - Quel que soit l'ensemble algébrique $V$ , $Z_V(t)$ (qu'on sait déjà être une série formelle à coefficients dans $Z$ ) est en fait une fraction rationnelle (en $t$ ) à coefficients dans $Z$ .

Théorème 3 (Weil). - Si $V$ est une courbe projective non singulière irréduc-

tible et de genre $g$ , on a

$$(19) \qquad Z_V(t) = P(t) / (1 - t)(1 - qt) ,$$

où $P(t)$ est un polynôme à coefficients entiers de la forme

$$(20) \qquad 1 + \ldots + q^g t^{2g} = (1 - \alpha_1 t)(1 - \alpha_2 t)\ldots(1 - \alpha_{2g} t) ,$$

les $\alpha_i$ (qui sont évidemment des entiers algébriques, et qui sont les inverses des racines de $P(t)$ ) possédant en outre les propriétés suivantes:

(HR) Pour chaque valeur de $i$ , $|\alpha_i| = q^{1/2}$ .

(EF) $\alpha \longmapsto q\alpha^{-1}$ est une permutation de l'ensemble des $\alpha_i$ .

(Si on revient à la variable $s$ telle que $t = q^{-s}$ , (HR) signifie que "tous les zéros de la fonction $\zeta_V(s) = Z_V(q^{-s})$ sont sur la droite $\mathrm{Re}(s) = 1/2$ ": c'est l'"hypothèse de Riemann" pour la fonction $\zeta_V(s)$ ... Par ailleurs, compte tenu de (19) et (20), (EF) équivaut à affirmer que $P(t)$ vérifie l'"équation fonctionnelle" $P(t) = q^g t^{2g} P(1/qt)$ ).

Plus généralement:

Théorème 4 (Dwork). - Si $V$ est une hypersurface projective non singulière plongée dans un espace projectif de dimension $n$ ( $V$ est donc elle-même de dimension $n - 1$ ), si $V$ est de degré $d$ et si $n$ ou $d$ est impair ( * ), on a

$$(21) \qquad Z_V(t) = P(t)^{(-1)^n} / (1 - t)(1 - qt)\ldots(1 - q^{n-1}t) ,$$

$P(t)$ étant un polynôme à coefficients entiers, de terme constant égal à 1 et de degré $d^{-1}\left\{(-1)^{n+1}(d - 1) + (d - 1)^{n+1}\right\}$ .

( * ) Cette hypothèse ( n ou d impair ) peut être supprimée: voir [20].

Pour $n = 2$, ce théorème 4 redonne partiellement le théorème 3 (il redonne le théorème 3, à l'exception des précisions (HR) et (EF) relatives aux zéros de $P(t)$), puisque le genre d'une courbe plane projective non-singulière et de degré $d$ est donné par $g = (d-1)(d-2)/2$.

*

Voici quelques indications bibliographiques relatives aux démonstrations de ces théorèmes.

Pour le théorème 3, voir les deux mémoires de Weil sur les courbes algébriques [18] (méthodes géométriques, très techniques); voir également le livre de Weil [We], chapitre VII, §6 (méthodes d'analyse de Fourier sur l'anneau des adèles du corps des fonctions algébriques $K[V]$ de la courbe $V$, relativement élémentaires).

Pour le théorème 2, voir l'article original de Dwork [6] (voir aussi [5]); signalons également les exposés de séminaires [Be] et [Sf], ainsi que le chapitre 3 de [Br]); la démonstration de Dwork utilise essentiellement l'analyse p-adique.

Pour le théorème 4, voir le mémoire de Dwork [7], ainsi que les articles [20] et [21], qui sont le développement des méthodes p-adiques inaugurées dans [5] et [6].

Indiquons enfin que le théorème 3 avait été démontré dans des cas particuliers par Davenport et Hasse (courbes planes du type $Y^p - Y = X^m$ ou $Y^n = 1 - X^m$ : voir [3]), et que les théorèmes 2 et 4 avaient été conjecturés (et démontrés dans certains cas particuliers) par Weil, dans son article [19].

*

Dans ce qui suit, nous allons donner, "à la manière de [3] et [19] ", le calcul explicite des fonctions $Z$ de quelques variétés algébriques simples, et nous vérifierons ainsi sur des exemples les théorèmes 2 à 4: voir le paragraphe 5 ci-dessous. Nous utiliserons les résultats du chapitre 6, paragraphe 4, ainsi qu'un théorème de Davenport et Hasse relatif au comportement des sommes de Gauss par "extension du corps de base", théorème dont l'énoncé et la démonstration vont faire l'objet du paragraphe 4.

(9.4). Le théorème de Davenport et Hasse.

Théorème 5 (Davenport-Hasse). - Soient $K = F_q$ un corps fini à $q$ éléments, $K_m = F_{q^m}$ une extension de degré $m$ de $K$, $Tr$ et $N$ la trace et la norme relatives à l'extension $K_m / K$, $\theta$ un caractère additif non trivial (c'est-à-dire distinct du caractère unité) de $K$, et $\chi$ un caractère multiplicatif de $K$. Posons $\Theta = \theta \circ Tr$ et $X = \chi \circ N$. Alors

(i) $\Theta$ est un caractère additif non trivial de $K_m$ ; $X$ est un caractère multiplicatif de $K_m$ ; si $\chi$ est non trivial, $X$ est lui-même non trivial.

(ii) Les sommes de Gauss $\tau(\chi) = \tau(\chi|\theta)$ (relative à $K$) et $\tau(X) = \tau(X|\Theta)$ (relative à $K_m$) sont liées par

$$\tau(X) = (-1)^{m-1}\tau(\chi)^m . \tag{22}$$

(Remarque. Si on prend pour $\theta$ le caractère "habituel" $x \longmapsto \zeta^{Tr_{K/F_p}(x)}$, où $\zeta$ est une racine primitive $p^{\text{ième}}$ de l'unité dans $C$, $\Theta$ n'est autre, à cause de la transitivité de la trace, que $x \longmapsto \zeta^{Tr_{K_m/F_p}(x)}$, c'est-à-dire le caractère additif "habituel" (relatif à $K_m$) construit avec la même racine primitive $p^{\text{ième}}$ de l'unité que $\theta$).

Démonstration. (i) résulte immédiatement du fait que $Tr : K_m^+ \longrightarrow K^+$ et $N : K_m^* \longrightarrow K^*$ sont des homomorphismes surjectifs (voir chapitre 1, théorème 6). Prouvons (ii). Pour tout polynôme unitaire $P$ à coefficients dans $K$, disons $P(U) = U^h + a_1 U^{h-1} + \ldots + a_h$, convenons de poser

$$\varphi(P) = \theta(a_1)\chi(a_h) ; \tag{23}$$

à l'aide de $\Theta$ et $\mathcal{X}$, définissons de même $\Phi(Q)$ pour tout polynôme unitaire $Q$ à coefficients dans $K_m$ ; $\varphi$ et $\Phi$ sont évidemment des "caractères multiplicatifs" sur $K[U]$ et $K_m[U]$ respectivement:

$$\varphi(P_1P_2) = \varphi(P_1)\varphi(P_2) , \quad \Phi(Q_1Q_2) = \Phi(Q_1)\Phi(Q_2) . \tag{24}$$

Considérons alors les "séries L" associées à $\varphi$ et à $\Phi$, c'est-à-dire les séries formelles en $t$ et $u$ définies respectivement par

$$L(t,\varphi) = \sum_P \varphi(P)\, t^{\deg(P)} , \tag{25}$$

$$L(u,\Phi) = \sum_Q \Phi(Q)\, u^{\deg(Q)} , \tag{26}$$

$P$ parcourant l'ensemble des polynômes unitaires de $K[U]$ et $Q$ l'ensemble des polynômes unitaires de $K_m[U]$. On a

$$L(t,\varphi) = c_0 + c_1 t + c_2 t^2 + \ldots \tag{27}$$

avec $c_0 = \varphi(1) = 1$, $c_1 = \sum_{a_1 \in K} \theta(a_1)\chi(a_1) = \tau(\chi|\theta)$, et, pour $h \geqslant 2$,

$$c_h = \left\{ \sum_{a_1 \in K} \theta(a_1) \right\} \left\{ \sum_{a_h \in K} \chi(a_h) \right\} = 0 ,$$

puisque, $\theta$ étant supposé non trivial, le premier facteur du second membre est nul (voir chapitre 5, théorème 2, (8) ). Ainsi

$$L(t,\varphi) = 1 + \tau(\chi|\theta)\, t , \tag{28}$$

et de même

$$L(u, \bar{\Phi}) = 1 + \tau(X|\Theta)\, u \ . \tag{29}$$

Par ailleurs, comme tout polynôme unitaire de $K[U]$ se décompose d'une manière et une seule en produit de polynômes irréductibles et unitaires de $K[U]$, et que de plus $\varphi$ est un "caractère multiplicatif", la définition (25) donne, par la transformation eulérienne classique,

$$L(t, \varphi) = \prod_{\substack{P \\ \text{irréd} \\ \text{unit.}}} 1 / (1 - \varphi(P)\, t^{\deg(P)}) \ ; \tag{30}$$

de même,

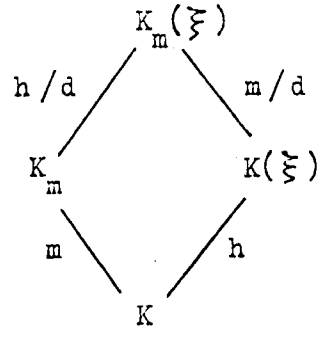
$$L(u, \bar{\Phi}) = \prod_{\substack{Q \\ \text{irréd} \\ \text{unit.}}} 1 / (1 - \bar{\Phi}(Q)\, u^{\deg(Q)}) \ . \tag{31}$$

Considérons alors $L(t^m, \bar{\Phi})$, qui peut s'écrire, en groupant, pour chaque $P$ (irréductible et unitaire dans $K[U]$), les $Q$ (irréductibles et unitaires dans $K_m[U]$) qui divisent $P$ :

$$L(t^m, \bar{\Phi}) = \prod_{P} \left\{ \prod_{Q \mid P} 1 / (1 - \bar{\Phi}(Q)\, t^{m \deg(Q)}) \right\}. \tag{32}$$

Donnons à $P$ une valeur fixée, et transformons le produit entre accolades. Posons $h = \deg(P)$, et soit $\xi$ une racine de $P$ dans une cloture algébrique de $K$ et $K_m$. On a $[K_m : K] = m$ par définition de $K_m$, et $[K(\xi) : K] = \deg(P) = h$ parce que $P$ est irréductible (et coïncide donc avec le polynôme minimal de $\xi$ sur $K$). Dans ces conditions, le degré $[K_m(\xi) : K]$ est égal au plus petit commun multiple de $m$ et $h$, puisque $K_m(\xi)$ est le plus petit corps (dans la cloture algébrique choisie de $K$ et $K_m$) qui contienne à la fois $K_m$ et $K(\xi)$ (voir chapitre 1, paragraphe 5, remarque 3); si $d$ désigne le plus grand commun diviseur $(m, h)$ de $m$ et

h , on a donc $\left[K_m(\xi) : K(\xi)\right] = m/d$ et $\left[K_m(\xi) : K_m\right] = h/d$ (voir le diagramme ci-contre).




L'avant-dernière égalité signifie évidemment que le polynôme P se décompose dans $K_m[U]$ en produit de d facteurs irréductibles et unitaires $Q_1$ , ... , $Q_d$ de même degré $h/d$ (rappelons que $K_m / K$ est abélienne); posons $h/d = k$ , et désignons par $a_1$ et $a_h$ la trace et la norme de $-\xi$ par rapport à K , et par $b_1$ et $b_k$ la trace et la norme de $-\xi$ par rapport à $K_m$ ; on a alors

$$P(U) = U^h + a_1 U^{h-1} + \ldots + a_h , \tag{33}$$

d'une part, et d'autre part, Q désignant celui des $Q_i$ dont $\xi$ est racine,

$$Q(U) = U^k + b_1 U^{k-1} + \ldots + b_k ; \tag{34}$$

ainsi,

$$\varphi(P) = \theta(a_1)\chi(a_h) , \qquad \Phi(Q) = \Theta(b_1)\chi(b_k) . \tag{35}$$

Or, on a évidemment, par définition de $b_1$ et par transitivité de la trace,

$$\begin{aligned} \mathrm{Tr}(b_1) &= \mathrm{Tr}_{K_m / K}(b_1) = \mathrm{Tr}_{K_m / K} \circ \mathrm{Tr}_{K_m(\xi)/ K_m}(-\xi) = \mathrm{Tr}_{K_m(\xi)/ K}(-\xi) \\ &= \mathrm{Tr}_{K(\xi) / K} \circ \mathrm{Tr}_{K_m(\xi) / K(\xi)}(-\xi) = \mathrm{Tr}_{K(\xi) / K}(-(m/d)\xi) \\ &= (m/d)\, \mathrm{Tr}_{K(\xi) / K}(-\xi) = (m/d)\, a_1 . \end{aligned}$$

Calcul analogue pour les normes; ainsi, on a

$$\mathrm{Tr}(b_1) = (m/d)\, a_1 , \qquad N(b_k) = a_h^{m/d} , \tag{36}$$

d'où immédiatement, compte tenu de (33) et (34),

(37) $$\bar{\Phi}(Q) = \varphi(P)^{m/d} ,$$

ce qui montre en particulier que les $d$ polynômes $Q = Q_1 , \dots , Q_d$ qui divisent $P$ donnent la même valeur au caractère $\bar{\Phi}$ . D'où

(38) $$\prod_{Q \mid P} 1 / (1 - \bar{\Phi}(Q)\, t^{m \deg(Q)}) = 1 / (1 - \varphi(P)^{m/d}\, t^{mh/d})^d .$$

Soient maintenant respectivement $\zeta_m$ et $\zeta_k$ une racine primitive $m^{\text{ième}}$ et une racine primitive $k^{\text{ième}}$ de l'unité dans $C$ ; quel que soit le nombre complexe $\varphi$ , on a l'égalité

(39) $$(1 - \varphi^{m/d}\, t^{mh/d})^d = \prod_{j=0}^{m-1} (1 - \varphi(\zeta_m^j t)^h) :$$

les deux membres sont en effet deux polynomes en $t$ à coefficients complexes, de même degré $mh$ , ayant même terme constant $1$ , et ayant pour racines les mêmes nombres $\varphi^{1/h}\, \zeta_k^{-i}\, \zeta_m^{-j}$ $( 0 \leq i < d , \ 0 \leq j < m )$ avec le même ordre de multiplicité $d$ (rappel: $k = h/d$ ...); grâce à (39), (38) devient ainsi, puisque $h = \deg(P)$,

(40) $$\prod_{Q \mid P} 1 / (1 - \bar{\Phi}(Q)\, t^{m \deg(Q)}) = \prod_{j=0}^{m-1} 1 / (1 - \varphi(P)(\zeta^j t)^{\deg(P)})$$

( $\zeta$ signifie $\zeta_m$ ); revenant aux formules (32) et (30), on obtient

(41) $$L(t^m, \bar{\Phi}) = \prod_{j=0}^{m-1} L(\zeta^j t , \varphi) ,$$

puis, en utilisant les relations (28) et (29),

(41) $$1 + \tau(X|\Theta) t^m = \prod_{j=0}^{m-1} (1 + \tau(\chi|\theta) \zeta^j t) ;$$

de là le résultat cherché, en identifiant les coefficients de $t^m$ dans les deux membres et en remarquant que $\prod_{0 \leq j \leq m-1} \zeta^j = (-1)^{m-1}$ .

Corollaire. - Soient $n \geqslant 2$ un entier et $\chi_1 , \dots , \chi_n$ $n$ caractères

multiplicatifs non triviaux de $K$ ; $m$ , $K_m$ et $N$ (= $N_{K_m/K}$ ) ayant la même signification que précédemment, soient $\chi_1$ , ... , $\chi_n$ les n caractères multiplicatifs non triviaux de $K_m$ égaux respectivement à $\chi_1 \circ N$ , ... , $\chi_n \circ N$ . Alors

(i) Si le caractère $\chi_1 \chi_2 \dots \chi_n$ est lui-même non trivial, on a, pour les sommes de Jacobi,

$$\pi(\chi_1 , \dots , \chi_n) = (-1)^{(n-1)(m-1)} \pi(\chi_1 , \dots , \chi_n)^m . \tag{42}$$

(ii) Si au contraire le caractère $\chi_1 \chi_2 \dots \chi_n$ est trivial, on a ( * )

$$\pi(\chi_1 , \dots , \chi_n) = (-1)^{n(m-1)} \pi(\chi_1 , \dots , \chi_n)^m . \tag{43}$$

Démonstration. Appliquer le théorème 5 et les formules (33) et (32) du chapitre 5 (proposition 6).

(9.5). Calcul explicite de quelques fonctions zêta.

Les notations ( $K$ , $q$ , $m$ , $K_m$ , $V$ , $Z_V(t)$ , ... ) restent les mêmes que dans les paragraphes précédents. Nous allons utiliser systématiquement l'évidence suivante:

Proposition 5. - Dire que $Z_V(t)$ est une fraction rationnelle sur $Z$ , de décomposition sur $C$ égale à

$$\prod_{1 \le i \le I} (1 - \alpha_i t) \Big/ \prod_{1 \le j \le J} (1 - \beta_j t) \tag{44}$$

équivaut à dire qu'il existe deux familles d'entiers algébriques $\alpha_1$ , ... , $\alpha_I$ et $\beta_1$ , ... , $\beta_J$ telles que, pour tout $m \geqslant 1$ , on ait

$$N_m = \beta_1^m + \dots + \beta_J^m - \alpha_1^m - \dots - \alpha_I^m . \tag{45}$$

( * ) éventuellement au signe près (mais peu importe...)

Démonstration. En effet, le logarithme de la fraction rationnelle écrite en (44) est évidemment égal à

$$\sum_{m \geqslant 1} \frac{\beta_1^m + \ldots - \alpha_1^m - \ldots}{m} t^m ,$$

tandis que, par définition, le logarithme de $Z_V(t)$ est égal à

$$\sum_{m \geqslant 1} \frac{N_m}{m} t^m .$$

*

Espace affine à n dimensions. Si V = l'espace affine à n dimensions, on a évidemment $N_m = \mathrm{card}((K_m)^n) = q^{mn} = (q^n)^m$ ; ainsi, la relation (45) est vérifiée avec $I = 0$ , $J = 1$ , $\beta_1 = q^n$ , et on peut affirmer ceci:

Proposition 6. - La fonction Z de l'espace affine à n dimensions sur $K = F_q$ est égale à $1 / (1 - q^n t)$ .

Espace projectif à n dimensions. Dans ce cas, on a

$$N_m = ((q^m)^{n+1} - 1)/(q^m - 1) = (q^n)^m + (q^{n-1})^m + \ldots + 1 ;$$

la relation (45) est vérifiée avec $I = 0$ , $J = n + 1$ , les $\beta$ égaux à $1$ , $q$ , ... , $q^{n-1}$ , $q^n$ ; d'où

Proposition 7. - La fonction Z de l'espace projectif à n dimensions sur $K = F_q$ est égale à $1 / (1 - t)(1 - qt)\ldots(1 - q^{n-1}t)(1 - q^n t)$ .

En particulier, la fonction Z de la droite projective sur $K = F_q$ est égale à $1 / (1 - t)(1 - qt)$ : ce qui vérifie le théorème 3 pour $g = 0$ (et même le démontre dans ce cas, puisque d'après le théorème de Chevalley toute courbe de genre 0 sur un corps fini admet un point rationnel sur ce

corps et est donc birégulièrement équivalente à la droite projective sur ce corps).

Voici quelques exemples plus particuliers.

Courbe projective plane d'équation $Y^2 = 1 - X^3$ (avec $q \equiv 1 \pmod 6$).
Le nombre de points à distance finie et rationnels sur $K = F_q$ a été calculé au chapitre 6, paragraphe 5 (équation (E3) et formule (28)): c'est

$$N^{aff} = q + \pi(\chi,\varphi) + \pi(\bar{\chi},\varphi), \tag{46}$$

$\chi$ et $\varphi$ étant des caractères d'ordres respectifs 3 et 2 sur $K^*$. Avec les notations du paragraphe 4 ( $X = \chi \circ N$ et de même $\Phi = \varphi \circ N$, et $N = N_{K_m/K}$ ), on obtient plus généralement le nombre $N_m^{aff}$ de points de la courbe à distance finie et rationnels sur $K_m$ :

$$N_m^{aff} = q^m + \pi(X,\Phi) + \pi(\bar{X},\Phi). \tag{47}$$

Comme d'autre part la courbe a exactement un point (d'inflexion) à l'infini, rationnel sur $K$ donc sur chaque $K_m$, le nombre $N_m^{proj}$ de points de la courbe à distance finie ou infinie et rationnels sur $K_m$ est donné par

$$N_m^{proj} = q^m + 1 + \pi(X,\Phi) + \pi(\bar{X},\Phi). \tag{48}$$

Posons alors

$$\alpha_1 = -\pi(\chi,\varphi) \; ; \quad \alpha_2 = -\pi(\bar{\chi},\varphi). \tag{49}$$

Le corollaire du paragraphe 4 (formule (42)) permet de réécrire la relation (48) sous la forme suivante:

$$N_m^{proj} = q^m + 1 - \alpha_1^m - \alpha_2^m. \tag{50}$$

En vertu de la proposition 5 énoncée au début de ce paragraphe, on obtient donc finalement

Proposition 8. - Pour $q \equiv 1 \pmod 6$, la fonction Z de la courbe projective plane sur $K = F_q$ d'équation (affine) $Y^2 = 1 - X^3$ est égale à $(1 - \alpha_1 t)(1 - \alpha_2 t) / (1 - t)(1 - qt)$ ($\alpha_1$ et $\alpha_2$ étant définis en (48)).

Ceci vérifie évidemment le théorème 3 avec $g = 1$, puisque $\alpha_1$ et $\alpha_2$ sont complexes conjugués de module $q^{1/2}$.

Courbe projective plane d'équation $Y^2 = 1 - X^3$ (avec $q \equiv -1 \pmod 6$). Le calcul est analogue à celui de l'alinéa précédent, mais se trouve compliqué par le fait que l'expression de $N_m^{proj}$ dépend maintenant de la parité de $m$ ; en effet, si $m$ est impair, on a $q^m \equiv -1 \pmod 6$, donc $(q^m - 1, 3) = 1$, d'où (voir chapitre 6, paragraphe 4), $N_m^{aff} = q^m$ et par conséquent

(51) pour $m$ impair, $N_m^{proj} = q^m + 1$.

Supposons maintenant $m$ pair, disons $m = 2\mu$ ; comme $q^2 \equiv 1 \pmod 6$, on peut choisir dans le dual du groupe multiplicatif $K_2^* = F_{q^2}^*$ un caractère $\chi'$ d'ordre 3 et un caractère $\varphi'$ d'ordre 2, puis construire les sommes de Jacobi $\pi(\chi', \varphi')$ et $\pi(\bar{\chi}', \varphi')$ (relatives à $K_2$), et enfin poser

(52) $$\alpha'_1 = -\pi(\chi', \varphi') \; ; \quad \alpha'_2 = -\pi(\bar{\chi}', \varphi') \; ;$$

le raisonnement de l'alinéa précédent, appliqué au "corps de base" $K_2$ et à $K_m = K_{2\mu}$, extension de degré $\mu$ de $K_2$, donne alors

(53) pour $m = 2\mu$ pair,

$$N_m^{proj} = q^m + 1 - \alpha_1'^{\mu} - \alpha_2'^{\mu}.$$

Admettons alors provisoirement le résultat suivant:

Lemme 1. - Les sommes de Jacobi $\pi(\chi', \varphi')$ et $\pi(\bar{\chi}', \varphi')$ introduites ci-dessus sont toutes deux égales à $q$ (c'est-à-dire à $(q^2)^{1/2}$ ...).

Posons alors $\alpha_1 = iq^{1/2}$ et $\alpha_2 = -iq^{1/2}$ ; les formules (51) et (53) donnent alors le résultat suivant, valable quelle que soit la parité de $m$ :

$$N_m^{proj} = q^m + 1 - \alpha_1^m - \alpha_2^m . \tag{54}$$

Ceci est formellement identique à (50), de sorte qu'on peut conclure comme à l'alinéa précédent (pour $q \equiv 1 \pmod 6$ )); on peut même en dire un peu plus, puisque $(1 - \alpha_1 t)(1 - \alpha_2 t) = (1 - iq^{1/2}t)(1 + iq^{1/2}t) = 1 + qt^2$ ; ainsi

Proposition 9. - Pour $q \equiv -1 \pmod 6$ ), la fonction $Z$ de la courbe projective plane d'équation (affine) $Y^2 = 1 - X^3$ sur $K = F_q$ est égale à $(1 + qt^2) / (1 - t)(1 - qt)$ .

Naturellement, ici encore, le théorème 3 se trouve vérifié.

Reste à démontrer le lemme 1: ce que nous allons faire par un raisonnement d'"aller et retour entre calcul de sommes de Jacobi et calcul du nombre de points sur des courbes" (à ce propos, voir l'introduction de l'article de Weil [19] ). Remarquons d'abord que le corollaire du théorème 5 (paragraphe 4), appliqué au "corps de base" $F_{p^2}$ et à $F_{q^2}$ , extension de degré $f$ de $F_{p^2}$ , permet de se limiter au cas où $q = p$ , c'est-à-dire où $K = F_p$ (noter que puisque $q = p^f \equiv -1 \pmod 6$ ), on a nécessairement $p \equiv -1 \pmod 6$ ), et $f$ est forcément impair...). Posons alors pour abréger

$$\pi = \pi(\chi', \varphi') , \quad \bar{\pi} = \pi(\bar{\chi}', \varphi') ; \tag{55}$$

$\pi$ et $\overline{\pi}$ sont complexes conjugués, et le nombre $N_2^{proj}$ de points de la courbe $Y^2 = 1 - X^3$ rationnels sur $K_2 = F_{p^2}$ est donné par

$$N_2^{proj} = p^2 + 1 + \pi + \overline{\pi} \tag{56}$$

(cas particulier de la formule (48) ci-dessus); comme $p^2 \equiv 1 \pmod 6$, on a ainsi

$$\pi + \overline{\pi} \equiv -2 + N_2^{proj} \pmod 6. \tag{57}$$

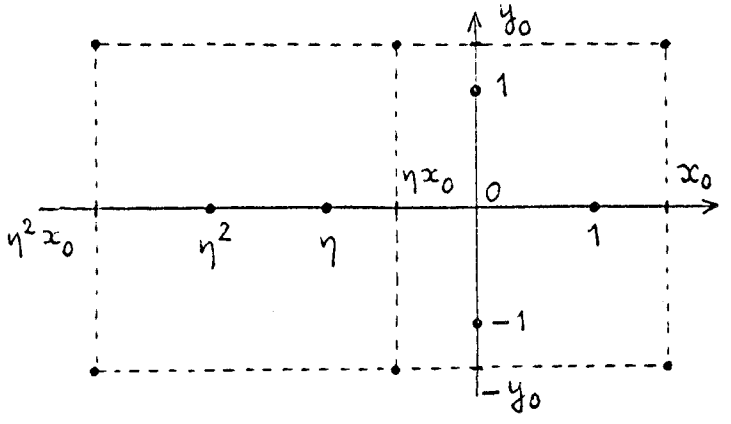
Par ailleurs, précisément parce que $p^2 \equiv 1 \pmod 6$, $K_2 = F_{p^2}$ contient deux racines carrées ( $1$ et $-1$ ) et trois racines cubiques (disons, $1$, $\eta$ et $\eta^2$ ) de l'unité; les points de la courbe rationnels sur $K_2$ se répartissent donc de la façon suivante:

un point à l'infini;

deux points sur l'axe des $Y$ ;

trois points sur l'axe des $X$ ;

enfin, les points à distance finie et non sur les axes, qui se groupent six par six, en familles du type $(\eta^\varepsilon x_0 , (-1)^{\varepsilon'} y_0)_{0 \le \varepsilon < 3,\ 0 \le \varepsilon' < 2}$ , avec évidemment $y_0^2 = 1 - x_0^3$ , $x_0 y_0 \neq 0$ (voir figure ci-dessous; en fait, la courbe possède, quand on la "dessine" dans le plan affine sur $K_2$ , un groupe de symétries d'ordre $6$ , phénomène qui ne se présente pas, et pour cause, en géométrie analytique réelle (les seules racines de l'unité dans le corps des réels sont $1$ et $-1$ ...)).



Il résulte de ce bilan que $N_2^{proj}$ est de la forme $1 + 2 + 3 + 6N'$, donc divisible par 6 ; la congruence (57) se réduit ainsi à

$$\pi + \bar{\pi} \equiv -2 \pmod 6 . \tag{58}$$

Maintenant, $\pi$ et $\bar{\pi}$ sont deux entiers de $Q(e^{2\pi i/3})$, conjugués, et tels que $\pi\bar{\pi} = p^2$ (voir chapitre 5...); comme $p$, congru à $-1$ modulo 6, est inerte dans $Q(e^{2\pi i/3})$, on a nécessairement

$$\pi = \zeta p , \quad \bar{\pi} = \bar{\zeta} p , \tag{59}$$

où $\zeta$ et $\bar{\zeta}$ sont des unités de $Q(e^{2\pi i/3})$, donc des racines $6^{\text{ièmes}}$ de l'unité. Compte tenu de (59) (et toujours du fait que $p \equiv -1 \pmod 6$), la congruence (58) devient

$$\zeta + \bar{\zeta} \equiv 2 \pmod 6 . \tag{60}$$

Mais, en donnant à $\zeta$ les valeurs $1$, $e^{\pi i/3}$, $e^{2\pi i/3}$, ..., $e^{5\pi i/3}$, on trouve respectivement pour $\zeta + \bar{\zeta}$ les valeurs $2$, $1$, $-1$, $-2$, $-1$, $1$ : la relation (60) implique donc $\zeta = \bar{\zeta} = 1$, soit, en revenant à (59), $\pi = \bar{\pi} = p$, c.q.f.d. (puisqu'on a vu qu'on pouvait se limiter au cas $q = p$ ...)

*

Courbes projectives planes d'équations $Y^3 = 1 - X^3$, $Y^2 = 1 - X^4$ (avec $p \neq 2, 3$).

Les fonctions Z de ces deux courbes se calculent exactement comme celle de la courbe $Y^2 = 1 - X^3$ étudiée ci-dessus; donnons cette détermination sous forme d'exercices:

Exercice 1. - a) Etudier la courbe projective plane V définie sur $K = F_q$

par l'équation (affine) $Y^3 = 1 - X^3$ (genre, points à l'infini,...); montrer qu'elle est non-singulière.

b) On suppose $q \equiv 1 \pmod 6$, et on désigne par $\chi$ un caractère multiplicatif d'ordre 3 sur K; montrer que si $\alpha_1 = -\pi(\chi,\chi)$ et $\alpha_2 = -\pi(\overline{\chi},\overline{\chi})$, la fonction Z de V est donnée par

$$Z_V(t) = (1 - \alpha_1 t)(1 - \alpha_2 t) / (1 - t)(1 - qt) . \tag{61}$$

c) On suppose au contraire $q \equiv -1 \pmod 6$; montrer que dans ce cas

$$Z_V(t) = (1 + qt^2) / (1 - t)(1 - qt) . \tag{62}$$

Exercice 2. - a) Etudier la courbe projective plane définie sur $K = F_q$ par l'équation (affine) $Y^2 = 1 - X^4$ (genre, points à l'infini, singularités); on désignera par V un "modèle projectif non-singulier" de la courbe proposée (c'est-à-dire, en langage naïf, une courbe projective "fictive" obtenue en "démultipliant" les "points multiples" de la courbe proposée...).

b) On suppose $q \equiv 1 \pmod 4$, et on désigne par $\varphi$ et $\psi$ respectivement un caractère multiplicatif d'ordre 2 et un caractère multiplicatif d'ordre 4 sur K; montrer que si $\alpha_1 = -\pi(\psi,\varphi)$ et $\alpha_2 = -\pi(\overline{\psi},\varphi)$, la fonction Z de V est est donnée par

$$Z_V(t) = (1 - \alpha_1 t)(1 - \alpha_2 t) / (1 - t)(1 - qt) . \tag{63}$$

c) On suppose au contraire $q \equiv -1 \pmod 4$; montrer que dans ce cas

$$Z_V(t) = (1 + qt^2) / (1 - t)(1 - qt) . \tag{64}$$

d) Etudier de la même manière la courbe $Y^2 = X - X^3$ et calculer sa fonction Z (se reporter au chapitre 6, paragraphe 5, équations (E4) et (E5)).

*

Calculons maintenant des fonctions Z de surfaces projectives.

La "sphère" $X^2 + Y^2 + Z^2 = 1$ (avec p impair).

Soit donc $K = F_q$ (avec p , donc q , impairs) et calculons la fonction Z de la surface projective définie sur K par l'équation (affine) $X^2 + Y^2 + Z^2 = 1$ ; soit $\varphi$ le caractère de Legendre sur K ; la formule (23) du chapitre 6, théorème 3, donne

$$N_1^{aff} = q^2 + \pi(\varphi,\varphi,\varphi) \tag{65}$$

(il s'agit évidemment du nombre de points à distance finie et rationnels sur $K = K_1$ ); ajoutons à ceci les points à l'infini rationnels sur K , qui forment évidemment un cercle projectif sur K et sont par conséquent en nombre $q + 1$ (voir chapitre 6, début du paragraphe 5); nous obtenons

$$N_1^{proj} = q^2 + q + 1 + \pi(\varphi,\varphi,\varphi) . \tag{66}$$

Mais la somme de Jacobi $\pi(\varphi,\varphi,\varphi)$ se calcule explicitement grâce à la proposition 6, formule (33), du chapitre 5: elle vaut $\tau(\varphi)^3/\tau(\varphi^3) = \tau(\varphi)^3/\tau(\varphi) = \tau(\varphi)^2 = \varphi(-1)q = (-1)^{(q-1)/2} q$ (on s'est aussi servi du fait que $\varphi$ est d'ordre 2 donc égal à son conjugué, et du lien entre caractère de Legendre et caractérisation des carrés dans K ...); ainsi

$$N_1^{proj} = q^2 + \{1 + (-1)^{(q-1)/2}\} q + 1 . \tag{67}$$

Il suffit naturellement de remplacer q par $q^m$ dans cette formule pour trouver la valeur de $N_m^{proj}$ ; le résultat se présente un peu différemment selon que q est congru à 1 ou à $-1$ modulo 4 : dans le premier cas, on a évidemment $N_m^{proj} = q^{2m} + 2q^m + 1$ ; dans le second cas, comme le "signe" $(-1)^{(q^m - 1)/2}$ est égal au "signe" $(-1)^m$ , on a la formule ana-

logue $N_m^{proj} = q^{2m} + q^m + (-q)^m + 1$. Dans les deux cas, on peut appliquer la proposition 5 avec $I = 0$, $J = 4$, $\beta_1 = q^2$, $\beta_2 = q$, $\beta_3 = q$ (dans le premier cas) ou $-q$ (dans le second cas), enfin $\beta_4 = 1$, d'où en définitive le résultat suivant:

Proposition 10. - La fonction $Z$ de la surface projective définie sur $K = F_q$ par l'équation (affine) $X^2 + Y^2 + Z^2 = 1$ est égale

si $q \equiv 1 \pmod 4$, à $1 / (1-t)(1-qt)^2(1-q^2t)$ ;

si $q \equiv -1 \pmod 4$, à $1 / (1-t)(1-qt)(1+qt)(1-q^2t)$ .

Ceci est naturellement conforme au théorème 4, avec $P(t) = 1 - qt$ (premier cas) ou $1 + qt$ (second cas), polynôme qui se retrouve au dénominateur (puisque $n = 3$ est impair) et dont le degré est

$$1 = 2^{-1}\left\{(-1)^{3+1}(2-1) + (2-1)^{3+1}\right\}.$$

Surface projective d'équation $X^3 + Y^3 + Z^3 = 1$ (avec $q \equiv 1 \pmod 6$).

Soit $\chi$ un caractère multiplicatif d'ordre 3 sur $K$ ; la formule (23) du chapitre 6 donne ici pour $N_1^{aff}$ la valeur

$$q^2 + \pi(\chi,\chi,\chi) + \pi(\bar\chi,\bar\chi,\bar\chi) + 3\pi(\chi,\bar\chi,\bar\chi) + 3\pi(\bar\chi,\chi,\chi) .$$

La proposition 6, formule (32), du chapitre 5, et le fait que $\chi$ est un caractère cubique, donc que $\chi(-1) = \chi((-1)^3) = \chi(-1)^3 = 1$ (et de même pour $\bar\chi$), permettent de simplifier légèrement ce résultat:

$$(68)\quad N_1^{aff} = q^2 - \pi(\chi,\chi) - \pi(\bar\chi,\bar\chi) + 3\pi(\chi,\bar\chi,\bar\chi) + 3\pi(\bar\chi,\chi,\chi) .$$

Pour avoir $N_1^{proj}$, il faut ajouter à ceci le nombre de points à l'infini de la surface étudiée, c'est-à-dire le nombre de points de la courbe projective

d'équation affine $X^3 + Y^3 + 1 = 0$ ; le nombre de points à distance finie sur cette courbe a été calculé au chapitre 6 (équation (E6) et formule (39): le changement de 1 en $-1$ ne change évidemment rien dans le résultat); ce nombre est $q - 2 + \pi(\chi,\chi) + \pi(\bar{\chi},\bar{\chi})$ ; quant au nombre de points à l'infini, il est égal à 3 , puisque K contient trois racines cubiques de $-1$ ; ainsi, la courbe projective étudiée contient donc

$$q + 1 + \pi(\chi,\chi) + \pi(\bar{\chi},\bar{\chi})$$

points, de sorte que

$$N_1^{proj} = q^2 + q + 1 + 3\pi(\chi,\bar{\chi},\bar{\chi}) + 3\pi(\bar{\chi},\chi,\chi) . \tag{69}$$

Posons alors

$$\pi_1 = \pi(\chi,\bar{\chi},\bar{\chi}) ; \quad \pi_2 = \pi(\bar{\chi},\chi,\chi) ; \tag{70}$$

les formules (69) et (42) donnent, par un type de raisonnement déjà fait plusieurs fois:

$$N_m^{proj} = q^{2m} + q^m + 1 + \pi_1{}^m + \pi_2{}^m \tag{71}$$

(noter que $n - 1 = 3 - 1 = 2$ , de sorte qu'il n'apparaît pas de signe " $-$ " dans le membre de droite de (42)); on peut donc appliquer la proposition 5 avec $I = 0$ , $J = 9$ , les $\beta$ étant respectivement $q^2$ , $q$ , $1$ , $\pi_1$ , $\pi_1$ , $\pi_1$ , $\pi_2$ , $\pi_2$ et $\pi_2$ ; et finalement

Proposition 11. - La fonction Z de la surface projective définie sur $K = F_q$ ( $q \equiv 1 \pmod 6$ ) par l'équation (affine) $X^3 + Y^3 + Z^3 = 1$ est égale à $1 / (1 - t)(1 - qt)(1 - q^2t)(1 - \pi_1 t)^3(1 - \pi_2 t)^3$.

Bien entendu, on s'aperçoit une fois de plus que le théorème 4 est véri-

fié: on a $P(t) = (1 - \pi_1 t)^3(1 - \pi_2 t)^3$ , ce polynôme se trouve au dénominateur, il est de degré

$$6 = 3^{-1}\left\{(-1)^{3+1}(3-1) + (3-1)^{3+1}\right\},$$

etc...

Le lecteur se fabriquera lui-même d'autres exemples, s'il cela peut le distraire.

(9.6). Quelques remarques pour terminer.

Elles concerneront le théorème 3, dans le cas où $g \geqslant 1$.

Remarque 1. - En se servant du théorème de Riemann-Roch, on peut assez facilement voir que le théorème 3 est équivalent à l'assertion suivante:

si $V$ est une courbe projective non-singulière de genre $g$ définie sur $K = F_q$ , et si $N$ est le nombre de points de $V$ rationnels sur $K$ , $N$ , $g$ et $q$ sont liés par l'inégalité

$$|q + 1 - N| \leq 2gq^{1/2} ; \tag{72}$$

à ce sujet, voir par exemple [18] , ou [Jo] . Pour $g = 1$ , cette inégalité prouve que toute courbe projective non-singulière de genre 1 définie sur un corps fini $K$ admet au moins un point rationnel sur $K$ (ce qui permet, en caractéristique différente de 2 et 3 , de mettre la courbe sous la "forme normale de Weierstrass"; ce qui permet également, dans tous les cas, de la munir d'une loi de groupe rationnelle sur $K$ et admettant ledit point rationnel sur $K$ comme élément neutre, donc d'en faire une "variété abélienne", etc...).

Noter d'autre part que (72) a été prouvée dans des cas particuliers au chapitre 6 (formules (29) et (36): $N$ signifiait $N_1^{aff} = N_1^{proj} - 1$ ).

Remarque 2. - Admettons le théorème 3, et plaçons-nous dans le cas où $g = 1$. La proposition 5, formule (45), avec $\beta_1 = q$, $\beta_2 = 1$, $\alpha_1$ et $\alpha_2$ = les inverses des racines du numérateur de $Z_V(t)$, montre immédiatement que

$$(73) \qquad Z_V(t) = (1 - (q + 1 - N_1)t + qt^2) / (1 - t)(1 - qt) .$$

Ceci explique pourquoi les courbes $Y^2 = 1 - X^3$, $Y^3 = 1 - X^3$, avec $q \equiv -1 \pmod 6$, et $Y^2 = 1 - X^4$ (désingularisée) avec $q \equiv -1 \pmod 4$ ont des fonctions $Z$ de la même forme $(1 + qt^2) / (1 - t)(1 - qt)$ : ces courbes ont ceci de commun que $N_1 = N_1^{proj} = q + 1$, puisqu'elles n'ont qu'un point à l'infini rationnel sur $K = F_q$, et que par ailleurs $N_1^{aff} = q$ (voir chapitre 6, paragraphe 4, deuxième partie de la remarque 1).

Remarque 3. - Cette formule (73) montre plus généralement que la connaissance de $N_1$ (c'est-à-dire du nombre de points de $V$ rationnels sur $K = F_q$) détermine entièrement (pour une courbe de genre 1, et toujours en admettant le théorème 3) la fonction $Z_V(t)$ de la courbe $V$ considérée, donc la collection de tous les $N_m = N_m^{proj}$ ; ceci est intéressant du fait que, comme on l'a constaté notamment pour la courbe $Y^2 = 1 - X^3$ dans le cas où $q$ est congru à $-1$ modulo 6, le calcul de $N_1$ peut être immédiat, tandis que le calcul (du moins, explicite) de $N_2$, par exemple, peut être beaucoup plus difficile.

Thème d'exercices sur cette remarque. - Au paragraphe précédent, on a, à trois reprises (une fois explicitement: lemme 1, et deux fois implicitement: exercices 1 et 2) calculé des sommes de Jacobi de manière à déterminer des fonctions $Z$ ; inverser cette démarche pour, dans les trois cas cités, expliciter les sommes de Jacobi en question à partir du fait supposé connu (voir remarque 2) que lesdites fonctions $Z$ valent $(1 + qt^2) / (1 - t)(1 - qt)$ .