COURS DE L'INSTITUT FOURIER

JEAN-RENÉ JOLY

Chapitre 6 Équations additives sur un corps fini (« Estimations de Weil »)

Cours de l'institut Fourier, tome 4 (1971), p. 1-17

<http://www.numdam.org/item?id=CIF_1971__4__A6_0>

Chapitre 6

Equations additives sur un corps fini

("Estimations de Weil")

(6.1). Introduction; énoncé de deux théorèmes.

Soient K un corps fini à $q = p^f$ éléments, n un entier positif et $F \in K[X] = K[X_1, \ldots, X_n]$ un polynôme additif sur K sans terme constant, c'est-à-dire de la forme

$$(1) \qquad F(X) = a_1 X_1^{d_1} + a_2 X_2^{d_2} + \ldots + a_n X_n^{d_n} ,$$

avec $d_1 \geqslant 1$, $d_2 \geqslant 1$, ... , $d_n \geqslant 1$ et les $a_i \in K$.

Problème 1. "Evaluer" le nombre de solutions dans K^n de l'équation sans second membre (donc sans terme constant) $F(X) = 0$.

Problème 2. "Evaluer" de même, pour tout élément non nul b de K , le nombre de solutions dans K^n de l'équation avec second membre $F(X) = b$.

Une solution "approchée" de ces deux problèmes est donnée par les deux théorèmes suivants, dus à Weil ([19]; voir également également les deux articles de Hua et Vandiver, [8] et [9]), et où on suppose essentiellement $a_1 \neq 0$, $a_2 \neq 0$, ... , $a_n \neq 0$ ($\overline{d}_i$ a la même signification que d'habitude: $\overline{d}_i = (q - 1 , d_i)$):

Théorème 1. - Le nombre N de solutions de l'équation $F(X) = 0$ vérifie

$$(2) \qquad \left| N - q^{n-1} \right| \leq (q - 1)\, q^{n/2 - 1} \prod_{i=1}^{n} (\overline{d}_i - 1) .$$

Théorème 2. - Pour tout élément non nul b de K, le nombre N_b de solutions de l'équation $F(X) = b$ vérifie

$$(3) \qquad \left| N_b - q^{n-1} \right| \leqslant q^{(n-1)/2} \prod_{i=1}^{n} (\bar{d}_i - 1) .$$

Les théorèmes 1 et 2 vont être prouvés respectivement au paragraphe 2 et au paragraphe 3, à l'aide des propriétés des sommes de Gauss et de Jacobi établies au chapitre 5. Ces théorèmes seront commentés au paragraphe 4.

(6.2). Démonstration du théorème 1.

Les résultats du chapitre 1, paragraphe 4, montrent qu'on ne modifie pas l'ensemble des solutions de l'équation $F(X) = 0$ en remplaçant, pour chaque variable X_i, l'exposant d_i par l'exposant $\bar{d}_i$; ce qui nous permet de faire l'hypothèse suivante:

(H) Chaque exposant d_i divise $q - 1$.

L'inégalité à démontrer s'écrit alors

$$(4) \qquad \left| N - q^{n-1} \right| \leqslant (q-1)\, q^{n/2 - 1} \prod_{i=1}^{n} (d_i - 1) .$$

Prouvons donc (4). Soit θ un caractère additif non trivial de K (par exemple $x \longmapsto \zeta^{\mathrm{Tr}(x)}$: voir chapitre 5, paragraphes 2 et 3).

Lemme 1. - On a l'égalité

$$(5) \qquad q\, N = \sum_{x \in K^n} \sum_{y \in K} \theta(yF(x)) .$$

Démonstration. Il suffit de noter que pour tout $x \in K^n$, l'application $y \longmapsto \theta(yF(x))$ est un caractère additif de K, égal au caractère 1 si et seulement si $F(x) = 0$, et d'appliquer alors le théorème 2, (ii) du chapitre 5.

Dans (5), intervertissons l'ordre des sommations, et isolons les termes correspondant à $y = 0$; nous obtenons

$$(6) \qquad q\,N = q^n + \sum_{y \in K^*} \sum_{x \in K^n} \theta(yF(x)) \ .$$

Divisons les deux membres par q , faisons passer q^{n-1} dans le membre de gauche, explicitons $F(x)$ à l'aide de (1) et utilisons le fait que θ est un caractère additif; nous arrivons à une nouvelle égalité

$$(7) \qquad N - q^{n-1} = q^{-1} \sum_{y \in K^*} \prod_{i=1}^{n} \sum_{x_i \in K} \theta(a_i y x_i^{d_i})$$

Le théorème 1 résulte immédiatement de l'égalité (7) et du lemme 2 ci-dessous, qui permet, dans le membre de droite de (7), de majorer en module chaque somme $\sum_{x_i \in K} \theta(a_i y x_i^{d_i})$ par $q^{1/2}(d_i - 1)$:

Lemme 2. - Soient d un entier divisant $q - 1$ et λ un caractère additif de K autre que le caractère unité 1 . Alors

$$(8) \qquad \left| \sum_{x \in K} \lambda(x^d) \right| \leq q^{1/2}(d - 1) \ .$$

Démonstration. Puisque d divise $q - 1$, le quotient K^*/K^{*d} est un groupe cyclique d'ordre d (chapitre 1, théorème 4, (ii)) et son dual est également cyclique d'ordre d (chapitre 5, proposition 4). Soit χ un générateur de ce dual: les caractères de K^*/K^{*d} sont exactement les χ^j $(0 \leq j \leq d - 1)$, et on peut évidemment considérer ces χ^j comme caractères multiplicatifs de K^* égaux à 1 sur le sous-groupe K^{*d} . Si alors, pour tout $u \in K$, on désigne par $m(u)$ le nombre de solutions dans K de l'"équation binôme" $U^d = u$, on a l'égalité

$$(9) \qquad m(u) = \sum_{0 \leq j \leq d-1} \chi^j(u) \ ;$$

en effet, le paragraphe 4 du chapitre 1, d'une part, et les paragraphes 1 et 3 du chapitre 5, d'autre part, montrent que les deux membres de (9) valent simultanément 1 , d ou 0 selon que $u = 0$, que $u \in K^{*d}$ ou que $u \in K^* - K^{*d}$; par ailleurs, il est évident que

$$(10) \qquad \sum_{x \in K} \lambda(x^d) = \sum_{u \in K} m(u)\lambda(u) \ .$$

Le rapprochement des formules (9) et (10) donne

$$(11) \qquad \sum_{x \in K} \lambda(x^d) = \sum_{j=0}^{d-1} \sum_{u \in K} \chi^j(u)\lambda(u) \ .$$

Pour chaque valeur de j , posons

$$\tau(j) = \sum_{u \in K} \chi^j(u)\lambda(u) \ ;$$

c'est la somme de Gauss associée aux caractères χ^j et λ ; d'après le paragraphe 3 du chapitre 5, formules (15), (18) et (20), on a

$$\tau(0) = 0 \ ; \quad |\tau(j)| = q^{1/2} \quad \text{pour} \quad 1 \leq j \leq d-1 \ ;$$

il suffit de porter ceci dans la relation (11) pour obtenir l'inégalité (8) cherchée, et achever ainsi de démontrer le théorème 1.

Remarque. - On peut prouver le théorème 1 par une autre méthode, due à Korobov, et ne faisant pas intervenir de sommes de Gauss: à ce sujet, voir [BS] , pp. 15 et 18.

(6.3). Démonstration du théorème 2.

Ici encore, nous ferons l'hypothèse

(H) Chaque exposant d_i divise $q - 1$.

L'inégalité à démontrer s'écrit alors

$$(12) \qquad \left| N_b - q^{n-1} \right| \leq q^{(n-1)/2} \prod_{i=1}^{n} (d_i - 1).$$

Le second membre ne dépendant ni des a_i, ni de b, nous supposerons également que $b = 1$ (quitte éventuellement à remplacer $F(X)$ par $b^{-1} F(X)$, on peut naturellement toujours faire cette hypothèse).

Cela étant, au travail! Soit $L(U) = L(U_1, \ldots, U_n)$ la forme linéaire $a_1U_1 + a_2U_2 + \ldots + a_nU_n$ par rapport à n variables U_i. Pour tout $u_i \in K$, désignons comme au paragraphe précédent par $m_i(u_i)$ le nombre de solutions de l'"équation binôme" $X_i^{d_i} = u_i$ (équation en l'unique variable X_i). Il est clair que le nombre N_1 de solutions de l'équation $F(X) = 1$ est donné par

$$(13) \qquad N_1 = \sum_{L(u)=1} m_1(u_1)\, m_2(u_2) \ldots m_n(u_n) .$$

Pour tout indice i ($1 \leq i \leq n$), désignons d'autre part par χ_i un caractère multiplicatif de K^* qui soit un générateur du dual de K^*/K^{*d_i} (voir paragraphe précédent, démonstration du lemme 2); on a

$$(14) \qquad m_i(u_i) = \sum_{j_i=0}^{d_i-1} \chi_i^{j_i}(u_i) ,$$

(c'est une simple réécriture de la formule (9) du paragraphe précédent); compte tenu de (14), l'égalité (13) devient

$$(15) \qquad N_1 = \sum_{L(u)=1} \sum_{j_1=0}^{d_1-1} \ldots \sum_{j_n=0}^{d_n-1} \chi_1^{j_1}(u_1) \ldots \chi_n^{j_n}(u_n) .$$

Posons $j = (j_1, \ldots, j_n)$, et mettons à part les termes de la somme ci-dessus correspondant à $j = 0$, termes égaux à 1 et en nombre q^{n-1} (le nombre de points de l'hyperplan affine $L(U) = 1$); intervertissons d'autre part l'ordre des sommations; nous obtenons

$$(16)\qquad N_1 - q^{n-1} = \sum_{j \neq 0} \sum_{L(u)=1} \chi_1^{j_1}(u_1) \dots \chi_n^{j_n}(u_n) \ .$$

Maintenant, il est facile de vérifier que si $j \neq 0$, mais si au moins une composante j_i de j est nulle, alors

$$(17)\qquad \sum_{L(u)=1} \chi_1^{j_1}(u_1) \dots \chi_n^{j_n}(u_n) = 0$$

(raisonner comme pour la formule (31) du chapitre 5, paragraphe 5); compte tenu de (17), l'égalité (16) peut s'écrire

$$(18)\qquad N_1 - q^{n-1} = \sum_{\substack{j_1 \neq 0 \\ \dots\dots \\ j_n \neq 0}} \sum_{L(u)=1} \chi_1^{j_1}(u_1) \dots \chi_n^{j_n}(u_n) \ .$$

Faisons alors le changement de variables $x_1 = a_1 u_1$, ..., $x_n = a_n u_n$; l'égalité (18) devient

$$N_1 - q^{n-1} = \sum_{\substack{j_1 \neq 0 \\ \dots\dots \\ j_n \neq 0}} \bar{\chi}_1^{j_1}(a_1) \dots \bar{\chi}_n^{j_n}(a_n) \sum_{x_1 + \dots + x_n = 1} \chi_1^{j_1}(x_1) \dots \chi_n^{j_n}(x_n)$$

ou encore, en utilisant la définition des sommes de Jacobi,

$$(19)\qquad N_1 - q^{n-1} = \sum_{\substack{j_1 \neq 0 \\ \dots\dots \\ j_n \neq 0}} \bar{\chi}_1^{j_1}(a_1) \dots \bar{\chi}_n^{j_n}(a_n)\, \pi(\chi_1^{j_1}, \dots, \chi_n^{j_n}) \ .$$

L'inégalité (12) résulte alors de la majoration (40) du module d'une somme de Jacobi non triviale (chapitre 5, paragraphe 5, proposition 6, corollaire), et du fait que $j = (j_1, \dots, j_n)$ (dans la sommation du membre de droite) prend $(d_1 - 1)(d_2 - 1)\dots(d_n - 1)$ valeurs distinctes. Le théorème 2 se trouve ainsi démontré.

Remarque. - La démonstration du lemme 2 (paragraphe 2) fait intervenir

la construction suivante, qui ressert au paragraphe 3:

soit d un entier divisant $q-1$ (de sorte que le groupe K^*/K^{*d} est cyclique d'ordre d) et soit χ un générateur du groupe dual de K^*/K^{*d} ; par composition avec l'homomorphisme canonique de K^* sur K^*/K^{*d} , χ donne un caractère multiplicatif de K , et ce caractère, qu'on peut encore noter χ , est évidemment d'ordre d . Inversement, soit χ un caractère multiplicatif d'ordre d sur K ; on a, pour tout $x \in K^*$, $\chi^d(x) = 1 = \chi(x^d)$, d'où $\chi(K^{*d}) = 1$; χ peut ainsi se factoriser à travers K^*/K^{*d} , et le caractère de K^*/K^{*d} qui en résulte est évidemment d'ordre d , donc générateur du dual de K^*/K^{*d} .

Ainsi, le caractère χ construit lors de la démonstration du lemme 2 est un caractère multiplicatif d'ordre d sur K , et tout caractère multiplicatif d'ordre d sur K s'obtient par cette construction.

(6.4). De inaequalitatibus (2)-(3) commentationes nonnullae.

Remarque 1. - Les inégalités (2) et (3) montrent essentiellement que N et N_b sont de l'ordre de grandeur de q^{n-1} , donc qu'il y a "à peu près autant de points" dans l'hypersurface $F(X) = 0$ ou $F(X) = b$ que dans n'importe quel hyperplan de K^n : ce qui est assez satisfaisant pour l'esprit...

En particulier, si l'un des exposants d_i est premier avec $q-1$, donc si $\overline{d_i} = 1$, les théorèmes 1 et 2 donnent exactement

$$N = N_b = q^{n-1} .$$

Ce résultat est évident sans calcul: si en effet (par exemple) $\overline{d_1} = 1$,

et si on considère l'équation $F(X) = b$, elle a le même nombre de solutions que l'équation

$$a_1 X_1 + a_2 X_2^{d_2} + \ldots + a_n X_n^{d_n} = b \ ;$$

dans cette dernière équation, on peut choisir arbitrairement $x_2, \ldots, x_n$, ce qui fait q^{n-1} choix possibles: et pour chacun de ces choix, il y a exactement une valeur possible pour x_1 , soit

$$x_1 = a_1^{-1} (b - a_2 x_2^{d_2} - \ldots - a_n x_n^{d_n}) \ ;$$

d'où au total exactement q^{n-1} solutions pour l'équation étudiée.

Remarque 2. - Les théorèmes 1 et 2 montrent notamment que si q est "assez grand" vis-à-vis du facteur $\prod_i (\bar{d}_i - 1)$, alors l'équation $F(X) = b$ ($b \neq 0$) admet certainement une solution, et l'équation $F(X) = 0$ admet certainement une solution non triviale. Voyons-le concrètement sur deux exemples classiques.

Exemple 1. - Problème: montrer que, quel que soit le nombre premier p , la congruence en nombres entiers

$$3X^3 + 4Y^3 + 5Z^3 \equiv 0 \pmod{p} \qquad (20)$$

admet une solution (x , y , z) non triviale (une solution (x , y , z) étant évidemment dite triviale si x , y et z sont tous trois divisibles par p).

Corrigé: pour $p = 2$, 3 ou 5 , on a des solutions évidentes; supposons donc $p \geqslant 7$, et appliquons le théorème 1 à $K = F_p$, avec $a_1 = 3$, $a_2 = 4$, $a_3 = 5$ (non nuls dans K) et $d_1 = d_2 = d_3 = 3$; on a alors $\prod_i (\bar{d}_i - 1) \leqslant \prod_i (d_i - 1) = 8$, et par conséquent

$$|N - p^2| \leqslant 8(p-1)p^{1/2} \ ;$$

mais pour $p \geqslant 67$, on a $p^2 - 8(p-1)p^{1/2} > 1$, donc $N > 1$ et en fait $N \geqslant 2$; autrement dit, pour $p \geqslant 67$, la congruence (20) admet toujours une solution non triviale. Le problème posé est ainsi résolu pour $p = 2$, 3 , 5 et $p = 67$, 71 , 73 , ... Reste un nombre fini de valeurs de p : 7 , 11 , 13 , ... , 59 , 61 , que le lecteur désoeuvré pourra examiner directement "à la main" (*).

Exemple 2. - On peut prouver exactement de la même manière le résultat suivant, démontré primitivement en 1832 par Libri (voir [23]).

quel que soit l'exposant n , la congruence en nombres entiers

$$X^n + Y^n \equiv Z^n \pmod{p} \tag{21}$$

admet au moins une solution non triviale pour tout nombre premier p suffisamment grand.

Il se trouve (voir la fin de l'article de Libri cité) que plusieurs "géomètres" avaient tenté, au début du XIX$^{\text{ème}}$ siècle, de démontrer le théorème de Fermat en prouvant au préalable la conjecture suivante:

quel que soit $n \geqslant 3$, il existe une infinité de nombres premiers p tels que la congruence (21) n'ait que la solution triviale.

(*) L'intérêt de cet exemple est le suivant: la congruence (20) a une solution non triviale pour tout p , et il est facile d'en déduire que l'équation $3X^3 + 4Y^3 + 5Z^3 = 0$ a partout localement une solution non triviale sur Z ; mais on peut prouver que cette équation n'a pas globalement de solution non triviale sur Z (Selmer: voir [Ca] , p. 202).

L'idée était sans doute excellente, mais la conjecture était malheureusement fausse...

Remarque 3. - Dans la démonstration du théorème 2, la relation (19) est une égalité et donne la valeur exacte de N_1 ; revenant alors à l'équation $F(X) = b$ écrite sous la forme $b^{-1}F(X) = 1$, et tenant compte de l'hypothèse (H), ainsi que de la remarque terminant le paragraphe 3, on voit qu'on a en fait prouvé ceci:

Théorème 3. - Le nombre de solutions de l'équation

$$a_1 X_1^{d_1} + \dots + a_n X_n^{d_n} = b \quad , \tag{22}$$

où les a_i et b sont tous supposés différents de 0 , et où les d_i sont tous supposés strictement positifs, est donné par la formule

$$N_b = q^{n-1} + \sum_j \overline{\chi}_1^{j_1}(b^{-1}a_1)\dots\overline{\chi}_n^{j_n}(b^{-1}a_n)\tau(\chi_1^{j_1},\dots,\chi_n^{j_n}) \quad , \tag{23}$$

où chaque χ_i est un caractère multiplicatif fixé, d'ordre $\overline{d_i}$, et où la sommation est étendue à l'ensemble des $j = (j_1 , \dots , j_n)$ tels que $1 \leq j_1 \leq d_1 - 1 , \dots , 1 \leq j_n \leq d_n - 1$.

Remarque 4. - N et N_b ($b \neq 0$) ayant toujours la même signification, désignons en outre par N' le nombre de solutions dans K^{n+1} de l'équation ci-dessous (équation à $n + 1$ variables et à coefficients tous différents de 0):

$$a_1 X_1^{d_1} + \dots + a_n X_n^{d_n} - b X_{n+1}^{q-1} = 0 \; ; \tag{24}$$

on vérifie sans peine le résultat suivant (donner à X_{n+1} une valeur arbitraire $x_{n+1} \in K$, puis résoudre l'équation par rapport aux variables

X_1 , ... , X_n "restantes"):

Théorème 4. - Les trois nombres N , N_b et N' sont liés par

$$N' = (q-1)N_b + N . \tag{25}$$

Exercice: compte tenu de l'égalité (25), "comparer" le théorème 1 et le théorème 2...

(6.5). A titre d'exercice...

Le but de ce paragraphe est d'appliquer les théorèmes précédents (en fait, surtout le théorème 3) au calcul du nombre de solutions de certaines équations à deux ou trois variables sur K : ce calcul montrera "comment se servir pratiquement" de l'horrible formule (23); en outre, les résultats obtenus resserviront aux chapitres 8 et 9. Pour simplifier, nous désignerons les variables par X , Y et Z au lieu de X_1 , X_2 et X_3 : à ceci près, nous conservons les notations et conventions des quatre premiers paragraphes.

Les équations $X^2 + Y^2 = 1$, $X^2 - Y^2 = 1$.

On cherche le nombre de solutions sur $K = F_q$ ($q = p^f$, p impair) des équations

(E1) $X^2 + Y^2 = 1$; (E2) $X^2 - Y^2 = 1$;

soit φ l'unique caractère multiplicatif d'ordre 2 de K (voir paragraphe 3, remarque; par hypothèse, $q-1$ est pair); ce caractère ("caractère de Legendre") peut être défini explicitement par $\varphi(0) = 0$, $\varphi(x) = 1$ si x est un carré dans K^* , et $\varphi(x) = -1$ si x est dans K^* mais n'est pas un carré; le théorème 3 donne alors immédiatement (N_k désignant

naturellement, ici et dans la suite, le nombre de solutions de l'équation (Ek)) $N_1 = q + \pi(\varphi,\varphi)$, $N_2 = q + \varphi(-1)\pi(\varphi,\varphi)$; mais, comme $\varphi^2 = 1$, on a d'autre part $\pi(\varphi,\varphi) = -\varphi(-1)$ (chapitre 5, formule (24)); ainsi,

$$(26) \qquad N_1 = \begin{cases} q + 1 & \text{si } -1 \text{ n'est pas un carré dans } K, \\ q - 1 & \text{si } -1 \text{ est un carré dans } K ; \end{cases}$$

$$(27) \qquad N_2 = q - 1 \quad \text{dans les deux cas.}$$

(Noter que d'après le chapitre 1, paragraphe 4, "critère d'Euler généralisé", -1 est un carré dans K si et seulement si $q \equiv 1 \pmod 4$)).

Remarque 1. - Dans le plan affine à deux dimensions sur K, les équations (E1) et (E2) représentent des coniques C_1 et C_2 (un "cercle" et une "hyperbole" respectivement), et ces coniques ont, en tant que courbes projectives, au moins un point rationnel sur K, c'est-à-dire à coordonnées dans K (appliquer le théorème de Chevalley, ou le théorème 2 du chapitre 4, aux équations homogénéisées $X^2 \pm Y^2 - T^2 = 0$); en faisant pivoter une droite autour d'un tel point rationnel, on obtient pour les coniques projectives C_1 et C_2 des représentations unicursales qui les mettent en correspondance bijective avec la droite projective sur K (laquelle possède $q + 1$ points); ainsi, C_1 et C_2 contiennent exactement $q + 1$ points à distance finie ou infinie; de là

$N_2 = (q + 1) - 2 = q - 1$, puisqu'il y a exactement deux points à l'infini sur l'"hyperbole" C_2 ;

$N_1 = q + 1$ si -1 n'est pas un carré dans K, puisque dans ce cas, C_1 n'a pas de points à l'infini, les "points cycliques" n'étant pas rationnels sur K ;

enfin, $N_1 = (q+1) - 2 = q - 1$ si -1 est un carré dans K, puisque dans ce cas, C_1 possède deux points à l'infini.

L'équation $Y^2 = 1 - X^3$ (avec $q \equiv 1 \pmod 6$).

On cherche le nombre de solutions sur $K = F_q$ ($q = p^f$, $p \neq 2$, $p \neq 3$, $q \equiv 1 \pmod 6$) de l'équation

$$X^3 + Y^2 = 1 . \tag{E3}$$

(Le cas $q \equiv -1 \pmod 6$ se traite instantanément: pourquoi?). Soient φ le caractère d'ordre 2 et χ un caractère d'ordre 3 de K^* ($q-1$ est par hypothèse divisible à la fois par 2 et par 3 ...); le théorème 3 donne ici, puisque $\chi^2 = \overline{\chi}$,

$$N_3 = q + \pi(\chi, \varphi) + \pi(\overline{\chi}, \varphi) . \tag{28}$$

Cette formule (28) donne directement l'inégalité

$$|N_3 - q| \leq 2\sqrt{q} , \tag{29}$$

qu'on peut également déduire du théorème 2.

L'équation $Y^2 = 1 - X^4$ (avec $q \equiv 1 \pmod 4$).

Même "topo" qu'à l'alinéa précédent. Soient φ le caractère d'ordre 2 et ψ un caractère d'ordre 4 de K^* ; le théorème 3 donne pour

$$X^4 + Y^2 = 1 \tag{E4}$$

une expression du nombre N_4 de solutions sous la forme

$$N_4 = q + \pi(\psi, \varphi) + \pi(\psi^2, \varphi) + \pi(\psi^3, \varphi) ; \tag{30}$$

mais $\psi^3 = \overline{\psi}$, $\psi^2 = \varphi$, $\pi(\varphi, \varphi) = -\varphi(-1)$, et enfin $\varphi(-1) = 1$, puisque $q \equiv 1 \pmod 4$ et que par conséquent -1 est un carré dans K ; finalement,

(31) $$N_4 = q - 1 + \pi(\psi, \varphi) + \pi(\bar{\psi}, \varphi) .$$

L'équation $Y^2 = X - X^3$ (avec $q \equiv 1 \pmod{12}$).

On s'intéresse maintenant au nombre N_5 de solutions sur $K = F_q$ ($q = p^f$, $p \neq 2, 3$, $q \equiv 1 \pmod{12}$) de l'équation

(E5) $$Y^2 = X - X^3 ,$$

qui n'est pas d'un des types étudiés aux paragraphes 1, 2 et 3. Par hypothèse, $q - 1$ est divisible à la fois par 2 , 3 et 4 ; nous désignerons comme précédemment par φ , χ et ψ le caractère d'ordre 2 , un caractère d'ordre 3 et un caractère d'ordre 4 de K^* ; nous utiliserons d'autre part le lemme suivant:

Lemme 3. - Soit $P(X)$ un polynôme à une variable X sur le corps K ; le nombre N de solutions dans K de l'équation

(E) $$Y^2 = P(X)$$

est donné par

(32) $$N = q + \sum_{x \in K} \varphi(P(x))$$

Démonstration. Pour chaque $x \in K$, l'équation (en l'unique variable Y) $Y^2 = P(x)$ admet

$1 = 1 + \varphi(P(x))$ solution si $P(x) = 0$,

$2 = 1 + \varphi(P(x))$ solutions si $P(x)$ est un carré dans K^* ,

$0 = 1 + \varphi(P(x))$ solution si $P(x)$ est dans K^* mais n'est pas un carré;

(comparer avec la formule (9) du paragraphe 2); il suffit alors de "promener" x dans K et d'additionner pour obtenir

$$N = \sum_{x \in K} 1 + \sum_{x \in K} \varphi(P(x)) ,$$

c.q.f.d.

Revenons alors à l'équation (E5), et appliquons le lemme avec $P(X) = X - X^3 = X(1 - X^2)$; nous obtenons

(33) $N_5 = q + S$, avec $S = \sum_{x \in K} \varphi(x)\varphi(1 - x^2)$;

étudions S ; il est clair que

(34) $$S = \sum_{x \in K} (1 + \varphi(x))\varphi(1 - x^2) - \sum_{x \in K} \varphi(1 - x^2) ;$$

des raisonnements déjà faits prouvent que

$$\sum_{x \in K} \varphi(1 - x^2) = \sum_{x \neq 1} \varphi(1 - x^2) = \sum_{x \neq 1} \varphi\left(\frac{1 + x}{1 - x}\right) =$$

$$= \sum_{y \neq -1} \varphi(y) = -\varphi(-1) = -1 ;$$

par ailleurs, il est (presque) clair que

$$\sum_{x \in K} (1 + \varphi(x))\varphi(1 - x^2) = \sum_{z \in K} \varphi(1 - z^4) ;$$

(petit exercice de dénombrement facile mais fastidieux, donc laissé au lecteur: si x est un carré, alors x^2 est une puissance quatrième, etc...); mais, d'après le lemme 3, le membre de droite de la dernière égalité vaut $N_4 - q$ (N_4 étant toujours le nombre de solutions de $Y^2 = 1 - X^4$); remontant la filière, nous obtenons alors successivement $S = N_4 - q + 1$, puis $N_5 = N_4 + 1$, et enfin, en utilisant la formule (31) de l'alinéa précédent,

(35) $$N_5 = q + \pi(\psi, \varphi) + \pi(\bar{\psi}, \varphi) .$$

Cette formule (35) implique l'inégalité

(36) $$|N_5 - q| \leq 2\sqrt{q} .$$

Remarque 2. - Les inégalités (29) et (36) sont deux cas particuliers du résultat général suivant ("théorème de Hasse": pour une démonstration élémentaire, voir par exemple [GL] , chapitre 10): le nombre N de solutions sur $K = F_q$ ($q = p^f$, $p \neq 2$, 3) d'une équation de la forme

(37) $$Y^2 = X^3 + aX + b \qquad (a , b \in K)$$

vérifie l'inégalité

(38) $$|N - q| \leq 2\sqrt{q} .$$

L'équation $Y^3 = 1 - X^3$ (avec $q \equiv 1 \pmod 6$).

On cherche maintenant le nombre de solutions sur F_q ($q \equiv 1 \pmod 6$) (nombre qu'on note N_6) de l'équation

(E6) $$X^3 + Y^3 = 1 .$$

Si χ désigne un caractère multiplicatif d'ordre 3 sur K , un calcul analogue à ceux faits pour les équations (E1) à (E4) donne

(39) $$N_6 = q - 2 + \pi(\chi,\chi) + \pi(\bar{\chi},\bar{\chi}) .$$

Pour nous changer les idées, étudions maintenant des équations à trois variables.

L'équation $X^2 + Y^2 + Z^2 = 1$.

On cherche le nombre N_7 de solutions sur F_q (comme pour l'équation (E1), on suppose p , et donc q , impair) de l'équation

(E7) $$X^2 + Y^2 + Z^2 = 1 .$$

Si φ désigne le caractère de Legendre sur $K = F_q$, on trouve, grâce à

la formule (23),

$$N_7 = q^2 + \pi(\varphi,\varphi,\varphi) \cdot \tag{40}$$

La formule (33) du chapitre 5 permet de transformer la somme de Jacobi figurant au second membre en $\tau(\varphi)^3/\tau(\varphi) = \tau(\varphi)^2 = \varphi(-1)\,q$ (chapitre 5, formule (19): noter que $\varphi = \overline{\varphi}$); comme, d'après le critère d'Euler généralisé (comparer avec l'étude de l'équation (E1)), on a $\varphi(-1) = (-1)^{(q-1)/2}$, la formule (40) donne finalement

$$N_7 = q^2 + (-1)^{(q-1)/2}\, q \,. \tag{41}$$

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

On cherche le nombre N_8 de solutions sur $K = F_q$ ($q \equiv 1 \pmod 6$) de l'équation

$$X^3 + Y^3 + Z^3 = 1 \,. \tag{E8}$$

Si χ désigne un caractère d'ordre 3 de K^*, la formule (23) donne

$$N_8 = q^2 + \pi(\chi,\chi,\chi) + \pi(\overline{\chi},\overline{\chi},\overline{\chi}) + \ldots \tag{42}$$
$$\ldots + 3\pi(\chi,\chi,\overline{\chi}) + 3\pi(\overline{\chi},\overline{\chi},\chi) \,.$$

Comme $\chi^3 = \overline{\chi}^3 = 1$, les deux premières sommes de Jacobi, au second membre, valent respectivement (utiliser la formule (32) du chapitre 5, et le fait que $\chi(-1) = \overline{\chi}(-1) = 1$, puisque $(-1)^3 = -1$) $-\pi(\chi,\chi)$ et $-\pi(\overline{\chi},\overline{\chi})$; (42) devient ainsi

$$N_8 = q^2 - (\pi(\chi,\chi) + \pi(\overline{\chi},\overline{\chi})) + \ldots \tag{43}$$
$$\ldots + 3(\pi(\chi,\chi,\overline{\chi}) + \pi(\overline{\chi},\overline{\chi},\chi)) \,.$$

Les résultats ci-dessus nous resservirons notamment au chapitre 9, pour le calcul explicite de certaines "fonctions zêta".