Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 19 (1973)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÉBRIQUES SUR UN CORPS FINI
Autor: Joly, Jean-René
Kapitel: Chapitre 6 ÉQUATIONS DIAGONALES (II)
DOI: https://doi.org/10.5169/seals-46287

Notes sur le chapitre 5

§ **1**: le fait que $\mathbf{F}_p^+$ est en dualité avec lui-même par $(x, y) \mapsto e^{2\pi ixy/p}$ est évident, et connu « depuis toujours ». Les caractères multiplicatifs de $\mathbf{F}_p$ se sont introduits progressivement à partir du milieu du XVIII^e siècle avec l'étude des restes quadratiques (Euler, Legendre, Gauss), cubiques (Gauss, Jacobi, Eisenstein) et biquadratiques (Gauss, Jacobi).

§ **2**: les sommes de Gauss apparaissent (sous la forme déguisée des *périodes cyclotomiques*) dans la dernière section des *Disquisitiones Arithmeticae*: Gauss les utilise pour étudier, avant la lettre, le groupe de Galois de l'extension $\mathbf{Q}(e^{2\pi i/p})/\mathbf{Q}$; à ce sujet, voir par exemple [**8**], pp. 453-460. Par la suite, les sommes de Gauss reparaissent systématiquement dans les travaux arithmétiques de Gauss, Jacobi, Eisenstein, Kummer, Stickelberger, en relation notamment avec l'étude des lois de réciprocité, et avec la représentation des nombres premiers par des formes quadratiques binaires à coefficients entiers; pour une synthèse de ces travaux, voir le livre centenaire de Bachmann (*Die Lehre von der Kreistheilung*, Teubner, Leipzig, 1872), ainsi que Stickelberger (1890). (L'utilisation de la somme de Gauss $\tau = \sum_{x \bmod p} \left(\frac{x}{p}\right) e^{2\pi ix/p}$ pour démontrer la loi de réciprocité quadratique est bien connue: voir [**8**], pp. 116-117, ou [**17**], chap. 1, sect. 3.3).

§ **3-4**: les sommes de Jacobi apparaissent également dans les travaux mentionnés ci-dessus; elles y sont *définies* à partir des sommes de Gauss par une formule qui coïncide avec la formule (3.3.2). Elles sont étudiées systématiquement chez Stickelberger (1890), Davenport-Hasse (1934) et Weil (1949) (ce dernier article contient d'ailleurs d'intéressantes indications historiques).

CHAPITRE 6

ÉQUATIONS DIAGONALES (II)

Ce chapitre utilise les propositions 3 et 5 du chapitre 5 pour établir des formules donnant le nombre exact $N(b)$ de solutions dans k^n d'une équation diagonale $a_1 X_1^{d_1} + \ldots + a_n X_n^{d_n} = b$ à coefficients dans k (k désigne toujours un corps fini à q éléments). Ces formules font intervenir des sommes de

Gauss et de Jacobi; si on sait calculer ces sommes, on obtient explicitement $N(b)$; sinon, l'évaluation du module des sommes de Gauss et de Jacobi donnée au chapitre 5 (prop. 8, prop. 9, cor. 1 et prop. 10, cor. 1) permet d'écrire une estimation approchée de $N(b)$; cette estimation est (sauf dans des cas exceptionnels) de la forme $N(b) = q^{n-1} + O(q^{n-(3/2)})$, q étant considéré comme « infiniment grand », et la constante impliquée par le O ne dépendant que du nombre de variables n et des degrés partiels d_i: c'est là un type de résultat dont on a déjà vu un exemple au chapitre 4 (th. 6, cor. 1), et qu'on retrouvera systématiquement au chapitre 8.

Dans tout le présent chapitre, les notations sont les suivantes: k désigne un corps fini à $q = p^f$ éléments; n est un entier $\geqslant 2$; $a_1, \ldots, a_n$ sont n éléments de k, qu'on suppose tous différents de 0; $d_1, \ldots, d_n$ sont n entiers $\geqslant 1$; F désigne le polynôme diagonal $a_1 X_1^{d_1} + \ldots + a_n X_n^{d_n}$; b est un élément quelconque de k; $N(b)$ désigne le nombre de solutions dans k^n de l'équation $F = b$; si $b = 0$ (équation « sans second membre » ou « sans terme constant »), on écrit N au lieu de $N(0)$; enfin, pour $i = 1, \ldots, n$, on pose $\delta_i = (q-1, d_i)$ et $h_i = (q-1)/\delta_i$.

§ 1. *Equations diagonales sans terme constant.*

On s'intéresse d'abord au cas où $b = 0$, et on cherche à évaluer $N = N(0)$. La lettre β désigne un caractère additif non trivial de k, fixé une fois pour toutes.

1.1. On aura besoin du résultat suivant:

LEMME 1. — *Soient γ un caractère additif non trivial de k, d un entier $\geqslant 1$, et χ un caractère multiplicatif de k, d'ordre $\delta = (q-1, d)$. Alors*

$$\sum_{x \in k} \gamma(x^d) = \sum_{j=1}^{\delta-1} \tau(\chi^j \mid \gamma). \tag{1.1.1}$$

Démonstration. — Si, pour tout $a \in k$, $m(a)$ désigne le nombre de solutions dans k de l'équation $X^d = a$, le membre de gauche de (1.1.1) peut évidemment s'écrire $\sum_{a \in k} m(a)\gamma(a)$; mais on a vu (chap. 5, prop. 5) que $m(a)$ est égal à $\sum_{j=0}^{\delta-1} \chi^j(a)$; ledit membre de gauche vaut donc $\sum_{j=0}^{\delta-1} \sum_{a \in k} \chi^j(a)\gamma(a)$, ce qui se décompose en

$$\sum_{j=0}^{\delta-1} \chi^j(0)\gamma(0) + \sum_{a \in k^*} \chi^0(a)\gamma(a) + \sum_{j=1}^{\delta-1} \sum_{a \in k^*} \chi^j(a)\gamma(a);$$

dans cette somme de trois termes, le premier vaut 1 (chap. 5, convention (1.4.1)), et le second, qui est une somme de Gauss correspondant au caractère multiplicatif trivial χ^0 et au caractère additif non trivial γ, vaut -1 (chap. 5, sect. 2.2, (i)). Seul reste donc le troisième terme, évidemment égal au membre de droite de (1.1.1): le lemme est ainsi prouvé.

1.2. Calculons alors N; partons de la formule (1.3.1) du chapitre 5, et isolons, dans la somme de droite, les q^n termes (égaux à 1) correspondant à $y = 0$; il vient

$$N = q^{n-1} + q^{-1} \sum_{y \in k^*} \sum_{\mathbf{x} \in k^n} \beta(yF(\mathbf{x})),$$

ou encore, compte tenu de la définition de F et du fait que β est un caractère additif,

$$N = q^{n-1} + q^{-1} \sum_{y \in k^*} \prod_{i=1}^{n} B(i, y), \tag{1.2.1}$$

avec par définition $B(i, y) = \sum_{x_i \in k} \beta(ya_i x_i^{d_i})$; le lemme 1, appliqué au caractère additif non trivial $\gamma = \beta_{ya_i}$, et la proposition 6 du chapitre 5, permettent de transformer le second membre et d'écrire

$$B(i, y) = \sum_{j_i=1}^{\delta_i - 1} \bar{\chi}^{j_i}(ya_i)\, \tau(\chi_i^{j_i}). \tag{1.2.2}$$

Désignons alors par θ un caractère multiplicatif d'ordre $q-1$ de k, fixé une fois pour toutes (par exemple celui défini au chapitre 5 par (1.4.2)) et faisons $\chi_i = \theta^{h_i}$; (1.2.2) devient

$$B(i, y) = \sum_{j_i=1}^{\delta_i - 1} \bar{\theta}^{j_i h_i}(ya_i)\, \tau(\theta^{j_i h_i}). \tag{1.2.3}$$

Notons J l'ensemble des vecteurs entiers $\mathbf{j} = (j_1, \ldots, j_n)$ tels que $1 \leqslant j_i \leqslant \delta_i - 1$ pour $i = 1, \ldots, n$; pour tout $\mathbf{j} \in J$, posons $s(\mathbf{j}) = j_1/\delta_1 + \ldots + j_n/\delta_n$; désignons par I le sous-ensemble de J formé des $\mathbf{j}$ tels que $s(\mathbf{j})$ soit entier; enfin, pour tout $\mathbf{j} \in J$, posons

$$C(\mathbf{j}) = \prod_{i=1}^{n} \bar{\theta}^{j_i h_i}(a_i); \qquad T(\mathbf{j}) = \prod_{i=1}^{n} \tau(\theta^{j_i h_i}). \tag{1.2.4}$$

Avec ces notations, (1.2.1) et (1.2.3) donnent

$$N = q^{n-1} + q^{-1} \sum_{\mathbf{j} \in J} S(\mathbf{j})\, C(\mathbf{j})\, T(\mathbf{j}), \tag{1.2.5}$$

$S(\mathbf{j})$ désignant (provisoirement) la quantité $\sum_{y \in k^*} \theta^{(q-1)s(\mathbf{j})}(y)$; mais les relations d'orthogonalité (1.1.1) (chap. 5, sect. 1.1) montrent que $S(\mathbf{j}) = 0$, *sauf si* $(q-1)\, s(\mathbf{j})$ *est divisible par* $q-1$ (c'est-à-dire si $s(\mathbf{j})$ est entier, donc par définition si $\mathbf{j} \in I$) *auquel cas* $S(\mathbf{j}) = q-1$; cette remarque permet, dans (1.2.5), de limiter la sommation aux $\mathbf{j} \in I$, et de remplacer tous les termes $S(\mathbf{j})$ par $q-1$; on arrive ainsi au résultat suivant:

THÉORÈME 1. — *L'ensemble* I *et les quantités* $C(\mathbf{j})$ *et* $T(\mathbf{j})$ *étant définis comme ci-dessus, le nombre* N *de solutions dans* k^n *de l'équation diagonale* $F = 0$ *est donné exactement par*

$$N = q^{n-1} + q^{-1}(q-1) \sum_{\mathbf{j} \in I} C(\mathbf{j})\, T(\mathbf{j}). \tag{1.2.6}$$

COROLLAIRE 1. — *Si* $A_1 = \mathrm{card}\,(I)$, *on a l'inégalité*

$$|N - q^{n-1}| \leqslant A_1 (q-1)\, q^{(n/2)-1}. \tag{1.2.7}$$

Démonstration. — Il suffit de remarquer que, dans la formule (1.2.6), chaque quantité $C(\mathbf{j})$ est une racine de l'unité, donc un nombre complexe de module 1, et que chaque quantité $T(\mathbf{j})$ est un produit de n sommes de Gauss non triviales relatives à k, donc un nombre complexe de module $q^{n/2}$ (chap. 5, prop. 8).

COROLLAIRE 2. — *Si* $A_2 = \mathrm{card}\,(J) = (\delta_1 - 1) \ldots (\delta_n - 1)$, *on a l'inégalité*

$$|N - q^{n-1}| \leqslant A_2 q^{n/2}. \tag{1.2.8}$$

Démonstration. — C'est une conséquence immédiate de (1.2.7), puisque $A_1 \leqslant A_2$ (en effet, $I \subset J$) et que $q - 1 \leqslant q$.

La constante A_2 ne dépend essentiellement que du degré $d = \sup d_i$ de F, et du nombre de variables n figurant dans F; d'autre part, pour $n \geqslant 3$, on a évidemment $n/2 \leqslant n - (3/2)$; le corollaire 2 permet donc d'énoncer ceci:

COROLLAIRE 3. — *Il existe une constante* A_2 *ne dépendant que du degré et du nombre de variables de* F, *et telle que (si* $n \geqslant 3$*)*

$$|N - q^{n-1}| \leqslant A_2 q^{n-(3/2)}. \tag{1.2.9}$$

Ainsi, pour $n \geqslant 3$, l'hypersurface $F = 0$ (qui est alors absolument irréductible, ce qui ne serait pas le cas pour $n \leqslant 2$) a un nombre N de points rationnels sur k qui est voisin (en un sens bien précis) de q^{n-1}: ce q^{n-1}

est lui-même le nombre de points rationnels sur k de n'importe quel hyperplan défini sur k. Ce corollaire 3 montre également que si q est supérieur à une certaine constante ne dépendant que de d et n, alors $N \geqslant 1$: l'équation $F = 0$ admet donc une solution dès que q est assez grand.

Le corollaire 3 est un cas particulier d'un résultat très général qui sera démontré au chapitre 8 (th. 4): on examinera plus en détail à cette occasion les conséquences qu'on peut tirer d'une inégalité telle que (1.2.9).

Revenons au corollaire 1; si I est vide, on a $A_1 = 0$; ainsi:

COROLLAIRE 4. — *Si l'ensemble I est vide, on a $N = q^{n-1}$.*

Un cas où I est vide est celui où l'un des δ_i est égal à 1 (on a même alors $A_2 = 0$); mais dans cette situation, l'égalité $N = q^{n-1}$ peut se prouver directement: il suffit de remarquer (comme au chap. 4, sect. 3.1) qu'on ne modifie pas N en remplaçant dans F les d_i par les δ_i, et de noter par ailleurs que si dans une équation diagonale l'un des exposants (disons d_1) est égal à 1, alors le nombre total de solutions de l'équation est q^{n-1}: car on peut se fixer arbitrairement les valeurs de $X_2, \ldots, X_n$ dans k (d'où q^{n-1} possibilités), et $F = 0$ devient alors une équation du premier degré en l'unique variable X_1.

Un cas plus général où I est vide est celui où l'un des entiers δ_i est premier avec les $n - 1$ autres (on laisse au lecteur le soin de le vérifier); ceci se produit notamment si l'un des d_i est premier avec les $n - 1$ autres. Exemple: quel que soit q, des équations telles que

$$X^2 + Y^3 + Z^3 = 0; \quad X^2 + Y^2 + Z^5 = 0,$$

admettent exactement q^2 solutions sur $k = \mathbf{F}_q$.

Un autre cas où I est vide est celui où n est impair, et où $d_i = 2$ pour $i = 1, \ldots, n$; ce cas a déjà été vu au chapitre 4, section 4.3, (3), et sera examiné à nouveau dans la section 3.1 ci-dessous.

§ 2. *Equations diagonales avec terme constant.*

On suppose maintenant $b \neq 0$, et on cherche à évaluer $N(b)$.

2.1. Désignons par $L(U) = L(U_1, \ldots, U_n)$ la forme linéaire $b^{-1}a_1U_1 + \ldots + b^{-1}a_nU_n$, et pour tout i ($1 \leqslant i \leqslant n$) et tout $u_i \in k$, notons $m_i(u_i)$ le nombre de solutions dans k de l'équation à une variable U_i: $U_i^{d_i} = u_i$ (chap. 5, sect. 1.5); χ_i désignant un caractère multiplicatif de k d'ordre $\delta_i = (q-1, d_i)$, on a alors (*loc. cit.*, prop. 5)

$$(2.1.1) \qquad m_i(u_i) = \sum_{j_i=0}^{\delta_i - 1} \chi_i^{j_i}(u_i) ;$$

par ailleurs, il est clair que

$$(2.1.2) \qquad N(b) = \sum_{\mathbf{u} \in H} m_1(u_1) \dots m_n(u_n) ,$$

H désignant l'hyperplan affine de k^n formé des points $\mathbf{u} = (u_1, ..., u_n)$ tels que $L(\mathbf{u}) = 1$; (2.1.1) et (2.1.2) donnent alors

$$(2.1.3) \qquad N(b) = \sum_{\mathbf{u} \in H} \prod_{i=1}^{n} \sum_{j_i=0}^{\delta_i - 1} \chi_i^{j_i}(u_i) .$$

Isolons dans le membre de droite les q^{n-1} termes (égaux à 1) correspondant à $\mathbf{j} = 0$ (c'est-à-dire à $(j_1, ..., j_n) = (0, ..., 0)$) et, pour les autres, intervertissons l'ordre des sommations; il vient

$$(2.1.4) \qquad N(b) = q^{n-1} + \sum_{\mathbf{j} \neq 0} \sum_{\mathbf{u} \in H} \prod_{i=1}^{n} \chi_i^{j_i}(u_i) .$$

Or, un raisonnement analogue à celui fait au chapitre 5, section 4.2, montre que si $\mathbf{j}$ n'est pas nul, mais si l'une au moins des composantes j_i de $\mathbf{j}$ est nulle, alors $\sum_{\mathbf{u} \in H} \prod_{i=1}^{n} \chi_i^{j_i}(u_i) = 0$; (2.1.4) se réduit donc à

$$(2.1.5) \qquad N(b) = q^{n-1} + \sum_{\mathbf{j} \in J} \sum_{\mathbf{u} \in H} \prod_{i=1}^{n} \chi_i^{j_i}(u_i) ,$$

J ayant la même signification qu'au paragraphe 1.

Effectuons alors le changement de variables $\mathbf{u} \mapsto \mathbf{x}$ défini par $x_i = b^{-1} a_i u_i$ $(1 \leqslant i \leqslant n)$, et désignons par H_1 l'hyperplan affine de k^n formé des $\mathbf{x} = (x_1, ..., x_n)$ tels que $x_1 + ... + x_n = 1$; (2.1.5) devient

$$(2.1.6) \qquad N(b) = q^{n-1} + \sum_{\mathbf{j} \in J} \prod_{i=1}^{n} \bar{\chi}_i^{j_i}(b^{-1} a_i) \sum_{\mathbf{x} \in H_1} \prod_{i=1}^{n} \chi_i^{j_i}(x_i) .$$

La quantité $\sum_{\mathbf{x} \in H_1} \prod_{i=1}^{n} \chi_i^{j_i}(x_i)$ n'est autre que la somme de Jacobi $\pi(\chi_1^{j_1}, ..., \chi_n^{j_n})$ (chap. 5, déf. 3), qu'on notera $\pi(\mathbf{j})$ pour alléger l'écriture; convenons d'autre part, pour tout $\mathbf{j} \in J$, de poser

$$(2.1.7) \qquad C(b, \mathbf{j}) = \prod_{i=1}^{n} \bar{\chi}_i^{j_i}(b^{-1} a_i) ;$$

(si on fait $\chi_i = \theta^{h_i}$ comme au paragraphe 1, on a en particulier $C(1, \mathbf{j}) = C(\mathbf{j})$); on arrive alors à ceci:

THÉORÈME 2. — *Le second membre b étant supposé non nul, et les quantités $C(b, \mathbf{j})$ et $\pi(\mathbf{j})$ étant définies comme ci-dessus, le nombre $N(b)$ de solutions dans k^n de l'équation diagonale $F = b$ est donné exactement par*

$$N(b) = q^{n-1} + \sum_{\mathbf{j} \in J} C(b, \mathbf{j})\, \pi(\mathbf{j}) . \tag{2.1.8}$$

COROLLAIRE 1. — *Posons (comme dans le corollaire 2 du théorème 1) $A_2 = \text{card}(J) = (\delta_1 - 1) \ldots (\delta_n - 1)$; on a alors l'inégalité*

$$| N(b) - q^{n-1} | \leqslant A_2 q^{(n-1)/2} . \tag{2.1.9}$$

Démonstration. — Il suffit de remarquer que dans la formule (2.1.8), chaque quantité $C(b, \mathbf{j})$ est une racine de l'unité, donc un nombre complexe de module 1, et que chaque quantité $\pi(\mathbf{j})$ est une somme de Jacobi non triviale à n caractères relative à k, donc un nombre complexe de module au plus égal à $q^{(n-1)/2}$ (chap. 5, prop. 10, cor. 1).

Pour $n \geqslant 2$, on a évidemment $(n-1)/2 \leqslant n - (3/2)$; ainsi:

COROLLAIRE 2. — *Il existe une constante A_2, ne dépendant que du degré et du nombre de variables de F, et telle que (si $n \geqslant 2$)*

$$| N(b) - q^{n-1} | \leqslant A_2 q^{n-(3/2)} . \tag{2.1.10}$$

Ce corollaire appelle naturellement les mêmes remarques que le corollaire 3 du théorème 1.

2.2. Supposons toujours $b \neq 0$, et soit N_1 le nombre de solutions dans k^{n+1} de l'équation diagonale sans second membre

$$a_1 X_1^{d_1} + \ldots + a_n X_n^{d_n} - b X_{n+1}^{q-1} = 0 ; \tag{2.2.1}$$

on vérifie sans peine que N, $N(b)$ et N_1 sont liés par

$$N_1 = N + (q-1) N(b) ; \tag{2.2.2}$$

mais le théorème 1 permet d'exprimer N et N_1 à l'aide de sommes de Gauss: (2.2.2) permettrait donc également d'exprimer $N(b)$ à l'aide de sommes de Gauss; la formule qui en résulterait est peu maniable, et il est inutile de l'écrire ici explicitement: signalons simplement que cette formule est identique à celle qu'on pourrait déduire de (2.1.8) en appliquant la proposition 10 du chapitre 5 à chacune des sommes de Jacobi $\pi(\mathbf{j})$ qui y figurent.

§ 3. « *Exemplis gaudeamus* ».

A titre d'application des théorèmes 1 et 2, on va calculer dans ce paragraphe le nombre de solutions de certains types simples (et classiques) d'équations diagonales.

3.1. On s'intéresse d'abord aux équations de la forme

$$a_1 X_1^2 + \ldots + a_n X_n^2 = b\,;$$

on peut se limiter au cas où p est impair; $q = p^f$ est alors impair, et on a $\delta_i = 2$ pour $i = 1, \ldots, n$; l'ensemble J des paragraphes 1 et 2 est formé du seul élément $\mathbf{j} = (1, \ldots, 1)$; enfin, les caractères $\chi_i = \theta^{(q-1)/\delta_i}$ sont tous égaux à l'unique caractère d'ordre 2 de k^*, c'est-à-dire au caractère de Legendre de k, qu'on notera φ (voir chap. 5, sect. 1.5).

(1) Supposons d'abord *n impair*. Si $b = 0$, on utilise le corollaire 1 du théorème 1, en remarquant que I est vide: on a donc $N = q^{n-1}$. Si $b \neq 0$, on utilise le théorème 2, qui donne ici

$$N(b) = q^{n-1} + \varphi(b^{-n} a_1 \ldots a_n)\, \pi(\varphi, \ldots, \varphi)\,; \tag{3.1.1}$$

comme $\varphi^n = \varphi \neq \varepsilon$ et que $\bar{\varphi} = \varphi$, on a $\pi(\varphi, \ldots, \varphi) = \tau(\varphi)^{n-1}$ et $\tau(\varphi)^2 = q\varphi(-1)$ (chap. 5, prop. 10, (ii) et prop. 7); ainsi,

$$\pi(\varphi, \ldots, \varphi) = \big(q\varphi(-1)\big)^{(n-1)/2}\,; \tag{3.1.2}$$

le rapprochement de (3.1.1) et (3.1.2), et le fait que φ vaut 1 sur les carrés et -1 sur les non carrés de k^*, permettent alors de conclure:

PROPOSITION 1. — *Pour n impair (et $p \neq 2$), le nombre N de solutions dans k^n de l'équation $a_1 X_1^2 + \ldots + a_n X_n^2 = b$ (où les a_i sont supposés tous différents de 0) est donné par les formules suivantes :*

(i) *Si* $b = 0, N = q^{n-1}$.

(ii) *Si* $b \neq 0, N = \begin{cases} q^{n-1} + q^{(n-1)/2}, & \text{si } (-1)^{(n-1)/2} a_1 \ldots a_n b \in k^{*2}, \\ q^{n-1} - q^{(n-1)/2}, & \text{si } (-1)^{(n-1)/2} a_1 \ldots a_n b \notin k^{*2}. \end{cases}$

(2) Supposons maintenant *n pair*. Si $b = 0$, on utilise le théorème 1, en remarquant que $I = J$; on trouve

$$N = q^{n-1} + q^{-1}(q-1)\,\varphi(a_1 \ldots a_n)\,\tau(\varphi)^n\,;$$

mais $\tau(\varphi)^n = \big(\tau(\varphi)^2\big)^{n/2} = \big(q\varphi(-1)\big)^{n/2}$; ainsi

(3.1.3) $$N = q^{n-1} + q^{-1}(q-1)\varphi\left((-1)^{n/2}a_1 \dots a_n\right) q^{n/2} .$$

Si $b \neq 0$, on utilise le théorème 2, en remarquant que

$$\pi(\varphi, \dots, \varphi) = -\varphi(-1)\tau(\varphi)^{n-2} = -\varphi(-1)\left(q\varphi(-1)\right)^{(n-2)/2}$$

(chap. 5, prop. 10, (i) puis (ii), et prop. 7; noter que $\varphi^n = \varepsilon$). Au total:

PROPOSITION 2. — *Pour n pair (et $p \neq 2$), N est donné par les formules suivantes :*

(i) *Si* $b = 0$, $N = \begin{cases} q^{n-1} + q^{n/2} - q^{(n/2)-1}, & \text{si } (-1)^{n/2}a_1 \dots a_n \in k^{*2}, \\ q^{n-1} - q^{n/2} + q^{(n/2)-1}, & \text{si } (-1)^{n/2}a_1 \dots a_n \notin k^{*2}; \end{cases}$

(ii) *Si* $b \neq 0$, $N = \begin{cases} q^{n-1} - q^{(n/2)-1}, & \text{si } (-1)^{n/2}a_1 \dots a_n \in k^{*2}, \\ q^{n-1} + q^{(n/2)-1}, & \text{si } (-1)^{n/2}a_1 \dots a_n \notin k^{*2}. \end{cases}$

On retrouve ainsi, et de manière plus naturelle, les résultats du chapitre 5, section 4.3, (3) et (4).

3.2. On s'intéresse maintenant aux équations de la forme $a_1 X_1^{d_1} + a_2 X_2^{d_2} = b$, avec a_1, a_2 et $b \neq 0$. Pour simplifier, on écrira X, Y au lieu de X_1, X_2, et on se limitera au cas où $a_1 = a_2 = b = 1$; on supposera d'autre part $q - 1$ divisible par d_1 et d_2 (on a toujours le droit de le faire: voir chap. 4, sect. 1.3 et 3.1). Si alors on note χ_1 et χ_2 des caractères multiplicatifs d'ordre d_1 et d_2 de k, et si J désigne l'ensemble des couples d'entiers (j_1, j_2) tels que $1 \leqslant j_1 \leqslant d_1 - 1$, $1 \leqslant j_2 \leqslant d_2 - 1$, le théorème 2 permet d'énoncer:

PROPOSITION 3. — *Le nombre N de solutions sur k de l'équation* $X^{d_1} + Y^{d_2} = 1$ *est donné par*

(3.2.1) $$N = q + \sum_{j \in J} \pi(\chi_1^{j_1}, \chi_2^{j_2}) .$$

3.3. La proposition 3 permet notamment de calculer le nombre de points rationnels sur k de certaines courbes de genre 1 [1]).

(1) *La courbe* $Y^2 = 1 - X^3$ (*avec* $q \equiv 1 \pmod 6$). Si φ désigne le caractère de Legendre et si χ est un caractère d'ordre 3 de k^* (donc tel que $\chi^2 = \bar{\chi}$), (3.2.1) donne

(3.3.1) $$N_1 = q + \pi(\varphi, \chi) + \pi(\varphi, \bar{\chi}) .$$

[1]) Les exemples ci-dessous resserviront aux chapitres 8 et 9.

(2) *La courbe* $Y^2 = 1 - X^4$ (*avec* $q \equiv 1 \pmod 4$). Si φ désigne toujours le caractère de Legendre, et si ψ est un caractère d'ordre 4 de k^* (donc tel que $\psi^2 = \varphi$ et $\psi^3 = \bar{\psi}$), (3.2.1) donne

$$N_2 = q - 1 + \pi(\varphi, \psi) + \pi(\varphi, \bar{\psi}). \tag{3.3.2}$$

(Se rappeler que $\pi(\varphi, \varphi) = -\varphi(-1)$, et noter que $\varphi(-1) = 1$, puisque $q \equiv 1 \pmod 4$, et que -1 est donc un carré dans k).

(3) *La courbe* $Y^3 = 1 - X^3$ (*avec* $q \equiv 1 \pmod 3$). Si χ désigne un caractère d'ordre 3 de k^* (donc tel que $\chi^2 = \bar{\chi}$), (3.2.1) donne

$$N_3 = q - 2 + \pi(\chi, \chi) + \pi(\bar{\chi}, \bar{\chi}). \tag{3.3.3}$$

(Noter que $\pi(\chi, \bar{\chi}) = \pi(\bar{\chi}, \chi) = -\chi(-1)$: chap. 5, prop. 9, (i); et remarquer que $\chi(-1) = 1$, puisque $-1 = (-1)^3$).

3.4. Considérons maintenant *la courbe* V_4 *d'équation* $Y^2 = X - X^3$; elle est également de genre 1 (on suppose pour simplifier $q \equiv 1 \pmod 4$); l'équation, en revanche, n'est plus diagonale: on peut toutefois, grâce à (3.3.2), calculer le nombre N_4 de points de C_4 rationnels sur k; en fait (et avec les notations de la section 3.3, (2)):

$$N_4 = q + \pi(\varphi, \psi) + \pi(\varphi, \bar{\psi}). \tag{3.4.1}$$

Un procédé de démonstration est le suivant (on laisse au lecteur le soin de régler les détails); tout d'abord, la congruence $q \equiv 1 \pmod 4$ entraîne que -1 est un carré dans k, et que -4 est une puissance 4-ième dans k: pour vérifier ce dernier point, appliquer les « lois complémentaires »

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

([**17**], p. 15), et se rappeler que $q = p^f$; soient donc a et i deux éléments de k tels que $i^2 = -1$, $a^4 = -4$, et $a^2 = 2i$. Soient d'autre part V_2, V_2' et V_4' les courbes d'équations respectives $Y^2 = 1 - X^4$, $Y^2 = a^4 - X^4$ et $2a^2 Y^2 = X + X^3$, et soient N_2, N_2' et N_4' leurs nombres de points rationnels sur k (toutes ces courbes sont considérées comme *affines*). Il est clair que $N_2 = N_2'$, et comme $2a^2 = 4i$, on voit également sans peine que $N_4 = N_4'$: compte tenu de (3.3.2), il suffit alors de prouver que $N_4' = N_2' + 1$, ce qui se déduit facilement de l'existence d'une application birationnelle $\lambda: V_2' \to V_4'$, définie par

$$\lambda(x, y) = \left(x^2/(y + a^2),\ x/(y + a^2)\right).$$

La relation (3.4.1) (c'est-à-dire l'égalité $N_4 = N_2 + 1$) peut aussi se démontrer en appliquant aux deux polynômes $P_2(X) = 1 - X^4$ et $P_4(X) = X - X^3$ le lemme suivant (qui se prouve sans difficulté):

LEMME 1. — *(On suppose $p \neq 2$). Soit $P(X)$ un polynôme à une variable X et à coefficients dans k. Si φ désigne le caractère de Legendre de k, le nombre N_P de solutions sur k de l'équation $Y^2 = P(X)$ est donné par*

$$N_P = q + \sum_{x \in k} \varphi(P(x)). \tag{3.4.2}$$

Au sujet de cette seconde méthode, voir Morlaye (1972).

3.5. Dans la section 3.3, on a supposé q congru à 1 modulo 6 (ou modulo 4, ou modulo 3) pour pouvoir calculer N_1, N_2 et N_3 par application directe de la proposition 3. On laisse au lecteur le soin de vérifier (ce qui est immédiat) les assertions suivantes:

si $q \equiv -1 \pmod 6$, on a $N_1 = q$; si $q \equiv -1 \pmod 4$, on a $N_2 = q + 1$; si $q \equiv -1 \pmod 3$, on a $N_3 = q$; enfin, si $q \equiv -1 \pmod 4$, on a $N_4 = q$.

Notes sur le chapitre 6

§ **1-2**: le lien entre nombre de solutions d'une congruence diagonale modulo p et sommes de Gauss et de Jacobi avait déjà été remarqué par Gauss et Jacobi eux-mêmes, notamment pour les congruences $aX^3 - bY^3 \equiv 1 \pmod p$, $aX^4 - bY^4 \equiv 1 \pmod p$, $Y^2 \equiv aX^4 - b \pmod p$; à ce sujet, voir Weil (1949), pp. 497-498. La congruence $X^n + Y^n + 1 \equiv 0 \pmod p$ a été étudiée par Libri (1832) pour $n = 3, 4$, puis, beaucoup plus tard, par Pellet, Jacobsthal, ainsi que Dickson (1909), Hurwitz (1909), Schur (1916), Mordell (1922), etc., pour n quelconque, en relation avec le théorème de Fermat. La congruence $X_1^k + \ldots + X_s^k \equiv m \pmod p$ a été étudiée notamment par Hardy-Littlewood (1922) dans leurs travaux sur le problème de Waring. Le théorème 2, pour deux variables, est dû à Davenport-Hasse (1934), et, indépendamment, à Hua-Vandiver (1949, a; b) et Weil (1949) pour un nombre de variables quelconque.

§ **3**: les propositions 1 et 2 (pour $q = p$) figurent déjà dans Lebesgue (1837), où elles sont d'ailleurs démontrées d'une autre manière. La proposition 3 et les exemples de la section 3.3 sont empruntés à Davenport-Hasse (1934). Le lien entre nombre de solutions de $Y^2 = X - X^3$ et de $Y^2 = 1 - X^4$ semble avoir été remarqué (incidemment) pour la première fois par

Jacobsthal (1907). Pour $q = p \equiv 1 \pmod 4$, la formule (3.4.1) peut, avec les notations de l'appendice du chapitre 5 (sect. A.1, exemple 2) et compte de la proposition 12 *(ibid.)*, s'écrire $N_4 = p - \lambda - \bar{\lambda}$. Plus généralement, si $D \in \mathbf{Z}$, et si $N_4(D)$ désigne le nombre de solutions de la congruence $Y^2 \equiv DX - X^3 \pmod p$ (ou, ce qui revient au même, de $Y^2 \equiv X^3 - DX \pmod p$), on a

$$N_4(D) = p - \left(\frac{D}{\bar{\lambda}}\right)_4 \lambda - \left(\frac{D}{\lambda}\right)_4 \bar{\lambda};$$

cette formule est due à Davenport-Hasse (1934), et a été redémontrée par Rajwade (1970); Morlaye (1972) vient de donner une version élémentaire de la démonstration de Davenport-Hasse. La courbe $Y^2 = X^3 - DX$, considérée comme variété abélienne de dimension 1 définie sur $\mathbf{Q}$, a servi de « banc d'essai » aux conjectures de Birch et Swinnerton-Dyer; voir Birch-Swinnerton-Dyer (1965), ou Cassels-Fröhlich, *Algebraic Number Theory*, chap. XII (Academic Press, 1967).

CHAPITRE 7

THÉORÈME D'AX

Le résultat central de ce chapitre est le théorème suivant, dû à Ax (1964), et qui précise le théorème de Chevalley-Warning (chap. 3, sect. 1.1):

THÉORÈME 1. — *Soient k un corps fini à $q = p^f$ éléments, F un polynôme de degré d, à n variables et à coefficients dans k, et b le plus grand entier* strictement *inférieur à n/d. Si alors N désigne le nombre de zéros de F dans k^n, N est divisible par q^b.*

La démonstration de ce théorème est un peu analogue à celle du théorème 1 du chapitre 6 (ou plus précisément de son corollaire 1): elle consiste (du moins en principe): (1) à exprimer N à l'aide de sommes de Gauss, donc d'entiers du corps L des racines $p(q-1)$-ièmes de l'unité; (2) à calculer la « valeur absolue $\mathfrak{P}$-adique » de ces sommes en chaque idéal premier $\mathfrak{P}$ de L au-dessus de p; (3) à en déduire enfin l'inégalité $|N|_p \leqslant |q^b|_p$, où $|\ .\ |_p$